



**KEN PAXTON**  
ATTORNEY GENERAL OF TEXAS

**Joint Statement of the Office of the Texas Attorney General  
and the 31<sup>st</sup> Judicial District Attorney's Office**

In January 2018, the Hemphill County Sheriff's Office requested the assistance of the Office of the Attorney General with the investigation into the death of Thomas Brown of Canadian, Texas. Since that time, investigators with the Special Investigations Group in the Attorney General's Office, along with other law enforcement agencies, have put thousands of hours of work into this case, interviewed numerous witnesses, and submitted various items of evidence to undergo forensic testing. Additionally, in early 2021, the Attorney General's Office established a Cold Case and Missing Persons Unit that also reviewed this matter enlisting independent experts to possibly identify any further leads that could be developed. As of today, this case remains a questionable death investigation without sufficient evidence to conclude that Tom Brown's death was attributed to a criminal act, an accidental death, or a suicide. It was initially thought that a formal grand jury investigation into this case might produce new evidence or leads but, after careful and thorough deliberation, we do not believe presenting this case to a grand jury at this time would be fruitful or ethical. There is insufficient evidence to establish probable cause. Further, the legal standard at trial of beyond a reasonable doubt, that Mr. Brown's death was the result of an intentional, or unintentional, criminal act, is not supported by any evidence collected at this time. It is the longstanding practice of the 31<sup>st</sup> Judicial District Attorney to not present suspicious deaths to a Grand Jury if evidence shows the death was the result of a suicide.

Because of the amount of public interest in this case, the amount of time that has elapsed, and the amount of erroneous information that has circulated around the investigation, we believe it is necessary to be open and transparent about the facts in this case. While it is not common practice to disclose evidence in a pending investigation, we believe providing a general synopsis of the known facts in the case will dispel conjecture and provide a thorough explanation for the inevitable, but frustrating, conclusion that this investigation has reached an impasse and should be suspended until such time as additional reliable evidence may be discovered.

Attached to this statement you will find a summary of the investigative actions that have taken place in this case along with a general overview of the evidence that has been developed and reviewed by law enforcement over the past several years.

The Honorable Ken Paxton  
Attorney General, the State of Texas

The Honorable Franklin McDonough  
31<sup>st</sup> Judicial District Attorney

# **CX9512431186 Thomas Brown Investigation**

## **Summary of Investigative Findings**

### **Investigative Actions Taken by the Office of the Attorney General from February 2018 to October 2021:**

Total Number of Items Submitted for Forensic Testing and/or Analysis: 35

Total Number of Witnesses Contacted or Interviewed: 71 individuals on at least 99 separate occasions

Total Number of Polygraphs Conducted: 9

Total Number of Formal Searches Conducted: 9

Total Number of Search Warrants and Subpoenas Issued: 150

Total Number of Trips to Canadian, Texas: 9

### **General Overview of Evidence Reviewed During the Investigation:**

#### **❖ RELEVANT TIMELINE INFORMATION (VERIFIED THROUGH MULTIPLE SOURCES OF FORENSIC DATA)**

- Wednesday, November 23, 2016, 6:04 PM -Thomas Brown leaves his house.
- 9:11 PM - Internet search for a suicide hotline on THOMAS BROWN'S phone.
- 11:26 PM - THOMAS BROWN'S Dodge Durango observed headed towards town.
- 11:28 PM to 11:36 PM - Last known credit card transaction by THOMAS BROWN at Fronk's Oil and Gas pumping gas.
- Thursday, November 24, 2016, 12:23 AM - THOMAS BROWN'S iPhone loses power (the phone dies, it is not shut off).
- 1:10 AM - Dodge Durango seen headed in the direction of THOMAS BROWN'S house.
- 1:11 AM - Dodge Durango seen headed back in the direction of town (away from THOMAS BROWN'S house).

- 5:28 AM - Dodge Durango seen headed in the direction of THOMAS BROWN'S house.
- 5:30 AM - Dodge Durango seen headed into town (away from THOMAS BROWN'S house).
- 5:56 AM - Dodge Durango presumably seen driving into the water treatment facility (never seen coming back out).
- 8:30 AM - Dodge Durango located at the water treatment facility.

#### ❖ ITEMS OF EVIDENTIARY INTEREST

- 11/24/16 - Dodge Durango belonging to THOMAS BROWN found
- Soil sample taken from apparent wet spot near driver's side of vehicle
  - Testing by the University of North Texas yielded no results
- .25 caliber casing found on floorboard of front passenger side.
  - Casing did not provide any forensic evidence. No latent prints could be identified on the casing and casing could not be tested further for DNA per DPS lab.
- 01/27/17 - Backpack belonging to THOMAS BROWN found containing his school-issued laptop.
  - Nothing of forensic value found on laptop.
- 10/14/17 - iPhone belonging to THOMAS BROWN found on (see additional information on iPhone below).
- 10/14/17 Gun case found.
  - Forensic testing by DPS-no profile could be obtained from hair samples found on the case
- Records produced from Apple, Inc. indicate that THOMAS BROWN'S iCloud account did not contain data that is commonly backed up such as iMessages and photographs. It is of interest because IP logs and data access logs were blank.
- Records from Facebook indicate THOMAS BROWN'S Facebook page had been removed. Per a representative from Facebook, removing a Facebook account can only be done with the account owner's password.
- January to February 2019 - Skeletal remains positively identified as THOMAS BROWN located in.
  - Partial skeletal remains were discovered on January 9, 2019, by PYNE GREGORY, former Hemphill County Deputy, at approximately 9:45 a.m. while he was on duty.
  - Other remains, though not all remains, discovered in OAG search on February 12, 2019.

#### ❖ BLOOD EVIDENCE FROM VEHICLE OWNED BY THOMAS BROWN

- Two small stains in the Dodge Durango were collected by HCSO and submitted for testing by DPS and were positively identified as THOMAS BROWN'S blood. One swipe on the driver's side door and a small swipe of blood in another area that will not be released. Neither swipe contained a significant amount of blood.
- Photographs of the interior of the vehicle taken on November 24, 2016 by Hemphill County Sheriff's Office (HCSO) depict a messy car with multiple pieces of debris all over the vehicle. No blood evidence was discovered or observed on these items and the vehicle components were dusty.
- When the Durango was recovered, no observations were made by anyone, (including family), that the vehicle had been thoroughly cleaned within the last 24 hours such as wet carpet or residual odor from cleaning products.
- When the Durango was returned to HCSO for further processing, more photographs were taken depicting the vehicle in the same condition as when it was recovered on November 24, 2016. The Texas Ranger assigned to the case made no observations that would suggest the vehicle needed to be processed for additional blood evidence. (Multiple photographs are attached.)
- The red markings depicted in the photos are paint and not blood. The investigative team learned that the students at Canadian High School painted the streets before football games and both red and yellow paint were found in THOMAS BROWN'S vehicle.

#### ❖ KLEIN INVESTIGATIONS & CONSULTING (KIC) LUMINOL TESTING OF DODGE DURANGO

- On 11-23-17, PHILIP KLEIN, a private investigator hired by PENNY MEEK, mother of the deceased, conducted his own luminol test inside the vehicle and concluded there was blood "all over the vehicle." The investigative team stands by its position that this test was not properly conducted, and the results are invalid.
  - Luminol does not require an alternative light source and must be done in darkness.
  - The second spot of blood only known by investigators was not discovered, photographed, or mentioned in the KIC test.
  - Photographs provided by KIC depict a car that appeared to be covered in blood, however, photographs also depict the individual conducting the test, believed to be PHILIP KLEIN, also covered in blood. This is likely because the blue light used during the testing was illuminating light against dark objects. [Photos attached.]
- On 11-30-17, KIC sent an email containing a memo stating KIC had conducted the luminol test, taken samples of what appeared to be blood, and explained that they would have the samples tested. [Memo attached.]
  - On 7-20-20, PHILIP KLEIN told SGT. KADING with the Office of the Attorney General that he had never heard back from the lab where he sent

the suspected blood swabs from the luminol testing but stated that he would follow up with the lab.

- On 8-17-20, SGT. KADING received a memo from PHILIP KLEIN explaining that he had conducted the luminol test using proper evidence retrieval and used a luminol product from Pioneer Forensics. [Pioneer Forensics Instruction Manual attached]. KLEIN stated that he used a blue light and yellow glasses during the testing, but per Pioneer Forensics, no alternative light source should be used. This memo further states that no blood samples were in fact taken because HCSO had told KIC to leave the scene untouched and not take samples from the vehicle.
- On 8-17-20, CHIEF DEPUTY BRENT CLAPP with HCSO told SGT. KADING that PHILIP KLEIN had called the week of August 10, 2020 asking which deputy had been present for the luminol test. KLEIN stated the deputy's last name was "Martinez." CLAPP advised that there were no deputies present for the testing and that they have never had a deputy named "Martinez."
- HCSO was never involved in the luminol test conducted by KIC. CLAPP forwarded SGT. KADING an email exchange between himself and KLIEN from December 4 and 5, 2017. On December 4, 2017, CLAPP asks KLIEN for any updates from KLIENS trip to Canadian, Texas two weeks prior, not yet knowing about the luminol testing. KLIEN tells CLAPP about the luminol test in the email exchange. (Email exchange attached.)

#### ❖ THOMAS BROWN'S IPHONE

- During a search conducted in October 2017, an iPhone was located that was later confirmed through digital forensics as belonging to THOMAS BROWN.
  - Phone was analyzed by the FBI, OAG Digital Forensics, and an independent digital forensics expert.
  - The phone contains THOMAS BROWN'S data. This data cannot be transferred from phone to phone because it contains internal applications that are connected to the IMEI of the device purchased from Verizon Wireless.
  - IMIE Number of Phone is xxxxxxxxxxx7160 and matches Verizon wireless records and box that phone came in provided by family.
  - SIM card # xxxxxxxxxxxxxxx3865 was activated with this iPhone and was verified by Verizon Wireless. This sim card has never been placed in another phone per Verizon Wireless.
- The search for a suicide hotline occurred at 9:11 pm. This entry cannot be altered on the phone because all activity is timestamped. [Report Attached]
- The phone died at 12:23 a.m. on November 24, 2016. It was not shut off.

- The phone never had power again until it was powered on by the FBI after it was discovered in October of 2017.
- The phone was in almost perfect condition- no scratches, nicks etc. FBI confirmed the moisture indicators had not been activated on the phone. Although it is not impossible the phone had been outside since November 24, 2016, it is not probable. The area where the phone was found had been recently mowed and had been mowed several times over the summer. Hemphill County received approximately 26 inches of rain from November 24, 2016 to October 14, 2017. [Sourced from <http://www.theweathercollector.com/>.] There was also a severe ice storm on January 15, 2017.
- PENNY MEEK texted a witness in January of 2017 asking if their child knew the passcode to THOMAS BROWN'S phone and clarified this was a four-digit number. The child began asking numerous friends if they had the passcode. The circumstances surrounding the passcode created misinformation that HCSO had asked for the passcode in 2017. The investigative team has confirmed that HCSO did not ask the family for the passcode in 2017. [Redacted text message string attached.]
- The digital forensic evidence indicates that it is more likely than not the battery case was on THOMAS BROWN'S phone the night of his disappearance. The phone records show a "plug in"/charging event earlier in the evening while THOMAS BROWN was at his house. There is never an "unplug" event the rest of the evening suggesting that the "plug in" event was the result of the built-in battery charging case attached to the phone and not another type of charging source that would require an "unplug" event before relocating the phone. Further evidence to support this theory are that THOMAS BROWN'S friends stated he was religious about keeping his phone charged and that he almost always had his battery charging case on the phone.

#### ❖ HEMPHILL COUNTY SHERIFFS' OFFICE (HCSO)

- PENNY MEEK and PHILLIP KLEIN stated they were shown a photograph of THOMAS BROWN at the gas pumps at Fronk's Oil and Gas on the night of his disappearance by NATHAN LEWIS. This prompted the investigative team to determine if the photo existed and to try to locate the photograph.
- The Hemphill County Sheriff's Office was shut down for over 24 hours while investigators of the OAG physically searched the office and forensically downloaded and analyzed all target computers and the server. All in-car camera data was obtained. No evidence was found to support that the photo existed on any HCSO equipment at any time.
- It is the opinion of the investigative team that the Fronk's Oil and Gas Video was mishandled, and that SHERIFF NATHAN LEWIS failed to document the collection and eventual loss of this evidence. His report about the video was not written until January of 2018. Criminal intent for Tampering with Evidence cannot be established. Several other witnesses, including people not associated with the Hemphill County

- Sheriff's Office, claimed to have seen the video or had credible information about the video, however, the video would not have provided any footage of THOMAS BROWN getting gas. The camera that would capture this view was facing the ground.
- PYNE GREGORY found the skull belonging to THOMAS BROWN at approximately 9:30 am on January 9, 2019, not in the middle of the night as some have stated.
  - No evidence was established that any HCSO employee was involved in the disappearance or death of THOMAS BROWN at any time.

#### ❖ THE PARTIAL SKELETAL REMAINS FOUND IN JANUARY AND FEBRUARY 2019

- **The remains do not support any finding in the cause or manner of death.**
- Remains examined by the University of North Texas (UNT) noted the following:
  - Skeletal remains positively identified through dental records as THOMAS BROWN.
  - MAXILLA- Comminuted fracture of the posterior maxillary socket for teeth 8-10, however, no fractures of the associated facial wall socket. This is consistent with a blunt force trauma impact to the anterior teeth, but no determination could be made if this trauma occurred perimortem or early in the postmortem stage. UNT determined the trauma appeared to be from front to back. Evidence of postmortem scavenging noted though it is unlikely that scavenging caused this injury.
  - ZYGOMATIC ARCH and greater wing of the SPHENOID- Skeletal damage consistent with blunt force trauma that may have resulted from a single application of force. Neither post or early perimortem can be excluded as the cause of the damage.
  - Regarding all other bones recovered -No skeletal injuries resulting from perimortem trauma were observed, however, the majority of the remains were not recovered. Evidence of postmortem scavenging noted.
- UNT concluded that the trauma observed on the skull could not be attributed to a single or to multiple incidents if the trauma occurred perimortem without further information.
- The investigative team determined that although a technical finding of “blunt force trauma” was observed in the maxilla, zygomatic arch, and greater wing of the sphenoid, these injuries would not have caused death or incapacitation. Furthermore, it was determined that the injuries could not be solely attributed to a perimortem incident.
  - The investigative team asked experts at UNT if there could have been a gun shot into the head through the base of the neck without any evidence on the skull. UNT's expert opinion is that this did not occur because there would have been other indicators.

## ❖ EVIDENCE SUPPORTING CAUSE OR MANNER OF DEATH

### ➤ CRIMINAL ACT/HOMICIDE

#### ▪ Physical Evidence

- .25 caliber casing found on passenger floorboard; however, the casing did not provide any forensic evidence.
- Trace amount of blood located in the Durango that was THOMAS BROWN'S blood.
- Blunt force trauma to the maxilla, zygomatic arch, and greater wing of the sphenoid but undetermined whether this trauma occurred peri or postmortem.
- Items belonging to THOMAS BROWN located in various places miles away from where his vehicle and skeletal remains were located.

#### ▪ Circumstantial Evidence

- No known motives or threats.

### ➤ ACCIDENTAL DEATH

- No evidence other than blunt force trauma located on the skeletal remains but inconclusive without further evidence to support the trauma occurred perimortem.

### ➤ SUICIDE

#### ▪ Physical Evidence

- Search on 11-23-16 at 9:11 pm for a suicide hotline.
- Blunt force trauma to the maxilla, zygomatic arch, and greater wing of the sphenoid but undetermined whether this trauma occurred peri or postmortem.

#### ▪ Circumstantial Evidence

- Multiple witnesses stated THOMAS BROWN struggled with his mental health surrounding issues concerning his family history and his faith.
- Evidence from THOMAS BROWN'S phone showed he frequently joked about suicide or dying to his friends.
- One witness stated to investigators that only a few months before BROWN disappeared, he was seeking help with mental health issues. This witness offered to help BROWN get therapy and drive him to Amarillo for confidentiality purposes. Per the witness, BROWN declined because he did not want to tell his mother, and he was still a minor.
- Evidence shows that THOMAS BROWN had a fixation on wearing diapers stemming from his childhood that was known to his family and a few close friends. The investigation revealed that this fixation was a major stressor in BROWN'S life that he had kept secret from friends for a long period of time. Brown had recently confided in a few friends about the diaper fetish in the six months leading up to his disappearance (verified by phone records). It should be noted that the investigative team determined that the diaper fetish had little to no relevance in the criminal investigation and should be disregarded as sensationalism.



- THOMAS BROWN had recently been told that his grandfather committed suicide off Lake Marvin Road and not that he died from a heart attack as he previously believed.
- Recent incidents including quitting football, breaking up with SAIGE PENNINGTON, and where to attend college considered sources of stress in BROWN'S life.
- When PENNY MEEK is first interviewed by HSCO, she stated that she believed her son had committed suicide by playing the "choking game."
- Instagram post by THOMAS BROWN highlighting both Kirk Cobain and Judy Garland who both committed suicide.

## ❖ THE UNEXPLAINED and CONTRADICTING EVIDENCE

- THOMAS BROWN'S Dodge Durango
  - Through video enhancements by the FBI, the Dodge Durango was verified to be driving around town at approximately 1:10 a.m. on November 24<sup>th</sup> and again at 5:28 a.m., near the intersection of Birch and 2<sup>nd</sup>. The vehicle is then presumably seen driving into the sewage area at 5:56 a.m. (and never coming out). If THOMAS BROWN was behind the wheel of the Durango at these times, he would have been driving from the time he was pumping gas at Fronk's, (around 11:30 p.m.) until the Durango is last seen at 5:56 a.m. without having the use of his cell phone (the phone died at 12:23 a.m.), even though a charging cord was found in his vehicle
- On the evening of THOMAS BROWN'S disappearance, TUCKER BROWN, brother of THOMAS BROWN, rode around with former HCSO Deputy PYNE GREGORY from approximately 4:00 a.m. until 6 a.m.
  - The family of THOMAS BROWN has told numerous media sources and investigators that TUCKER BROWN rode around with GREGORY because GREGORY needed TUCKER BROWN to show him where SAIGE PENNINGTON, the ex-girlfriend of THOMAS BROWN, lived. Evidence shows that TUCKER BROWN called HCSO at 3:33 a.m. and requested to ride with a deputy, which is verified through phone records and dispatch logs.
  - The family has also stated that about 15 minutes before the Durango pulled into the sewage area that GREGORY and TUCKER drove through the pavilion area and TUCKER noticed the gate to the sewage area was open.
  - Video at the pavilion does not show any vehicles driving through the pavilion area from 3:45 am until the Durango presumptively pulls in past the gate at 5:56 a.m.
  - GREGORY'S report also stated that TUCKER actively kept him from that area.
  - A recovered iMessage from TUCKER BROWN'S iCloud account, at 5:47 a.m. from TUCKER TO PENNY MEEK states, "We drove out to Saige's, to the Y, and then to the lake. We still haven't found anything." Video confirms that TUCKER was dropped off at approximately 5:56 a.m.
- Items belonging to THOMAS BROWN located in various places miles apart along Lake Marvin Road and not found all together with the Dodge Durango or the skeletal remains

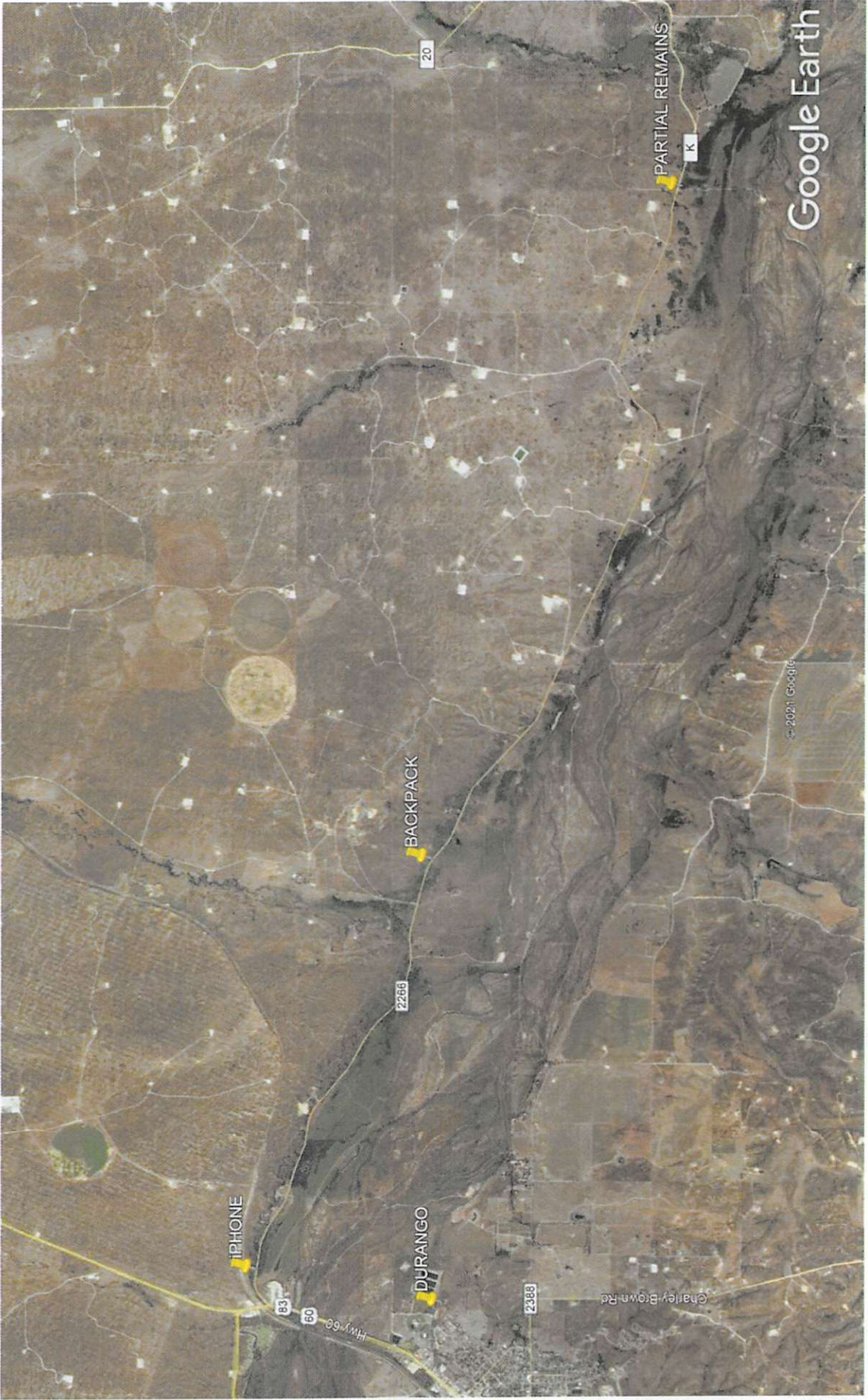
as you would expect in an apparent suicide. No items found near the skeletal remains or the Durango that could be attributed to the method of committing suicide.

- Various witnesses indicated deception on polygraph exams. Some of these same witnesses have given contradictory statements about seemingly irrelevant facts over the course of the investigation.
- Digital forensics indicate it is more likely than not that THOMAS BROWN had his battery case on his phone the night of his disappearance. Phone records show his phone would have had a charging/ “plug-in” event prior departing his home around 6:04 p.m. that evening. Because there is never an “unplug” event later that same evening, it would seem to indicate that BROWN turned his charging case on while at his house (as opposed to plugging his phone into a charging cable connected to an outlet and then unplugging it before leaving the house) and then left the house with the phone while the case was still charging the phone. The phone is later found without a case and BROWN’S mother has stated the case has been in her possession since BROWN’S disappearance. To date, the case has not been produced to investigators.
- Per a search warrant issued to Apple, Inc., THOMAS BROWN’S iCloud account contained very little data while TUCKER BROWN’S account had thousands of photographs, messages, and other data (verified through digital forensics). The brothers shared an iCloud account. Per a search warrant issued to Facebook, THOMAS BROWN’S Facebook account was deleted-no information could be obtained on when the account was deleted. During the investigation, PENNY MEEK provided information to law enforcement that PHILLIP KLEIN had taken down THOMAS BROWN’S Facebook account. When the investigative team asked PHILLIP KLEIN if he had taken down the account, he denied doing so and stated he thought PENNY MEEK had taken down the account.

## ❖ CONCLUSION

- Friends of THOMAS BROWN who were with BROWN, or in communication with BROWN, on the night of his disappearance include: KALEB KING, CHRISTIAN WEBB, MICHAEL CASELTINE AND SAIGE PENNINGTON. These individuals have fully cooperated with this investigation and are not considered to be persons of interest in this case at this time.
- The investigative team has determined that CHRISTOPHER JONES is an unreliable witness who has told multiple versions of stories over the years. All statements were fully investigated. JONES has been accounted for on the night of November 23, 2016. No credible evidence currently exists that JONES is a person of interest in this case.
- NATHAN LEWIS and PYNE GREGORY are accounted for on the evening of THOMAS BROWN’S disappearance (verified through the search conducted at HCSO, phone records and video evidence.) There is currently no credible evidence to suggest that LEWIS and GREGORY are persons of interest in this case.
- Search warrant affidavits are open records and all search warrant affidavits served in this case are attached to this press packet.

- A suspended case is still considered an open case and no other documents outside of this press packet will be released at this time.
- This investigative summary does not contain all evidence investigated or known by the OAG investigators in this case and should not be viewed as a document reflecting all evidence in the case. This document is meant to inform the public of the significant and contentious issues surrounding the investigation into the death of THOMAS BROWN. This Office is releasing this investigative summary because it believes it is in the best interest of the public, witnesses in the investigation and, most importantly of THOMAS BROWN, to disseminate factual and credible information that has been gathered after a thorough and exhaustive investigation over the past several years.



Google Earth

© 2021 Google

ORIGINAL SCENE PHOTOGRAPHS HCSO 11-24-16



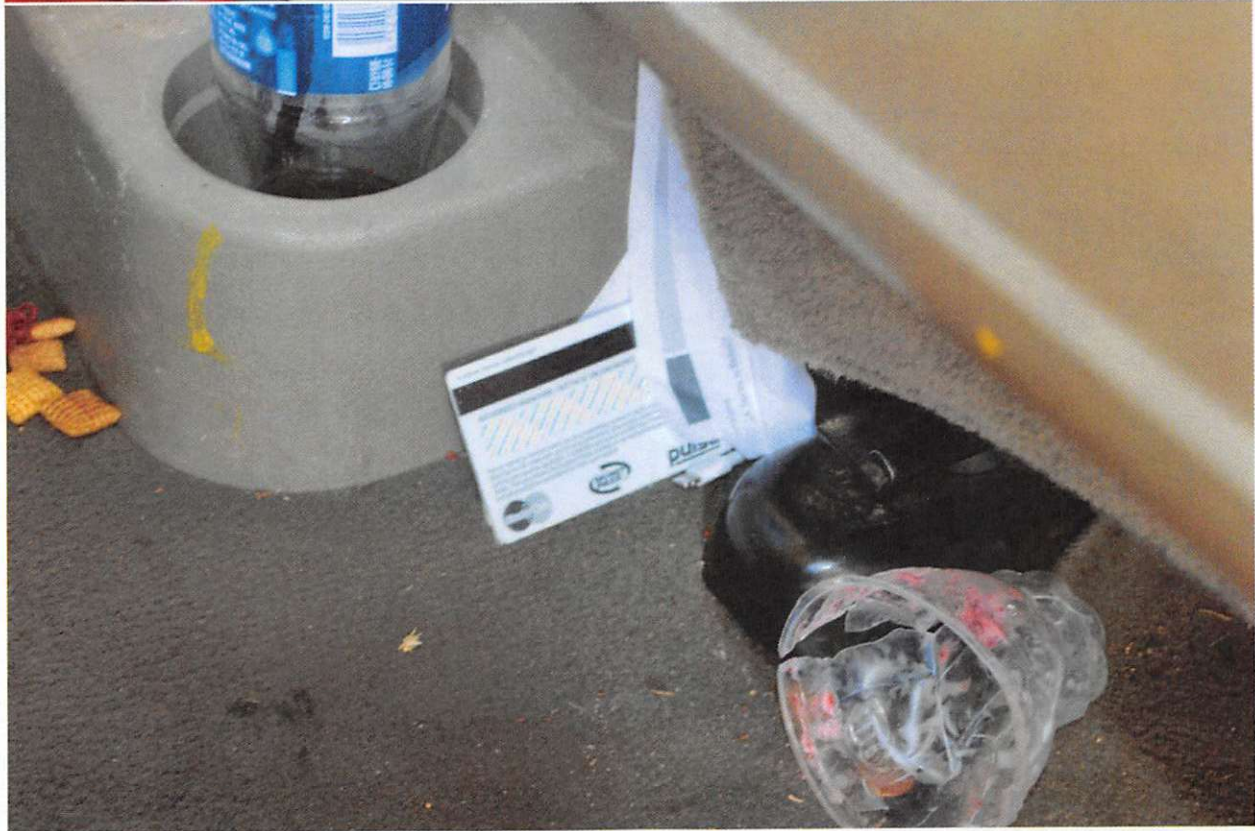
ORIGINAL SCENE PHOTOGRAPHS HCSO 11-24-16



ORIGINAL SCENE PHOTOGRAPHS HCSO 11-24-16

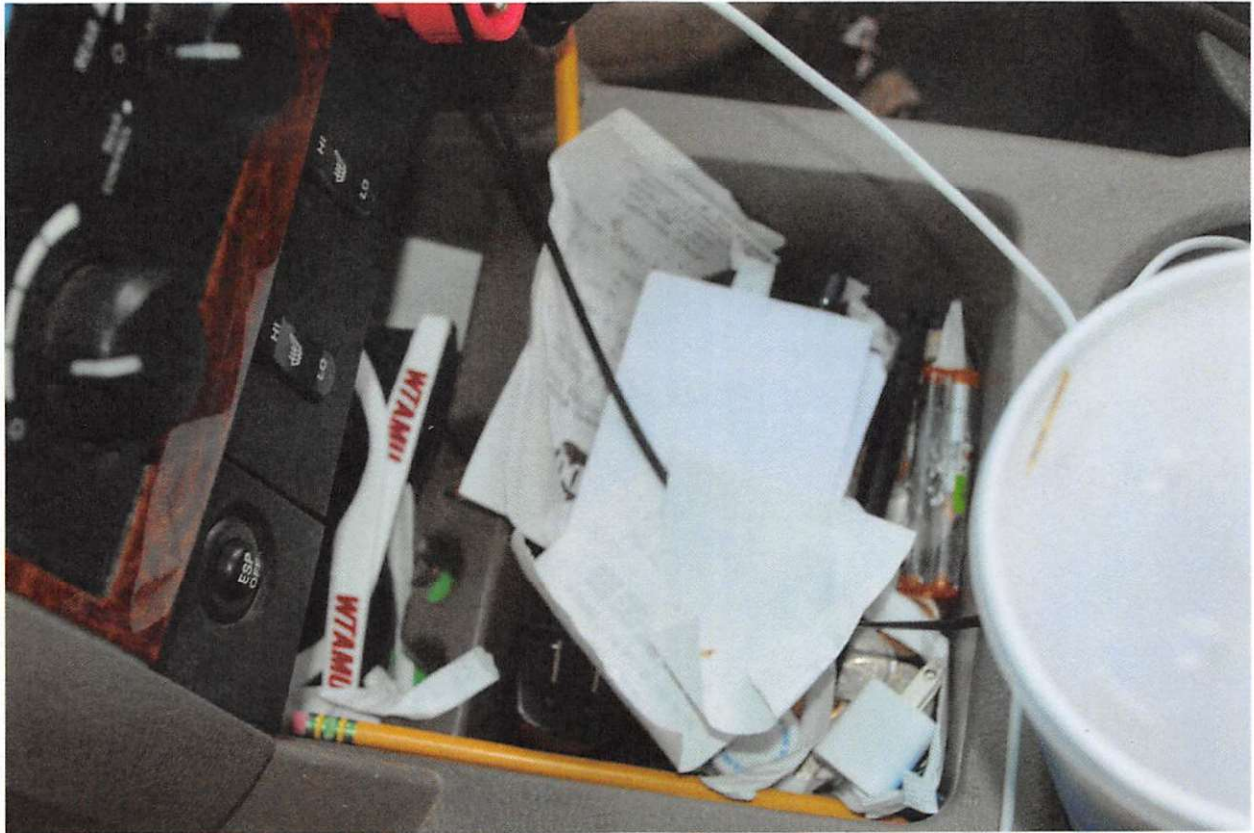


ORIGINAL SCENE PHOTOGRAPHS HCSO 11-24-16





ORIGINAL SCENE PHOTOGRAPHS HCSO 11-24-16



DURANGO RE-EXAMINED AT HCSO WITH HELP OF DPS TEXAS RANGERS ON 12-5-16



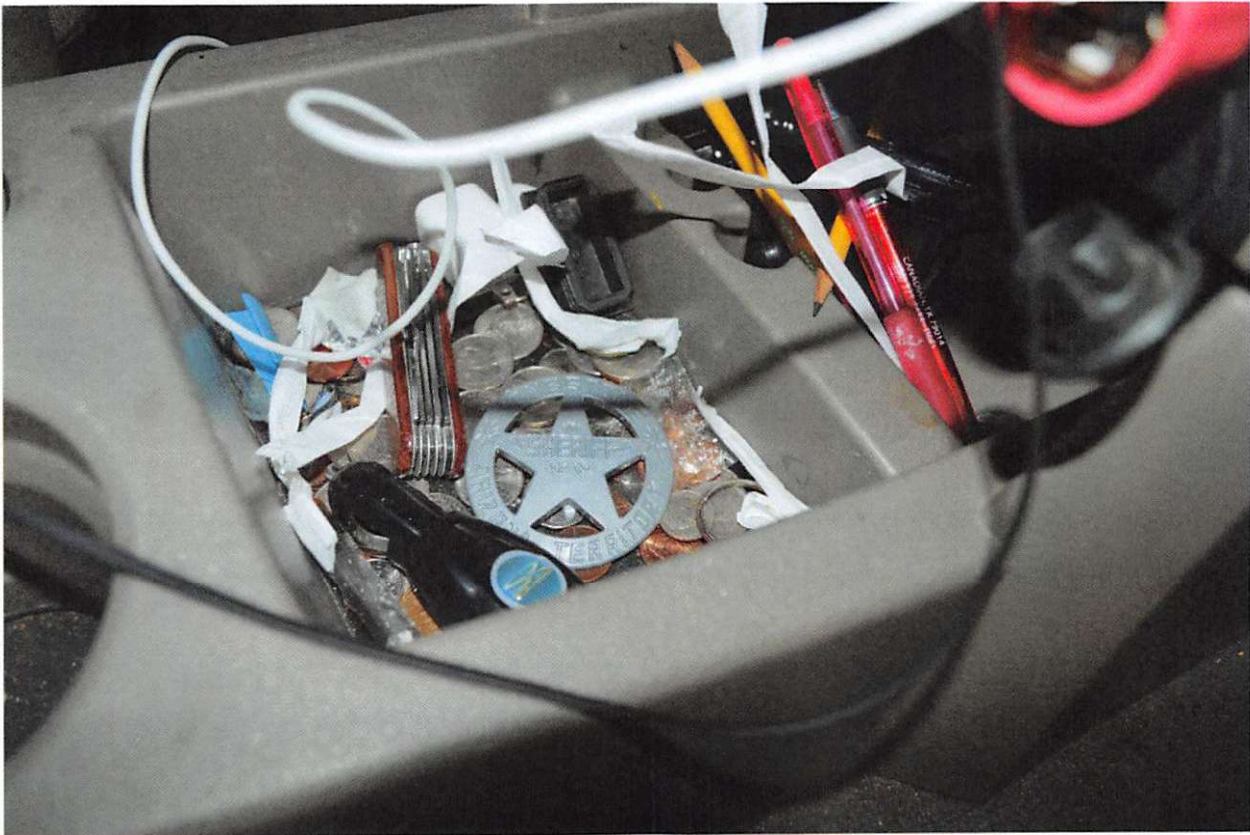
DURANGO RE-EXAMINED AT HCSO WITH HELP OF DPS TEXAS RANGERS ON 12-5-16



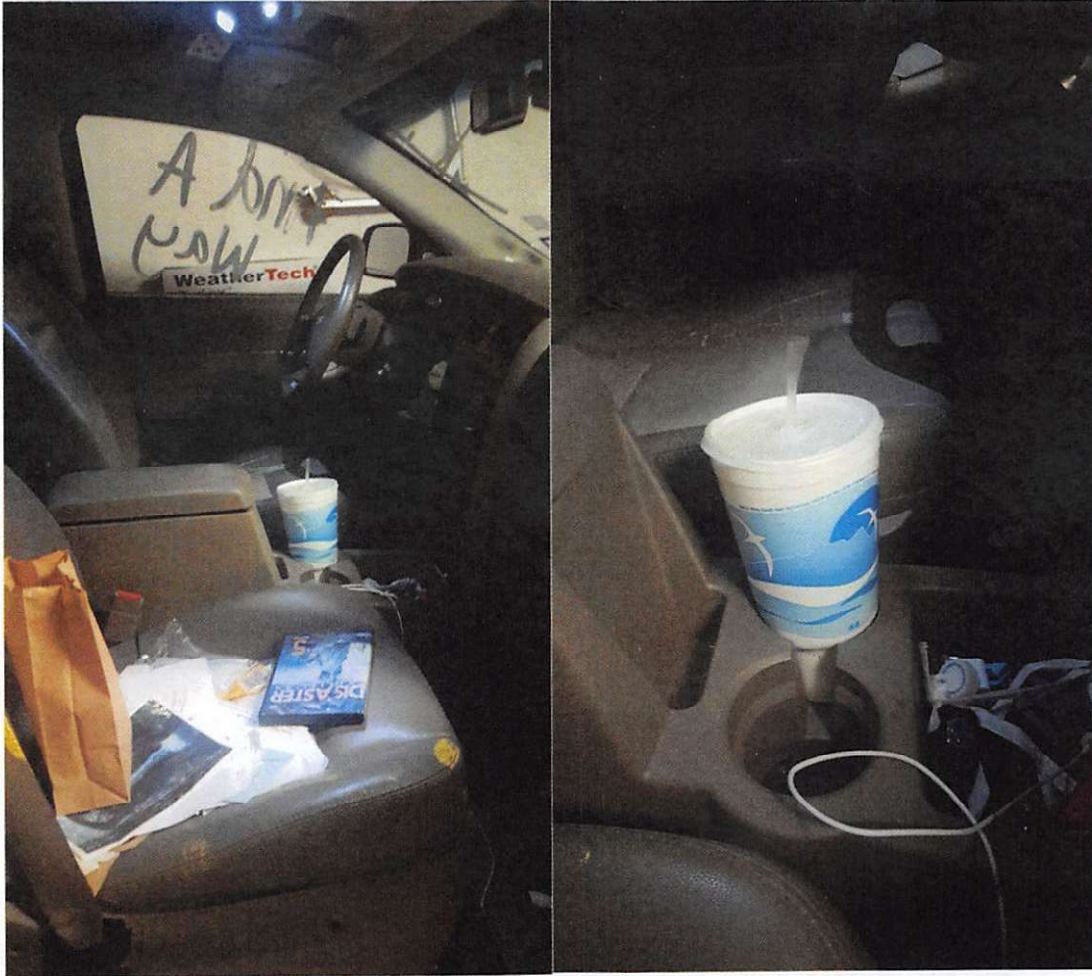
DURANGO RE-EXAMINED AT HCSO WITH HELP OF DPS TEXAS RANGERS ON 12-5-16



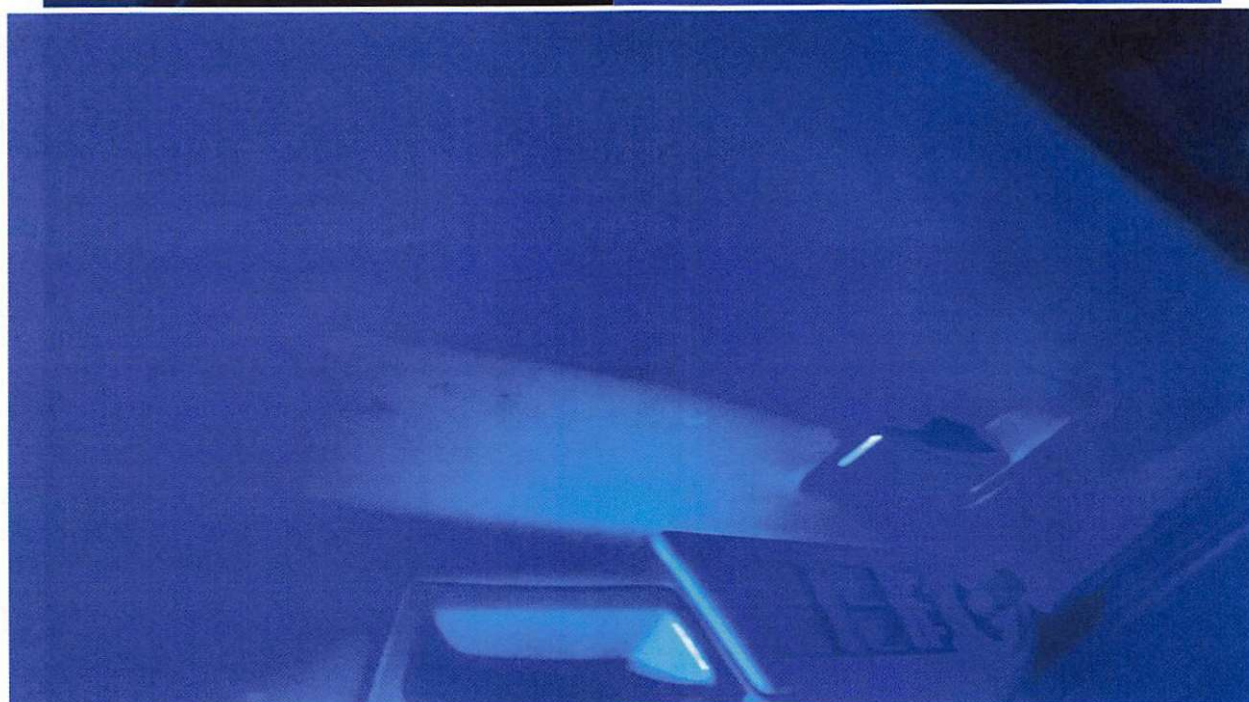
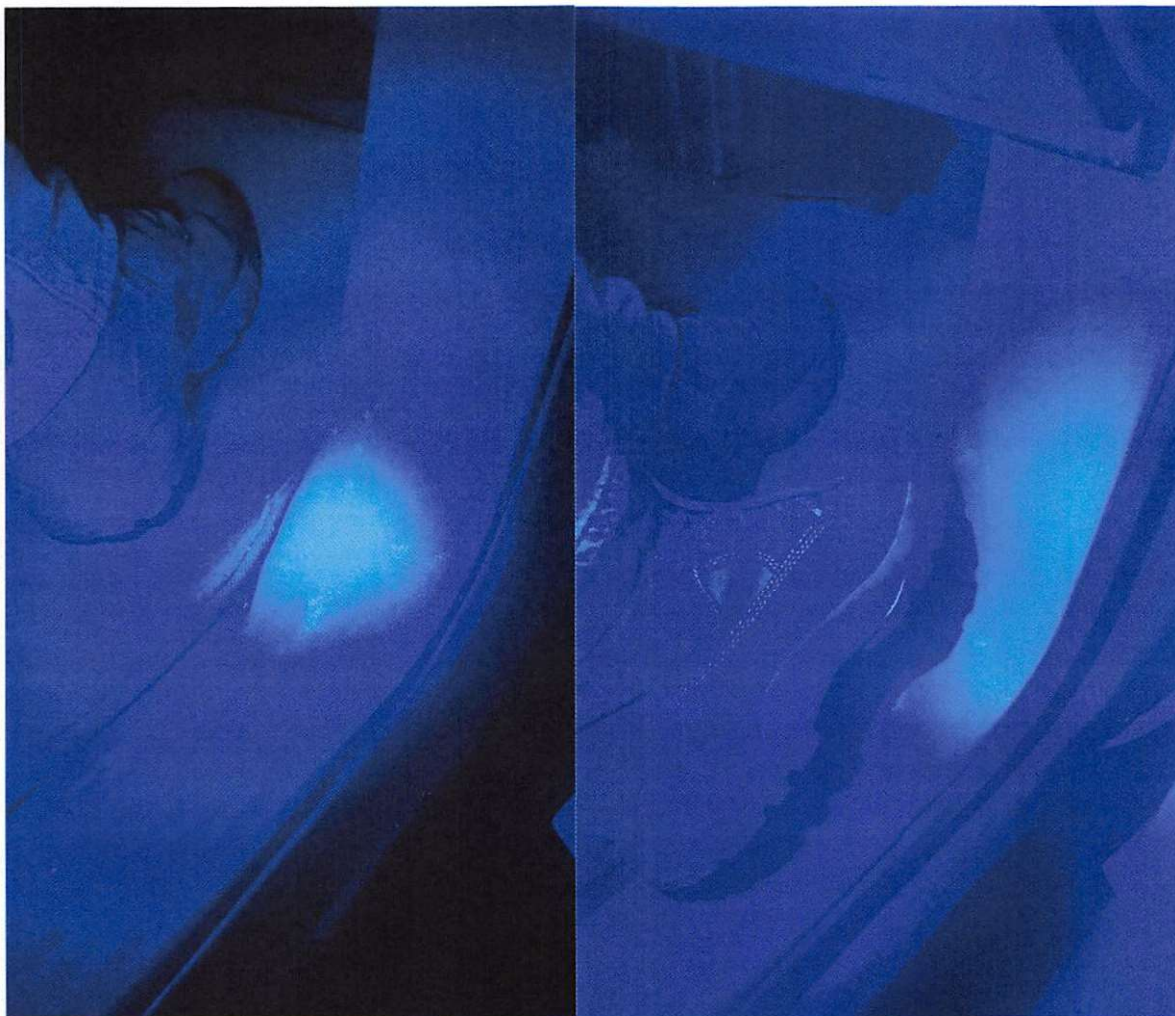
DURANGO RE-EXAMINED AT HCSO WITH HELP OF DPS TEXAS RANGERS ON 12-5-16



KLEIN INVESTIGATIONS LUMINOL TEST 11-23-17



KLEIN INVESTIGATIONS LUMINOL TEST 11-23-17

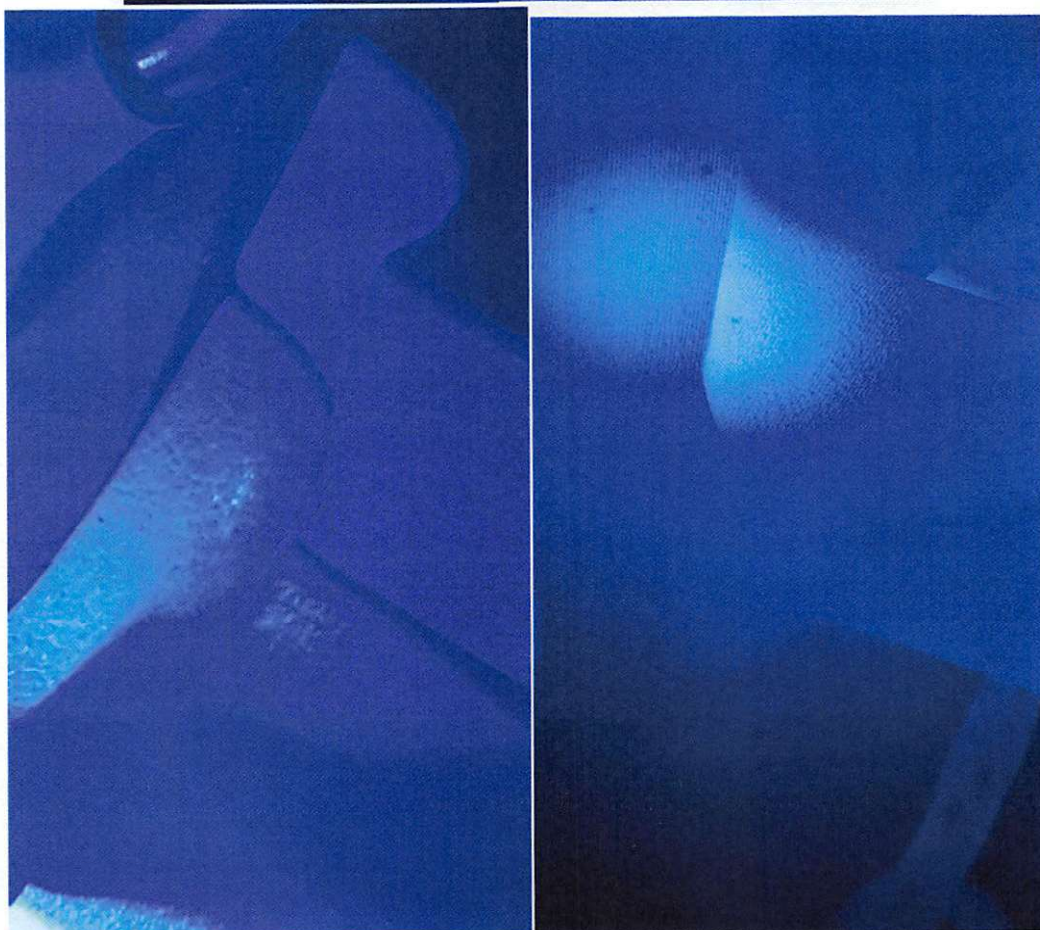


KLEIN INVESTIGATIONS LUMINOL TEST 11-23-17





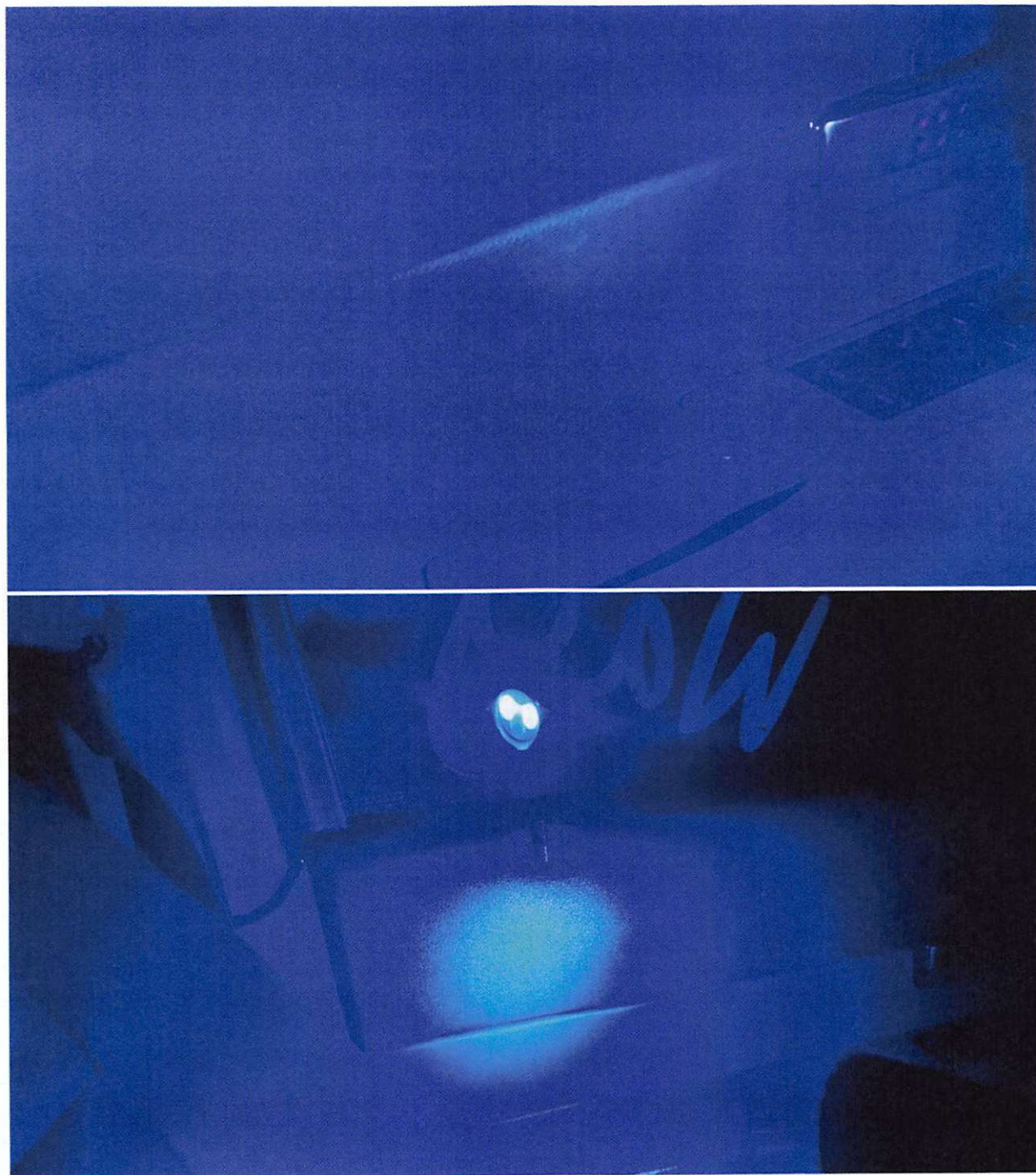
KLEIN INVESTIGATIONS LUMINOL TEST 11-23-17



