

INVENTORY

IN THE COUNTY COURT OF LANCASTER COUNTY, NEBRASKA

**IN THE MATTER OF THE SEARCH WARRANT
OF THE DESCRIBED PREMISES OF
LINCOLN POLICE DEPARTMENT
575 SOUTH 10TH STREET
LINCOLN, LANCASTER COUNTY, NEBRASKA**

**CLERK OF THE
DISTRICT COURT**

2024 MAY 10 PM 3:50

LANCASTER COUNTY

**STATE OF NEBRASKA)
)
COUNTY OF LANCASTER)**

ss.

**INVENTORY OF PROPERTY
SEIZED BY VIRTUE OF THE
SEARCH WARRANT ISSUED HEREIN**

Corey Weinmaster, being first duly sworn on oath, deposes and says the following is an inventory of the property seized by virtue of the Search Warrant issued herein:

The following is a list of the items seized and removed as evidence during the execution of the search warrant at the premise of the Lincoln Police Department, 575 South 10th Street, Lincoln, Lancaster County, Nebraska.

iPhone 11 under LPD Property
Q2408383

- Application Usage Log - 16311
- Call Log - 1973
- Chats - 831
- Contacts - 543
- Cookies - 293
- Credit Cards - 1
- Device Connectivity - 208
- Device Events - 31503
- Device Notifications - 1664
- Devices - 9
- Emails - 168
- Installed Applications - 15
- Instant Messages - 36
- Journeys - 36
- Locations - 1333
- Notes - 4
- Recordings - 1
- Searched Items - 283
- SIM Data - 9
- Social Media - 55
- Transfers - 37
- User Accounts - 19
- Voicemail - 1
- Web Bookmarks - 6
- Web History - 4234
- Wireless Networks - 365
- Timeline - 139192
- Audio - 1593
- Images - 14574
- Videos - 4049

iPhone 12 under LPD Property
Q2408384


- Application Usage Log - 8051
- Call Log - 1129
- Cell Towers - 101
- Chats - 465
- Contacts - 482
- Cookies - 241
- Device Connectivity - 27
- Device Events - 21924
- Device Notifications - 680
- Device - 4
- Emails - 18
- Installed Applications - 7
- Instant Messages - 12
- Journeys - 2

- Locations - 1411
- Notes - 2
- Recordings - 1
- Searched Items - 180
- SIM Data - 9
- Social Media - 231
- User Accounts - 17
- Web Bookmarks - 6
- Web History - 1116
- Wireless Networks - 815
- Timeline - 77982
- Audio - 86
- Images - 7605
- Videos - 1211

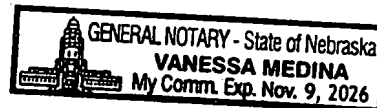
Inventory made in the presence of Derek Dittman.


Corey Weinmaster

SUBSCRIBED to in my presence and sworn to before me this 10th day of
May, 2024.



Notary Public



RECEIPT OF SEIZED ITEMS

The following is a list of the items seized and removed as evidence during the execution of a search warrant at the premise of the Lincoln Police Department, 575 South 10th Street, Lincoln, Lancaster County, Nebraska.

iPhone 11 under LPD Property Q2408383

- Application Usage Log – 16311
- Call Log – 1973
- Chats – 831
- Contacts – 543
- Cookies – 293
- Credit Cards – 1
- Device Connectivity – 208
- Device Events – 31503
- Device Notifications – 1664
- Devices – 9
- Emails – 168
- Installed Applications – 15
- Instant Messages – 36
- Journeys – 36
- Locations – 1333
- Notes – 4
- Recordings – 1
- Searched Items – 283
- SIM Data – 9
- Social Media – 55
- Transfers – 37
- User Accounts – 19
- Voicemail – 1
- Web Bookmarks – 6
- Web History – 4234
- Wireless Networks – 365
- Timeline – 139192
- Audio – 1593
- Images – 14574
- Videos – 4049

iPhone 12 under LPD Property Q2408384

- Application Usage Log – 8051
- Call Log – 1129
- Cell Towers – 101
- Chats – 465

