

RECEIPT

The undersigned hereby acknowledges receipt of the following described property seized from the Phone in a Red Case, to include any digital device within, located in the Lincoln Police Property & Evidence Unit at 575 South 10th Street, Lincoln, Lancaster County, NE labeled with Property number Q2408380 labeled with Case number C4-032267, for the following items.

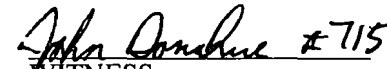
No data extraction obtained

LANCASTER COUNTY
2024 JUN -5 PM 2: 56

CLERK OF THE
DISTRICT COURT

DATED this 31st day of May 2024


Law Enforcement Officer


WITNESS

IN THE COUNTY OF LANCASTER COUNTY, NEBRASKA

LANCASTER COUNTY

2024 JUN -5 PM 2:56

CLERK OF THE DISTRICT COURT

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

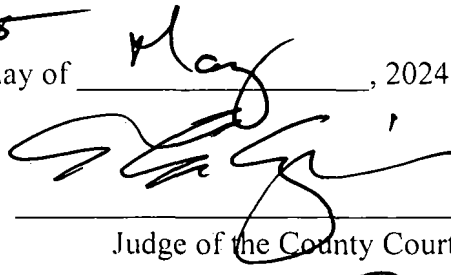
TO: Patrick Sullivan, a law enforcement officer with the Lincoln Police Department, Lincoln, Lancaster County, Nebraska, any and all law enforcement officers, and agents thereof.

WHEREAS, Patrick Sullivan 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.

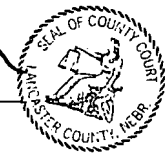
THEREFORE, you are commanded to search and seize the items as described in **Attachment A**, hereby attached and incorporated by reference, to include any specific authorization as contained in **Attachment A**.

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 31st day of May, 2024.



Judge of the County Court



Thomas E. Zumi

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:

- **PHONE IN A RED CASE**, 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 **Q2408380** and Case Number **C4-032267**.

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 **April 7, 2024** to **April 26, 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.
17. Wireless networks, Bluetooth, IP addresses, and synchronization connection history.
18. Memos and notes (typed and voice).
19. User dictionary.
20. Calendar information.
21. 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.

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.


Joseph makes an automated message plays explaining that the calls are recorded and monitored. Joseph calls Scott on April 17, 18, 19, 20, and 22 of 2024. During each call Joseph has Scott three-way call E.B. During these phone calls Scott sets up an application for E.B. and Joseph to communicate. During these calls Scott also talks about how the application is not working. On April 25, 2024 at approximately 10:15 AM Officer Dahlgren #1660 with the Lincoln Police Department contacts E.B. at her place of work. E.B. confirms Scott would three way call her so Joseph could talk to her. E.B. stated an application was also created so she could communicate with Joseph, but it did not work. E.B. stated she then had communication with Joseph through Instagram. E.B. stated Joseph wanted her to change her story.

On April 26, 2024 at approximately 1:31 PM, Scott was arrested and his phone was seized. I called the known listed number for Scott (402-460-1632) and the phone we had seized rang with my work number appearing on the screen. This phone was tagged into the Lincoln Police Department's property unit under Q2408380.

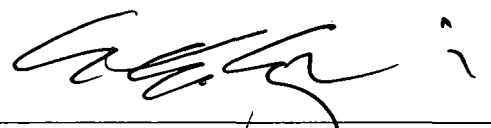
The above does constitute grounds of probable cause for the issuance of a search warrant to search and seize the evidence specifically identified in Attachment A, to include any specific authorization requested authorization to be ordered by the court.

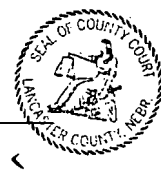
Further AFFIANT saith not;

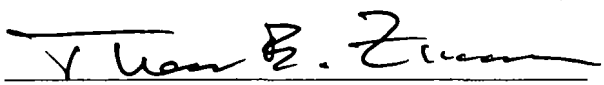
Dated this 31st day of May, 2024.

 #1804
Investigator P Sullivan #1804 AFFIANT

SUBSCRIBED to in my presence and sworn to before me this 31st day of May, 2024.


Judge of the County Court




Printed Name of Judge