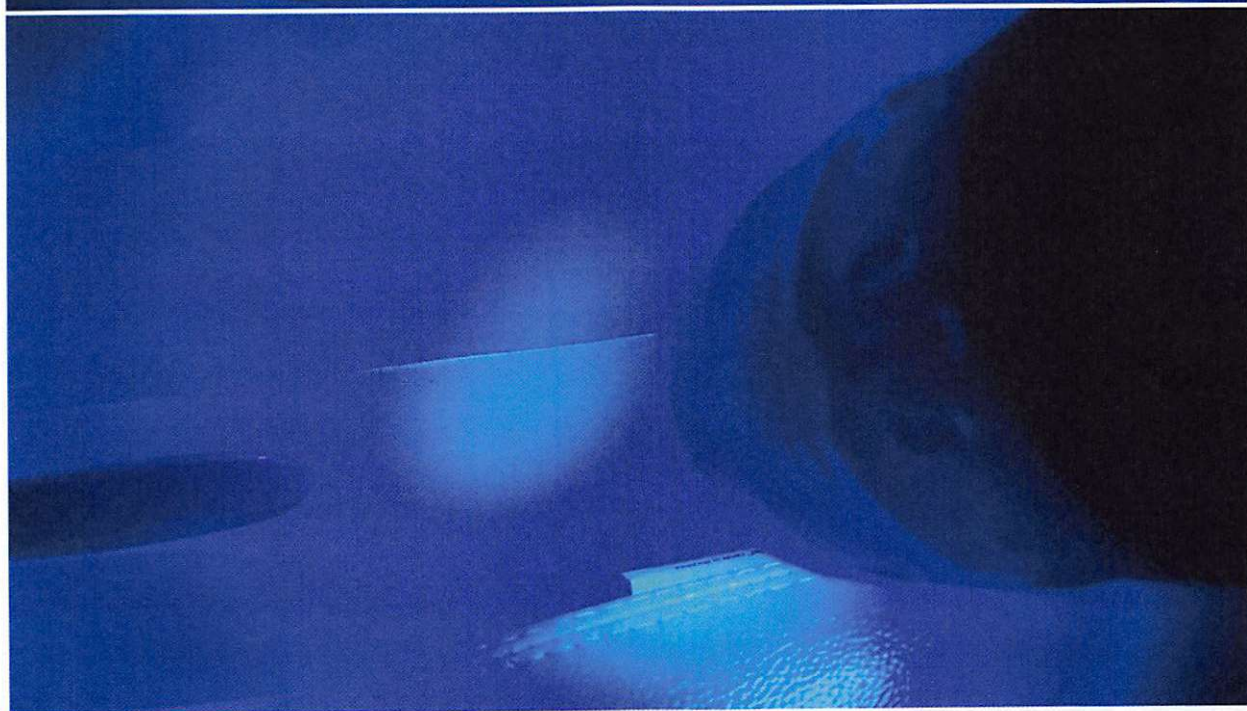
KLEIN INVESTIGATIONS LUMINOL TEST 11-23-17



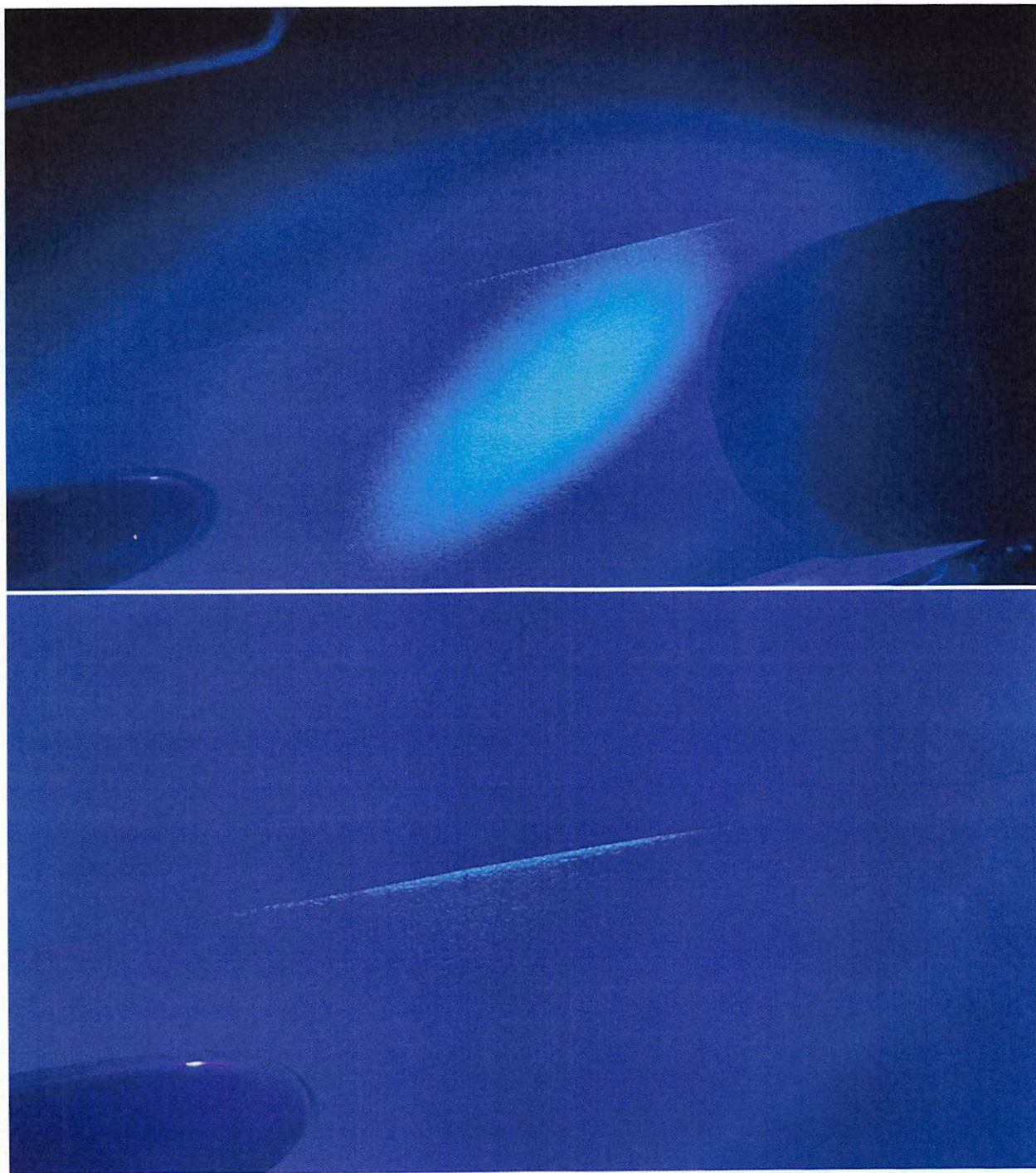
KLEIN INVESTIGATIONS LUMINOL TEST 11-23-17



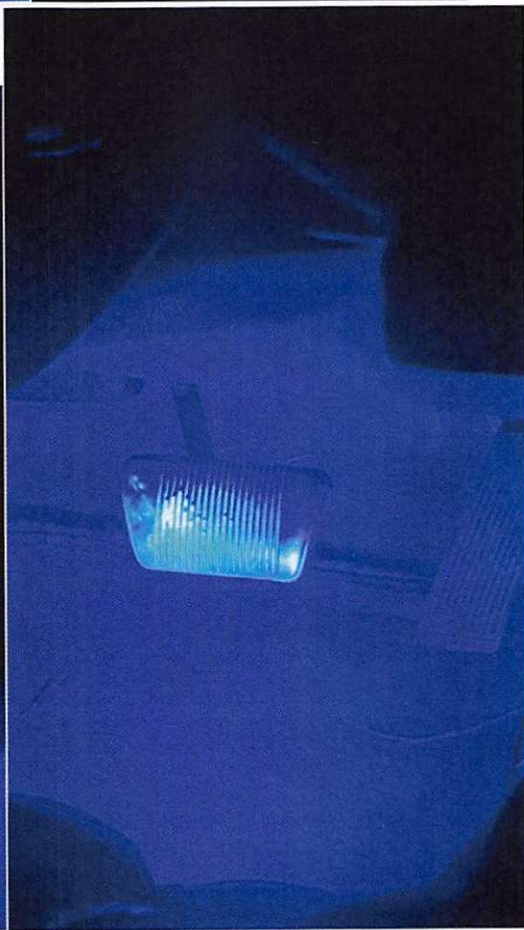
KLEIN INVESTIGATIONS LUMINOL TEST 11-23-17



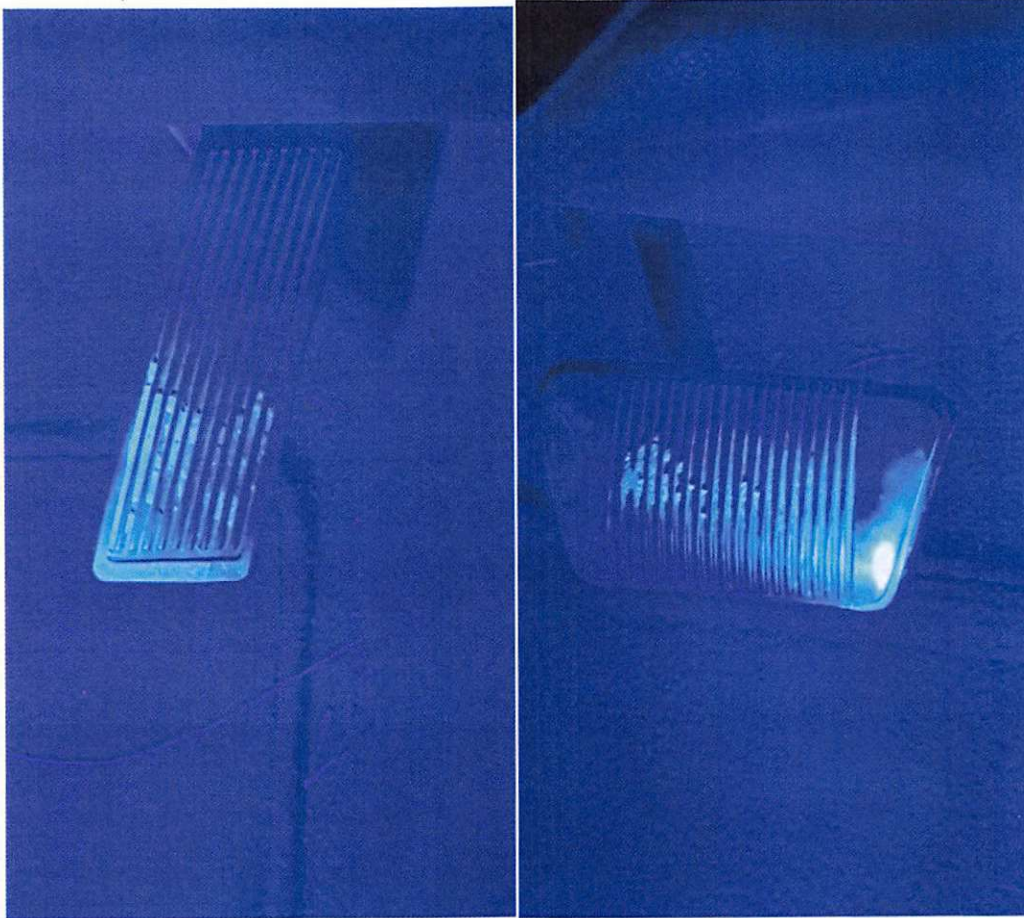
KLEIN INVESTIGATIONS LUMINOL TEST 11-23-17



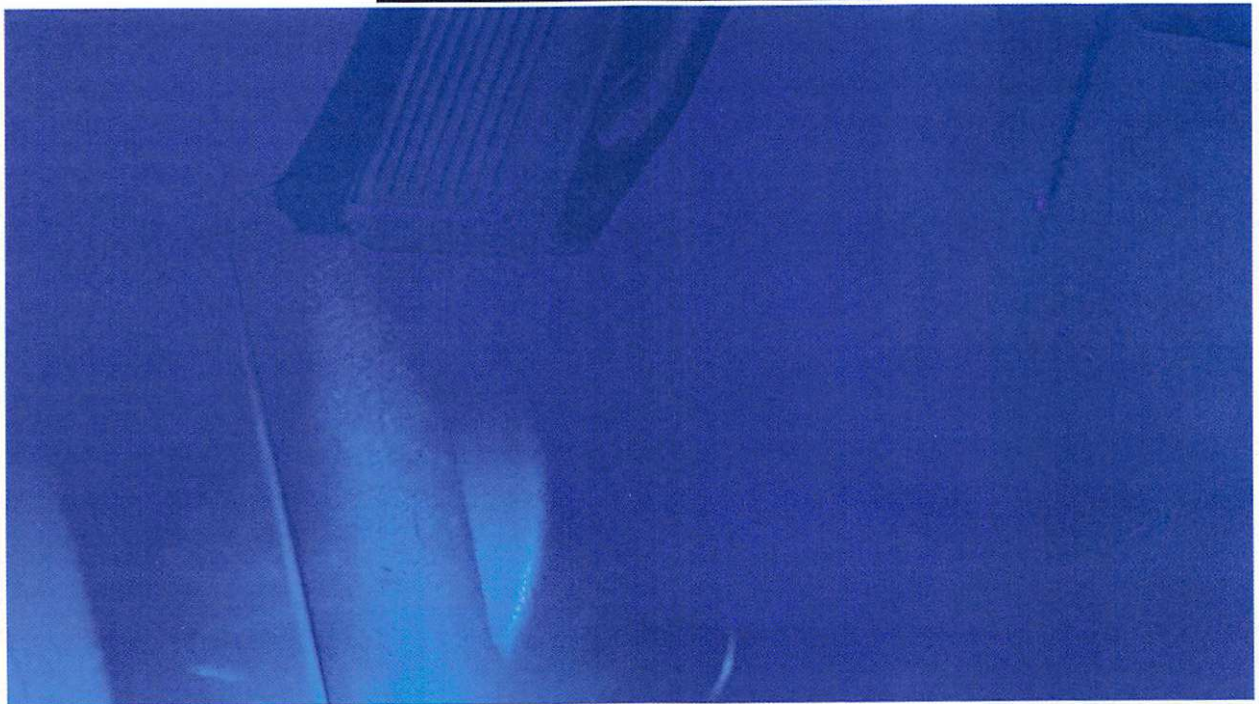
KLEIN INVESTIGATIONS LUMINOL TEST 11-23-17



KLEIN INVESTIGATIONS LUMINOL TEST 11-23-17

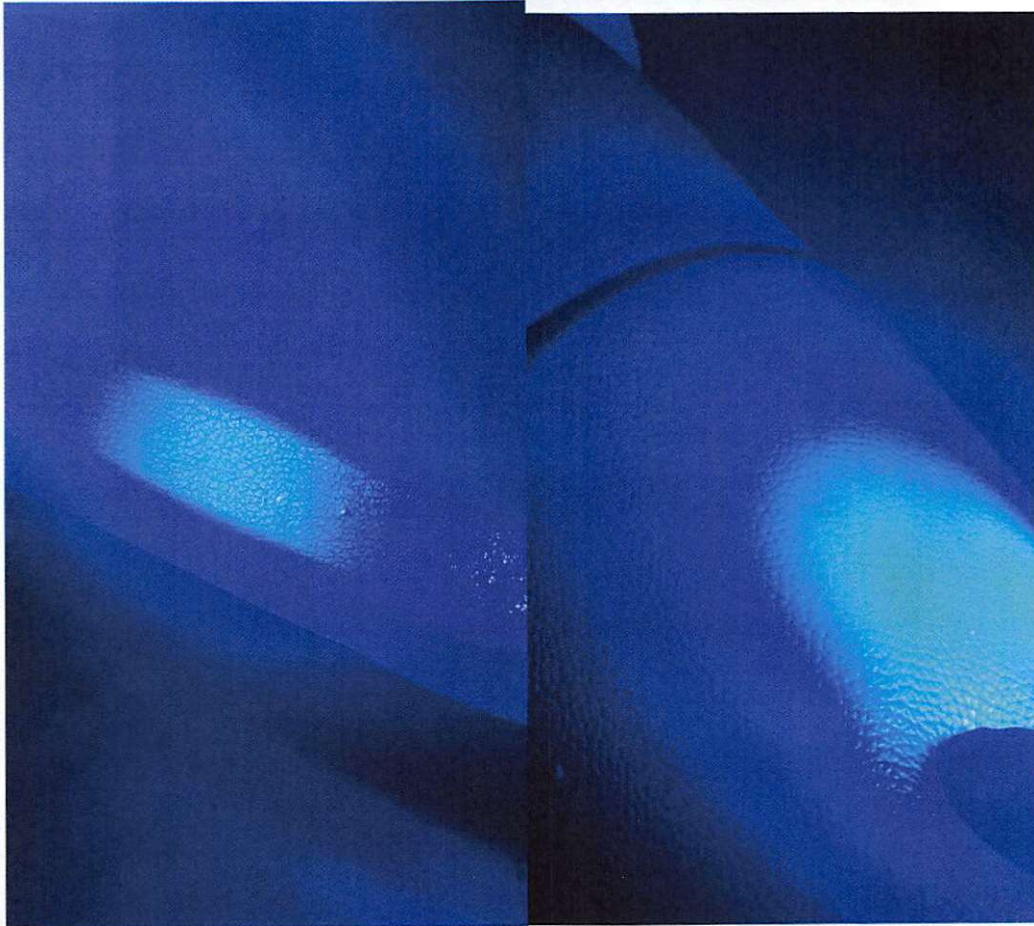
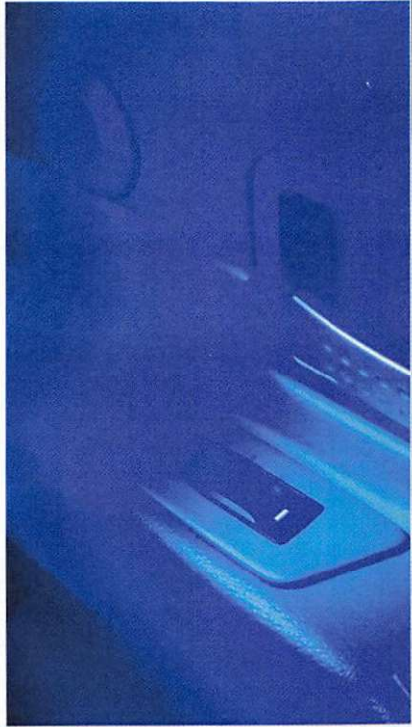


KLEIN INVESTIGATIONS LUMINOL TEST 11-23-17

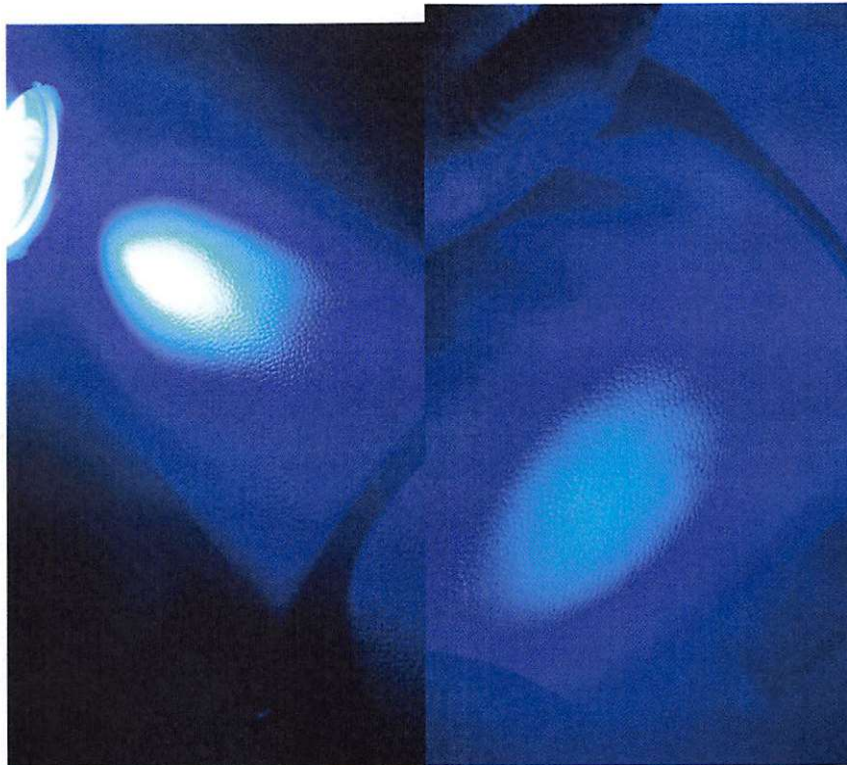




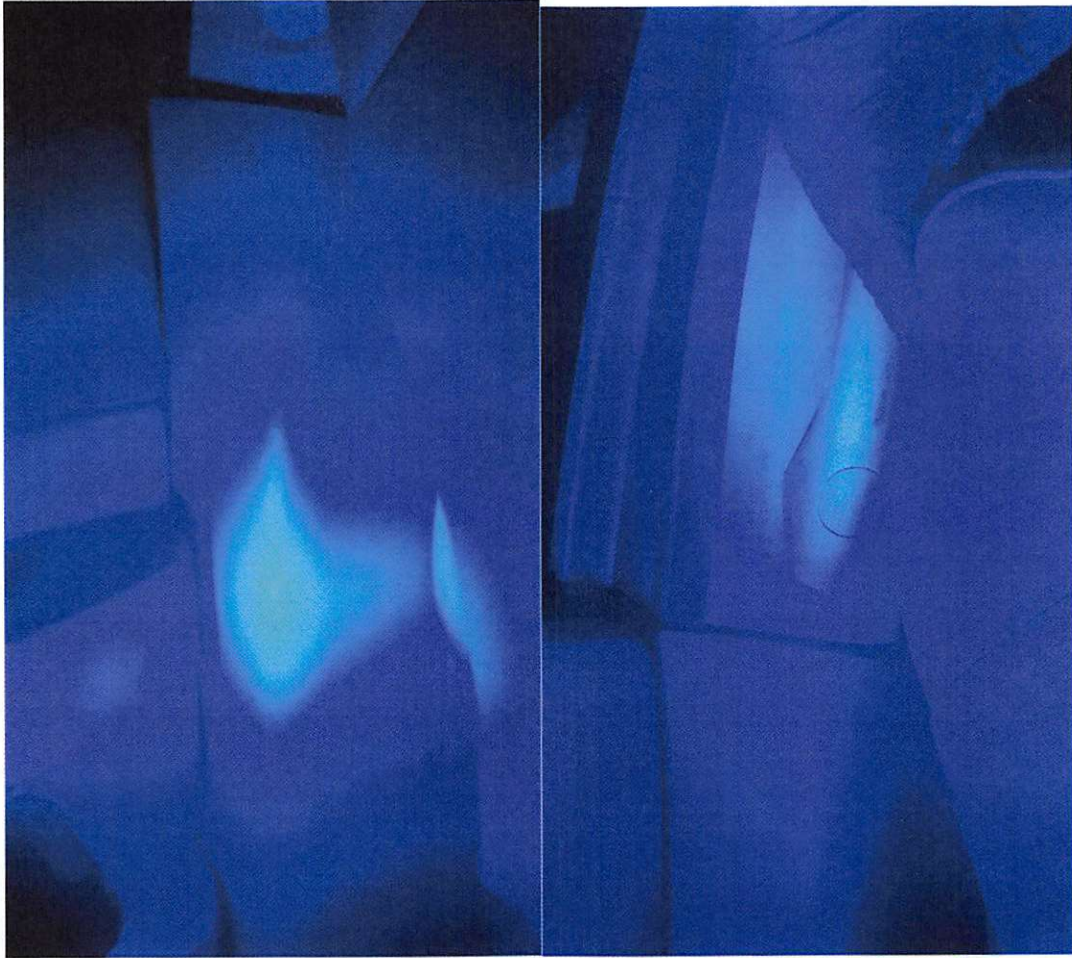
KLEIN INVESTIGATIONS LUMINOL TEST 11-23-17



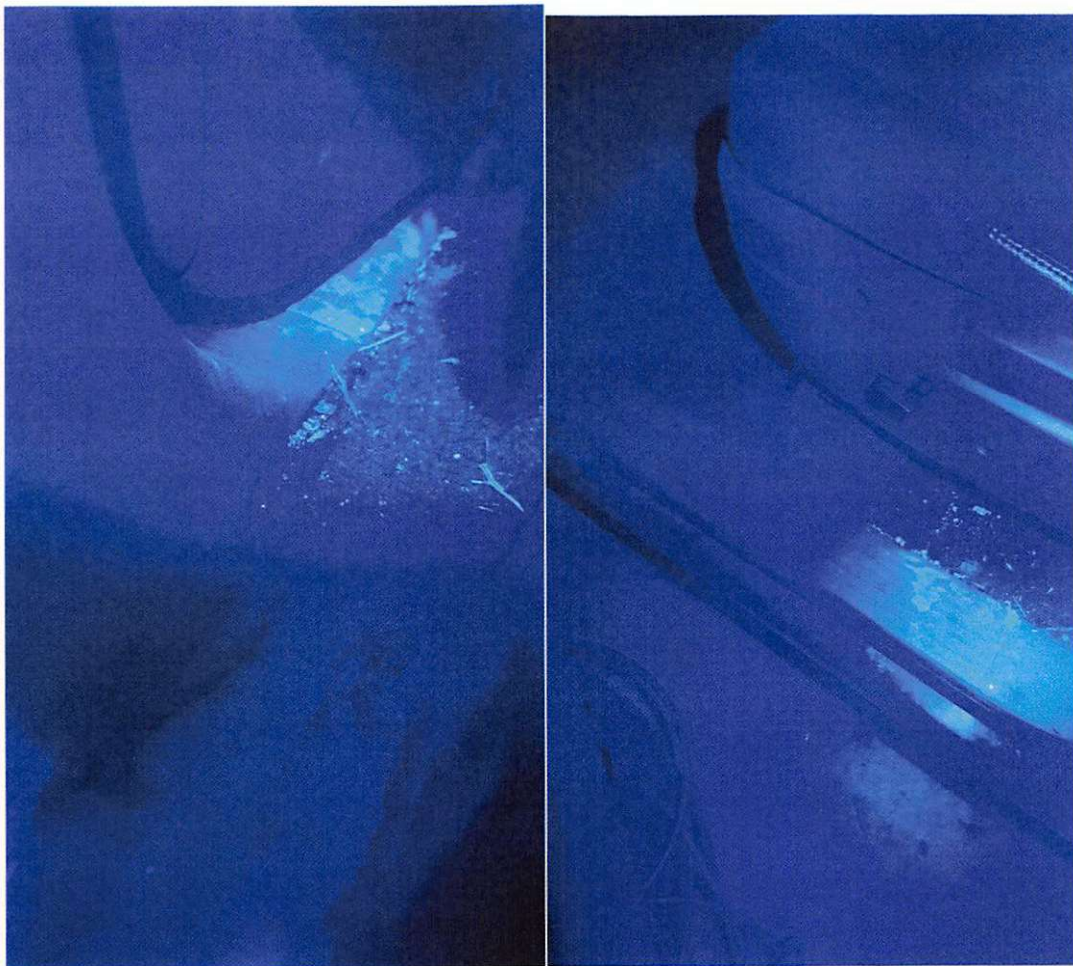
KLEIN INVESTIGATIONS LUMINOL TEST 11-23-17



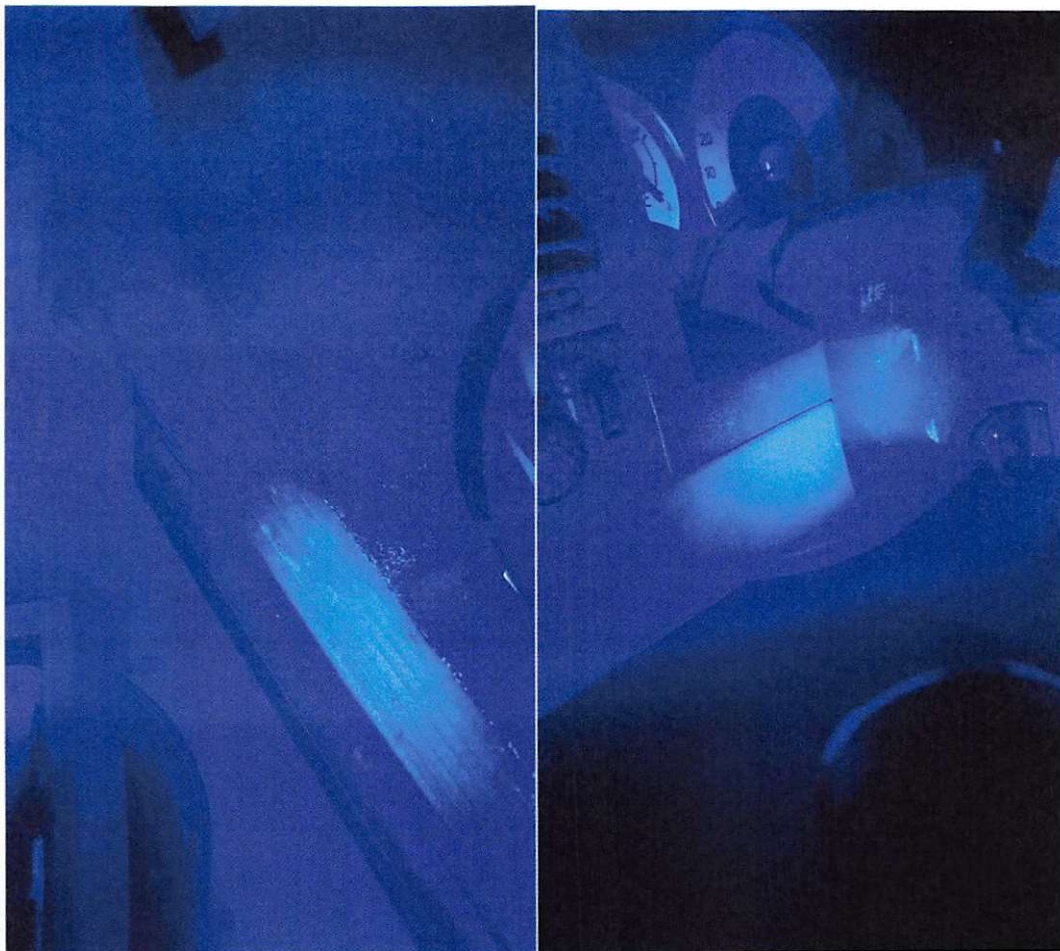
KLEIN INVESTIGATIONS LUMINOL TEST 11-23-17



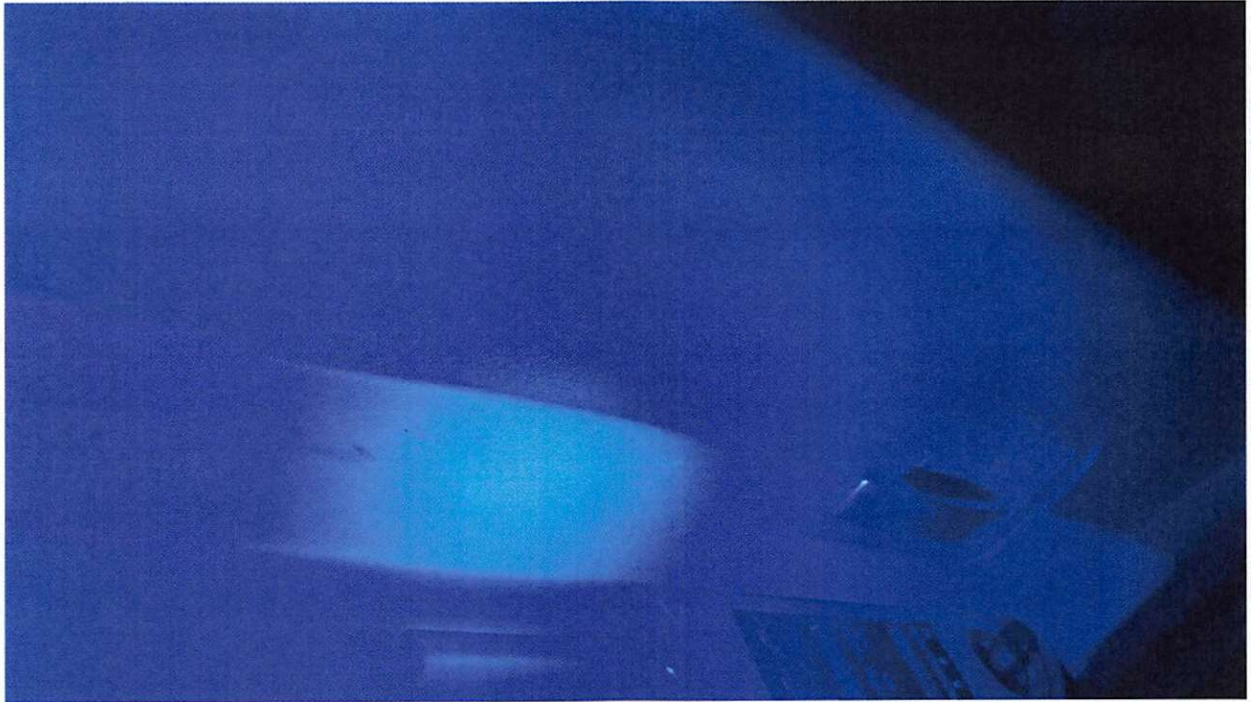
KLEIN INVESTIGATIONS LUMINOL TEST 11-23-17



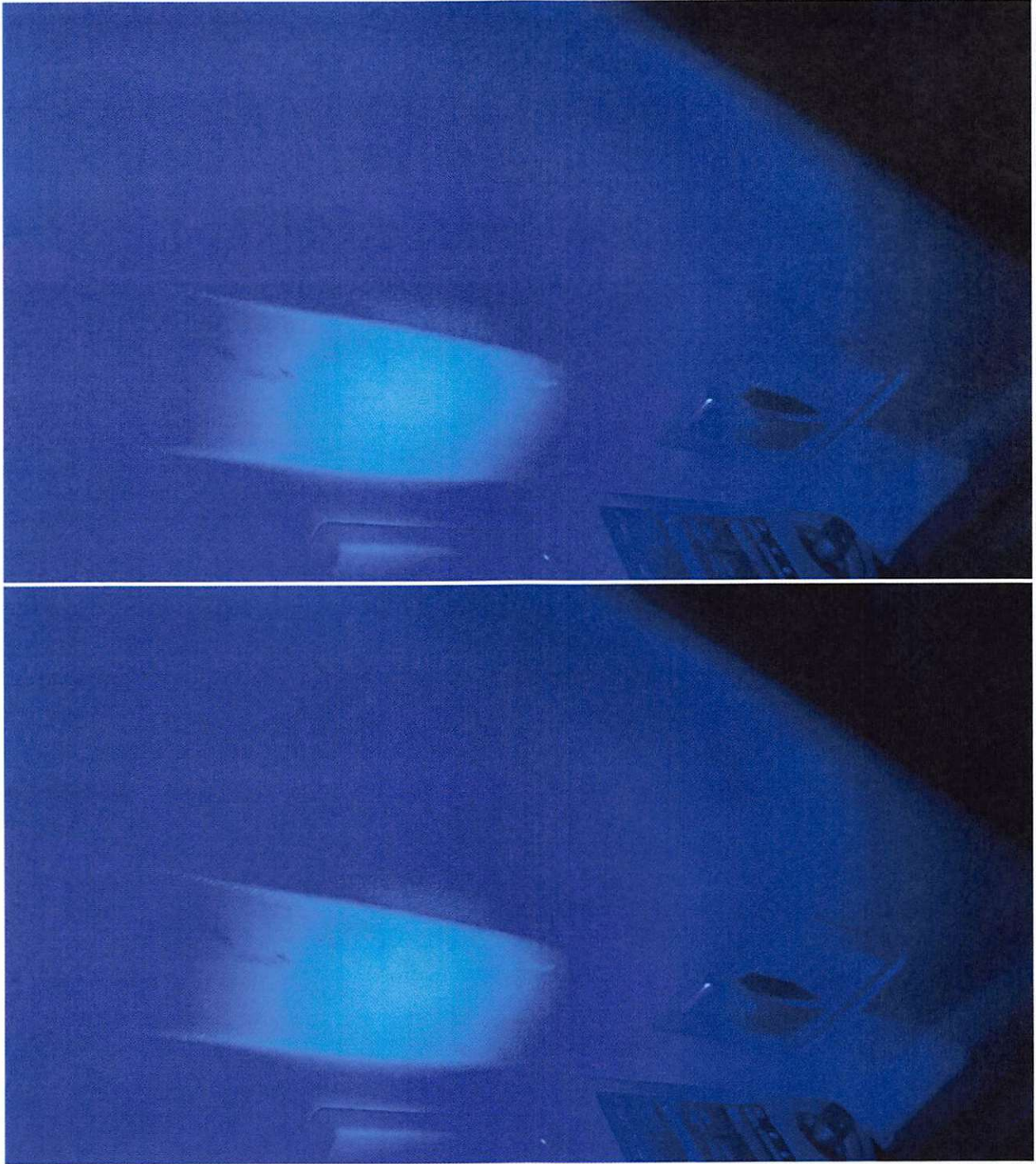
KLEIN INVESTIGATIONS LUMINOL TEST 11-23-17



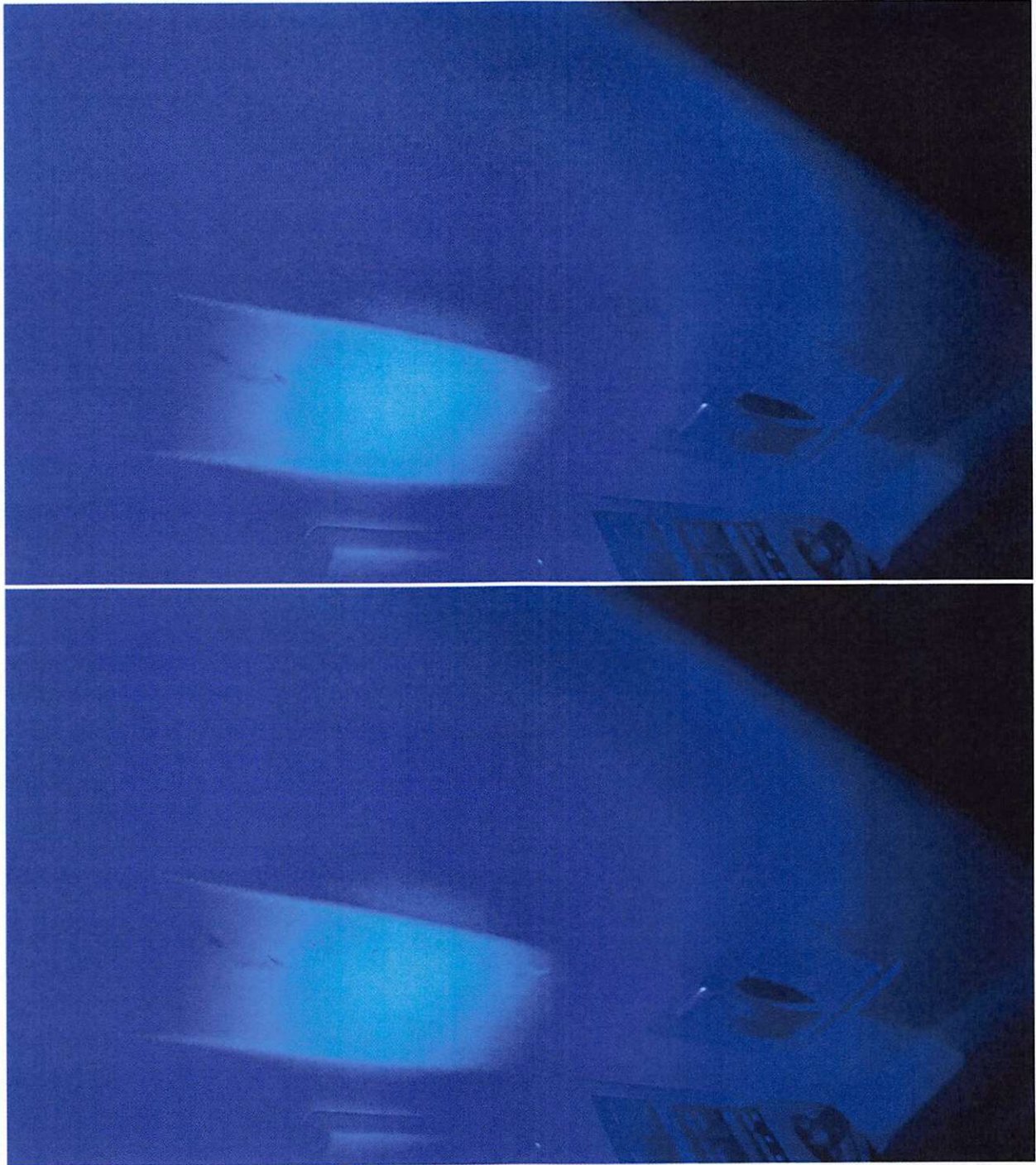
KLEIN INVESTIGATIONS LUMINOL TEST 11-23-17



KLEIN INVESTIGATIONS LUMINOL TEST 11-23-17



KLEIN INVESTIGATIONS LUMINOL TEST 11-23-17







## Law Enforcement Memo

**To :** Ranger Mike Smith  
The Texas Department of Public Safety

**From :** Philip R. Klein, TPLI-PPO

**Subject :** Re-Review : Tom Browns Auto

**Date :** November 30, 2017

### Background and History

Investigators with KIC Texas have canvassed the auto Mr. Brown used the night of his disappearance. Investigators with HCSO and DPS – TR have also canvassed the auto. Post the final canvass by LE – KIC Texas requested of the family that they put the auto in the garage and hold it there until further noticed as KIC Investigators wanted to do one more sweep on the auto.

On November 23, 2017, KIC Investigators obtained permission from the owners of the auto to inspect it and do a luminal test on the interior. The final inspection began at 6:43 p.m. at the family home in Canadian, Texas.

### Report To Law Enforcement

Investigators broke down the auto to four parts – being front dash, front seat / passenger area, back seat (middle), and rear. Investigators used a D-43 scope blue light – with photo. The following are the results :

#### Front Dash

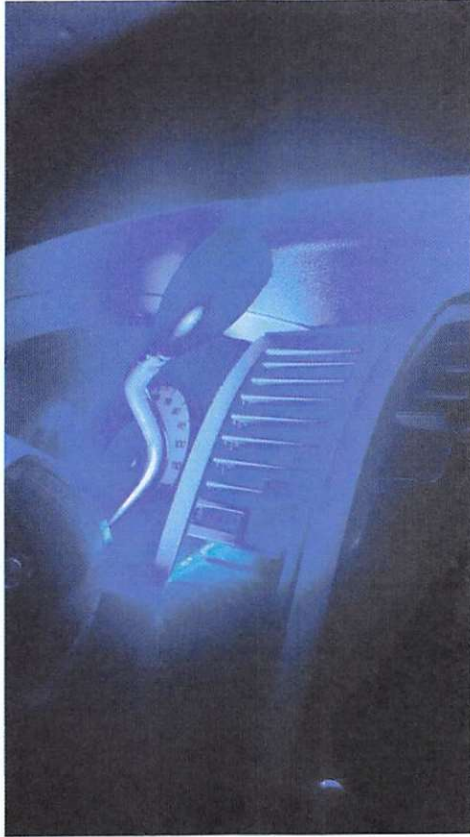
Investigators were able to find a positive return on the following :



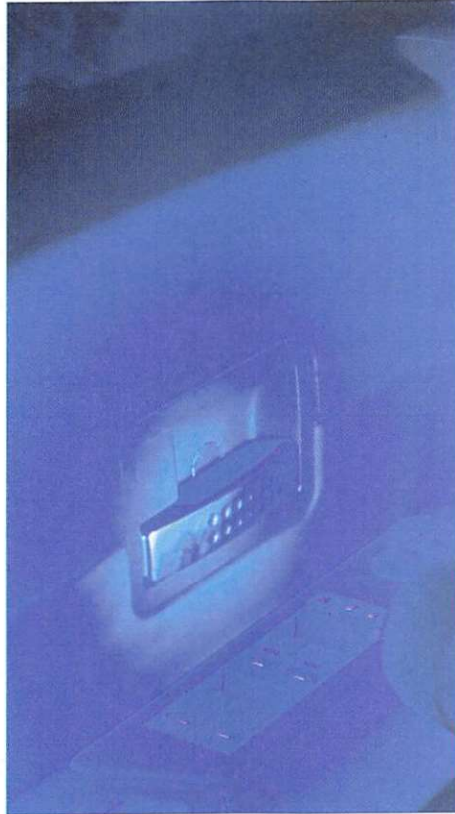
**Front Left – Positive Reading**



**Spatter (wipped) – Between AC Control And Radio**



**Swip On Steering Column**



**Swipe On Drivers Door**



**Swipe Drivers Door**



**Drivers Door Droplets / Swipe**

**Front Seat / Passenger Area / Drivers**



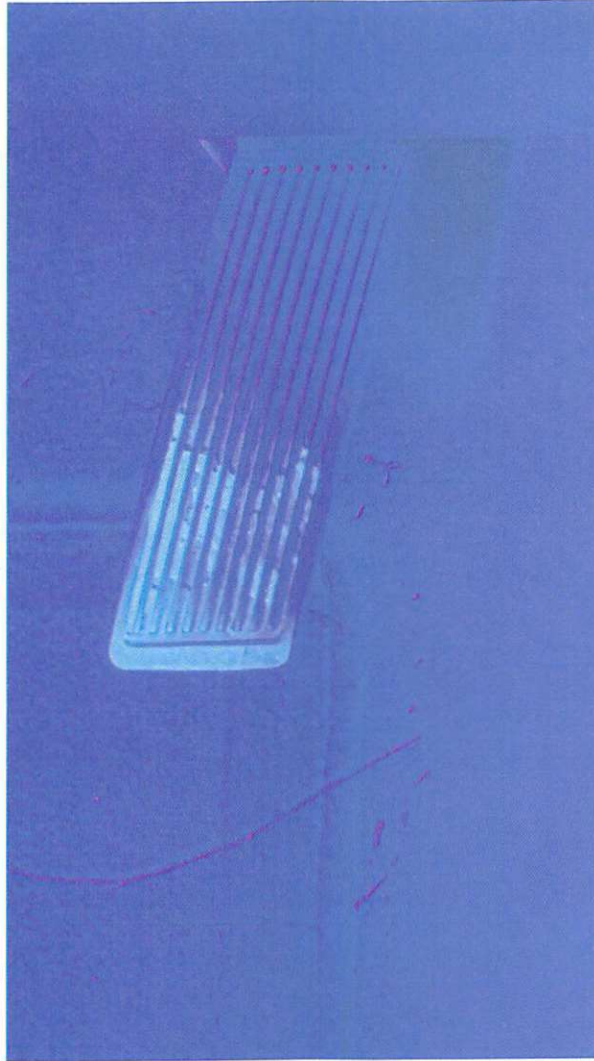
**Right Front Passenger Entry**



**Secondary View Pass**



**Brake Peddle**



**Accelerator – Positive**



**Swip – Arm Rest Bench (Cleaned)**



**Heavy Droplets Between Drives Seat / Door Guard / Back Seat**



**Exterior View : Front Drivers Seat**





**Postive : Smear**

**Report Overview**

Investigators have reviewed the evidence – and we believe that with the positive finding of blood and its compare to the subject Thomas Browns being positive – we believe that the returns that are associated with the luminal test – are positive. Samples were taken of each found location and will be submitted for testing for blood pathogins.

If the positive site readings are positive for blood we believe the following :

- 1) Subject Brown was injured possibly by gunshot while sitting in the front seat. We deem this from the dropletts herein submitted and the .25 cal shell found in the auto.
- 2) There was some type of an attempt at cleaning the auto before the auto was submitted to LE or KIC. This is obvious with the smear. Again meaning there was more blood than first thought.
- 3) That there was a substance that looks like a blood smear on the bottom of a subjects shoe – which indicates a large quantity of blood (if found to be).

- 4) There was more blood (or substances of a pathagin) in the auto than first thought. This indicates a large injury not compadible with life.
- 5) There is a spatter pattern and smear that can now be found in the front drivers compartment. This is clear indication of some type of serious wound. This is not just a smear from a small cut.

If you need any further information please let us know.

PRK/w



**Investigators Memo**

**To :** Rachel Kading  
Office of the Attorney General

**From :** Philip R. Klein, TPLI-PPO

**Subject :** Requested Information :

- [REDACTED]
- (2) Luminol Certification and Report – Toms Auto
- (3) Samples / Chain of Evidence From Auto

**Date :** August 11, 2020

**Background and History**

We have been asked to report to the OAG the information that has been listed above. This request comes to us regarding the information taken by our investigative team that may be in our possession.

**Information Resources Request**

The following is our information responsive to the request.

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

### **Luminol Certification and Report Regarding Toms Auto**

In November of 2017, investigators Klein and Holmes obtained entry to the auto (Durango) that was used by Tom the night of his disappearance.

The auto had been secured by the family and put into a garage. Early, the auto had been left in the street in front of the home. The auto had been searched by KIC and the HSCO. As well, investigator Trace Sargent and her K9 Dog Chance had searched the auto. K9 Chance had alerted to the area around the auto, as well, inside the back area and both front seats. Chance did not alert to the far back of the auto. Please see the attached photos.

On November 23, 2017, the auto was secured and draped under proper evidence retrieval protocols. Luminol product by Pioneer Forensics was sprayed in the front compartments. Proper Yellow Glasses were donned by Investigator Klein and Holmes. A blue light was applied to the area. Photographs were taken, please see attached.

Post interior search, HCSO was notified of the results and the auto was secured. We were advised by HCSO (? Deputy) to keep the auto secured and call the Texas Ranger in charge the next morning as they would try to call him that evening.

Such results were reported to Texas Ranger Smith the next day – to which no samples or information was obtained by myself. As well, an email was sent to the Ranger and deputy Brent Clapp, no return was given.

On November 25, 2017 the auto was released to the family. They still hold the auto to this day.

### **Lab Samples Of Interior of Auto**

Investigators were told not to take evidence from the auto, and that we would receive instructions from HCSO or the Texas Rangers. On November 25, 2017, we assumed after we had advised them what we had found that they would be coming out to do their testing. According to our clients they did not come out – and we were advised by CD Clapp they did not come up because the evidence would have been tainted.

### **Supplemental Evidence**

KIC Investigators would like to note our meeting of April 21, 2017. In such meeting, the persons involved were :

#### **KIC Staff**

- Klein, P.
- Gear, C
- Holmes, MJ
- Sargent, T

### **Law Enforcement**

- Lewis, N
- Clapp, B
- Smith, M

### **Discussion Notes**

- 1) KIC Staff asked to run the cadaver dog (Chance) on the backpack. It was denied.
- 2) KIC Staff discussed current working theories.
- 3) KIC Staff was steered away from Lake Marvin
- 4) KIC Staff was leaned towards run away or suicide

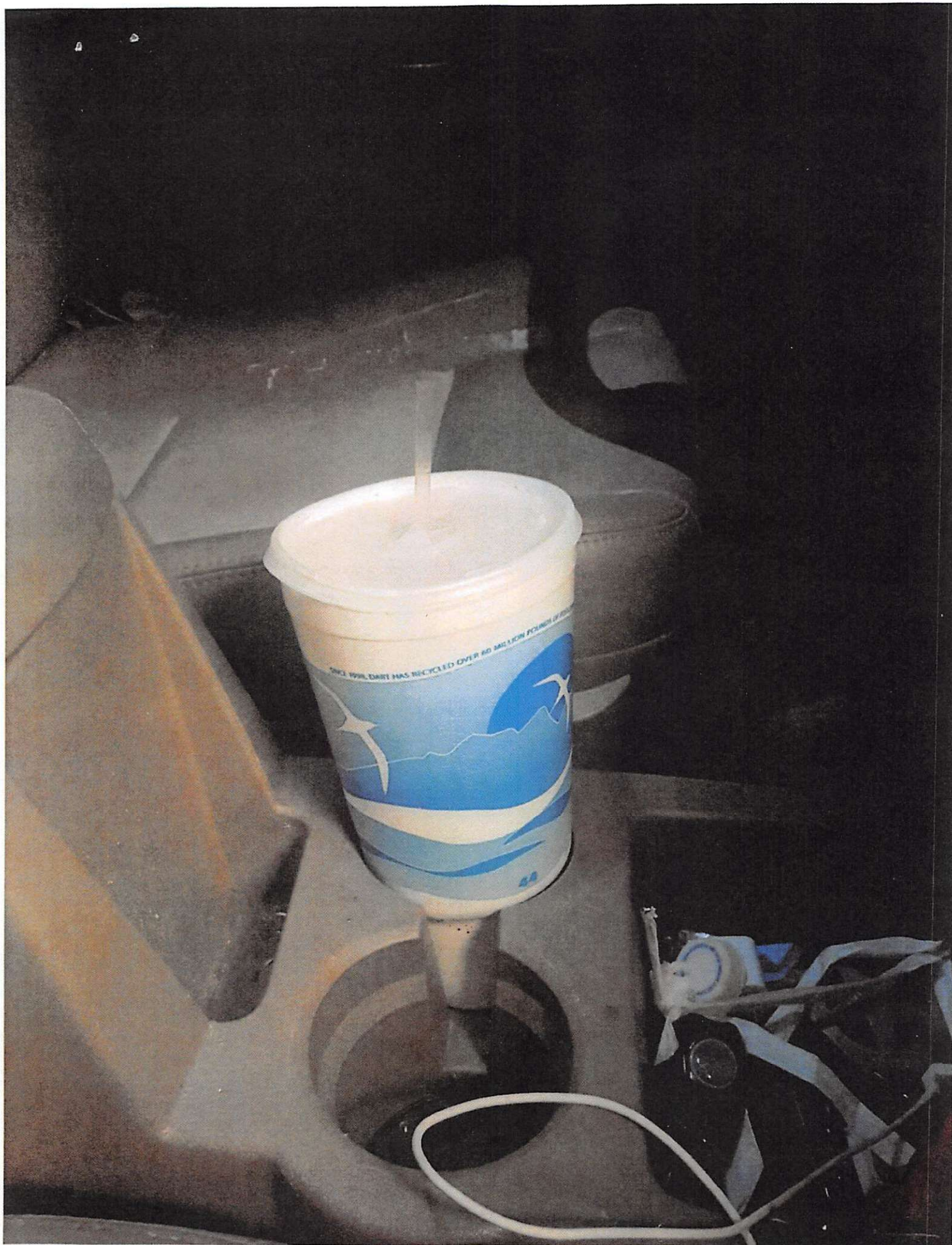
It is noted in our notes, that we were discouraged by how LE was ambiguous and dismissive of the time and hours we put into the case. Further we were discouraged with the dismissiveness that was shown to our team. We believe that the meeting was recorded by the sheriff or the Ranger.

It should be noted that post this meeting all communications broke down. A recording later in the year (attached) showed the manipulation of Lewis towards the Browns. This is as well, post, the interview with the local paper and the plant that Philip Klein lied on the phone and recorder situation found by TXDOT, which post discovery of the body the witness further testified that through the Chief of the Fire Department, the lie tip came from Lewis himself. This was the first time that Nathan Lewis became a concern to KIC Investigators.