LANCASTER COUNTY
2024 MAY 10 PM 3:50
CLERK OF THE
DISTRICT COURT

- Contacts – 482
- Cookies – 241
- Device Connectivity – 27
- Device Events – 21924
- Device Notifications – 680
- Device – 4
- Emails – 18
- Installed Applications – 7
- Instant Messages – 12
- Journeys – 2
- Locations – 1411
- Notes – 2
- Recordings – 1
- Searched Items – 180
- SIM Data – 9
- Social Media – 231
- User Accounts – 17
- Web Bookmarks – 6
- Web History – 1116
- Wireless Networks – 815
- Timeline – 77982
- Audio – 86
- Images – 7605
- Videos – 1211

Date 5/7/24

Cory L. Mawster #883
Law Enforcement Officer

Witness [Signature] 1551

ATTACHMENT A: Digital Device(s) to Be Searched

Law enforcement and those assisting law enforcement is directed to seize and search the following:

- Red Apple iPhone, to include any digital device within, located in the Lincoln Police Property & Evidence Unit at 575 South 10th Street, Lincoln, Lancaster County, Nebraska, labeled with Property Number **Q2408383** and Case Number **C4-035447**.
- Black Apple iPhone, to include any digital device within, located in the Lincoln Police Property & Evidence Unit at 575 South 10th Street, Lincoln, Lancaster County, Nebraska, labeled with Property Number **Q2408384** and Case Number **C4-035447**.

for the following evidence, to include any live and/or deleted data to include including any live and/or deleted data for the time frame of **January 1st, 2024** to **April 26th, 2024**, specifically for the seizure of following items:

1. Device identifiers, information and configurations.
2. User account information and any associated accounts on the device.
3. Databases and file systems.
4. Device activity logs and application usage logs
5. Call logs.
6. Contact lists.
7. Short Message Service (SMS), Multimedia Messaging Service (MMS) messages and instant messages.
8. Chat messages from installed applications.
9. Email messages.
10. Installed applications and their corresponding accounts and data.
11. Images and associated metadata.
12. Videos, and associated metadata.
13. Audio files, including voicemails, and associated metadata.
14. Document files and associated metadata.
15. Internet browsing history, including bookmarks, searches, browser cookies and other associated cache files.
16. Location data to include cellular tower connections, GPS (Global Positioning System) fixes, waypoints, routes, tracks, maps, and associated metadata.

To obtain and search the data from the aforementioned digital device, law enforcement and/or those assisting may:

1. Obtain data from the physical memory of the digital device itself as well as from any data storage devices housed within the digital device, specifically Secure Digital (SD) and Subscriber Identification Module (SIM) cards;
2. Obtain data from the aforementioned digital device's active file system, as well as unallocated space as to recover deleted data and file fragments;
3. Obtain data by making unobtrusive revocable setting changes to permit the digital extraction of the data unless the digital device requires disassembly to obtain the desired data which may render the device inoperable;
4. Copy, forensically image, view, photograph, record, and/or conduct forensic analysis of the data obtained;
5. Enlist the aid of non-law enforcement, who are trained in conducting forensic analysis of the data in retrieving and analyzing the data. When files have been deleted, they can be potentially recovered later using forensic tools. A person with familiarity with how digital devices work may, after examining the data, be able to draw conclusions about how the device was used, the purpose of its use, who used it, where, and when; and/or
6. Be required to examine every file and scan its contents briefly to determine whether it falls within the scope of the warrant. This is necessary as it is difficult to know prior to the search the level of technical ability of the device's user and data can be hidden, moved, encoded or mislabeled to evade detection.
7. Remove the digital device to another location conduct the digital forensic examination and/or analysis.

The search of digital devices is a lengthy process requiring special steps to ensure the integrity of the digital devices. In the event the search and/or seizure of evidence is not completed within ten (10) days, law enforcement is authorized to return the search warrant within ten (10) days upon completion of the search and seizure.

ATTACHMENT B: Technical Information Regarding the Search of Digital Devices

Through your Affiant's training and past experience, and from information provided by Electronic Evidence Unit forensic examiners, your Affiant is aware that:

Digital device data can provide valuable insight for criminal investigations. Digital devices are used by the general public for communication, access to and sharing of information, research, socialization, entertainment, mapping, shopping, note taking and other functionality. Individuals also use digital devices for the aforementioned purposes, and as a tool for facilitating criminal activity.

