

CR 24-1

IN THE COUNTY COURT OF LANCASTER COUNTY, NEBRASKA

IN THE MATTER OF THE)
SEARCH WARRANT FOR)
PROPERTY LOCATED IN THE)
LINCOLN POLICE)
DEPARTMENT PROPERTY)
UNIT, 575 SOUTH 10TH)
STREET, LINCOLN,)
LANCASTER COUNTY, NE)
Q2402078)

SEARCH WARRANT
RETURN

CLERK OF THE
DISTRICT COURT

2024 MAR 25 PM 4:20

LANCASTER COUNTY

STATE OF NEBRASKA)
COUNTY OF LANCASTER)

ss.

The undersigned states that he/she received the search warrant issued herein on the 25th day of February, 2024 and that he/she executed the same on the 16th day of March, 2024 seized the property/person described in the inventory filed herein and by delivering a copy of the said order for said property/person at the place from which the property/person was taken.

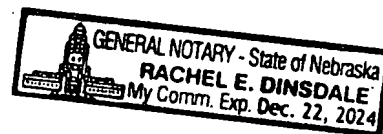
DATE this 21 day of March, 2024.

Zach Anshasi
Deputy Zach Anshasi

SUBSCRIBED AND SWORN to before me this 21st day of March, 2024.

Rachel E. Dinsdale
Notary Public

C4000930



[Handwritten mark]

IN THE COUNTY COURT OF LANCASTER COUNTY, NEBRASKA

IN THE MATTER OF THE)
SEARCH WARRANT FOR)
PROPERTY LOCATED IN THE)
LINCOLN POLICE DEPARTMENT)
PROPERTY UNIT, 575 SOUTH)
10TH STREET, LINCOLN,)
LANCASTER COUNTY, NE)
Q2402078)

INVENTORY

CLERK OF THE
DISTRICT COURT

2024 MAR 25 PM 4:21

LANCASTER COUNTY

STATE OF NEBRASKA)
) ss.
County of Lancaster)

Deputy Zach Anshasi being first duly sworn upon oath, deposes and states the following is an inventory of property seized by virtue of the warrant issued herein:

- Phone Contents from Samsung Galaxy Phone, Serial Number R5CT84873XE

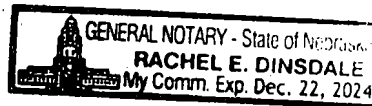
DATED this 21 day of March, 2024.

Zach Anshasi
Deputy Zach Anshasi

SUBSCRIBED AND SWORN to before me this 21st day of March, 2024.

Rachel E Dinsdale
Notary Public

C4000930



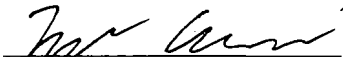
RECEIPT

The undersigned hereby acknowledges receipt of the following described property seized from LPD Property Unit, Property #: Q2402078 , Lancaster County, Nebraska:

Phone Contents from Samsung Galaxy Phone, Serial Number: R5CT84873XE

LANCASTER COUNTY
2024 MAR 25 PM 4:21
CLERK OF THE
DISTRICT COURT

DATED this ____ 16th ____ day of March, 2024.



Law Enforcement Officer

WITNESS

IN THE COUNTY OF LANCASTER COUNTY, NEBRASKA

STATE OF NEBRASKA)
COUNTY OF LANCASTER)

ss. SEARCH WARRANT

TO: Zach Anshasi a Deputy Sheriff with the Lancaster County Sheriff's Office , Lancaster County, Nebraska, and any and all law enforcement officers.

