

IN THE COUNTY COURT OF LANCASTER COUNTY, NEBRASKA

IN THE MATTER OF THE SEARCH)
WARRANT OBTAINED FROM)
THE LANCASTER COUNTY SHERIFF'S)
OFFICE/ LINCOLN POLICE DEPARTMENT)
ELECTRONICS EVIDENCE UNIT, 605)
SOUTH 10TH STREET, LINCOLN,)
LANCASTER COUNTY, NE- Q2323415)
AND Q2321064)

OR 24-1

SEARCH WARRANT
RETURN

LANCASTER COUNTY

2024 JAN -4 PM 3:04

CLERK OF THE
DISTRICT COURT

STATE OF NEBRASKA)
COUNTY OF LANCASTER)

ss.

The undersigned states that he/she received the search warrant issued herein on the 24th day of October, 2023 and that he/she executed the same on the 24th day of October, 2023 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.

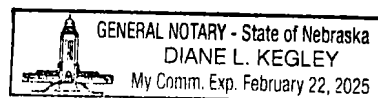
DATE this 2nd day of January, 2024.

Jeremy Schwarz
Deputy Jeremy Schwarz

SUBSCRIBED AND SWORN to before me this 2nd day of January, 2024.

Diane L. Kegley
Notary Public

C3007115



[Handwritten signature]

IN THE COUNTY COURT OF LANCASTER COUNTY, NEBRASKA

IN THE MATTER OF THE SEARCH)
WARRANT OBTAINED FROM)
THE LANCASTER COUNTY SHERIFF'S)
OFFICE/ LINCOLN POLICE)
DEPARTMENT ELECTRONICS)
EVIDENCE UNIT, 605 SOUTH 10TH)
STREET, LINCOLN, LANCASTER)
COUNTY, NE- Q2323415)
AND Q2321064)

INVENTORY

LANCASTER COUNTY
2024 JAN -4 PM 3:04
CLERK OF THE
DISTRICT COURT

STATE OF NEBRASKA)
) ss.
County of Lancaster)

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

- a. A full file extraction of the black Kyocera, Model 37110 (Duraforce Max) labeled with property number Q2323415 and case number C3007115
- b. A limited extraction of images from the black unknown make and model cellular phone labeled with property report Q2321064 and case number C3007115

DATED this 2nd day of January, 2024

Jeremy Schwarz
Deputy Jeremy Schwarz

SUBSCRIBED AND SWORN to before me this 2nd day of January, 2024.

Diane L. Kegley
Notary Public

C3007115



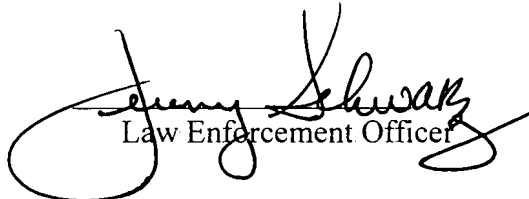
RECEIPT

The undersigned hereby acknowledges receipt of the following described property seized from the Electronic Evidence Unit located at 605 S. 10th Street, Lincoln, Lancaster County, Nebraska.

- a. A full file extraction of the black Kyocera, Model 37110 (Duraforce Max) labeled with Property Number Q2323415 and case number C3007115.
- b. A limited extraction of images from the black unknown make and model cellular phone labeled with Property Report Q2321064 and case number C3007115.

LANCASTER COUNTY
2024 JAN -4 PM 3:04
CLERK OF THE
DISTRICT COURT

DATED this 13th day of December, 2023.


Law Enforcement Officer


WITNESS

C3007115

IN THE COUNTY OF LANCASTER COUNTY, NEBRASKA

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

CLERK OF THE DISTRICT COURT

LANCASTER COUNTY
2021 JAN -4 PM 3:04

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

WHEREAS, Jeremy Schwarz, 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 Electronic Evidence Unit located at 605 S. 10th Street, Lincoln, Lancaster County, Nebraska, for the following items:

- a. A black Kyocera, Model 37110 (Duraforce Max) located in the Electronic Evidence Unit, 605 S. 10th Street, Lincoln, Lancaster County, Nebraska, and labeled with Property Number Q2323415 and case number C3007115.
- b. A black unknown make and model cellular phone located in the Electronic Evidence Unit, 605 S. 10th Street, Lincoln, Lancaster County, Nebraska and labeled with Property Report Q2321064 and case number C3007115.

