

IN THE DISTRICT 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 10<sup>TH</sup> STREET, LINCOLN, )  
LANCASTER COUNTY, NE- )  
Q2401857 )

CR24-1

SEARCH WARRANT  
RETURN

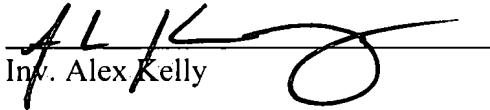
LANCASTER COUNTY  
2024 MAR -8 AM 10:09  
CLERK OF THE  
DISTRICT COURT

STATE OF NEBRASKA )  
COUNTY OF LANCASTER )

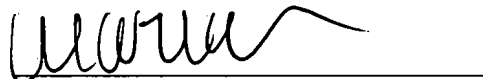
ss.

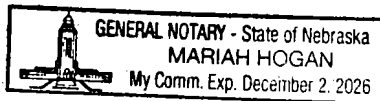
The undersigned states that he/she received the search warrant issued herein on the 16th day of February, 2024 and that he/she executed the same on the 29th day of February, 2024 seized the property/person described in the inventory filed herein and by delivering a copy of the said order for said property/person at the place from which the property/person was taken.

DATE this 1 day of March, 2024.

  
Inv. Alex Kelly

SUBSCRIBED AND SWORN to before me this 1 day of March, 2024.

  
Notary Public



C3009314



S

**RECEIPT**

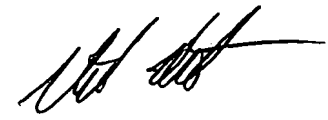
The undersigned hereby acknowledges receipt of the following described property seized from a grey colored android cellphone with black case having blue trim, assigned to case C4-008441 and property number Q2401857, in Lincoln, Lancaster County, Nebraska:

- Activity Sensor Data
- Applications
- Application Usage Log
- Archives
- Audio
- Calendar
- Call Log
- Cell Towers
- Chats
- Configurations
- Contacts
- Cookies
- Credit Cards
- Databases
- Device Connectivity
- Device Events
- Device Info
- Devices
- Documents
- Emails
- Exchange
- Images
- Installed Applications
- Instant Messages
- Journeys
- Locations
- Mobile Cards
- Notes
- Passwords
- Searched Items
- Shortcuts
- SIM Data
- Social Media
- Text
- Transfers
- Uploads
- User Accounts
- Videos
- Voicemails
- Web Bookmarks
- Web History
- Wireless Networks

**LANCASTER COUNTY**  
**2024 MAR -8 AM 10: 09**  
**CLERK OF THE DISTRICT COURT**

DATED this 29<sup>th</sup> day of February, 2024.

  
 \_\_\_\_\_  
 Law Enforcement Officer

  
 \_\_\_\_\_  
 Witness

IN THE DISTRICT COURT OF LANCASTER COUNTY, NEBRASKA

IN THE MATTER OF THE SEARCH )  
WARRANT OBTAINED FROM )  
THE LANCASTER COUNTY SHERIFF'S ) INVENTORY  
OFFICE/ LINCOLN POLICE )  
DEPARTMENT ELECTRONICS )  
EVIDENCE UNIT, 605 SOUTH 10<sup>TH</sup> )  
STREET, LINCOLN, LANCASTER )  
COUNTY, NE- Q2401857 )

STATE OF NEBRASKA )  
 ) ss.  
County of Lancaster )

Inv. Alex Kelly being first duly sworn upon oath, deposes and states the following is an inventory of property seized by virtue of the warrant issued herein:

- Activity Sensor Data
- Applications
- Application Usage Log
- Archives
- Audio
- Calendar
- Call Log
- Cell Towers
- Chats
- Configurations
- Contacts
- Cookies
- Credit Cards
- Databases
- Device Connectivity
- Device Events
- Device Info
- Devices
- Documents
- Emails
- Exchange
- Images
- Installed Applications
- Instant Messages

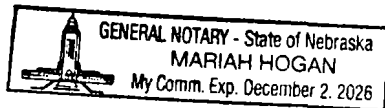
LANCASTER COUNTY  
2024 MAR -8 AM 10: 12  
CLERK OF THE  
DISTRICT COURT

- Journeys
- Locations
- Mobile Cards
- Notes
- Passwords
- Searched Items
- Shortcuts
- SIM Data
- Social Media
- Text
- Transfers
- Uploads
- User Accounts
- Videos
- Voicemails
- Web Bookmarks
- Web History
- Wireless Networks

DATED this 7 day of March, 2024.

AK  
Inv Alex Kelly

SUBSCRIBED AND SWORN to before me this 7 day of March,  
2024.