Digital devices are often used to communicate via voice, text messaging, social media or other communication applications; and share data with other users and that such digital data can be transferred between various digital devices. Information associated with such data may show evidence of current, on-going, future, and past criminal activity as well as assist law enforcement in determining identity and culpability of participants, including identifying those with knowledge of a criminal offense or identify those who have aided a criminal participant in the commission of a criminal offense, victims and/or witnesses. As such, digital devices possessed by criminal participants can serve both as an instrument for committing crime as well as a storage medium for evidence of the crime, including communications to plan, execute, and otherwise document the commission of a crime.

There have been numerous instances where criminal participants utilized digital devices to photograph themselves, associates and/or co-conspirators, and victims; instances in which digital devices were used by criminal participants to create videos of their criminal activity; instances where criminals participants have used digital devices' internet applications to research crimes they have or intend to participate in; instances in which criminal participants have maintained notes within digital devices; and instances in which criminal participants used global positioning, mapping and other location services to facilitate in-person meetings with co-conspirators and/or a victim.

On a digital device, data can be created in a matter of moments because most operations can be performed almost instantly, which would be relevant to the incident being investigated. The data can be created intentionally or accidentally by the user, or automatically by the device itself as a part of its regular functioning.

Electronic evidence can remain on the digital devices for indefinite periods of time after the data was created, even if deleted by the user. Data generally is stored on the physical memory of the digital device, but also can be stored on removable storage devices such as Secure Digital (SD) and Subscriber Identification Module (SIM) cards. A forensic

examiner may be able to recover information deleted by the user throughout the working life span of the device.

The following are examples of how types of data on digital devices can assist investigators. A full, all-inclusive list would be impossible due to the ever-increasing development of digital devices and their applications:

1. Phone information, configurations, calendar events, notes and user account information which can be used to identify or confirm who owns or was using a digital device. Because of their small size, digital devices can easily be passed from one person. As such it is necessary to document evidence that reveals or suggests who possessed or used the device. This evidence is akin to the search for venue items when executing a search warrant at a residence.
2. Call logs can establish familiarity between people involved in an incident. These records are consistently stamped with dates and times which can be significant regarding the reconstruction of the timeline of events regarding an investigation. Associated contact lists stored in the device can provide names to correspond with voice calls as well as other forms of communication. Voicemails can indicate the purpose of the phone call when the phone call was not answered. This information can also be invaluable to establish conspirators, witnesses, and suspect information.
3. Data from associated supplemental software applications (apps), both standard and manually installed, stored on the digital devices can demonstrate the user's association with investigated people, locations, and events. Digital devices can run apps which allow them to increase their functionality. Common programs include social media applications, such as Facebook, as well as messaging applications Snapchat and Facebook Messenger to name a few. These applications are increasingly used as alternative methods for users to communicate from the standard messaging service as they offer additional functionality. Many of these applications can determine the user's geographic location which can be instrumental to completing an investigation.
4. Media files such as images, videos, audio, and documents provide first-hand documentation of actions regarding an event. Additionally, files can contain embedded metadata that show additional information which is valuable to investigators such as when and where the file was created. Digital devices can create, store and exchange media with other devices and computers.

Your Affiant seeks to complete a comprehensive and unbiased examination of the data on the device for information which could aid in the investigation; seeking only prescribed information would jeopardize the completeness of the search as it is typically unknown how the electronic device was used or the technical ability and intent of the user before

the device has been examined. As with other types of evidence, the context, location, and data surrounding information in the device data is often necessary to understand whether evidence falls within the scope of the search warrant. This type of information will be important to the forensic examiner's ability to piece together and recognize evidence of the above-listed crimes.

Your Affiant knows that digital devices are constantly changing system data on the device as programmed by their manufacturer. Additionally, your Affiant knows that searching the digital device itself would irreversibly alter data and/or evidence on the device. To search a device for evidence, the commonly accepted best practice of digital forensics is to utilize forensic software to obtain an extraction of the data on the device. Attempts will be made to obtain the devices data by only making unobtrusive revocable changes to the system settings to permit the extraction of the data. If necessary, the digital device may require disassembly to obtain the desired data which may render the device inoperable. These processes do not change or alter any of the user data stored on the device. The extraction is then searched using analysis software to locate, identify, and seize the evidence authorized by this warrant. The device and the image are then preserved in evidence.

