

LPD Case Number: C4-011086

IN THE COUNTY COURT OF LANCASTER COUNTY, NEBRASKA

CR24-1

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

SEARCH WARRANT RETURN

LANCASTER COUNTY
2024 APR - 9 PM 3: 52
CLERK OF THE
DISTRICT COURT

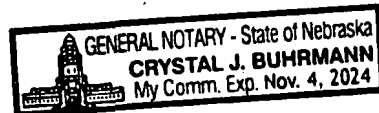
STATE OF NEBRASKA)
)
COUNTY OF LANCASTER)
 ss.

The undersigned states that he received the Search Warrant issued herein on the 29th day of March, 2024, and that he executed the same on the 5th day of April, 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.

Corey Weinmaster #883
Corey Weinmaster #883

SUBSCRIBED to in my presence and sworn to before me this 5th day of
April, 2024.

Crystal J. Buhrmann
Notary Public



SL

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**

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

ss.

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

Robert Norton, 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 a search warrant at the premise of the Lincoln Police Department, 575 South 10th Street, Lincoln, Lancaster County, Nebraska.

Samsung Galaxy S22 under LPD Property Q2402482

- Call Log - 2726
- Chats - 1425
- Contacts - 6658
- Device Connectivity - 142
- Device Events - 72
- Device Users - 2
- Emails - 676
- Instant Messages - 656
- Locations - 3326
- Notes - 6
- Passwords - 908
- Searched Items - 116
- SIM Data - 9
- Social Media - 1098
- User Accounts - 251
- User Dictionary - 9309
- Web Bookmarks - 23
- Web History - 16749
- Wireless Networks - 10
- Audio - 182
- Documents - 5

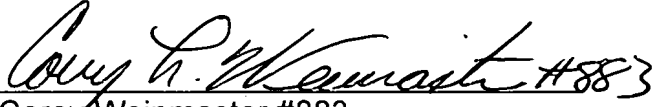
LANCASTER COUNTY
2024 APR - 9 PM 3:52
CLERK OF THE
DISTRICT COURT

- Images - 39788
- Videos - 654

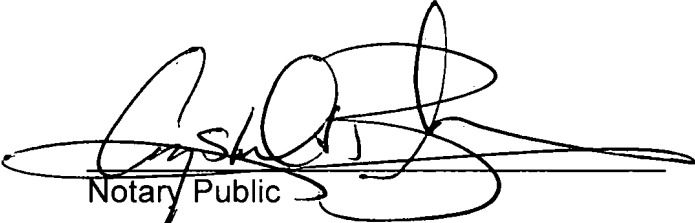
Samsung Galaxy Tablet under LPD Property Q2402370

- Call Log - 702
- Chats - 201
- Device Connectivity - 9
- Device Units - 100
- Device Users - 1
- Devices - 2
- Emails - 574
- Locations - 382
- Passwords - 832
- Searched Items - 79
- SIM Data - 7
- Social Media - 266
- User Accounts - 45
- User Dictionary - 1287
- Web Bookmarks - 14
- Web History - 11329
- Wireless Networks - 2
- Documents - 7
- Images - 3198
- Videos - 110

Inventory made in the presence of Derek Dittman #1551.


Corey Weinmaster #883

SUBSCRIBED to in my presence and sworn to before me this 8th day of
April, 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.

Samsung Galaxy S22 under LPD Property Q2402482

- Call Log – 2726
- Chats – 1425
- Contacts – 6658
- Device Connectivity – 142
- Device Events – 72
- Device Users – 2
- Emails – 676
- Instant Messages – 656
- Locations – 3326
- Notes – 6
- Passwords – 908
- Searched Items – 116
- SIM Data – 9
- Social Media – 1098
- User Accounts – 251
- User Dictionary – 9309
- Web Bookmarks – 23
- Web History – 16749
- Wireless Networks – 10
- Audio – 182
- Documents – 5
- Images – 39788
- Videos – 654

LANCASTER COUNTY
2024 APR -9 PM 3:52
CLERK OF THE
DISTRICT COURT

Samsung Galaxy Tablet under LPD Property Q2402370

- Call Log – 702
- Chats – 201
- Device Connectivity – 9
- Device Events – 100
- Device Users – 1
- Devices – 2
- Emails – 574
- Locations – 382
- Passwords – 832
- Searched Items – 79

- SIM Data – 7
- Social Media – 266
- User Accounts – 45
- User Dictionary – 1287
- Web Bookmarks – 14
- Web History – 11329
- Wireless Networks – 2
- Documents – 7
- Images – 3198
- Videos – 110

Date 4/5/24

Cory L. Stewart #883
Law Enforcement Officer

Witness  1551

IN THE COUNTY OF LANCASTER COUNTY, NEBRASKA

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

TO: Robert Norton, a Police Officer with the Lincoln Police Department, Lancaster County, Nebraska, and any and all law enforcement officers.

