

IN THE COUNTY COURT OF LANCASTER COUNTY NEBRASKA

STATE OF NEBRASKA)
) SS
COUNTY OF LANCASTER)

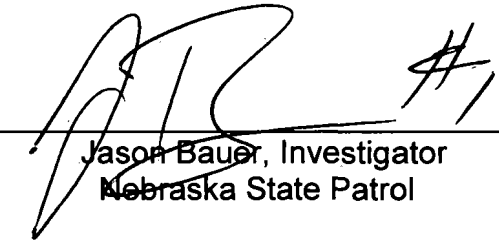
CR24-1

RETURN AND INVENTORY

Investigator Jason Bauer of the Nebraska State Patrol, being first duly sworn, deposes and says that, on this 2nd day of January, 2024, I served the warrant on the cell phone listed below. Inv. Bauer obtained the signed Search Warrant on November 30, 2023; after the warrant was signed, the phone was provided to the Nebraska State Patrol Technical Crimes Unit for download. Inv. Bauer was notified by Lisa Banks of the Nebraska State Patrol Technical Crimes Unit on December 19, 2023, that the download was complete for the device listed below.

- 1. A Samsung Cell phone with IMEI: 358997696318406 owned by Winter ALLEN.

DATED this 2nd day of January, 2024.


Jason Bauer, Investigator
Nebraska State Patrol

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




Notary

LANCASTER COUNTY
2024 JAN 11 PM 3:46
CLERK OF THE
DISTRICT COURT



002162734D02

5

IN THE COUNTY COURT OF LANCASTER COUNTY NEBRASKA

STATE OF NEBRASKA)
) SS
COUNTY OF LANCASTER)

LANCASTER COUNTY

2024 JAN 11 PM 3:46

SEARCH WARRANT
NSP23038899

CLERK OF THE
DISTRICT COURT

TO Nebraska State Patrol: Investigator Jason Bauer and all officers acting at his direction:

This matter came on for hearing on the 30th day of November, 2023, upon the sworn application and affidavit for issuance of a search warrant of Investigator Jason Bauer of the Nebraska State Patrol and the Court, being fully advised in the premises finds as follows:

That the Court has jurisdiction of this matter pursuant to the sections 29-812 through 29-821, Nebraska Revised Statutes as amended.

That the search warrant will be served on the following electronic devices: A Samsung Cell phone with IMEI: 358997696318406 owned by Winter ALEN.

That said property is concealed or kept in, on, or about the following described place or person, to-wit: the Nebraska State Patrol office Troop H Headquarters located at 4600 Innovation Drive, Lincoln, Lancaster County, Nebraska.

That based upon the sworn affidavit and application for issuance of a search warrant of Investigator Jason Bauer of the Nebraska State Patrol, dated the 30th day of November, 2023, that there is probable cause to believe that concealed or kept in the aforementioned electronic devices, hereinafter described, the following property, to-wit:

Sent, received, or stored digital data which would result in the seizure of evidence relating to a criminal investigation as required by Nebraska State Statute 29-1401 (in-custody death). including but not limited to:

1. All visual depictions of sent and/or received files (including but not limited to still images, videos, films or other recordings) or other computer graphic files which are evidence of manufacture, distribute, deliver, dispense, or possess with intent to manufacture, distribute, deliver, or dispense a controlled substance.
2. Any and all electronic data contained in the cellular phones, including any names, co-conspirators, associates, phone numbers, addresses, contact information, data, text messages, images, voice memos, photographs, videos, internet sites, internet access, documents, emails and email accounts, social media accounts, cloud storage accounts, or other information, ledgers, contained in the cellular phone internal, external or removable memory or memories, which includes any smart cards, SIM cards or flash cards.
3. Any and all computer passwords and other data security devices designed to restrict access to or hide computer software, documentation, or data. Data security devices may consist of hardware, software, or other programming code.
4. Any and all documents, records, emails, and internet history (in documentary or electronic form) pertaining to a criminal investigation as required by Nebraska State Statute 29-1401 (in-custody death) whether transmitted or received.
5. Any and all records, documents, invoices, notes and materials that pertain to accounts with any Internet Service Provider, including but not limited to social media accounts, cloud storage accounts, and email

accounts, as well as any and all records relating to the ownership or use of the computer hardware, digital device and/or digital media account.