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;

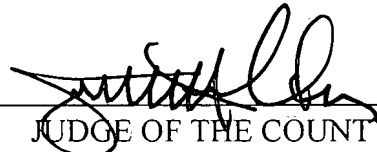
q. Any live and deleted passwords, password files, keys, encryption codes, or other information necessary to access the digital device, software or data stored on the digital device;

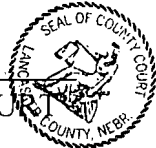
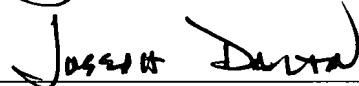
r. Any live and deleted records, documents, programs, applications, information, or materials created, modified, or stored in any form on the digital devices listed in this affidavit, that show the actual user(s) of the computers or digital devices including web browser history; temporary Internet files; 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 24 day of October, 2023



JUDGE OF THE COUNTY COURT



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)

Jeremy Schwarz, being first duly sworn upon oath deposes and states that he is a Investigator for the Lancaster County Sheriff's Office, Lancaster County, Nebraska. AFFIANT further states he is currently involved in the investigation of possession of child pornography N.R.S. 28-813.01, occurring at the Lancaster County Sheriff's Office located at 575 S. 10th Street, 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:

- a. A black Kyocera, Model 37110 (Duraforce Max) located in the Electronic Evidence Unit, 605 S. 10th Street, Lincoln, Lancaster County, Nebraska, and labeled with Property Number Q2323415 and case number C3007115.
- b. A black unknown make and model cellular phone located in the Electronic Evidence Unit, 605 S. 10th Street, Lincoln, Lancaster County, Nebraska and labeled with Property Report Q2321064 and case number C3007115.

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

CLERK OF THE
DISTRICT COURT
2024 JAN -4 PM 3:04
LANCASTER COUNTY

Facts:

On August 22, 2023, Deputies with the Lancaster County Sheriff's Office received intake number 01019750 from the Nebraska Department of Health and Human Services. The intake alleged that Jarrett Owens sent a nude image depicting his penis to a 12-year-old female herein referred to their initials, D.W.

Deputy Jason Brownell, an employee of the Lancaster County Sheriff's Office, currently assigned to the Patrol Division, spoke with Lisa Moser, a Coordinator for Services with Region V Health Systems. According to Lisa Moser, she began working with Carrie Wilson and her daughter, D.W., when D.W. began to struggle in school. Carrie Wilson felt that D.W. may also benefit from spending time with horses and thus she reached out to her friend, Jarrett Owens. According to Lisa Moser, she reached out to Carrie Wilson on August 19, 2023, and inquired about D.W. and her experience with horse riding. Lisa Moser learned Carrie Wilson discontinued the lessons because Jarrett Owens sent a 'dick pick' to D.W. on or about August 8, 2023.

According to investigative reports and conversations with Inv. Joanna Dimas, an employee of the Lancaster County Sheriff's Office who is actively investigating Jarrett Owens, Carrie Wilson, and D.W.'s current guardian, Scott Eiland, both spoke with Deputy Brownell. Scott Eiland stated that D.W. is his ex-stepdaughter. Scott Eiland has continued to care for D.W. and is her legal guardian due to D.W.'s biological father suffering from liver failure. Carrie Wilson lives with and cares for D.W.'s biological father during the week and spends weekends with D.W. and Scott Eiland. Scott Eiland also said that D.W.'s father is abusive towards D.W.

Furthermore, Carrie Wilson told Deputy Brownell that she had known Jarrett Owens for a period of approximately 11 years and had met through a mutual love for horseback riding. Carrie Wilson felt that riding horses would help D.W. to deal with the current turmoil in her life. Carrie Wilson asked Jarrett Owens to bring his horse to Waverly, Lancaster County, Nebraska for

D.W. to ride and he agreed. Jarrett Owens brought his horse to Waverly, Lancaster County, Nebraska on two separate occasions. When Jarrett Owens was unable to bring his horse to Waverly, Lancaster County, Nebraska, Carrie Wilson arranged for D.W. to go to Milford, Seward County, Nebraska to ride at Jarrett Owens' residence. D.W. then told Carrie Wilson she did not want to go because Jarrett Owens sent her a picture of his penis and she was uncomfortable. D.W. showed the photograph to Carrie Wilson and this was provided to Deputy Brownell.