WHEREAS, Robert Norton, 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 Lincoln, Lancaster County, Nebraska, for the following items:

- a. 1 each, Samsung, electronic tablet, located in the Lincoln Police Property Evidence Unit at 575 South 10th. Lincoln, Lancaster County, NE, labeled with Property Number Q2402370 labeled with Case Number C4-011086 ;
- b. 1 each, Samsung, electronic smartphone, located in the Lincoln Police Property Evidence Unit at 575 South 10th. Lincoln, Lancaster County, NE, labeled with Property Number Q2402482 labeled with Case Number C4-011086;

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,

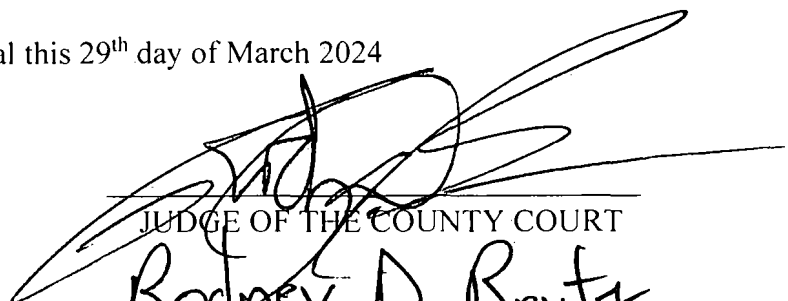
mp4, mov, and wmv along with any descriptive metadata within or associated with the visual recording files, which may include date and time the recording was created, the device used to create the recording and location the recording was made;

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 29th day of March 2024



JUDGE OF THE COUNTY COURT
Rodney D. Rantz

Printed Name of County Court Judge



IN THE COUNTY COURT OF LANCASTER COUNTY, NEBRASKA

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

Robert Norton, being first duly sworn upon oath deposes and states that he is a Investigator for the Lincoln Police Department, Lancaster County, Nebraska. AFFIANT further states he is currently involved in the investigation of Child Abuse (Nebraska State Statue 28-707) and Possession of a Controlled Substance (Nebraska State Statue 28-416(3), occurring at 911 Washington Street #3, Lincoln, 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: (EXAMPLES)

- a. 1 each, Samsung, electronic tablet, located in the Lincoln Police Property Evidence Unit at 575 South 10th, Lincoln, Lancaster County, NE, labeled with Property Number Q2402370 labeled with Case Number C4-011086 ;
b. 1 each, Samsung, electronic smartphone, located in the Lincoln Police Property Evidence Unit at 575 South 10th, Lincoln, Lancaster County, NE, labeled with Property Number Q2402482 labeled with Case Number C4-011086;

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 February 6, 2024, at approximately 2153 hours, officers with the Lincoln Police Department and Lincoln Fire & Rescue personnel, were detailed to 911 Washington Street #3, Lincoln, Lancaster County, Nebraska, on a medical call after a 2-year-old child fell out of a 2nd floor window.

Upon officers' arrival inside the residence, they contacted Breanna Abbott, who was caring for her 4 children, including the 2-year-old male child who fell out the window, referred to hereafter as J.A. Breanna reported to officers that she was the only one home with her children when the incident involving J.A. occurred. However, Breanna's 10-year-old daughter, referred to hereafter as S.M., said two other adults were present in the residence when the accident occurred. Breanna changed her statement when she was advised of S.M.'s statement and said her two friends were present but left the residence approximately 2 hours prior to the accident. Breanna failed to identify these two adults.

Breanna provided verbal and written consent for officers to search her above-mentioned residence. Officers detected a strong odor of marijuana coming from inside the residence. While searching the north bedroom of the residence, officers located narcotics, including baggies with suspected methamphetamine residue and drug paraphernalia. The baggies were sent to the Nebraska State Patrol Laboratory for analysis, later yielding a positive confirmation for methamphetamine, a Schedule II narcotic.

Officers also located four electronic surveillance cameras and a Samsung tablet inside the residence. Your AFFIANT knows through training and experience that these types of cameras are capable of recording and storing data on user-controlled cloud-based storage. This data can be viewed and backed up to a smartphone and electronic tablet. The Samsung tablet was tagged into the Lincoln Police Departments Property Unit under property number Q2402370.

Breanna told officers that while inside her bedroom she heard J.A. crying. Breanna exited her bedroom and began looking throughout her residence for J.A. but could not locate him. A short time later, Breanna discovered an east living room window to be open, which had a couch placed directly below the window.

