

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-)
Q2402278)

C224-1

SEARCH WARRANT
RETURN

LANCASTER COUNTY
2024 MAR 18 PM 4:03
CLERK OF THE
DISTRICT COURT

STATE OF NEBRASKA)
) ss.
COUNTY OF LANCASTER)

The undersigned states that he/she received the search warrant issued herein on the 1st day of March, 2024 and that he/she executed the same on the 8th day of March, 2024 seized the property/person described in the inventory filed herein and by delivering a copy of the said order for said property/person at the place from which the property/person was taken.

DATE this 16 day of March, 2024.

[Signature] 902254
Deputy Timothy Dowhower

SUBSCRIBED AND SWORN to before me this 16th day of March, 2024.



[Signature]
Notary Public

C3009415



S

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- Q2402278)

INVENTORY

LANCASTER COUNTY
2024 MAR 18 PM 4:03
CLERK OF THE
DISTRICT COURT

STATE OF NEBRASKA)
County of Lancaster) ss.
County of Lancaster)

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

- Data available up to the point of the first unlock from purple iPhone property number Q2402278

DATED this 16 day of March, 2024.

[Signature]
Deputy Timothy Dowhower

SUBSCRIBED AND SWORN to before me this 16th day of March, 2024.

[Signature]
Notary Public



C3009415

RECEIPT

The undersigned hereby acknowledges receipt of the following described property seized from a residence located at 605 S 10th Street, Lancaster County, Nebraska, in accordance with a Search Warrant issued therefore by the County Court, Lancaster County, Nebraska:

Before first unlock data from purple iPhone property number Q2402278.

LANCASTER COUNTY
2024 MAR 18 PM 4:03
CLERK OF THE
DISTRICT COURT

DATED this 8th day of March 2024.

[Signature] 902214
Affiant

Mariah Hogan
Witness

LANCASTER COUNTY
2024 MAR 18 PM 4: 03

CLERK OF THE
DISTRICT COURT

IN THE COUNTY OF LANCASTER COUNTY, NEBRASKA

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

TO: Deputy Timothy Dowhower 902214, a Deputy Sheriff with the Lancaster County Sheriff's Office , Lancaster County, Nebraska, and any and all law enforcement officers.

WHEREAS, Deputy Timothy Dowhower, 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 purple iPhone, 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, 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 1st day of March, 2024



JUDGE OF THE COUNTY COURT





Printed Name of County Court Judge

IN THE COUNTY COURT OF LANCASTER COUNTY, NEBRASKA

LANCASTER COUNTY
2024 MAR 18 PM 4:03
CLERK OF THE
DISTRICT COURT

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

Deputy Timothy Dowhower 902214 being first duly sworn upon oath deposes and states that he is a Deputy Sheriff for the Lancaster County Sheriff's Office, Lancaster County, Nebraska. AFFIANT further states he is currently involved in the investigation of four separate Flights to Avoid as well as multiple traffic infractions occurring at Hickman Road and Titan Drive, 68th Street and Princeton Road, 82nd Street and Bennett Road, and 82nd Street and Wittstruck Road in Lancaster County, Nebraska between 12-14-2023 and 2-6-2024. As part of the investigation, AFFIANT has consulted with other involved law enforcement and reviewed case reports for case numbers C3009415, C4000003, C4000793, and C4001009. AFFIANT states as follows:

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

1 purple iPhone, located in the Electronic Evidence Unit at 575 South 10th Street, Lincoln, Lancaster County, Nebraska, labeled with Property Number Q2402278 labeled with Case Number C4001009;

The item to be searched is currently located at the Electronic Evidence Unit, 575 South 10th Street, Lincoln, Lancaster County, Nebraska. The item(s) to be searched shall be delivered to the Electronic Evidence Unit located at 605 South 10th Street, Lincoln, Lancaster County, 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 have 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 12-14-2023 AFFIANT observed a red sedan with 34 county plates westbound on Hickman Road between Titan Drive and Terrace View Drive traveling faster than the posted 35 mph speed limit. RADAR was activated which produced a strong steady tone, consistent with the vehicle's speed. RADAR displayed 63 mph. AFFIANT activated overhead lights and pulled into the traffic lane behind the vehicle. The vehicle accelerated into Hickman and turned south/left onto Conestoga Avenue and accelerated through this residential area. Due to narrow streets and parked cars a pursuit was not initiated. This incident is documented in case C3009415.