The digital device has been stored in a manner in which its/their contents are, to the extent material to this investigation, substantially the same state as when it first came into the possession of law enforcement.

IN THE COUNTY COURT OF LANCASTER COUNTY, NEBRASKA

STATE OF NEBRASKA)
)
COUNTY OF LANCASTER)

ss. AFFIDAVIT FOR SEARCH WARRANT

Kevin Meyer, being first duly sworn upon oath deposes and states that he is an Investigator for the Lincoln Police Department, Lincoln, Lancaster County, Nebraska. AFFIANT states he is currently involved in the investigation of Possession of a Firearm by a Prohibited Juvenile Offender in violation of Nebraska Revised Statute 28-1204.05 (F4) and Deliver; Manufacture; Intent to Deliver Controlled Substance, Schedule 1,2,3 in violation of Nebraska Revised Statute 28-416(1)(2)(B) (F2A) occurring on 04-26-2024, in the 6900 block of Rexford Driver, Lincoln, Lancaster County Nebraska. AFFIANT has reviewed case reports regarding this investigation prepared by other involved Law Enforcement Officers.

Attachments

- Attachment A: Digital Devices to Be Searched
- Attachment B: Technical Information Regarding the Search of Digital Devices.

Affiant's Background

Your AFFIANT has been a police officer for the Lincoln Police Department since 2013. Your AFFIANT has spent 5 years as a patrol officer, 3 years as a narcotics investigator with the Lincoln-Lancaster County Narcotics Task Force and is currently assigned as an investigator for the Capital Region Safe Streets Task Force. Your AFFIANT has training and experience in investigating a wide range of crimes to include narcotics and weapon related offenses. Your AFFIANT has authored numerous search warrants pertaining to the aforementioned investigations.

This Affidavit is submitted in support of a search warrant. Since this Affidavit is being submitted for the limited purpose of securing a search warrant, your Affiant has not set forth every fact known to me regarding this investigation. The statements contained in this Affidavit are based in part on the investigation that your Affiant has conducted, and information provided to your Affiant by other law enforcement officers verbally, and through written reports.

Case Facts

In 2023, investigators with the Capital Region Safe Streets Task Force began monitoring Kaeydan Gonzales' (12-16-2007) social media accounts for evidence of criminal activity due to his association with other individuals known to law enforcement. One of these accounts was his Instagram account, KG12.16. Investigators were able to determine that this account belonged to Gonzales based on selfie style photos and videos he took of himself as well as the name of his account as it references his initials and date of birth.

During one of his social media posts, Gonzales posted a link to his Telegram account. Telegram is a social media platform where individuals can post photographs and have conversations with other members of the group. The link that Gonzales posted took your AFFIANT to a group titled, KgGetsDough. The "owner" of the group was listed as Kaeydan Go. Based on the initials "KG" and the name "Kaeydan Go", this further led your Affiant to believe this Telegram account was run by Gonzales. On 02-08-2024, Gonzales made three separate posts to the account. The first post was a video that showed a large baggie of marijuana. The caption of this video read, "125Oz", which your Affiant took to mean that Gonzales was selling ounce quantities of marijuana for \$125 U.S. Currency. The second post showed a pink and blue box with the title "Juice Box". Additional writing on the packaging read, "1 gram each", "100 juice box carts", and ... "that gets you high" with several marijuana leaves on the box. From your Affiant's training and experience, this is believed to be commercially available THC products. The last photograph showed several similar boxes in a fridge. There were at least four different boxes of what appeared to be commercially available THC products. The caption on this photo was a mushroom emoji followed by a chocolate bar emoji.

On 02-20-2024, your Affiant observed Gonzales post a photo on his known Instagram story with the caption, "2gs in hml". Your affiant took this to mean that he had 2000mg THC products for sale.