WHEREAS, Zach Anshasi has filed an Affidavit before the undersigned Judge of the County Court of Lancaster County, Nebraska, a copy of which affidavit is attached hereto and made a part hereof; 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 the Lincoln Police Department Property Unit, 575 S 10th Street, Lincoln, Lancaster County, Nebraska, for the following items:

Black Samsung Phone in a clear Pelican Case that is tagged in the Lincoln Police Department Property Unit under property number Q2402078 and case number C4000930

Evidence to be searched for includes:

- a. Evidence of other accounts associated with this device including email addresses, social media accounts, messaging "app" accounts, and other accounts that may be accessed through the digital device that will aid in determining the possessor/user of the device;
b. Evidence of use of the device to communicate with others about the above-listed crime(s), via email, chat sessions, instant messages, text messages, app communications, social media, internet usage, and other similar digital communications;
c. Photographs, images, videos, documents, and related data created, accessed, read, modified, received, stored, sent, moved, deleted or otherwise manipulated;
d. Evidence of use of the device to conduct internet searches relating to above listed crime(s);
e. Information that can be used to calculate the position of the device between the above dates, including location data; GPS satellite data; GPS coordinates for routes and destination queries between the above-listed dates; "app" data or usage

information and related location information; IP logs or similar internet connection information, and images created, accessed or modified between the above-listed dates, together with their metadata and EXIF tags;

f. Evidence of the identity of the person in possession of the device(s) and the associated times and dates. Such evidence may be found in digital communications, photos and video and associated metadata, IP logs, documents, social media activity, and similar data;

g. Records linking the suspect(s), co-conspirators, victim(s), witness(es) to a certain screen name, handle, email address, Social media identity, etc.;

h. Records showing a relationship with victim(s), location(s), other suspects, etc.;

i. Names, nicknames, account ID's, phone numbers, or addresses of specific persons;

j. Records showing a relationships to particular areas or locations.;

k. Photographs, images, videos, documents that contain or are evidence of above listed crime(s);

l. Evidence of purchases, such as items used in planning or carrying out above listed crimes(s);

m. Internet research history conducted while planning, executing, or covering up to commit above listed crimes(s);

n. Any live and deleted user attribution data including user accounts, e-mail accounts, passwords, PIN codes, patterns, account names, user names, screen names, remote data storage accounts, documents, files, calendars, metadata, recycle bin files, and any other information and evidence that may demonstrate attribution to a particular user or users;

o. Any live and deleted applications, programs, or software, used to facilitate the creation, storage, display, or transmission of digital visual recordings and the logs and data associated with the applications, programs or software, and any device backup files;

p. Any live and deleted audio or visual recording files including files bearing file extensions jpg, jpeg, png, gif, tif, wav, aiff, mp3, mp4, avi, mpg, mpeg, flv, mp4, mov, and wmv along with any descriptive metadata within or associated with the visual recording files, which may include date and time the recording was created, the device used to create the recording and location the recording was made;

q. Any live and deleted passwords, password files, keys, encryption codes, or other information necessary to access the digital device, software or data stored on the digital device;

r. Any live and deleted records, documents, programs, applications, information, or materials created, modified, or stored in any form on the digital devices listed in this affidavit, that show the actual user(s) of the computers or digital devices including web browser history; temporary Internet files; cookies, bookmarked or favorite web pages; e-mail addresses used from the computer; MAC IDs and/or Internet Protocol addresses used by the computer; e-mails, instant messages, text messages (SMS/MMS), application data and other electronic communications; address books; contact lists; records of social networking and online service usage; calendar entries, notes, journals, and any software that would allow others to control the digital device such as viruses, Trojan horses, malware, and other forms of malicious software.

Your AFFIANT would also like to advise the court that the examination of digital devices is a lengthy process requiring special steps to ensure the integrity of the electronic evidence. Therefore, it may not be possible to complete a return for the court within the 10 days normally required by the court

Given under my hand and seal this 25 day of February 2014



JUDGE OF THE COUNTY COURT

Jason Deval
Printed Name of County Court Judge



LANCASTER COUNTY

2024 MAR 25 PM 4:21

CLERK OF THE DISTRICT COURT

IN THE COUNTY COURT OF LANCASTER COUNTY, NEBRASKA

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

Zach Anshasi being first duly sworn upon oath deposes and states that he is a Deputy Sheriff for the Lancaster County Sheriff's Office, Lancaster County, Nebraska. AFFIANT further states he is currently involved in the investigation of the Violation of a Domestic Abuse protection order (42.924), occurring at 3151 Olive Creek Rd, Lancaster County, Nebraska. As part of the investigation, AFFIANT has consulted with other involved law enforcement and reviewed case reports. AFFIANT states as follows:

