

MAR 26 2024

FILED
Clerk of District Court

LPD Case Number: C3-109298

IN THE COUNTY COURT OF LANCASTER COUNTY, NEBRASKA


CR 24-1

IN THE MATTER OF THE SEARCH WARRANT
OF THE DESCRIBED PREMISES OF
LINCOLN POLICE DEPARTMENT PROPERTY UNIT
575 S. 10TH ST
LINCOLN, LANCASTER COUNTY, NEBRASKA

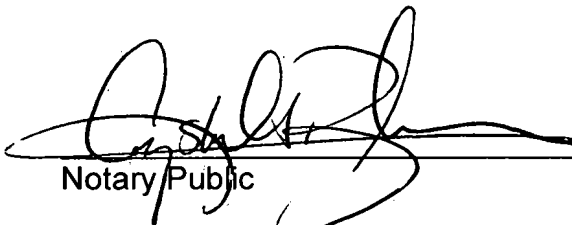
SEARCH WARRANT RETURN

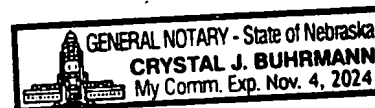
STATE OF NEBRASKA)
)
) ss.
COUNTY OF LANCASTER)

The undersigned states that he received the Search Warrant issued herein on the 15th day of March, 2024, and that he executed the same on the 25th day of March, 2024, by seizing the property described in the Inventory filed herein and by delivering a copy of the Search Warrant for the said property at the place from which the property is taken.


Sgt. Derek Dittman #1551

SUBSCRIBED to in my presence and sworn to before me this 25th day of March, 2024.


Notary Public





MAR 26 2024

FILED
Clerk of District Court

INVENTORY

IN THE COUNTY COURT OF LANCASTER COUNTY, NEBRASKA

**IN THE MATTER OF THE SEARCH WARRANT
OF THE DESCRIBED PREMISES OF
LINCOLN POLICE DEPARTMENT PROPERTY UNIT
575 S. 10TH ST
LINCOLN, LANCASTER COUNTY, NEBRASKA**

STATE OF NEBRASKA)
)
COUNTY OF LANCASTER)

ss.


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

Derek Dittman, 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 undersigned hereby acknowledges receipt of the following described property seized from the following devices labeled with case number C3-109298 and their associated property numbers, located in the Lincoln Police Department Property Unit at 575 S. 10th St., Lincoln, Lancaster County, Nebraska:

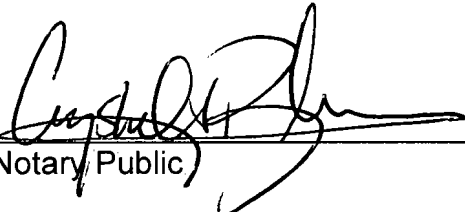
- Q2404400 HP laptop computer - physical image of hard drive
- Q2404402 red Samsung SGH-A797 phone – logical extraction
- Q2404405 blue Samsung SGH-877 phone – physical extraction
- Q2404407 black flip phone model EA211101 – manual search of device
- Q2404409 Seagate 4TB hard drive – physical image of hard drive
- Q2404417 notebook with brown cover – manual search of contents
- Q2404420 writeable DVD discs – manual search of discs' contents

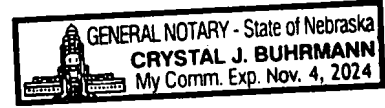
Inventory made in the presence of Inv. Corey Weinmaster #883.



Sgt. Derek Dittman #1551

SUBSCRIBED to in my presence and sworn to before me this 25th day of March, 2024.


Notary Public



RECEIPT

The undersigned hereby acknowledges receipt of the following described property seized from the following devices labeled with case number C3-109298 and their associated property numbers, located in the Lincoln Police Department Property Unit at 575 S. 10 St., Lincoln, Lancaster County, Nebraska:

- Q2404400 HP laptop computer – physical image of hard drive
- Q2404402 red Samsung SGH-A797 phone – logical extraction
- Q2404405 blue Samsung SGH-877 phone – physical extraction
- Q2404407 black flip phone model EA211101 – manual search of device
- Q2404409 Seagate 4TB hard drive – physical image of hard drive
- Q2404417 notebook with brown cover – manual search of contents
- Q2404420 writeable DVD discs – manual search of discs' contents


FILED
Clerk of District Court

MAR 26 2024

CLERK'S OFFICE, DISTRICT COURT
LANCASTER COUNTY, NEBRASKA

DATED this 25th day of March, 2024.


