|  |  |  |
| --- | --- | --- |
| IN THE CIRCUIT COURT OF {{COUNTY|upper }} COUNTY, MISSOURI | | |
|  | )  )  )  )  ) | Sikeston DPS: {{ CASE }} |
| STATE OF MISSOURI  COUNTY OF {{COUNTY|upper }} |
|  |  |  |
| **AFFIDAVIT AND APPLICATION FOR A SEARCH WARRANT** | | |

**INTRODUCTION AND AGENT BACKGROUND**

1. I, {{ NAME|title }}, knowing that false statements are punishable by law, hereby affirm and state that the facts contained herein are true to the best of my information and belief. Based on the following information, I hereby request the Court find probable cause and make this Affidavit in support of the issuance of a Search Warrant.
2. I am a {{ RANK|title }} with the {{ AGENCY }}, located in the County of {{ COUNTY|title }}, State of Missouri. I am a “Peace Officer” as defined in RSMO § 542.261. I have been employed as a peace officer for more than {{ YEARS }} years. I have training pertaining to the investigation of criminal offenses and as part of my regular duties, I have previously participated in the investigation of various criminal offenses, including the offense which is currently under investigation and is the subject of this Affidavit.
3. I have been assigned to investigate a {{CRIME|title}}, a violation of RSMO § {{RSMO}}. The incident occurred in {{COUNTY|title}} County on or about {{MONTH|title}} {{DAY}}, {{YEAR}}.

**PERSON, PLACE, OR THING TO BE SEARCHED**

See Attachment "A"

**ITEMS TO BE SEARCHED AND SEIZED**

See Attachment "B"

**STATEMENT OF PROBABLE CAUSE**

1. {Type your probable cause statement here. Remember that you have to establish probable cause for what you want to search and also establish that it’s probable that the evidence you wish to search for will be at that location.}

{%p **if** CSAM%}

**CHILD SEXUAL ABUSE MATERIAL**

1. Based upon my knowledge, experience, and training in child exploitation and child sexual abuse material investigations, and the training and experience of other law enforcement officers with whom I have had discussions, I know there are certain characteristics common to individuals involved in the receipt, distribution, and collection of child sexual abuse material. Child sexual abuse material collectors may receive sexual gratification, stimulation, and satisfaction from contact with children or from fantasies they may have viewing children engaged in sexual activity or in sexually suggestive poses.
2. This satisfaction may come from viewing children in person, in photographs, other visual media, or from literature describing such activity. Collectors of child sexual abuse material often collect sexually explicit or suggestive materials in a variety of media including photographs, magazines, motion pictures, videotapes, books, drawings or other visual media. Child sexual abuse material collectors not only use these materials for their own sexual arousal and gratification, they have been known to use these materials to lower the inhibitions of children they are attempting to seduce, to arouse the selected child partner, or to demonstrate the desired sexual acts.
3. Child sexual abuse material collectors typically retain pictures, films, photographs, negatives, magazines, correspondence, books, tape recordings, mailing lists, child erotica, and videotapes for many years. Due to it’s illegal nature, child sexual abuse material is a scarce resource that collectors are reluctant to delete or destroy. As such, collectors of child sexual abuse material often maintain their collections in a digital or electronic format in a safe, secure and private environment. These collections are often maintained for several years and are kept close by, usually at the collector’s residence, to enable the collector to view the collection, which is valued highly.
4. Child sexual abuse material collectors also may correspond with and/or meet others to share information and materials. Once a child sexual abuse material collector makes a connection with another, these relationships are highly coveted. Child sexual abuse material collectors rarely destroy correspondence from other child sexual abuse material distributors or collectors and will often conceal such correspondence as they do their sexually explicit material. They will often maintain lists of names, addresses and email addresses, and telephone numbers, and usernames of individuals with whom they have been in contact and who share the same interests in child sexual abuse material.
5. Collectors of child sexual abuse material prefer not to be without their child sexual abuse material for any prolonged time period. This behavior has been documented by law enforcement officers involved in the investigation of child sexual abuse material throughout the world.
6. Based on the details of this investigation outlined in this affidavit, I believe that the person(s) described in the attachment to this search warrant exhibits the common characteristics described above of someone involved in the distribution, receipt, possession or collection of child sexual abuse material.