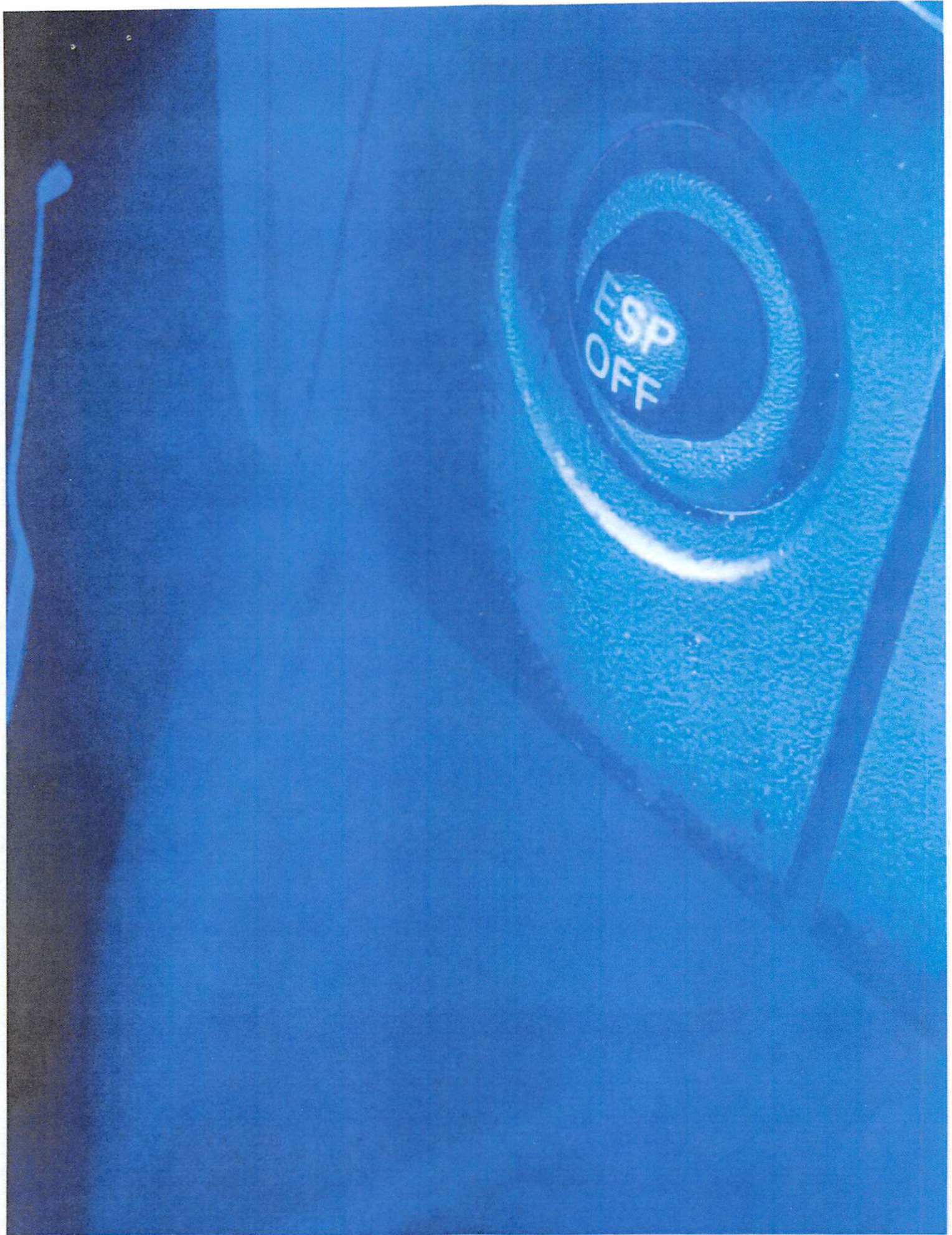
If you need any other information – please let us know.

PRK/w

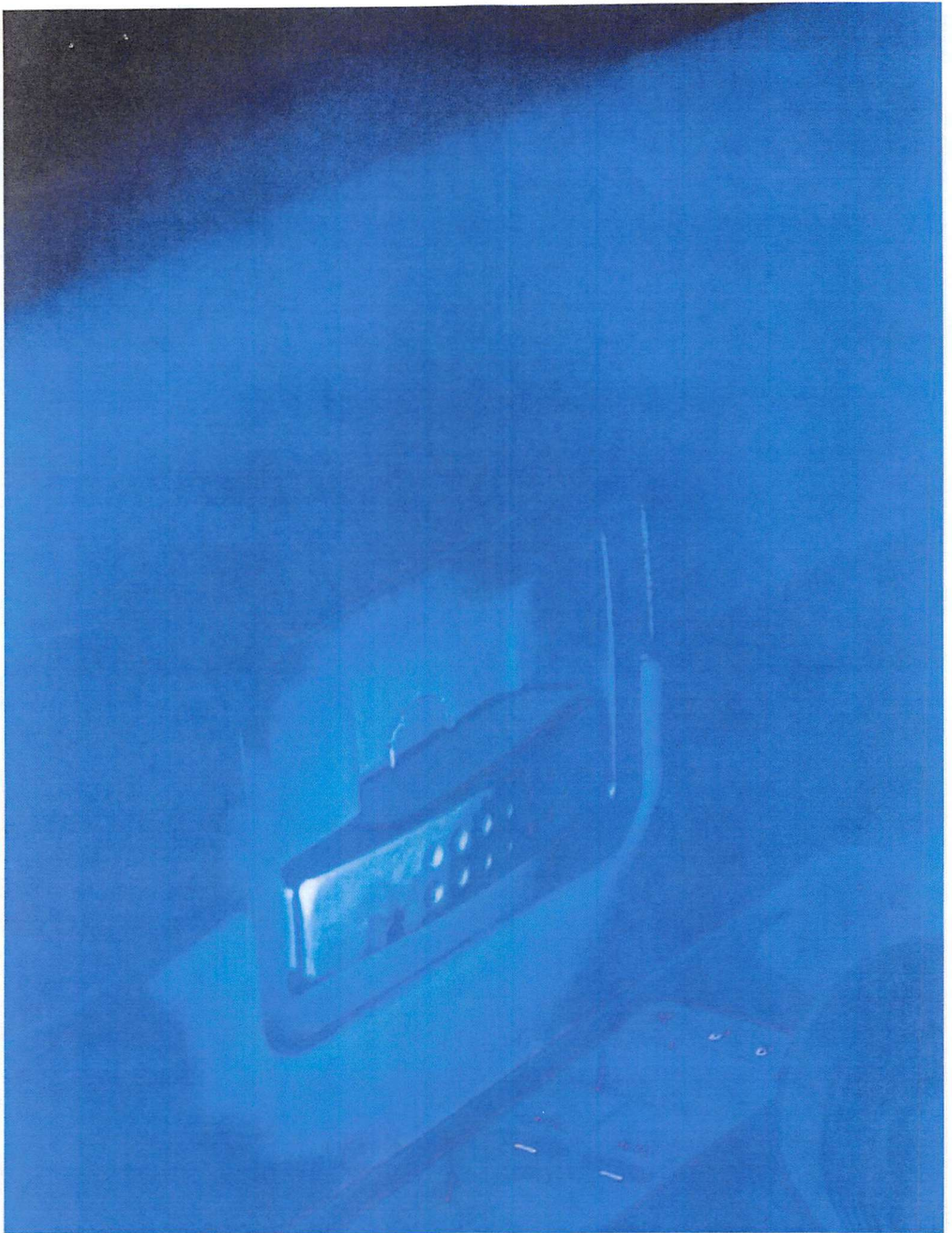
cc. file

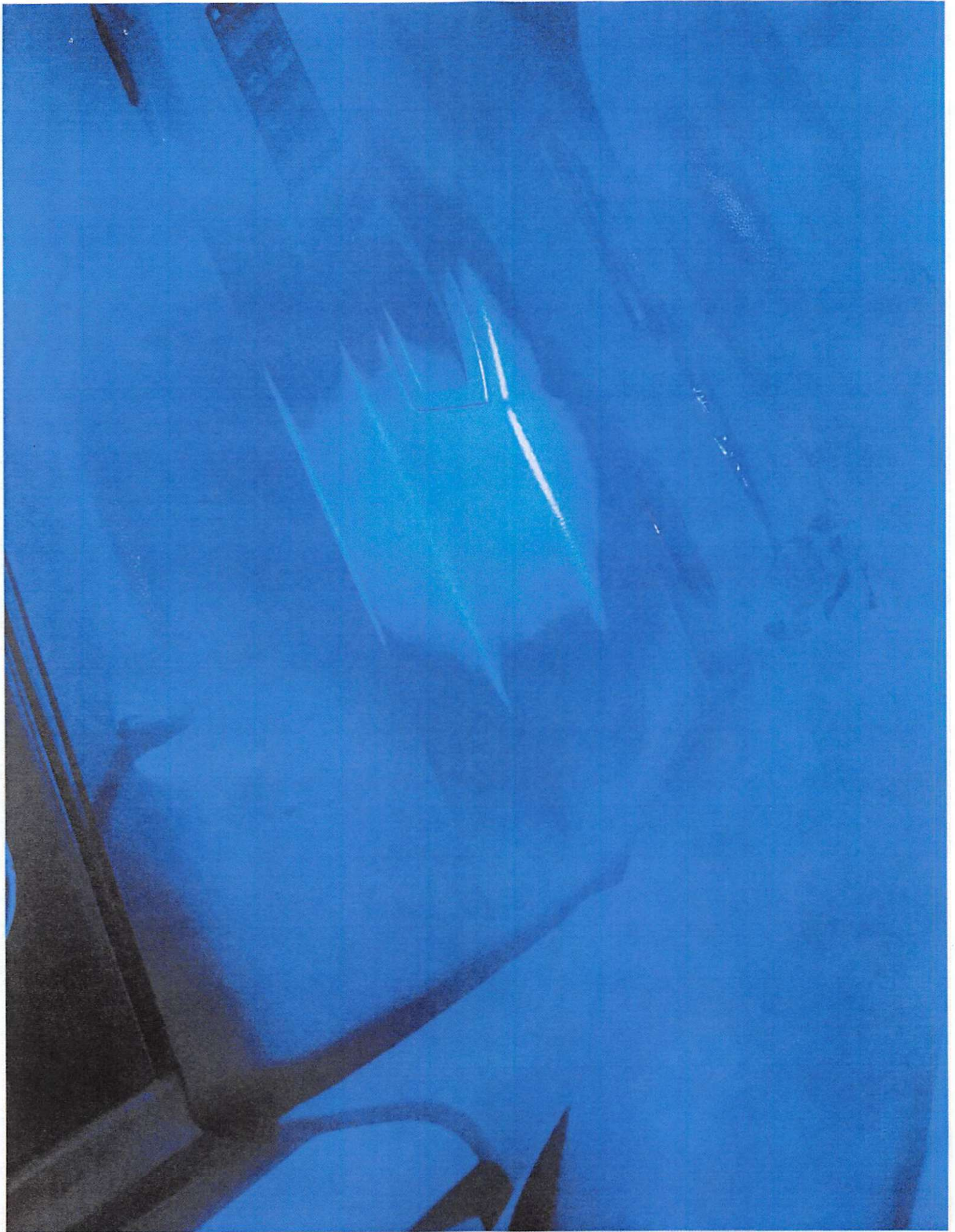


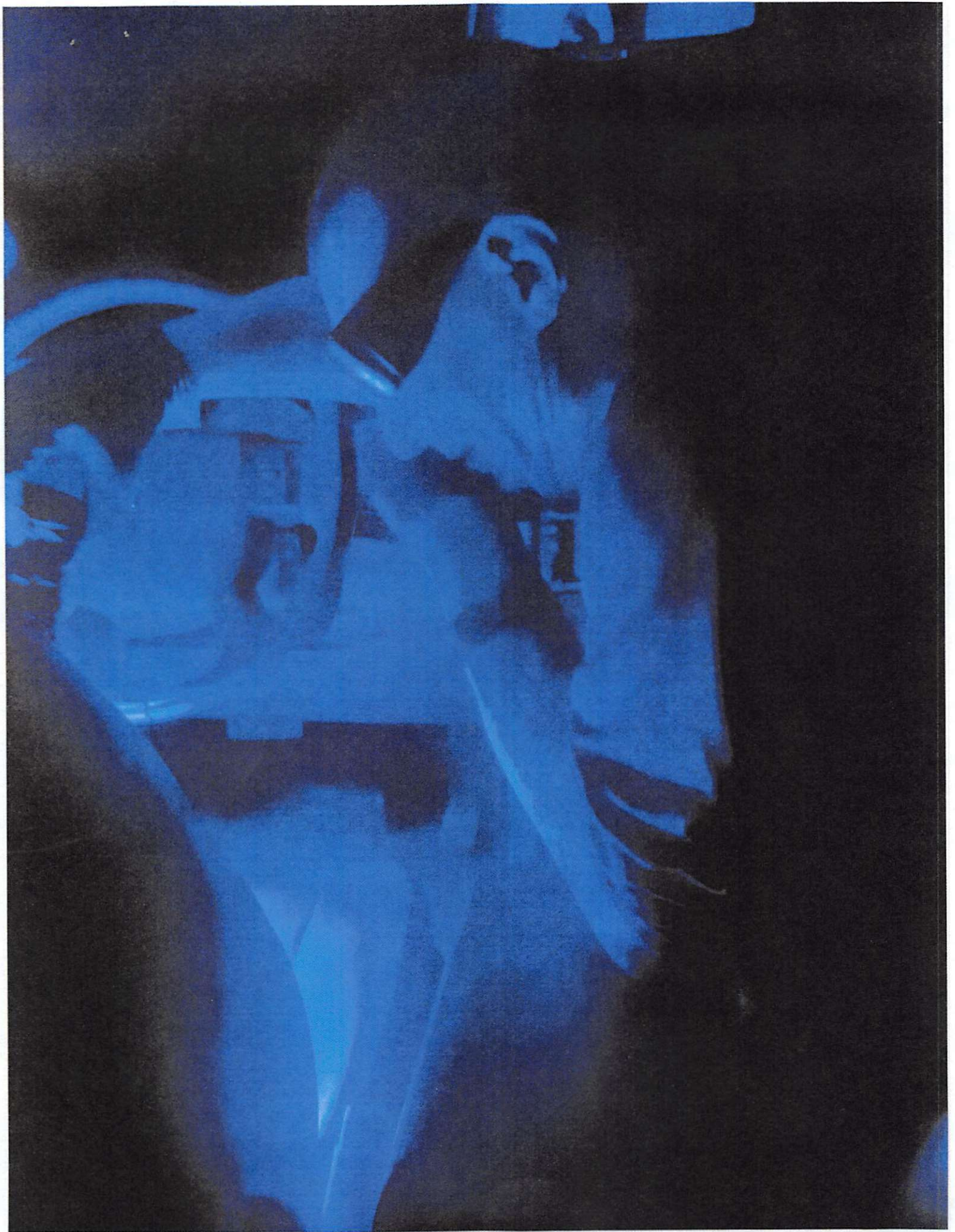


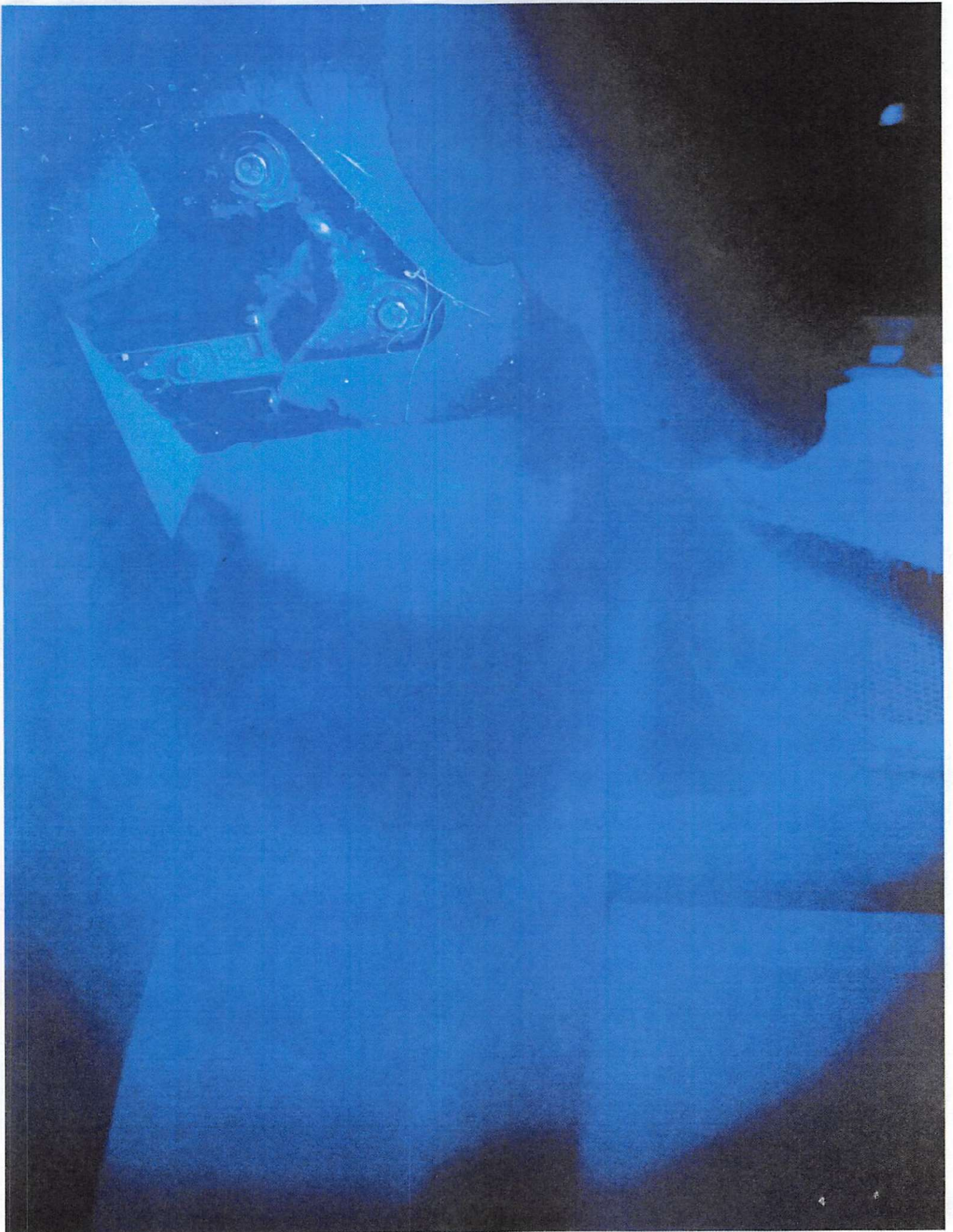






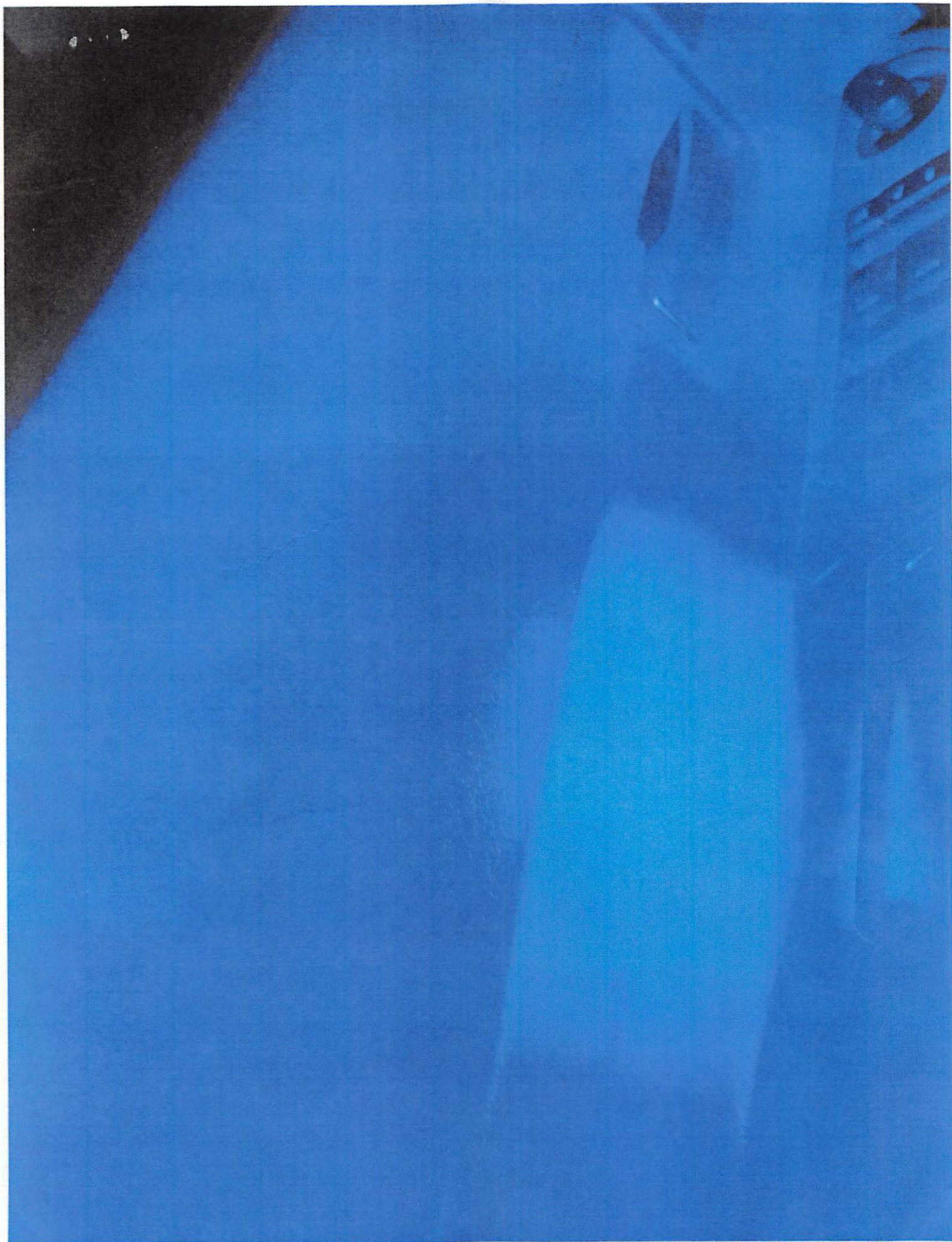














#### Instructions for use:

Luminol is a highly sensitive blood reagent used to detect latent bloodstaining. A strong steady chemi-luminescent reaction takes place when the luminol formula is applied to blood, even in trace amounts. This reaction lasts about 5 seconds and then slowly diminishes. Luminol must be used in near total darkness for best results. Our Luminol formula has been used extensively in forensic applications and is well documented in forensic literature. This formula has been used successfully to detect latent blood evidence 96 months old. The kits are designed for easy mixing at the scene to ensure the highest sensitivity of the reagent. Luminol should be used immediately after mixing! The Luminol sensitivity will dissipate within 2 hours after mixing so having the ability to mix and use at the scene is crucial. Luminol will not fix blood evidence like other reagents such as leuco-crystal violet, so the gentle application in an even fine mist is essential. Your scene, substrate materials, volume, light and equipment will influence each exposure. Luminol is not blood specific and will react to detergents, bleach and common household oxidizers so be cautious in your evaluation in determining blood. A more specific blood reagent like phenolphthalein is usually used after the Luminol detection spray for a positive blood determination. A short video showing the use and limitations of this luminol can be seen at <https://www.youtube.com/watch?v=p4YuyRHbrcc>

1. Remove top from Bottle A and add all contents of Component B to Bottle A.
2. Replace cap with sprayer.
3. Warm solution to room temperature and shake gently until all powder is dissolved.
4. Darken the environment as completely as possible.
5. Spray upon suspected blood.
6. A glowing bluish light reaction is an indication of blood.





## Luminol Specifications

Luminol is a blood specific reagent used to illuminate trace amounts of bloodstained evidence. Luminol has an extremely high sensitivity and will detect blood at 1:1,000,000. The reagent produces a chemi-luminescence reaction when applied to blood. Luminol must be used sparingly as it does not maintain specific pattern evidence. It will continue to create chemi-luminescence when sprayed for multiple applications. Luminol illuminated evidence should be photographed immediately or treated with a fixing blood reagent to preserve the stains for bloodstain pattern analysis or physical match comparison. Luminol treated stains can be analyzed for DNA subsequent to use if the sample has not been diluted due to excessive use.

### *Instructions for use*

Luminol can be sprayed directly upon the suspected bloodstain(s), if blood is present a low blue light reaction takes place called chemi-luminescence. Luminol is best viewed in absolute darkness. Any ambient light will diminish the intensity of the reaction. This will be a steady reaction which slowly dims. Subsequent application may be applied if imaging is necessary and any sampling has been completed. Luminol will react with multiple oxidizers and cleaners creating a flash reaction which should not be considered as a positive blood reaction. Extreme caution must be exercised when cleanup is suspected.

### *Mixing instructions*

Luminol kits are shipped with the chemistry separated for the longest shelf life. This ensures maximum sensitivity when prepared. A simple two component mixture is combined in field or lab for immediate usage. To activate the reagent add component B to bottle A and mix thoroughly. Once mixed luminol has a reactive life of 8 hours maximum. Luminol sensitivity will diminish slowly over the eight hour life span so plan your application accordingly, If possible use within the first hour for best results.

Available in 2oz, 4oz and 8 oz mist for small detail work; 16oz or 32oz with an adjustable sprayer for crime scene work.



---

**Kading, Rachel**

**From:** Brent Clapp <brent@hemphillso.com>  
**Sent:** Monday, August 17, 2020 1:45 PM  
**To:** Kading, Rachel  
**Subject:** FW: Updates

This is the email chain from which I was notified by Klein of the luminol tests.

Brent Clapp  
Sheriff  
Hemphill County Sheriff's Office  
(806) 323-5324 Office  
(806) 323-8355 Fax



---

**From:** Philip Klein <philipklein@gt.twcbc.com>  
**Sent:** Tuesday, December 05, 2017 12:16 PM  
**To:** Brent Clapp <Brent@hemphillso.com>  
**Subject:** RE: Updates

Brent,

We had some attempted hacks – we are reestablishing all of the files for our agency. We will update you as we go. Sorry about that. We have a couple other LE groups that told us they were now blocked on theirs as well.

Bottom line – we are working it and I will update....PRK

---

**From:** Brent Clapp [<mailto:Brent@hemphillso.com>]  
**Sent:** Tuesday, December 05, 2017 7:57 AM

**To:** Philip Klein  
**Subject:** RE: Updates

Phil,

I am sure the dirt and snakes are a big problem. I am out on removing snakes. As far as the drop box, I was going to review some notes and interviews yesterday, but could not find the Brown file. Can you advise the status of the file please.

Brent Clapp  
Chief Deputy  
Hemphill County Sheriff's Office  
(806) 323-5324 Office  
(806) 323-5260 Fax

---

**From:** Philip Klein [<mailto:philipklein@gt.twcbc.com>]  
**Sent:** Monday, December 04, 2017 3:01 PM  
**To:** Brent Clapp <[Brent@hemphillso.com](mailto:Brent@hemphillso.com)>  
**Cc:** 'Jane Holmes' <[GeorgjaPI@outlook.com](mailto:GeorgjaPI@outlook.com)>; 'Caroline Gear' <[carolinegear@gt.twcbc.com](mailto:carolinegear@gt.twcbc.com)>; 'charley klein' <[charleyklein@gt.twcbc.com](mailto:charleyklein@gt.twcbc.com)>  
**Subject:** RE: Updates

Hey Brent –

It was good to see you the other night. Yes – I believe we were productive while there and let me give you a brief overview :

1. First – we finished the culverts on Lake Marvin Road – they were very very full of heavy soil which I believe needs to be removed. (Snakes as well).
2. Second – we did some interviews with Ricky Ivy and Dainel Whitley (sp). They were productive.
3. Third – we did an Luminol Spray with lighting on the young man's auto. That report was sent to Ranger Smith on Thursday of last week. The overview is that it tested positive in 14 locations. Photos were sent to Smith – per his request regarding evidence a few months ago – if he didn't share let me know.

Thanks much – and I hope you are well...my best...PRK

---

**From:** Brent Clapp [<mailto:Brent@hemphillso.com>]  
**Sent:** Monday, December 04, 2017 1:24 PM  
**To:** Philip Klein  
**Subject:** Updates

Phil,

I was just wondering if you had any updates on what you learned when you were here a couple weeks ago. I checked the Drop Box file for your normal updates and the Brown file appears to have been deleted.

Thanks.

Brent Clapp  
Chief Deputy  
Hemphill County Sheriff's Office  
(806) 323-5324 Office  
(806) 323-5260 Fax



# FORENSIC EXAMINATION REPORT

CASE NUMBER CX9512431186

Examiner Les St. James  
Case generated Monday, April 15, 2019  
Report generated Wednesday, June 17, 2020

Case overview

## CASE OVERVIEW

### CASE PROCESSING DETAILS

#### SCAN 1

Scanned by Les St. James

Scan date Monday, April 15, 2019 10:02:47 AM

## EVIDENCE OVERVIEW

Evidence items 3

Combined results 1,219,970

PHYSICALDRIVE3 DIGINTEL HOTSWAP\_BAY1 SCSI DISK DEVICE (3.64 TB)  
(489)

Evidence number PhysicalDrive3 DIGINTEL  
HotSwap\_Bay1 SCSI Disk Device (3.64  
TB)

Location PhysicalDrive3

0D45B51CF0ECC2545ABEDC76F84A62789E9F07DF\_MEM.ZIP (6,787)

Evidence number 0d45b51cf0ecc2545abedc76f84a62789e9f07df\_mem.zip

Location 0d45b51cf0ecc2545abedc76f84a62789e9f07df\_mem.zip

Platform Mobile

0D45B51CF0ECC2545ABEDC76F84A62789E9F07DF\_FILES\_FULL.ZIP  
(1,212,694)

Evidence number 0d45b51cf0ecc2545abedc76f84a62789e9f07df\_files\_full.zip

Location 0d45b51cf0ecc2545abedc76f84a62789e9f07df\_files\_full.zip

Platform Mobile

Exported results

Record 1

Tags	Of interest
Comments	
Item	<a href="https://www.google.com/search?q=suicide+hotline&amp;prmd=ivn&amp;source=Inms&amp;tbn=isch&amp;sa=X&amp;ved=0ahUKewiM3qPitcDQAhVK4oMKHZPmBd8Q_AUIBygB&amp;biw=375&amp;bih=559&amp;dpr=2">https://www.google.com/search?q=suicide+hotline&amp;prmd=ivn&amp;source=Inms&amp;tbn=isch&amp;sa=X&amp;ved=0ahUKewiM3qPitcDQAhVK4oMKHZPmBd8Q_AUIBygB&amp;biw=375&amp;bih=559&amp;dpr=2</a>
Type	Safari Tabs
Artifact category	Artifacts
Date and time	
Source	<ul style="list-style-type: none"> <li>0d45b51cf0ecc2545abedc76f84a62789e9f07df_files_full.zip\private\var\mobile\Containers\Data\Applications\121F435F-2F72-421C-BC97-85E9A82581F0\Library\Safari\BrowserState.db</li> </ul>
Location	<ul style="list-style-type: none"> <li>Table: tabs(id: 535)</li> </ul>
Evidence number	<ul style="list-style-type: none"> <li>0d45b51cf0ecc2545abedc76f84a62789e9f07df_files_full.zip</li> </ul>

Record 2

Tags	Of interest
Comments	
Item	<a href="https://www.google.com/search?q=suicide+hotline&amp;biw=375&amp;bih=559&amp;prmd=ivn&amp;source=Inms&amp;sa=X&amp;ved=0ahUKEwic-4_Ly8DQAhUp5IMKHVD9B-IQ_AUIBCgA&amp;dpr=2">https://www.google.com/search?q=suicide+hotline&amp;biw=375&amp;bih=559&amp;prmd=ivn&amp;source=Inms&amp;sa=X&amp;ved=0ahUKEwic-4_Ly8DQAhUp5IMKHVD9B-IQ_AUIBCgA&amp;dpr=2</a>
Type	Safari Tabs
Artifact category	Artifacts
Date and time	
Source	<ul style="list-style-type: none"> <li>0d45b51cf0ecc2545abedc76f84a62789e9f07df_files_full.zip\private\var\mobile\Containers\Data\Applications\121F435F-2F72-421C-BC97-85E9A82581F0\Library\Safari\BrowserState.db</li> </ul>
Location	<ul style="list-style-type: none"> <li>Table: tabs(id: 535)</li> </ul>
Evidence number	<ul style="list-style-type: none"> <li>0d45b51cf0ecc2545abedc76f84a62789e9f07df_files_full.zip</li> </ul>

Record 3

Tags	Of interest
Comments	
Item	suicide hotline
Type	Google Searches
Artifact category	Artifacts
Date and time	
Source	<ul style="list-style-type: none"> <li>0d45b51cf0ecc2545abedc76f84a62789e9f07df_files_full.zip\private\var\mobile\Containers\Data\Applications\121F435F-2F72-421C-BC97-85E9A82581F0\Library\Safari\BrowserState.db</li> </ul>
Location	<ul style="list-style-type: none"> <li>Table: tabs(id: 535)</li> </ul>
Evidence number	<ul style="list-style-type: none"> <li>0d45b51cf0ecc2545abedc76f84a62789e9f07df_files_full.zip</li> </ul>

Record 4

Tags	Of interest
Comments	
Item	suicide hotline
Type	Google Searches
Artifact category	Artifacts
Date and time	
Source	<ul style="list-style-type: none"> <li>0d45b51cf0ecc2545abedc76f84a62789e9f07df_files_full.zip\private\var\mobile\Containers\Data\Applications\121F435F-2F72-421C-BC97-85E9A82581F0\Library\Safari\BrowserState.db</li> </ul>
Location	<ul style="list-style-type: none"> <li>Table: tabs(id: 535)</li> </ul>
Evidence number	<ul style="list-style-type: none"> <li>0d45b51cf0ecc2545abedc76f84a62789e9f07df_files_full.zip</li> </ul>

Record 5

Tags	Of interest
Comments	
Item	suicide hotline
Type	Google Searches
Artifact category	Artifacts
Date and time	11/23/2016 9:11:15 PM
Source	<ul style="list-style-type: none"> <li>0d45b51cf0ecc2545abedc76f84a62789e9f07df_files_full.zip\private\var\mobile\Containers\Data\Applications\121F435F-2F72-421C-BC97-85E9A82581F0\Library\Safari\BrowserState.db</li> </ul>
Location	<ul style="list-style-type: none"> <li>Table: tabs(id: 535)</li> </ul>
Evidence number	<ul style="list-style-type: none"> <li>0d45b51cf0ecc2545abedc76f84a62789e9f07df_files_full.zip</li> </ul>



Exported results

Record 6

Tags	Of interest
Comments	
Item	suicide hotline
Type	Google Searches
Artifact category	Artifacts
Date and time	11/23/2016 9:11:15 PM
Source	<ul style="list-style-type: none"> <li>0d45b51cf0ecc2545abedc76f84a62789e9f07df_files_full.zip\private\var\mobile\Containers\Data\Applicati on\121F435F-2F72-421C-BC97-85E9A82581F0\Library\Safari\BrowserState.db</li> </ul>
Location	<ul style="list-style-type: none"> <li>File Offset 69808</li> </ul>
Evidence number	<ul style="list-style-type: none"> <li>0d45b51cf0ecc2545abedc76f84a62789e9f07df_files_full.zip</li> </ul>

Record 7

Tags	Of interest
Comments	
Item	suicide hotline
Type	Google Searches
Artifact category	Artifacts
Date and time	
Source	<ul style="list-style-type: none"> <li>0d45b51cf0ecc2545abedc76f84a62789e9f07df_files_full.zip\private\var\mobile\Containers\Data\Applicati on\121F435F-2F72-421C-BC97-85E9A82581F0\Library\Safari\BrowserState.db</li> </ul>
Location	<ul style="list-style-type: none"> <li>File Offset 71376</li> </ul>
Evidence number	<ul style="list-style-type: none"> <li>0d45b51cf0ecc2545abedc76f84a62789e9f07df_files_full.zip</li> </ul>

Record 8

Tags	Of interest
Comments	
Item	suicide hotline
Type	Google Searches
Artifact category	Artifacts
Date and time	
Source	<ul style="list-style-type: none"> <li>0d45b51cf0ecc2545abedc76f84a62789e9f07df_files_full.zip\private\var\mobile\Containers\Data\Applicati on\121F435F-2F72-421C-BC97-85E9A82581F0\Library\Safari\BrowserState.db</li> </ul>
Location	<ul style="list-style-type: none"> <li>File Offset 73296</li> </ul>
Evidence number	<ul style="list-style-type: none"> <li>0d45b51cf0ecc2545abedc76f84a62789e9f07df_files_full.zip</li> </ul>

Record 9

Tags	Of interest
Comments	
Item	suicide hotline
Type	Google Searches
Artifact category	Artifacts
Date and time	11/23/2016 9:11:15 PM
Source	<ul style="list-style-type: none"> <li>0d45b51cf0ecc2545abedc76f84a62789e9f07df_files_full.zip\private\var\mobile\Containers\Data\Applicati on\121F435F-2F72-421C-BC97-85E9A82581F0\Library\Safari\BrowserState.db</li> </ul>
Location	<ul style="list-style-type: none"> <li>File Offset 396916</li> </ul>
Evidence number	<ul style="list-style-type: none"> <li>0d45b51cf0ecc2545abedc76f84a62789e9f07df_files_full.zip</li> </ul>

Record 10

Tags	Of interest
Comments	
Item	<a href="https://www.google.com/search?site=&amp;source=hp&amp;ei=U1o2WP3nFcjJwTlvonoDQ&amp;q=suicide+hotline&amp;oq=suicide+hotline&amp;gs_l=mobile-gws-hp.3..015.3653.7721.0.8006.16.16.0.11.11.0.255.2756.0j14j2.16.0....0...1c1.64.mobile-gws-hp..0.15.855.0..0i131k1.8q7EmOJA_D8">https://www.google.com/search?site=&amp;source=hp&amp;ei=U1o2WP3nFcjJwTlvonoDQ&amp;q=suicide+hotline&amp;oq=suicide+hotline&amp;gs_l=mobile-gws-hp.3..015.3653.7721.0.8006.16.16.0.11.11.0.255.2756.0j14j2.16.0....0...1c1.64.mobile-gws-hp..0.15.855.0..0i131k1.8q7EmOJA_D8</a>
Type	Safari History
Artifact category	Artifacts
Date and time	
Source	<ul style="list-style-type: none"> <li>0d45b51cf0ecc2545abedc76f84a62789e9f07df_files_full.zip\private\var\mobile\Containers\Data\Applicati on\121F435F-2F72-421C-BC97-85E9A82581F0\Library\Safari\BrowserState.db</li> </ul>
Location	<ul style="list-style-type: none"> <li>File Offset 69808</li> </ul>
Evidence number	<ul style="list-style-type: none"> <li>0d45b51cf0ecc2545abedc76f84a62789e9f07df_files_full.zip</li> </ul>

Exported results

Record 11

Tags	Of interest
Comments	
Item	<a href="https://www.google.com/search?q=suicide+hotline&amp;prmd=ivn&amp;source=Inms&amp;tbn=isch&amp;sa=X&amp;ved=0ahUKewiM3qPitcDQAhVK4oMKHZPmBd8Q_AUIBygB&amp;biw=375&amp;bih=559&amp;dpr=2">https://www.google.com/search?q=suicide+hotline&amp;prmd=ivn&amp;source=Inms&amp;tbn=isch&amp;sa=X&amp;ved=0ahUKewiM3qPitcDQAhVK4oMKHZPmBd8Q_AUIBygB&amp;biw=375&amp;bih=559&amp;dpr=2</a>
Type	Safari History
Artifact category	Artifacts
Date and time	
Source	<ul style="list-style-type: none"> <li>0d45b51cf0ecc2545abedc76f84a62789e9f07df_files_full.zip\private\var\mobile\Containers\Data\Applicati on\121F435F-2F72-421C-BC97-85E9A82581F0\Library\Safari\BrowserState.db</li> </ul>
Location	<ul style="list-style-type: none"> <li>File Offset 71376</li> </ul>
Evidence number	<ul style="list-style-type: none"> <li>0d45b51cf0ecc2545abedc76f84a62789e9f07df_files_full.zip</li> </ul>

Record 12

Tags	Of interest
Comments	
Item	<a href="https://www.google.com/search?q=suicide+hotline&amp;biw=375&amp;bih=559&amp;prmd=ivn&amp;source=Inms&amp;sa=X&amp;ved=0ahUKEwic-4_Ly8DQAhUp5IMKHVD9B-IQ_AUIBCgA&amp;dpr=2">https://www.google.com/search?q=suicide+hotline&amp;biw=375&amp;bih=559&amp;prmd=ivn&amp;source=Inms&amp;sa=X&amp;ved=0ahUKEwic-4_Ly8DQAhUp5IMKHVD9B-IQ_AUIBCgA&amp;dpr=2</a>
Type	Safari History
Artifact category	Artifacts
Date and time	
Source	<ul style="list-style-type: none"> <li>0d45b51cf0ecc2545abedc76f84a62789e9f07df_files_full.zip\private\var\mobile\Containers\Data\Applicati on\121F435F-2F72-421C-BC97-85E9A82581F0\Library\Safari\BrowserState.db</li> </ul>
Location	<ul style="list-style-type: none"> <li>File Offset 73296</li> </ul>
Evidence number	<ul style="list-style-type: none"> <li>0d45b51cf0ecc2545abedc76f84a62789e9f07df_files_full.zip</li> </ul>

Record 13

Tags	Of interest
Comments	
Item	<a href="https://www.google.com/search?site=&amp;source=hp&amp;ei=U1o2WP3nFcjJwTIvonoDQ&amp;q=suicide+hotline&amp;oq=suicide+hotline&amp;gs_l=mobile-gws-hp.3..0l5.3653.7721.0.8006.16.16.0.11.11.0.255.2756.0j14j2.16.0....0..1c.1.64.mobile-gws-hp.0.15.855.0..0i131k1.8q7EmOjA_D8">https://www.google.com/search?site=&amp;source=hp&amp;ei=U1o2WP3nFcjJwTIvonoDQ&amp;q=suicide+hotline&amp;oq=suicide+hotline&amp;gs_l=mobile-gws-hp.3..0l5.3653.7721.0.8006.16.16.0.11.11.0.255.2756.0j14j2.16.0....0..1c.1.64.mobile-gws-hp.0.15.855.0..0i131k1.8q7EmOjA_D8</a>
Type	Safari History
Artifact category	Artifacts
Date and time	
Source	<ul style="list-style-type: none"> <li>0d45b51cf0ecc2545abedc76f84a62789e9f07df_files_full.zip\private\var\mobile\Containers\Data\Applicati on\121F435F-2F72-421C-BC97-85E9A82581F0\Library\Safari\BrowserState.db</li> </ul>
Location	<ul style="list-style-type: none"> <li>File Offset 396916</li> </ul>
Evidence number	<ul style="list-style-type: none"> <li>0d45b51cf0ecc2545abedc76f84a62789e9f07df_files_full.zip</li> </ul>

To: Penny Meek Cell

Mon, Jan 9, 6:30 PM

Would you ask [REDACTED] if [REDACTED] knows Tom's phone password. It would be a 4 digit #.

[REDACTED] said he didn't know it. Sorry!

No problem. Does [REDACTED] know anyone who might know it?

[REDACTED] said maybe [REDACTED] or [REDACTED]

Ask [REDACTED] to ask them for me? I don't have their phone numbers.

Mon, Jan 9, 8:33 PM

I'm sorry they don't know either.

Ok. Thanks

IN THE MATTER OF

THE STATE OF TEXAS

THOMAS BROWN

§  
§  
§  
§  
§

A CRIMINAL INVESTIGATION

HEMPHILL COUNTY

Brown,  
Webb, King

**AFFIDAVIT REQUESTING AN ORDER FOR DISCLOSURE OF HISTORICAL  
LOCATION-BASED ELECTRONIC COMMUNICATIONS DATA FOR A MOBILE  
TELEPHONES**

The affiant, Brent Clapp, a peace officer employed by the Hemphill County Sheriff's Office (hereinafter "law enforcement agency"), located at 401 Purcell, Canadian, Texas, do have probable cause to make this application for a court order authorizing Celco Partnership, dba Verizon Wireless and AT&T Mobility (hereinafter "common communications carriers") to provide authorized commissioned peace officers of the Hemphill County Sheriff's Office and agents of the Federal Bureau of Investigation (FBI), disclosure historical location-based data, as authorized by 18 U.S.C. §3117(a), 2703(d), and Article 18.21, Texas Code of Criminal Procedure, related to telephone numbers (806) 282-5391 associated with Thomas Brown, (806) 323-3117 associated with Christian Webb, and (806) 255-0036 associated with Kaleb King. The target telephones (806) 282-5391, (806) 323-3117, and (806) 255-0036 are mobile telephone instruments.

In support, the Affiant respectfully shows the court as follows: On 11/24/2016, at approximately 2:30 a.m, Thomas Kelly Brown, born 09/13/1998, was reported missing by his mother, Penny Meek, born 01/12/1966. Thomas had last been seen with friends in Canadian at approximately 11:30 p.m. on November 23<sup>rd</sup>. Brown was to be home by midnight according to his mother Penny. Deputies were dispatched and conducted a search of places in Hemphill County that were known to be frequented by Brown and his acquaintances. Deputies Gregory and DeHerrera searched until approximately 6:00 a.m. when Sheriff Lewis and Deputy J. Ortega took over the search.

Several attempts were made by family and friends to contact Brown on his cell phone (806) 282-5391 shortly after midnight, but all attempts went straight to voicemail leading investigators to believe his phone was powered off.

At approximately 9:30 a.m. Brown's vehicle was located abandoned near the sewer treatment ponds on the north edge of the city. Video surveillance in the area showed Brown's vehicle arriving in the area where it was left shortly before 6:00 a.m. on 11/24/2016. Texas Game Warden Derrick Nalls was contacted to provide his tracking K9. The area was thoroughly searched by Warden Nalls, his K9, and Warden Collins. The Wardens completed their search of the area at approximately 4:00 pm with limited success. Nalls explained that his K9 had picked up scent east of the vehicle then lost it. Throughout the next week the area of the Canadian river was extensively searched by air, on foot and horseback. Sometime thereafter, Brown's school backpack was located in some brush near Marvin Lake.

During the course of the investigation, investigators determined the last two people to physically see Brown were Christian Webb and Kaleb King. Further investigation revealed King, Webb, and Brown were all together just before midnight and just before Brown's cell phone was turned off. Webb's cell phone number was confirmed as (806) 323-3117 and King's cell phone number was confirmed as (806) 255-0036. The last trace of Brown's whereabouts were discovered near Webb's residence by Marvin Lake. On 01/10/2017, King sent a text message to Brown's ex-girlfriend, Saige Pennington, asking Pennington if she knew Brown's passcode to his cellphone. King also texted saying he needed it because investigators were asking. To date, investigators have not recovered Brown's cell phone. Neither has any investigator asked King for Brown's phone passcode.

#### I.

The Affiant is a peace officer commissioned by the law enforcement agency, assigned as the Chief Deputy of the Hemphill County Sheriff's Office, and the Affiant is an authorized peace officer as that term is defined in Article 18.21 §1(2), Texas Code of Criminal Procedure and 18 U.S.C. §3105.

#### II.

The Affiant seeks a court order authorizing the common communications carrier to disclose location-based data that will assist the above law enforcement agency and the FBI in determining the historical locations of the target telephones (806) 282-5391, (806) 323-3117, and (806) 255-

0036 (differentiated from the first or last call-site used to make or receive a call, which simply identifies the location of the telephone company's infrastructure). Further, that the common communications carrier provide historical call detail records, including incoming and outgoing calls, SMS messages, MMS messages, and data connections with cell site information and/or historical location-based/GPS information (NELOS Report) for target telephone from 11/20/2016 to 03/29/2017.

### III.

The affiant believes that information obtained from the order authorizing location-based data will likely produce information that is relevant and material to an ongoing missing person investigation. In support, the affiant respectfully shows the court as follows: That historical call detail records with cellsite information along with historical location-based information (NELOS Report / RTT Report) for target telephones (806) 282-5391, (806) 323-3117, and (806) 255-0036 for the specified date range of 11/20/2016 to 03/29/2017 may show approximate locations for Brown, Webb, and King before, during, and after Brown was reported missing. Records may show Brown's last known approximate locations providing investigators with an area to search and/or conduct additional investigation which may lead to Brown's recovery. Records may also reveal contacts, associates, friends, and family members who may provide information and/or evidence crucial to this investigation or who may be suspects in Brown's disappearance. Therefore, your Affiant is requesting the Court grant an order for any and all subscriber information, historical incoming and outgoing call, text, MMS, and data connection call detail records with cell site information and historical location-based information (NELOS Report/RTT Data) for target telephones (806) 282-5391, (806) 323-3117, and (806) 255-0036 for the specified date range of 11/20/2016 to 03/29/2017.

### IV.

The common communications carrier has refused to provide the law enforcement agency access to location-based information without being served with an appropriate court order.

### V.

That the court shall seal the application and order upon issuance of the order, as authorized by Article 18.21, §2(g), Texas Code of Criminal Procedure.

VI.

That the investigation is extensive and ongoing and that to reveal access by the law enforcement agency and the FBI to the location-based information related to the target telephone to anyone outside the investigation would severely jeopardize the investigation; therefore, information regarding access by the law enforcement agency and the FBI to the location-based information should not be revealed by common communications carrier or its employees to any person outside the investigation, except as authorized by the court.

VII.

The common communications carrier should be ordered not to reveal any information about the entry of this order, application, or affidavit in this matter and that subsequent access by the law enforcement agency and the FBI to the location-based data.

VIII.

The State is requesting that the law enforcement agency and the FBI be allowed to receive location-based information within a period not to exceed ten (10) days after the date the order is entered, and further that any reasonable costs incurred during the period covered by the court are to be reimbursed to the common communications carrier by the law enforcement agency and/or the FBI.

IX.

The Affiant request that this authorization extend to any changes in the event that any two of the following occurs during the period for which the order authorizing the release of historical location-based data and records for the target telephones (806) 282-5391, (806) 323-3117, and (806) 255-0036 occurs: the telephone number, the telephone instrument, or the MEID/ESN/IMSI, change; provided that both the subscribers, and either the telephone numbers, the telephone instruments, or the MEID/ESN/IMSI remain the same;


**WHEREFORE, PREMISED CONSIDERED,** the State respectfully requests that the Court enter an order directing the common communications carrier to provide the law enforcement agency and the FBI with the historical location-based information and all call detail records with cell site information pertaining to the location of the target telephones (806) 282-5391, (806) 323-3117, and (806) 255-0036 and technical assistance necessary to interpret the data provided. Further, that all records and information required be provided in a commercially reasonable electronic format specified by the law enforcement agency; and that all records are delivered



forthwith via electronic mail (unless otherwise specified) to the email address specified by Affiant, at the intervals requested.

**IT IS FURTHER REQUESTED** that the Court seal the order, application and affidavit, and further that the Court order the common communications carrier, their agents and employees not to divulge, reveal, or disclose the existence of the order, application, and affidavit, the existence of this investigation or the existence of the location-based data to any person outside this investigation, unless otherwise ordered by the Court.

  
\_\_\_\_\_  
PEACE OFFICER  
HEMPHILL COUNTY, TEXAS

SUBSCRIBED AND SWORN TO before me, the undersigned authority on this the  
30<sup>th</sup> day of March, 2017.  
  
\_\_\_\_\_  
District Judge, 31<sup>st</sup> District Court, State of Texas  
223d

IN THE MATTER OF

THOMAS BROWN

A CRIMINAL INVESTIGATION

§  
§  
§  
§  
§

THE STATE OF TEXAS

HEMPHILL COUNTY

**ORDER FOR DISCLOSURE OF HISTORICAL LOCATION-BASED ELECTRONIC  
COMMUNICATION DATA FOR A MOBILE TELEPHONES**

Came on this day to be heard the Application of the State of Texas for historical location-based information, as authorized by 18 U.S.C. §3117(a), 2703(d), and Article 18.21 §14, Texas Code of Criminal Procedure, related to telephone numbers (806) 282-5391 associated with Thomas Brown, (806) 323-3117 associated with Christian Webb, and (806) 255-0036 associated with Kaleb King. The target telephones (806) 282-5391, (806) 323-3117, and (806) 255-0036 are mobile telephone instruments.

IT APPEARING that the application has been made in good faith in the furtherance of a pending missing person investigation, and it appearing, based on the underlying specific articulable fact based affidavit of an authorized peace officer, Brent Clapp, with the Hemphill County Sheriff's Office, which has offered probable cause that historical location-based information (NELOS Report/RTT Data) and all incoming and outgoing call detail records with cell site information about the target telephones (806) 282-5391, (806) 323-3117, and (806) 255-0036 will be relevant and material to an ongoing missing person investigation.

IT IS ORDERED, pursuant to Article 18.21 §14 C.C.P., that Cellco Partnership, dba Verizon Wireless and AT&T Mobility, (hereinafter "common communications carriers") disclose historical location-based data (NELOS Reports / RTT Data) that will assist the law enforcement agency and the Federal Bureau of Investigation (FBI) in determining the locations of the target telephones (806) 282-5391, (806) 323-3117, and (806) 255-0036 (differentiated from the first or last cell-site used to make or receive a call, which simply identifies the location of the common

communications carrier infrastructure) during the specified date range of 11/20/2016 to 03/29/2017.

IT IS ORDERED that the common communications carriers provide to the law enforcement agency and/or the FBI any and all subscriber information to include the MEID/ESN/MIN/IMSI, any and all historical incoming and outgoing call, SMS text, MMS call detail records, and data connection and/or IP destination records with cell site information and historical location-based information (NELOS Report / RTT Data) for target telephones (806) 282-5391, (806) 323-3117, and (806) 255-0036 for the specified date range of 11/20/2016 to 03/29/2017.

IT IS ORDERED that the common communications carriers provide all records and information in a commercially reasonable electronic format specified by the law enforcement agency and/or the FBI; and that the common communications carrier deliver all records forthwith via electronic mail (unless otherwise specified) to the email address specified by Affiant at the intervals requested.