6. Digital documents and records regarding the ownership and/or possession of the searched property.

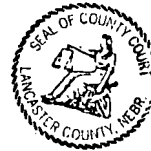
During the course of the search, photographs of the searched property may also be taken to record the condition thereof and/or the location of items therein.

YOU ARE, THEREFORE, ORDERED, with the necessary and proper assistance, to search the afore described location and/or person, for the purpose of seizing and searching the before described computers and/or digital devices, information/files, and if found, to seize and deal with the same as provided by law, and to make return of this warrant to me within thirty days after the date thereof.

IT IS FURTHER ORDERED, that execution of the Search Warrant be forthwith during DAY TIME HOURS.

IT IS FURTHER ORDERED, that Nebraska State Patrol, Investigator Jason Bauer, make return of this Search Warrant to me within Sixty days after the date hereof.

GIVEN under my hand this 30th day of November, 2023.





Judge

IN THE COUNTY COURT OF LANCASTER COUNTY NEBRASKA

STATE OF NEBRASKA
COUNTY OF LANCASTER

LANCASTER COUNTY AFFIDAVIT AND APPLICATION
FOR ISSUANCE OF A
SEARCH WARRANT
NSP23038899
2024 JAN 11 PM 3:46
CLERK OF THE
DISTRICT COURT

The complaint and affidavit of Inv. Jason Bauer, Nebraska State Patrol, on this 30th day of November, 2023, who being first duly sworn, upon oath says:

Your affiant has been a sworn officer with the Nebraska State Patrol for 16 years and have been a certified Law Enforcement Officer in Nebraska for the past 23. In your affiants Law Enforcement career, he has been a certified Police Canine Handler and Uniformed Officer. Since 2015, your affiant has been an investigator with the Nebraska State Patrol assigned to the Criminal/Drug Division. During your affiant's career with the Nebraska State Patrol, your affiant has had the opportunity to investigator a wide variety of criminal and drug cases. Your affiant is also a member of the TRIDENT (Tri-Cities Drug Enforcement Team), and in that capacity has been deputized buy the Federal Bureau of Investigation as a federal law enforcement officer.

Additionally, your affiant holds a Bachelor of Art Degree in Sociology from Hastings College. Furthermore, your affiant has received specialized training on a variety of topics to include violent crimes and death investigations. Your affiant is assigned to investigate criminal complaints in approximately 16 counties in central Nebraska, to include misdemeanor and felony offenses. Your affiant is also a member of the Nebraska State Patrol Special Investigations Team, and in commonly assigned to investigator officers involved shootings throughout the State of Nebraska.

Your affiant is presently assisting with an investigation of the death of JORGE LUIS SANTANA-RAMIREZ which occurred in Lancaster County, Nebraska on October 23, 2023. The circumstances surrounding this death led investigators to believe that this incident required the initiation of a criminal investigation as required by Nebraska State Statute 29-1401 (in-custody death).

That he has just and reasonable grounds to believe and does believe, that there is concealed or kept hereinafter described, the following property, to-wit:

Computers and/or digital devices/information/files, more fully described in **Attachment A**, including, sent and/or received digital data which would depict evidence pertaining to a criminal investigation as required by Nebraska State Statute 29-1401 (in custody death).

That said property is concealed or kept in, on, or about the following described place or person, to-wit: computers and/or digital devices/information/files, more fully described in **Attachment A**, located at 1600 Innovation Drive Lincoln, NE 68521, more fully described in **Attachment B**, under the care, custody and control of the Nebraska State Patrol Technical Crimes Unit.

That the following are the grounds for issuance of a search warrant for said property and the reasons for his belief, to-wit:

I am an Investigator with the Nebraska State Patrol. I am currently assigned to the Criminal/Drug Investigative Division located in Grand Island, NE. During my career with the Nebraska State Patrol, I have had the opportunity to conduct, coordinate and/or participate in investigations

relating to all types of crimes, to include, a criminal investigation as required by Nebraska State Statute 29-1401 (in-custody death).

Based on the information set forth below, your affiant has probable cause to believe that evidence of a criminal investigation as required by Nebraska State Statute 29-1401 (in custody death), is located at the Nebraska State Patrol Troop H Headquarters Office, more fully described in **Attachment B**.