{%p endif %}

{%p **if** GANG%}

**GANG CRIMES**

1. Based upon my knowledge, experience, and training in gang investigations, and the training and experience of other law enforcement officers with whom I have had discussions, I know there are certain characteristics, traits, and methodologies common among gangs and gang members. I know that criminal street gangs are generally defined as an ongoing organization of three or more persons with a common name, or identifying mark or symbol, having as one of its primary activities the commission of specified crimes, and whose members individually or collectively engage in criminal activity. It is my experience that most street gang members are known by street names or monikers to their fellow gang members, and that they frequently write their names or monikers of their associates on walls, furniture, miscellaneous items or papers, both within and on their residences and within and on their vehicles. I know that gang members also identify themselves with colors, identifying marks, or symbols. These colors, identifying marks, or symbols are used by gang members to readily identify each other or identify unknown members from different areas. The symbols used by gangs are often commonly found symbols such as sports team logos, product logos, or hand signs which indicate gang identity or affiliation. I am also aware that gang members often possess written documents related to gang membership. These documents often include information about gang membership such as a gang roster of members, monikers, and graffiti regarding the writer's gang. Quite often gang members keep written correspondence directed to or received from gang members in-custody intended to keep members appraised of what is going on with the gang and its enemies and allies.
2. I know that respect is paramount within the gang culture and that gang members often earn respect through the commission of violent crimes. Members of a gang viewed with the highest levels of respect often become "shot callers" within the gang and are responsible for giving direction to the gangs membership. I am aware that in the gang culture if members of the gang are engaged in criminal activity, all present gang members must remain present and aid in the commission of that crime. If a gang member were to leave the area or flee from the commission of the crime, they would be considered a coward. Assistance in the commission of the crime could be limited to remaining on scene and providing protection or acting as a look-out. Their mere presence adds to the intimidation of the persons attempting to come to the aid of the victim. If an active member of the gang were not to take part in the robbery in some manner, they would lose respect amongst the gang.