Law Enforcement Officer


Witness

MAR 26 2024

FILED
Clerk of District Court

IN THE COUNTY OF LANCASTER COUNTY, NEBRASKA

STATE OF NEBRASKA)
) **ss. SEARCH WARRANT**
COUNTY OF LANCASTER)

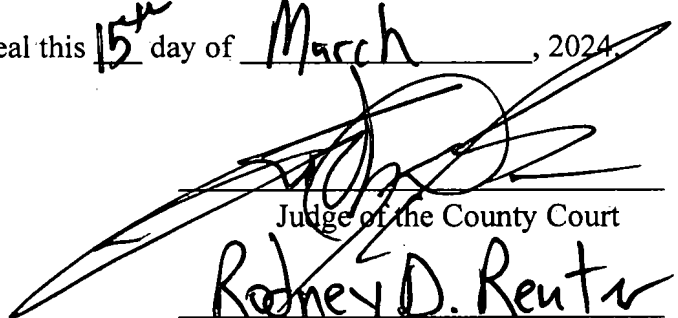
TO: Derek Dittman, a law enforcement officer with the Lincoln Police Department, Lincoln, Lancaster County, Nebraska, any and all law enforcement officers, and agents thereof.

WHEREAS, Derek Dittman has filed an Affidavit before the undersigned Judge of the County Court of Lancaster County, Nebraska, and said written Affidavit, having been duly considered, the court finds that the facts set forth in said Affidavit are true, and that those facts do constitute grounds and probable cause for the issuance of a Search Warrant.

THEREFORE, you are commanded to search and seize the items as described in Attachment A, hereby attached and incorporated by reference, to include any specific authorization as contained in Attachment A.

THEREFORE, you are commanded to execute and return this Search Warrant in the manner as prescribed in Attachment A.

Given under my hand and seal this 15th day of March, 2024.



Judge of the County Court
Rodney D. Reuter

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 devices located in the Lincoln Police Property & Evidence Unit at 575 South 10th Street, Lincoln, Lancaster County, Nebraska, labeled with Property Numbers Q2404400, Q2404402, Q2404405, Q2404407, Q2404409, Q2404417 and Q2404420 and associated Case Number C3-109298.

HP laptop computer, red Samsung SGH-A797 cell phone, blue Samsung SGH-877 cell phone, black flip phone model EA211101, Seagate 4TB hard drive, notebook with brown cover, multiple writeable DVD discs

for the following evidence, to include any live and/or deleted data, 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. Short Message Service (SMS), Multimedia Messaging Service (MMS) messages and instant messages.
6. Chat messages from installed applications.
7. Email messages.
8. Installed applications and their corresponding accounts and data.
9. Images and associated metadata.
10. Videos, and associated metadata.
11. Document files and associated metadata.
12. Internet browsing history, including bookmarks, searches, browser cookies and other associated cache files.
13. Location data to include cellular tower connections, GPS (Global Positioning System) fixes, waypoints, routes, tracks, maps, and associated metadata.
14. Wireless networks, Bluetooth, IP addresses, and synchronization connection history.
15. Memos and notes (typed and voice).
16. User dictionary.
17. Passwords, keychains.

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.

MAR 26 2024

FILED
Clerk of District Court

IN THE COUNTY COURT OF LANCASTER COUNTY, NEBRASKA

STATE OF NEBRASKA)
) ss. AFFIDAVIT FOR SEARCH WARRANT
COUNTY OF LANCASTER)

Derek Dittman, being first duly sworn upon oath deposes and states that he is a Sergeant for the Lincoln Police Department, Lincoln, Lancaster County, Nebraska. AFFIANT states he is currently involved in the investigation of the state violation of possession of sexually explicit conduct, NRS 28-813.0, and the federal violation of certain activities relating to material constituting or containing child pornography, 18 U.S. Code 2252A(a)(2), occurring on December 4, 2023, at 104 Austin St. Waco, York County Nebraska. AFFIANT has reviewed case reports regarding this investigation prepared by other involved Law Enforcement Officers.