On 01-01-2024 Sgt. Bryant of the Lancaster Sheriff's Office was running stationary radar at the intersection of 82nd Street and Wittstruck Road. At approximately 0513 hours, Sgt. Bryant observed a southbound vehicle approaching at a high rate of speed. A clock of 68 mph in a 55 mph zone was obtained. As soon as Sgt. Bryant turned on his headlights, he observed the vehicle to accelerate at a high rate of speed as it passed, indicating to Sgt. Bryant it was going to flee. Sgt. Bryant turned on the vehicle and activated all emergency equipment. As Sgt. Bryant attempted to catch up with the southbound vehicle, its speeds were well in excess of 100 mph. Sgt. Bryant observed it to briefly brake at 82nd Street and Roca before running the stop sign. By the time Sgt. Bryant was able to safely clear the intersection of 82/Roca, he observed that the vehicle was well ahead, almost to Martell Road. Seeing the vehicle was not slowing and driving in a reckless manner, Sgt. Bryant terminated the pursuit at 82nd Street and Martell Road before the vehicle could reach Hickman. The pursuit lasted approximately 2 miles. The only description Sgt. Bryant could get of the vehicle was that it was a dark colored 4-door sedan covered in dirt. Sgt. Bryant also observed that the driver's side taillight was burnt out. This incident is documented in case C4000003.

On 1-29-2024, at approximately 0145 hours, Sgt. Bryant was running stationary radar at 82nd Street and Wittstruck Road. A northbound vehicle was clocked at 50 mph in a 55 mph zone; however, when it passed Sgt. Bryant could clearly see it matched the description of the red sedan from C4000003. Sgt. Bryant also noticed the distinctive faulty taillight on the driver's side. Sgt. Bryant attempted to catch up to the vehicle and noticed it was gaining speed. A same lane radar of 80mph was obtained. Before Sgt. Bryant ever activated his emergency lights the vehicle made an abrupt turn to go west on Bennet Road. Sgt. Bryant activated all emergency equipment and a pursuit was initiated. Speeds of approximately 85 mph were reached while travelling westbound on Bennet Road. The vehicle did slow down for the stop signs at 68th and 54th, but never came to a complete stop. The vehicle continued southbound on 54th from Bennet Road. Speeds reached approximately 110 mph. The vehicle did slow down for the 3-way stop at 54th and Bennet. This allowed Sgt. Bryant to catch up and observe the plate AGX629. The vehicle continued on S. 54th after not coming to a complete stop at 54/Roca. The vehicle continued south on 54th with speeds ranging from 55 - 90 mph. At one point, the vehicle travelled in the northbound lanes, but Sgt. Bryant could clearly see there was no traffic ahead. Once they reached 54/Hickman, the vehicle again slowed down, but violated the stop sign at 54/Hickman and continued east on Hickman Road. Due to the vehicle heading into Hickman, Sgt. Bryant terminated the pursuit and went westbound on Hickman Rd. This is clearly the same vehicle that has run from Sgt. Bryant and AFFIANT in the past and was fictitiously plated. AGX629 comes back to a 2014 Buick LaCrosse registered to an address on Eden Road.

On 02-06-2024 at approximately 0455 hours, while observing traffic near S. 96th Street and Panama Road, Deputy Ewbank with the Lancaster County Sheriff's Office saw a red

Cadillac pass his location traveling westbound on Panama. Deputy Ewbank started following the vehicle westbound on Panama and observed its taillights a good distance ahead of his vehicle. This vehicle had the same partially defective driver-side taillight as the related cases involving a similar vehicle fleeing traffic stops. While passing the railroad tracks near S. 82nd and Panama Deputy Ewbank was able to clock the Cadillac with his radar traveling 80-90 mph in the posted 55 mph zone. Due to the hills, Deputy Ewbank lost sight of the vehicle and eventually observed it turn southbound on S. 68th Street from Panama Road. Deputy Ewbank began attempting to catch up to the vehicle and activated his emergency lights and sirens just north of 68th/Princeton. The vehicle immediately braked and turned westbound on Princeton Road. At first, it appeared the vehicle was stopping but began taking off at a high rate of speed failing to yield to Deputy Ewbank's emergency lights. The vehicle was clocked with radar traveling westbound on Princeton between 70-85 mph until reaching the Princeton Cemetery at S 12th/ Princeton. The vehicle initially stopped in the drive of the cemetery but began driving away again, traveling northbound on S. 12th until it reached Hwy 77 and continued northbound. Eventually, the vehicle turned westbound onto Broad Street and continued westbound through a field. Due to the muddy conditions, the pursuit was terminated. The vehicle was later located in the roadway at 25235 SW 29th Street unoccupied. A search of the area utilizing a Lincoln Police Department canine and drone was unsuccessful. The driver of the vehicle displayed the same driving behavior and disregard (speeding, violating stop signs, fleeing) as the driver of the three related case numbers involving the same fictitiously plated vehicle (maroon Cadillac sedan NE:34-B570). Of note, during a search of the vehicle, a bill of sale and title belonging to Clinton Hummer was located along with multiple court documents, and a daily planner with Hummer's name was found in the vehicle. Additionally, paperwork that is suspected to belong to Sarah Bowland (active Lancaster County warrant) was also found in the vehicle along with multiple pieces of female clothing. The vehicle was processed and towed to Midwest Towing.