[Signature]  
Notary Public

C3009314



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

e. Information that can be used to calculate the position of the device around the time frame of the crime(s), 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 person(s);

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

k. Photographs, images, videos, and 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;

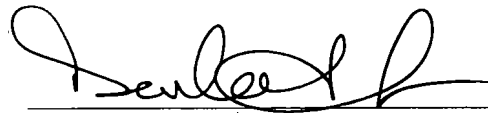
p. Any live and deleted audio or visual recording files including files bearing file extensions jpg, jpeg, png, gif, tif, wav, aiff, mp3, mp4, avi, mpg, mpeg, flv, mp4, mov, and wmv along with any descriptive metadata within or associated with the visual recording files, which may include date and time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

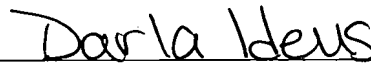
r. Any live and deleted records, documents, programs, applications, information, or materials created, modified, or stored in any form on the digital devices listed in this affidavit, that show the actual user(s) of the computers or digital devices including web browser history; temporary Internet files;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

This Court, being duly advised that the examination of digital devices is a lengthy process requiring special steps to ensure the integrity of the electronic evidence, finds 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 16 day of February, 2024.



JUDGE OF THE DISTRICT COURT



Printed Name of District Court Judge



IN THE DISTRICT COURT OF LANCASTER COUNTY, NEBRASKA

LANCASTER COUNTY  
2024 MAR - 8 AM 10: 12  
CLERK OF THE  
DISTRICT COURT

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

1. Alex Kelly, 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 a theft/fraud investigation, occurring in Lancaster County, Nebraska. As part of the investigation, AFFIANT has consulted with other involved law enforcement and reviewed case reports. AFFIANT states as follows:

2. The item(s) to be searched for digital evidence are particularly described as:

a. Black iPhone with blue iPhone case, associated with Lincoln Police Department case number C4-008441, and assigned property number Q2401857, located in the Electronic Evidence Unit, located at 605 South 10<sup>th</sup> St., Lincoln, Lancaster County, Nebraska.

3. The item to be searched is currently located in the Electronic Evidence Unit, located at 605 South 10<sup>th</sup> St., Lincoln, Lancaster County, Nebraska. The item to be searched shall remain in the Electronic Evidence Unit, located at 605 South 10<sup>th</sup> St., Lincoln, Lancaster County, Nebraska, for digital forensic processing and analysis. The Electronic Evidence Unit forensic examiners may designate additional forensic services as deemed 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.

### **THE RELEVANT FACTS**

4. On December 11, 2023, around 8:41 AM, Delaney Wiley called and reported a belated theft from motor vehicle with subsequent unauthorized use of financial transaction devices, which initiated from the parking lot at 2400 W. Van Dorn St., Lincoln, Nebraska (Vondra Vet Clinic), on 12/08/2023, sometime between approx. 7:30 AM and 1:30 PM. Wiley advised that her unlocked parked vehicle had been accessed by an unknown person(s) who removed her wallet which contained various items, including four bank cards. At the same time of the report from Wiley, another individual, April VanAndel reported her unlocked park vehicle at the same location and time frame was also accessed by an unknown person(s) who removed her wallet which contained various items, including three bank cards. The discovery of the theft came about when the victim(s) received notifications of unauthorized bank card transactions that occurred on December 8, 2023. No surveillance video is available of the theft from the motor vehicle(s).
5. Regarding the bank cards stolen from Wiley, unauthorized transactions were made at Target (8201 S 40th St., Lincoln, Nebraska) on 12/08/2023, between 1:38 PM and 1:55 PM, according to the transaction record from the store. During the unauthorized transactions, multiple gift cards were purchased, among other lesser valued items, for a total of \$910.20, using the stolen bank cards. An additional transaction was attempted, but was declined, for a total of 1030.00. These two transactions together totaled \$1940.20. Surveillance footage was obtained from Target, which showed the person responsible for

the transactions and an associated vehicle. Through investigation, the person responsible for using the bank cards at Target was identified as Lashana Westbrook, and an associated vehicle was identified as an unregistered 2010 Dodge Caliber VIN 1B3CB3HA3AD647963. Investigation also determined that Westbrook is the user of the vehicle.

6. Regarding the bank cards stolen from Vanandel, unauthorized transactions were made at Baker's (4405 N. 72<sup>nd</sup> St., Omaha, Nebraska) on 12/08/2023, between 5:33 PM and 5:37 PM, according to the transaction record from the store. During the unauthorized transactions, four separate transactions were made using one of the stolen bank cards, and all four transactions were successful. The items purchased included multiple gift cards and a bottle of soda. The first transaction was for \$2.39, the second transaction was for \$858.90, the third transaction was for \$963.90, and the fourth transaction was for \$456.95. These four transactions totaled 2,282.14. Surveillance footage was obtained from Baker's, which showed the person responsible for the transactions and an associated vehicle. The person responsible and the associated vehicle are believed to be the same person and vehicle as from the Target transaction, Lashana Westbrook and an unregistered 2010 Dodge Caliber.
7. Additionally, during the Baker's transaction, Westbrook is observed to receive a cellphone call which is recorded on surveillance footage. The cell phone display shows while Westbrook is holding the cell phone and has a name listed as the caller, which is indicative the caller is likely already saved in the contacts of the cell phone. The name displayed is not readily discernable, but is recognizable as a proper name not an unlisted number. The phone call is short in duration, and within a minute of the call taking place, an unidentified

female joined Westbrook at the register. The transaction(s) continue at the register with Westbrook and the unidentified female partaking together in the fraudulent transaction(s).