I make this affidavit in support of an application for a search warrant of Cell phones, computers and/or digital devices/information/files, more fully described in **Attachment A**, contained within a Commercial Building, more fully described in **Attachment B**. There is probable cause to believe that the seizure of the cell phones, computers and/or digital devices/information/files and search of the computers and/or digital devices/information/files will result in the seizure of evidence relating to a criminal investigation as required by Nebraska State Statute 29-1401 (in-custody death).

The information contained within this affidavit is based upon information I have gained from my investigation, my personal observations, my training and experience, and/or information related to me by other law enforcement officers and/or agents. Since this affidavit is being submitted for the limited purpose of securing a search warrant, I have not included each and every fact known to me concerning this investigation. I have set forth the facts that I believe are necessary to establish probable cause to believe that there is evidence of a criminal investigation as required by Nebraska State Statute 29-1401 (in-custody death).

- On October 23, 2023, a Seward County Deputy was traveling on Interstate 80 near mile marker 382 in Seward County, Nebraska when they observed a silver Honda Civic traveling eastbound in excess of the posted 75 miles per hour speed limit. The deputy attempted to initiate a traffic stop at which time the vehicle failed to stop and a pursuit was initiated. The vehicle was believed to be occupied by two individuals. The vehicle came to a stop at which time a female passenger was observed exiting the vehicle as the male driver stayed within the driver seat of the vehicle.
- After reviewing the Deputy's body worn camera, as SANTANA-RAMIREZ stayed in the vehicle. The deputy stated he was unable to see SANTANA-RAMIREZ's hands and he believed SANTANA-RAMIREZ to be loading a possible weapon. Deputy instructed SANTANA-RAMIREZ to show his hands. SANTANA-RAMIREZ refused to comply with officers. The Deputy advises 'gun' and fires his duty issued weapon in the direction of the SANTANA-RAMIREZ. SANTANA-RAMIREZ was pronounced deceased at the scene.
- Your affiant along with other investigators the Nebraska State Patrol's Special Investigations Team were requested to investigate the officer involved shooting. Investigators applied for and received a search warrant to search the Honda Civic. The investigators served the search warrant and located items of evidentiary value to including one cell phone.
- Additionally, Investigators conducted an interview of the female passenger, identified as WINTER ALLEN. During this interview, Investigators located an additional cell phone, which ALLEN had in her possession at the time of the shooting.

Your affiant previously consulted with the Nebraska State Patrol Technical Crimes Unit and knows in prior cases, computers and other digital devices were seized and found to contain evidence and trace evidence identifying individuals and/or accomplices' pertaining to a criminal investigation as required by Nebraska State Statute 29-1401 (in-custody death). In cases outside of Nebraska, the

same techniques have been able to confirm through forensic examinations and confessions the same result.

As set forth above, there is probable cause to believe that some of the information for which this affidavit seeks authority to search is generated or stored on a cell phone, computer and/or digital devices. The affiant has requested the assistance of the Nebraska State Patrol Technical Crimes Unit and/or other law enforcement officers/entities to aid in the search and seizure of computers and computer-generated evidence. Conducting a search of a computer system, documenting the search, and making evidentiary and discovery copies is a lengthy process.

Your affiant knows that in prior cases, computers, computer equipment, cellular phones, and digital media were seized and found to contain evidence establishing ownership of the digital devices, involvement in criminal activity and ownership or use of any Internet service accounts, to include, social media accounts, cloud storage accounts, email accounts, credit card accounts, telephone accounts, correspondence and other identification documents.

Your affiant knows that digital media can contain a substantial amount of information relevant to the investigation of a case. Criminals often use digital devices/media, including, computers and cellular phones to communicate with accomplices and will sometimes store accomplices' contact information in a digital format. These communications can occur through electronic mail (email), instant messaging, text messaging, social media accounts, cloud storage accounts, and/or phone calls. To the extent that criminals use services such as phone services, email, instant messaging, social media accounts, cloud storage accounts, and/or text messages, these messages can sometimes be found on the digital media itself. Criminals also use cellular phones and other digital media to document criminal activities both by photographs, videos and digital memos. Your affiant knows that these photographs, videos and memos are also stored on the device itself. The digital information can also be located on the SIM (Subscriber Identity Module) which is a smart card located in the phone and also contains cellular network and phone information. Removable memories, including, flash cards/memory, are also sometimes located in cellular phones that allows the user to store vast amounts of electronic data.