IT IS ORDERED that the normal operations of the common communications carriers shall not be disrupted and that the common communications carriers be compensated at the prevailing rates by the State of Texas, through the law enforcement agency and/or the FBI; and

IT IS FURTHER ORDERED that the common communications carriers, its agents and employees shall not disclose to any person outside of this investigation the existence of this order, application, and affidavit, the existence of this investigation or the existence of the location based information provided under the authority of this order, unless otherwise ordered by the Court;

IT IS FURTHER ORDERED that this authorization shall extend to any changes in any of the following data occurring during the period for which the order authorizing the historical

location-based data and records are in effect for the target telephones (806) 282-5391, (806) 323-3117, and (806) 255-0036; the telephone numbers, the telephone instruments, or the MEID/ESN/IMSI; provided that the subscribers, the common communications carriers, and either the telephone numbers, the telephone instruments, or the MEID/ESN/IMSI remained the same; and further provided that the Court is notified without reasonable delay of any changes in the telephone numbers, the telephone instruments, or the MEID/ESN/IMSI;

IT IS ORDERED that this order, application, and affidavit any amendments thereto be placed under the seal of the Court until further order of the Court; and

IT IS FURTHER ORDERED, consistent with the provisions of Article 18.21 §10, TEX. CODE CRIM. PROC., that no cause of action shall lie against the common communications carriers for complying with this order,

IT IS FURTHER ORDERED that the law enforcement agency and the FBI be allowed to receive the historical records within a period not to exceed ten (10) days after the date the order is entered, and further that any reasonable costs incurred during the period covered by the court are to be reimbursed to the common communications carriers by the law enforcement agency and/or the FBI.

Entered and signed this 30<sup>th</sup> day of March, 2017,

at 3:25 o'clock P.m., to certify which witness my hand this day.



DISTRICT JUDGE

2234 31<sup>st</sup> DISTRICT COURT

IN THE MATTER OF

THOMAS BROWN

A CRIMINAL INVESTIGATION

§  
§  
§  
§  
§

THE STATE OF TEXAS

HEMPHILL COUNTY

McGWIER

**ORDER FOR DISCLOSURE OF HISTORICAL LOCATION-BASED ELECTRONIC COMMUNICATION DATA FOR A MOBILE TELEPHONES**

Came on this day to be heard the Application of the State of Texas for historical location-based information, as authorized by 18 U.S.C. §3117(a), 2703(d), and Article 18.21 §14, Texas Code of Criminal Procedure, related to telephone number (720) 415-7672 associated with Nathan McGwier and/or Thomas Brown. The target telephone (720) 415-7672 is a mobile telephone instrument.

IT APPEARING that the application has been made in good faith in the furtherance of a pending missing person investigation, and it appearing, based on the underlying specific articulable fact based affidavit of an authorized peace officer, Brent Clapp, with the Hemphill County Sheriff's Office, which has offered probable cause that any and all subscriber information and incoming and outgoing call detail records with cell site information for the target telephone (720) 415-7672 will be relevant and material to an ongoing missing person investigation.

IT IS ORDERED, pursuant to Article 18.21 §14 C.C.P., that Celco Partnership, dba Verizon Wireless, (hereinafter "common communications carrier") disclose subscriber information and incoming and outgoing call detail records with cell site information that will assist the law enforcement agency and the Federal Bureau of Investigation (FBI) in determining the locations of the target telephone (720) 415-7672 (differentiated from the first or last cell-site used to make or receive a call, which simply identifies the location of the common communications carrier infrastructure) during the specified date range of 11/20/2016 to 04/07/2017.

IT IS ORDERED that the common communications carriers provide to the law enforcement agency and/or the FBI any and all subscriber information to include the MBID/ESN/MIN/IMSI, any and all historical incoming and outgoing call, SMS text, and MMS call detail records with cell site information for target telephone (720) 415-7672 for the specified date range of 11/20/2016 to 04/07/2017.

IT IS ORDERED that the common communications carriers provide all records and information in a commercially reasonable electronic format specified by the law enforcement agency and/or the FBI; and that the common communications carrier deliver all records forthwith via electronic mail (unless otherwise specified) to the email address specified by Affiant at the intervals requested.

IT IS ORDERED that the normal operations of the common communications carriers shall not be disrupted and that the common communications carriers be compensated at the prevailing rates by the State of Texas, through the law enforcement agency and/or the FBI; and

IT IS FURTHER ORDERED that the common communications carriers, its agents and employees shall not disclose to any person outside of this investigation the existence of this order, application, and affidavit, the existence of this investigation or the existence of the location based information provided under the authority of this order, unless otherwise ordered by the Court;

IT IS FURTHER ORDERED that this authorization shall extend to any changes in any of the following data occurring during the period for which the order authorizing the historical location-based data and records are in effect for the target telephone (720) 415-7672: the telephone number, the telephone instrument, or the MEID/ESN/IMSI; provided that the subscriber, the common communications carrier, and either the telephone number, the telephone instrument, or the MBID/ESN/IMSI remained the same; and further provided that the Court is notified without

reasonable delay of any changes in the telephone numbers, the telephone instruments, or the MEID/ESN/IMSI;


IT IS ORDERED that this order, application, and affidavit any amendments thereto be placed under the seal of the Court until further order of the Court; and

IT IS FURTHER ORDERED, consistent with the provisions of Article 18.21 §10, TEX. CODE CRIM. PROC., that no cause of action shall lie against the common communications carriers for complying with this order,

~~IT IS FURTHER ORDERED~~ that the law enforcement agency and the FBI be allowed to receive the historical records within a period not to exceed ten (10) days after the date the order is entered, and further that any reasonable costs incurred during the period covered by the court are to be reimbursed to the common communications carriers by the law enforcement agency and/or the FBI.

Entered and signed this 7<sup>th</sup> day of April, 2017,

at 1:45 o'clock p.m., to certify which witness my hand this day.

  
\_\_\_\_\_  
DISTRICT JUDGE  
3<sup>rd</sup> DISTRICT COURT  
223d

IN THE MATTER OF

THOMAS BROWN

A CRIMINAL INVESTIGATION

§  
§  
§  
§  
§

THE STATE OF TEXAS

HEMPHILL COUNTY

**AFFIDAVIT REQUESTING AN ORDER FOR DISCLOSURE OF HISTORICAL  
LOCATION-BASED ELECTRONIC COMMUNICATIONS DATA FOR A MOBILE  
TELEPHONES**

The affiant, Brent Clapp, a peace officer employed by the Hemphill County Sheriff's Office (hereinafter "law enforcement agency"), located at 401 Purcell, Canadian, Texas, do have probable cause to make this application for a court order authorizing Celco Partnership, dba Verizon Wireless (hereinafter "common communications carrier") to provide authorized commissioned peace officers of the Hemphill County Sheriff's Office and agents of the Federal Bureau of Investigation (FBI), disclosure historical location-based data, as authorized by 18 U.S.C. §3117(a), 2703(d), and Article 18.21, Texas Code of Criminal Procedure, related to telephone number (720) 415-7672 associated with Nathan McGwier and/or Thomas Brown. The target telephone (720) 415-7672 is a mobile telephone instrument.

In support, the Affiant respectfully shows the court as follows: On 11/24/2016, at approximately 2:30 a.m., Thomas Kelly Brown, born 09/13/1998, was reported missing by his mother, Penny Meek, born 01/12/1966. Thomas had last been seen with friends in Canadian at approximately 11:30 p.m. on November 23<sup>rd</sup>. Brown was to be home by midnight according to his mother Penny. Deputies were dispatched and conducted a search of places in Hemphill County that were known to be frequented by Brown and his acquaintances. Deputies Gregory and DeHerrera searched until approximately 6:00 a.m. when Sheriff Lewis and Deputy J. Ortega took over the search.

Several attempts were made by family and friends to contact Brown on his cell phone (806) 282-5391 shortly after midnight, but all attempts went straight to voicemail leading investigators to believe his phone was powered off.

At approximately 9:30 a.m. Brown's vehicle was located abandoned near the sewer treatment ponds on the north edge of the city. Video surveillance in the area showed Brown's vehicle arriving in the area where it was left shortly before 6:00 a.m. on 11/24/2016. Texas



Game Warden Derrick Nalls was contacted to provide his tracking K9. The area was thoroughly searched by Warden Nalls, his K9, and Warden Collins. The Wardens completed their search of the area at approximately 4:00 pm with limited success. Nalls explained that his K9 had picked up scent east of the vehicle then lost it. Throughout the next week the area of the Canadian river was extensively searched by air, on foot and horseback. Sometime thereafter, Brown's school backpack was located in some brush near Marvin Lake.

During the course of the investigation, investigators determined the last two people to physically see Brown were Christian Webb and Kaleb King. Further investigation revealed King, Webb, and Brown were all together just before midnight and just before Brown's cell phone was turned off. Webb's cell phone number was confirmed as (806) 323-3117. On 04/06/2017, call detail records were obtained and reviewed for (806) 323-3117. The records showed over 3500 text messages with telephone number (720) 415-7672.

Investigators determined through database checks that (720) 415-7672 was being used by Nathan McGwier. According to database checks and driver's license information, McGwier lives in Denver, Colorado. On 04/06/2017, call detail records were obtained and reviewed for (720) 415-7672. Call records showed contact with only three number with a Texas Panhandle area code. Phone number (720) 415-7672 contacted Webb, Macy Patterson, and Eli Klein. Webb is one of Brown's close friends and was one of the last people who was with Brown before his disappearance. Prior investigation showed Patterson was one of Brown's very close friends with whom he shared a lot of personal feelings with. Patterson currently resides in Denver, Colorado and attends an art academy. Phone number (720) 415-7672 called Klein who played football with Brown last year and graduated last year. Klein was identified as one of Brown's friends. Phone number (720) 415-7672 doesn't contact any other Texas numbers. In addition, further investigation to date showed McGwier has no connections to any persons living or from Texas except for Patterson who lives in Denver, and possibly Webb with whom he became friends with on social media. Phone number (720) 415-7672 began to contact Macy Patterson on 11/24/2016. Further, it began contacting Webb on 12/26/2016 and contacted Klein on 02/19/2016 which are all contacts after his disappearance. From 12/26/2016 to 04/06/2017, phone number (720) 415-7672 exchanged text messages with Webb 3550 times. Records also

showed the phone was in the region or area of western Oklahoma on 11/23/2016 which is the night Brown disappeared. Investigators believe that if Brown is alive, he may be using McGwier's cell phone, (720) 415-7672, to contact close friends. Cellsite and location information will assist investigators in identifying persons involved in Brown's disappearance and possibly in locating Brown.

I.

The Affiant is a peace officer commissioned by the law enforcement agency, assigned as the Chief Deputy of the Hemphill County Sheriff's Office, and the Affiant is an authorized peace officer as that term is defined in Article 18.21 §1(2), Texas Code of Criminal Procedure and 18 U.S.C. §3105.

II.

The Affiant seeks a court order authorizing the common communications carrier to disclose location-based data that will assist the above law enforcement agency and the FBI in determining the historical locations of the target telephone (720) 415-7672 (differentiated from the first or last cell-site used to make or receive a call, which simply identifies the location of the telephone company's infrastructure). Further, that the common communications carrier provide historical call detail records, including incoming and outgoing calls, SMS messages, MMS messages, and data connections with cell site information for target telephone from 11/20/2016 to 04/07/2017.

III.

The affiant believes that information obtained from the order authorizing location-based data will likely produce information that is relevant and material to an ongoing missing person investigation. In support, the affiant respectfully shows the court as follows: That subscriber information and historical call detail records with cellsite information for target telephone (720) 415-7672 for the specified date range of 11/20/2016 to 04/07/2017 may show approximate locations for McGwier and/or Brown before, during, and after Brown was reported missing. Records may show their last known approximate locations providing investigators with an area to search and/or conduct additional investigation which may lead to Brown's recovery. Records may also reveal contacts, associates, friends, and family members who may provide information and/or evidence crucial to this investigation or who may be suspects in Brown's disappearance. Therefore, your Affiant is

requesting the Court grant an order for any and all subscriber information, historical incoming and outgoing call, text, and MMS call detail records with cell site information for target telephone (720) 415-7672 for the specified date range of 11/20/2016 to 04/07/2017.

IV.

The common communications carrier has refused to provide the law enforcement agency access to location-based information without being served with an appropriate court order.

V.

That the court shall seal the application and order upon issuance of the order, as authorized by Article 18.21, §2(g), Texas Code of Criminal Procedure.

VI.

That the investigation is extensive and ongoing and that to reveal access by the law enforcement agency and the FBI to the location-based information related to the target telephone to anyone outside the investigation would severely jeopardize the investigation; therefore, information regarding access by the law enforcement agency and the FBI to the location-based information should not be revealed by common communications carrier or its employees to any person outside the investigation, except as authorized by the court.

VII.

The common communications carrier should be ordered not to reveal any information about the entry of this order, application, or affidavit in this matter and that subsequent access by the law enforcement agency and the FBI to the location-based data.

VIII.

The State is requesting that the law enforcement agency and the FBI be allowed to receive location-based information within a period not to exceed ten (10) days after the date the order is entered, and further that any reasonable costs incurred during the period covered by the court are to be reimbursed to the common communications carrier by the law enforcement agency and/or the FBI.

IX.

The Affiant request that this authorization extend to any changes in the event that any two of the following occurs during the period for which the order authorizing the release of historical

location-based data and records for the target telephone (720) 415-7672 occurs: the telephone number, the telephone instrument, or the MEID/ESN/IMSI, change; provided that both the subscribers, and either the telephone numbers, the telephone instruments, or the MEID/ESN/IMSI remain the same;

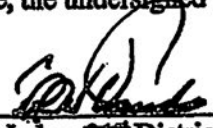
**WHEREFORE, PREMISED CONSIDERED**, the State respectfully requests that the Court enter an order directing the common communications carrier to provide the law enforcement agency and the FBI with all call detail records with cell site information pertaining to the location of the target telephone (720) 415-7672 and technical assistance necessary to interpret the data provided. Further, that all records and information required be provided in a commercially reasonable electronic format specified by the law enforcement agency; and that all records are delivered forthwith via electronic mail (unless otherwise specified) to the email address specified by Affiant, at the intervals requested.

**IT IS FURTHER REQUESTED** that the Court seal the order, application and affidavit, and further that the Court order the common communications carrier, their agents and employees not to divulge, reveal, or disclose the existence of the order, application, and affidavit, the existence of this investigation or the existence of the location-based data to any person outside this investigation, unless otherwise ordered by the Court.

  
\_\_\_\_\_  
PEACE OFFICER  
HEMPHILL COUNTY, TEXAS

SUBSCRIBED AND SWORN TO before me, the undersigned authority on this the

7 day of April, 2017.

  
\_\_\_\_\_  
District Judge, ~~31<sup>st</sup>~~ District Court, State of Texas  
223d



**IT IS ORDERED** that the common communications carriers provide to the law enforcement agency and/or the FBI any and all subscriber information to include the MEID/ESN/MIN/IMSI, any and all historical incoming and outgoing call, SMS text, and MMS call detail records with cell site information for target telephone (720) 415-7672 for the specified date range of 11/20/2016 to 04/07/2017.

**IT IS ORDERED** that the common communications carriers provide all records and information in a commercially reasonable electronic format specified by the law enforcement agency and/or the FBI; and that the common communications carrier deliver all records forthwith via electronic mail (unless otherwise specified) to the email address specified by Affiant at the intervals requested.

**IT IS ORDERED** that the normal operations of the common communications carriers shall not be disrupted and that the common communications carriers be compensated at the prevailing rates by the State of Texas, through the law enforcement agency and/or the FBI; and

**IT IS FURTHER ORDERED** that the common communications carriers, its agents and employees shall not disclose to any person outside of this investigation the existence of this order, application, and affidavit, the existence of this investigation or the existence of the location based information provided under the authority of this order, unless otherwise ordered by the Court;

**IT IS FURTHER ORDERED** that this authorization shall extend to any changes in any of the following data occurring during the period for which the order authorizing the historical location-based data and records are in effect for the target telephone (720) 415-7672: the telephone number, the telephone instrument, or the MEID/ESN/IMSI; provided that the subscriber, the common communications carrier, and either the telephone number, the telephone instrument, or the MEID/ESN/IMSI remained the same; and further provided that the Court is notified without

reasonable delay of any changes in the telephone numbers, the telephone instruments, or the MEID/ESN/IMSI's;


IT IS ORDERED that this order, application, and affidavit any amendments thereto be placed under the seal of the Court until further order of the Court; and

IT IS FURTHER ORDERED, consistent with the provisions of Article 18.21 §10, TEX. CODE CRIM. PROC., that no cause of action shall lie against the common communications carriers for complying with this order,

IT IS FURTHER ORDERED that the law enforcement agency and the FBI be allowed to receive the historical records within a period not to exceed ten (10) days after the date the order is entered, and further that any reasonable costs incurred during the period covered by the court are to be reimbursed to the common communications carriers by the law enforcement agency and/or the FBI.

Entered and signed this 1<sup>st</sup> day of April, 2017,

at 1:45 o'clock p.m., to certify which witness my hand this day.

  
\_\_\_\_\_  
DISTRICT JUDGE  
3<sup>rd</sup> DISTRICT COURT  
223d

IN THE MATTER OF

THOMAS BROWN

A CRIMINAL INVESTIGATION

§  
§  
§  
§  
§

THE STATE OF TEXAS

HEMPHILL COUNTY

**AFFIDAVIT REQUESTING AN ORDER FOR DISCLOSURE OF HISTORICAL  
LOCATION-BASED ELECTRONIC COMMUNICATIONS DATA FOR A MOBILE  
TELEPHONES**

The affiant, Brent Clapp, a peace officer employed by the Hemphill County Sheriff's Office (hereinafter "law enforcement agency"), located at 401 Purcell, Canadian, Texas, do have probable cause to make this application for a court order authorizing Cellco Partnership, dba Verizon Wireless (hereinafter "common communications carrier") to provide authorized commissioned peace officers of the Hemphill County Sheriff's Office and agents of the Federal Bureau of Investigation (FBI), disclosure historical location-based data, as authorized by 18 U.S.C. §3117(a), 2703(d), and Article 18.21, Texas Code of Criminal Procedure, related to telephone number (720) 415-7672 associated with Nathan McGwier and/or Thomas Brown. The target telephone (720) 415-7672 is a mobile telephone instrument.

In support, the Affiant respectfully shows the court as follows: On 11/24/2016, at approximately 2:30 a.m., Thomas Kelly Brown, born 09/13/1998, was reported missing by his mother, Penny Meek, born 01/12/1966. Thomas had last been seen with friends in Canadian at approximately 11:30 p.m. on November 23<sup>rd</sup>. Brown was to be home by midnight according to his mother Penny. Deputies were dispatched and conducted a search of places in Hemphill County that were known to be frequented by Brown and his acquaintances. Deputies Gregory and DeHerrera searched until approximately 6:00 a.m. when Sheriff Lewis and Deputy J. Ortega took over the search.

Several attempts were made by family and friends to contact Brown on his cell phone (806) 282-5391 shortly after midnight, but all attempts went straight to voicemail leading investigators to believe his phone was powered off.

At approximately 9:30 a.m. Brown's vehicle was located abandoned near the sewer treatment ponds on the north edge of the city. Video surveillance in the area showed Brown's vehicle arriving in the area where it was left shortly before 6:00 a.m. on 11/24/2016. Texas



Game Warden Derrick Nalls was contacted to provide his tracking K9. The area was thoroughly searched by Warden Nalls, his K9, and Warden Collins. The Wardens completed their search of the area at approximately 4:00 pm with limited success. Nalls explained that his K9 had picked up scent east of the vehicle then lost it. Throughout the next week the area of the Canadian river was extensively searched by air, on foot and horseback. Sometime thereafter, Brown's school backpack was located in some brush near Marvin Lake.

During the course of the investigation, investigators determined the last two people to physically see Brown were Christian Webb and Kaleb King. Further investigation revealed King, Webb, and Brown were all together just before midnight and just before Brown's cell phone was turned off. Webb's cell phone number was confirmed as (806) 323-3117. On 04/06/2017, call detail records were obtained and reviewed for (806) 323-3117. The records showed over 3500 text messages with telephone number (720) 415-7672.

Investigators determined through database checks that (720) 415-7672 was being used by Nathan McGwier. According to database checks and driver's license information, McGwier lives in Denver, Colorado. On 04/06/2017, call detail records were obtained and reviewed for (720) 415-7672. Call records showed contact with only three number with a Texas Panhandle area code. Phone number (720) 415-7672 contacted Webb, Macy Patterson, and Eli Klein. Webb is one of Brown's close friends and was one of the last people who was with Brown before his disappearance. Prior investigation showed Patterson was one of Brown's very close friends with whom he shared a lot of personal feelings with. Patterson currently resides in Denver, Colorado and attends an art academy. Phone number (720) 415-7672 called Klein who played football with Brown last year and graduated last year. Klein was identified as one of Brown's friends. Phone number (720) 415-7672 doesn't contact any other Texas numbers. In addition, further investigation to date showed McGwier has no connections to any persons living or from Texas except for Patterson who lives in Denver, and possibly Webb with whom he became friends with on social media. Phone number (720) 415-7672 began to contact Macy Patterson on 11/24/2016. Further, it began contacting Webb on 12/26/2016 and contacted Klein on 02/19/2016 which are all contacts after his disappearance. From 12/26/2016 to 04/06/2017, phone number (720) 415-7672 exchanged text messages with Webb 3550 times. Records also

The Affiant believes that information obtained from the order authorizing location-based data will likely produce information that is relevant and material to an ongoing missing person investigation. In support, the affiant respectfully shows the court as follows: That subscriber information and historical call detail records with cellsite information for target telephone (720) 415-7672 for the specified date range of 11/20/2016 to 04/07/2017 may show approximate locations for McGwier and/or Brown before, during, and after Brown was reported missing. Records may show their last known approximate locations providing investigators with an area to search and/or conduct additional investigation which may lead to Brown's recovery. Records may also reveal contacts, associates, friends, and family members who may provide information and/or evidence crucial to this investigation or who may be suspects in Brown's disappearance. Therefore, your Affiant is

### III

The Affiant seeks a court order authorizing the common communications carrier to disclose location-based data that will assist the above law enforcement agency and the FBI in determining the historical locations of the target telephone (720) 415-7672 (differentiated from the first or last cell-site used to make or receive a call, which simply identifies the location of the telephone company's infrastructure). Further, that the common communications carrier provide historical call detail records, including incoming and outgoing calls, SMS messages, MMS messages, and data connections with cell site information for target telephone from 11/20/2016 to 04/07/2017.

### II

The Affiant is a peace officer commissioned by the law enforcement agency, assigned as the Chief Deputy of the Hemphill County Sheriff's Office, and the Affiant is an authorized peace officer as that term is defined in Article 18.21 §(2), Texas Code of Criminal Procedure and 18 U.S.C. §3105.

### I

showed the phone was in the region or area of western Oklahoma on 11/23/2016 which is the night Brown disappeared. Investigators believe that if Brown is alive, he may be using McGwier's cell phone, (720) 415-7672, to contact close friends. Cellsite and location information will assist investigators in identifying persons involved in Brown's disappearance and possibly in locating Brown.

requesting the Court grant an order for any and all subscriber information, historical incoming and outgoing call, text, and MMS call detail records with cell site information for target telephone (720) 415-7672 for the specified date range of 11/20/2016 to 04/07/2017.

IV.

The common communications carrier has refused to provide the law enforcement agency access to location-based information without being served with an appropriate court order.

V.

That the court shall seal the application and order upon issuance of the order, as authorized by Article 18.21, §2(g), Texas Code of Criminal Procedure.

VI.

That the investigation is extensive and ongoing and that to reveal access by the law enforcement agency and the FBI to the location-based information related to the target telephone to anyone outside the investigation would severely jeopardize the investigation; therefore, information regarding access by the law enforcement agency and the FBI to the location-based information should not be revealed by common communications carrier or its employees to any person outside the investigation, except as authorized by the court.

VII.

The common communications carrier should be ordered not to reveal any information about the entry of this order, application, or affidavit in this matter and that subsequent access by the law enforcement agency and the FBI to the location-based data.

VIII.

The State is requesting that the law enforcement agency and the FBI be allowed to receive location-based information within a period not to exceed ten (10) days after the date the order is entered, and further that any reasonable costs incurred during the period covered by the court are to be reimbursed to the common communications carrier by the law enforcement agency and/or the FBI.

IX.

The Affiant request that this authorization extend to any changes in the event that any two of the following occurs during the period for which the order authorizing the release of historical

location-based data and records for the target telephone (720) 415-7672 occurs; the telephone number, the telephone instrument, or the MEID/ESN/IMSI, change; provided that both the subscribers, and either the telephone numbers, the telephone instruments, or the MEID/ESN/IMSI remain the same;

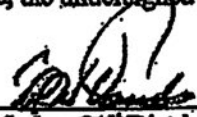
**WHEREFORE, PREMISED CONSIDERED**, the State respectfully requests that the Court enter an order directing the common communications carrier to provide the law enforcement agency and the FBI with all call detail records with cell site information pertaining to the location of the target telephone (720) 415-7672 and technical assistance necessary to interpret the data provided. Further, that all records and information required be provided in a commercially reasonable electronic format specified by the law enforcement agency; and that all records are delivered forthwith via electronic mail (unless otherwise specified) to the email address specified by Affiant, at the intervals requested.

**IT IS FURTHER REQUESTED** that the Court seal the order, application and affidavit, and further that the Court order the common communications carrier, their agents and employees not to divulge, reveal, or disclose the existence of the order, application, and affidavit, the existence of this investigation or the existence of the location-based data to any person outside this investigation, unless otherwise ordered by the Court.

  
\_\_\_\_\_  
PEACE OFFICER  
HEMPHILL COUNTY, TEXAS

SUBSCRIBED AND SWORN TO before me, the undersigned authority on this the

7 day of April, 2017.

  
\_\_\_\_\_  
District Judge, 31<sup>st</sup> District Court, State of Texas  
229

IN THE MATTER OF  
THOMAS BROWN  
A MISSING PERSON INVESTIGATION

§  
§  
§  
§  
§

IN THE DISTRICT COURT  
  
IN AND FOR  
HEMPHILL COUNTY, TEXAS

**ORDER FOR DISCLOSURE OF HISTORICAL ELECTRONIC COMMUNICATIONS  
DATA FOR CELLULAR TELEPHONE TOWERS**

Came on this day to be heard the Application of the State of Texas for an Order requiring cellular telephone service providers Metro PCS, AT&T, Sprint, Verizon, T-Mobile, Cricket Communications, Flat Wireless and Nextel Communications to disclose the records and other information described in Attachment A to this Order.

IT APPEARING that the application has been made in good faith in the furtherance of the missing person investigation, and it appearing, based on the underlying specific articulable fact based affidavit of an authorized peace officer, Brent Clapp, with the Hemphill County Sheriff's Office, which has offered probable cause that the records and other information described in Attachment A to this Order will be relevant and material to ongoing above mentioned investigation.

IT IS ORDERED, pursuant to 18 U.S.C. § 2703(d) and Article 18.21 Sec. 5A, Texas Code of Criminal Procedure, that Metro PCS, AT&T, Sprint, Verizon, T-Mobile, Cricket Communications, Flat Wireless and Nextel Communications to disclose the records and other information described in Attachment A to this Order.

IT IS ORDERED that the common communications carrier provide all records and information described in Attachment A in a commercially reasonable electronic format specified by the law enforcement agency and/or the FBI; and that the common communications carrier deliver all records forthwith via electronic mail (unless otherwise specified) to the email address specified by the law enforcement agency and/or the FBI.

IT IS ORDERED that the normal operations of the common communications carriers shall not be disrupted and that the common communications carriers be compensated at the prevailing rates by the State of Texas, through the law enforcement agency and/or the FBI; and

IT IS FURTHER ORDERED that the common communications carriers, its agents and employees shall not disclose to any person outside of this investigation the existence of this order, application, and affidavit, the existence of this investigation or the existence of the information provided under the authority of this order, unless otherwise ordered by the Court;

IT IS ORDERED that this order, application, and affidavit any amendments thereto be placed under the seal of the Court until further order of the Court; and

IT IS FURTHER ORDERED, consistent with the provisions of Article 18.21 §10, Texas Code of Criminal Procedure, that no cause of action shall lie against the common communications carrier for complying with this order,

IT IS FURTHER ORDERED that the law enforcement agency and the FBI be allowed to receive the records and information described in Attachment A within a period not to exceed ten (10) days after the date the order is entered, and further that any reasonable costs incurred during the period covered by the court are to be reimbursed to the common communications carriers by the law enforcement agency and/or the FBI.

Entered and signed this 25<sup>th</sup> day of January, 2018,

at 8:55 o'clock a.m., to certify which witness my hand this day.

  
DISTRICT JUDGE  
HEMPHILL COUNTY, TEXAS

## ATTACHMENT A

### **I. The Cell Towers**

This Order applies to certain records and information associated with the following cellular telephone towers ("cell towers") at the following dates and times:

<u>Cell Towers</u>	<u>Date</u>	<u>Times</u>
1) The cell towers that provided cellular service to the town of Canadian, Texas 79014	November 23, 2016	From 11:30 pm to 11:59 pm CST
	November 24, 2016	From 12:00 am to 7:00 am CST

### **II. Records and Other Information to Be Disclosed**

For each cell tower described in Part I of this Attachment, the Service Providers named in the Order are required to disclose to the United States all records and other information (not including the contents of communications) about all communications made using the cell tower during the corresponding times listed in Part I, including the records that identify:

- A. The telephone call number and unique identifiers for each wireless device in the vicinity of the tower ("the locally served wireless device") that registered with the tower, including Electronic Serial Numbers ("ESN"), Mobile Electronic Identity Numbers ("MEIN"), Mobile Identification Numbers ("MIN"), Subscriber Identity Modules ("SIM"), Mobile Subscriber Integrated Services Digital Network Numbers ("MSISDN"), International Mobile Subscriber Identifiers ("IMSI"), and International Mobile Equipment Identities ("IMEI");
- B. The source and destination telephone numbers associated with each communication (including the number of the locally served wireless device and the number of the telephone that called, or was called by, the locally served wireless device);
- C. The date, time, and duration of each communication;
- D. The "sectors" (i.e., the faces of the towers) that received a radio signal from each locally served wireless device; and

- E. The type of communication transmitted through the tower (such as phone call or text message).

These records should include records about communications that were initiated before or terminated after the specified time period, as long as part of the communication occurred during the relevant time period identified in Part I.



IN THE MATTER OF  
THOMAS BROWN  
A MISSING PERSON INVESTIGATION

§  
§  
§  
§  
§

IN THE 31<sup>st</sup> DISTRICT COURT  
IN AND FOR  
HEMPHILL COUNTY, TEXAS

**AFFIDAVIT REQUESTING AN ORDER FOR DISCLOSURE OF HISTORICAL  
ELECTRONIC COMMUNICATIONS DATA FOR CELLULAR TELEPHONE  
TOWERS**

The affiant, Chief Deputy Brent Clapp, a peace officer employed by the Hemphill County Sheriff's Office (hereinafter "law enforcement agency"), located at 401 Purcell, Canadian, Texas, do have probable cause to make this application for a court order requiring Metro PCS, AT&T, Sprint, Verizon Wireless, T-Mobile, Cricket Communications, Flat Wireless, and Nextel Communications (hereinafter "common communications carriers") to provide authorized commissioned peace officers of the Hemphill County Sheriff's Office and agents of the Federal Bureau of Investigation (FBI), disclosure of certain records and other information pertaining to the cellular telephone towers described in Part I of Attachment A. The records and other information to be disclosed are described in Part II of Attachment A. The disclosure of such records are authorized by 18 U.S.C. § 2703(d) and Article 18.21 Sec. 5A, Texas Code of Criminal Procedure.

In support, the Affiant respectfully shows the court as follows: On 11/24/2016, at approximately 2:30 a.m., Thomas Kelly Brown, born 09/13/1998, was reported missing by his mother, Penny Meek, born 01/12/1966. Thomas had last been seen with friends in Canadian at approximately 11:30 p.m. on November 23<sup>rd</sup>. Brown was to be home by midnight according to his mother Penny. Deputies were dispatched and conducted a search of places in Hemphill County that were known to be frequented by Brown and his acquaintances. Deputies Gregory and DeHerrera searched until approximately 6:00 a.m. when Sheriff Lewis and Deputy J. Ortega took over the search.

Several attempts were made by family and friends to contact Brown on his cell phone (806) 282-5391 shortly after midnight, but all attempts went straight to voicemail leading investigators to believe his phone was powered off.

At approximately 9:30 a.m. Brown's vehicle was located abandoned near the sewer treatment ponds on the north edge of the city. Video surveillance in the area showed Brown's

vehicle arriving in the area where it was left shortly before 6:00 a.m. on 11/24/2016. Texas Game Warden Derrick Nalls was contacted to provide his tracking K9. The area was thoroughly searched by Warden Nalls, his K9, and Warden Collins. The Wardens completed their search of the area at approximately 4:00 pm with limited success. Nalls explained that his K9 had picked up scent east of the vehicle then lost it. Throughout the next week the area of the Canadian river was extensively searched by air, on foot and horseback. Sometime thereafter, Brown's school backpack was located in some brush near Marvin Lake.

Investigators have viewed and reviewed video surveillance obtained in Canadian in and around the times that Brown disappeared. Shortly after Brown is believed to have fueled up his Durango at Fronk's gas station, there is video surveillance showing a vehicle matching the description of Brown's Durango driving around the Canadian, Texas until approximately 5:56AM on 11/24/2016.

A tower dump will provide information as to cell phones in the town around the time of Thomas Brown's disappearance that were on and active. Investigators are requesting a court order for tower dump information in order to identify persons who may have been in Canadian, Texas, and active on their cell phone around the time of Brown's disappearance.

#### I.

The Affiant is a peace officer commissioned by the law enforcement agency, assigned to the Amarillo Police Department Special Crimes Unit, and the Affiant is an authorized peace officer as that term is defined in Article 18.21 §1(2), Texas Code of Criminal Procedure and 18 U.S.C. §3105.

#### II.

The Affiant seeks a court order authorizing the common communications carriers to disclose records and other information pertaining to the cellular telephone towers described in Part I of Attachment A and the records and other information described in Part II of Attachment A.

#### III.

The Affiant believes that the facts set forth in the previous section show that there are reasonable grounds to believe that the records and other information described in Attachment A are relevant and material to an ongoing criminal investigation. Specifically, these items will help

the law enforcement agency and the FBI to identify and locate the individual(s) who are responsible for the events described above, and to determine the nature and scope of their activities. Accordingly, the law enforcement agency requests that the common communications carriers be directed to produce all items described in Part II of Attachment A.

#### IV.

The common communications carrier has refused to provide the law enforcement agency access to location-based information without being served with an appropriate court order.

#### V.

That the court shall seal the application and order upon issuance of the order, as authorized by Article 18.21, §2(g), Texas Code of Criminal Procedure.

#### VI.

The law enforcement agency further requests that the Order require the common communications carriers not to notify any person, including individual(s) whose wireless devices connected to the cellular telephone towers described in Part I of Attachment A, of the existence of the Order until further order of the Court. This requirement is justified because the Order relates to an ongoing criminal investigation that is neither public nor known to all of the targets of the investigation, and its disclosure may alert the targets to the ongoing investigation. Accordingly, there is reason to believe that notification of the existence of the Order will seriously jeopardize the investigation, including, among other ways, by giving targets an opportunity to flee or continue flight from prosecution, destroy or tamper with evidence, change patterns of behavior, or notify confederates. 18 U.S.C.

#### VII.

The common communications carrier should be ordered not to reveal any information about the entry of this order, application, or affidavit in this matter and that subsequent access by the law enforcement agency and the FBI to the location-based data.

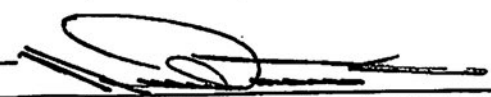
#### VIII.

The State is requesting that the law enforcement agency and the FBI be allowed to receive information pertaining to the cellular telephone towers described in Part I of Attachment A and the records and other information described in Part II of Attachment A within a period not to exceed ten (10) days after the date the order is entered, and further that any reasonable costs incurred during the period covered by the court are to be reimbursed to the common communications carrier by the law enforcement agency and/or the FBI.

**WHEREFORE, PREMISED CONSIDERED,** the State respectfully requests that the Court enter an order directing the common communications carriers to provide the law enforcement agency and the FBI with the records and information described in Attachment A and the technical assistance necessary to interpret the data provided. Further, that all records and information required be provided in a commercially reasonable electronic format specified by the law enforcement agency; and that all records are delivered forthwith via electronic mail (unless otherwise specified) to the email address specified by Affiant, at the intervals requested.

**IT IS FURTHER REQUESTED** that the Court seal the order, application and affidavit, and further that the Court order the common communications carriers, their agents and employees not to divulge, reveal, or disclose the existence of the order, application, and affidavit, the existence of this investigation or the existence of the location-based data to any person outside this investigation, unless otherwise ordered by the Court.

  
\_\_\_\_\_  
PEACE OFFICER  
HEMPHILL COUNTY, TEXAS

SUBSCRIBED AND SWORN TO before me, the undersigned authority on this the  
25 day of January, 2018   
\_\_\_\_\_  
District Judge, Hemphill County, State of Texas

IN THE MATTER OF

§  
§  
§  
§  
§

THE STATE OF TEXAS

THOMAS BROWN

A CRIMINAL INVESTIGATION

HEMPHILL COUNTY

**AFFIDAVIT REQUESTING AN ORDER FOR DISCLOSURE OF HISTORICAL LOCATION-BASED ELECTRONIC COMMUNICATIONS DATA FOR A MOBILE TELEPHONES**

The affiant, Brent Clapp, a peace officer employed by the Hemphill County Sheriff's Office (hereinafter "law enforcement agency"), located at 401 Purcell., Canadian, Texas, do have probable cause to make this application for a court order authorizing AT&T Mobility (hereinafter "common communications carrier") to provide authorized commissioned peace officers of the Hemphill County Sheriff's Office and agents of the Federal Bureau of Investigation (FBI), disclosure historical location-based data, as authorized by 18 U.S.C. §3117(a), 2703(d), and Article 18.21, Texas Code of Criminal Procedure, related to telephone numbers (806) 323-3196 associated with Chris Meek. The target telephone (806) 323-3196 is a mobile telephone instrument.

In support, the Affiant respectfully shows the court as follows: On 11/24/2016, at approximately 2:30 a.m., Thomas Kelly Brown, born 09/13/1998, was reported missing by his mother, Penny Meek, born 01/12/1966. Thomas had last been seen with friends in Canadian at approximately 11:30 p.m. on November 23<sup>rd</sup>. Brown was to be home by midnight according to his mother Penny. Deputies were dispatched and conducted a search of places in Hemphill County that were known to be frequented by Brown and his acquaintances. Deputies Gregory and DeHerrera searched until approximately 6:00 a.m. when Sheriff Lewis and Deputy J. Ortega took over the search.

Several attempts were made by family and friends to contact Brown on his cell phone (806) 282-5391 shortly after midnight, but all attempts went straight to voicemail leading investigators to believe his phone was powered off.

At approximately 9:30 a.m. Brown's vehicle was located abandoned near the sewer treatment ponds on the north edge of the city. Video surveillance in the area showed Brown's vehicle arriving in the area where it was left shortly before 6:00 a.m. on 11/24/2016. Texas

Game Warden Derrick Nalls was contacted to provide his tracking K9. The area was thoroughly searched by Warden Nalls, his K9, and Warden Collins. The Wardens completed their search of the area at approximately 4:00 pm with limited success. Nalls explained that his K9 had picked up scent east of the vehicle then lost it. Throughout the next week the area of the Canadian river was extensively searched by air, on foot and horseback. Sometime thereafter, Brown's school backpack was located in some brush near Marvin Lake.

Investigators have viewed and reviewed video surveillance obtained in Canadian in and around the times that Brown disappeared. Shortly after Brown is believed to have fueled up his Durango at Fronk's gas station, there is video surveillance showing a vehicle matching the description of Brown's Durango driving in the neighborhood towards his home. Investigators maintain the belief that Brown could have made it home on the night he was reported missing. Brown lived with his mother Penny Meek, his step-father, Chris Meek, and his brother, Tucker Brown.

On or about 10/14/2017, a search was organized to search for evidence and clues into Brown's disappearance. During the search, Thomas Brown's cell phone was located in a bar ditch next to the road. The phone was not in its case and the phone did not have any signs of weather or water damage. The phone was clean and did not have any visible scratches. A cell phone in this condition is not consistent with a cell phone that would have been exposed to the elements, weather, and water sitting in a bar ditch for nearly 11 months.

Previous to the search on 10/14/2017, investigators interviewed Kaleb King and Christian Webb. Webb and King were the last people known to have been with Brown on the night he disappeared. During the interview with Webb, she confirmed that King had asked for Brown's passcode to his phone. During the interview with King, he confirmed he did as Webb for the passcode because Tom's mother, Penny Meek, had call his mother and asked King if he knew. In a follow up interview with King's mother, she confirmed Penny Meek was trying to find out Brown's passcode. According to Webb and King and the text messages in their phone, these exchanges happened on or about 01/10/2017.

To date, Penny nor Chris Meek have ever asked investigators about Brown's phone nor advised investigators about any knowledge of Brown's phone's whereabouts. Investigators believe the common public is aware of the storage ability of cell phone, of their evidentiary value

in investigations, and of law enforcement's ability to extract and exploit evidence located on a cell phone.

Prior interviews of Brown's friends revealed that Brown carried his phone inside a case containing an extra battery. Further, friends stated Brown had the phone inside a case on the night he disappeared and he was eccentric about always keeping his phone charged. When the phone was recovered, it was not inside the case. After the phone was recovered in the bar ditch, Penny Meek told investigators that she had Brown's cellphone case.

According to Brown's phone records, the last connected call to Brown's phone was an incoming call from Penny Meek at approximately 12:23AM on 11/24/2016. According to witness statements, Penny Meek and Tucker Brown were awake and contacting persons during the early morning hours of 11/24/2016 regarding Brown's whereabouts. Chris Meek's exact location during those early morning hours on 11/24/2016 and thereafter are unknown and/or uncorroborated.

#### I.

The Affiant is a peace officer commissioned by the law enforcement agency, assigned as the Chief Deputy of the Hemphill County Sheriff's Office, and the Affiant is an authorized peace officer as that term is defined in Article 18.21 §1(2), Texas Code of Criminal Procedure and 18 U.S.C. §3105.

#### II.

The Affiant seeks a court order authorizing the common communications carrier to disclose location-based data (NELOS Report) that will assist the above law enforcement agency and the FBI in determining the historical location of the target telephone (806) 323-3196 (differentiated from the first or last cell-site used to make or receive a call, which simply identifies the location of the telephone company's infrastructure). Further, that the common communications carrier provide historical call detail records, including incoming and outgoing calls, SMS messages, MMS messages, and data connections with cell site information for target telephone from 11/20/2016 to 05/20/2017.

#### III.

The affiant believes that information obtained from the order authorizing location-based data will likely produce information that is relevant and material to an ongoing missing person investigation. In support, the affiant respectfully shows the court as follows: That subscriber information and historical call detail records with cellsite information for target telephone (806) 323-3196 for the specified date range of 11/20/2016 to 05/20/2017 may show approximate locations for Penny Meek and Tucker Brown before, during, and after Thomas Brown was reported missing. Records may show their last known approximate locations providing investigators with an area to search and/or conduct additional investigation which may lead to Brown's recovery. Records may also assist in ruling out Penny Meek and Tucker Brown as potential suspects in Brown's disappearance. Records may reveal contacts, associates, friends, and family members who may provide information and/or evidence crucial to this investigation or who may be suspects in Brown's disappearance. Therefore, your Affiant is requesting the Court grant an order for any and all subscriber information, historical incoming and outgoing call, text, and MMS call detail records with cell site information, and historical location information (NELOS Report) for target telephone (806) 323-3196 for the specified date range of 11/20/2016 to 05/20/2017.

IV.

The common communications carrier has refused to provide the law enforcement agency access to location-based information without being served with an appropriate court order.

V.

That the court shall seal the application and order upon issuance of the order, as authorized by Article 18.21, §2(g), Texas Code of Criminal Procedure.

VI.

That the investigation is extensive and ongoing and that to reveal access by the law enforcement agency and the FBI to the location-based information related to the target telephone to anyone outside the investigation would severely jeopardize the investigation; therefore, information regarding access by the law enforcement agency and the FBI to the location-based information should not be revealed by common communications carrier or its employees to any person outside the investigation, except as authorized by the court.

VII.



The common communications carrier should be ordered not to reveal any information about the entry of this order, application, or affidavit in this matter and that subsequent access by the law enforcement agency and the FBI to the location-based data.

VIII.

The State is requesting that the law enforcement agency and the FBI be allowed to receive location-based information within a period not to exceed ten (10) days after the date the order is entered, and further that any reasonable costs incurred during the period covered by the court are to be reimbursed to the common communications carrier by the law enforcement agency and/or the FBI.

IX.

The Affiant request that this authorization extend to any changes in the event that any two of the following occurs during the period for which the order authorizing the release of historical location-based data and records for the target telephone (806) 323-3196 occurs: the telephone number, the telephone instrument, or the MEID/ESN/IMSI, change; provided that both the subscribers, and either the telephone numbers, the telephone instruments, or the MEID/ESN/IMSI remain the same;

**WHEREFORE, PREMISED CONSIDERED,** the State respectfully requests that the Court enter an order directing the common communications carrier to provide the law enforcement agency and the FBI with all call detail records with cell site information pertaining to the location of the target telephone (806) 323-3196 and technical assistance necessary to interpret the data provided. Further, that all records and information required be provided in a commercially reasonable electronic format specified by the law enforcement agency; and that all records are delivered forthwith via electronic mail (unless otherwise specified) to the email address specified by Affiant, at the intervals requested.

**IT IS FURTHER REQUESTED** that the Court seal the order, application and affidavit, and further that the Court order the common communications carrier, their agents and employees not to divulge, reveal, or disclose the existence of the order, application, and affidavit, the existence of this investigation or the existence of the location-based data to any person outside this investigation, unless otherwise ordered by the Court.

  
PEACE OFFICER  
HEMPHILL COUNTY, TEXAS

SUBSCRIBED AND SWORN TO before me, the undersigned authority on this the  
2<sup>nd</sup> day of November, 2017.

  
District Judge, 31<sup>st</sup> District Court, State of Texas

IN THE MATTER OF  
THOMAS BROWN  
A CRIMINAL INVESTIGATION

§  
§  
§  
§  
§

THE STATE OF TEXAS  
  
HEMPHILL COUNTY

**ORDER FOR DISCLOSURE OF HISTORICAL LOCATION-BASED ELECTRONIC  
COMMUNICATION DATA FOR A MOBILE TELEPHONES**

Came on this day to be heard the Application of the State of Texas for historical location-based information, as authorized by 18 U.S.C. §3117(a), 2703(d), and Article 18.21 §14, Texas Code of Criminal Procedure, related to telephone numbers (806) 323-3196 associated with Chris Meek. The target telephone (806) 323-3196 is a mobile telephone instrument.

IT APPEARING that the application has been made in good faith in the furtherance of a pending missing person investigation, and it appearing, based on the underlying specific articulable fact based affidavit of an authorized peace officer, Brent Clapp, with the Hemphill County Sheriff's Office, which has offered probable cause that any and all subscriber information and incoming and outgoing call detail records with cell site information for the target telephone number (806) 323-3196 will be relevant and material to an ongoing missing person investigation.

IT IS ORDERED, pursuant to Article 18.21 §14 C.C.P., that AT&T Mobility, (hereinafter "common communications carrier") disclose subscriber information and incoming and outgoing call detail records with cell site information that will assist the law enforcement agency and the Federal Bureau of Investigation (FBI) in determining the locations of the target telephone (806) 323-3196 (differentiated from the first or last cell-site used to make or receive a call, which simply identifies the location of the common communications carrier infrastructure) during the specified date range of 11/20/2016 to 05/20/2017.

IT IS ORDERED that the common communications carriers provide to the law enforcement agency and/or the FBI any and all subscriber information to include the

MEID/ESN/MIN/IMSI, any and all historical incoming and outgoing call, SMS text, and MMS call detail records with cell site information for target telephones, and historical location information (NELOS Report) for target telephone (806) 323-3196 for the specified date range of 11/20/2016 to 05/20/2017.

IT IS ORDERED that the common communications carriers provide all records and information in a commercially reasonable electronic format specified by the law enforcement agency and/or the FBI; and that the common communications carrier deliver all records forthwith via electronic mail (unless otherwise specified) to the email address specified by Affiant at the intervals requested.

IT IS ORDERED that the normal operations of the common communications carriers shall not be disrupted and that the common communications carriers be compensated at the prevailing rates by the State of Texas, through the law enforcement agency and/or the FBI; and

IT IS FURTHER ORDERED that the common communications carriers, its agents and employees shall not disclose to any person outside of this investigation the existence of this order, application, and affidavit, the existence of this investigation or the existence of the location based information provided under the authority of this order, unless otherwise ordered by the Court;

IT IS FURTHER ORDERED that this authorization shall extend to any changes in any of the following data occurring during the period for which the order authorizing the historical location-based data and records are in effect for the target telephone (806) 323-3196: the telephone number, the telephone instrument, or the MEID/ESN/IMSI; provided that the subscriber, the common communications carrier, and either the telephone number, the telephone instrument, or the MEID/ESN/IMSI remained the same; and further provided that the Court is notified without

reasonable delay of any changes in the telephone numbers, the telephone instruments, or the MEID/ESN/IMSI's;

IT IS ORDERED that this order, application, and affidavit any amendments thereto be placed under the seal of the Court until further order of the Court; and

IT IS FURTHER ORDERED, consistent with the provisions of Article 18.21 §10, TEX. CODE CRIM. PROC., that no cause of action shall lie against the common communications carriers for complying with this order,

IT IS FURTHER ORDERED that the law enforcement agency and the FBI be allowed to receive the historical records within a period not to exceed ten (10) days after the date the order is entered, and further that any reasonable costs incurred during the period covered by the court are to be reimbursed to the common communications carriers by the law enforcement agency and/or the FBI.

Entered and signed this 2<sup>nd</sup> day of November, 2012.

at 9:05 o'clock a.m., to certify which witness my hand this day.

  
\_\_\_\_\_  
DISTRICT JUDGE  
31<sup>st</sup> DISTRICT COURT

IN THE MATTER OF

THOMAS BROWN

A CRIMINAL INVESTIGATION

§  
§  
§  
§  
§

THE STATE OF TEXAS

HEMPHILL COUNTY

P. MEEK  
TUCKER BROWN

**AFFIDAVIT REQUESTING AN ORDER FOR DISCLOSURE OF HISTORICAL LOCATION-BASED ELECTRONIC COMMUNICATIONS DATA FOR A MOBILE TELEPHONES**

The affiant, Brent Clapp, a peace officer employed by the Hemphill County Sheriff's Office (hereinafter "law enforcement agency"), located at 401 Purcell, Canadian, Texas, do have probable cause to make this application for a court order authorizing AT&T Mobility (hereinafter "common communications carrier") to provide authorized commissioned peace officers of the Hemphill County Sheriff's Office and agents of the Federal Bureau of Investigation (FBI), disclosure historical location-based data, as authorized by 18 U.S.C. §3117(a), 2703(d), and Article 18.21, Texas Code of Criminal Procedure, related to telephone numbers (806) 323-2809 associated with Penny Meek, and (806) 255-0242 associated with Tucker Brown. The target telephones (806) 323-2809 and (806) 255-0242 are mobile telephone instruments.

In support, the Affiant respectfully shows the court as follows: On 11/24/2016, at approximately 2:30 a.m., Thomas Kelly Brown, born 09/13/1998, was reported missing by his mother, Penny Meek, born 01/12/1966. Thomas had last been seen with friends in Canadian at approximately 11:30 p.m. on November 23<sup>rd</sup>. Brown was to be home by midnight according to his mother Penny. Deputies were dispatched and conducted a search of places in Hemphill County that were known to be frequented by Brown and his acquaintances. Deputies Gregory and DeHerrera searched until approximately 6:00 a.m. when Sheriff Lewis and Deputy J. Ortega took over the search.

Several attempts were made by family and friends to contact Brown on his cell phone (806) 282-5391 shortly after midnight, but all attempts went straight to voicemail leading investigators to believe his phone was powered off.

At approximately 9:30 a.m. Brown's vehicle was located abandoned near the sewer treatment ponds on the north edge of the city. Video surveillance in the area showed Brown's vehicle arriving in the area where it was left shortly before 6:00 a.m. on 11/24/2016. Texas

Game Warden Derrick Nalls was contacted to provide his tracking K9. The area was thoroughly searched by Warden Nalls, his K9, and Warden Collins. The Wardens completed their search of the area at approximately 4:00 pm with limited success. Nalls explained that his K9 had picked up scent east of the vehicle then lost it. Throughout the next week the area of the Canadian river was extensively searched by air, on foot and horseback. Sometime thereafter, Brown's school backpack was located in some brush near Marvin Lake.

Investigators have viewed and reviewed video surveillance obtained in Canadian in and around the times that Brown disappeared. Shortly after Brown is believed to have fueled up his Durango at Fronk's gas station, there is video surveillance showing a vehicle matching the description of Brown's Durango driving in the neighborhood towards his home. Investigators maintain the belief that Brown could have made it home on the night he was reported missing.

On or about 10/14/2017, a search was organized to search for evidence and clues into Brown's disappearance. During the search, Thomas Brown's cell phone was located in a bar ditch next to the road. The phone was not in its case and the phone did not have any signs of weather or water damage. The phone was clean and did not have any visible scratches. A cell phone in this condition is not consistent with a cell phone that would have been exposed to the elements, weather, and water sitting in a bar ditch for nearly 11 months.

Previous to the search on 10/14/2017, investigators interviewed Kaleb King and Christian Webb. Webb and King were the last people known to have been with Brown on the night he disappeared. During the interview with Webb, she confirmed that King had asked for Brown's passcode to his phone. During the interview with King, he confirmed he did as Webb for the passcode because Tom's mother, Penny Meek, had call his mother and asked King if he knew. In a follow up interview with King's mother, she confirmed Penny Meek was trying to find out Brown's passcode. According to Webb and King and the text messages in their phone, these exchanges happened on or about 01/10/2017.

To date, Penny Meek never asked investigators about Brown's phone nor advised investigators about any knowledge of Brown's phone's whereabouts. Investigators believe the common public are aware of the storage ability of cell phone, of their evidentiary value in investigations, and of law enforcement's ability to extract and exploit evidence located on a cell phone.

Prior interviews of Brown's friends revealed that Brown carried his phone inside a case containing an extra battery. Further, friends stated Brown had the phone inside a case on the night he disappeared and he was eccentric about always keeping his phone charged. When the phone was recovered, it was not inside the case. After the phone was recovered in the bar ditch, Penny Meek told investigators that she had Brown's cellphone case.

According to Brown's phone records, the last connected call to Brown's phone was an incoming call from Penny Meek at approximately 12:23AM on 11/24/2016. According to witness statements, Penny Meek and Tucker Brown were awake and contacting persons during the early morning hours of 11/24/2016 regarding Brown's whereabouts.