{%p endif %}

{%p **if** NARCOTICS%}

**INFORMATION SPECIFIC TO DRUG CRIMES**

1. I know from training and experience that purveyors (suppliers) of illegal drugs often use computers, cell phones, and cameras to facilitate drug transactions, keep records, tally sheets, names, phone numbers and/or addresses of associates who are aficionados (supporters). I know from training and experience that purveyors of illegal drugs are often in possession of firearms which are used to help protect their narcotics and proceeds from narcotics. Further, I know from training and experience that purveyors of illegal drugs often accept goods and/or services in lieu of currency in exchange for drugs and that often times the goods have been reported as stolen.
2. With this training and experience, I am familiar with the operations, habits, workings and parlance (a particular way of speaking when specialized) of persons engaged in narcotic trafficking activities and organizations, including the frequent use of “slang” or coded language used to disguise, and covertly communicate about illegal drug transactions.
3. As a result my training and experience, the following generalities about drug dealers are known:
4. Drug dealers often place assets in names other than their own to avoid detection of these assets by government agencies, but continue to use those assets and to exercise dominion and control over them. Drug dealers frequently maintain, on hand, quantities of United States currency in order to maintain and finance their on-going drug businesses.
5. Drug dealers maintain books, records, receipts, notes, ledgers, tally sheets, and other annotations relating to the quantity, transportation, ordering, sale, and distribution of controlled substances, although such language may be coded and such documents may be prepared in or contain code, and commonly maintain such where the drug dealers have ready access to them, such as their homes, offices, cellular phones or other electronic storage device, or automobiles, and such are often maintained for a period of time extending beyond the time during which they actually possess illegal controlled substances in order to keep track of drug transactions, monetary transactions, drug sources and drug customers for future reference.
6. Drug dealers commonly secrete drugs, evidence of financial transactions relating to obtaining, transferring, secreting, or spending of the proceeds of their engaging in drug dealing activities, and proceeds of drug sales, including caches of currency, financial instruments, precious metals, jewelry, and other items of value, in secure locations within residences, offices, garages, businesses, automobiles, public or private storage facilities, and safe deposit boxes, for ready access and also to conceal such items from law enforcement authorities.
7. Drug dealers commonly maintain addresses or telephone numbers in books, papers, electronic storage devices, as well as stored within their telephones, which reflect names, addresses, and/or telephone numbers for their associates in the drug distribution organization, although said items may be in code.
8. Drug dealers must use telephones and other forms of communication such as pagers, text messages or e-mail messages, to keep in frequent communication with their criminal associates, including their suppliers and customers; when drug dealers entrust a customer or associate with a method of contact, for example a telephone number, this indicates that the drug dealer feels safe using that method of contact and in all probability discusses his/her criminal activities with others through the same facility.
9. Drug dealers frequently take or cause to be taken photographs or video recordings of themselves, their associates, their property, and their product, and maintain these photographs or video recordings in their residences, automobiles and/or contained in electronic storage devices including capable cellular telephones.
10. Drug dealers keep equipment or paraphernalia for manufacturing, packaging, diluting, weighing, and distributing controlled substances, such as chemicals, syringes, prescription bottles, plastic bags, cooking containers, scales which read in grams, and heat sealers for use in sealing plastic bags containing drugs; Drug dealers also keep certain types of drug paraphernalia used in abusing drugs on an essentially continuous basis for use whenever needed.
11. Upper level drug dealers may obtain large quantities of their illegal controlled substances from foreign countries and/or foreign nationals, and drug dealers involved in smuggling operations commonly possess documents such as telephone records, visas, passports, letters, shipping receipts, wire transfer receipts, and so forth, which pertain to the obtaining, shipment, transportation, or payment for the illegal substances.
12. Drug dealers frequently continue their illegal activity over months and even years. Drug dealers typically obtain and distribute controlled substances on a regular basis, much as any distributor of a legitimate commodity would purchase stock for sale. Similarly such drug dealers will have an “inventory” which will fluctuate in size, depending upon the supply and demand for the product.
13. Drug dealers commonly “front” drugs (provide controlled substances on consignment) to their clients. As well, drug dealers often employ individuals to perform controlled substances pick-ups, deliveries and/or hand to hand transactions as a way to insulate the drug dealer from other individuals and from potential prosecution.