The item(s) to be searched for digital evidence are particularly described as:
a. 1 each, Black Samsung Phone in a clear Pelican Case , located in the Lincoln Police Property Evidence Unit at 575 South 10th , Lincoln, Lancaster County, NE, labeled with Property Number Q2402078 labeled with Case Number C4000930 ;

The items to be searched are currently located at the Lincoln Police Department Property Unit, 575 South 10th, Lincoln, Lancaster County, State of Nebraska. The item(s) to be searched shall be delivered to the Electronic Evidence Unit located at 605 South 10th, Lincoln, Lancaster County, State of Nebraska for digital forensic processing and analysis. The Electronic Evidence Unit forensic examiners may designate additional forensic services, as they may deem necessary to complete the analysis. Once examination and analysis has been completed, the listed evidence shall be returned to the Lincoln Police Department Property Unit, where it will be held until any final disposition by the Court

Facts:

On 02-03-2024, Deputies were dispatched to 3151 Olive Creek Rd reference a possible protection order violation in progress. While en-route to the residence, an NCJIS check revealed the reporting party, Joy Robinson, to

have an active/served protection order against her husband, Jason Robinson. Jason was served the protection order on 01-23-2024. The protection order prohibits Jason from telephoning, contacting, or otherwise communicating with the Joy, with no exceptions. The order also removes and excludes Jason from Joy's residence, regardless of the ownership of the residence, located at 3151 Olive Creek Rd Martell NE.

Upon arrival, Deputies cleared the property, including all outbuildings. Outside a large outbuilding, fresh tire tracks in the mud, leading from Olive Creek Rd. to approximately 10 feet from the building's door were observed. Deputies also obtained fresh discarded beer cans that were located near the tire tracks; one can was an empty crushed 12oz Budweiser beer can, and the other was an empty 12 oz can of Zip Line Copper Alt. beer.

Joy Robinson was contacted on the front porch of her residence. Joy informed Deputies she had not been near the shop in days. Joy also showed Deputies the refrigerator where her beer is stored, and neither kind of aforementioned beer was observed in the refrigerator. Joy informed Deputies that she had received multiple text messages from Jason within the last hour, as well as three missed calls. Joy showed Deputies the texts, including those which read 'at shop now' and 'Im sorry I love you.' The text messages were photographed. Joy stated that while she did not see Jason on the property, she did notice the motion activated light on the outbuilding come on earlier.

Investigation revealed Jason was staying with neighbors two properties to the west of Joy's residence. Upon arrival, Deputies observed a white 2008 Chevrolet Silverado bearing NE: ALP813 in the driveway. The vehicle was registered to Jason. Deputies also observed mud on the pickup and an incomplete six-pack of Zipline Copper Alt in the passenger seat.

Deputies then made contact with David and Lenore Drevo, owners of the property. The couple stated they believed Jason was on location in a basement bedroom. The Drevos gave consent for Deputies to enter the residence, where they located Jason supine on a bed in a basement bedroom. Deputies observed Jason to be heavily intoxicated due to his slurred speech, bloodshot

watery eyes, and the odor of alcohol that emitted from his breath and person. Jason seemed to have difficulty answering Deputies' questions, but, when asked, stated that no one else had access to his phone that he was aware of. When asked what Jason had to drink that night, he stated that he drank a Budweiser beer. Deputies also observed Jason to have mud on his right sock and pant leg. Jason could not locate his cellphone, and Deputies attempted to assist him by calling the phone number provided by Joy Robinson earlier. Jason provided Deputies permission to check his vehicle for his cellphone. The cellphone was located in Jason's vehicle on the center console, and observed to be ringing due to Deputies' calls.