On 02-21-2024, Investigators with the Capital Region Safe Streets Task Force along with the Lincoln Police Department SWAT team, served a residential search warrant at 1640 Washington Street #5, Lincoln, Lancaster County, Nebraska. This was the known residence of Kaeydan Gonzales who lived there along with his brother, Kaeylab Gonzales (07-29-2004). During a search of the residence, Investigators located approximately 398.9 grams of marijuana, 30.2 grams of suspected Psilocybin

mushrooms, 68 commercially available chocolate mushroom bars, 122 THC vape cartridges, \$6380 U.S. Currency, 9mm ammunition and evidence of sales. The THC vape cartridges that were seized during the warrant matched the same items that Gonzales had advertised in the days prior to the warrant being served.

On 04-26-2024 at approximately 1357 hours, Investigators with the Capital Region Safe Streets Task Force conducted a field contact of a black 2009 Toyota Camry bearing Nebraska plate YYP 456 in the 6900 block of Rexford Driver, Lincoln, Lancaster County, Nebraska. Investigator Villamonte #1700 contacted Cindy Nguyen (08-18-2004) as the driver and Kaeydan Gonzales (12-16-2007) as the front passenger. Investigator Villamonte immediately noted an odor of marijuana emanating from within the vehicle and asked both occupants to step out of the vehicle. Your AFFIANT approached the passenger side of the vehicle and observed Gonzales remove a satchel style bag from around his body and place it next to him. Investigator Villamonte was giving Gonzales commands to exit the vehicle, but Gonzales ignored these commands and began digging between the passenger seat and passenger door area. Investigator Lind #1638 opened the front passenger door and your AFFIANT observed Gonzales attempting to conceal a baggie of marijuana next to his seat. Gonzales was removed from the vehicle and detained. A probable cause search of the vehicle was then conducted.

Your AFFIANT observed that the bag that he had removed was a black, Louis Vuitton, satchel. Upon opening the bag, your AFFIANT immediately observed two handguns. The first firearm was a Glock 43 9mm handgun with a 50 round drum magazine. The handgun had a red aftermarket trigger installed. Your AFFIANT cleared the firearm and observed it to have s/n: BZWP942. This was later run through the police information channel and was determined to have been stolen from a Gage County deputy that lived in the city limits of Lincoln. This case was documented under C4-004529. The second firearm was found to be a Polymer80 9mm handgun with an aftermarket slide. This firearm had no serial number. The firearm was loaded with 15 rounds of 9mm which were in a translucent extended magazine. This Polymer80 handgun had a laser/light combination with the laser illuminating a blue light. During a further search of the satchel, 4 rounds of loose 9mm ammunition were also located in a side pocket.

The baggie of marijuana that Gonzales was attempting to conceal was found to have a total weight of 20.1 grams. During a further search of the vehicle, Investigator Villamonte located a backpack in the back seat. Within this backpack, Investigator Villamonte located an additional baggie of marijuana with a total weight of 23.3 grams along with two commercially available THC cartridges. These THC cartridges appeared similar to what Gonzales had been advertising for sale in February.

Upon contact with Gonzales, he was found to be in possession of two cellular telephones. The first phone was a black Apple iPhone in a clear case and the second was a red Apple iPhone in a clear case.

Investigator Villamonte conducted a criminal history check on Kaeydan Gonzales. Investigators with the Capital Region Safe Streets Task Force had contacted Gonzales in 2022 and arrested him for possession of a defaced firearm. This arrest resulted in a juvenile felony adjudication on 03-08-2023, where a Judge advised that Gonzales cannot possess firearms.

Your AFFIANT knows from training and experience that individuals often use cellular telephones in order to facilitate the sale of narcotics. Based on the numerous narcotic advertisements on social media along with the collection of physical evidence on two separate occasions, your AFFIANT believes that there will be evidence of narcotics sales on one or both of Gonzales' cellular telephones.

The above does constitute grounds of probable cause for the issuance of a search warrant to search and seize the evidence specifically identified in Attachment A, to include any specific authorization requested authorization to be ordered by the court.

Further AFFIANT saith not;

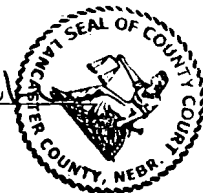
Dated this 3RD day of May, 2024.