{%p endif %}

{%p **if** CELL\_PHONE%}

**MOBILE DEVICES**

1. I know from my training and experience that mobile devices, including cellular telephones and tablet computers, commonly contain live and deleted user attribution data including, but not limited to, user accounts, e-mail accounts, passwords, PIN codes, patterns, account names, user names, screen names, remote data storage accounts, documents, files, pictures, videos, metadata, or other information and evidence that may demonstrate attribution to a particular user or users.
2. I know from my training and experience that mobile devices can be connected to a cellular network (Mobile Network Operator) or to the Internet via Wi-Fi. This connectivity allows users to make and receive calls, send and receive text messages, take and send pictures and videos, communicate using third party applications “apps”, access social media, navigate using mapping and navigation apps and access the World Wide Web. I know that videos and images can be e-mailed, sent through messaging systems such as SMS (Short Message Service) and MMS (Multi-media Message Service) messages and other forms of communication located within specialized applications. I know when mobile devices are examined it is common to identify e-mail addresses and other on-line account details which could contain evidence of distribution of images, videos, text communication, file sharing, and remote cloud storage. I also know that metadata associated with these images and videos may include details such as the camera used, date and time the image or video were recorded, and GPS location information.
3. I know from my training and experience that mobile device users can install applications that can be used to hide and even encrypt data and conceal specific data from detection. These applications are generally accessed by covert means known by the user and often require a PIN code, pattern, password, or a unique biometric feature such as a fingerprint. I also know that users sometimes hide contraband images and other content in other applications and folders such as calendars and games as a way to avoid detection. For these reasons, I know it is necessary to search all data on the device.
4. I also know based on my training and experience that people using mobile devices commonly keep contact lists containing names and phone numbers. I know these names and numbers can be useful in identifying possible victims, associates, suspects, co-conspirators, and other relevant individuals.
5. I know based on my training and experience that mobile devices commonly have Global Positioning System (GPS) and other similar geo-location sensors. These sensors may track the historical location of the device geographically and provide a historical record. I also know that these systems leave log files. I know that these log files can be recovered and used to locate a device’s geographic historical location on a specific date and time. I know that this information could be used to include or exclude the user from involvement with the planning, execution, and potential post crime cover-up activities.
6. I know that some mobile devices may contain a Subscriber Identity Module (SIM cards) that may contain data associated with the device and user attribution such as contact lists, call logs, SMS messages, telephone number, and other user data commonly found in cellular telephones. This data can be recovered forensically.
7. I also know that some mobile devices may contain removable media cards. These cards are commonly referred to as SD cards or MicroSD cards. These cards can be used to store additional data associated with the mobile device including photographic images, videos, text files and other digital data. I know that additional data contained within these files may also provide dates, times, locations, settings, devices used, and user attribution information. This data can be recovered forensically.
8. I know that these mobile devices can be used to delete, create, share, and store files and other data including, but not limited to, documents, photographs, videos, electronic mail, search history, financial transactions and other relevant live and deleted user information. I also know that such devices can be used to communicate and instantly share information with others and that data can be transferred between various devices – wirelessly and by connected cables.
9. I also know that if these items are not seized and isolated from network connectivity in a timely manner, potential inculpatory and exculpatory evidence may be destroyed, transferred, encrypted, modified, or otherwise lost forever. I know that data recovered from mobile devices can be used to corroborate or refute data recovered or obtained from other mobile devices and/or from service provider records.
10. I know from my training and experience, and from information provided to me by other investigatorsthat it is necessary to search live and deleted data recovered from digital devices from the time when the device was first used through the time when the device was seized. This is specifically necessary to establish associations between a particular device and associated applications and files to a particular user (or users). This scope of time is necessary to identify potential inculpatory and exculpatory evidence during the planning, execution and post event activities of potential criminal activity. These activities may include communication, contact, calendar entries, pictures, videos, and location information (including GPS, navigation, and maps). This scope of time is also necessary to determine accurate device date and time settings, including time zone changes, and to determine if the date and time settings are correct and if they are set to synch or not synch with the network. I know from my training and experience that it is important to understand events of a particular day and time in proper context that may exist months before certain criminal acts and to attribute particular users of a device and associated applications when the device was initially setup.