Affiant's Background

Your Affiant has been a police officer for the Lincoln Police Department since 2005. Your Affiant has training and experience in conducting criminal investigations including homicides, burglaries, robberies, sexual assaults, human trafficking, child enticement, and possession of child pornography.

This Affidavit is submitted in support of a search warrant. Your Affiant may not have set forth every fact known to your Affiant regarding this investigation. The information contained in this Affidavit is from your Affiant's criminal investigation and may include information provided by other law enforcement, or others.

Case Facts

Beginning in May of 2023, Jay Gilmore was on a four year supervised release term from federal imprisonment after he was convicted of receipt and distribution of child pornography. Some of the conditions Gilmore agreed to, for his supervised release, were to not be in possession of unapproved computers or electronic devices, and to notify his supervising officer of the electronic devices he had access to. Additional conditions required Gilmore to allow a probation officer to search his property and any electronic devices that were in his possession. As part of his release, Gilmore was supplied with a cell phone from Probation that had special software installed to allow U.S. Probation to monitor his usage, and he was allowed to utilize this phone. U.S. Probation Officer Theresa Rerucha was assigned to supervise Gilmore.

On November 28, 2023, Ofc. Rerucha was contacted by a State of Nebraska probation officer, Ofc. Otte, who also supervised Gilmore. Ofc. Otte told Ofc. Rerucha she had been contacted by Gilmore's sister, Chrystal Mulder, who reported Gilmore had several electronic devices in his possession, and he had been taking photos of neighborhood children. Ofc. Rerucha contacted Mulder, and Mulder verified Gilmore was in possession of an unapproved smartphone and Mulder's adult daughter had told Mulder she observed photos on Gilmore's phone of neighborhood children playing outside.

On December 4, 2023, Ofc. Rerucha and several other U.S. Probation officers contacted Gilmore at his residence, 104 Austin St., Waco, NE, and searched his bedroom and vehicle pursuant to his supervised release terms and conditions. The officers located several unapproved electronic devices, storage medium, and a laptop. U.S. Probation Officer Jonathan Lordino asked Gilmore for consent to search a Samsung Galaxy Z Flip 3, which was located during the search, and Gilmore granted consent. Ofc. Lordino viewed the internet browsing history and observed searches for several terms that would lead one to believe Gilmore was viewing child pornography. Ofc. Lordino also observed sexually explicit material of adults and anime. In addition, a notebook was located that appeared to have websites and search terms related to child pornography written in it. Several items were seized from the search and transported to the U.S. Probation office in Lincoln, NE. Gilmore was arrested on a supervised release violation.

On December 6, 2023, U.S. Probation Officer Leslie Van Winkle conducted a forensic search of one of the seized items, a Samsung Galaxy A03s cell phone. The search yielded images of child pornography. After locating these images, Ofc. Van Winkle contacted your Affiant, notified him of her findings, and turned over the Samsung Galaxy A03s, the Samsung Galaxy Z Flip 3, an Apple iPod, an SD card, and a thumb drive. Ofc. Van Winkle provided a copy of Gilmore's supervised release conditions to your Affiant, who reviewed them. A search of these items was completed to assist U.S. Probation under the authority of the conditional release requirements, along with the consent given by Gilmore to Ofc. Lordino. At the time of the search, child pornography was observed on the Samsung Galaxy A03s.

Through further investigation, your Affiant learned there were additional seized electronic devices remaining which had not been turned over to him initially. On March 8, 2024, your Affiant came into possession of the remaining items that were seized from Gilmore's possession. The additional items included an HP laptop, a red Samsung SGH-A797 phone, a blue Samsung SGH-A877 phone, a black ATT phone model EA211101, an external hard drive, a notebook with brown cover, and several writeable DVD's.