#### I.

The Affiant is a peace officer commissioned by the law enforcement agency, assigned as the Chief Deputy of the Hemphill County Sheriff's Office, and the Affiant is an authorized peace officer as that term is defined in Article 18.21 §1(2), Texas Code of Criminal Procedure and 18 U.S.C. §3105.

#### II.

The Affiant seeks a court order authorizing the common communications carrier to disclose location-based data (NELOS Report) that will assist the above law enforcement agency and the FBI in determining the historical locations of the target telephones (806) 323-2809 and (806) 255-0242 (differentiated from the first or last cell-site used to make or receive a call, which simply identifies the location of the telephone company's infrastructure). Further, that the common communications carrier provide historical call detail records, including incoming and outgoing calls, SMS messages, MMS messages, and data connections with cell site information for target telephone from 11/20/2016 to 05/20/2017.

#### III.

The affiant believes that information obtained from the order authorizing location-based data will likely produce information that is relevant and material to an ongoing missing person investigation. In support, the affiant respectfully shows the court as follows: That subscriber information and historical call detail records with cellsite information for target telephones (806) 323-2809 and (806) 255-0242 for the specified date range of 11/20/2016 to 05/20/2017 may show approximate



locations for Penny Meek and Tucker Brown before, during, and after Thomas Brown was reported missing. Records may show their last known approximate locations providing investigators with an area to search and/or conduct additional investigation which may lead to Brown's recovery. Records may also assist in ruling out Penny Meek and Tucker Brown as potential suspects in Brown's disappearance. Records may reveal contacts, associates, friends, and family members who may provide information and/or evidence crucial to this investigation or who may be suspects in Brown's disappearance. Therefore, your Affiant is requesting the Court grant an order for any and all subscriber information, historical incoming and outgoing call, text, and MMS call detail records with cell site information, and historical location information (NELOS Report) for target telephones (806) 323-2809 and (806) 255-0242 for the specified date range of 11/20/2016 to 05/20/2017.

IV.

The common communications carrier has refused to provide the law enforcement agency access to location-based information without being served with an appropriate court order.

V.

That the court shall seal the application and order upon issuance of the order, as authorized by Article 18.21, §2(g), Texas Code of Criminal Procedure.

VI.

That the investigation is extensive and ongoing and that to reveal access by the law enforcement agency and the FBI to the location-based information related to the target telephone to anyone outside the investigation would severely jeopardize the investigation; therefore, information regarding access by the law enforcement agency and the FBI to the location-based information should not be revealed by common communications carrier or its employees to any person outside the investigation, except as authorized by the court.

VII.

The common communications carrier should be ordered not to reveal any information about the entry of this order, application, or affidavit in this matter and that subsequent access by the law enforcement agency and the FBI to the location-based data.

VIII.

The State is requesting that the law enforcement agency and the FBI be allowed to receive location-based information within a period not to exceed ten (10) days after the date the order is entered, and further that any reasonable costs incurred during the period covered by the court are to be reimbursed to the common communications carrier by the law enforcement agency and/or the FBI.

IX.

The Affiant request that this authorization extend to any changes in the event that any two of the following occurs during the period for which the order authorizing the release of historical location-based data and records for the target telephones (806) 323-2809 and (806) 255-0242 occurs: the telephone number, the telephone instrument, or the MEID/ESN/IMSI, change; provided that both the subscribers, and either the telephone numbers, the telephone instruments, or the MEID/ESN/IMSI remain the same;

**WHEREFORE, PREMISED CONSIDERED,** the State respectfully requests that the Court enter an order directing the common communications carrier to provide the law enforcement agency and the FBI with all call detail records with cell site information pertaining to the location of the target telephones (806) 323-2809 and (806) 255-0242 and technical assistance necessary to interpret the data provided. Further, that all records and information required be provided in a commercially reasonable electronic format specified by the law enforcement agency; and that all records are delivered forthwith via electronic mail (unless otherwise specified) to the email address specified by Affiant, at the intervals requested.

**IT IS FURTHER REQUESTED** that the Court seal the order, application and affidavit, and further that the Court order the common communications carrier, their agents and employees not to divulge, reveal, or disclose the existence of the order, application, and affidavit, the existence of this investigation or the existence of the location-based data to any person outside this investigation, unless otherwise ordered by the Court.

  
\_\_\_\_\_  
PEACE OFFICER  
HEMPHILL COUNTY, TEXAS

SUBSCRIBED AND SWORN TO before me, the undersigned authority on this the  
\_\_\_\_ day of \_\_\_\_\_, 201\_\_\_\_.

( ) .

District Judge, 31<sup>st</sup> District Court, State of Texas

( )

( )

IN THE MATTER OF  
THOMAS BROWN  
A CRIMINAL INVESTIGATION

§  
§  
§  
§  
§

THE STATE OF TEXAS  
  
HEMPHILL COUNTY

**ORDER FOR DISCLOSURE OF HISTORICAL LOCATION-BASED ELECTRONIC  
COMMUNICATION DATA FOR A MOBILE TELEPHONES**

Came on this day to be heard the Application of the State of Texas for historical location-based information, as authorized by 18 U.S.C. §3117(a), 2703(d), and Article 18.21 §14, Texas Code of Criminal Procedure, related to telephone numbers (806) 323-2809 associated with Penny Meek, and (806) 255-0242 associated with Tucker Brown. The target telephones (806) 323-2809 and (806) 255-0242 are mobile telephone instruments.

IT APPEARING that the application has been made in good faith in the furtherance of a pending missing person investigation, and it appearing, based on the underlying specific articulable fact based affidavit of an authorized peace officer, Brent Clapp, with the Hemphill County Sheriff's Office, which has offered probable cause that any and all subscriber information and incoming and outgoing call detail records with cell site information for the target telephone numbers (806) 323-2809 and (806) 255-0242 will be relevant and material to an ongoing missing person investigation.

IT IS ORDERED, pursuant to Article 18.21 §14 C.C.P., that AT&T Mobility, (hereinafter "common communications carrier") disclose subscriber information and incoming and outgoing call detail records with cell site information that will assist the law enforcement agency and the Federal Bureau of Investigation (FBI) in determining the locations of the target telephones (806) 323-2809 and (806) 255-0242 (differentiated from the first or last cell-site used to make or receive a call, which simply identifies the location of the common communications carrier infrastructure) during the specified date range of 11/20/2016 to 05/20/2017.

IT IS ORDERED that the common communications carriers provide to the law enforcement agency and/or the FBI any and all subscriber information to include the MEID/ESN/MIN/IMSI, any and all historical incoming and outgoing call, SMS text, and MMS call detail records with cell site information for target telephones, and historical location information (NELOS Report) for target telephones (806) 323-2809 and (806) 255-0242 for the specified date range of 11/20/2016 to 05/20/2017.

IT IS ORDERED that the common communications carriers provide all records and information in a commercially reasonable electronic format specified by the law enforcement agency and/or the FBI; and that the common communications carrier deliver all records forthwith via electronic mail (unless otherwise specified) to the email address specified by Affiant at the intervals requested.

IT IS ORDERED that the normal operations of the common communications carriers shall not be disrupted and that the common communications carriers be compensated at the prevailing rates by the State of Texas, through the law enforcement agency and/or the FBI; and

IT IS FURTHER ORDERED that the common communications carriers, its agents and employees shall not disclose to any person outside of this investigation the existence of this order, application, and affidavit, the existence of this investigation or the existence of the location based information provided under the authority of this order, unless otherwise ordered by the Court;

IT IS FURTHER ORDERED that this authorization shall extend to any changes in any of the following data occurring during the period for which the order authorizing the historical location-based data and records are in effect for the target telephones (806) 323-2809 and (806) 255-0242: the telephone number, the telephone instrument, or the MEID/ESN/IMSI; provided that the subscriber, the common communications carrier, and either the telephone number, the

telephone instrument, or the MEID/ESN/IMSI remained the same; and further provided that the Court is notified without reasonable delay of any changes in the telephone numbers, the telephone instruments, or the MEID/ESN/IMSI;

IT IS ORDERED that this order, application, and affidavit any amendments thereto be placed under the seal of the Court until further order of the Court; and

IT IS FURTHER ORDERED, consistent with the provisions of Article 18.21 §10, TEX. CODE CRIM. PROC., that no cause of action shall lie against the common communications carriers for complying with this order,

IT IS FURTHER ORDERED that the law enforcement agency and the FBI be allowed to receive the historical records within a period not to exceed ten (10) days after the date the order is entered, and further that any reasonable costs incurred during the period covered by the court are to be reimbursed to the common communications carriers by the law enforcement agency and/or the FBI.

Entered and signed this \_\_\_\_\_ day of \_\_\_\_\_, 201 \_\_\_\_\_,

at \_\_\_\_\_ o'clock \_\_.m., to certify which witness my hand this day.

---

DISTRICT JUDGE  
31<sup>st</sup> DISTRICT COURT

**SEARCH WARRANT**

**THE STATE OF TEXAS** §

§

**COUNTY OF HEMPHILL** §

To the Sheriff or any Peace Officer of Hemphill County, Texas, or any Peace Officer of the State of Texas:

Whereas, the Affiant whose name appears on the affidavit attached hereto is a peace officer under the laws of Texas and did heretofore this day subscribe and swear to said affidavit before me (which said affidavit is here now made a part hereof for all purposes and incorporated herein as if written verbatim within the confines of this Warrant), and whereas I find that the verified facts stated by Affiant in said affidavit show that Affiant has probable cause for the belief he/she expresses herein and establishes the existence of proper grounds for issuance of this Warrant;

Now, therefore, you are commanded to enter the suspected place as described in said affidavit, to-wit:

**Instagram, LLC  
1601 Willow Road  
Menlo Park, CA 94025**

At said place you shall search for and, if same be found, seize and bring before me the property described in the affidavit, to-wit:

- a. All stored files, maintained by Instagram, LLC including server storage space, belonging to or associated with the customer or individual subscriber/user account:

**tommy\_gun2.0**

These files may include, but are not limited to: subscriber's full name(s), subscriber's address (es), subscriber's telephone number(s), e-mail address (es) associated with the subscriber(s), account or log-in name(s), any other information pertaining to the identity of the subscriber(s), billing information, credit card or payment information, types of services utilized by the subscriber and the lengths of such services or any other identifying or pertinent records relating to the subscriber, including IP addresses, and

dates and times of uploads of images if available.

b. All business records or files maintained by Instagram, LLC belonging to or associated with the customer or individual subscriber/user **tommy\_gun2.0**. These records may include, but are not limited to: account application information, credit card or other billing information, account access information, user logon information (including secondary user log on names), account usage reports, e-mail transaction information, text messages, images, news group access and posting information and any other information, both in electronic computer data and written record format, that records the activities of these accounts relating to the subscriber's use of the services offered by Instagram, LLC.

c. All stored electronic mail (e-mail) or messages (text messages) of any kind maintained by Instagram, LLC that were sent to, from and/or through the accounts of or associated with the customer or individual subscriber/user account utilizing **tommy\_gun2.0**.

d. All stored electronic content maintained by Instagram, LLC (including Internet history, file transfer protocol logs, text messages, web access logs, electronically stored images, etc.) as well as all connection log files listing all account activity conducted by the subscriber/user associated with the customer or individual subscriber/user account utilizing the username or account name of **tommy\_gun2.0**, including dates, times, methods of connecting (e.g. telnet, ftp, http, etc.), telephone dial-up connection records and any other connection information or Internet traffic data.

e. Any and all email transactions and/ or file transfer protocol logs maintained by Instagram, LLC associated with the screen name or user name of **tommy\_gun2.0**.

**This Court ORDERS the Custodian of Records / Instagram, LLC, 1601 Willow Road, Menlo Park, CA. 94025 shall disclose responsive data, if any, by sending to Sergeant Rachel Kading of the Office of the Texas Attorney General located at 300 West 15<sup>th</sup> Street, Austin TX, 78701 Mail Code 065 by courier service or to PO BOX 12548, Austin TX 78711 MC065 using the US Postal Service, notwithstanding 18 U.S.C. 2252A or similar statute or code, where all received data will be analyzed.**



Further, Affiant is **ORDERED**, pursuant to the provisions of Article 18.10, Texas Code of Criminal Procedure, to retain custody of any property seized pursuant to this Warrant, until further order of this Court or any other court of appropriate jurisdiction shall otherwise direct the manner of safekeeping of said property. This Court grants you leave and authority to remove such seized property from this county, if and only if such removal is necessary for the safekeeping of such seized property by Affiant, or if the provisions of Article 18.10, T.C.C.P. otherwise authorize such removal. Affiant is further **ORDERED** to give notice to this Court, as a part of the inventory to be filed subsequent to the execution of this Warrant, and as required by Article 18.10, T.C.C.P., of the place where the property seized hereunder is kept, stored and held.

Herein fail not but have you then and there this Warrant within ten days, exclusive of the day of its execution, with your return thereon, showing how you executed the same.

ISSUED THIS THE 6<sup>th</sup> day of June, A.D., 2018, at 4:35 o'clock P.M.  
to certify which, witness my hand this day.



---

STEVEN EMMERT, 31<sup>ST</sup> DISTRICT JUDGE  
HEMPHILL COUNTY, TEXAS

**THE STATE OF TEXAS**

,

,

**COUNTY OF HEMPHILL**

,

**AFFIDAVIT FOR SEARCH WARRANT**

BEFORE ME, THE UNDERSIGNED AUTHORITY, PERSONALLY APPEARED THE AFFIANT HEREIN, A PEACE OFFICER UNDER THE LAWS OF TEXAS, WHO, BEING DULY SWORN, ON OATH MADE THE FOLLOWING STATEMENTS:

My name is Rachel Kading and I am commissioned as a peace officer by the Texas Office of the Attorney General.

There is in Menlo Park, California, a Communications Service Provider known as **Instagram, LLC**. Instagram, LLC, is located at **1601 Willow Road, Menlo Park, CA 94025**.

Instagram, LLC, in its capacity as a Communications Service provider, provides individuals or subscribers with access to the worldwide Internet. Instagram, LLC also provides subscribers with communications services such as: e-mail services, photo storage services, chat service, and access solution services. These services allow customers reserve or maintain storage space on Instagram, LLC computer servers. Subscribers can use Instagram, LLC servers to store their electronic communications (commonly known as e-mail, text messages, and/or chat communication), graphic images, text files, file transfer protocol logs, programs, and other types of data or information stored in electronic form.

Said suspected place and premises are in charge of and controlled by each of the following:

**Instagram, LLC**  
**1601 Willow Road**  
**Menlo Park, CA. 94025**

There is at said suspected place and premises the following item(s) which are implements or instruments used in the commission of a crime and, or item(s) constituting evidence of a criminal offense or constituting evidence tending to show that a particular person committed a criminal offense:

- a. All stored files, maintained by Instagram, LLC. including server storage space, belonging to or associated with the customer or individual subscriber/user account:

**tommy\_gun2.0**

These files may include, but are not limited to: subscriber's full name(s), subscriber's address (es), subscriber's telephone number(s), e-mail address (es) associated with the subscriber(s), account or log-in name(s), any other information pertaining to the identity of the subscriber(s), billing information, credit card or payment information, types of services utilized by the subscriber and the lengths of such services or any other identifying or pertinent records relating to the subscriber, including IP addresses, and dates and times of uploads of images if available.

- b. All business records or files maintained by Instagram, LLC belonging to or associated with the customer or individual subscriber/user **tommy\_gun2.0**. These records may include, but are not limited to: account application information, credit card or other billing information, account access information, user logon information (including secondary user log on names), account usage reports, e-mail transaction information, text messages, images, news group access and posting information and any other information, both in electronic computer data and written record format, that records the activities of these accounts relating to the subscriber's use of the services offered by Instagram, LLC.

- c. All stored electronic mail (e-mail) or messages (text messages) of any kind maintained by Instagram, LLC that were sent to, from and/or through the accounts of or associated

with the customer or individual subscriber/user account utilizing **tommy\_gun2.0**.

d. All stored electronic content maintained by Instagram, LLC (including Internet history, file transfer protocol logs, text messages, web access logs, electronically stored images, etc.) as well as all connection log files listing all account activity conducted by the subscriber/user associated with the customer or individual subscriber/user account utilizing the username or account name of **tommy\_gun2.0**, including dates, times, methods of connecting (e.g. telnet, ftp, http, etc.), telephone dial-up connection records and any other connection information or Internet traffic data.

e. Any and all email transactions and/ or file transfer protocol logs maintained by Instagram, LLC associated with the screen name or user name of **tommy\_gun2.0**.

It is the belief of the Affiant, that: the Instagram account of **tommy\_gun2.0**, contains evidence of the offense of Tampering with or Fabricating Physical Evidence, Texas Penal Code section 37.09, a felony offense.

**AFFIANT HAS PROBABLE CAUSE FOR THE SAID BELIEF BY REASON OF THE FOLLOWING FACTS, TO WIT:**

Your Affiant is Rachel Kading, a peace officer certified by The State of Texas, who is currently employed as a Sergeant with the Office of the Texas Attorney General (OAG). Affiant has been a law enforcement officer for over 15 years. Affiant is currently assigned to the Criminal Investigation Division, Special Investigations Unit, where her duties include investigations involving a wide array of criminal offences ranging from simple fraud to homicides. Affiant has specialized training in the areas of criminal investigations, child abuse and exploitation, narcotics and financial crimes, provided by federal, state, and local agencies. Affiant has previously been involved in the execution search warrants involving persons crimes and narcotics.

On January 26, 2018, Hemphill County Sherriff, NATHAN LEWIS, formally asked the Attorney General's Office to assist in the investigation into the disappearance of THOMAS KELLY BROWN, who was last seen on 11-23-16 in Canadian, Texas. Multiple agencies have been assisting Hemphill County in this investigation.

No viable leads had been developed until 10-14-17, when a private investigator hired by the Brown family and deputies from the Hemphill County Sheriff's Office searched an area between Lake Marvin Road and State Highway (SH) 60 in Hemphill County. During the search on 10-14-17, an Apple iPhone 6S (A1688) was located approximately 45 feet from the SH 60 and Lake Marvin Road intersection and approximately 3 feet south of Lake Marvin Road. The Apple iPhone 6S was in near perfect condition and did not appear to have been outside in the elements since BROWN's disappearance on 11-23-16. The roadway had been mowed several times between November 2016 and October of 2017 and received a significant amount of rain during that time. The Apple iPhone 6S's weather sensors had not activated and the phone was free of nicks, scrapes and/or damage it would have sustained if exposed to the elements on the side of the busy roadway. The Apple iPhone 6S was analyzed by the Federal Bureau of Investigation (FBI) and the contents of the phone were provided to this Affiant. The recovered Apple iPhone 6S was identified as belonging to THOMAS KELLY BROWN as identifying information was located on the phone. The Apple iPhone 6S's contents identified that BROWN had social media accounts that he used regularly to communicate with friends and family.

This affiant is also aware that after BROWN disappeared, his Facebook account was no longer visible on Facebook indicating that it had been deactivated. BROWN'S mother, PENNY MEEK, told this affiant, that she didn't know BROWN'S login information and that someone had hacked BROWN's account. PENNY MEEK further stated that BROWN's account was deleted by her private investigator, PHILIP KLIEN. KLIEN advised this affiant, that PENNY MEEK deactivated the account, therefore, she had to know the account login information to do so. It is unknown if MEEK also had access to BROWN'S Instagram account. Additionally, this affiant saw text messages from PENNY MEEK to ROBIN KING that were sent and received on 1-9-17. MEEK was asking KING if she could ask her son KALEB KING if he knew the passcode to BROWN'S phone. This affiant believes MEEK was in possession of BROWN'S phone at that time.

On 3-29-18, BROWN'S mother PENNY MEEK, and his stepfather CHRIS MEEK, were each administered a polygraph examination conducted by the Texas Department of Public Safety polygraph examiner to determine if they had personal knowledge of the circumstances surrounding BROWN's iPhone. PENNY MEEK and CHRIS MEEK both showed signs of deception on the question regarding possessing BROWN's phone after his disappearance. In addition, PENNY MEEK showed signs of deception on questions relating to BROWN'S location and showed deception on having contact with BROWN. Due to the totality of the circumstances, Affiant has probable cause to believe that PENNY MEEK and CHRIS MEEK knowing that an investigation was being conducted on BROWN's disappearance, concealed BROWN's Apple iPhone with intent to impair its availability as evidence in the investigation. Possessing BROWN's iPhone could have allowed PENNY MEEK and CHRIS MEEK to access, to alter, destroy, and or conceal BROWN's social media account, specifically Instagram, with intent to impair its verity, legibility, and/or availability as evidence in the investigation.

In addition, the social media accounts located in BROWN's iPhone 6S included an Instagram account under the username "tommy\_gun2.0". The Apple iPhone 6S's contents only provided the Instagram username and confirmed that the "tommy\_gun2.0" account exists, but did not show content related to the Instagram account. Since there was no Instagram data and/or content located on the phone. This affiant believes the Instagram contents had been deleted from the phone. This affiant believes this due to the fact that other social media and electronic service accounts located inside the cell phone (Snapchat, Facebook, Yahoo, Gmail) all contained data and/or account activity.

Based upon all the foregoing, there is probable cause to believe that evidence and instrumentalities used in the commission of Tampering with or Fabricating Physical Evidence, Texas Penal Code section 37.09, a felony offense are located on the Instagram, LLC account tommy\_gun2.0, currently stored on the computer servers located with:

**Instagram, LLC**  
**1601 Willow Road, Menlo Park, CA. 94025**


By nature of Instagram, LLC being a Communications Provider, it is realized that many other individuals, organizations, businesses, and other entities utilize this company's services and have no association with the subject investigation. These other unnamed individuals, organizations, businesses, and other entities may have various amounts of information maintained in various forms with Instagram, LLC with a reasonable expectation of privacy. It is Affiant's intent that the search conducted at Instagram, LLC be as unobtrusive as possible, and that it relate to the above listed user account associated with the content that may have been deleted or altered. Further, it is Affiant's intent to use whatever means or methodology is on hand to conduct this search, with limited or no interruption of the service provided to these other unnamed individuals. It is for these reasons that Affiant requests that Instagram, LLC locate and isolate the above named information on their servers and make a copy of such information in a readable format to provide to Affiant for review as part of this investigation.

All information noted in this affidavit for search warrant has been related to Affiant by the person(s) and/or source(s) attributed or referenced. Affiant further believes in good faith that the information provided herein to be true and correct. Because the sole purpose of this affidavit is to establish probable cause that a criminal offense has occurred, not every relevant fact known to Affiant, or to other investigators, is included within. Rather, only those facts necessary to establish probable cause have been discussed.

WHEREFORE, AFFIANT ASKS FOR ISSUANCE OF A WARRANT THAT WILL AUTHORIZE THE SEARCH OF SAID SUSPECTED PLACE FOR SAID PROPERTY AND SEIZURE OF THE SAME AND TO TAKE CUSTODY OF ALL SEIZED PROPERTY AND SAFE KEEP SUCH PROPERTY AS PROVIDED BY STATUTE.

  
\_\_\_\_\_  
AFFIANT, SERGEANT RACHEL AKDING

SUBSCRIBED AND SWORN TO BEFORE ME BY SAID AFFIANT ON THIS THE  
6<sup>th</sup> day of June, A.D., 2018.

  
\_\_\_\_\_  
STEVEN EMMERT, 31<sup>ST</sup> DISTRICT JUDGE  
HEMPHILL COUNTY, TEXAS



Instagram Search Warrant  
Instagram User Acct: tommy\_gun2.0

**IN RE: Search Warrant for** )  
)  
Instagram Account: )  
User: tommy\_gun2.0 )  
)  
)  
)  
\_\_\_\_\_ )

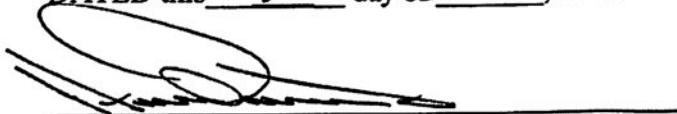
**NON-DISCLOSURE ORDER**

Upon the ex parte application of Sergeant Rachel Kading, a commissioned peace officer with the Office of the Attorney General, this Court orders the non-disclosure of the existence of the search warrant to the account holder. The Office of the Attorney General is conducting an active investigation and Instagram User: tommy\_gun2.0 is related to that investigation. Disclosure to the account holder of the service of this search warrant, at this time, could jeopardize the integrity of the investigation.

**IT IS HEREBY ORDERED** that Instagram not disclose the existence of the attached search warrant pending further order of this Court except that copies may be provided to the office of the 31<sup>st</sup> Judicial District Attorney, and the District Attorney may provide copies to a defendant in a criminal proceeding as part of the criminal discovery process, and;

**IT IS FURTHER ORDERED** that a copy of this non-disclosure order be left at the premises along with the search warrant.

DATED this 1<sup>st</sup> day of June, 2018.



Honorable Steven Emmert  
31<sup>st</sup> Judicial District Court

**THE STATE OF TEXAS**

§

§

**COUNTY OF HEMPHILL**

§

**SEARCH WARRANT**

To the Sheriff or any Peace Officer of Hemphill County, Texas, or any Peace Officer of the State of Texas:

Whereas, the Affiant whose name appears on the affidavit attached hereto is a peace officer under the laws of Texas and did heretofore this day subscribe and swear to said affidavit before me (which said affidavit is here now made a part hereof for all purposes and incorporated herein as if written verbatim within the confines of this Warrant), and whereas I find that the verified facts stated by Affiant in said affidavit show that Affiant has probable cause for the belief he/she expresses herein and establishes the existence of proper grounds for issuance of this Warrant;

Now, therefore, you are commanded to enter the suspected place as described in said affidavit, to-wit:

**Facebook, Inc.  
1601 Willow Road,  
Menlo Park, CA 94025**

At said place you shall search for and, if same be found, seize and bring before me the property described in the affidavit for the said Facebook, Inc account(s), to-wit:

**Facebook User ID: 100004122395944**

a. All stored files, maintained by Facebook, Inc. including server storage space,

belonging to or associated with the said customer or individual subscriber/user accounts.

These files may include, but are not limited to: subscriber's full name(s), subscriber's address (es), subscriber's telephone number(s), e-mail address(es) associated with the subscriber(s), account or log-in name(s), any other information pertaining to the identity of the subscriber(s), billing information, credit card or payment information, types of services utilized by the subscriber and the lengths of such services or any other identifying or pertinent records relating to the subscriber, including IP addresses, and dates and times of uploads of images if available.

b. All business records or files maintained by Facebook, Inc. belonging to or associated with the said customer or individual subscriber/user accounts.

These records may include, but are not limited to: account application information, credit card or other billing information, account access information, user logon information (including secondary user log on names), account usage reports, e-mail transaction information, text messages, images, news group access and posting information and any other information, both in electronic computer data and written record format, that records the activities of these accounts relating to the subscriber's use of the services offered by Facebook, Inc.

c. All stored electronic mail (e-mail) or messages (text messages) of any kind sent to, from and/or through the accounts of or associated with the said customer or individual subscriber/user accounts.

d. All stored electronic content (including Internet history, file transfer protocol logs, text messages, web access logs, electronically stored images, etc.) as well as all connection log files listing all account activity conducted by the subscriber/user associated with the said customer or individual subscriber/user accounts.

**Include dates, times, methods of connecting (e.g. telnet, ftp, http, etc.), telephone dial-up connection records and any other connection information or Internet traffic data.**

**e. Any and all email transactions and/ or file transfer protocol logs associated with said customer or individual subscriber/user accounts.**

**f. Any and all data or images, including metadata, associated with said customer or individual subscriber/user accounts.**

**g. Basic Facebook, Inc. subscriber information (BSI) for Facebook, Inc. accounts associated with said customer or individual subscriber/user accounts.**

**Include, but not limit to, user identification numbers, e-mail addresses, date and time stamps of account creation date display in GMT, most recent logins in GMT, registered mobile numbers, and verification on whether the associated accounts are publicly viewable.**

**i. Any Neoprint information associated with said customer or individual subscriber/user accounts.**

**Include, but is not limit to, profile contact information, mini-feed, status update history, shares, notes, wall postings, friend listing with friends Facebook ID's, group listings with Facebook Group ID's, future and past events and video listing with filenames.**

**This Court ORDERS the Custodian of Records / Facebook, Inc. 1601 Willow Road, Menlo Park, CA 94025 to collect all data, as previously outlined within this warrant, and to present said data to Sergeant Rachel Kading of the Office of the Texas Attorney General located at 300 West 15<sup>th</sup> Street, Austin TX, 78701 Mail Code 065 by courier service or to PO BOX**

12548, Austin TX 78711 MC065 using the US Postal Service, notwithstanding 18 U.S.C. 2252A or similar statute or code, where all received data will be analyzed.

Further, Affiant is **ORDERED**, pursuant to the provisions of Article 18.10, Texas Code of Criminal Procedure, to retain custody of any property seized pursuant to this Warrant, until further order of this Court or any other court of appropriate jurisdiction shall otherwise direct the manner of safekeeping of said property. This Court grants you leave and authority to remove such seized property from this county, if and only if such removal is necessary for the safekeeping of such seized property or for completion of forensic analysis, or if the provisions of Article 18.10, T.C.C.P. otherwise authorize such removal. Affiant is further **ORDERED** to give notice to this Court, as a part of the inventory to be filed subsequent to the execution of this Warrant, and as required by Article 18.10, T.C.C.P., of the place where the property seized hereunder is kept, stored and held.

Herein fail not, but have you then and there this Warrant within ten days, exclusive of the day of its execution, with your return thereon, showing how you executed the same.

ISSUED THIS THE 12<sup>th</sup> day of June, A.D., 2018, at 3:45 o'clock P.M.  
to certify which, witness my hand this day.



STEVEN EMMERT, 31<sup>ST</sup> DISTRICT JUDGE  
HEMPHILL COUNTY, TEXAS

**THE STATE OF TEXAS** §  
§  
**COUNTY OF HEMPHILL** §

**AFFIDAVIT FOR SEARCH WARRANT**

BEFORE ME, THE UNDERSIGNED AUTHORITY, PERSONALLY APPEARED THE AFFIANT HEREIN, A PEACE OFFICER UNDER THE LAWS OF TEXAS, WHO, BEING DULY SWORN, ON OATH MADE THE FOLLOWING STATEMENTS:

My name is Rachel Kading and I am commissioned as a peace officer by the Office of the Attorney General.

There is in Menlo Park, California, a Communications Service Provider known as **Facebook, Inc.** Facebook, Inc. is located at **1601 Willow Road, Menlo Park, CA 94025.** Facebook, Inc., in its capacity as a Communications Service provider, provides individuals or subscribers with access to the worldwide Internet. Facebook, Inc. also provides subscribers with communications services such as: e-mail services, photo storage services, chat service, and access solution services. These services allow customers reserve or maintain storage space on Facebook, Inc. computer servers. Subscribers can use the servers of Facebook, Inc. to store their electronic communications (commonly known as e-mail or text messages), images, graphic images, text files, file transfer protocol logs, programs, and other types of data or information stored in electronic form.

Said suspected place and premises are in charge of and controlled by each of the following:

**Custodian of Records, Facebook, Inc.**  
**1601 Willow Road, Menlo Park, CA 94025**

There is at said suspected place and premises the following item(s) which are implements or instruments used in the commission of a crime and, or item(s) constituting evidence of a criminal offense or constituting evidence tending to show that a particular person committed a criminal offense. Said evidence is located in and associated with the Facebook, Inc. account(s), to-wit:

**Facebook User ID: 100004122395944**

a. Stored files, maintained by Facebook, Inc. including server storage space, belonging to or associated with the customer or individual subscriber/user accounts with the said customer or individual subscriber/user accounts.

These files may include, but are not limited to: subscriber's full name(s), subscriber's address(es), subscriber's telephone number(s), e-mail address(es) associated with the subscriber(s), account or log-in name(s), any other information pertaining to the identity of the subscriber(s), billing information, credit card or payment information, types of services utilized by the subscriber and the lengths of such services or any other identifying or pertinent records relating to the subscriber, including IP addresses, dates and times of uploads of images if available, location data and searches.

b. Business records or files, maintained by Facebook, Inc. belonging to or associated with the customer or individual subscriber/users with said customer or individual subscriber/user accounts.

These records may include, but are not limited to: account application information, credit

card or other billing information, account access information, user logon information (including secondary user log on names), account usage reports, e-mail transaction information, text messages, news group access and posting information and any other information, both in electronic computer data and written record format, that records the activities of these accounts relating to the subscriber's use of the services offered by the Internet Solutions Provider.

c. Stored electronic mail (e-mail) or messages (text messages) of any kind received by or sent from the accounts of, or associated with, the customer or individual subscriber/users account utilizing the said customer or individual subscriber/user accounts.

This should include all stored electronic content (including Internet history, file transfer protocol logs, text messages, web access logs, electronically stored images, dates, times, methods of connecting (e.g. telnet, ftp, http, etc.), telephone dial-up connection records and any other connection information or Internet traffic data, etc.) as well as all connection log files listing all account activity conducted by the said customer or individual subscriber/user accounts.

**It is the belief of the Affiant, that: the Facebook account associated with the Facebook User ID of 100004122395944, contains evidence of the offense of Tampering with or Fabricating Physical Evidence, Texas Penal Code section 37.09, a felony offense.**

**AFFIANT HAS PROBABLE CAUSE FOR THE SAID BELIEF BY REASON OF THE FOLLOWING FACTS, TO WIT:**

**Your Affiant is Rachel Kading, a peace officer certified by The State of Texas, who is currently employed as a Sergeant with the Office of the Texas Attorney General (OAG). Affiant has been a law enforcement officer for over 15 years. Affiant is currently assigned to the Criminal**



Investigation Division, Special Investigations Unit, where her duties include investigations involving a wide array of criminal offences ranging from simple fraud to homicides. Affiant has specialized training in the areas of criminal investigations, child abuse and exploitation, narcotics and financial crimes, provided by federal, state, and local agencies. Affiant has previously been involved in the execution search warrants involving persons crimes and narcotics.

On January 26, 2018, Hemphill County Sherriff, NATHAN LEWIS, formally asked the Texas Attorney General's Office to assist in the investigation into the disappearance of THOMAS KELLY BROWN, who was last seen on 11-23-16 in Canadian, Texas. Multiple agencies have been assisting Hemphill County in this investigation.

No viable leads had been developed until 10-14-17, when a private investigator hired by the Brown family and deputies from the Hemphill County Sheriff's Office searched an area between Lake Marvin Road and State Highway (SH) 60 in Hemphill County. During the search on 10-14-17, an Apple iPhone 6S (A1688) was located approximately 45 feet from the SH 60 and Lake Marvin Road intersection and approximately 3 feet south of Lake Marvin Road. The Apple iPhone 6S was in near perfect condition and did not appear to have been outside in the elements since BROWN'S disappearance on 11-23-16. The roadway had been mowed several times between November 2016 and October of 2017 and received a significant amount of rain during that time. The Apple iPhone 6S's weather sensors had not activated and the phone was free of nicks, scrapes and/or damage it would have sustained if exposed to the elements on the side of the busy roadway. The Apple iPhone 6S was analyzed by the Federal Bureau of Investigation (FBI) and the contents of the phone were provided to this Affiant. The recovered Apple iPhone 6S was identified as belonging to THOMAS KELLY BROWN as identifying information was located on the phone. The Apple iPhone 6S's contents identified that BROWN had social media accounts that he used regularly to communicate with friends and family. These accounts included a Facebook account under account identification number 100004122395944. This affiant does not know if all data contained in BROWN'S Facebook account was present on the phone.

**This affiant is also aware that after BROWN disappeared, his Facebook account was no longer visible on Facebook indicating that it had been deactivated. BROWN'S mother, PENNY MEEK, told this affiant, that she didn't know BROWN'S login information and that someone had hacked BROWN's account. PENNY MEEK further stated that BROWN's account was deleted by her private investigator, PHILIP KLIEN. KLIEN advised this affiant that PENNY MEEK deactivated the Facebook account, therefore, she had to know the account login information to do so. Additionally, this affiant saw text messages from PENNY MEEK to ROBIN KING that were sent and received on 1-9-17. MEEK was asking KING if she could ask her son KALEB KING if he knew the passcode to BROWN'S phone. This affiant believes MEEK was in possession of BROWN'S phone at that time.**

**On 3-29-18, PENNY MEEK, and BROWN'S stepfather CHRIS MEEK, were each administered a polygraph examination by a Texas Department of Public Safety polygraph examiner to determine if they had personal knowledge of the circumstances surrounding BROWN's iPhone. PENNY MEEK and CHRIS MEEK both showed signs of deception on the question regarding possessing BROWN's phone after his disappearance. In addition, PENNY MEEK showed signs of deception on questions relating to BROWN'S location and showed deception on having contact with BROWN. Due to the totality of the circumstances, Affiant has probable cause to believe that PENNY MEEK and CHRIS MEEK knowing that an investigation was being conducted on BROWN'S disappearance, concealed BROWN's Apple iPhone with intent to impair its availability as evidence in the investigation. Possessing BROWN's iPhone potentially allowed PENNY MEEK and CHRIS MEEK to access to alter, destroy, and or conceal BROWN'S social media account, specifically Facebook with intent to impair its verity, legibility, and/or availability as evidence in the investigation.**

**Based upon all the foregoing, there is probable cause to believe that evidence and instrumentalities used in the commission of Tampering with or Fabricating Physical Evidence, Texas Penal Code section 37.09, a felony offense are located on the Facebook account associated**

with the **Facebook User ID of 100004122395944**, currently stored on the computer servers located with:

**Facebook, Inc.**  
**1601 Willow Road, Menlo Park, CA 94025**

By nature of Facebook, Inc. being a Communications Provider, it is realized that many other individuals, organizations, businesses, and other entities utilize this company's services and have no association with the subject investigation. These other unnamed individuals, organizations, businesses, and other entities may have various amounts of information maintained in various forms with Facebook, Inc. with a reasonable expectation of privacy. It is Affiant's intent that the search conducted at Facebook, Inc. be as unobtrusive as possible, and that it relate to the above listed user identification number associated with the Online Solicitation of a Minor content only. Further, it is Affiant's intent to use whatever means or methodology is on hand to conduct this search, with limited or no interruption of the service provided to these other unnamed individuals. It is for these reasons that Affiant requests that Facebook, Inc. locate and isolate the above named information on their servers and make a copy of such information in a readable format to provide to Affiant for review as part of this investigation.

All information noted in this affidavit for search warrant has been related to Affiant by the person(s) and/or source(s) attributed or referenced. Affiant further believes in good faith that the information provided herein to be true and correct. Because the sole purpose of this affidavit is to establish probable cause that a criminal offense has occurred, not every relevant fact known to Affiant, or to other investigators, is included within. Rather, only those facts necessary to establish probable cause have been discussed.

WHEREFORE, AFFIANT ASKS FOR ISSUANCE OF A WARRANT THAT WILL AUTHORIZE THE SEARCH OF SAID SUSPECTED PLACE FOR SAID PROPERTY AND SEIZURE OF THE SAME AND TO TAKE CUSTODY OF ALL SEIZED PROPERTY AND SAFE KEEP SUCH PROPERTY AS PROVIDED BY STATUTE.

  
AFFIANT, SERGEANT RACHEL KADING

SUBSCRIBED AND SWORN TO BEFORE ME BY SAID AFFIANT ON THIS THE 1<sup>st</sup> day of June, A.D., 2018.

  
STEVEN EMMERT, 31<sup>ST</sup> DISTRICT JUDGE  
HEMPHILL COUNTY, TEXAS



**SEARCH WARRANT**

**THE STATE OF TEXAS** §

§

**COUNTY OF HEMPHILL** §

To the Sheriff or any Peace Officer of Hemphill County, Texas, or any Peace Officer of the State of Texas:

Whereas, the Affiant whose name appears on the affidavit attached hereto is a peace officer under the laws of Texas and did heretofore this day subscribe and swear to said affidavit before me (which said affidavit is here now made a part hereof for all purposes and incorporated herein as if written verbatim within the confines of this Warrant), and whereas I find that the verified facts stated by Affiant in said affidavit show that Affiant has probable cause for the belief he/she expresses herein and establishes the existence of proper grounds for issuance of this Warrant.

Now, therefore, you are commanded to enter the suspected place as described in said affidavit, to forthwith search the place therein named, to wit:

**AT&T and all subsidiaries including but not limited to New Cingular Wireless**

**AT&T Mobility**

**11760 US Hwy. 1, Suite 600**

**North Palm Beach, FL 33408**

hereinafter, PROVIDER, with the authority to search for and to seize or to compel agents of said PROVIDER to search for, seize and to turn over to the government Electronic Customer Data as defined in the Texas Code of Criminal Procedure (T.C.C.P.) Chapter 18, and held in electronic storage by the PROVIDER for the Electronic Customer Data belonging to or associated with, the customer or individual subscriber/user accounts, from **September 1, 2016 through May 25, 2018.**

**806-323-2809**

At said place you shall search for and, if same be found, seize and bring before me the property described in the affidavit, to-wit:

The Electronic Customer Data that is the subject of this warrant includes:

- 1.) All subscriber information, including any available telephone numbers, email addresses, IP addresses (including ports), etc., and/or unique account, equipment, and/or network addressing, these may include the Electronic Serial Number (ESNs), International Mobile Subscriber Identifier (IMSI), Temporary Mobile Subscriber Identity number (TMSI), International Mobile Equipment Identifiers (IMEIs), Mobile Equipment Identifiers (MEIDs), Mobile Station Identifiers (MSIDs), Mobile Identification Numbers (MINs), Mobile Dialed Numbers (MDN), Integrated Circuit Card IDs (ICCID), Personal Unlocking/Unblocking Codes (PUKs), PINs (personal identification numbers), Blackberry PINs (personal identification numbers/codes), Apple's Unique Device Identifier (ID) (UDID), and/or Media Access Control (MAC) address(es), and all billing/payment information and accounts notes, for the specified cellular/wireless telephones, and for any other cellular/wireless telephones on the same account as the target numbers.
- 2.) All outgoing and incoming communications/call detail records (CDRs), with cell sites, including all telephone numbers, chirp numbers/direct connects/walkie-talkie/Universal Fleet Mobile Identifier (UFMI) numbers, email addresses (electronic mail), Internet Protocol (IP) addresses, World Wide Web (www) addresses, dialed/communicated with (outgoing and/or incoming). This includes local and long distance telephone connection records, including all text [short message service SMS] detail records, email detail records [including IP (Internet Protocol) logs, email header information, and email addresses], IP connection detail records/logs, and video, audio, and/or photo image transactions records, such as multimedia messaging service (MMS) (picture/video messaging) detail records/logs, sent or received, to provide dates, times, and methods of voicemail access, including all available SS7 signaling records of these communications, and, records of session times and durations, and to include content/text of messages if available. Cell Sites are required if they are available on any and all transactional/addressing and routing data.
- 3.) Cell sites activations and all registration information, including signal strengths, logs, etc. (if obtainable), including any location information delivered to a public safety answering point (PSAP) pursuant to a 911 call.
- 4.) If available, an engineering map; showing all cell-site antenna/tower locations, sectors, azimuths, beam widths, pilot PN (pseudo noise) offsets, and true orientations. And, a list of any and all cellular sites numbers [Long Term Evolution (LTE) —complete CGI or eNodeB and Cell Site, NodeB, Local Area Codes (LACs), Cellular Identifiers (CIDs), intercept access points (IAP) system identities, repolls, switches, etc.], locations, addresses, neighbor lists, etc., and/or latitude and

longitude of any said sites. Also, that cellular sites lists, including latitudes and longitudes, be provided, via electronic mail, or via shipping when email is not available, in an electronic format, if available and/or possible. Furthermore, the concerned carrier(s) will provide RF (radio frequency) propagation maps/surveys and cellular antenna/tower maintenance records, and cellular antenna/tower maintenance records procedures, upon request. These maps/surveys and maintenance records will be provided in electronic format, such as original color format, if available.

- 5.) Should the cellular/wireless number/equipment which is the current target of this Order have changed, during the requested period, including the MINs/MSIDs, MDNs, ESNs, MEIDs, IMEIs, IMSIs, ICCIDs, PUKs, IP addresses, UDIDs, PINs and/or MAC addresses, or combinations thereof, have been changed by the subscribers during the period of time(s) covered by this Order, then this Order will apply to any other MINs/MSIDs, MDNs, ESNs, MEIDs, IMEIs, IMSIs, ICCIDs, PUKs, IP addresses, UDIDs, PINs, email addresses, and/or MAC addresses. Furthermore if requested the specific manufacturer and model of said handset shall be released verbally or in writing by the Agency making this request.
- 6.) Any Internet Service Provider (ISP), email company or email server entity (public or private), website hosting company, and/or website or internet service providing company and/or entity, provide any subscriber information, email addresses, email logs (with header information, Internet Protocol (IP) logs, website addresses, etc., for any email addresses, IP addresses, user names, etc., identified from the original records pertaining to the target devices. Such as, if the original target devices' records reveal Internet activity, such as email activity, web activity, and/or other Internet connected applications, then this Order will also order the release of all subscriber information pertaining to user identifying, *and* addressing and routing (transactional) information pertaining to that Internet activity (without content information) for the effective period of this order. This includes application of this Order to Microsoft's "Sidekick"/"Danger" products/services. Also to include all location based information for all Google products (GMAIL, Google Voice, etc.) and all Apple products
- 7.) Also, whenever possible, that the provider(s) provision, upon the specific requests of the prosecutors/officers/agents/designees, a twenty-four (24) hour switch-technician/employee/vendor to assist in providing data to comply with this Order and/or the interpretation of the provided data.
- 8.) Any required information on demand, if possible and upon the specific request of the prosecutors/officers/agents/designees. Further, that any so ordered provider(s), or those possessing said information, provide, upon the specific request of the prosecutors/officers/agents/designees, any historical geo-location services/global positioning system (GPS) data/enhanced 911 (E911) records including but not limited to any available ranging data [distance from tower, range to tower



(RTT/REVEAL/Historic MLTs or other similar un-named records held by ANY PROVIDER)], which may be available to any involved provider(s) and/or parties. This includes specifically Sprint's PCMD data (per call measure data) and AT&T's NLEOs report. This also includes all location data captured by Google and Apple.

- 9.) All call/communication detail, direct connect, subscriber, numeric messages, alpha-numeric/text messages, email records, IP logs, etc., and any related records and/or access be provided, upon the specific request of prosecutors/officers/agents/designees of specific data from specific time period within the confines of this Order, in an electronic format specified by prosecutors/agents/officers/designees. Also, that the records/data be forwarded via email (in a common electronic format as described herein) if possible, upon the specific request of prosecutors/agents/officers/designees, to the listed prosecutor/officer and/or his/her designees. These designees may include, but are not limited to, prosecutors/officers/agents/designees and/or representatives of the Hemphill County District Attorney, Attorney General's Office of Texas (OAG) and the Texas Department of Public Safety (DPS).
  
- 10.) If e-mail is not available/possible, that the providers provide the required data electronically on a common storage medium, such as CD-ROM (compact disc read only memory) discs, and/or thumb drive. Also, that all providers provide, when possible and so requested, all requested data in ASCII, comma separated values (.csv), or fixed length (SDF) format. This is to include that any and all records/data will be provided in all available formats of data, upon request, to include, but not limited to, documents/files currently produced in Microsoft Word, Microsoft Excel, PDF (portable document format), CSV (comma separated value), other electronic formats, and/or pulled from such systems such as "CDR Live," "X-Mine," "CEER," and any other electronic medium that is/was in use and/or in development. All CDRs [call/communication detail records (CDRs), including IP (internet protocol) logs, email logs, etc.] will be provided in spreadsheet (Excel, CSV, etc.) format if possible. Only where this is not possible, to provide information in dark, clean typeface, machine-scanable/Optical Character Recognition (OCR) interpretable hardcopy. This includes the faxing of any necessary requested records at the highest possible quality setting. Further, that upon the specific request of prosecutors/agents/officers/designees, that any provided data, including account specific data and cellular site lists, be provided by the necessary providers in a business records affidavit format that complies with the laws of the State of Texas.
  
- 11.) Provide any and all data and services that are ordered herein, verbally, to prosecutors/officers (or designees) if specifically requested to do so. Communications providers are also ordered to notify prosecutors/officers (or designees) if devices roamed (and what specific networks are roamed to/from) from a home/primary network to another network and it is known by the home/primary network to what roaming network the devices roamed. This includes verbally notifying prosecutors/officers (or designees) of the last known

network registrations/activity during the above mentioned time frame. And, if the accounts were active accounts, including if the account was inactivated or closed for non-payment, and, how many minutes and/or credits remained on prepaid type accounts. The concerned communications carriers are also ordered to retain, indefinitely, hard and soft copies of all records and/or data provided as a result of this Order.

- 12.) **RETAIL OUTLETS OR ANY ENTITIES** are ordered to release, upon specific request, all purchase, payment (cash, credit, check, prepaid card, etc.), and activation information (even if through third parties) for all target devices, accounts, and subsequent payments, such as prepaid minute cards. This includes the specific data, time, location (including the specific store, register, clerk, etc.) that all devices, account changes, purchases, payments, etc., occurred. It is also ordered that all involved retailers (and neighboring businesses/residences) release any available surveillance video from the aforementioned transactions, both from within, and from the outside of the stores, and the area of the stores, where any of the aforementioned transactions occurred.
- 13.) Finally, that this Order will apply to any and all companies/entities which may provide and/or carry wireless/telecommunication services for the target mobile numbers/unique account identifiers/equipment, and/or, any other entity who may possess the requested information, such as Internet companies/entities. This may be required because of number portability and/or if the original carrier was modified due to roaming and/or other considerations/reasons.

**This Court ORDERS the Custodian of Records / AT&T, 11760 US Hwy. 1, North Palm Beach, FL 33408 shall disclose responsive data, if any, by sending to Sergeant Rachel Kading of the Office of the Texas Attorney General located at 300 West 15<sup>th</sup> Street, Austin TX, 78701 Mail Code 065 by courier service or to PO BOX 12548, Austin TX 78711 -MC 065 using the US Postal Service, notwithstanding 18 U.S.C. 2252A or similar statute or code, where all received data will be analyzed.**

Further, Affiant is **ORDERED**, pursuant to the provisions of Article 18.10, Texas Code of Criminal Procedure, to retain custody of any property seized pursuant to this Warrant, until further order of this Court or any other court of appropriate jurisdiction shall otherwise direct the manner of safekeeping of said property. This Court grants you leave and authority to remove such seized property from this county, if and only if such removal is necessary for the safekeeping of such seized property by Affiant, or if the provisions of Article 18.10, T.C.C.P.

otherwise authorize such removal. Affiant is further ORDERED to give notice to this Court, as a part of the inventory to be filed subsequent to the execution of this Warrant, and as required by Article 18.10, T.C.C.P., of the place where the property seized hereunder is kept, stored and held.

Herein fail not but have you then and there this Warrant within ten days, exclusive of the day of its execution, with your return thereon, showing how you executed the same.

ISSUED THIS THE 6<sup>th</sup> day of June A.D., 2018, at 4:35 o'clock P.M.  
to certify which, witness my hand this day.



---

STEVEN EMMERT, 31<sup>ST</sup> DISTRICT JUDGE  
HEMPHILL COUNTY, TEXAS

**THE STATE OF TEXAS** §  
§  
**COUNTY OF HEMPHILL** §

**AFFIDAVIT FOR SEARCH WARRANT**

BEFORE ME, THE UNDERSIGNED AUTHORITY, PERSONALLY APPEARED THE AFFIANT HEREIN, A PEACE OFFICER UNDER THE LAWS OF TEXAS, WHO, BEING DULY SWORN, ON OATH MADE THE FOLLOWING STATEMENTS:

My name is Rachel Kading and I am commissioned as a peace officer by the Texas Office of the Attorney General.

There is in North Palm Beach, Florida, a Communications Service Provider known as **AT&T Mobility, LLC**, located at **11760 US Hwy. 1, Suite 600, North Palm Beach, FL 33408**.

AT&T Mobility, LLC, in its capacity as a Communications Service provider, provides individuals or subscribers with access to mobile phone services used to make phone calls or send and receive text messages. AT&T also provides subscribers with internet services which provide subscribers to e-mail services, photo storage services, chat service, and access solution services. These services allow customers reserve or maintain storage space on AT&T Mobility computer servers. Subscribers can use AT&T servers to store their electronic communications (commonly known as e-mail, text messages, and/or chat communication), graphic images, text files, file transfer protocol logs, programs, and other types of data or information stored in electronic form.

Said suspected place and premises are in charge of and controlled by each of the following:

**AT&T Mobility**  
**11760 US Hwy. 1, Suite 600**  
**North Palm Beach, FL 33408**

There is at said suspected place and premises the following item(s) which are implements or instruments used in the commission of a crime and, or item(s) constituting evidence of a criminal offense or constituting evidence tending to show that a particular person committed a criminal offense:

- a. All stored Electronic Customer Data as defined in the Texas Code of Criminal Procedure (T.C.C.P.) Chapter 18, maintained by AT&T Mobility belonging to or associated with the customer or individual subscriber/user account:

**806-323-2809**

The Electronic Customer Data that is the subject of this warrant includes:

- 1) All subscriber information, including any available telephone numbers, email addresses, IP addresses (including ports), etc., and/or unique account, equipment, and/or network addressing, these may include the Electronic Serial Number (ESNs), International Mobile Subscriber Identifier (IMSI), Temporary Mobile Subscriber Identity number (TMSI), International Mobile Equipment Identifiers (IMEIs), Mobile Equipment Identifiers (MEIDs), Mobile Station Identifiers (MSIDs), Mobile Identification Numbers (MINs), Mobile Dialed Numbers (MDN), Integrated Circuit Card IDs (ICCID), Personal Unlocking/Unblocking Codes (PUKs), PINs (personal identification numbers), Blackberry PINs (personal identification numbers/codes), Apple's Unique Device Identifier (ID) (UDID), and/or Media Access Control (MAC) address(es), and all billing/payment information and accounts notes, for the specified cellular/wireless telephones, and for any other cellular/wireless telephones on the same account as the target numbers.
- 2) All outgoing and incoming communications/call detail records (CDRs), with cell sites, including all telephone numbers, chirp numbers/direct connects/walkie-talkie/Universal Fleet Mobile Identifier (UFMI) numbers, email addresses (electronic mail), Internet Protocol (IP) addresses, World Wide Web (www) addresses, dialed/communicated with (outgoing and/or incoming). This includes local and long distance telephone connection records, including all text [short message service SMS] detail records, email detail records [including IP (Internet Protocol) logs, email header information, and email addresses], IP connection detail records/logs, and video, audio, and/or photo image transactions records, such as multimedia messaging service (MMS) (picture/video messaging) detail records/logs, sent or received, to provide dates, times, and methods of voicemail access, including all available SS7 signaling records of these communications, and, records of session times and durations, and to include content/text of messages if available. Cell Sites are required if they are available on any and all transactional/addressing and routing data.