Kevin Meyer #1716
Kevin Meyer, AFFIANT

SUBSCRIBED to in my presence and sworn to before me this 3rd day of May, 2024.

Lawrie J. Gard
Judge of the County Court

Lawrie J. Gard
Printed Name of Judge



ATTACHMENT A: Digital Device(s) to Be Searched

Law enforcement and those assisting law enforcement is directed to seize and search the following:

- Red Apple iPhone, to include any digital device within, located in the Lincoln Police Property & Evidence Unit at 575 South 10th Street, Lincoln, Lancaster County, Nebraska, labeled with Property Number **Q2408383** and Case Number **C4-035447**.
- Black Apple iPhone, to include any digital device within, located in the Lincoln Police Property & Evidence Unit at 575 South 10th Street, Lincoln, Lancaster County, Nebraska, labeled with Property Number **Q2408384** and Case Number **C4-035447**.

for the following evidence, to include any live and/or deleted data to include including any live and/or deleted data for the time frame of **January 1st, 2024** to **April 26th, 2024**, specifically for the seizure of following items:

1. Device identifiers, information and configurations.
2. User account information and any associated accounts on the device.
3. Databases and file systems.
4. Device activity logs and application usage logs
5. Call logs.
6. Contact lists.
7. Short Message Service (SMS), Multimedia Messaging Service (MMS) messages and instant messages.
8. Chat messages from installed applications.
9. Email messages.
10. Installed applications and their corresponding accounts and data.
11. Images and associated metadata.
12. Videos, and associated metadata.
13. Audio files, including voicemails, and associated metadata.
14. Document files and associated metadata.
15. Internet browsing history, including bookmarks, searches, browser cookies and other associated cache files.
16. Location data to include cellular tower connections, GPS (Global Positioning System) fixes, waypoints, routes, tracks, maps, and associated metadata.

To obtain and search the data from the aforementioned digital device, law enforcement and/or those assisting may:

1. Obtain data from the physical memory of the digital device itself as well as from any data storage devices housed within the digital device, specifically Secure Digital (SD) and Subscriber Identification Module (SIM) cards;
2. Obtain data from the aforementioned digital device's active file system, as well as unallocated space as to recover deleted data and file fragments;
3. Obtain data by making unobtrusive revocable setting changes to permit the digital extraction of the data unless the digital device requires disassembly to obtain the desired data which may render the device inoperable;
4. Copy, forensically image, view, photograph, record, and/or conduct forensic analysis of the data obtained;
5. Enlist the aid of non-law enforcement, who are trained in conducting forensic analysis of the data in retrieving and analyzing the data. When files have been deleted, they can be potentially recovered later using forensic tools. A person with familiarity with how digital devices work may, after examining the data, be able to draw conclusions about how the device was used, the purpose of its use, who used it, where, and when; and/or
6. Be required to examine every file and scan its contents briefly to determine whether it falls within the scope of the warrant. This is necessary as it is difficult to know prior to the search the level of technical ability of the device's user and data can be hidden, moved, encoded or mislabeled to evade detection.
7. Remove the digital device to another location conduct the digital forensic examination and/or analysis.

The search of digital devices is a lengthy process requiring special steps to ensure the integrity of the digital devices. In the event the search and/or seizure of evidence is not completed within ten (10) days, law enforcement is authorized to return the search warrant within ten (10) days upon completion of the search and seizure.

ATTACHMENT B: Technical Information Regarding the Search of Digital Devices

Through your Affiant's training and past experience, and from information provided by Electronic Evidence Unit forensic examiners, your Affiant is aware that:

Digital device data can provide valuable insight for criminal investigations. Digital devices are used by the general public for communication, access to and sharing of information, research, socialization, entertainment, mapping, shopping, note taking and other functionality. Individuals also use digital devices for the aforementioned purposes, and as a tool for facilitating criminal activity.

Digital devices are often used to communicate via voice, text messaging, social media or other communication applications; and share data with other users and that such digital data can be transferred between various digital devices. Information associated with such data may show evidence of current, on-going, future, and past criminal activity as well as assist law enforcement in determining identity and culpability of participants, including identifying those with knowledge of a criminal offense or identify those who have aided a criminal participant in the commission of a criminal offense, victims and/or witnesses. As such, digital devices possessed by criminal participants can serve both as an instrument for committing crime as well as a storage medium for evidence of the crime, including communications to plan, execute, and otherwise document the commission of a crime.