Your Affiant knows that these digital devices can store a large number of digital data, including, photographs, videos, phone numbers and call history. Some digital devices can also contain contact information and calendar information and can be linked, either by wire or wireless, with computers. Camera phones can contain images and videos. This information can be valuable evidence in determining other participants in a criminal enterprise. Likewise, your affiant knows that images in a camera can contain evidence of where a subject has been and with whom the subject has associated.

Your affiant knows from training and professional and personal experience that computers, computer equipment, cellular phones, and digital media are personal items. These items have become an important part of a person's way to communicate, express themselves, and store digital data. They contain private conversations and the whereabouts of computers, computer equipment, cellular phones, and digital media are known to their owners at all times.

Your affiant knows from training and experience, and after previously consulting with the Nebraska State Patrol Technical Crimes Unit, that searches and seizures of computers, computer equipment, cellular phones, and digital media require investigators to perform an exhaustive search procedure of any and all the data, including, programs, directories, folders, sub-folders, files, and/or applications contained on computers, computer equipment, cellular phones, and digital media. This

exhaustive search includes a search of all digital data in allocated space (files accessible by the user) and/or unallocated space (files deleted or no longer used and not accessible by the user) and/or random access memory (RAM) or file slack on a computer, computer equipment, cellular phone or digital media, and can include, any and all digital files, digital file properties (metadata, exif data), and information that may have been created, viewed, modified, downloaded or copied during activity that has occurred since the computer, computer equipment, cellular phone or digital media was last booted. The search procedure of electronic data contained in computer hardware, computer software, cellular phone and/or digital data/memory storage devices may include the following techniques (the following is a non-exclusive list, as other search procedures may be used):

1. examination of all of the data contained in such computer hardware, computer software, and/or memory storage devices to view the data and determine whether that data falls within the items to be seized as set forth herein;
2. searching for and attempting to recover any deleted, hidden, or encrypted data to determine whether that data falls within the list of items to be seized as set forth herein (any data that is encrypted and unreadable will not be returned unless law enforcement personnel have determined that the data is not (1) an instrumentality of the offenses, (2) a fruit of the criminal activity, (3) contraband, (4) otherwise unlawfully possessed, or (5) evidence of the offenses specified above)
3. surveying various file directories and the individual files they contain;
4. opening files in order to determine their contents;
5. scanning storage areas;
6. performing keyword searches through all electronic storage areas to determine whether occurrences of language contained in such storage areas exist that are likely to appear in the evidence described in **Attachment A**; and/or
7. performing any other data analysis technique that may be necessary to locate and retrieve the evidence described in **Attachment A**.

Your affiant knows from training and experience, and after previously consulting with the Nebraska State Patrol Technical Crimes Unit, that dates and times (date stamp and/or time stamp), can be subjective until an exhaustive search procedure of any and all the data, including, programs, directories, folders, sub-folders, files, and/or applications contained on computers, computer equipment, cellular phones, and digital media has been completed. Dates and times can be altered, manipulated, added, or removed from computers, computer equipment, cellular phones, and digital media/digital data by, including, user preference, user time and date format, operating system, application, or software time and date format, automatic and/or manual operating system, application, or software updates. Your affiant knows from training and experience that an exhaustive search procedure of any and all the data, including, programs, directories, folders, sub-folders, files, and/or applications contained on computers, computer equipment, cellular phones, and digital media can establish a historical and current timeline for the individual using or in control of the computers, computer equipment, cellular phones, and digital media for a period of time, and can identify conspirators, co-conspirators, and witnesses during an investigation. Your affiant knows that digital data, including, messages, photographs and videos, can have date stamps and time stamps removed, modified, or corrupted when the digital data is deleted (move to unallocated space) and/or partially or entirely overwritten by other forms of digital data. Therefore, dates and times can be removed from, including, programs, directories, folders, sub-folders, files, and/or applications contained on computers, computer equipment, cellular phones, and digital media, and it is not feasible to limit the search and seizure of digital data to a date or time for the computer, computer equipment, cellular phones, and/or digital media. Investigators need to search and seize any and all data, more fully described in **Attachment A**, to determine if the digital data is relevant or irrelevant to

the investigation relating to testimony, corroborating evidence, a potential exhibit in the form of documentary material or demonstrative evidence.