{%p endif %}

{%p **if** INFO %}

**BACKGROUND AND EXPLANATION OF VEHICLE INFOTAINMENT SYSTEMS**

1. Modern vehicles hold a vast amount of data that can be used to uncover critical information during an investigation and help determine what happened, where it occurred, and who was involved. Modern vehicles are complex networks of highly integrated electronic systems that generate and store massive amounts of information. A typical vehicle has more than 75 computer systems that are constantly collecting performance metrics, monitoring sensor data, scanning external environmental conditions, processing telemetry data, and communicating with other vehicles and infrastructure. As such, the vehicle can typically generate approximately 25GB worth of data per hour.
2. This data is stored by vehicle systems as it is collected and processed. Vehicle Event data can include event logs associated with activity such as door opens, gear shifts, odometer reads, ignition cycles, speed logs, and more. Location data and navigation information such as track logs, saved locations, active routes and previous destinations is commonly stored in these systems. These vehicle systems also collect data that can be used to identify devices such as mobile phones that have been connected via the USB ports, over Bluetooth or wireless network and may contain significant data from those devices such a contacts, text messages, and photos or videos.
3. Vehicle Infotainment Systems are a combination of the vehicle systems described above which are used to deliver entertainment and information to the driver and the passengers through audio/video interfaces, control elements like touch screen displays, button panel, voice commands, and more. Each infotainment system is comprised of several key components. The Integrated Head-Unit is the primary way to interact with the infotainment system and is often a touch screen based, tablet-like device, mounted on the vehicle's dashboard. Some high-end infotainment systems have a Heads-Up Display feature that displays the vehicle's real-time information on the transparent screen integrated with the vehicle's windshield. Heads-up display helps in reducing the driver's distraction while driving and assists him with key details like speed, navigation maps, electronic digital cluster information, climate, and multimedia options. A recent innovation in modern vehicles are their integration with the driver's smartphone such as Apple's CarPlay system.
4. This allows the driver to integrate and control their iPhone using the vehicles interface and voice commands. Additionally, newer vehicles are equipped with optional Wi-Fi hotspots allowing passenger's to connect their smartphones to the vehicle to browse the internet using the vehicle's LTE mobile data connection as well as information related to hands-free cellular telephone support and operation, vehicle navigation (trackpoints/track logs, locations, routes), vehicle radio and media streaming functions, Bluetooth operation, internet connectivity, event logs such as (vehicle lighting condition/operation, odometer reading, gear shifts, door operation) and more
5. Event Data Recorders (EDR) are a part of the vehicle Airbag Control Module (ACM) and, in combination with the Powertrain Control Module (PCM) and Telematics/Infotainment System data, create a comprehensive set of records of the vehicle and occupant's activity . The ACM is responsible for analyzing real-time driving conditions and other related variables to perform necessary safety measures in protecting occupants of the vehicle. These safety measures include decisions on whether or not to activate the vehicle's supplemental inflatable restraints such as the driver and or passenger airbags, and or seatbelt pretensioners. In addition, the ACM communicates with and records data from internal and external sensors that provide data related to the collision to include possibly: engine revolutions per minute (RPM); throttle position; brake switch status; and pre-collision vehicle speed.
6. Certain Telematics/Infotainment systems from specific vehicle manufacturers can be imaged and the data extricated for analysis that could be helpful to investigators in reconstructing incidents and determining pre-incident vehicle condition and potential distractions. At the time of this investigation, the Sikeston Department of Public Safety has access to the software and hardware needed to image the ACM and the Telematics/Infotainment system.

{%p endif %}

1. I have read this affidavit and the facts contained in here are the truth to the best of my knowledge.

\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_   
(Signature of Affiant)

{{ RANK|title }} {{ NAME|title }}

{{ AGENCY }}

DATE: {{ TODAY }}   
TIME:

I have reviewed this Affidavit and Application and hereby apply for a search warrant based upon this Affidavit and place my signature upon this Application.

\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_   
(Signature of Prosecuting Attorney)

DATE:

TIME:

Witness my hand and the seal of this Court on {{ TODAY }}.

\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_   
(Signature of Judge)

DATE:

TIME:

|  |  |  |
| --- | --- | --- |
| IN THE CIRCUIT COURT OF {{COUNTY|upper }} COUNTY, MISSOURI | | |
|  | )  )  )  )  ) | Sikeston DPS: {{ CASE }} |
| STATE OF MISSOURI  COUNTY OF {{COUNTY|upper }} |
|  |  |  |
| **SEARCH WARRANT** | | |

**THE STATE OF MISSOURI TO ANY PEACE OFFICER IN THE STATE:**

**WHEREAS**, proof having been made before me by {{ RANK|title }} {{ NAME|title }}, the Judge of this Court has found probable cause to believe the allegations of the complaint to be true and that there is probable cause to believe that evidence pertaining to {{CRIME|title}}, a violation of RSMO § {{RSMO}} is presently located at the location(s) described herein.