A purple iPhone, property number Q2402278 was located inside the vehicle and was seized as evidence. This cell phone is believed to belong to the party responsible, Clinton Hummer. Other papers located inside the car indicate Hummer was in control of the vehicle. Data from this phone would help in the investigation, with location data on the above dates, as well as any communication in reference to contacts with law enforcement.

Officer Lancaster with Lincoln Police Department also had this vehicle flee a traffic stop on 01-18-2024. This incident is documented under LPD case number C4-004833.

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 criminal investigations, undercover narcotics investigations, child abuse investigations and cell phone forensics. Your AFFIANT has more than twenty years of law enforcement experience. Through your AFFIANT's training and past experience, your AFFIANT is aware that cellular telephone data can provide valuable insight for criminal and traffic investigations. Cellular telephones are used by the general public for communication, access to and sharing of information, research, socialization, entertainment, mapping, shopping, note taking and other functionality. Your AFFIANT knows from training and criminal investigation experience that individuals also use cellular telephones for the aforementioned purposes, and as a tool for facilitating criminal activity. The data contained on cellular telephones seized in investigations can provide a wealth of information that can assist investigators in determining identity and culpability of participants, including identifying those with knowledge of a criminal offense or identify those who have aided a criminal participant in the commission of a criminal offense. As such, a cellular telephone possessed by criminal participants can serve both as an instrument for committing crime as well as a storage medium for evidence of the crime, including communications to plan, execute, and otherwise document the commission of a crime. Cellular telephones contain location data that can assist in an investigation by both corroborating and disproving statements. Cellular telephones can also show any possible relationships between parties involved through past communications, location data, and contact information stored.

Your AFFIANT is aware from past criminal investigation experience of numerous instances where cellular telephones were used by criminal participants to communicate via voice, text messaging, social media or other communication applications; instances in which criminal participants utilized cellular telephones to photograph themselves, associates and co-conspirators; instances in which cellular telephones were used by criminal participants to create videos of their criminal activity; instances where criminal participants have used cellular based

internet applications to research crimes they have or intend to participate in; instances in which criminal participants have maintained notes within cellular telephones and instances in which criminal participants used global positioning, mapping and other location services to facilitate in-person meetings with co-conspirators or a victim;

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

Through your Affiant's training and experience with examining digital devices, your Affiant is aware cellular telephones typically contain electronic records concerning calls made to, from, or missed by cellular telephone. In addition, digital devices typically contain electronic records of messages sent to and from the device, and other types of communications between persons. Digital devices typically contain a "contact list" of stored names, telephone numbers, usernames, and accounts.

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

Your AFFIANT knows digital data can be found in numerous locations, and formats. Evidence can be embedded into unlikely files for the type of evidence, such as a photo included in a document or converted into a PDF file or other format in an effort to conceal their existence. Information on devices and media can be stored in random order; with deceptive file names; hidden from normal view; encrypted or password protected; and stored on unusual devices for the type of data, such as routers, printers, scanners, game consoles, or other devices that are similarly capable of storing digital data.

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

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

software or use of special settings are usually required for the task. However, it is technically possible to delete this information.

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

Your AFFIANT knows, as with other types of evidence, the context, location, and data surrounding information in the device data is often necessary to understand whether evidence falls within the scope of the warrant. This type of information will be important to the forensic examiner's ability to piece together and recognize evidence of the above-listed crimes.

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

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

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

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

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

Your AFFIANT knows from my training and experience, and from information provided to me by Electronic Evidence Unit Personnel that it is necessary to search live and deleted data recovered from digital devices from the time when the device was first used through the time when the device was seized. This is specifically necessary to establish associations between a particular device and associated applications and files to a particular user (or users). This scope of time is necessary to identify potential inculpatory and exculpatory evidence during the

planning, execution and post event activities of potential criminal activity. These activities may include communication, contact, calendar entries, pictures, videos, location information (including GPS, navigation, and maps), This scope of time is also necessary to determine accurate device date and time settings, including time zone changes, and allow for the analysis any associated data within a proper context. I know from my training and experience that it is important to understand events of a particular day and time in proper context that may exist before and to attribute particular users of a device and associated applications.

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

The above does constitute grounds of probable cause for the issuance of a Search Warrant for the purple iPhone property number Q2402278 located in the Electronics Evidence Unit Lincoln, Lancaster County, Nebraska, for the following items:

Location data, communications involving contact with law enforcement, pictures or video of law enforcement contacts

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.

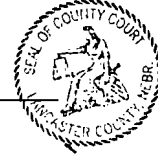
Further AFFIANT saith not;

Dated this March day of 1st, 2024.

[Signature] 902214
Deputy Timothy Dowhower 902214, AFFIANT

SUBSCRIBED to in my presence and sworn to before me this 1st day of March, 2024.

[Signature]
Judge of the County Court



[Signature]
Printed Name of Judge