8. During follow-up investigation into the unauthorized use of the bank cards stolen from Wiley, an online transaction was made through online retailer Wayfair, using the illegally obtained gift cards from Target, on 12/08/2023. Transactions records were produced by Wayfair which showed the online transaction order method to be mobile web, which is indicative a mobile device such as a cell phone was used to place the order to Wayfair. Further information provided on the order form listed a phone number believed to be associated with Westbrook and an email address which shares naming similarities with Westbrook. The billing and shipping address listed on the transaction record is 3617 Baldwin Ave. #2, Lincoln, Nebraska, which was determined to be the current address for Westbrook through investigation techniques.
9. On January 31, 2024, around 8:45 PM, law enforcement conducted surveillance on Westbrook as part of an on-going criminal investigation to apprehend Westbrook for various criminal violations, including a flee to avoid arrest from 01/29/2024, stemming from her identification as the person responsible for multiple thefts and unauthorized credit card transactions. During this time, Westbrook was observed driving the unregistered 2010 Dodge Caliber VIN 1B3CB3HA3AD647963 around 33<sup>rd</sup> St. and Holdrege St., Lincoln, Nebraska. She stopped the vehicle and exited it near the intersection of 36<sup>th</sup> St. and Baldwin Ave. and was taken into custody for related cases. During a search incident to arrest, Inv. Gruber of the Lincoln Police Department, located a purse on her person and a cell phone inside the purse. The cell phone was described as a black iPhone in a blue case, and it was placed into evidence under LPD property report Q2401857. The cell phone was

later taken to the Electronic Evidence Unit for continued storage. The cell phone seized by Inv. Gruber has the same appearance and personalized background image on the screen as the cell phone observed in the Baker's surveillance footage being used by Westbrook during the unauthorized credit card transactions.

### **DIGITAL STORAGE DEVICES**

- 10.** Your affiant is a certified law enforcement officer in the state of Nebraska with nearly 14 years of experience investigating crimes including, but not limited to homicides, narcotics, sexual assaults, thefts, and burglaries. Your affiant is assigned to the Criminal Investigations Division of the Lancaster County Sheriff's Office and has received training and experience in technologically based investigative tools, including cellular telephones. Through such training and experience, your affiant understands the capabilities of cellular devices and the valuable information contained within pertaining to criminal investigations. Furthermore, most people possess cellular telephones and other connected devices (tablets, watches, laptops, etc.) used to communicate electronically. It can be generally recognized that cellular telephones tend to accompany their users everywhere, and thus, it may be inferred that a suspect's cell phone probably accompanied the suspect at the time of the crime.
- 11.** 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.
- 12.** Your AFFIANT also knows from training and experience that computers and mobile device, 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.

13. 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.
14. 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.
15. Your AFFIANT is aware 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 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.

16. 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;
17. Through 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. Digital devices typically contain a "contact list" of stored names, telephone numbers, usernames, and accounts.
18. 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.

**19.** 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 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.

**20.** 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.

**21.** 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.

22. 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.
23. 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.
24. Your AFFIANT knows the forensic examiner may also need the following items 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.
25. 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.

26. 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.
27. 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.
28. Your AFFIANT knows from my training and experience, and from information provided to me by Electronic Evidence Unit technical investigators 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.

29. Furthermore, has been recognized by the Nebraska Supreme Court that law enforcement cannot predict where evidence of a crime will be located in a cell phone or call records or in what format, such as texts, videos, photographs, emails, or applications. And it has been further stated that there is no way for law enforcement to know where in the digital information associated with cell phones it will find evidence of the specified crime. Consequently, a brief examination of all electronic data associated with a cell phone is usually necessary to find where the information to be seized is located, and such examination is reasonable under the Fourth Amendment.

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

31. Based on the foregoing information, the above does constitute grounds of probable cause for the issuance of a Search Warrant for Black iPhone with blue iPhone case, associated with Lincoln Police Department case number C4-008441, and assigned property number Q2401857, located in the Electronic Evidence Unit, located at 605 South 10<sup>th</sup> St., Lincoln, Lancaster County, Nebraska, for the following items:

**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, voice calls, 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 or transactions relating to above listed crime(s);

e. Information that can be used to calculate the position of the device around the time frame of the crime(s), 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 person(s);

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

k. Photographs, images, videos, and 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 16<sup>th</sup> day of February, 2024.

  
Alex Kelly, AFFIANT

SUBSCRIBED to in my presence and sworn to before me this 16 day of February, 2024.

  
JUDGE OF THE DISTRICT COURT

Darla Ideus  
Printed Name of District Court Judge