**YOU ARE COMMANDED TO SEARCH THE FOLLOWING LOCATION(s):**

See Attachment "A"

**FOR THE FOLLOWING PROPERTY OR PERSON(s):**

See Attachment "B"

**NOW, THEREFORE**, you are directed to execute this search warrant, to seize, photograph, or copy the property, article, substance, or person found thereon or therein, and make return of this warrant to this court within ten (10) days after filing.

Witness my hand and the seal of this Court on {{ TODAY }} at \_\_\_\_\_\_\_\_\_ AM / PM.

\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

Circuit / Associate Circuit Judge

TIME:

**ATTACHMENT "A"**

**TO MAKE A SEARCH:**

{%p **if** DNA %}

{{ SUS\_NAME|title}}

{{ SUS\_DOB }}

{{ SUS\_SOC }}

This person is believed to be currently located at the following address:

{{ SUS\_ADDRESS }}, {{ SUS\_CITY|title }}, {{ SUS\_STATE|title }}

{%p endif %}

{%p **if** CELL\_PHONE %}

Items that are the subject of this warrant are currently stored at the secure Property/Evidence facility of the {{ AGENCY }} in {{ COUNTY|title }} County, Missouri. The devices to be searched are particularly described as:

1. One each, {{ BRAND }} brand, model {{ MODEL }}, {{ OS }} cellular telephone, {{ PHONE\_COLOR }} in color, bearing identifying number {{ IMEI}}, sealed in an evidence envelope {{ AGENCY }} labeled with Case Number {{ CASE }} and Evidence Item number {{ ITEM\_NUMBER }};

{%p endif %}

{%p **if** RESIDENTIAL %}

{{STREET|title}}, {{CITY|title}}, {{STATE|title}} {{ZIP}}

{{DESCRIPTION}}

The search is to include all rooms, attics, basements, and all other parts therein as well as the surrounding grounds or curtilage, storage rooms, or outbuildings of any kind located on the premises. The search will include all persons that may be contacted and are present at the time of the search warrant. The search will also include all vehicles in the immediate vicinity of the Subject Premises that can be connected to the property by one of more of the following: paperwork, registration, keys and/or verbal claim of ownership by residents at the involved location. {{ RANK|title }} {{ NAME|title }} and/or those under their direction are authorized during the execution of this search warrant to video tape, photograph, take digital images such as 3-D mapping images, and collect any measurements of physical items within the location at the discretion of the searching officers both inside and outside of the location. These images or recordings may include any and all items, vehicles at the location, and all persons present at the location during the period of execution of this search warrant.

{%p endif %}

{%p **if** VEHICLE %}

{{ VEH\_YEAR }} {{ VEH\_MAKE }} {{ VEH\_MODEL }}   
Plate: {{ LIC\_PLATE }}   
VIN: {{ VIN }}   
Color: {{ VEH\_COLOR }}

{%p endif %}

{%p **if** INFO %}

{{ VEH\_YEAR }} {{ VEH\_MAKE }} {{ VEH\_MODEL }}   
Plate: {{ LIC\_PLATE }}   
VIN: {{ VIN }}   
Color: {{ VEH\_COLOR }}

{%p endif %}

**End of Attachment "A"**

**ATTACHMENT "B"**

{%p **if** VEHICLE %}

{{ VEH\_YEAR }} {{ VEH\_MAKE }} {{ VEH\_MODEL }}   
Plate: {{ LIC\_PLATE }}   
VIN: {{ VIN }}   
Color: {{ VEH\_COLOR }}

{%p endif %}

{%p **if** INFO %}

{{ VEH\_YEAR }} {{ VEH\_MAKE }} {{ VEH\_MODEL }}   
Plate: {{ LIC\_PLATE }}   
VIN: {{ VIN }}   
Color: {{ VEH\_COLOR }}

{%p endif %}

{%p **if** residential %}

{{STREET|title}}, {{CITY|title}}, {{STATE|title}} {{ZIP}}

{%p endif %}

**FOR THE FOLLOWING PROPERTY:**

{If you selected specialized language, some items may show up for you here. If not, you’ll have to manually list what you wish to search for. It’s important to note that you need to be particular. If something is there and you don’t need it, remove it. If you add things, make sure you’re particular enough in describing them not to be seen as overbroad. REMOVE THIS PART BEFORE SUBMISSION}