Your AFFIANT knows Jarrett Owens voluntarily spoke with Inv. Joanna Dimas on September 9, 2023, at the Lancaster County Sheriff's Office located at 575 S. 10th Street, Lincoln, Lancaster County, Nebraska. Jarrett Owens told Inv. Dimas that he had agreed to bring his horse to Waverly, Lancaster County, Nebraska at the request of Carrie Wilson. Jarrett Owens and D.W. began to communicate via text message and Snapchat. Jarrett Owens would tell D.W. that he was there for her and would refer to her as "hun." Jarrett Owens told D.W. that he loved her and that she could confide in him. Jarrett Owens also confided in D.W. about his struggles with mental health. Jarrett Owens admitted that he sent a nude photograph with his exposed penis to D.W. but that he was intending to send them to an adult female ex-girlfriend. In the message with D.W. after sending the picture, Jarrett Owens tells D.W. "I was wanting to see a females body to do something".

Your AFFIANT knows Jarrett Owens gave Inv. Joanna Dimas written consent for a full file extraction of his cellular phone before leaving the Lancaster County Sheriff's Office. Your AFFIANT knows Inv. Tyler Loos, an employee of the Lancaster County Sheriff's Office and assigned to the Criminal Investigative Division Electronic Evidence Unit, conducted a full file extraction of Jarrett Owens Kyocera, Model 37110 (Duraforce Max) cellular phone. The phone number is 402-217-4400. The phone was returned to Jarrett Owens when the process was complete.

Your AFFIANT knows Inv. Joanna Dimas analyzed Jarrett Owens cellular phone and located approximately 15 separate images of Child Sexual Abuse Material. These images included adolescent females, nude or partially nude, adolescent females in sexually explicit poses and an adolescent male receiving fellatio from a nude, adult female.

On September 18th, 2023, Jarrett Owens voluntarily came to the Lancaster County Sheriff's Office and spoke to your AFFIANT. After he waived his constitutional rights, Jarrett Owens told your AFFIANT, that the images from his phone did appear to be of adolescent females. Jarrett Owens stated he views pornography daily and admitted that he views child pornography regularly. Jarrett Owens stated he uses a website called IMGSRU to view pornography and this pornography is of all ages, including adolescents, because he "enjoys the female body." Jarrett Owens told Investigator Schwarz that he knows the females are underage but that he "wouldn't do anything."

During the interview Jarrett Owens told your AFFIANT he lost his cellular phone i.e., the Kyocera, Model 37110 (Duraforce Max) cellular phone while horseback near Rock Creek Station, Fairbury, Jefferson County, Nebraska between 4:00 p.m. and 5:00 p.m., on Sunday, September 17, 2023.

Your AFFIANT knows on Tuesday, September 19, 2023, Inv. Joanna Dimas authored a search warrant for Jarrett Owens camper located at MidWest Feeding Company located at 851 238 Road, Milford, Seward County, Nebraska for any and all electronic devices capable of connecting to the internet, proof of occupancy, technology capable of video recording and/or photography, and any and all Child Sexual Abuse Material. The warrant was signed by a Lancaster County District Court Judge.

At 9:16 a.m., your AFFIANT and Inv. Joanna Dimas served the warrant at MidWest Feeding Company located at 851 238 Road, Milford, Seward County, Nebraska. Your AFFIANT located a black Kyocera phone in a hygiene bag next to the back door of the camper. Your AFFIANT and Inv. Joanna Dimas believed this was the same cellular phone Jarrett Owens claimed he lost. This

phone was placed into LPD Property and labeled with Report number Q2321064.

Your AFFIANT knows on or about September 30, 2023, Inv. Joanna Dimas learned Joesphine Owens-Hamilton, daughter of Jarrett Owens, received a phone call from Marci McGowan, Jarrett Owen's girlfriend. Marci McGowan informed Joesphine Owens she had her father's cellular phone and was going to send it to her.

On Monday, October 2, 2023, your AFFIANT contacted Joesphine Owens-Hamilton about the cellular phone and possible relevance to the case. Joesphine Owens agreed to turn it over to the Scotts Bluff County Sheriff's Office upon receipt and to have the Sheriff's Office mail the phone to Inv. Dimas.