- 3) Cell sites activations and all registration information, including signal strengths, logs, etc. (if obtainable), including any location information delivered to a public safety answering point (PSAP) pursuant to a 911 call.
- 4) If available, an engineering map; showing all cell-site antenna/tower locations, sectors, azimuths, beam widths, pilot PN (pseudo noise) offsets, and true orientations. And, a list of any and all cellular sites numbers [Long Term Evolution (LTE) —complete CGI or eNodeB and Cell Site, NodeB, Local Area Codes (LACs), Cellular Identifiers (CIDs), intercept access points (IAP) system identities, repolls, switches, etc.], locations, addresses, neighbor lists, etc., and/or latitude and longitude of any said sites. Also, that cellular sites lists, including latitudes and longitudes, be provided, via electronic mail, or via shipping when email is not available, in an electronic format, if available and/or possible. Furthermore, the concerned carrier(s) will provide RF (radio frequency) propagation maps/surveys and cellular antenna/tower maintenance records, and cellular antenna/tower maintenance records procedures, upon request. These maps/surveys and maintenance records will be provided in electronic format, such as original color format, if available.
- 5) Should the cellular/wireless number/equipment which is the current target of this Order have changed, during the requested period, including the MINs/MSIDs, MDNs, ESNs, MEIDs, IMEIs, IMSIs, ICCIDs, PUKs, IP addresses, UDIDs, PINs and/or MAC addresses, or combinations thereof, have been changed by the subscribers during the period of time(s) covered by this Order, then this Order will apply to any other MINs/MSIDs, MDNs, ESNs, MEIDs, IMEIs, IMSIs, ICCIDs, PUKs, IP addresses, UDIDs, PINs, email addresses, and/or MAC addresses. Furthermore if requested the specific manufacturer and model of said handset shall be released verbally or in writing by the Agency making this request.
- 6) Any Internet Service Provider (ISP), email company or email server entity (public or private), website hosting company, and/or website or internet service providing company and/or entity, provide any subscriber information, email addresses, email logs (with header information, Internet Protocol (IP) logs, website addresses, etc., for any email addresses, IP addresses, user names, etc., identified from the original records pertaining to the target devices. Such as, if the original target devices' records reveal Internet activity, such as email activity, web activity, and/or other Internet connected applications, then this Order will also order the release of all subscriber information pertaining to user identifying, *and* addressing and routing (transactional) information pertaining to that Internet activity (without content information) for the effective period of this order. This includes application of this Order to Microsoft's "Sidekick"/"Danger" products/services. Also to include all location based information for all Google products (GMAIL, Google Voice, etc.) and all Apple products

- 7) Also, whenever possible, that the provider(s) provision, upon the specific requests of the prosecutors/officers/agents/designees, a twenty-four (24) hour switch-technician/employee/vendor to assist in providing data to comply with this Order and/or the interpretation of the provided data.
- 8) Any required information on demand, if possible and upon the specific request of the prosecutors/officers/agents/designees. Further, that any so ordered provider(s), or those possessing said information, provide, upon the specific request of the prosecutors/officers/agents/designees, any historical geo-location services/global positioning system (GPS) data/enhanced 911 (E911) records including but not limited to any available ranging data [distance from tower, range to tower (RTT/REVEAL/Historic MLTs or other similar un-named records held by ANY PROVIDER)], which may be available to any involved provider(s) and/or parties. This includes specifically Sprint's PCMD data (per call measure data) and AT&T's NLEOs report. This also includes all location data captured by Google and Apple.
- 9) All call/communication detail, direct connect, subscriber, numeric messages, alphanumeric/text messages, email records, IP logs, etc., and any related records and/or access be provided, upon the specific request of prosecutors/officers/agents/designees of specific data from specific time period within the confines of this Order, in an electronic format specified by prosecutors/agents/officers/designees. Also, that the records/data be forwarded via email (in a common electronic format as described herein) if possible, upon the specific request of prosecutors/agents/officers/designees, to the listed prosecutor/officer and/or his/her designees. These designees may include, but are not limited to, prosecutors/officers/agents/designees and/or representatives of the Hemphill County District Attorney, Attorney General's Office of Texas (OAG) and the Texas Department of Public Safety (DPS).
- 10) If e-mail is not available/possible, that the providers provide the required data electronically on a common storage medium, such as CD-ROM (compact disc read only memory) discs, and/or thumb drive. Also, that all providers provide, when possible and so requested, all requested data in ASCII, comma separated values (.csv), or fixed length (SDF) format. This is to include that any and all records/data will be provided in all available formats of data, upon request, to include, but not limited to, documents/files currently produced in Microsoft Word, Microsoft Excel, PDF (portable document format), CSV (comma separated value), other electronic formats, and/or pulled from such systems such as "CDR Live," "X-Mine," "CEER," and any other electronic medium that is/was in use and/or in development. All CDRs [call/communication detail records (CDRs), including IP (internet protocol) logs, email logs, etc.] will be provided in spreadsheet (Excel, CSV, etc.) format if possible. Only where this is not possible, to provide information in dark, clean typeface, machine-scanable/Optical Character Recognition (OCR) interpretable hardcopy. This includes the faxing of any necessary requested records at the highest possible quality setting. Further, that upon the specific request of

prosecutors/agents/officers/designees, that any provided data, including account specific data and cellular site lists, be provided by the necessary providers in a business records affidavit format that complies with the laws of the State of Texas.

- 11) Provide any and all data and services that are ordered herein, verbally, to prosecutors/officers (or designees) if specifically requested to do so. Communications providers are also ordered to notify prosecutors/officers (or designees) if devices roamed (and what specific networks are roamed to/from) from a home/primary network to another network and it is known by the home/primary network to what roaming network the devices roamed. This includes verbally notifying prosecutors/officers (or designees) of the last known network registrations/activity during the above mentioned time frame. And, if the accounts were active accounts, including if the account was inactivated or closed for non-payment, and, how many minutes and/or credits remained on prepaid type accounts. The concerned communications carriers are also ordered to retain, indefinitely, hard and soft copies of all records and/or data provided as a result of this Order.
  
- 12) RETAIL OUTLETS OR ANY ENTITIES are ordered to release, upon specific request, all purchase, payment (cash, credit, check, prepaid card, etc.), and activation information (even if through third parties) for all target devices, accounts, and subsequent payments, such as prepaid minute cards. This includes the specific data, time, location (including the specific store, register, clerk, etc.) that all devices, account changes, purchases, payments, etc., occurred. It is also ordered that all involved retailers (and neighboring businesses/residences) release any available surveillance video from the aforementioned transactions, both from within, and from the outside of the stores, and the area of the stores, where any of the aforementioned transactions occurred.
  
- 13) Finally, that this Order will apply to any and all companies/entities which may provide and/or carry wireless/telecommunication services for the target mobile numbers/unique account identifiers/equipment, and/or, any other entity who may possess the requested information, such as Internet companies/entities. This may be required because of number portability and/or if the original carrier was modified due to roaming and/or other considerations/reasons.

It is the belief of the Affiant, that: the AT&T accounts of 806-323-2809, contains evidence of the offense of Tampering with or Fabricating Physical Evidence, Texas Penal Code section 37.09, a felony offense.



**AFFIANT HAS PROBABLE CAUSE FOR THE SAID BELIEF BY REASON OF THE FOLLOWING FACTS, TO WIT:**

Your Affiant is Rachel Kading, a peace officer certified by The State of Texas, who is currently employed as a Sergeant with the Office of the Texas Attorney General (OAG). Affiant has been a law enforcement officer for over 15 years. Affiant is currently assigned to the Criminal Investigation Division, Special Investigations Unit, where her duties include investigations involving a wide array of criminal offences ranging from simple fraud to homicides. Affiant has specialized training in the areas of criminal investigations, child abuse and exploitation, narcotics and financial crimes, provided by federal, state, and local agencies. Affiant has previously been involved in the execution search warrants involving persons crimes and narcotics.

On January 26, 2018, Hemphill County Sherriff, NATHAN LEWIS, formally asked the Texas Attorney General's Office to assist in the investigation into the disappearance of THOMAS KELLY BROWN, who was last seen on 11-23-16 in Canadian, Texas. Multiple agencies have been assisting Hemphill County in this investigation.

No viable leads had been developed until 10-14-17, when a private investigator hired by the Brown family and deputies from the Hemphill County Sheriff's Office searched an area between Lake Marvin Road and State Highway (SH) 60 in Hemphill County. During the search on 10-14-17, an Apple iPhone 6S (A1688) was located approximately 45 feet from the SH 60 and Lake Marvin Road intersection and approximately 3 feet south of Lake Marvin Road. The Apple iPhone 6S was in near perfect condition and did not appear to have been outside in the elements since BROWN's disappearance on 11-23-16. The roadway had been mowed several times between November 2016 and October of 2017 and received a significant amount of rain during that time. The Apple iPhone 6S's weather sensors had not activated and the phone was free of nicks, scrapes and/or damage it would have sustained if exposed to the elements on the side of the busy roadway. The Apple iPhone 6S was analyzed by the Federal Bureau of Investigation (FBI) and the contents of the phone were provided to this Affiant. The recovered Apple iPhone 6S was identified as belonging to THOMAS KELLY BROWN as identifying information was located on the phone. This affiant believes the phone was placed on Lake Marvin Road just prior

to the search.

On 3-29-18, PENNY MEEK was administered a polygraph. PENNY MEEK failed questions regarding having THOMAS BROWNS phone and questions relating to having contact with THOMAS BROWN after his disappearance. In addition, PENNY MEEK failed questions regarding moving THOMAS BROWN'S body.

Based upon all the foregoing, there is probable cause to believe that evidence and instrumentalities used in the commission of Tampering with or Fabricating Physical Evidence, Texas Penal Code section 37.09, a felony offense are located in the account data for Penny Meek, 806-323-2809, currently stored on the computer servers located with:

**AT&T Mobility**  
**11760 US Hwy. 1, Suite 600**  
**North Palm Beach, FL 33408**

By nature of AT&T Mobility, being a Communications Provider, it is realized that many other individuals, organizations, businesses, and other entities utilize this company's services and have no association with the subject investigation. These other unnamed individuals, organizations, businesses, and other entities may have various amounts of information maintained in various forms with AT&T Mobility with a reasonable expectation of privacy. It is Affiant's intent that the search conducted at AT&T Mobility be as unobtrusive as possible, and that it relate to the above listed user account associated with the content that may have been deleted or altered. Further, it is Affiant's intent to use whatever means or methodology is on hand to conduct this search, with limited or no interruption of the service provided to these other unnamed individuals. It is for these reasons that Affiant requests that AT&T Mobility locate and isolate the above named information on their servers and make a copy of such information in a readable format to provide to Affiant for review as part of this investigation.

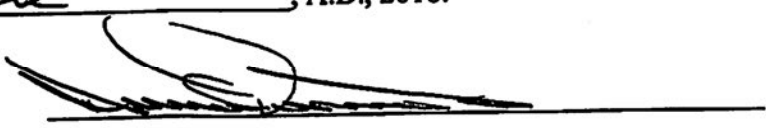
All information noted in this affidavit for search warrant has been related to Affiant by the person(s) and/or source(s) attributed or referenced. Affiant further believes in good faith that the information provided herein to be true and correct. Because the sole purpose of this affidavit is

to establish probable cause that a criminal offense has occurred, not every relevant fact known to Affiant, or to other investigators, is included within. Rather, only those facts necessary to establish probable cause have been discussed.

WHEREFORE, AFFIANT ASKS FOR ISSUANCE OF A WARRANT THAT WILL AUTHORIZE THE SEARCH OF SAID SUSPECTED PLACE FOR SAID PROPERTY AND SEIZURE OF THE SAME AND TO TAKE CUSTODY OF ALL SEIZED PROPERTY AND SAFE KEEP SUCH PROPERTY AS PROVIDED BY STATUTE.

  
AFFIANT, SERGEANT RACHEL KADING

SUBSCRIBED AND SWORN TO BEFORE ME BY SAID AFFIANT ON THIS THE  
6<sup>th</sup> day of June, A.D., 2018.

  
STEVEN EMMERT, 31<sup>ST</sup> DISTRICT JUDGE  
HEMPHILL COUNTY, TEXAS

IN RE: Search Warrant for )  
 )  
AT&T MOBILITY )  
806-323-2809 )  
 )  
 )  
\_\_\_\_\_ )

**NON-DISCLOSURE ORDER**

Upon the ex parte application of Sergeant Rachel Kading, a commissioned peace officer with the Office of the Attorney General, this Court orders the non-disclosure of the existence of the search warrant to the account holder. The Office of the Attorney General is conducting an active investigation and 806-323-2809 is related to that investigation. Disclosure to the account holder of the service of this search warrant, at this time, could jeopardize the integrity of the investigation.

**IT IS HEREBY ORDERED** that AT&T Mobility not disclose the existence of the attached search warrant pending further order of this Court except that copies may be provided to the office of the 31<sup>st</sup> Judicial District Attorney, and the District Attorney may provide copies to a defendant in a criminal proceeding as part of the criminal discovery process, and;

**IT IS FURTHER ORDERED** that a copy of this non-disclosure order be left at the premises along with the search warrant.

DATED this 6<sup>th</sup> day of June 2018.



Honorable Steven Emmert  
31<sup>st</sup> Judicial District Court

**SEARCH WARRANT**

**THE STATE OF TEXAS**

**§**

**§**

**COUNTY OF HEMPHILL**

**§**

To the Sheriff or any Peace Officer of Hemphill County, Texas, or any Peace Officer of the State of Texas:

Whereas, the Affiant whose name appears on the affidavit attached hereto is a peace officer under the laws of Texas and did heretofore this day subscribe and swear to said affidavit before me (which said affidavit is here now made a part hereof for all purposes and incorporated herein as if written verbatim within the confines of this Warrant), and whereas I find that the verified facts stated by Affiant in said affidavit show that Affiant has probable cause for the belief he/she expresses herein and establishes the existence of proper grounds for issuance of this Warrant.

Now, therefore, you are commanded to enter the suspected place as described in said affidavit, to forthwith search the place therein named, to wit:

**AT&T and all subsidiaries including but not limited to New Cingular Wireless**

**AT&T Mobility**

**11760 US Hwy. 1, Suite 600**

**North Palm Beach, FL 33408**

hereinafter, PROVIDER, with the authority to search for and to seize or to compel agents of said PROVIDER to search for, seize and to turn over to the government Electronic Customer Data as defined in the Texas Code of Criminal Procedure (T.C.C.P.) Chapter 18, and held in electronic storage by the PROVIDER for the Electronic Customer Data belonging to or associated with, the customer or individual subscriber/user accounts, from **September 1, 2016 through May 25, 2018.**

**806-323-3196**

At said place you shall search for and, if same be found, seize and bring before me the property described in the affidavit, to-wit:

The Electronic Customer Data that is the subject of this warrant includes:

- 1.) All subscriber information, including any available telephone numbers, email addresses, IP addresses (including ports), etc., and/or unique account, equipment, and/or network addressing, these may include the Electronic Serial Number (ESNs), International Mobile Subscriber Identifier (IMSI), Temporary Mobile Subscriber Identity number (TMSI), International Mobile Equipment Identifiers (IMEIs), Mobile Equipment Identifiers (MEIDs), Mobile Station Identifiers (MSIDs), Mobile Identification Numbers (MINs), Mobile Dialed Numbers (MDN), Integrated Circuit Card IDs (ICCID), Personal Unlocking/Unblocking Codes (PUKs), PINs (personal identification numbers), Blackberry PINs (personal identification numbers/codes), Apple's Unique Device Identifier (ID) (UDID), and/or Media Access Control (MAC) address(es), and all billing/payment information and accounts notes, for the specified cellular/wireless telephones, and for any other cellular/wireless telephones on the same account as the target numbers.
- 2.) All outgoing and incoming communications/call detail records (CDRs), with cell sites, including all telephone numbers, chirp numbers/direct connects/walkie-talkie/Universal Fleet Mobile Identifier (UFMI) numbers, email addresses (electronic mail), Internet Protocol (IP) addresses, World Wide Web (www) addresses, dialed/communicated with (outgoing and/or incoming). This includes local and long distance telephone connection records, including all text [short message service SMS] detail records, email detail records [including IP (Internet Protocol) logs, email header information, and email addresses], IP connection detail records/logs, and video, audio, and/or photo image transactions records, such as multimedia messaging service (MMS) (picture/video messaging) detail records/logs, sent or received, to provide dates, times, and methods of voicemail access, including all available SS7 signaling records of these communications, and, records of session times and durations, and to include content/text of messages if available. Cell Sites are required if they are available on any and all transactional/addressing and routing data.
- 3.) Cell sites activations and all registration information, including signal strengths, logs, etc. (if obtainable), including any location information delivered to a public safety answering point (PSAP) pursuant to a 911 call.
- 4.) If available, an engineering map; showing all cell-site antenna/tower locations, sectors, azimuths, beam widths, pilot PN (pseudo noise) offsets, and true orientations. And, a list of any and all cellular sites numbers [Long Term Evolution (LTE) —complete CGI or eNodeB and Cell Site, NodeB, Local Area Codes (LACs), Cellular Identifiers (CIDs), intercept access points (IAP) system identities, repolls, switches, etc.], locations, addresses, neighbor lists, etc., and/or latitude and

longitude of any said sites. Also, that cellular sites lists, including latitudes and longitudes, be provided, via electronic mail, or via shipping when email is not available, in an electronic format, if available and/or possible. Furthermore, the concerned carrier(s) will provide RF (radio frequency) propagation maps/surveys and cellular antenna/tower maintenance records, and cellular antenna/tower maintenance records procedures, upon request. These maps/surveys and maintenance records will be provided in electronic format, such as original color format, if available.

- 5.) Should the cellular/wireless number/equipment which is the current target of this Order have changed, during the requested period, including the MINs/MSIDs, MDNs, ESNs, MEIDs, IMEIs, IMSIs, ICCIDs, PUKs, IP addresses, UDIDs, PINs and/or MAC addresses, or combinations thereof, have been changed by the subscribers during the period of time(s) covered by this Order, then this Order will apply to any other MINs/MSIDs, MDNs, ESNs, MEIDs, IMEIs, IMSIs, ICCIDs, PUKs, IP addresses, UDIDs, PINs, email addresses, and/or MAC addresses. Furthermore if requested the specific manufacturer and model of said handset shall be released verbally or in writing by the Agency making this request.
- 6.) Any Internet Service Provider (ISP), email company or email server entity (public or private), website hosting company, and/or website or internet service providing company and/or entity, provide any subscriber information, email addresses, email logs (with header information, Internet Protocol (IP) logs, website addresses, etc., for any email addresses, IP addresses, user names, etc., identified from the original records pertaining to the target devices. Such as, if the original target devices' records reveal Internet activity, such as email activity, web activity, and/or other Internet connected applications, then this Order will also order the release of all subscriber information pertaining to user identifying, *and* addressing and routing (transactional) information pertaining to that Internet activity (without content information) for the effective period of this order. This includes application of this Order to Microsoft's "Sidekick"/"Danger" products/services. Also to include all location based information for all Google products (GMAIL, Google Voice, etc.) and all Apple products
- 7.) Also, whenever possible, that the provider(s) provision, upon the specific requests of the prosecutors/officers/agents/designees, a twenty-four (24) hour switch-technician/employee/vendor to assist in providing data to comply with this Order and/or the interpretation of the provided data.
- 8.) Any required information on demand, if possible and upon the specific request of the prosecutors/officers/agents/designees. Further, that any so ordered provider(s), or those possessing said information, provide, upon the specific request of the prosecutors/officers/agents/designees, any historical geo-location services/global positioning system (GPS) data/enhanced 911 (E911) records including but not limited to any available ranging data [distance from tower, range to tower

(RTT/REVEAL/Historic MLTs or other similar un-named records held by ANY PROVIDER)], which may be available to any involved provider(s) and/or parties. This includes specifically Sprint's PCMD data (per call measure data) and AT&T's NLEOs report. This also includes all location data captured by Google and Apple.

- 9.) All call/communication detail, direct connect, subscriber, numeric messages, alpha-numeric/text messages, email records, IP logs, etc., and any related records and/or access be provided, upon the specific request of prosecutors/officers/agents/designees of specific data from specific time period within the confines of this Order, in an electronic format specified by prosecutors/agents/officers/designees. Also, that the records/data be forwarded via email (in a common electronic format as described herein) if possible, upon the specific request of prosecutors/agents/officers/designees, to the listed prosecutor/officer and/or his/her designees. These designees may include, but are not limited to, prosecutors/officers/agents/designees and/or representatives of the Hemphill County District Attorney, Attorney General's Office of Texas (OAG) and the Texas Department of Public Safety (DPS).
  
- 10.) If e-mail is not available/possible, that the providers provide the required data electronically on a common storage medium, such as CD-ROM (compact disc read only memory) discs, and/or thumb drive. Also, that all providers provide, when possible and so requested, all requested data in ASCII, comma separated values (.csv), or fixed length (SDF) format. This is to include that any and all records/data will be provided in all available formats of data, upon request, to include, but not limited to, documents/files currently produced in Microsoft Word, Microsoft Excel, PDF (portable document format), CSV (comma separated value), other electronic formats, and/or pulled from such systems such as "CDR Live," "X-Mine," "CEER," and any other electronic medium that is/was in use and/or in development. All CDRs [call/communication detail records (CDRs), including IP (internet protocol) logs, email logs, etc.] will be provided in spreadsheet (Excel, CSV, etc.) format if possible. Only where this is not possible, to provide information in dark, clean typeface, machine-scanable/Optical Character Recognition (OCR) interpretable hardcopy. This includes the faxing of any necessary requested records at the highest possible quality setting. Further, that upon the specific request of prosecutors/agents/officers/designees, that any provided data, including account specific data and cellular site lists, be provided by the necessary providers in a business records affidavit format that complies with the laws of the State of Texas.
  
- 11.) Provide any and all data and services that are ordered herein, verbally, to prosecutors/officers (or designees) if specifically requested to do so. Communications providers are also ordered to notify prosecutors/officers (or designees) if devices roamed (and what specific networks are roamed to/from) from a home/primary network to another network and it is known by the home/primary network to what roaming network the devices roamed. This includes verbally notifying prosecutors/officers (or designees) of the last known



network registrations/activity during the above mentioned time frame. And, if the accounts were active accounts, including if the account was inactivated or closed for non-payment, and, how many minutes and/or credits remained on prepaid type accounts. The concerned communications carriers are also ordered to retain, indefinitely, hard and soft copies of all records and/or data provided as a result of this Order.

- 12.) **RETAIL OUTLETS OR ANY ENTITIES** are ordered to release, upon specific request, all purchase, payment (cash, credit, check, prepaid card, etc.), and activation information (even if through third parties) for all target devices, accounts, and subsequent payments, such as prepaid minute cards. This includes the specific data, time, location (including the specific store, register, clerk, etc.) that all devices, account changes, purchases, payments, etc., occurred. It is also ordered that all involved retailers (and neighboring businesses/residences) release any available surveillance video from the aforementioned transactions, both from within, and from the outside of the stores, and the area of the stores, where any of the aforementioned transactions occurred.
- 13.) Finally, that this Order will apply to any and all companies/entities which may provide and/or carry wireless/telecommunication services for the target mobile numbers/unique account identifiers/equipment, and/or, any other entity who may possess the requested information, such as Internet companies/entities. This may be required because of number portability and/or if the original carrier was modified due to roaming and/or other considerations/reasons.

**This Court ORDERS the Custodian of Records / AT&T, 11760 US Hwy. 1, North Palm Beach, FL 33408 shall disclose responsive data, if any, by sending to Sergeant Rachel Kading of the Office of the Texas Attorney General located at 300 West 15<sup>th</sup> Street, Austin TX, 78701 Mail Code 065 by courier service or to PO BOX 12548, Austin TX 78711 -MC 065 using the US Postal Service, notwithstanding 18 U.S.C. 2252A or similar statute or code, where all received data will be analyzed.**

Further, Affiant is **ORDERED**, pursuant to the provisions of Article 18.10, Texas Code of Criminal Procedure, to retain custody of any property seized pursuant to this Warrant, until further order of this Court or any other court of appropriate jurisdiction shall otherwise direct the manner of safekeeping of said property. This Court grants you leave and authority to remove such seized property from this county, if and only if such removal is necessary for the safekeeping of such seized property by Affiant, or if the provisions of Article 18.10, T.C.C.P.

otherwise authorize such removal. Affiant is further ORDERED to give notice to this Court, as a part of the inventory to be filed subsequent to the execution of this Warrant, and as required by Article 18.10, T.C.C.P., of the place where the property seized hereunder is kept, stored and held.

Herein fail not but have you then and there this Warrant within ten days, exclusive of the day of its execution, with your return thereon, showing how you executed the same.

ISSUED THIS THE 6<sup>th</sup> day of June A.D., 2018, at 4:35 o'clock P.M.  
to certify which, witness my hand this day.



STEVEN EMMERT, 31<sup>ST</sup> DISTRICT JUDGE  
HEMPHILL COUNTY, TEXAS

**THE STATE OF TEXAS** §  
§  
**COUNTY OF HEMPHILL** §

**AFFIDAVIT FOR SEARCH WARRANT**

BEFORE ME, THE UNDERSIGNED AUTHORITY, PERSONALLY APPEARED THE AFFIANT HEREIN, A PEACE OFFICER UNDER THE LAWS OF TEXAS, WHO, BEING DULY SWORN, ON OATH MADE THE FOLLOWING STATEMENTS:

My name is Rachel Kading and I am commissioned as a peace officer by the Texas Office of the Attorney General.

There is in North Palm Beach, Florida, a Communications Service Provider known as **AT&T Mobility, LLC**, located at **11760 US Hwy. 1, Suite 600, North Palm Beach, FL 33408**.

AT&T Mobility, LLC, in its capacity as a Communications Service provider, provides individuals or subscribers with access to mobile phone services used to make phone calls or send and receive text messages. AT&T also provides subscribers with internet services which provide subscribers to e-mail services, photo storage services, chat service, and access solution services. These services allow customers reserve or maintain storage space on AT&T Mobility computer servers. Subscribers can use AT&T servers to store their electronic communications (commonly known as e-mail, text messages, and/or chat communication), graphic images, text files, file transfer protocol logs, programs, and other types of data or information stored in electronic form.

Said suspected place and premises are in charge of and controlled by each of the following:

**AT&T Mobility**  
**11760 US Hwy. 1, Suite 600**  
**North Palm Beach, FL 33408**

There is at said suspected place and premises the following item(s) which are implements or instruments used in the commission of a crime and, or item(s) constituting evidence of a criminal offense or constituting evidence tending to show that a particular person committed a criminal offense:

- a. All stored Electronic Customer Data as defined in the Texas Code of Criminal Procedure (T.C.C.P.) Chapter 18, maintained by AT&T Mobility belonging to or associated with the customer or individual subscriber/user account:

**806-323-3196**

The Electronic Customer Data that is the subject of this warrant includes:

- 1) All subscriber information, including any available telephone numbers, email addresses, IP addresses (including ports), etc., and/or unique account, equipment, and/or network addressing, these may include the Electronic Serial Number (ESNs), International Mobile Subscriber Identifier (IMSI), Temporary Mobile Subscriber Identity number (TMSI), International Mobile Equipment Identifiers (IMEIs), Mobile Equipment Identifiers (MEIDs), Mobile Station Identifiers (MSIDs), Mobile Identification Numbers (MINs), Mobile Dialed Numbers (MDN), Integrated Circuit Card IDs (ICCID), Personal Unlocking/Unblocking Codes (PUKs), PINs (personal identification numbers), Blackberry PINs (personal identification numbers/codes), Apple's Unique Device Identifier (ID) (UDID), and/or Media Access Control (MAC) address(es), and all billing/payment information and accounts notes, for the specified cellular/wireless telephones, and for any other cellular/wireless telephones on the same account as the target numbers.
- 2) All outgoing and incoming communications/call detail records (CDRs), with cell sites, including all telephone numbers, chirp numbers/direct connects/walkie-talkie/Universal Fleet Mobile Identifier (UFMI) numbers, email addresses (electronic mail), Internet Protocol (IP) addresses, World Wide Web (www) addresses, dialed/communicated with (outgoing and/or incoming). This includes local and long distance telephone connection records, including all text [short message service SMS] detail records, email detail records [including IP (Internet Protocol) logs, email header information, and email addresses], IP connection detail records/logs, and video, audio, and/or photo image transactions records, such as multimedia messaging service (MMS) (picture/video messaging) detail records/logs, sent or received, to provide dates, times, and methods of voicemail access, including all available SS7 signaling records of these communications, and, records of session times and durations, and to include content/text of messages if available. Cell Sites are required if they are available on any and all transactional/addressing and routing data.

- 3) Cell sites activations and all registration information, including signal strengths, logs, etc. (if obtainable), including any location information delivered to a public safety answering point (PSAP) pursuant to a 911 call.
- 4) If available, an engineering map; showing all cell-site antenna/tower locations, sectors, azimuths, beam widths, pilot PN (pseudo noise) offsets, and true orientations. And, a list of any and all cellular sites numbers [Long Term Evolution (LTE) —complete CGI or eNodeB and Cell Site, NodeB, Local Area Codes (LACs), Cellular Identifiers (CIDs), intercept access points (IAP) system identities, repolls, switches, etc.], locations, addresses, neighbor lists, etc., and/or latitude and longitude of any said sites. Also, that cellular sites lists, including latitudes and longitudes, be provided, via electronic mail, or via shipping when email is not available, in an electronic format, if available and/or possible. Furthermore, the concerned carrier(s) will provide RF (radio frequency) propagation maps/surveys and cellular antenna/tower maintenance records, and cellular antenna/tower maintenance records procedures, upon request. These maps/surveys and maintenance records will be provided in electronic format, such as original color format, if available.
- 5) Should the cellular/wireless number/equipment which is the current target of this Order have changed, during the requested period, including the MINs/MSIDs, MDNs, ESNs, MEIDs, IMEIs, IMSIs, ICCIDs, PUKs, IP addresses, UDIDs, PINs and/or MAC addresses, or combinations thereof, have been changed by the subscribers during the period of time(s) covered by this Order, then this Order will apply to any other MINs/MSIDs, MDNs, ESNs, MEIDs, IMEIs, IMSIs, ICCIDs, PUKs, IP addresses, UDIDs, PINs, email addresses, and/or MAC addresses. Furthermore if requested the specific manufacturer and model of said handset shall be released verbally or in writing by the Agency making this request.
- 6) Any Internet Service Provider (ISP), email company or email server entity (public or private), website hosting company, and/or website or internet service providing company and/or entity, provide any subscriber information, email addresses, email logs (with header information, Internet Protocol (IP) logs, website addresses, etc., for any email addresses, IP addresses, user names, etc., identified from the original records pertaining to the target devices. Such as, if the original target devices' records reveal Internet activity, such as email activity, web activity, and/or other Internet connected applications, then this Order will also order the release of all subscriber information pertaining to user identifying, *and* addressing and routing (transactional) information pertaining to that Internet activity (without content information) for the effective period of this order. This includes application of this Order to Microsoft's "Sidekick"/"Danger" products/services. Also to include all location based information for all Google products (GMAIL, Google Voice, etc.) and all Apple products

- 7) Also, whenever possible, that the provider(s) provision, upon the specific requests of the prosecutors/officers/agents/designees, a twenty-four (24) hour switch-technician/employee/vendor to assist in providing data to comply with this Order and/or the interpretation of the provided data.
- 8) Any required information on demand, if possible and upon the specific request of the prosecutors/officers/agents/designees. Further, that any so ordered provider(s), or those possessing said information, provide, upon the specific request of the prosecutors/officers/agents/designees, any historical geo-location services/global positioning system (GPS) data/enhanced 911 (E911) records including but not limited to any available ranging data [distance from tower, range to tower (RTT/REVEAL/Historic MLTs or other similar un-named records held by ANY PROVIDER)], which may be available to any involved provider(s) and/or parties. This includes specifically Sprint's PCMD data (per call measure data) and AT&T's NLEOs report. This also includes all location data captured by Google and Apple.
- 9) All call/communication detail, direct connect, subscriber, numeric messages, alpha-numeric/text messages, email records, IP logs, etc., and any related records and/or access be provided, upon the specific request of prosecutors/officers/agents/designees of specific data from specific time period within the confines of this Order, in an electronic format specified by prosecutors/agents/officers/designees. Also, that the records/data be forwarded via email (in a common electronic format as described herein) if possible, upon the specific request of prosecutors/agents/officers/designees, to the listed prosecutor/officer and/or his/her designees. These designees may include, but are not limited to, prosecutors/officers/agents/designees and/or representatives of the Hemphill County District Attorney, Attorney General's Office of Texas (OAG) and the Texas Department of Public Safety (DPS).
- 10) If e-mail is not available/possible, that the providers provide the required data electronically on a common storage medium, such as CD-ROM (compact disc read only memory) discs, and/or thumb drive. Also, that all providers provide, when possible and so requested, all requested data in ASCII, comma separated values (.csv), or fixed length (SDF) format. This is to include that any and all records/data will be provided in all available formats of data, upon request, to include, but not limited to, documents/files currently produced in Microsoft Word, Microsoft Excel, PDF (portable document format), CSV (comma separated value), other electronic formats, and/or pulled from such systems such as "CDR Live," "X-Mine," "CEER," and any other electronic medium that is/was in use and/or in development. All CDRs [call/communication detail records (CDRs), including IP (internet protocol) logs, email logs, etc.] will be provided in spreadsheet (Excel, CSV, etc.) format if possible. Only where this is not possible, to provide information in dark, clean typeface, machine-scanable/Optical Character Recognition (OCR) interpretable hardcopy. This includes the faxing of any necessary requested records at the highest possible quality setting. Further, that upon the specific request of

prosecutors/agents/officers/designees, that any provided data, including account specific data and cellular site lists, be provided by the necessary providers in a business records affidavit format that complies with the laws of the State of Texas.

- 11) Provide any and all data and services that are ordered herein, verbally, to prosecutors/officers (or designees) if specifically requested to do so. Communications providers are also ordered to notify prosecutors/officers (or designees) if devices roamed (and what specific networks are roamed to/from) from a home/primary network to another network and it is known by the home/primary network to what roaming network the devices roamed. This includes verbally notifying prosecutors/officers (or designees) of the last known network registrations/activity during the above mentioned time frame. And, if the accounts were active accounts, including if the account was inactivated or closed for non-payment, and, how many minutes and/or credits remained on prepaid type accounts. The concerned communications carriers are also ordered to retain, indefinitely, hard and soft copies of all records and/or data provided as a result of this Order.
  
- 12) RETAIL OUTLETS OR ANY ENTITIES are ordered to release, upon specific request, all purchase, payment (cash, credit, check, prepaid card, etc.), and activation information (even if through third parties) for all target devices, accounts, and subsequent payments, such as prepaid minute cards. This includes the specific data, time, location (including the specific store, register, clerk, etc.) that all devices, account changes, purchases, payments, etc., occurred. It is also ordered that all involved retailers (and neighboring businesses/residences) release any available surveillance video from the aforementioned transactions, both from within, and from the outside of the stores, and the area of the stores, where any of the aforementioned transactions occurred.
  
- 13) Finally, that this Order will apply to any and all companies/entities which may provide and/or carry wireless/telecommunication services for the target mobile numbers/unique account identifiers/equipment, and/or, any other entity who may possess the requested information, such as Internet companies/entities. This may be required because of number portability and/or if the original carrier was modified due to roaming and/or other considerations/reasons.

It is the belief of the Affiant, that: the AT&T accounts of 806-323-3196, contains evidence of the offense of Tampering with or Fabricating Physical Evidence, Texas Penal Code section 37.09, a felony offense.

**AFFIANT HAS PROBABLE CAUSE FOR THE SAID BELIEF BY REASON OF THE FOLLOWING FACTS, TO WIT:**

Your Affiant is Rachel Kading, a peace officer certified by The State of Texas, who is currently employed as a Sergeant with the Office of the Texas Attorney General (OAG). Affiant has been a law enforcement officer for over 15 years. Affiant is currently assigned to the Criminal Investigation Division, Special Investigations Unit, where her duties include investigations involving a wide array of criminal offences ranging from simple fraud to homicides. Affiant has specialized training in the areas of criminal investigations, child abuse and exploitation, narcotics and financial crimes, provided by federal, state, and local agencies. Affiant has previously been involved in the execution search warrants involving persons crimes and narcotics.

On January 26, 2018, Hemphill County Sherriff, NATHAN LEWIS, formally asked the Texas Attorney General's Office to assist in the investigation into the disappearance of THOMAS KELLY BROWN, who was last seen on 11-23-16 in Canadian, Texas. Multiple agencies have been assisting Hemphill County in this investigation.

No viable leads had been developed until 10-14-17, when a private investigator hired by the Brown family and deputies from the Hemphill County Sheriff's Office searched an area between Lake Marvin Road and State Highway (SH) 60 in Hemphill County. During the search on 10-14-17, an Apple iPhone 6S (A1688) was located approximately 45 feet from the SH 60 and Lake Marvin Road intersection and approximately 3 feet south of Lake Marvin Road. The Apple iPhone 6S was in near perfect condition and did not appear to have been outside in the elements since BROWN's disappearance on 11-23-16. The roadway had been mowed several times between November 2016 and October of 2017 and received a significant amount of rain during that time. The Apple iPhone 6S's weather sensors had not activated and the phone was free of nicks, scrapes and/or damage it would have sustained if exposed to the elements on the side of the busy roadway. The Apple iPhone 6S was analyzed by the Federal Bureau of Investigation (FBI) and the contents of the phone were provided to this Affiant. The recovered Apple iPhone 6S was identified as belonging to THOMAS KELLY BROWN as identifying information was located on the phone. This affiant believes the phone was placed on Lake Marvin Road just prior



to the search.

On 3-29-18, CHRIS MEEK was administered a polygraph. CHRIS MEEK failed questions regarding having THOMAS BROWNS after his disappearance. In addition, CHRIS MEEK failed questions regarding moving THOMAS BROWN'S body.

Based upon all the foregoing, there is probable cause to believe that evidence and instrumentalities used in the commission of Tampering with or Fabricating Physical Evidence, Texas Penal Code section 37.09, a felony offense are located in the account data for Chris Meek, 806-323-3196, currently stored on the computer servers located with:

**AT&T Mobility**  
**11760 US Hwy. 1, Suite 600**  
**North Palm Beach, FL 33408**

By nature of AT&T Mobility, being a Communications Provider, it is realized that many other individuals, organizations, businesses, and other entities utilize this company's services and have no association with the subject investigation. These other unnamed individuals, organizations, businesses, and other entities may have various amounts of information maintained in various forms with AT&T Mobility with a reasonable expectation of privacy. It is Affiant's intent that the search conducted at AT&T Mobility be as unobtrusive as possible, and that it relate to the above listed user account associated with the content that may have been deleted or altered. Further, it is Affiant's intent to use whatever means or methodology is on hand to conduct this search, with limited or no interruption of the service provided to these other unnamed individuals. It is for these reasons that Affiant requests that AT&T Mobility locate and isolate the above named information on their servers and make a copy of such information in a readable format to provide to Affiant for review as part of this investigation.


All information noted in this affidavit for search warrant has been related to Affiant by the person(s) and/or source(s) attributed or referenced. Affiant further believes in good faith that the information provided herein to be true and correct. Because the sole purpose of this affidavit is to establish probable cause that a criminal offense has occurred, not every relevant fact known to

Affiant, or to other investigators, is included within. Rather, only those facts necessary to establish probable cause have been discussed.

WHEREFORE, AFFIANT ASKS FOR ISSUANCE OF A WARRANT THAT WILL AUTHORIZE THE SEARCH OF SAID SUSPECTED PLACE FOR SAID PROPERTY AND SEIZURE OF THE SAME AND TO TAKE CUSTODY OF ALL SEIZED PROPERTY AND SAFE KEEP SUCH PROPERTY AS PROVIDED BY STATUTE.

  
AFFIANT, SERGEANT RACHEL KADING

SUBSCRIBED AND SWORN TO BEFORE ME BY SAID AFFIANT ON THIS THE  
6<sup>th</sup> day of June, A.D., 2018.

  
STEVEN EMMERT, 31<sup>ST</sup> DISTRICT JUDGE  
HEMPHILL COUNTY, TEXAS

IN RE: Search Warrant for )  
 )  
AT&T MOBILITY )  
806-323-3196 )  
 )  
\_\_\_\_\_ )

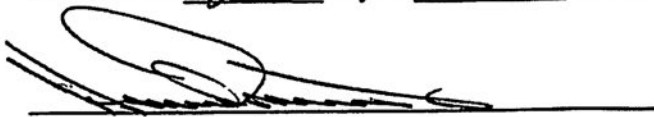
**NON-DISCLOSURE ORDER**

Upon the ex parte application of Sergeant Rachel Kading, a commissioned peace officer with the Office of the Attorney General, this Court orders the non-disclosure of the existence of the search warrant to the account holder. The Office of the Attorney General is conducting an active investigation and 806-323-3196 is related to that investigation. Disclosure to the account holder of the service of this search warrant, at this time, could jeopardize the integrity of the investigation.

**IT IS HEREBY ORDERED** that AT&T Mobility not disclose the existence of the attached search warrant pending further order of this Court except that copies may be provided to the office of the 31<sup>st</sup> Judicial District Attorney, and the District Attorney may provide copies to a defendant in a criminal proceeding as part of the criminal discovery process, and;

**IT IS FURTHER ORDERED** that a copy of this non-disclosure order be left at the premises along with the search warrant.

DATED this 6<sup>th</sup> day of June 2018.



Honorable Steven Emmert  
31<sup>st</sup> Judicial District Court

**SEARCH WARRANT**

**THE STATE OF TEXAS** §

§

**COUNTY OF HEMPHILL** §

To the Sheriff or any Peace Officer of Hemphill County, Texas, or any Peace Officer of the State of Texas:

Whereas, the Affiant whose name appears on the affidavit attached hereto is a peace officer under the laws of Texas and did heretofore this day subscribe and swear to said affidavit before me (which said affidavit is here now made a part hereof for all purposes and incorporated herein as if written verbatim within the confines of this Warrant), and whereas I find that the verified facts stated by Affiant in said affidavit show that Affiant has probable cause for the belief he/she expresses herein and establishes the existence of proper grounds for issuance of this Warrant.

Now, therefore, you are commanded to enter the suspected place as described in said affidavit, to forthwith search the place therein named, to wit:

**AT&T and all subsidiaries including but not limited to New Cingular Wireless**

**AT&T Mobility**

**11760 US Hwy. 1, Suite 600**

**North Palm Beach, FL 33408**

hereinafter, PROVIDER, with the authority to search for and to seize or to compel agents of said PROVIDER to search for, seize and to turn over to the government Electronic Customer Data as defined in the Texas Code of Criminal Procedure (T.C.C.P.) Chapter 18, and held in electronic storage by the PROVIDER for the Electronic Customer Data belonging to or associated with, the customer or individual subscriber/user accounts, from **September 1, 2016 through May 25, 2018.**

**806-228-1200 and 806-323-2164**

**and any other phone numbers attached**

**to social security number [REDACTED]**

[REDACTED]

At said place you shall search for and, if same be found, seize and bring before me the property described in the affidavit, to-wit:

The Electronic Customer Data that is the subject of this warrant includes:

- 1.) All subscriber information, including any available telephone numbers, email addresses, IP addresses (including ports), etc., and/or unique account, equipment, and/or network addressing, these may include the Electronic Serial Number (ESNs), International Mobile Subscriber Identifier (IMSI), Temporary Mobile Subscriber Identity number (TMSI), International Mobile Equipment Identifiers (IMEIs), Mobile Equipment Identifiers (MEIDs), Mobile Station Identifiers (MSIDs), Mobile Identification Numbers (MINs), Mobile Dialed Numbers (MDN), Integrated Circuit Card IDs (ICCID), Personal Unlocking/Unblocking Codes (PUKs), PINs (personal identification numbers), Blackberry PINs (personal identification numbers/codes), Apple's Unique Device Identifier (ID) (UDID), and/or Media Access Control (MAC) address(es), and all billing/payment information and accounts notes, for the specified cellular/wireless telephones, and for any other cellular/wireless telephones on the same account as the target numbers.
- 2.) All outgoing and incoming communications/call detail records (CDRs), with cell sites, including all telephone numbers, chirp numbers/direct connects/walkie-talkie/Universal Fleet Mobile Identifier (UFMI) numbers, email addresses (electronic mail), Internet Protocol (IP) addresses, World Wide Web (www) addresses, dialed/communicated with (outgoing and/or incoming). This includes local and long distance telephone connection records, including all text [short message service SMS] detail records, email detail records [including IP (Internet Protocol) logs, email header information, and email addresses], IP connection detail records/logs, and video, audio, and/or photo image transactions records, such as multimedia messaging service (MMS) (picture/video messaging) detail records/logs, sent or received, to provide dates, times, and methods of voicemail access, including all available SS7 signaling records of these communications, and, records of session times and durations, and to include content/text of messages if available. Cell Sites are required if they are available on any and all transactional/addressing and routing data.
- 3.) Cell sites activations and all registration information, including signal strengths, logs, etc. (if obtainable), including any location information delivered to a public safety answering point (PSAP) pursuant to a 911 call.
- 4.) If available, an engineering map; showing all cell-site antenna/tower locations, sectors, azimuths, beam widths, pilot PN (pseudo noise) offsets, and true orientations. And, a list of any and all cellular sites numbers [Long Term Evolution (LTE) —complete CGI or eNodeB and Cell Site, NodeB, Local Area Codes

(LACs), Cellular Identifiers (CIDs), intercept access points (IAP) system identities, repolls, switches, etc.], locations, addresses, neighbor lists, etc., and/or latitude and longitude of any said sites. Also, that cellular sites lists, including latitudes and longitudes, be provided, via electronic mail, or via shipping when email is not available, in an electronic format, if available and/or possible. Furthermore, the concerned carrier(s) will provide RF (radio frequency) propagation maps/surveys and cellular antenna/tower maintenance records, and cellular antenna/tower maintenance records procedures, upon request. These maps/surveys and maintenance records will be provided in electronic format, such as original color format, if available.

- 5.) Should the cellular/wireless number/equipment which is the current target of this Order have changed, during the requested period, including the MINs/MSIDs, MDNs, ESNs, MEIDs, IMEIs, IMSIs, ICCIDs, PUKs, IP addresses, UDIDs, PINs and/or MAC addresses, or combinations thereof, have been changed by the subscribers during the period of time(s) covered by this Order, then this Order will apply to any other MINs/MSIDs, MDNs, ESNs, MEIDs, IMEIs, IMSIs, ICCIDs, PUKs, IP addresses, UDIDs, PINs, email addresses, and/or MAC addresses. Furthermore if requested the specific manufacturer and model of said handset shall be released verbally or in writing by the Agency making this request.
- 6.) Any Internet Service Provider (ISP), email company or email server entity (public or private), website hosting company, and/or website or internet service providing company and/or entity, provide any subscriber information, email addresses, email logs (with header information, Internet Protocol (IP) logs, website addresses, etc., for any email addresses, IP addresses, user names, etc., identified from the original records pertaining to the target devices. Such as, if the original target devices' records reveal Internet activity, such as email activity, web activity, and/or other Internet connected applications, then this Order will also order the release of all subscriber information pertaining to user identifying, *and* addressing and routing (transactional) information pertaining to that Internet activity (without content information) for the effective period of this order. This includes application of this Order to Microsoft's "Sidekick"/"Danger" products/services. Also to include all location based information for all Google products (GMAIL, Google Voice, etc.) and all Apple products
- 7.) Also, whenever possible, that the provider(s) provision, upon the specific requests of the prosecutors/officers/agents/designees, a twenty-four (24) hour switch-technician/employee/vendor to assist in providing data to comply with this Order and/or the interpretation of the provided data.
- 8.) Any required information on demand, if possible and upon the specific request of the prosecutors/officers/agents/designees. Further, that any so ordered provider(s), or those possessing said information, provide, upon the specific request of the prosecutors/officers/agents/designees, any historical geo-location services/global

positioning system (GPS) data/enhanced 911 (E911) records including but not limited to any available ranging data [distance from tower, range to tower (RTT/REVEAL/Historic MLTs or other similar un-named records held by ANY PROVIDER)], which may be available to any involved provider(s) and/or parties. This includes specifically Sprint's PCMD data (per call measure data) and AT&T's NLEOs report. This also includes all location data captured by Google and Apple.

- 9.) All call/communication detail, direct connect, subscriber, numeric messages, alpha-numeric/text messages, email records, IP logs, etc., and any related records and/or access be provided, upon the specific request of prosecutors/officers/agents/designees of specific data from specific time period within the confines of this Order, in an electronic format specified by prosecutors/agents/officers/designees. Also, that the records/data be forwarded via email (in a common electronic format as described herein) if possible, upon the specific request of prosecutors/agents/officers/designees, to the listed prosecutor/officer and/or his/her designees. These designees may include, but are not limited to, prosecutors/officers/agents/designees and/or representatives of the Hemphill County District Attorney, Attorney General's Office of Texas (OAG) and the Texas Department of Public Safety (DPS).
  
- 10.) If e-mail is not available/possible, that the providers provide the required data electronically on a common storage medium, such as CD-ROM (compact disc read only memory) discs, and/or thumb drive. Also, that all providers provide, when possible and so requested, all requested data in ASCII, comma separated values (.csv), or fixed length (SDF) format. This is to include that any and all records/data will be provided in all available formats of data, upon request, to include, but not limited to, documents/files currently produced in Microsoft Word, Microsoft Excel, PDF (portable document format), CSV (comma separated value), other electronic formats, and/or pulled from such systems such as "CDR Live," "X-Mine," "CEER," and any other electronic medium that is/was in use and/or in development. All CDRs [call/communication detail records (CDRs), including IP (internet protocol) logs, email logs, etc.] will be provided in spreadsheet (Excel, CSV, etc.) format if possible. Only where this is not possible, to provide information in dark, clean typeface, machine-scanable/Optical Character Recognition (OCR) interpretable hardcopy. This includes the faxing of any necessary requested records at the highest possible quality setting. Further, that upon the specific request of prosecutors/agents/officers/designees, that any provided data, including account specific data and cellular site lists, be provided by the necessary providers in a business records affidavit format that complies with the laws of the State of Texas.
  
- 11.) Provide any and all data and services that are ordered herein, verbally, to prosecutors/officers (or designees) if specifically requested to do so. Communications providers are also ordered to notify prosecutors/officers (or designees) if devices roamed (and what specific networks are roamed to/from) from a home/primary network to another network and it is known by the



home/primary network to what roaming network the devices roamed. This includes verbally notifying prosecutors/officers (or designees) of the last known network registrations/activity during the above mentioned time frame. And, if the accounts were active accounts, including if the account was inactivated or closed for non-payment, and, how many minutes and/or credits remained on prepaid type accounts. The concerned communications carriers are also ordered to retain, indefinitely, hard and soft copies of all records and/or data provided as a result of this Order.

- 12.) **RETAIL OUTLETS OR ANY ENTITIES** are ordered to release, upon specific request, all purchase, payment (cash, credit, check, prepaid card, etc.), and activation information (even if through third parties) for all target devices, accounts, and subsequent payments, such as prepaid minute cards. This includes the specific data, time, location (including the specific store, register, clerk, etc.) that all devices, account changes, purchases, payments, etc., occurred. It is also ordered that all involved retailers (and neighboring businesses/residences) release any available surveillance video from the aforementioned transactions, both from within, and from the outside of the stores, and the area of the stores, where any of the aforementioned transactions occurred.
- 13.) Finally, that this Order will apply to any and all companies/entities which may provide and/or carry wireless/telecommunication services for the target mobile numbers/unique account identifiers/equipment, and/or, any other entity who may possess the requested information, such as Internet companies/entities. This may be required because of number portability and/or if the original carrier was modified due to roaming and/or other considerations/reasons.

**This Court ORDERS the Custodian of Records / AT&T, 11760 US Hwy. 1, North Palm Beach, FL 33408 shall disclose responsive data, if any, by sending to Sergeant Rachel Kading of the Office of the Texas Attorney General located at 300 West 15<sup>th</sup> Street, Austin TX, 78701 Mail Code 065 by courier service or to PO BOX 12548, Austin TX 78711 -MC 065 using the US Postal Service, notwithstanding 18 U.S.C. 2252A or similar statute or code, where all received data will be analyzed.**

Further, Affiant is **ORDERED**, pursuant to the provisions of Article 18.10, Texas Code of Criminal Procedure, to retain custody of any property seized pursuant to this Warrant, until further order of this Court or any other court of appropriate jurisdiction shall otherwise direct the manner of safekeeping of said property. This Court grants you leave and authority to remove such seized property from this county, if and only if such removal is necessary for the

safekeeping of such seized property by Affiant, or if the provisions of Article 18.10, T.C.C.P. otherwise authorize such removal. Affiant is further ORDERED to give notice to this Court, as a part of the inventory to be filed subsequent to the execution of this Warrant, and as required by Article 18.10, T.C.C.P., of the place where the property seized hereunder is kept, stored and held.

Herein fail not but have you then and there this Warrant within ten days, exclusive of the day of its execution, with your return thereon, showing how you executed the same.

ISSUED THIS THE 6<sup>th</sup> day of June, A.D., 2018, at 4:35 o'clock P.M.  
to certify which, witness my hand this day.



---

STEVEN EMMERT, 31<sup>ST</sup> DISTRICT JUDGE  
HEMPHILL COUNTY, TEXAS

**THE STATE OF TEXAS**

,

,

**COUNTY OF HEMPHILL**

,

**AFFIDAVIT FOR SEARCH WARRANT**

BEFORE ME, THE UNDERSIGNED AUTHORITY, PERSONALLY APPEARED THE AFFIANT HEREIN, A PEACE OFFICER UNDER THE LAWS OF TEXAS, WHO, BEING DULY SWORN, ON OATH MADE THE FOLLOWING STATEMENTS:

My name is Rachel Kading and I am commissioned as a peace officer by the Texas Office of the Attorney General.

There is in North Palm Beach, Florida, a Communications Service Provider known as **AT&T Mobility, LLC**, located at **11760 US Hwy. 1, Suite 600, North Palm Beach, FL 33408**.