At this point, Deputies confirmed the active protection order via LSO Records, and Jason was taken into custody and placed in the backseat of a marked patrol vehicle. Jason was then transported to the ADF where he was cited and lodged for violating a protection under AL7000311. Jason's cellphone was taken by Deputies and later tagged into LPD property.

Upon later investigation into Jason's jail calls, more evidence was obtained. On 02-03-2024 at approximately 14:35 hours, Jason made a call to his grandmother (Call ID # 114369077). At approximately 2:33 into the call, Jason can be clearly heard stating "I texted Joy and she called the police..." a short time later, Jason's grandmother stated "I thought she said you were at the shop?" to which Jason responded "I went down and looked at it, I was- I wasn't weak I was so upset because Kevin changed the fucking locks on the shop... she locked me out... so I did, I waited until everybody was in bed I just went down there and then I texted her"

On 02-03-2024 at approximately 20:55 hours, Jason made another call to the same phone number (Call ID # 114373783). At approximately 5:28 into the call, Jason stated "I can't lose my job, I mean realistically I just text Joy" to which Jason's grandmother responded "I can't speak to that right now."

On 02-04-2024 at approximately 15:42 hours, Jason made another call to the same phone number (Call ID # 114380659). At approximately 2:02 into the call, Jason stated "I'll just say this, this is what happened, I went out with my friend- Jason is then interrupted by his grandmother, who stated "you are being

recorded.” Jason responded by saying “I know, and I went through my attorney to get the tax stuff from Joy, so I texted her... nothing else happened, that was all.”

Digital Storage Devices

Your AFFIANT knows from training and experience that digital media devices and related digital storage devices, such as cell phones, can be used to create, edit, delete, share, and store files and other data including, live and deleted documents, photographs, videos, electronic mail (e-mail), search history and other relevant user information.

Your AFFIANT also knows from training and experience that computers and mobile devices, such as cell phones, connected to the Internet, are used to search the World Wide Web for content and such access can allow users to access and control data such as pictures, videos, documents, and other files.

Your AFFIANT also knows that such devices are often used to communicate and share data with other users and that such digital data can be transferred between various devices. Your AFFIANT knows that information associated with such data may show evidence of current, on-going, future, and past criminal activity. Your AFFIANT knows that this type of information can be used to identify and locate potential victims, witnesses, and co-conspirators.

Your AFFIANT also knows that data associated with these devices can often include user attribution data that can help identify the person(s) who sent, received, created, viewed, modified, or otherwise had control over particular content.

AFFIANT has been involved in investigations and has received training in various types of criminal investigations to include Protection Order Violations. Through your AFFIANT’s training and past experience, your AFFIANT is aware that cellular telephone data can provide valuable insight for Protection Order Violation investigations. Cellular telephones are used by the general public for communication, access to and sharing of information, research, socialization, entertainment, mapping, shopping, note taking and other functionality. Your AFFIANT knows from training and criminal investigation experience that individuals also use cellular telephones for the aforementioned purposes, and as a tool for facilitating criminal activity. The data

contained on cellular telephones seized in investigations can provide a wealth of information that can assist investigators 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. As such, a cellular telephone 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. Cellular telephones contain location data that can assist in an investigation by both corroborating and disproving statements. Cellular telephones can also show any possible relationships between parties involved through past communications, location data, and contact information stored.

Your AFFIANT is aware from past criminal investigation experience of numerous instances where cellular telephones were used by criminal participants to communicate via voice, text messaging, social media or other communication applications; instances in which criminal participants utilized cellular telephones to photograph themselves, associates and co-conspirators; instances in which cellular telephones were used by criminal participants to create videos of their criminal activity; instances where criminal participants have used cellular based internet applications to research crimes they have or intend to participate in; instances in which criminal participants have maintained notes within cellular telephones and instances in which criminal participants used global positioning, mapping and other location services to facilitate in- person meetings with co-conspirators or a victim;

Through your Affiant's training and criminal investigation experience examining cellular telephones, your Affiant is aware cellular telephones typically contain electronic records concerning calls made to, from, or missed by the cellular telephone. In addition, cellular telephones typically contain electronic records of text messages sent to and from the telephone, and other types of communication between persons. Cellular telephones typically contain a "phone book" of stored names and telephone numbers.