{%p **if** INFO %}

**Associated Devices:** Currently stored data originating from previously associated mobile devices, such as mobile phones, to include content that would tend to identify a particular occupant such as mobile device identifiers, telephone numbers, user accounts details, methods of payment, passwords, PIN codes, user voice profiles and other biometric identifiers, contact lists, call logs, text messages, e-mails, pictures, videos, web history, telephone numbers, addresses and/or GPS (Global Positioning System) coordinates, and other historical navigation information.

**Communication Information:** Live and deleted contact lists, call logs, text messages and multimedia messages (SMS and MMS messages), e-mails, chats, video call communication data, contact information, installed application information including their content and any other information which can be used to identify potentially associated persons.

**Historical Event Data:** Live and deleted historical event data such as when the headlights were turned on or off, when doors were opened or closed, when gears were changed, when breaks were applied, and when connections or disconnections were made to other devices such as Bluetooth, USB, media cards, and Wi-Fi.

**Historical Navigation Data:** Live and deleted historical navigation data tracks, routes, and waypoints, GPS fixes, favorites, past journeys, trip logs, and user entered data, Latitude, Longitude, and Altitude coordinates, and related dates and times.

**Internet Activity:** Live and deleted web browser history, web browser bookmarks, temporary Internet files, cookies, searched items, downloaded and uploaded files, social networking websites or applications, and access to data streaming stream services such as music, news, weather, maps, navigation, traffic data, and other web-based information and related content.

**Pairing Records:** All recovered data showing both successful, unsuccessful, or attempted pairing of devices to include information related to the specific devices such as associated device and and telephone number, the dates and times of the pairing events, and recording indicating what data was synced to the vehicle.

**Stored Files:** Live and deleted documents, programs, pictures, videos, audio files, text files, databases, application data, calendar entries, user dictionaries, tracking or other remote monitoring software, and any associated metadata.

**User Attribution Data:** Live and deleted user attribution data including, but not limited to, user accounts, e-mail accounts, passwords, PIN codes, passcode patterns, methods of payment, account names, user names, screen names, remote data storage accounts, documents, files, metadata, log files, user voice profiles and other biometric identifiers or any other information and evidence that may demonstrate attribution to a particular user or users.

{%p endif %}

{%p **if** DNA %}

Two (2) buccal swabs from {{ SUS\_NAME|title }} for the purposes of obtaining a sample of their DNA.

The requested evidence is relevant to this investigation in that the buccal swabs would be used for comparison purposes to any biological evidence associated with the investigation of this case. This evidence could also serve to exclude this individual as the source of any biological evidence.

A buccal swab is a minimally invasive procedure where a sterile cotton swab is rubbed against the interior of the subject’s mouth, specifically the swab is to be rubbed around the cheek and gum area inside of the mouth.

{%p endif %}

{%p **if** GANG %}

**Gang Indicia:** Any evidence of street gang membership, or affiliation with any street gang, such as any paraphernalia making any reference to the gang. Items such as any audio and/or video tapes making reference to any criminal street gang, and/or any drawings, miscellaneous writings, objects, and/or graffiti depicting gang members’ names, initials, logos, monikers, slogans, and/or containing mention of street gang membership affiliation, activity, and/or identity, as it is your Affiant’s experience that most street gang members are known by street names or monikers to their fellow gang members, and that they frequently write their names and/or monikers of their associates on walls, furniture, miscellaneous items or papers, both within and on their residences, and within and on their vehicles.

**Gang Photographs:** Paintings, drawings, developed and undeveloped film, photographs and/or photograph albums depicting persons, vehicles, weapons, and/or locations to be relevant on the question of gang membership or association, which depict items sought in this Search Warrant, and/or which depict evidence of any criminal activity.