AT&T Mobility, LLC, in its capacity as a Communications Service provider, provides individuals or subscribers with access to mobile phone services used to make phone calls or send and receive text messages. AT&T also provides subscribers with internet services which provide subscribers to e-mail services, photo storage services, chat service, and access solution services. These services allow customers reserve or maintain storage space on AT&T Mobility computer servers. Subscribers can use AT&T servers to store their electronic communications (commonly known as e-mail, text messages, and/or chat communication), graphic images, text files, file transfer protocol logs, programs, and other types of data or information stored in electronic form.

Said suspected place and premises are in charge of and controlled by each of the following:

**AT&T Mobility**  
**11760 US Hwy. 1, Suite 600**  
**North Palm Beach, FL 33408**

There is at said suspected place and premises the following item(s) which are implements or instruments used in the commission of a crime and, or item(s) constituting evidence of a criminal offense or constituting evidence tending to show that a particular person committed a criminal offense:

- a. All stored Electronic Customer Data as defined in the Texas Code of Criminal Procedure (T.C.C.P.) Chapter 18, maintained by AT&T Mobility belonging to or associated with the customer or individual subscriber/user account:

**806-228-1200 and 806-323-2164**  
**and any other phone numbers attached**  
**to social security number [REDACTED]**

The Electronic Customer Data that is the subject of this warrant includes:

- 1) All subscriber information, including any available telephone numbers, email addresses, IP addresses (including ports), etc., and/or unique account, equipment, and/or network addressing, these may include the Electronic Serial Number (ESNs), International Mobile Subscriber Identifier (IMSI), Temporary Mobile Subscriber Identity number (TMSI), International Mobile Equipment Identifiers (IMEIs), Mobile Equipment Identifiers (MEIDs), Mobile Station Identifiers (MSIDs), Mobile Identification Numbers (MINs), Mobile Dialed Numbers (MDN), Integrated Circuit Card IDs (ICCID), Personal Unlocking/Unblocking Codes (PUKs), PINs (personal identification numbers), Blackberry PINs (personal identification numbers/codes), Apple's Unique Device Identifier (ID) (UDID), and/or Media Access Control (MAC) address(es), and all billing/payment information and accounts notes, for the specified cellular/wireless telephones, and for any other cellular/wireless telephones on the same account as the target numbers.
- 2) All outgoing and incoming communications/call detail records (CDRs), with cell sites, including all telephone numbers, chirp numbers/direct connects/walkie-talkie/Universal Fleet Mobile Identifier (UFMI) numbers, email addresses (electronic mail), Internet Protocol (IP) addresses, World Wide Web (www) addresses, dialed/communicated with (outgoing and/or incoming). This includes local and long distance telephone connection records, including all text [short message service SMS] detail records, email detail records [including IP (Internet Protocol) logs, email header information,

██████████

and email addresses], IP connection detail records/logs, *and* video, audio, and/or photo image transactions records, such as multimedia messaging service (MMS) (picture/video messaging) detail records/logs, sent or received, to provide dates, times, and methods of voicemail access, including all available SS7 signaling records of these communications, and, records of session times and durations, and to include content/text of messages if available. Cell Sites are required if they are available on any and all transactional/addressing and routing data.

- 3) Cell sites activations and all registration information, including signal strengths, logs, etc. (if obtainable), including any location information delivered to a public safety answering point (PSAP) pursuant to a 911 call.
- 4) If available, an engineering map; showing all cell-site antenna/tower locations, sectors, azimuths, beam widths, pilot PN (pseudo noise) offsets, and true orientations. And, a list of any and all cellular sites numbers [Long Term Evolution (LTE) —complete CGI or eNodeB and Cell Site, NodeB, Local Area Codes (LACs), Cellular Identifiers (CIDs), intercept access points (IAP) system identities, repolls, switches, etc.], locations, addresses, neighbor lists, etc., and/or latitude and longitude of any said sites. Also, that cellular sites lists, including latitudes and longitudes, be provided, via electronic mail, or via shipping when email is not available, in an electronic format, if available and/or possible. Furthermore, the concerned carrier(s) will provide RF (radio frequency) propagation maps/surveys and cellular antenna/tower maintenance records, and cellular antenna/tower maintenance records procedures, upon request. These maps/surveys and maintenance records will be provided in electronic format, such as original color format, if available.
- 5) Should the cellular/wireless number/equipment which is the current target of this Order have changed, during the requested period, including the MINs/MSIDs, MDNs, ESNs, MEIDs, IMEIs, IMSIs, ICCIDs, PUKs, IP addresses, UDIDs, PINs and/or MAC addresses, or combinations thereof, have been changed by the subscribers during the period of time(s) covered by this Order, then this Order will apply to any other MINs/MSIDs, MDNs, ESNs, MEIDs, IMEIs, IMSIs, ICCIDs, PUKs, IP addresses, UDIDs, PINs, email addresses, and/or MAC addresses. Furthermore if requested the specific manufacturer and model of said handset shall be released verbally or in writing by the Agency making this request.
- 6) Any Internet Service Provider (ISP), email company or email server entity (public or private), website hosting company, and/or website or internet service providing company and/or entity, provide any subscriber information, email addresses, email logs (with header information, Internet Protocol (IP) logs, website addresses, etc., for any email addresses, IP addresses, user names, etc., identified from the original records pertaining to the target devices. Such as, if the original target devices' records reveal Internet activity, such as email activity, web activity, and/or other Internet connected

applications, then this Order will also order the release of all subscriber information pertaining to user identifying, *and* addressing and routing (transactional) information pertaining to that Internet activity (without content information) for the effective period of this order. This includes application of this Order to Microsoft's "Sidekick"/"Danger" products/services. Also to include all location based information for all Google products (GMAIL, Google Voice, etc.) and all Apple products

- 7) Also, whenever possible, that the provider(s) provision, upon the specific requests of the prosecutors/officers/agents/designees, a twenty-four (24) hour switch-technician/employee/vendor to assist in providing data to comply with this Order and/or the interpretation of the provided data.
- 8) Any required information on demand, if possible and upon the specific request of the prosecutors/officers/agents/designees. Further, that any so ordered provider(s), or those possessing said information, provide, upon the specific request of the prosecutors/officers/agents/designees, any historical geo-location services/global positioning system (GPS) data/enhanced 911 (E911) records including but not limited to any available ranging data [distance from tower, range to tower (RTT/REVEAL/Historic MLTs or other similar un-named records held by ANY PROVIDER)], which may be available to any involved provider(s) and/or parties. This includes specifically Sprint's PCMD data (per call measure data) and AT&T's NLEOs report. This also includes all location data captured by Google and Apple.
- 9) All call/communication detail, direct connect, subscriber, numeric messages, alpha-numeric/text messages, email records, IP logs, etc., and any related records and/or access be provided, upon the specific request of prosecutors/officers/agents/designees of specific data from specific time period within the confines of this Order, in an electronic format specified by prosecutors/agents/officers/designees. Also, that the records/data be forwarded via email (in a common electronic format as described herein) if possible, upon the specific request of prosecutors/agents/officers/designees, to the listed prosecutor/officer and/or his/her designees. These designees may include, but are not limited to, prosecutors/officers/agents/designees and/or representatives of the Hemphill County District Attorney, Attorney General's Office of Texas (OAG) and the Texas Department of Public Safety (DPS).
- 10) If e-mail is not available/possible, that the providers provide the required data electronically on a common storage medium, such as CD-ROM (compact disc read only memory) discs, and/or thumb drive. Also, that all providers provide, when possible and so requested, all requested data in ASCII, comma separated values (.csv), or fixed length (SDF) format. This is to include that any and all records/data will be provided in all available formats of data, upon request, to include, but not limited to, documents/files currently produced in Microsoft Word, Microsoft Excel, PDF (portable document format), CSV (comma separated value), other electronic

formats, and/or pulled from such systems such as "CDR Live," "X-Mine," "CEER," and any other electronic medium that is/was in use and/or in development. All CDRs [call/communication detail records (CDRs), including IP (internet protocol) logs, email logs, etc.] will be provided in spreadsheet (Excel, CSV, etc.) format if possible. Only where this is not possible, to provide information in dark, clean typeface, machine-scanable/Optical Character Recognition (OCR) interpretable hardcopy. This includes the faxing of any necessary requested records at the highest possible quality setting. Further, that upon the specific request of prosecutors/agents/officers/designees, that any provided data, including account specific data and cellular site lists, be provided by the necessary providers in a business records affidavit format that complies with the laws of the State of Texas.

- 11) Provide any and all data and services that are ordered herein, verbally, to prosecutors/officers (or designees) if specifically requested to do so. Communications providers are also ordered to notify prosecutors/officers (or designees) if devices roamed (and what specific networks are roamed to/from) from a home/primary network to another network and it is known by the home/primary network to what roaming network the devices roamed. This includes verbally notifying prosecutors/officers (or designees) of the last known network registrations/activity during the above mentioned time frame. And, if the accounts were active accounts, including if the account was inactivated or closed for non-payment, and, how many minutes and/or credits remained on prepaid type accounts. The concerned communications carriers are also ordered to retain, indefinitely, hard and soft copies of all records and/or data provided as a result of this Order.
- 12) RETAIL OUTLETS OR ANY ENTITIES are ordered to release, upon specific request, all purchase, payment (cash, credit, check, prepaid card, etc.), and activation information (even if through third parties) for all target devices, accounts, and subsequent payments, such as prepaid minute cards. This includes the specific data, time, location (including the specific store, register, clerk, etc.) that all devices, account changes, purchases, payments, etc., occurred. It is also ordered that all involved retailers (and neighboring businesses/residences) release any available surveillance video from the aforementioned transactions, both from within, and from the outside of the stores, and the area of the stores, where any of the aforementioned transactions occurred.
- 13) Finally, that this Order will apply to any and all companies/entities which may provide and/or carry wireless/telecommunication services for the target mobile numbers/unique account identifiers/equipment, and/or, any other entity who may possess the requested information, such as Internet companies/entities. This may be required because of number portability and/or if the original carrier was modified due to roaming and/or other considerations/reasons.



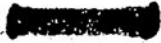
It is the belief of the Affiant, that: the AT&T accounts of 806-228-1200 and 806-323-2164, and any other phone numbers attached to social security number [REDACTED], contains evidence of the offense of Tampering with or Fabricating Physical Evidence, Texas Penal Code section 37.09, a felony offense.

**AFFIANT HAS PROBABLE CAUSE FOR THE SAID BELIEF BY REASON OF THE FOLLOWING FACTS, TO WIT:**

Your Affiant is Rachel Kading, a peace officer certified by The State of Texas, who is currently employed as a Sergeant with the Office of the Texas Attorney General (OAG). Affiant has been a law enforcement officer for over 15 years. Affiant is currently assigned to the Criminal Investigation Division, Special Investigations Unit, where her duties include investigations involving a wide array of criminal offences ranging from simple fraud to homicides. Affiant has specialized training in the areas of criminal investigations, child abuse and exploitation, narcotics and financial crimes, provided by federal, state, and local agencies. Affiant has previously been involved in the execution search warrants involving persons crimes and narcotics.

On January 26, 2018, Hemphill County Sherriff, NATHAN LEWIS, formally asked the Texas Attorney General's Office to assist in the investigation into the disappearance of THOMAS KELLY BROWN, who was last seen on 11-23-16 in Canadian, Texas. Multiple agencies have been assisting Hemphill County in this investigation.

No viable leads had been developed until 10-14-17, when a private investigator hired by the Brown family and deputies from the Hemphill County Sheriff's Office searched an area between Lake Marvin Road and State Highway (SH) 60 in Hemphill County. During the search on 10-14-17, an Apple iPhone 6S (A1688) was located approximately 45 feet from the SH 60 and Lake Marvin Road intersection and approximately 3 feet south of Lake Marvin Road. The Apple iPhone 6S was in near perfect condition and did not appear to have been outside in the elements since BROWN's disappearance on 11-23-16. The roadway had been mowed several times between November 2016 and October of 2017 and received a significant amount of rain during that time. The Apple iPhone 6S's weather sensors had not activated and the phone was free of



nicks, scrapes and/or damage it would have sustained if exposed to the elements on the side of the busy roadway. The Apple iPhone 6S was analyzed by the Federal Bureau of Investigation (FBI) and the contents of the phone were provided to this Affiant. The recovered Apple iPhone 6S was identified as belonging to THOMAS KELLY BROWN as identifying information was located on the phone. This affiant believes the phone was placed on Lake Marvin Road just prior to the search.

This affiant was told by BROWN'S mother, PENNY MEEK and by her private investigator, PHILIP KLIEN, that they were shown a photograph of BROWN at Fronks gas station. The photograph appeared to be from security footage. LEWIS denied the photograph existed to this affiant. Fronks is the last place BROWN was seen on 11-23-16. This affiant has never seen this photograph.

On 5-17-18, LEWIS was administered a polygraph examination conducted by the Texas Department of Public Safety polygraph examiner to determine if he had personal knowledge of the circumstances surrounding BROWN'S iPhone or the photograph at Fronks gas station. Each of these subjects were discussed at length during the pre-interview. LEWIS was asked in a series of questions if he had any involvement in BROWN'S disappearance. LEWIS showed deception on the polygraph.

This affiant is also aware of a text conversation between LEWIS and a confidential informant, RICKY IVY, utilizing one of the phone numbers listed in this warrant. LEWIS received a text from IVY that BROWN was killed and put through a wood chipper. IVY later left his phone at a different address and other people went through IVY'S phone. IVY'S phone eventually makes its way to Texas Ranger, MIKE SMITH. SMITH told this affiant and provided a copy of the message about BROWN. SMITH stated he asked LEWIS about the message and LEWIS never followed up on the tip. In addition, this affiant has received several tips and has been told by numerous people, that LEWIS is involved in the disappearance of BROWN.

Based upon all the foregoing, there is probable cause to believe that evidence and instrumentalities used in the commission of Tampering with or Fabricating Physical Evidence, Texas Penal Code section 37.09, a felony offense are located in the account data for LEWIS'

phones, 806-228-1200 and 806-323-2164, currently stored on the computer servers located with:

**AT&T Mobility  
11760 US Hwy. 1, Suite 600  
North Palm Beach, FL 33408**

By nature of AT&T Mobility, being a Communications Provider, it is realized that many other individuals, organizations, businesses, and other entities utilize this company's services and have no association with the subject investigation. These other unnamed individuals, organizations, businesses, and other entities may have various amounts of information maintained in various forms with AT&T Mobility with a reasonable expectation of privacy. It is Affiant's intent that the search conducted at AT&T Mobility be as unobtrusive as possible, and that it relate to the above listed user account associated with the content that may have been deleted or altered. Further, it is Affiant's intent to use whatever means or methodology is on hand to conduct this search, with limited or no interruption of the service provided to these other unnamed individuals. It is for these reasons that Affiant requests that AT&T Mobility locate and isolate the above named information on their servers and make a copy of such information in a readable format to provide to Affiant for review as part of this investigation.

All information noted in this affidavit for search warrant has been related to Affiant by the person(s) and/or source(s) attributed or referenced. Affiant further believes in good faith that the information provided herein to be true and correct. Because the sole purpose of this affidavit is to establish probable cause that a criminal offense has occurred, not every relevant fact known to Affiant, or to other investigators, is included within. Rather, only those facts necessary to establish probable cause have been discussed.

**WHEREFORE, AFFIANT ASKS FOR ISSUANCE OF A WARRANT THAT WILL AUTHORIZE THE SEARCH OF SAID SUSPECTED PLACE FOR SAID PROPERTY AND SEIZURE OF THE SAME AND TO TAKE CUSTODY OF ALL SEIZED PROPERTY AND SAFE KEEP SUCH PROPERTY AS PROVIDED BY STATUTE.**



AFFIANT, SERGEANT RACHEL KADING

SUBSCRIBED AND SWORN TO BEFORE ME BY SAID AFFIANT ON THIS THE

6<sup>th</sup> day of June, A.D., 2018.



STEVEN EMMERT, 31<sup>ST</sup> DISTRICT JUDGE  
HEMPHILL COUNTY, TEXAS

AT&T Search Warrant

IN RE: Search Warrant for )  
 )  
AT&T MOBILITY )  
806-228-1200 )  
806-323-2164 )  
Accounts belonging to [REDACTED] )  
\_\_\_\_\_ )

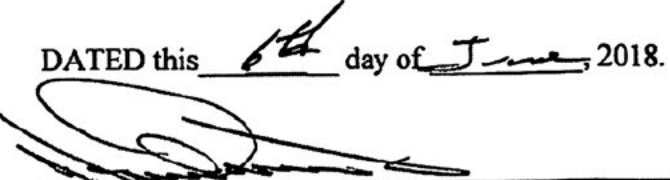
**NON-DISCLOSURE ORDER**

Upon the ex parte application of Sergeant Rachel Kading, a commissioned peace officer with the Office of the Attorney General, this Court orders the non-disclosure of the existence of the search warrant to the account holder. The Office of the Attorney General is conducting an active investigation and 806-228-1200 and, 806-323-2164, and any other phone numbers attached to social security number [REDACTED] is related to that investigation. Disclosure to the account holder of the service of this search warrant, at this time, could jeopardize the integrity of the investigation.

**IT IS HEREBY ORDERED** that AT&T Mobility not disclose the existence of the attached search warrant pending further order of this Court except that copies may be provided to the office of the 31<sup>st</sup> Judicial District Attorney, and the District Attorney may provide copies to a defendant in a criminal proceeding as part of the criminal discovery process, and;

**IT IS FURTHER ORDERED** that a copy of this non-disclosure order be left at the premises along with the search warrant.

DATED this 6<sup>th</sup> day of June, 2018.

  
\_\_\_\_\_  
Honorable Steven Emmert  
31<sup>st</sup> Judicial District Court

**SEARCH WARRANT**

**THE STATE OF TEXAS**                   §  
                                                         §  
**COUNTY OF HEMPHILL**               §

To the Sheriff or any Peace Officer of Hemphill County, Texas, or any Peace Officer of the State of Texas:

Whereas, the Affiant whose name appears on the affidavit attached hereto is a peace officer under the laws of Texas and did heretofore this day subscribe and swear to said affidavit before me (which said affidavit is here now made a part hereof for all purposes and incorporated herein as if written verbatim within the confines of this Warrant), and whereas I find that the verified facts stated by Affiant in said affidavit show that Affiant has probable cause for the belief he/she expresses herein and establishes the existence of proper grounds for issuance of this Warrant.

Now, therefore, you are commanded to enter the suspected place as described in said affidavit, to forthwith search the place therein named, to wit:

**AT&T and all subsidiaries including but not limited to New Cingular Wireless  
AT&T Mobility  
11760 US Hwy. 1, Suite 600  
North Palm Beach, FL 33408**

hereinafter, PROVIDER, with the authority to search for and to seize or to compel agents of said PROVIDER to search for, seize and to turn over to the government Electronic Customer Data as defined in the Texas Code of Criminal Procedure (T.C.C.P.) Chapter 18, and held in electronic storage by the PROVIDER for the Electronic Customer Data belonging to or associated with, the customer or individual subscriber/user accounts, from **May 23, 2018 through June 8, 2018.**

**806-228-0382 and any other accounts attached to this subscriber**

At said place you shall search for and, if same be found, seize and bring before me the property described in the affidavit, to-wit:

The Electronic Customer Data that is the subject of this warrant includes:

- 1.) All subscriber information, including any available telephone numbers, email addresses, IP addresses (including ports), etc., and/or unique account, equipment, and/or network addressing, these may include the Electronic Serial Number (ESNs), International Mobile Subscriber Identifier (IMSI), Temporary Mobile Subscriber Identity number (TMSI), International Mobile Equipment Identifiers (IMEIs), Mobile Equipment Identifiers (MEIDs), Mobile Station Identifiers (MSIDs), Mobile Identification Numbers (MINs), Mobile Dialed Numbers (MDN), Integrated Circuit Card IDs (ICCID), Personal Unlocking/Unlocking Codes (PUKs), PINs (personal identification numbers), Blackberry PINs (personal identification numbers/codes), Apple's Unique Device Identifier (ID) (UDID), and/or Media Access Control (MAC) address(es), and all billing/payment information and accounts notes, for the specified cellular/wireless telephones, and for any other cellular/wireless telephones on the same account as the target numbers.
- 2.) All outgoing and incoming communications/call detail records (CDRs), with cell sites, including all telephone numbers, chirp numbers/direct connects/walkie-talkie/Universal Fleet Mobile Identifier (UFMI) numbers, email addresses (electronic mail), Internet Protocol (IP) addresses, World Wide Web (www) addresses, dialed/communicated with (outgoing and/or incoming). This includes local and long distance telephone connection records, including all text [short message service SMS] detail records, email detail records [including IP (Internet Protocol) logs, email header information, and email addresses], IP connection detail records/logs, *and* video, audio, and/or photo image transactions records, such as multimedia messaging service (MMS) (picture/video messaging) detail records/logs, sent or received, to provide dates, times, and methods of voicemail access, including all available SS7 signaling records of these communications, and, records of session times and durations, and to include content/text of messages if available. Cell Sites are required if they are available on any and all transactional/addressing and routing data.
- 3.) Cell sites activations and all registration information, including signal strengths, logs, etc. (if obtainable), including any location information delivered to a public safety answering point (PSAP) pursuant to a 911 call.
- 4.) If available, an engineering map; showing all cell-site antenna/tower locations, sectors, azimuths, beam widths, pilot PN (pseudo noise) offsets, and true orientations. And, a list of any and all cellular sites numbers [Long Term Evolution (LTE) —complete CGI or eNodeB and Cell Site, NodeB, Local Area Codes (LACs), Cellular Identifiers (CIDs), intercept access points (IAP) system identities, repolls, switches, etc.], locations, addresses, neighbor lists, etc., and/or latitude and



longitude of any said sites. Also, that cellular sites lists, including latitudes and longitudes, be provided, via electronic mail, or via shipping when email is not available, in an electronic format, if available and/or possible. Furthermore, the concerned carrier(s) will provide RF (radio frequency) propagation maps/surveys and cellular antenna/tower maintenance records, and cellular antenna/tower maintenance records procedures, upon request. These maps/surveys and maintenance records will be provided in electronic format, such as original color format, if available.

- 5.) Should the cellular/wireless number/equipment which is the current target of this Order have changed, during the requested period, including the MINs/MSIDs, MDNs, ESNs, MEIDs, IMEIs, IMSIs, ICCIDs, PUKs, IP addresses, UDIDs, PINs and/or MAC addresses, or combinations thereof, have been changed by the subscribers during the period of time(s) covered by this Order, then this Order will apply to any other MINs/MSIDs, MDNs, ESNs, MEIDs, IMEIs, IMSIs, ICCIDs, PUKs, IP addresses, UDIDs, PINs, email addresses, and/or MAC addresses. Furthermore if requested the specific manufacturer and model of said handset shall be released verbally or in writing by the Agency making this request.
  
- 6.) Any Internet Service Provider (ISP), email company or email server entity (public or private), website hosting company, and/or website or internet service providing company and/or entity, provide any subscriber information, email addresses, email logs (with header information, Internet Protocol (IP) logs, website addresses, etc., for any email addresses, IP addresses, user names, etc., identified from the original records pertaining to the target devices. Such as, if the original target devices' records reveal Internet activity, such as email activity, web activity, and/or other Internet connected applications, then this Order will also order the release of all subscriber information pertaining to user identifying, *and* addressing and routing (transactional) information pertaining to that Internet activity (without content information) for the effective period of this order. This includes application of this Order to Microsoft's "Sidekick"/"Danger" products/services. Also to include all location based information for all Google products (GMAIL, Google Voice, etc.) and all Apple products
  
- 7.) Also, whenever possible, that the provider(s) provision, upon the specific requests of the prosecutors/officers/agents/designees, a twenty-four (24) hour switch-technician/employee/vendor to assist in providing data to comply with this Order and/or the interpretation of the provided data.
  
- 8.) Any required information on demand, if possible and upon the specific request of the prosecutors/officers/agents/designees. Further, that any so ordered provider(s), or those possessing said information, provide, upon the specific request of the prosecutors/officers/agents/designees, any historical geo-location services/global positioning system (GPS) data/enhanced 911 (E911) records including but not limited to any available ranging data [distance from tower, range to tower

(RTT/REVEAL/Historic MLTs or other similar un-named records held by ANY PROVIDER)], which may be available to any involved provider(s) and/or parties. This includes specifically Sprint's PCMD data (per call measure data) and AT&T's NLEOs report. This also includes all location data captured by Google and Apple.

- 9.) All call/communication detail, direct connect, subscriber, numeric messages, alpha-numeric/text messages, email records, IP logs, etc., and any related records and/or access be provided, upon the specific request of prosecutors/officers/agents/designees of specific data from specific time period within the confines of this Order, in an electronic format specified by prosecutors/agents/officers/designees. Also, that the records/data be forwarded via email (in a common electronic format as described herein) if possible, upon the specific request of prosecutors/agents/officers/designees, to the listed prosecutor/officer and/or his/her designees. These designees may include, but are not limited to, prosecutors/officers/agents/designees and/or representatives of the Hemphill County District Attorney, Attorney General's Office of Texas (OAG) and the Texas Department of Public Safety (DPS).
  
- 10.) If e-mail is not available/possible, that the providers provide the required data electronically on a common storage medium, such as CD-ROM (compact disc read only memory) discs, and/or thumb drive. Also, that all providers provide, when possible and so requested, all requested data in ASCII, comma separated values (.csv), or fixed length (SDF) format. This is to include that any and all records/data will be provided in all available formats of data, upon request, to include, but not limited to, documents/files currently produced in Microsoft Word, Microsoft Excel, PDF (portable document format), CSV (comma separated value), other electronic formats, and/or pulled from such systems such as "CDR Live," "X-Mine," "CEER," and any other electronic medium that is/was in use and/or in development. All CDRs [call/communication detail records (CDRs), including IP (internet protocol) logs, email logs, etc.] will be provided in spreadsheet (Excel, CSV, etc.) format if possible. Only where this is not possible, to provide information in dark, clean typeface, machine-scanable/Optical Character Recognition (OCR) interpretable hardcopy. This includes the faxing of any necessary requested records at the highest possible quality setting. Further, that upon the specific request of prosecutors/agents/officers/designees, that any provided data, including account specific data and cellular site lists, be provided by the necessary providers in a business records affidavit format that complies with the laws of the State of Texas.
  
- 11.) Provide any and all data and services that are ordered herein, verbally, to prosecutors/officers (or designees) if specifically requested to do so. Communications providers are also ordered to notify prosecutors/officers (or designees) if devices roamed (and what specific networks are roamed to/from) from a home/primary network to another network and it is known by the home/primary network to what roaming network the devices roamed. This includes verbally notifying prosecutors/officers (or designees) of the last known

network registrations/activity during the above mentioned time frame. And, if the accounts were active accounts, including if the account was inactivated or closed for non-payment, and, how many minutes and/or credits remained on prepaid type accounts. The concerned communications carriers are also ordered to retain, indefinitely, hard and soft copies of all records and/or data provided as a result of this Order.

- 12.) RETAIL OUTLETS OR ANY ENTITIES are ordered to release, upon specific request, all purchase, payment (cash, credit, check, prepaid card, etc.), and activation information (even if through third parties) for all target devices, accounts, and subsequent payments, such as prepaid minute cards. This includes the specific data, time, location (including the specific store, register, clerk, etc.) that all devices, account changes, purchases, payments, etc., occurred. It is also ordered that all involved retailers (and neighboring businesses/residences) release any available surveillance video from the aforementioned transactions, both from within, and from the outside of the stores, and the area of the stores, where any of the aforementioned transactions occurred.
- 13.) Finally, that this Order will apply to any and all companies/entities which may provide and/or carry wireless/telecommunication services for the target mobile numbers/unique account identifiers/equipment, and/or, any other entity who may possess the requested information, such as Internet companies/entities. This may be required because of number portability and/or if the original carrier was modified due to roaming and/or other considerations/reasons.

This Court **ORDERS** the Custodian of Records / AT&T, 11760 US Hwy. 1, North Palm Beach, FL 33408 shall disclose responsive data, if any, by sending to Sergeant Rachel Kading of the Office of the Texas Attorney General located at 300 West 15<sup>th</sup> Street, Austin TX, 78701 Mail Code 065 by courier service or to PO BOX 12548, Austin TX 78711 -MC 065 using the US Postal Service, notwithstanding 18 U.S.C. 2252A or similar statute or code, where all received data will be analyzed.

Further, Affiant is **ORDERED**, pursuant to the provisions of Article 18.10, Texas Code of Criminal Procedure, to retain custody of any property seized pursuant to this Warrant, until further order of this Court or any other court of appropriate jurisdiction shall otherwise direct the manner of safekeeping of said property. This Court grants you leave and authority to remove such seized property from this county, if and only if such removal is necessary for the safekeeping of such seized property by Affiant, or if the provisions of Article 18.10, T.C.C.P.

otherwise authorize such removal. Affiant is further ORDERED to give notice to this Court, as a part of the inventory to be filed subsequent to the execution of this Warrant, and as required by Article 18.10, T.C.C.P., of the place where the property seized hereunder is kept, stored and held.

Herein fail not but have you then and there this Warrant within ten days, exclusive of the day of its execution, with your return thereon, showing how you executed the same.

ISSUED THIS THE 22<sup>nd</sup> day of August, A.D., 2018, at 5:50 o'clock P.M.  
to certify which, witness my hand this day.



---

STEVEN EMMERT, 31<sup>ST</sup> DISTRICT JUDGE  
HEMPHILL COUNTY, TEXAS

**THE STATE OF TEXAS**

**COUNTY OF HEMPHILL**

**AFFIDAVIT FOR SEARCH WARRANT**

BEFORE ME, THE UNDERSIGNED AUTHORITY, PERSONALLY APPEARED THE AFFIANT HEREIN, A PEACE OFFICER UNDER THE LAWS OF TEXAS, WHO, BEING DULY SWORN, ON OATH MADE THE FOLLOWING STATEMENTS:

My name is Rachel Kading and I am commissioned as a peace officer by the Texas Office of the Attorney General.

There is in North Palm Beach, Florida, a Communications Service Provider known as **AT&T Mobility, LLC**, located at **11760 US Hwy. 1, Suite 600, North Palm Beach, FL 33408**.

AT&T Mobility, LLC, in its capacity as a Communications Service provider, provides individuals or subscribers with access to mobile phone services used to make phone calls or send and receive text messages. AT&T also provides subscribers with internet services which provide subscribers to e-mail services, photo storage services, chat service, and access solution services. These services allow customers reserve or maintain storage space on AT&T Mobility computer servers. Subscribers can use AT&T servers to store their electronic communications (commonly known as e-mail, text messages, and/or chat communication), graphic images, text files, file transfer protocol logs, programs, and other types of data or information stored in electronic form.

Said suspected place and premises are in charge of and controlled by each of the following:

**AT&T Mobility**  
**11760 US Hwy. 1, Suite 600**  
**North Palm Beach, FL 33408**

There is at said suspected place and premises the following item(s) which are implements or instruments used in the commission of a crime and, or item(s) constituting evidence of a criminal offense or constituting evidence tending to show that a particular person committed a criminal offense:

All stored Electronic Customer Data as defined in the Texas Code of Criminal Procedure (T.C.C.P.) Chapter 18, maintained by AT&T Mobility belonging to or associated with the customer or individual subscriber/user account:

**806-228-0382 and any other accounts attached to this subscriber**

The Electronic Customer Data that is the subject of this warrant includes:

- 1) All subscriber information, including any available telephone numbers, email addresses, IP addresses (including ports), etc., and/or unique account, equipment, and/or network addressing, these may include the Electronic Serial Number (ESNs), International Mobile Subscriber Identifier (IMSI), Temporary Mobile Subscriber Identity number (TMSI), International Mobile Equipment Identifiers (IMEIs), Mobile Equipment Identifiers (MEIDs), Mobile Station Identifiers (MSIDs), Mobile Identification Numbers (MINs), Mobile Dialed Numbers (MDN), Integrated Circuit Card IDs (ICCID), Personal Unlocking/Unblocking Codes (PUKs), PINs (personal identification numbers), Blackberry PINs (personal identification numbers/codes), Apple's Unique Device Identifier (ID) (UDID), and/or Media Access Control (MAC) address(es), and all billing/payment information and accounts notes, for the specified cellular/wireless telephones, and for any other cellular/wireless telephones on the same account as the target numbers.
  
- 2) All outgoing and incoming communications/call detail records (CDRs), with cell sites, including all telephone numbers, chirp numbers/direct connects/walkie-talkie/Universal Fleet Mobile Identifier (UFMI) numbers, email addresses (electronic mail), Internet Protocol (IP) addresses, World Wide Web (www) addresses, dialed/communicated with (outgoing and/or incoming). This includes local and long distance telephone connection records, including all text [short message service SMS] detail records, email detail records [including IP (Internet Protocol) logs, email header information, and email addresses], IP connection detail records/logs, and video, audio, and/or

photo image transactions records, such as multimedia messaging service (MMS) (picture/video messaging) detail records/logs, sent or received, to provide dates, times, and methods of voicemail access, including all available SS7 signaling records of these communications, and, records of session times and durations, and to include content/text of messages if available. Cell Sites are required if they are available on any and all transactional/addressing and routing data.

- 3) Cell sites activations and all registration information, including signal strengths, logs, etc. (if obtainable), including any location information delivered to a public safety answering point (PSAP) pursuant to a 911 call.
- 4) If available, an engineering map; showing all cell-site antenna/tower locations, sectors, azimuths, beam widths, pilot PN (pseudo noise) offsets, and true orientations. And, a list of any and all cellular sites numbers [Long Term Evolution (LTE) —complete CGI or eNodeB and Cell Site, NodeB, Local Area Codes (LACs), Cellular Identifiers (CIDs), intercept access points (IAP) system identities, repolls, switches, etc.], locations, addresses, neighbor lists, etc., and/or latitude and longitude of any said sites. Also, that cellular sites lists, including latitudes and longitudes, be provided, via electronic mail, or via shipping when email is not available, in an electronic format, if available and/or possible. Furthermore, the concerned carrier(s) will provide RF (radio frequency) propagation maps/surveys and cellular antenna/tower maintenance records, and cellular antenna/tower maintenance records procedures, upon request. These maps/surveys and maintenance records will be provided in electronic format, such as original color format, if available.
- 5) Should the cellular/wireless number/equipment which is the current target of this Order have changed, during the requested period, including the MINs/MSIDs, MDNs, ESNs, MEIDs, IMEIs, IMSIs, ICCIDs, PUKs, IP addresses, UDIDs, PINs and/or MAC addresses, or combinations thereof, have been changed by the subscribers during the period of time(s) covered by this Order, then this Order will apply to any other MINs/MSIDs, MDNs, ESNs, MEIDs, IMEIs, IMSIs, ICCIDs, PUKs, IP addresses, UDIDs, PINs, email addresses, and/or MAC addresses. Furthermore if requested the specific manufacturer and model of said handset shall be released verbally or in writing by the Agency making this request.
- 6) Any Internet Service Provider (ISP), email company or email server entity (public or private), website hosting company, and/or website or internet service providing company and/or entity, provide any subscriber information, email addresses, email logs (with header information, Internet Protocol (IP) logs, website addresses, etc., for any email addresses, IP addresses, user names, etc., identified from the original records pertaining to the target devices. Such as, if the original target devices' records reveal Internet activity, such as email activity, web activity, and/or other Internet connected applications, then this Order will also order the release of all subscriber information

pertaining to user identifying, *and* addressing and routing (transactional) information pertaining to that Internet activity (without content information) for the effective period of this order. This includes application of this Order to Microsoft's "Sidekick"/"Danger" products/services. Also to include all location based information for all Google products (GMAIL, Google Voice, etc.) and all Apple products

- 7) Also, whenever possible, that the provider(s) provision, upon the specific requests of the prosecutors/officers/agents/designees, a twenty-four (24) hour switch-technician/employee/vendor to assist in providing data to comply with this Order and/or the interpretation of the provided data.
- 8) Any required information on demand, if possible and upon the specific request of the prosecutors/officers/agents/designees. Further, that any so ordered provider(s), or those possessing said information, provide, upon the specific request of the prosecutors/officers/agents/designees, any historical geo-location services/global positioning system (GPS) data/enhanced 911 (E911) records including but not limited to any available ranging data [distance from tower, range to tower (RTT/REVEAL/Historic MLTs or other similar un-named records held by ANY PROVIDER)], which may be available to any involved provider(s) and/or parties. This includes specifically Sprint's PCMD data (per call measure data) and AT&T's NLEOs report. This also includes all location data captured by Google and Apple.
- 9) All call/communication detail, direct connect, subscriber, numeric messages, alphanumeric/text messages, email records, IP logs, etc., and any related records and/or access be provided, upon the specific request of prosecutors/officers/agents/designees of specific data from specific time period within the confines of this Order, in an electronic format specified by prosecutors/agents/officers/designees. Also, that the records/data be forwarded via email (in a common electronic format as described herein) if possible, upon the specific request of prosecutors/agents/officers/designees, to the listed prosecutor/officer and/or his/her designees. These designees may include, but are not limited to, prosecutors/officers/agents/designees and/or representatives of the Hemphill County District Attorney, Attorney General's Office of Texas (OAG) and the Texas Department of Public Safety (DPS).
- 10) If e-mail is not available/possible, that the providers provide the required data electronically on a common storage medium, such as CD-ROM (compact disc read only memory) discs, and/or thumb drive. Also, that all providers provide, when possible and so requested, all requested data in ASCII, comma separated values (.csv), or fixed length (SDF) format. This is to include that any and all records/data will be provided in all available formats of data, upon request, to include, but not limited to, documents/files currently produced in Microsoft Word, Microsoft Excel, PDF (portable document format), CSV (comma separated value), other electronic formats, and/or pulled from such systems such as "CDR Live," "X-Mine," "CEER,"



and any other electronic medium that is/was in use and/or in development. All CDRs [call/communication detail records (CDRs), including IP (internet protocol) logs, email logs, etc.] will be provided in spreadsheet (Excel, CSV, etc.) format if possible. Only where this is not possible, to provide information in dark, clean typeface, machine-scanable/Optical Character Recognition (OCR) interpretable hardcopy. This includes the faxing of any necessary requested records at the highest possible quality setting. Further, that upon the specific request of prosecutors/agents/officers/designees, that any provided data, including account specific data and cellular site lists, be provided by the necessary providers in a business records affidavit format that complies with the laws of the State of Texas.

- 11) Provide any and all data and services that are ordered herein, verbally, to prosecutors/officers (or designees) if specifically requested to do so. Communications providers are also ordered to notify prosecutors/officers (or designees) if devices roamed (and what specific networks are roamed to/from) from a home/primary network to another network and it is known by the home/primary network to what roaming network the devices roamed. This includes verbally notifying prosecutors/officers (or designees) of the last known network registrations/activity during the above mentioned time frame. And, if the accounts were active accounts, including if the account was inactivated or closed for non-payment, and, how many minutes and/or credits remained on prepaid type accounts. The concerned communications carriers are also ordered to retain, indefinitely, hard and soft copies of all records and/or data provided as a result of this Order.
- 12) RETAIL OUTLETS OR ANY ENTITIES are ordered to release, upon specific request, all purchase, payment (cash, credit, check, prepaid card, etc.), and activation information (even if through third parties) for all target devices, accounts, and subsequent payments, such as prepaid minute cards. This includes the specific data, time, location (including the specific store, register, clerk, etc.) that all devices, account changes, purchases, payments, etc., occurred. It is also ordered that all involved retailers (and neighboring businesses/residences) release any available surveillance video from the aforementioned transactions, both from within, and from the outside of the stores, and the area of the stores, where any of the aforementioned transactions occurred.
- 13) Finally, that this Order will apply to any and all companies/entities which may provide and/or carry wireless/telecommunication services for the target mobile numbers/unique account identifiers/equipment, and/or, any other entity who may possess the requested information, such as Internet companies/entities. This may be required because of number portability and/or if the original carrier was modified due to roaming and/or other considerations/reasons.

It is the belief of the Affiant, that: the AT&T accounts of **806-228-0382 and other accounts**

**held by same provider, contains evidence of the offense of Tampering with Witness, Texas Penal Code section 37.05, a felony offense.**

**AFFIANT HAS PROBABLE CAUSE FOR THE SAID BELIEF BY REASON OF THE FOLLOWING FACTS, TO WIT:**

Your Affiant is Rachel Kading, a peace officer certified by The State of Texas, who is currently employed as a Sergeant with the Office of the Texas Attorney General (OAG). Affiant has been a law enforcement officer for over 15 years. Affiant is currently assigned to the Criminal Investigation Division, Special Investigations Unit, where her duties include investigations involving a wide array of criminal offences ranging from simple fraud to homicides. Affiant has specialized training in the areas of criminal investigations, child abuse and exploitation, narcotics and financial crimes, provided by federal, state, and local agencies. Affiant has previously been involved in the execution search warrants involving persons crimes and narcotics.

On January 26, 2018, Hemphill County Sherriff, NATHAN LEWIS, formally asked the Texas Attorney General's Office to assist in the investigation into the disappearance of THOMAS KELLY BROWN, who was last seen on 11-23-16 in Canadian, Texas. Multiple agencies have been assisting Hemphill County in this investigation.

This affiant was told by BROWN'S mother, PENNY MEEK and by her private investigator, PHILIP KLIEN, that they were shown a photograph of BROWN at Fronks gas station. The photograph appeared to be from security footage. LEWIS denied the photograph existed to this affiant. Fronks is the last place BROWN was seen on 11-23-16. This affiant has never seen this photograph.

On 5-17-18, LEWIS was administered a polygraph examination conducted by the Texas Department of Public Safety polygraph examiner to determine if he had personal knowledge of the circumstances surrounding the photograph at Fronks gas station. This subject was discussed at length during the pre-interview. LEWIS was asked in a series of questions if he had any involvement in BROWN'S disappearance. LEWIS showed deception on the polygraph.

This affiant was told by BRENT CLAPP, Hemphill County Deputy, that the Sheriff's Office does not have the video from Fronks. LEWIS wrote a report stating he never possessed the video and only viewed the video with RON BISHOP. BISHOP is the technician whom provided technical security assistance for Fronks Oil and Gas.

SERGEANT CHRIS SMYTH with the Texas Attorney General's Office, Criminal Investigations Division told this affiant he spoke with BISHOP on the phone on or around May 30, 2018. BISHOP stated he download the requested video for the evening of November 23, 2016 through the early morning hours of November 24, 2016. BISHOP put the video on a thumb drive and brought the drive to LEWIS at the Hemphill County Sheriff's Office. BISHOP downloaded the player for the video onto LEWIS' computer and showed him how to watch the video. BISHOP left the thumb drive with LEWIS. BISHOP did not watch the video at length.

This affiant spoke with BISHOP in person on June 7, 2018. BISHOP stated he was now unsure of what happened. BISHOP could not remember if he left the thumb drive with LEWIS. BISHOP stated he assists law enforcement often and his common practice is to download the videos to thumb drives and to give law enforcement the drive. BISHOP was unsure of what he did in this case although he stated he does it the same every time. BISHOP appeared frightened as he spoke to this affiant. BISHOPS voice was shaking as he spoke and so were his hands. This affiant asked BISHOP if he had contact with LEWIS after he spoke with SERGEANT SMYTH on the phone. BISHOP denied contact.


Based upon all the foregoing, there is probable cause to believe that evidence and instrumentalities used in the commission of Tampering with a Witness, Texas Penal Code section 36.05, a felony offense are located in the account data for BISP HOP'S phone, **806-228-0382 and/or other accounts associated with this account**, currently stored on the computer servers located with:

**AT&T Mobility**  
**11760 US Hwy. 1, Suite 600**  
**North Palm Beach, FL 33408**


By nature of AT&T Mobility, being a Communications Provider, it is realized that many other individuals, organizations, businesses, and other entities utilize this company's services and have no association with the subject investigation. These other unnamed individuals, organizations, businesses, and other entities may have various amounts of information maintained in various forms with AT&T Mobility with a reasonable expectation of privacy. It is Affiant's intent that the search conducted at AT&T Mobility be as unobtrusive as possible, and that it relate to the above listed user account associated with the content that may have been deleted or altered. Further, it is Affiant's intent to use whatever means or methodology is on hand to conduct this search, with limited or no interruption of the service provided to these other unnamed individuals. It is for these reasons that Affiant requests that AT&T Mobility locate and isolate the above-named information on their servers and make a copy of such information in a readable format to provide to Affiant for review as part of this investigation.

All information noted in this affidavit for search warrant has been related to Affiant by the person(s) and/or source(s) attributed or referenced. Affiant further believes in good faith that the information provided herein to be true and correct. Because the sole purpose of this affidavit is to establish probable cause that a criminal offense has occurred, not every relevant fact known to Affiant, or to other investigators, is included within. Rather, only those facts necessary to establish probable cause have been discussed.

WHEREFORE, AFFIANT ASKS FOR ISSUANCE OF A WARRANT THAT WILL AUTHORIZE THE SEARCH OF SAID SUSPECTED PLACE FOR SAID PROPERTY AND SEIZURE OF THE SAME AND TO TAKE CUSTODY OF ALL SEIZED PROPERTY AND SAFE KEEP SUCH PROPERTY AS PROVIDED BY STATUTE.

  
AFFIANT, SERGEANT RACHEL KADING

SUBSCRIBED AND SWORN TO BEFORE ME BY SAID AFFIANT ON THIS THE  
22<sup>nd</sup> day of August, A.D., 2018.

  
STEVEN EMMERT, 31<sup>ST</sup> DISTRICT JUDGE  
HEMPHILL COUNTY, TEXAS

IN RE

AT&T Mobility

§  
§  
§  
§  
§

IN THE DISTRICT COURT FOR  
THE 31ST JUDICIAL DISTRICT,  
HEMPHILL COUNTY, TEXAS

**ORDER SEALING SEARCH WARRANT AFFIDAVIT  
{Article 18.011, Texas Code of Criminal Procedure}**

Upon consideration of the foregoing State's Motion and the affidavit for a search warrant tendered to the Court, the Court finds, in addition to probable cause supporting the issuance of said search warrant, that there is a compelling State interest in the confidentiality of information in the warrant affidavit **{Select and initial as applicable}**

       because public disclosure of the affidavit would jeopardize the safety of a victim, witness, or informant.

  X   because public disclosure of the affidavit would cause the destruction of evidence.

       because the affidavit contains information obtained from a court-ordered wiretap that has not expired.

THEREFORE, the search warrant affidavit described in the foregoing motion is hereby ordered SEALED for thirty (30) days, pursuant to Article 18.011, Texas Code of Criminal Procedure, unless this Court should subsequently find that there is no longer a compelling State interest in the confidentiality of information contained in the affidavit.

The Clerk shall attach to the original search warrant affidavit the foregoing State's Motion and this Order granting the motion to seal the affidavit, and shall not disclose the affidavit or any information contained therein to any person for a period of 30 days from this date, without the express written permission of this Court.

Ordered and signed on this the 22<sup>nd</sup> day of August, 2018, at 5:50 o'clock P.M.



JUDGE PRESIDING  
31st District Court  
Hemphill County, Texas

**SEARCH WARRANT**

**THE STATE OF TEXAS** §

§

**COUNTY OF HEMPHILL** §

To the Sheriff or any Peace Officer of Hemphill County, Texas, or any Peace Officer of the State of Texas:

Whereas, the Affiant whose name appears on the affidavit attached hereto is a peace officer under the laws of Texas and did heretofore this day subscribe and swear to said affidavit before me (which said affidavit is here now made a part hereof for all purposes and incorporated herein as if written verbatim within the confines of this Warrant), and whereas I find that the verified facts stated by Affiant in said affidavit show that Affiant has probable cause for the belief he/she expresses herein and establishes the existence of proper grounds for issuance of this Warrant.

Now, therefore, you are commanded to enter the suspected place as described in said affidavit, to forthwith search the place therein named, to wit:

**CELLCO PARTNERSHIP DBA VERIZON WIRELESS**

**180 Washington Valley Road**

**Bedminster, NJ 07921**

hereinafter, PROVIDER, with the authority to search for and to seize or to compel agents of said PROVIDER to search for, seize and to turn over to the government Electronic Customer Data as defined in the Texas Code of Criminal Procedure (T.C.C.P.) Chapter 18, and held in electronic storage by the PROVIDER for the Electronic Customer Data belonging to or associated with, the customer or individual subscriber/user accounts, from **September 1, 2016 through Current.**

**806-338-0628 and 903-583-2752 AND all account owned by the same subscriber(s)**

At said place you shall search for and, if same be found, seize and bring before me the property described in the affidavit, to-wit:

The Electronic Customer Data that is the subject of this warrant includes:

- 1.) All subscriber information, including any available telephone numbers, email addresses, IP addresses (including ports), etc., and/or unique account, equipment, and/or network addressing, these may include the Electronic Serial Number (ESNs), International Mobile Subscriber Identifier (IMSI), Temporary Mobile Subscriber Identity number (TMSI), International Mobile Equipment Identifiers (IMEIs), Mobile Equipment Identifiers (MEIDs), Mobile Station Identifiers (MSIDs), Mobile Identification Numbers (MINs), Mobile Dialed Numbers (MDN), Integrated Circuit Card IDs (ICCID), Personal Unlocking/Unblocking Codes (PUKs), PINs (personal identification numbers), Blackberry PINs (personal identification numbers/codes), Apple's Unique Device Identifier (ID) (UDID), and/or Media Access Control (MAC) address(es), and all billing/payment information and accounts notes, for the specified cellular/wireless telephones, and for any other cellular/wireless telephones on the same account as the target numbers.
- 2.) All outgoing and incoming communications/call detail records (CDRs), with cell sites, including all telephone numbers, chirp numbers/direct connects/walkie-talkie/Universal Fleet Mobile Identifier (UFMI) numbers, email addresses (electronic mail), Internet Protocol (IP) addresses, World Wide Web (www) addresses, dialed/communicated with (outgoing and/or incoming). This includes local and long distance telephone connection records, including all text [short message service SMS] detail records, email detail records [including IP (Internet Protocol) logs, email header information, and email addresses], IP connection detail records/logs, *and* video, audio, and/or photo image transactions records, such as multimedia messaging service (MMS) (picture/video messaging) detail records/logs, sent or received, to provide dates, times, and methods of voicemail access, including all available SS7 signaling records of these communications, and, records of session times and durations, and to include content/text of messages if available. Cell Sites are required if they are available on any and all transactional/addressing and routing data.
- 3.) Cell sites activations and all registration information, including signal strengths, logs, etc. (if obtainable), including any location information delivered to a public safety answering point (PSAP) pursuant to a 911 call.
- 4.) If available, an engineering map; showing all cell-site antenna/tower locations, sectors, azimuths, beam widths, pilot PN (pseudo noise) offsets, and true orientations. And, a list of any and all cellular sites numbers [Long Term Evolution (LTE) —complete CGI or eNodeB and Cell Site, NodeB, Local Area Codes (LACs), Cellular Identifiers (CIDs), intercept access points (IAP) system identities, repolls, switches, etc.], locations, addresses, neighbor lists, etc., and/or latitude and longitude of any said sites. Also, that cellular sites lists, including latitudes and longitudes, be provided, via electronic mail, or via shipping when email is not available, in an electronic format, if available and/or possible. Furthermore, the



concerned carrier(s) will provide RF (radio frequency) propagation maps/surveys and cellular antenna/tower maintenance records, and cellular antenna/tower maintenance records procedures, upon request. These maps/surveys and maintenance records will be provided in electronic format, such as original color format, if available.

- 5.) Should the cellular/wireless number/equipment which is the current target of this Order have changed, during the requested period, including the MINs/MSIDs, MDNs, ESNs, MEIDs, IMEIs, IMSIs, ICCIDs, PUKs, IP addresses, UDIDs, PINs and/or MAC addresses, or combinations thereof, have been changed by the subscribers during the period of time(s) covered by this Order, then this Order will apply to any other MINs/MSIDs, MDNs, ESNs, MEIDs, IMEIs, IMSIs, ICCIDs, PUKs, IP addresses, UDIDs, PINs, email addresses, and/or MAC addresses. Furthermore if requested the specific manufacturer and model of said handset shall be released verbally or in writing by the Agency making this request.
- 6.) Any Internet Service Provider (ISP), email company or email server entity (public or private), website hosting company, and/or website or internet service providing company and/or entity, provide any subscriber information, email addresses, email logs (with header information, Internet Protocol (IP) logs, website addresses, etc., for any email addresses, IP addresses, user names, etc., identified from the original records pertaining to the target devices. Such as, if the original target devices' records reveal Internet activity, such as email activity, web activity, and/or other Internet connected applications, then this Order will also order the release of all subscriber information pertaining to user identifying, *and* addressing and routing (transactional) information pertaining to that Internet activity (without content information) for the effective period of this order. This includes application of this Order to Microsoft's "Sidekick"/"Danger" products/services. Also to include all location based information for all Google products (GMAIL, Google Voice, etc.) and all Apple products
- 7.) Also, whenever possible, that the provider(s) provision, upon the specific requests of the prosecutors/officers/agents/designees, a twenty-four (24) hour switch-technician/employee/vendor to assist in providing data to comply with this Order and/or the interpretation of the provided data.
- 8.) Any required information on demand, if possible and upon the specific request of the prosecutors/officers/agents/designees. Further, that any so ordered provider(s), or those possessing said information, provide, upon the specific request of the prosecutors/officers/agents/designees, any historical geo-location services/global positioning system (GPS) data/enhanced 911 (E911) records including but not limited to any available ranging data [distance from tower, range to tower (RTT/REVEAL/Historic MLTs or other similar un-named records held by ANY PROVIDER)], which may be available to any involved provider(s) and/or parties.

This includes specifically Sprint's PCMD data (per call measure data) and AT&T's NLEOs report. This also includes all location data captured by Google and Apple.

- 9.) All call/communication detail, direct connect, subscriber, numeric messages, alpha-numeric/text messages, email records, IP logs, etc., and any related records and/or access be provided, upon the specific request of prosecutors/officers/agents/designees of specific data from specific time period within the confines of this Order, in an electronic format specified by prosecutors/agents/officers/designees. Also, that the records/data be forwarded via email (in a common electronic format as described herein) if possible, upon the specific request of prosecutors/agents/officers/designees, to the listed prosecutor/officer and/or his/her designees. These designees may include, but are not limited to, prosecutors/officers/agents/designees and/or representatives of the Hemphill County District Attorney, Attorney General's Office of Texas (OAG) and the Texas Department of Public Safety (DPS).
  