Through your Affiant's training and experience with examining digital devices, your Affiant is aware cellular telephones typically contain electronic records concerning calls made to, from, or missed by cellular telephone. In

addition, digital devices typically contain electronic records of messages sent to and from the device, and other types of communications between persons. Digital devices typically contain a “contact list” of stored names, telephone numbers, usernames, and accounts.

Your AFFIANT know evidence can remain on the device or media for indefinite periods of time after the communication originally took place, even if deleted by the user. A forensic examiner may be able to recover information deleted by the user throughout the working life span of the device.

Your AFFIANT knows 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.

Your AFFIANT knows, that, wholly apart from user-generated files and data, digital devices and media typically store, often without any conscious action by the user, electronic evidence pertaining to virtually all actions taken on the digital device, and often information about the geographic location at which the device was turned on and/or used. This data includes logs of device use; records of the creation, modification, deletion, and/or sending of files; and uses of the internet, such as uses of social media websites and internet searches/browsing.

Your AFFIANT knows device-generated data also includes information regarding the user identity at any particular date and time; usage logs and information pertaining to the physical location of the device over time; pointers to outside storage locations, such as cloud storage, or devices to which data may have been removed, and information about how that offsite storage is being used. If the device is synced with other devices, it will retain a record of that action. Digital device users typically do not erase or delete this evidence, because special software or use of special settings are usually required for the task. However, it is technically possible to delete this information.

Your AFFIANT knows digital devices can also reveal clues to other locations at which evidence may be found. For example, digital devices often maintain logs of connected digital or remote storage devices. A scanner or printer may store information that would identify the digital device associated with its use. Forensic

examination of the device can often reveal those other locations where evidence may be present.

Your AFFIANT knows, 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 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 the forensic examiner may also need the following items in order to conduct a thorough and accurate search of the devices: computer hardware, software, peripherals, internal or external storage devices, power supplies, cables; internet connection and use information; security devices; software; manuals; and related material.

Your AFFIANT knows, that searching the digital device itself would irreversibly alter data and/or evidence on the device. The commonly accepted best practice method to search a digital device for evidence involves creating a digital image of the device and then searching that image for the responsive evidence. Creating a forensic image does not alter any evidence on the device; it only copies the data into a searchable format. The image is then searched using search tools to locate and identify that evidence whose seizure is authorized by this warrant. The unaltered device and the image are then preserved in evidence.

Your AFFIANT knows modern digital devices and media can contain many gigabytes and even terabytes of data. Due to the potential for an extremely large volume of data contained in devices and media, and that fact that evidence can be stored/located in unanticipated locations or formats and/or embedded in other items stored on the device/media, investigators typically need to use specialized equipment in their search. Such large volumes of data also mean that searches can take days or even weeks to complete.

Your AFFIANT also requests authority to obtain assistance from a technical specialist, to review the digital device(s) and digital media for the best and least intrusive method of securing digital evidence that this warrant authorizes for seizure, and to assist in securing such evidence.

Based on all the foregoing information, there is probable cause to believe that evidence of the above-listed crimes exists in the above-described digital devices and that there is probable cause to search those devices for the evidence of the above crimes.

Your AFFIANT knows from my training and experience, and from information provided to me by Electronic Evidence Unit Personnel that 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, 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 allow for the analysis any associated data within a proper context. 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 before and to attribute particular users of a device and associated applications.

For the technical reasons described, the digital evidence listed above shall be submitted to the Electronic Evidence Unit located at 605 South 10th St, Lincoln, Lancaster County, State of Nebraska for digital forensic processing and analysis.