{%p endif %}

{%p **if** NARCOTICS %}

**Controlled Substances:** any controlled substances or items used to ingest, package, prepare or distribute controlled substances;

**Notes and Ledgers:** any written records relating to the distribution of controlled substances;

**United States Currency**;

**Indicia**: including, but not limited to, utility and telephone bills, canceled envelopes, and keys.

{%p endif %}

{%p **if** MURDER %}

**Firearms or Firearm Accessories:** any ammunition, spent casings/cartridges, spent slugs from guns, firearms, and any other weapons or items that could have been used as weapons based on the factual description above;

**Indicia**: including, but not limited to, utility and telephone bills, canceled envelopes, and keys.

**Biological Evidence:** including but not limited to substances such as blood spatter, blood pooling, hair, DNA, bone fragments or any other biological indication of injury;

**Electronic Devices:** cellular telephones, computers and other electronic smart devices or peripherals.

**Documents:** any written notes or documentation pertaining to events leading up to or explaining the murder;

**Trace Evidence:** any objects that may contain fingerprints, fibers, etc;

All of these items are evidence in this investigation that could potentially lead to further details surrounding this death investigation in that the described items could incriminate or exclude possible witnesses/suspects.

{%p endif %}

{%p **if** CELL\_PHONE%}

Live and deleted user attribution data including, but not limited to, user accounts, e-mail accounts, passwords, PIN codes, patterns, account names, user names, screen names, remote data storage accounts, documents, files, metadata, or any other information and evidence that may demonstrate attribution to a particular user or users;

Live and deleted application data, records, documents, financial transaction records and other items that may constitute evidence, contraband, fruits, and/or instrumentalities of violations of crimes, including but not limited to the crime(s) listed;

Live and deleted contact lists, call logs, text messages and multimedia messages (SMS and MMS messages), iMessages, e-mails, chats, video conference communication data, contact information, financial transactions, installed application information including content and any other information which can be used to identify potentially associated persons;

Live and deleted passwords, password files, PIN codes, encryption codes, or other information necessary to access the digital device or data stored on the digital device such as hidden file applications;

Live and deleted documents, programs, pictures, videos, audio files, text files, databases, application data, calendar entries, user dictionaries, malware, viruses, tracking or other remote monitoring software, and any associated metadata;

Live and deleted geo-location data including latitude, longitude, elevation, Global Positioning System (GPS), cell site locations, Wi-Fi connections, and any other location base information;

Live and deleted web browser history, web browser bookmarks, temporary Internet files, cookies, searched items, downloaded and uploaded files, social networking websites or applications;

Live and deleted data stored on removable media such as Subscriber Identity Modules (SIM cards), flash memory storage devices such as Secure Digital (SD) and Micro SD media cards and any associated technology;

I also understand that in order to successfully complete a forensic extraction from a mobile device, it may be necessary to repair the device, replace the display screen, replace the chassis, replace the battery, and repair or replace switches and other components that are necessary to make the device operational. I also understand that it may be necessary to employ advanced forensic processes to remove or bypass locked display screens and other data access restrictions. Advanced processes may include, but are not limited to, brute force attack methods, third party proprietary services and methods and destructive and potentially destructive processes such as gaining root and/or Super user level access and employing methods such as JTAG, ISP-JTAG and chip-off in order to extract data.

The executing law enforcement officer(s) may need to enlist the aid of a specialized computer forensic laboratory and/or certified digital evidence examiner(s) in repairing, searching, viewing, photographing, recording, copying, forensic imagining, and analysis of all of the information described.

**RETENTION OF FORENSIC IMAGES AND EXTRACTIONS**

The government will retain a forensic image or forensic extraction of each electronic storage device subjected to analysis for a number of reasons, including proving the authenticity of evidence to be used at trial; responding to questions regarding the corruption of data; establishing the chain of custody of data; refuting claims of fabricating, tampering, or destroying data; and addressing potential exculpatory evidence claims where, for example, a defendant claims that the government avoided its obligations by destroying data or returning it to a third party.

{%p endif %}

**End Attachment “B”**