There have been numerous instances where criminal participants utilized digital devices to photograph themselves, associates and/or co-conspirators, and victims; instances in which digital devices were used by criminal participants to create videos of their criminal activity; instances where criminals participants have used digital devices' internet applications to research crimes they have or intend to participate in; instances in which criminal participants have maintained notes within digital devices; and instances in which criminal participants used global positioning, mapping and other location services to facilitate in-person meetings with co-conspirators and/or a victim.

On a digital device, data can be created in a matter of moments because most operations can be performed almost instantly, which would be relevant to the incident being investigated. The data can be created intentionally or accidentally by the user, or automatically by the device itself as a part of its regular functioning.

Electronic evidence can remain on the digital devices for indefinite periods of time after the data was created, even if deleted by the user. Data generally is stored on the physical memory of the digital device, but also can be stored on removable storage devices such as Secure Digital (SD) and Subscriber Identification Module (SIM) cards. A forensic

examiner may be able to recover information deleted by the user throughout the working life span of the device.

The following are examples of how types of data on digital devices can assist investigators. A full, all-inclusive list would be impossible due to the ever-increasing development of digital devices and their applications:

1. Phone information, configurations, calendar events, notes and user account information which can be used to identify or confirm who owns or was using a digital device. Because of their small size, digital devices can easily be passed from one person. As such it is necessary to document evidence that reveals or suggests who possessed or used the device. This evidence is akin to the search for venue items when executing a search warrant at a residence.
2. Call logs can establish familiarity between people involved in an incident. These records are consistently stamped with dates and times which can be significant regarding the reconstruction of the timeline of events regarding an investigation. Associated contact lists stored in the device can provide names to correspond with voice calls as well as other forms of communication. Voicemails can indicate the purpose of the phone call when the phone call was not answered. This information can also be invaluable to establish conspirators, witnesses, and suspect information.
3. Data from associated supplemental software applications (apps), both standard and manually installed, stored on the digital devices can demonstrate the user's association with investigated people, locations, and events. Digital devices can run apps which allow them to increase their functionality. Common programs include social media applications, such as Facebook, as well as messaging applications Snapchat and Facebook Messenger to name a few. These applications are increasingly used as alternative methods for users to communicate from the standard messaging service as they offer additional functionality. Many of these applications can determine the user's geographic location which can be instrumental to completing an investigation.
4. Media files such as images, videos, audio, and documents provide first-hand documentation of actions regarding an event. Additionally, files can contain embedded metadata that show additional information which is valuable to investigators such as when and where the file was created. Digital devices can create, store and exchange media with other devices and computers.

Your Affiant seeks to complete a comprehensive and unbiased examination of the data on the device for information which could aid in the investigation; seeking only prescribed information would jeopardize the completeness of the search as it is typically unknown how the electronic device was used or the technical ability and intent of the user before

the device has been examined. As with other types of evidence, the context, location, and data surrounding information in the device data is often necessary to understand whether evidence falls within the scope of the search warrant. This type of information will be important to the forensic examiner's ability to piece together and recognize evidence of the above-listed crimes.

Your Affiant knows that digital devices are constantly changing system data on the device as programmed by their manufacturer. Additionally, your Affiant knows that searching the digital device itself would irreversibly alter data and/or evidence on the device. To search a device for evidence, the commonly accepted best practice of digital forensics is to utilize forensic software to obtain an extraction of the data on the device. Attempts will be made to obtain the devices data by only making unobtrusive revocable changes to the system settings to permit the extraction of the data. If necessary, the digital device may require disassembly to obtain the desired data which may render the device inoperable. These processes do not change or alter any of the user data stored on the device. The extraction is then searched using analysis software to locate, identify, and seize the evidence authorized by this warrant. The device and the image are then preserved in evidence.

The digital device has been stored in a manner in which its/their contents are, to the extent material to this investigation, substantially the same state as when it first came into the possession of law enforcement.