The above does constitute grounds of probable cause for the issuance of a Search Warrant for the Lincoln Police Department Property Unit at 575 S 10th Street , Lincoln, Lancaster County, Nebraska, for the following items:

A black Samsung Cellphone in a clear Pelican Case (and stored extraction) labeled under property number Q2402078.

Evidence to be searched for includes:

- a. Evidence of other accounts associated with this device including email addresses, social media accounts, messaging “app” accounts, and other accounts that may be accessed through the digital device that will aid in determining the possessor/user of the device;
- b. Evidence of use of the device to communicate with others about the above-listed crime(s), via email, chat sessions, instant messages, text messages, app communications, social media, internet usage, and other similar digital communications;
- c. Photographs, images, videos, documents, and related data created, accessed, read, modified, received, stored, sent, moved, deleted or otherwise manipulated;

d. Evidence of use of the device to conduct internet searches relating to above listed crime(s);

e. Information that can be used to calculate the position of the device between the above dates, including location data; GPS satellite data; GPS coordinates for routes and destination queries between the above-listed dates; “app” data or usage information and related location information; IP logs or similar internet connection information, and images created, accessed or modified between the above-listed dates, together with their metadata and EXIF tags;

f. Evidence of the identity of the person in possession of the device(s) and the associated times and dates. Such evidence may be found in digital communications, photos and video and associated metadata, IP logs, documents, social media activity, and similar data;

g. Records linking the suspect(s), co-conspirators, victim(s), witness(es) to a certain screen name, handle, email address, Social media identity, etc.;

h. Records showing a relationship with victim(s), location(s), other suspects, etc.;

i. Names, nicknames, account ID’s, phone numbers, or addresses of specific persons;

j. Records showing a relationships to particular areas or locations.;

k. Photographs, images, videos, documents that contain or are evidence of above listed crime(s);

l. Evidence of purchases, such as items used in planning or carrying out above listed crimes(s);

m. Internet research history conducted while planning, executing, or covering up to commit above listed crimes(s);

n. Any live and deleted user attribution data including user accounts, e-mail accounts, passwords, PIN codes, patterns, account names, user names, screen names, remote data storage accounts, documents, files, calendars, metadata, recycle bin files, and any other information and evidence that may demonstrate attribution to a particular user or users;

o. Any live and deleted applications, programs, or software, used to facilitate the creation, storage, display, or transmission of digital visual recordings and the logs and data associated with the applications, programs or software, and any device backup files;

p. Any live and deleted audio or visual recording files including files bearing file extensions jpg, jpeg, png, gif, tif, wav, aiff, mp3, mp4, avi, mpg, mpeg, flv,

mp4, mov, and wmv along with any descriptive metadata within or associated with the visual recording files, which may include date and time the recording was created, the device used to create the recording and location the recording was made;

q. Any live and deleted passwords, password files, keys, encryption codes, or other information necessary to access the digital device, software or data stored on the digital device;

r. Any live and deleted records, documents, programs, applications, information, or materials created, modified, or stored in any form on the digital devices listed in this affidavit, that show the actual user(s) of the computers or digital devices including web browser history; temporary Internet files; cookies, bookmarked or favorite web pages; e-mail addresses used from the computer; MAC IDs and/or Internet Protocol addresses used by the computer; e-mails, instant messages, text messages (SMS/MMS), application data and other electronic communications; address books; contact lists; records of social networking and online service usage; calendar entries, notes, journals, and any software that would allow others to control the digital device such as viruses, Trojan horses, malware, and other forms of malicious software.

Evidence to be searched for includes all aforementioned from 0000 hours on 02-02-2024 to 1200 hours on 02-04-2024

Your AFFIANT would also like to advise the court that the examination of digital devices is a lengthy process requiring special steps to ensure the integrity of the electronic evidence. Therefore, it may not be possible to complete a return for the court within the 10 days normally required by the court

Further AFFIANT saith not;

Dated this 25 day of February, 2024.

Zach Anshasi
Zach Anshasi, AFFIANT

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

[Signature]
Judge of the County Court

Josiah Davis
Printed Name of Judge