- 10.) If e-mail is not available/possible, that the providers provide the required data electronically on a common storage medium, such as CD-ROM (compact disc read only memory) discs, and/or thumb drive. Also, that all providers provide, when possible and so requested, all requested data in ASCII, comma separated values (.csv), or fixed length (SDF) format. This is to include that any and all records/data will be provided in all available formats of data, upon request, to include, but not limited to, documents/files currently produced in Microsoft Word, Microsoft Excel, PDF (portable document format), CSV (comma separated value), other electronic formats, and/or pulled from such systems such as "CDR Live," "X-Mine," "CEER," and any other electronic medium that is/was in use and/or in development. All CDRs [call/communication detail records (CDRs), including IP (internet protocol) logs, email logs, etc.] will be provided in spreadsheet (Excel, CSV, etc.) format if possible. Only where this is not possible, to provide information in dark, clean typeface, machine-scanable/Optical Character Recognition (OCR) interpretable hardcopy. This includes the faxing of any necessary requested records at the highest possible quality setting. Further, that upon the specific request of prosecutors/agents/officers/designees, that any provided data, including account specific data and cellular site lists, be provided by the necessary providers in a business records affidavit format that complies with the laws of the State of Texas.
  
- 11.) Provide any and all data and services that are ordered herein, verbally, to prosecutors/officers (or designees) if specifically requested to do so. Communications providers are also ordered to notify prosecutors/officers (or designees) if devices roamed (and what specific networks are roamed to/from) from a home/primary network to another network and it is known by the home/primary network to what roaming network the devices roamed. This includes verbally notifying prosecutors/officers (or designees) of the last known network registrations/activity during the above mentioned time frame. And, if the accounts were active accounts, including if the account was inactivated or closed

for non-payment, and, how many minutes and/or credits remained on prepaid type accounts. The concerned communications carriers are also ordered to retain, indefinitely, hard and soft copies of all records and/or data provided as a result of this Order.

- 12.) RETAIL OUTLETS OR ANY ENTITIES are ordered to release, upon specific request, all purchase, payment (cash, credit, check, prepaid card, etc.), and activation information (even if through third parties) for all target devices, accounts, and subsequent payments, such as prepaid minute cards. This includes the specific data, time, location (including the specific store, register, clerk, etc.) that all devices, account changes, purchases, payments, etc., occurred. It is also ordered that all involved retailers (and neighboring businesses/residences) release any available surveillance video from the aforementioned transactions, both from within, and from the outside of the stores, and the area of the stores, where any of the aforementioned transactions occurred.
- 13.) Finally, that this Order will apply to any and all companies/entities which may provide and/or carry wireless/telecommunication services for the target mobile numbers/unique account identifiers/equipment, and/or, any other entity who may possess the requested information, such as Internet companies/entities. This may be required because of number portability and/or if the original carrier was modified due to roaming and/or other considerations/reasons.

This Court **ORDERS** the **Custodian of Records / Verizon Wireless, 180 Washington Valley Road Bedminster, NJ 07921** shall disclose responsive data, if any, by sending to **Sergeant Rachel Kading of the Office of the Texas Attorney General located at 300 West 15<sup>th</sup> Street, Austin TX, 78701 Mail Code 065** by courier service or to **PO BOX 12548, Austin TX 78711 - MC 065** using the US Postal Service, notwithstanding 18 U.S.C. 2252A or similar statute or code, where all received data will be analyzed.

Further, Affiant is **ORDERED**, pursuant to the provisions of Article 18.10, Texas Code of Criminal Procedure, to retain custody of any property seized pursuant to this Warrant, until further order of this Court or any other court of appropriate jurisdiction shall otherwise direct the manner of safekeeping of said property. This Court grants you leave and authority to remove such seized property from this county, if and only if such removal is necessary for the safekeeping of such seized property by Affiant, or if the provisions of Article 18.10, T.C.C.P. otherwise authorize such removal. Affiant is further **ORDERED** to give notice to this Court, as a part of the inventory to be filed subsequent to the execution of this Warrant, and as required by Article 18.10, T.C.C.P., of the place where the property seized hereunder is kept, stored and held.

Herein fail not but have you then and there this Warrant within ten days, exclusive of the day of its execution, with your return thereon, showing how you executed the same.

ISSUED THIS THE 22<sup>nd</sup> day of August, A.D., 2018, at 5:30 o'clock P.M.  
to certify which, witness my hand this day.



---

STEVEN EMMERT, 31<sup>ST</sup> DISTRICT JUDGE  
HEMPHILL COUNTY, TEXAS

**THE STATE OF TEXAS**

'

'

**COUNTY OF HEMPHILL**

'

**AFFIDAVIT FOR SEARCH WARRANT**

BEFORE ME, THE UNDERSIGNED AUTHORITY, PERSONALLY APPEARED THE AFFIANT HEREIN, A PEACE OFFICER UNDER THE LAWS OF TEXAS, WHO, BEING DULY SWORN, ON OATH MADE THE FOLLOWING STATEMENTS:

My name is Rachel Kading and I am commissioned as a peace officer by the Texas Office of the Attorney General.

There is in Bedminster, New Jersey, a Communications Service Provider known as **Cellco Partnership DBA Verizon Wireless** located at **180 Washington Valley Road Bedminster, NJ 07921**.

Cellco Partnership DBA Verizon Wireless in its capacity as a Communications Service provider, provides individuals or subscribers with access to mobile phone services used to make phone calls or send and receive text messages. Verizon Wireless also provides subscribers with internet services which provide subscribers to e-mail services, photo storage services, chat service, and access solution services. These services allow customers reserve or maintain storage space on Verizon Wireless computer servers. Subscribers can use Verizon Wireless servers to store their electronic communications (commonly known as e-mail, text messages, and/or chat communication), graphic images, text files, file transfer protocol logs, programs, and other types of data or information stored in electronic form.

Said suspected place and premises are in charge of and controlled by each of the following:

**CELLCO PARTNERSHIP DBA VERIZON WIRELESS**  
**180 Washington Valley Road Bedminster, NJ 07921**

There is at said suspected place and premises the following item(s) which are implements or instruments used in the commission of a crime and, or item(s) constituting evidence of a criminal offense or constituting evidence tending to show that a particular person committed a criminal offense:

- a. All stored Electronic Customer Data as defined in the Texas Code of Criminal Procedure (T.C.C.P.) Chapter 18, maintained by Verizon Wireless belonging to or associated with the customer or individual subscriber/user account:

**806-338-0628 and 903-583-2752 AND all account owned by the same subscriber(s)**

The Electronic Customer Data that is the subject of this warrant includes:

- 1) All subscriber information, including any available telephone numbers, email addresses, IP addresses (including ports), etc., and/or unique account, equipment, and/or network addressing, these may include the Electronic Serial Number (ESNs), International Mobile Subscriber Identifier (IMSI), Temporary Mobile Subscriber Identity number (TMSI), International Mobile Equipment Identifiers (IMEIs), Mobile Equipment Identifiers (MEIDs), Mobile Station Identifiers (MSIDs), Mobile Identification Numbers (MINs), Mobile Dialed Numbers (MDN), Integrated Circuit Card IDs (ICCID), Personal Unlocking/Unblocking Codes (PUKs), PINs (personal identification numbers), Blackberry PINs (personal identification numbers/codes), Apple's Unique Device Identifier (ID) (UDID), and/or Media Access Control (MAC) address(es), and all billing/payment information and accounts notes, for the specified cellular/wireless telephones, and for any other cellular/wireless telephones on the same account as the target numbers.
- 2) All outgoing and incoming communications/call detail records (CDRs), with cell sites, including all telephone numbers, chirp numbers/direct connects/walkie-talkie/Universal Fleet Mobile Identifier (UFMI) numbers, email addresses (electronic mail), Internet Protocol (IP) addresses, World Wide Web (www) addresses, dialed/communicated with (outgoing and/or incoming). This includes local and long distance telephone connection records, including all text [short message service SMS] detail records, email detail records [including IP (Internet Protocol) logs, email header information, and email addresses], IP connection detail records/logs, and video, audio, and/or photo image transactions records, such as multimedia messaging service (MMS) (picture/video messaging) detail records/logs, sent or received, to provide dates, times, and methods of voicemail access, including all available SS7 signaling records of these communications, and, records of session times and durations, and to include content/text of messages if available. Cell Sites are required if they are available on any and all transactional/addressing and routing data.

- 3) Cell sites activations and all registration information, including signal strengths, logs, etc. (if obtainable), including any location information delivered to a public safety answering point (PSAP) pursuant to a 911 call.
- 4) If available, an engineering map; showing all cell-site antenna/tower locations, sectors, azimuths, beam widths, pilot PN (pseudo noise) offsets, and true orientations. And, a list of any and all cellular sites numbers [Long Term Evolution (LTE) —complete CGI or eNodeB and Cell Site, NodeB, Local Area Codes (LACs), Cellular Identifiers (CIDs), intercept access points (IAP) system identities, repolls, switches, etc.], locations, addresses, neighbor lists, etc., and/or latitude and longitude of any said sites. Also, that cellular sites lists, including latitudes and longitudes, be provided, via electronic mail, or via shipping when email is not available, in an electronic format, if available and/or possible. Furthermore, the concerned carrier(s) will provide RF (radio frequency) propagation maps/surveys and cellular antenna/tower maintenance records, and cellular antenna/tower maintenance records procedures, upon request. These maps/surveys and maintenance records will be provided in electronic format, such as original color format, if available.
- 5) Should the cellular/wireless number/equipment which is the current target of this Order have changed, during the requested period, including the MINs/MSIDs, MDNs, ESNs, MEIDs, IMEIs, IMSIs, ICCIDs, PUKs, IP addresses, UDIDs, PINs and/or MAC addresses, or combinations thereof, have been changed by the subscribers during the period of time(s) covered by this Order, then this Order will apply to any other MINs/MSIDs, MDNs, ESNs, MEIDs, IMEIs, IMSIs, ICCIDs, PUKs, IP addresses, UDIDs, PINs, email addresses, and/or MAC addresses. Furthermore if requested the specific manufacturer and model of said handset shall be released verbally or in writing by the Agency making this request.
- 6) Any Internet Service Provider (ISP), email company or email server entity (public or private), website hosting company, and/or website or internet service providing company and/or entity, provide any subscriber information, email addresses, email logs (with header information, Internet Protocol (IP) logs, website addresses, etc., for any email addresses, IP addresses, user names, etc., identified from the original records pertaining to the target devices. Such as, if the original target devices' records reveal Internet activity, such as email activity, web activity, and/or other Internet connected applications, then this Order will also order the release of all subscriber information pertaining to user identifying, *and* addressing and routing (transactional) information pertaining to that Internet activity (without content information) for the effective period of this order. This includes application of this Order to Microsoft's "Sidekick"/"Danger" products/services. Also to include all location based information for all Google products (GMAIL, Google Voice, etc.) and all Apple products

- 7) Also, whenever possible, that the provider(s) provision, upon the specific requests of the prosecutors/officers/agents/designees, a twenty-four (24) hour switch-technician/employee/vendor to assist in providing data to comply with this Order and/or the interpretation of the provided data.
- 8) Any required information on demand, if possible and upon the specific request of the prosecutors/officers/agents/designees. Further, that any so ordered provider(s), or those possessing said information, provide, upon the specific request of the prosecutors/officers/agents/designees, any historical geo-location services/global positioning system (GPS) data/enhanced 911 (E911) records including but not limited to any available ranging data [distance from tower, range to tower (RTT/REVEAL/Historic MLTs or other similar un-named records held by ANY PROVIDER)], which may be available to any involved provider(s) and/or parties. This includes specifically Sprint's PCMD data (per call measure data) and AT&T's NLEOs report. This also includes all location data captured by Google and Apple.
- 9) All call/communication detail, direct connect, subscriber, numeric messages, alphanumeric/text messages, email records, IP logs, etc., and any related records and/or access be provided, upon the specific request of prosecutors/officers/agents/designees of specific data from specific time period within the confines of this Order, in an electronic format specified by prosecutors/agents/officers/designees. Also, that the records/data be forwarded via email (in a common electronic format as described herein) if possible, upon the specific request of prosecutors/agents/officers/designees, to the listed prosecutor/officer and/or his/her designees. These designees may include, but are not limited to, prosecutors/officers/agents/designees and/or representatives of the Hemphill County District Attorney, Attorney General's Office of Texas (OAG) and the Texas Department of Public Safety (DPS).
- 10) If e-mail is not available/possible, that the providers provide the required data electronically on a common storage medium, such as CD-ROM (compact disc read only memory) discs, and/or thumb drive. Also, that all providers provide, when possible and so requested, all requested data in ASCII, comma separated values (.csv), or fixed length (SDF) format. This is to include that any and all records/data will be provided in all available formats of data, upon request, to include, but not limited to, documents/files currently produced in Microsoft Word, Microsoft Excel, PDF (portable document format), CSV (comma separated value), other electronic formats, and/or pulled from such systems such as "CDR Live," "X-Mine," "CEER," and any other electronic medium that is/was in use and/or in development. All CDRs [call/communication detail records (CDRs), including IP (internet protocol) logs, email logs, etc.] will be provided in spreadsheet (Excel, CSV, etc.) format if possible. Only where this is not possible, to provide information in dark, clean typeface, machine-scanable/Optical Character Recognition (OCR) interpretable hardcopy. This includes the faxing of any necessary requested records at the highest possible quality setting. Further, that upon the specific request of



prosecutors/agents/officers/designees, that any provided data, including account specific data and cellular site lists, be provided by the necessary providers in a business records affidavit format that complies with the laws of the State of Texas.

- 11) Provide any and all data and services that are ordered herein, verbally, to prosecutors/officers (or designees) if specifically requested to do so. Communications providers are also ordered to notify prosecutors/officers (or designees) if devices roamed (and what specific networks are roamed to/from) from a home/primary network to another network and it is known by the home/primary network to what roaming network the devices roamed. This includes verbally notifying prosecutors/officers (or designees) of the last known network registrations/activity during the above mentioned time frame. And, if the accounts were active accounts, including if the account was inactivated or closed for non-payment, and, how many minutes and/or credits remained on prepaid type accounts. The concerned communications carriers are also ordered to retain, indefinitely, hard and soft copies of all records and/or data provided as a result of this Order.
  
- 12) RETAIL OUTLETS OR ANY ENTITIES are ordered to release, upon specific request, all purchase, payment (cash, credit, check, prepaid card, etc.), and activation information (even if through third parties) for all target devices, accounts, and subsequent payments, such as prepaid minute cards. This includes the specific data, time, location (including the specific store, register, clerk, etc.) that all devices, account changes, purchases, payments, etc., occurred. It is also ordered that all involved retailers (and neighboring businesses/residences) release any available surveillance video from the aforementioned transactions, both from within, and from the outside of the stores, and the area of the stores, where any of the aforementioned transactions occurred.
  
- 13) Finally, that this Order will apply to any and all companies/entities which may provide and/or carry wireless/telecommunication services for the target mobile numbers/unique account identifiers/equipment, and/or, any other entity who may possess the requested information, such as Internet companies/entities. This may be required because of number portability and/or if the original carrier was modified due to roaming and/or other considerations/reasons.

It is the belief of the Affiant, that: the Verizon Wireless accounts of **806-338-0628 and 903-583-2752 AND all account owned by the same subscriber(s)**, contains evidence of the offense of Tampering with or Fabricating Physical Evidence, Texas Penal Code section 37.09, a felony offense.

**AFFIANT HAS PROBABLE CAUSE FOR THE SAID BELIEF BY REASON OF THE FOLLOWING FACTS, TO WIT:**

Your Affiant is Rachel Kading, a peace officer certified by The State of Texas, who is currently employed as a Sergeant with the Office of the Texas Attorney General (OAG). Affiant has been a law enforcement officer for over 15 years. Affiant is currently assigned to the Criminal Investigation Division, Special Investigations Unit, where her duties include investigations involving a wide array of criminal offences ranging from simple fraud to homicides. Affiant has specialized training in the areas of criminal investigations, child abuse and exploitation, narcotics and financial crimes, provided by federal, state, and local agencies. Affiant has previously been involved in the execution search warrants involving persons crimes and narcotics.

On January 26, 2018, Hemphill County Sherriff, NATHAN LEWIS, formally asked the Texas Attorney General's Office to assist in the investigation into the disappearance of THOMAS KELLY BROWN, who was last seen on 11-23-16 in Canadian, Texas. Multiple agencies have been assisting Hemphill County in this investigation.

This affiant was told by BROWN'S mother, PENNY MEEK and by her private investigator, PHILIP KLIEN, that they were shown a photograph of BROWN at Fronks gas station. The photograph appeared to be from security footage. LEWIS denied the photograph existed to this affiant. Fronks is the last place BROWN was seen alive on 11-23-16. This affiant has never seen this photograph.

This affiant was told by BRENT CLAPP, Hemphill County Deputy, that the Sheriff's Office does not have the video from Fronks. LEWIS wrote a report stating he never possessed the video and only viewed the video with RON BISHOP. BISHOP is the technician whom provided technical security assistance for Fronks Oil and Gas.

SERGEANT CHRIS SMYTH with the Texas Attorney General's Office, Criminal Investigations Division told this affiant he spoke with BISHOP on the phone on or around May 30, 2018. BISHOP stated he download the requested video for the evening of November 23, 2016 through

the early morning hours of November 24, 2016. BISHOP put the video on a thumb drive and brought the drive to LEWIS at the Hemphill County Sheriff's Office. BISHOP downloaded the player for the video onto LEWIS' computer and showed him how to watch the video. BISHOP left the thumb drive with LEWIS. BISHOP did not watch the video at length.

This affiant contacted Dollar General, located north of Fronks to determine if the photograph was obtained from their security cameras. This affiant learned the outside cameras at this location are on the north side of the building and face the parking lot and 2cnd Street, the street that Fronks and Dollar General sit on. This affiant was told the Hemphill County Sheriff's Department was given a copy of the video from the evening BROWN went missing. LEWIS was asked for the copy of the video and LEWIS stated there was never video recovered from Dollar General.

Three managers at Dollar General, ASHLEY WILSON, SHARON HAVEL and ELIZABETH GALLEGOS, each independently stated the Sheriff's Department was given the video from the night BROWN disappeared. ASHLEY WILSON was the manager on duty when the deputies came to retrieve the video. WILSON did not know the deputies name but described him as a "skinny white guy with glasses". This affiant showed WILSON photographs of the entire Hemphill County Sherriff's Office staff. WILSON identified PYNE GREGORY as the deputy whom retrieved the video.

Based upon all the foregoing, there is probable cause to believe that evidence and instrumentalities used in the commission of Tampering with or Fabricating Physical Evidence, Texas Penal Code section 37.09, a felony offense are located in the account data for PYNE GREGORY'S phone(s), 806-338-0628 and 903-583-2752, currently stored on the computer servers located with:

**CELLCO PARTNERSHIP DBA VERIZON WIRELESS**

**180 Washington Valley Road**

**Bedminster, NJ 07921**

By nature of Cellco Partnership, being a Communications Provider, it is realized that many other individuals, organizations, businesses, and other entities utilize this company's services and have

no association with the subject investigation. These other unnamed individuals, organizations, businesses, and other entities may have various amounts of information maintained in various forms with Cellco Partnership with a reasonable expectation of privacy. It is Affiant's intent that the search conducted at Cellco Partnership be as unobtrusive as possible, and that it relate to the above listed user account associated with the content that may have been deleted or altered. Further, it is Affiant's intent to use whatever means or methodology is on hand to conduct this search, with limited or no interruption of the service provided to these other unnamed individuals. It is for these reasons that Affiant requests that Cellco Partnership locate and isolate the above named information on their servers and make a copy of such information in a readable format to provide to Affiant for review as part of this investigation.

All information noted in this affidavit for search warrant has been related to Affiant by the person(s) and/or source(s) attributed or referenced. Affiant further believes in good faith that the information provided herein to be true and correct. Because the sole purpose of this affidavit is to establish probable cause that a criminal offense has occurred, not every relevant fact known to Affiant, or to other investigators, is included within. Rather, only those facts necessary to establish probable cause have been discussed.

WHEREFORE, AFFIANT ASKS FOR ISSUANCE OF A WARRANT THAT WILL AUTHORIZE THE SEARCH OF SAID SUSPECTED PLACE FOR SAID PROPERTY AND SEIZURE OF THE SAME AND TO TAKE CUSTODY OF ALL SEIZED PROPERTY AND SAFE KEEP SUCH PROPERTY AS PROVIDED BY STATUTE.



AFFIANT, SERGEANT RACHEL KADING

SUBSCRIBED AND SWORN TO BEFORE ME BY SAID AFFIANT ON THIS THE  
22<sup>nd</sup> day of August, A.D., 2018.



---

STEVEN EMMERT, 31<sup>ST</sup> DISTRICT JUDGE  
HEMPHILL COUNTY, TEXAS

IN RE

CELLCO PARTNERSHIP  
dba VERIZON WIRELESS

§  
§  
§  
§  
§  
§

IN THE DISTRICT COURT FOR  
THE 31ST JUDICIAL DISTRICT,  
HEMPHILL COUNTY, TEXAS

**ORDER SEALING SEARCH WARRANT AFFIDAVIT  
{Article 18.011, Texas Code of Criminal Procedure}**

Upon consideration of the foregoing State's Motion and the affidavit for a search warrant tendered to the Court, the Court finds, in addition to probable cause supporting the issuance of said search warrant, that there is a compelling State interest in the confidentiality of information in the warrant affidavit **{Select and initial as applicable}**

     because public disclosure of the affidavit would jeopardize the safety of a victim, witness, or informant.

  X   because public disclosure of the affidavit would cause the destruction of evidence.

     because the affidavit contains information obtained from a court-ordered wiretap that has not expired.

THEREFORE, the search warrant affidavit described in the foregoing motion is hereby ordered SEALED for thirty (30) days, pursuant to Article 18.011, Texas Code of Criminal Procedure, unless this Court should subsequently find that there is no longer a compelling State interest in the confidentiality of information contained in the affidavit.

The Clerk shall attach to the original search warrant affidavit the foregoing State's Motion and this Order granting the motion to seal the affidavit, and shall not disclose the affidavit or any information contained therein to any person for a period of 30 days from this date, without the express written permission of this Court.

Ordered and signed on this the 22<sup>nd</sup> day of August, 2018, at 5:50 o'clock P.M.



JUDGE PRESIDING  
31st District Court  
Hemphill County, Texas

**THE STATE OF TEXAS**

§  
§  
§

**COUNTY OF HEMPHILL**

**SEARCH WARRANT**

To the Sheriff or any Peace Officer of Hemphill County, Texas, or any Peace Officer of the State of Texas:

Whereas, the Affiant whose name appears on the affidavit attached hereto is a Peace Officer under the laws of Texas and did heretofore this day subscribe and swear to said affidavit before me (which said affidavit is here now made a part hereof for all purposes and incorporated herein as if written verbatim within the confines of this Warrant), and whereas I find that the verified facts stated by Affiant in said affidavit show that Affiant has probable cause for the belief he/she expresses herein and establishes the existence of proper grounds for issuance of this Warrant;

Now, therefore, you are commanded to enter the suspected place as described in said affidavit, to-wit:

**Apple, Inc.  
One Apple Park Way, MS: 169-5CLP  
Cupertino, CA 95014**

At said place you shall search for and, if same be found, seize and bring before me the property described in the affidavit, to-wit:

a. All stored files, maintained by Apple, Inc. including but not limited to the server storage space, app data, device settings, home screen app organization, iMessage, text (sms), MMS messages, photos, videos, purchase history, device ids associated to the named subscriber, ip logs where accessed, associated accounts, iTunes, subscriber/user account:

**brownthomas786@yahoo.com and tuckerbrown120@yahoo.com**

These files may include, but are not limited to: subscriber's full name(s), subscriber's address(es), subscriber's telephone number(s), e-mail address(es) associated with the subscriber(s), account or log-in name(s), any other information pertaining to the identity of the subscriber(s), billing information, credit card or payment information, types of services utilized by the subscriber and the lengths of such services or any other identifying or pertinent records relating to the subscriber, including IP addresses, and dates and times of access if available.

b. All business records or files maintained by Apple, Inc. belonging to or associated with the customer or individual subscriber/user **brownthomas786@yahoo.com** and **tuckerbrown120@yahoo.com**. These records may include, but are not limited to: account application information, credit card or other billing information, account access information, user logon information (including secondary user log on names), account usage reports, e-mail transaction information, text messages, images, news group access and posting information and any other information, both in electronic computer data and written record format, that records the activities of these accounts relating to the subscriber's use of the services offered by Apple, Inc.

c. All stored electronic mail (e-mail) or messages (SMS, MMS, or iMessage) of any kind maintained by Apple, Inc. that were sent to, from and/or through the accounts of or associated with the customer or individual subscriber/user account utilizing **brownthomas786@yahoo.com** and **tuckerbrown120@yahoo.com**.

d. All stored electronic content maintained by Apple, Inc. (including Internet history, file transfer protocol logs, text messages, web access logs, electronically stored images, etc.) as well as all connection log files listing all account activity conducted by the subscriber/user associated with the customer or individual subscriber/user account utilizing the username or account name of **brownthomas786@yahoo.com** and **tuckerbrown120@yahoo.com** including dates, times, methods of connecting (e.g. telnet, ftp, http, etc.), telephone dial-up connection records and any other connection information or Internet traffic data.

e. Any and all email transactions and/ or file transfer protocol logs maintained by Apple, Inc. associated with the screen name or user name of **brownthomas786@yahoo.com** and **tuckerbrown120@yahoo.com**.

f. Any and all data or images maintained by Apple, Inc. associated with the screen name or user name of **brownthomas786@yahoo.com** and **tuckerbrown120@yahoo.com** including but not limited to stored photos, documents, contacts, calendars, bookmarks, Safari browsing history, Maps Search History, Messages and iOS device backups

This Court **ORDERS** the Apple, Inc., One Apple Park Way, MS: 169-5CLP Cupertino, CA 95014 to collect all data, as previously outlined within this warrant, and to disclose responsive data, if any, by sending such to **SGT. RACHEL KADING** located at 300 West 15<sup>th</sup> Street, Austin, TX 78701 using the U.S. Postal Service or another courier service, an online records portal, or other acceptable means of electronic delivery, to **rachel.kading@oag.texas.gov** notwithstanding 18 U.S.C. 2252A or similar statute or code, where all received data will be analyzed.



Further, Affiant is **ORDERED**, pursuant to the provisions of Article 18.10, Texas Code of Criminal Procedure, to retain custody of any property seized pursuant to this Warrant, until further order of this Court or any other court of appropriate jurisdiction shall otherwise direct the manner of safekeeping of said property. This Court grants you leave and authority to remove such seized property from this county, if and only if such removal is necessary for the safekeeping of such seized property by Affiant, or if the provisions of Article 18.10, T.C.C.P. otherwise authorize such removal. Affiant is further **ORDERED** to give notice to this Court, as a part of the inventory to be filed subsequent to the execution of this Warrant, and as required by Article 18.10, T.C.C.P., of the place where the property seized hereunder is kept, stored and held.

Herein fail not, but have you then and there this warrant within ten days, exclusive of the day of its execution, with your return thereon, showing how you executed the same.

ISSUED THIS THE 5th day of February, A.D., 2020, at 11:40 o'clock A.M. to certify which, witness my hand this day.



---

**STEVEN EMMERT, 31ST DISTRICT JUDGE  
HEMPHILL COUNTY, TEXAS**

**THE STATE OF TEXAS**  
**COUNTY OF HEMPHILL**

§  
§  
§

**AFFIDAVIT FOR SEARCH WARRANT**

**BEFORE ME, THE UNDERSIGNED AUTHORITY, PERSONALLY APPEARED THE AFFIANT HEREIN, A PEACE OFFICER UNDER THE LAWS OF TEXAS, WHO, BEING DULY SWORN, ON OATH MADE THE FOLLOWING STATEMENTS:**

My name is **Sgt. Rachel Kading** and the **Office of Attorney General of Texas** commissions me as a Texas peace officer.

**1. There is in Cupertino, California, a Communications Service Provider known as Apple, Inc. located at One Apple Park Way, Cupertino, CA 95014.**

This Company, in its capacity as an Internet service/company, provides access to a worldwide computer network, commonly known as the Internet, to individuals and/or other users who have a subscription to, membership with, or affiliation with their company, organization or commercial service. Apple, Inc. also provides web hosting and access solutions to its customers in which they reserve and/or maintain computer disk storage space on their own computer system servers for the use of the Internet subscribers/customers/users associated with their company. Items contained on the previously mentioned storage space can include electronic communications (commonly known as e-mail) between subscriber(s) and other parties, graphic image and/or text files, Internet history or internet hyperlinks, file transfer protocol logs, website access logs, programs and other types of data or information stored in electronic form(s). Internet Service Companies, such as Apple, Inc., also maintain records pertaining to the individual's and/or other users who have subscriber accounts with their company. This information can include registration information, account application information, credit card or other billing information, account access information, user logon information (including secondary user log on names), account usage reports, e-mail transaction information, news group access and posting information and other information both in computer data and written record format that records the activities of these accounts relating to the subscriber's use of the services offered by the Internet Service Provider. Said suspected place and premises are in charge of and controlled by each of the following:

**Apple Privacy and Law Enforcement Compliance  
Apple, Inc.  
One Apple Park Way  
Cupertino, CA. 95014**

**2. There is at said suspected place and premises the following item(s) which are implements or instruments used in the commission of a crime and, or item(s) constituting evidence of a criminal offense or constituting evidence tending to show that a particular person committed a criminal offense: Texas Penal Code 37.09 Tampering with or Fabricating Physical Evidence, a felony offense.**

a. All stored files, maintained by Apple, Inc. including but not limited to the server storage space, app data, device settings, home screen app organization, iMessage, text (sms), MMS messages, photos, videos, purchase history, device ids associated to the named subscriber, ip logs where accessed, associated accounts, iTunes, subscriber/user account:

**brownthomas786@yahoo.com and tuckerbrown120@yahoo.com**

These files may include, but are not limited to: subscriber's full name(s), subscriber's address(es), subscriber's telephone number(s), e-mail address(es) associated with the subscriber(s), account or log-in name(s), any other information pertaining to the identity of the subscriber(s), billing information, credit card or payment information, types of services utilized by the subscriber and the lengths of such services or any other identifying or pertinent records relating to the subscriber, including IP addresses, and dates and times of access if available.

b. All business records or files maintained by Apple, Inc. belonging to or associated with the customer or individual subscriber/user **brownthomas786@yahoo.com and tuckerbrown120@yahoo.com**. These records may include, but are not limited to: account application information, credit card or other billing information, account access information, user logon information (including secondary user log on names), account usage reports, e-mail transaction information, text messages, images, news group access and posting information and any other information, both in electronic computer data and written record format, that records the activities of these accounts relating to the subscriber's use of the services offered by Apple, Inc.

c. All stored electronic mail (e-mail) or messages (SMS, MMS, or iMessage) of any kind maintained by Apple, Inc. that were sent to, from and/or through the accounts of or associated with the customer or individual subscriber/user account utilizing **brownthomas786@yahoo.com and tuckerbrown120@yahoo.com**.

d. All stored electronic content maintained by Apple, Inc. (including Internet history, file transfer protocol logs, text messages, web access logs, electronically stored images, etc.) as well as all connection log files listing all account activity conducted by the subscriber/user associated with the customer or individual subscriber/user account utilizing the username or account name of **brownthomas786@yahoo.com and tuckerbrown120@yahoo.com** including dates, times, methods of connecting (e.g. telnet, ftp, http, etc.), telephone dial-up connection records and any other connection information or Internet traffic data.

e. Any and all email transactions and/ or file transfer protocol logs maintained by Apple, Inc. associated with the screen name or user name of **brownthomas786@yahoo.com and tuckerbrown120@yahoo.com**.

f. Any and all data or images maintained by Apple, Inc. associated with the screen name or user name of **brownthomas786@yahoo.com and tuckerbrown120@yahoo.com** including but not limited to stored photos, documents, contacts, calendars, bookmarks, Safari browsing history, Maps Search History, Messages and iOS device backups

**3. It is the belief of the Affiant, that: The Apple iCloud account of brownthomas786@yahoo.com and tuckerbrown120@yahoo.com contains evidence of the Texas Penal Code 37.09 Tampering with or Fabricating Physical Evidence, a felony offense.**

**4. AFFIANT HAS PROBABLE CAUSE FOR THE SAID BELIEF BY REASON OF THE FOLLOWING FACTS, TO WIT:**

Your Affiant is Rachel Kading, a peace officer certified by The State of Texas, who is currently employed as a Sergeant with the Office of the Texas Attorney General (OAG). Affiant has been a law enforcement officer for over 16 years. Affiant is currently assigned to the Criminal Investigation Division, Special Investigations Unit, where her duties include investigations involving a wide array of criminal offences ranging from simple fraud to homicides. Affiant has specialized training in the areas of criminal investigations, child abuse and exploitation, narcotics and financial crimes, provided by federal, state, and local agencies. Affiant has previously been involved in the execution of search warrants involving persons crimes and narcotics.

On January 26, 2018, Hemphill County Sherriff, NATHAN LEWIS, formally asked the Texas Attorney General's Office to assist in the investigation into the disappearance of THOMAS KELLY BROWN, who was last seen on 11-23-16 in Canadian, Texas. On January 9, 2019, THOMAS BROWN'S remains were located near Lake Marvin in Hemphill County, Texas. A cause or manner of death has not yet been determined.

On 10-14-17 a private investigator hired by the Brown family and deputies from the Hemphill County Sheriff's Office searched an area between Lake Marvin Road and State Highway (SH) 60 in Hemphill County. During the search on 10-14-17, an Apple iPhone 6S (A1688) was located approximately 45 feet from the SH 60 and Lake Marvin Road intersection and approximately 3 feet south of Lake Marvin Road. The Apple iPhone 6S was in near perfect condition and did not appear to have been outside in the elements since BROWN's disappearance on 11-23-16. The roadway had been mowed several times between November 2016 and October of 2017 and received a significant amount of rain during that time. The Apple iPhone 6S's weather sensors had not activated and the phone was free of nicks, scrapes and/or damage it would have sustained if exposed to the elements on the side of the busy roadway. The

Apple iPhone 6S was analyzed by the Federal Bureau of Investigation (FBI) and the contents of the phone were provided to this Affiant. The recovered Apple iPhone 6S was identified as belonging to THOMAS KELLY BROWN as identifying information was located on the phone. This affiant believes the phone was placed on Lake Marvin Road just prior to the search.

In addition, two Apple Id's were associated to the phone, brownthomas786@yahoo.com and tuckerbrown120@yahoo.com. The phone was powered off on November 24, 2016 at 12:23 am and did not have power until November 4, 2017 when the FBI analyzed the phone.

On 3-29-18, PENNY MEEK, BROWN'S mother, was administered a polygraph. PENNY MEEK showed deception regarding having THOMAS BROWNS phone and questions relating to having contact with THOMAS BROWN after his disappearance. In addition, PENNY MEEK showed deception on questions regarding moving THOMAS BROWN'S body.

On 3-29-18, CHRIS MEEK, BROWN'S stepfather, was administered a polygraph. CHRIS MEEK showed deception regarding having THOMAS BROWNS phone and questions relating to having contact with THOMAS BROWN after his disappearance. In addition, CHRIS MEEK showed deception on questions regarding moving THOMAS BROWN'S body.

On 2-13-19, OAG, Certified Forensics Digital Examiners re-analyzed the phone. Examiners found several searches for "Suicide Hotline" on the evening of November 23, 2016.

When PENNY MEEK was first interviewed, the interview was audio and video recorded, by Hemphill County Sheriff's Office four days after THOMAS BROWNS disappearance. PENNY MEEK was asked what she thinks happened to BROWN. PENNY MEEK responded by saying "he committed" suicide" by "playing the choking game". PENNY MEEK had also asked BROWN'S friends for the passcode to BROWN'S phone in January of 2017, after BROWN'S disappearance.

On 1-22-20, SGT. KADING was made aware that there was a witness named KIMBERLY TYSON whom had text messages on her phone she sent to THOMAS BROWN. TYSON shared screenshots of these messages with CHANDRA YOUNG. YOUNG then shared the messages

with SGT. KADING. The messages were sent from TYSON to BROWN, starting November 24, 2016 through October 1, 2017. The messages were blue from November 24, 2016 through December 25, 2016, indicating the messages were iMessages. On January 4, 2017 the messages turned green indicating the messages were now being sent as SMS messages. The last message on October 1, 2017 also showed it had been read. These messages from TYSON do not appear in the data download from BROWN'S phone or in records from Verizon Wireless. It is this affiant's belief that either the sim card was removed from BROWN'S phone and inserted into another phone allowing the person to read text messages, or the messages were being accessed through the iCloud account associated with BROWN'S phone.

Based upon all the foregoing, there is probable cause to believe that evidence and instrumentalities used in the commission of Tampering with or Fabricating Physical Evidence, Texas Penal Code section 37.09, a felony offense are located on the Apple iCloud accounts: **brownthomas786@yahoo.com** and **tuckerbrown120@yahoo.com**, and or associated accounts that are currently stored on the computer servers located with:

**Apple, Inc.  
One Apple Park Way  
Cupertino, CA. 95014**

By nature of Apple, Inc. being a communications provider, it is realized that many other individuals, organizations, businesses, and other entities utilize this company's services and have no association with the subject investigation. These other unnamed individuals, organizations, businesses, and other entities may have various amounts of information maintained in various forms with Apple, Inc. with a reasonable expectation of privacy. It is Affiant's intent that the search conducted at Apple, Inc. be as unobtrusive as possible, and that it relates to the above listed email address associated Tampering with or Fabricating Physical Evidence. Further, it is Affiant's intent to use whatever means or methodology is on hand to conduct this search, with limited or no interruption of the service provided to these other unnamed individuals. It is for these reasons that Affiant requests that Apple, Inc. locate and isolate the above-named information on their servers and make a copy of such information in a readable format to provide to Affiant for review as part of this investigation.

All information noted in this affidavit for search warrant has been related to Affiant by the person(s) and/or source(s) attributed or referenced. Affiant further believes in good faith that the information provided herein to be true and correct. Because the sole purpose of this affidavit is to establish probable cause that a criminal offense has occurred, not every relevant fact known to


Affiant, or to other investigators, is included within. Rather, only those facts necessary to establish probable cause have been discussed.

**WHEREFORE**, Affiant asks for the issuance of a warrant that will authorize the search of said suspected place for said property and seizure of the same and to take custody of all seized property and safe keep such property as provided by statute.

  
AFFIANT,

SUBSCRIBED AND SWORN TO BEFORE ME BY SAID AFFIANT ON THIS THE

5 day of February, A.D., 2020.

  
STEVEN EMMERT, 31ST DISTRICT JUDGE  
HEMPHILL COUNTY, TEXAS

**IN RE: Search Warrant for** )  
)  
Apple, Inc )  
brownthomas786@yahoo.com )  
tuckerbrown120@yahoo.com )  
\_\_\_\_\_ )

**NON-DISCLOSURE ORDER**

Upon the ex parte application of Sergeant Rachel Kading, a commissioned peace officer with the Office of the Attorney General, this Court orders the non-disclosure of the existence of the search warrant to the account holder. The Office of the Attorney General is conducting an active investigation and **brownthomas786@yahoo.com** and **tuckerbrown120@yahoo.com** are related to that investigation. Disclosure to the account holder of the service of this search warrant, at this time, could jeopardize the integrity of the investigation.

**IT IS HEREBY ORDERED** that Apple, Inc not disclose the existence of the attached search warrant pending further order of this Court except that copies may be provided to the office of the 31<sup>st</sup> Judicial District Attorney, and the District Attorney may provide copies to a defendant in a criminal proceeding as part of the criminal discovery process, and;

**IT IS FURTHER ORDERED** that a copy of this non-disclosure order be left at the premises along with the search warrant.

DATED this 5th day of February, 2020.



\_\_\_\_\_  
STEVEN EMMERT, 31<sup>ST</sup> DISTRICT JUDGE  
HEMPHILL COUNTY, TEXAS



**THE STATE OF TEXAS**  
**COUNTY OF HEMPHILL**

§  
§  
§

**SEARCH WARRANT**

To the Sheriff or any Peace Officer of Hemphill County, Texas, or any Peace Officer of the State of Texas:

Whereas, the Affiant whose name appears on the affidavit attached hereto is a Peace Officer under the laws of Texas and did heretofore this day subscribe and swear to said affidavit before me (which said affidavit is here now made a part hereof for all purposes and incorporated herein as if written verbatim within the confines of this Warrant), and whereas I find that the verified facts stated by Affiant in said affidavit show that Affiant has probable cause for the belief he/she expresses herein and establishes the existence of proper grounds for issuance of this Warrant;

Now, therefore, you are commanded to enter the suspected place as described in said affidavit, to-wit:

**Google, Inc.**  
**1600 Amphitheatre Parkway**  
**Mountain View, CA 94043**

At said place you shall search for and, if same be found, seize and bring before me the property described in the affidavit, to-wit:

a. All stored files, maintained by Google, Inc. including but not limited to the server storage space, app data, email contents, contacts, associated accounts, accounts email address has accessed or used to sign up for accounts, subscriber information for

**msskiptracer@gmail.com**

These files may include, but are not limited to: subscriber's full name(s), subscriber's address(es), subscriber's telephone number(s), additional e-mail address(es) associated with the subscriber(s), account or log-in name(s), any other information pertaining to the identity of the subscriber(s), billing information, credit card or payment information, types of services utilized by the subscriber and the lengths of such services or any other identifying or pertinent records relating to the subscriber, including IP addresses, and dates and times of access if available.

b. All business records or files maintained by Google, Inc. belonging to or associated with the customer or individual subscriber/user **msskiptracer@gmail.com**. These records may include, but are not limited to: account application information, credit card or other billing information, account access information, user logon information (including secondary user log on names), account usage reports, e-mail transaction information, text messages, images, news group access and posting information and any other information, both in electronic computer data and written record format, that records the activities of these accounts relating to the subscriber's use of the services offered by Google, Inc.

c. All stored electronic mail (e-mail) or messages (SMS, MMS, or iMessage) of any kind maintained by Google, Inc. that were sent to, from and/or through the accounts of or associated with the customer or individual subscriber/user account utilizing **msskiptracer@gmail.com**.

d. All stored electronic content maintained by Google, Inc. (including Internet history, file transfer protocol logs, text messages, web access logs, electronically stored images, etc.) as well as all connection log files listing all account activity conducted by the subscriber/user associated with the customer or individual subscriber/user account utilizing the username or account name of **msskiptracer@gmail.com** including dates, times, methods of connecting (e.g. telnet, ftp, http, etc.), telephone dial-up connection records and any other connection information or Internet traffic data.

e. Any and all email transactions and/ or file transfer protocol logs maintained by Google, Inc. associated with the screen name or user name of **msskiptracer@gmail.com**

f. Any and all data or images maintained by Google, Inc. associated with the screen name or user name of **msskiptracer@gmail.com** including but not limited to stored photos, documents, contacts, calendars, bookmarks, browsing history, Maps Search History, Messages and device backups

**This Court ORDERS the Google, Inc., 1600 Amphitheatre Parkway, Mountain View, CA, 94043 to collect all data, as previously outlined within this warrant, and to disclose responsive data, if any, by sending such to SGT. RACHEL KADING located at 300 West 15<sup>th</sup> Street, Austin, TX 78701 using the U.S. Postal Service or another courier service, an online records portal, or other acceptable means of electronic delivery, to [rachel.kading@oag.texas.gov](mailto:rachel.kading@oag.texas.gov) notwithstanding 18 U.S.C. 2252A or similar statute or code, where all received data will be analyzed.**

Further, Affiant is **ORDERED**, pursuant to the provisions of Article 18.10, Texas Code of Criminal Procedure, to retain custody of any property seized pursuant to this Warrant, until further order of this Court or any other court of appropriate jurisdiction shall otherwise direct the manner of safekeeping of said property. This Court grants you leave and authority to remove such seized property from this county, if and only if such removal is necessary for the safekeeping of such seized property by Affiant, or if the provisions of Article 18.10, T.C.C.P. otherwise authorize such removal. Affiant is further **ORDERED** to give notice to this Court, as a part of the inventory to be filed subsequent to the execution of this Warrant, and as required by Article 18.10, T.C.C.P., of the place where the property seized hereunder is kept, stored and held.

Herein fail not but have you then and there this warrant within ten days, exclusive of the day of its execution, with your return thereon, showing how you executed the same.

ISSUED THIS THE 5th day of February, A.D., 2020, at 11:35 o'clock A.M. to certify which, witness my hand this day.



---

**STEVEN EMMERT, 31<sup>ST</sup> DISTRICT JUDGE  
HEMPHILL COUNTY, TEXAS**

**THE STATE OF TEXAS**  
**COUNTY OF HEMPHILL**

§  
§  
§

**AFFIDAVIT FOR SEARCH WARRANT**

**BEFORE ME, THE UNDERSIGNED AUTHORITY, PERSONALLY APPEARED THE AFFIANT HEREIN, A PEACE OFFICER UNDER THE LAWS OF TEXAS, WHO, BEING DULY SWORN, ON OATH MADE THE FOLLOWING STATEMENTS:**

My name is Sgt. Rachel Kading and the Office of Attorney General of Texas commissions me as a Texas peace officer.

1. **There is in Mountain View, California, a Communications Service Provider known as Google, Inc. located at 1600 Amphitheatre Parkway, Mountain View, CA 94043.**

This Company, in its capacity as an Internet service/company, provides access to a worldwide computer network, commonly known as the Internet, to individuals and/or other users who have a subscription to, membership with, or affiliation with their company, organization or commercial service. Google, Inc. also provides web hosting and access solutions to its customers in which they reserve and/or maintain computer disk storage space on their own computer system servers for the use of the Internet subscribers/customers/users associated with their company. Items contained on the previously mentioned storage space can include electronic communications (commonly known as e-mail) between subscriber(s) and other parties, graphic image and/or text files, Internet history or internet hyperlinks, file transfer protocol logs, website access logs, programs and other types of data or information stored in electronic form(s). Internet Service Companies, such as Google, Inc., also maintain records pertaining to the individual's and/or other users who have subscriber accounts with their company. This information can include registration information, account application information, credit card or other billing information, account access information, user logon information (including secondary user log on names), account usage reports, e-mail transaction information, news group access and posting information and other information both in computer data and written record format that records the activities of these accounts relating to the subscriber's use of the services offered by the Internet Service Provider. Said suspected place and premises are in charge of and controlled by each of the following:

**Google, Inc.**  
**1600 Amphitheatre Parkway**  
**Mountain View, CA 94043**

2. **There is at said suspected place and premises the following item(s) which are implements or instruments used in the commission of a crime and, or item(s) constituting evidence of a criminal offense or constituting evidence tending to show that a particular person committed a criminal offense: Texas Penal Code 37.09 Tampering with or Fabricating Physical Evidence, a felony offense.**

a. All stored files, maintained by Google, Inc. including but not limited to the server storage space, app data, device settings, home screen app organization, iMessage, text (sms), MMS messages, photos, videos, purchase history, device ids associated to the named subscriber, ip logs where accessed, associated accounts, subscriber/user account:

**msskiptracer@gmail.com**

These files may include, but are not limited to: subscriber's full name(s), subscriber's address(es), subscriber's telephone number(s), e-mail address(es) associated with the subscriber(s), account or log-in name(s), any other information pertaining to the identity of the subscriber(s), billing information, credit card or payment information, types of services utilized by the subscriber and the lengths of such services or any other identifying or pertinent records relating to the subscriber, including IP addresses, and dates and times of access if available.

b. All business records or files maintained by Google, Inc. belonging to or associated with the customer or individual subscriber/user **msskiptracer@gmail.com**. These records may include, but are not limited to: account application information, credit card or other billing information, account access information, user logon information (including secondary user log on names), account usage reports, e-mail transaction information, text messages, images, news group access and posting information and any other information, both in electronic computer data and written record format, that records the activities of these accounts relating to the subscriber's use of the services offered by Google, Inc.

c. All stored electronic mail (e-mail) or messages (SMS, MMS, or iMessage) of any kind maintained by Google, Inc. that were sent to, from and/or through the accounts of or associated with the customer or individual subscriber/user account utilizing **msskiptracer@gmail.com**.

d. All stored electronic content maintained by Google, Inc. (including Internet history, file transfer protocol logs, text messages, web access logs, electronically stored images, etc.) as well as all connection log files listing all account activity conducted by the subscriber/user associated with the customer or individual subscriber/user account utilizing the username or account name of **msskiptracer@gmail.com** including dates, times, methods of connecting (e.g. telnet, ftp, http, etc.), telephone dial-up connection records and any other connection information or Internet traffic data.

e. Any and all email transactions and/ or file transfer protocol logs maintained by Google, Inc. associated with the screen name or user name of **msskiptracer@gmail.com**.

f. Any and all data or images maintained by Google, Inc. associated with the screen name or user name of **msskiptracer@gmail.com** including but not limited to stored photos, documents, contacts, calendars, bookmarks, browsing history, Maps Search History, Messages and device backups.

**3. It is the belief of the Affiant, that: The email account of msskiptracer@gmail.com contains evidence of the Texas Penal Code 37.09 Tampering with or Fabricating Physical Evidence, a felony offense.**

**4. AFFIANT HAS PROBABLE CAUSE FOR THE SAID BELIEF BY REASON OF THE FOLLOWING FACTS, TO WIT:**

Your Affiant is Rachel Kading, a peace officer certified by The State of Texas, who is currently employed as a Sergeant with the Office of the Texas Attorney General (OAG). Affiant has been a law enforcement officer for over 16 years. Affiant is currently assigned to the Criminal Investigation Division, Special Investigations Unit, where her duties include investigations involving a wide array of criminal offences ranging from simple fraud to homicides. Affiant has specialized training in the areas of criminal investigations, child abuse and exploitation, narcotics and financial crimes, provided by federal, state, and local agencies. Affiant has previously been involved in the execution of search warrants involving persons crimes and narcotics.

On January 26, 2018, Hemphill County Sherriff, NATHAN LEWIS, formally asked the Texas Attorney General's Office to assist in the investigation into the disappearance of THOMAS KELLY BROWN, who was last seen on 11-23-16 in Canadian, Texas. On January 9, 2019, THOMAS BROWN'S remains were located near Lake Marvin in Hemphill County, Texas. A cause or manner of death has not yet been determined. This is an ongoing open investigation.

On 1-17-20 unknown persons sent TUCKER BROWN, BROWN'S brother, a message that said "Hey buddy I can't keep it a secret any longer. The truth is gonna come out." The message came from 806-601-0029. CLAUDIA GONZALES, OAG Crime Analyst, determined the number belonged to Bandwidth Communications. Bandwidth Communications is a voice over internet provider, not a cell phone provider. On 1-21-20 TUCKER BROWN received another text that stated, "we are done it's time".

This affiant sent Bandwidth Communications an exigent request for subscriber information based on evidence retention. This affiant sent a subsequent subpoena on 1-21-20. Bandwidth Communications sent a response indicating the number was assigned to an app called Pinger. Pinger is an app that provides a spoof number to make calls and send text messages. This affiant requested a subpoena for Pinger to obtain subscriber information and it was served on 1-21-20. This affiant received a response from PINGER identifying the customers utilizing 806-601-0029. There were three emails identified, however only one of them utilized the service on 1-17-20 and 1-20-20. This account was registered under **msskiptracer@gmail.com**.

This affiant believes this email address belongs to MICHELLE GOMEZ. GOMEZ is a private investigator (not retained by the family) whom believes TUCKER BROWN is a suspect in the death of THOMAS BROWN. This affiant believes the text messages were sent to illicit a response from TUCKER BROWN. The sender fabricated physical evidence in the case sending the messages anonymously, creating the illusion the messages were coming from someone whom has knowledge of THOMAS BROWN'S death, and TUCKER BROWN'S involvement.

Based upon all the foregoing, there is probable cause to believe that evidence and instrumentalities used in the commission of Tampering with or Fabricating Physical Evidence, Texas Penal Code section 37.09, a felony offense are located on the Google, Inc account: **msskiptracer@gmail.com**, and or associated accounts that are currently stored on the computer servers located with:


**Google, Inc.  
1600 Amphitheatre Parkway  
Mountain View, CA 94043**

By nature of Google, Inc. being a communications provider, it is realized that many other individuals, organizations, businesses, and other entities utilize this company's services and have no association with the subject investigation. These other unnamed individuals, organizations, businesses, and other entities may have various amounts of information maintained in various forms with Google, Inc. with a reasonable expectation of privacy. It is Affiant's intent that the search conducted at Google, Inc. be as unobtrusive as possible, and that it relates to the above listed email address associated Tampering with or Fabricating Physical Evidence. Further, it is Affiant's intent to use whatever means or methodology is on hand to conduct this search, with limited or no interruption of the service provided to these other unnamed individuals. It is for


these reasons that Affiant requests that Google, Inc. locate and isolate the above-named information on their servers and make a copy of such information in a readable format to provide to Affiant for review as part of this investigation.

All information noted in this affidavit for search warrant has been related to Affiant by the person(s) and/or source(s) attributed or referenced. Affiant further believes in good faith that the information provided herein to be true and correct. Because the sole purpose of this affidavit is to establish probable cause that a criminal offense has occurred, not every relevant fact known to Affiant, or to other investigators, is included within. Rather, only those facts necessary to establish probable cause have been discussed.

**WHEREFORE**, Affiant asks for the issuance of a warrant that will authorize the search of said suspected place for said property and seizure of the same and to take custody of all seized property and safe keep such property as provided by statute.

  
AFFIANT,

SUBSCRIBED AND SWORN TO BEFORE ME BY SAID AFFIANT ON THIS THE  
5 day of February, A.D., 2020.

  
\_\_\_\_\_  
**STEVEN EMMERT, 31<sup>ST</sup> DISTRICT JUDGE**  
**HEMPHILL COUNTY, TEXAS**



Google Search Warrant

**IN RE: Search Warrant for** )  
 )  
**Google, Inc** )  
**msskiptracer@gmail.com** )  
\_\_\_\_\_ )

**NON-DISCLOSURE ORDER**

Upon the ex parte application of Sergeant Rachel Kading, a commissioned peace officer with the Office of the Attorney General, this Court orders the non-disclosure of the existence of the search warrant to the account holder. The Office of the Attorney General is conducting an active investigation and **msskiptracer@gmail.com** is related to that investigation. Disclosure to the account holder of the service of this search warrant, at this time, could jeopardize the integrity of the investigation.

**IT IS HEREBY ORDERED** that Apple, Inc not disclose the existence of the attached search warrant pending further order of this Court except that copies may be provided to the office of the 31<sup>st</sup> Judicial District Attorney, and the District Attorney may provide copies to a defendant in a criminal proceeding as part of the criminal discovery process, and;

**IT IS FURTHER ORDERED** that a copy of this non-disclosure order be left at the premises along with the search warrant.

DATED this 5th day of February, 2020.



\_\_\_\_\_  
STEVEN EMMERT, 31<sup>ST</sup> DISTRICT JUDGE  
HEMPHILL COUNTY, TEXAS