Although the crime of possession of child pornography occurred in Waco, York County, Nebraska, the evidence, and the discovery of the crime, is existing in Lincoln, Lancaster County, Nebraska. Due to his training and experience, your Affiant has knowledge that child pornography can be stored on the electronic devices that were seized from Gilmore's residence. Your Affiant believes he has probable cause that state and federal law violations have occurred. Once the evidence is searched and seized, it will be shared with the appropriate law enforcement entities.

Attachments

Attachment A: Property to be searched and seized
Attachment B: Technical information for the service provider

Your Affiant requests authorization to search for and seize the listed items in Attachment A.

Attachment B contains technical information pertinent to the service provider and is intended to provide an overview of the service. This information is based on the training and experience of Your Affiant and/or other members of the Lincoln Police Department.

The above are hereby attached and incorporated by reference.

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.

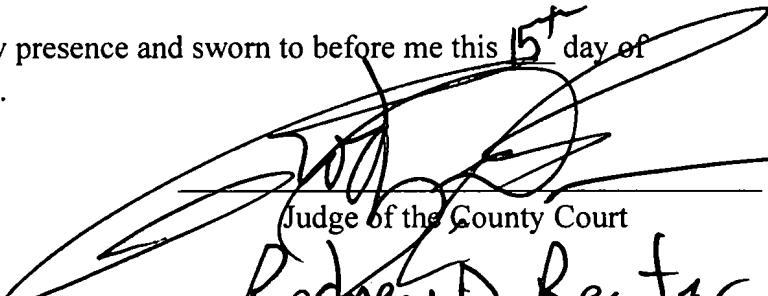
Further AFFIANT saith not;

Dated this 15 day of March 2024.



Derek Dittman AFFIANT

SUBSCRIBED to in my presence and sworn to before me this 15th day of March, 2024.



Judge of the County Court
Rodney D. Reuter
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 devices located in the Lincoln Police Property & Evidence Unit at 575 South 10th Street, Lincoln, Lancaster County, Nebraska, labeled with Property Numbers Q2404400, Q2404402, Q2404405, Q2404407, Q2404409, Q2404417 and Q2404420 and associated Case Number C3-109298.

HP laptop computer, red Samsung SGH-A797 cell phone, blue Samsung SGH-877 cell phone, black flip phone model EA211101, Seagate 4TB hard drive, notebook with brown cover, multiple writeable DVD discs

for the following evidence, to include any live and/or deleted data, 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. Short Message Service (SMS), Multimedia Messaging Service (MMS) messages and instant messages.
6. Chat messages from installed applications.
7. Email messages.
8. Installed applications and their corresponding accounts and data.
9. Images and associated metadata.
10. Videos, and associated metadata.
11. Document files and associated metadata.
12. Internet browsing history, including bookmarks, searches, browser cookies and other associated cache files.
13. Location data to include cellular tower connections, GPS (Global Positioning System) fixes, waypoints, routes, tracks, maps, and associated metadata.
14. Wireless networks, Bluetooth, IP addresses, and synchronization connection history.
15. Memos and notes (typed and voice).
16. User dictionary.
17. Passwords, keychains.

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.

Digital devices typically retain some evidence of all activity taken via the device or associated media; and, as such, could contain evidence of crime. For example, data, whether stored intentionally or unintentionally, can contain evidence of knowledge, intent, efforts to conceal, sell or dispose of evidence or proceeds of criminal activity, accomplice identity, association with victims, or geographic location of the device possessor at particular dates and times. This information can be in numerous forms, such as photographs; address books or contact lists; or communications with others through means such as phone calls, email, instant messaging, social media, chat sessions, or other digital communications.

Digital data can be found in numerous locations, and formats. Evidence can be embedded into unlikely files for the type of evidence, such as a photo included in a document or converted into a PDF file or other format in an effort to conceal their existence.

Information on devices and media can be stored in random order; with deceptive file names; hidden from normal view; encrypted or password protected; and stored on unusual devices for the type of data, such as routers, printers, scanners, game consoles, or other devices that are similarly capable of storing digital data.

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.