Ultimately, Breanna exited her residence and located J.A. lying on the grass. The window screen was on the ground, possibly suggesting that J.A. was climbing on the living room couch and fell out the window after pushing the

window screen to the already open window. Breanna entered the residence and called 911 after J.A. appeared unconscious and his breathing to be labored.

J.A. was transported to Bryan West Hospital, where he was discovered to have a skull fracture, requiring immediate advanced medical treatment at Children's Hospital in Omaha, Nebraska.

An Affidavit was filed for temporary custody of Breanna's four children, including J.A., placing the children in temporary custody of the Nebraska Department of Health and Human Services.

On February 8, 2024, Breanna agreed to meet with Investigator Robert Norton of the Lincoln Police Departments Special Victims Unit at the Lincoln Police Department Headquarters for an interview. Breanna was advised that she was not under arrest and free to leave at any time. Breanna said she understood and agreed to speak about the investigation involving J.A.

During the interview, Breanna identified the two friends who visited her residence the night of the incident involving J.A. as Jose Gonzalez and Mariah Kerr. Furthermore, Breanna stated that approximately 2 hours prior to J.A.'s fall from the window, she smoked meth in her bedroom with Jose and Mariah, while her children were home.

Breanna confirmed that she has 4 surveillance cameras inside her residence, and said the cameras are capable of recording. Breanna indicated she was viewing the children on a device, which she failed to identify, while smoking methamphetamine in her bedroom.

Breanna admitted to utilizing her smartphone and exchanging text messages with Jose about J.A.'s accident. Investigator Norton asked Breanna if she would voluntarily consent to a forensic extraction of her smartphone. Breanna signed the consent form; however, wrote, 'Fuck You', on the form. Your AFFIANT did not interpret this as consent, so the smartphone was seized and tagged into the Lincoln Police Department's Property Unit under property number.

On February 15, 2024, Investigator Norton interviewed Jose in Omaha, Nebraska. Jose confirmed that he visited Breanna's above-mentioned residence with Mariah on February 6, 2024. Jose stated that while smoking methamphetamine with Breanna in her bedroom, they heard J.A. crying. Breanna reportedly exited the bedroom and ultimately discovered that J.A. had fallen out of the living room window and onto the ground outside. Jose reported he had

smoked methamphetamine with Breanna before at her residence while Breanna's children were home.

Jose confirmed that Breanna has surveillance cameras inside her residence that she monitors utilizing her electronic tablet. He stated that after the accident, Breanna told Mariah that she erased the surveillance footage of the incident involving J.A. because she was smoking methamphetamine when it occurred. Jose also said he had text communication with Breanna after the accident, requesting that Breanna not tell the police he was there because he's on house arrest.

Breanna's four children, including J.A., later completed a hair follicle test after J.A.'s accident. All the children received a positive hair follicle test for the presence of methamphetamine.

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 child abuse and narcotic investigations. Through your AFFIANT's training and past experience, your AFFIANT is aware that cellular telephone data can provide valuable insight for child abuse and narcotic 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 knows 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:

a. 1 each, Samsung, electronic tablet, located in the Lincoln Police Property Evidence Unit at 575 South 10th. Lincoln, Lancaster County, NE, labeled with Property Number Q2402370 labeled with Case Number C4-011086 ;

b. 1 each, Samsung, electronic smartphone, located in the Lincoln Police Property Evidence Unit at 575 South 10th. Lincoln, Lancaster County, NE, labeled with Property Number Q2402482 labeled with Case Number C4-011086;

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.

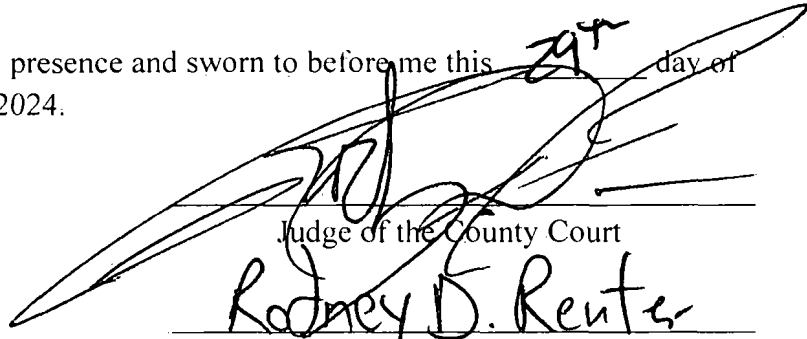
Further AFFIANT saith not;

Dated this 29th day of March 2024.



Robert Norton, AFFIANT

SUBSCRIBED to in my presence and sworn to before me this 29th day of March, 2024.



Judge of the County Court

Rodney D. Renter

Printed Name of Judge