On Saturday, October 7, 2023, Joesphine Owens-Hamilton informed your AFFIANT she had received the phone and would turn it over to her husband, Deputy Kale Hamilton, an employee of the Scotts Bluff County Sheriff's Office located at 1825 10th Street #5, Gering, Scotts Bluff County, Nebraska.

On October 11, 2023, your AFFIANT was contacted by Lt. Ray Huffman, Scotts Bluff County Sheriff's Office and informed Joesphine Owens-Hamilton turned the phone over to her husband, Dep. Kale Hamilton, and the phone is now in the hands of the Scotts Bluff County Sheriff's Office.

Your AFFIANT contacted Inv. Jordan McBride, an employee of the Gering Police Department located at 1025 P. Street, Gering, Scotts Bluff County, Nebraska and asked to mail the phone to Inv. Joanna Dimas. Your AFFIANT knows Inv. Joanna Dimas received the phone on October 16, 2023, she placed the phone into LPD Property and labeled the phone with Property Report number Q2323415.

Your AFFIANT knows on October 18, 2023, Inv. Loos examined both phones (Q2321064 and Q2323415) and discovered the phone located inside Jarrett Owens camper and inside his black hygiene bag at MidWest Feeding Company located at 851 238 Road, Milford, Seward County, Nebraska, is new and was not known to your AFFIANT or Inv. Joanna Dimas. Furthermore, your AFFIANT knows the Kyocera, Model 37110 (Duraforce Max) cellular phone that

Jarrett Owens claims he lost on Sunday, September 17, 2023, was the cellular phone mailed from Marci McGowan to Joesphine Owens-Hamilton and is the same phone that contained the Child Sexual Abuse Material identified by Inv. Dimas.

Your AFFIANT knows the Kyocera, Model 37110 (Duraforce Max) that was previously downloaded by Inv. Tyler Loos and later reportedly lost by Jarrett Owens was, in fact, not lost and was with Marci McGowan. Additionally, prior to the arrest of Jarrett Owens on September 18, 2023, Jarrett Owens was unaware investigators located child sexual abuse material.

Your AFFIANT is asking the court for authorization to conduct a full file extraction of the Kyocera, Model 37110 (Duraforce Max) to identify any new child sexual abuse material that may have been downloaded following the initially interview with Inv. Joanna Dimas on September 9, 2023.

Additionally, your AFFIANT is also asking the court for authorization to conduct a full file extraction of the black cellular phone located in Jarrett Owens hygiene bag found inside his camper parked at the MidWest Feeding Company located at 851 238 Road, Milford, Seward County, Nebraska during a search warrant on September 19, 2023.

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 possession of child pornography N.R.S. 28-813.01. Through your AFFIANT's training and past experience, your AFFIANT is aware that cellular telephone data can provide valuable insight for possession of child pornography N.R.S. 28-813.01 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 is currently located inside 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:

- c. A black Kyocera, Model 37110 (Duraforce Max) located in the Electronic Evidence Unit, 605 S. 10th Street, Lincoln, Lancaster County, Nebraska, and labeled with Property Number Q2323415 and case number C3007115.
- d. A black unknown make and model cellular phone located in the Electronic Evidence Unit, 605 S. 10th Street, Lincoln, Lancaster County, Nebraska and labeled with Property Report Q2321064 and case number C3007115.

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 relationship 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, usernames, 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;

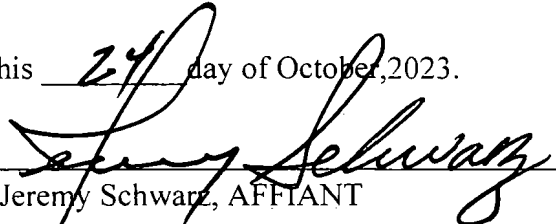
q. Any live and deleted passwords, password files, keys, encryption codes, or other information necessary to access the digital device, software or data stored on the digital device;

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

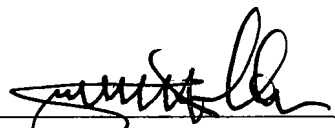
Further AFFIANT saith not;

Dated this 24 day of October, 2023.

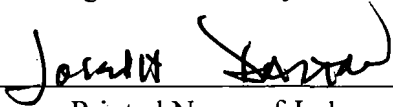


Jeremy Schwarz, AFFIANT

SUBSCRIBED to in my presence and sworn to before me this 24 day of October 2023.



Judge of the County Court



Printed Name of Judge