Your affiant knows from training and experience, and after previously consulting with the Nebraska State Patrol Technical Crimes Unit, that allocated space (files accessible by the user) and unallocated space (files deleted or no longer used and not accessible by the user) contain digital data, including, programs, directories, folders, sub-folders, files, messages, photographs, videos, and/or applications contained on computers, computer equipment, cellular phones, and digital media. Your affiant knows from training and experience that individuals can delete digital data (unallocated space), including, programs, directories, folders, sub-folders, files, messages, photographs, videos, and/or applications contained on computers, computer equipment, cellular phones, and digital media. Your affiant knows that individuals use allocated space (usable data) and unallocated space (deleted data), in addition to legitimate purposes, to store, including, phone numbers, names, photographs, videos, and other information such as addresses, email addresses, instant messenger contact name(s), home and work addresses, and other information for contacting the corresponding individuals. Your affiant knows that this information is invaluable during the course of an investigation to establish conspirators, co-conspirators, and witnesses. Your affiant knows that individuals will delete digital data, therefore moving the digital data to unallocated (deleted) space in an attempt to hide, including, phone numbers, names, photographs, videos and other information such as addresses, email addresses, instant messenger contact name(s), home and work addresses, and other information in an attempt to avoid detection during an investigation. Your affiant knows that computers, computer equipment, cellular phones, and digital media may automatically move digital data to unallocated (deleted) space, including, programs, directories, folders, sub-folders, files, messages, photographs, videos and/or applications to create usable (allocated) space for more recently created, received, sent, viewed, or saved digital data. Your affiant knows that random access memory (RAM) and file slack can contain digital data created, viewed, modified, downloaded or copied during activity that has occurred since the computer, cellular phone or digital media was last booted. Your affiant knows that RAM and file slack can store, including, photographs, videos, messages, passwords, passcodes, recently typed information, and computer or cellular network connection information. Therefore, investigators are required to perform an exhaustive search procedure of any and all the data, including, allocated space (usable data), unallocated space (deleted data), random access memory (RAM) or file slack, including, programs, directories, folders, sub-folders, files, message, photographs, videos and/or applications contained on computers, computer equipment, cellular phones, and digital media to determine if the digital data is relevant or irrelevant to the investigation relating to testimony, corroborating evidence, a potential exhibit in the form of documentary material or demonstrative evidence.

Your affiant knows from training and experience, and after previously consulting with the Nebraska State Patrol Technical Crimes Unit, that computers, computer equipment, cellular phones, and digital media store information and interact with all software/hardware components of the computer, computer equipment, cellular phone, and digital media. Therefore, it is not feasible to limit the search and seizure of evidence to a specific location, file, folder, software and/or application of the computer, computer equipment, cellular phones, and/or digital media. Investigators need to search and seize any and all data, more fully described in **Attachment A**, to complete the examination of the digital device that may have data stored in several locations. When installing software and/or applications on a computer, computer equipment, cellular phone or digital media, applications will request permission, by default or with user preference, to interact with other software/hardware components of the computer, computer equipment, cellular phone or digital media. For example, when applications, including, Facebook, Twitter, Skype and SnapChat, are installed on a cellular phone, the applications interact with several different software/hardware components of the cellular

phone, including, messages, photographs, videos, contacts, calendars, gps, and operating system files. Furthermore, applications interact and are linked to other installed and/or un-installed applications. For example, applications including, Facebook and Instagram, interact and can share media directionally or bi-directionally across their respective software platforms and applications and/or directly with the digital device.

Your affiant knows from training and experience, and after previously consulting with the Nebraska State Patrol Technical Crimes Unit, that computers, computer equipment, cellular phones, and digital media contain factory installed and user installed software and applications, including, social media accounts, cloud storage accounts and email services that allow users to communicate outside of traditional short message service (SMS), multimedia message service (MMS) or phone call. Applications, including, Facebook, Twitter, Skype and SnapChat, allow users to initiate/receive phone calls, send/receive messages, photographs and videos, and transfer digital information/files between one or multiple users. These applications interact directly and indirectly with the computer, computer equipment, cellular phone or digital media's software/hardware, and the applications store digital information, including names, co-conspirators, associates, phone numbers, addresses, contact information, data, text, messages, photographs, voice memos, videos, internet sites, internet access, documents or other information, ledgers, contained in the computer, computer equipment or cellular phone internal, external or removable memory or memories, which includes any smart cards, SIM cards or flash card/drives, and/or contained in software or applications in the computer, computer equipment or cellular phone. Because of the way software/applications/hardware interact with computers, cellular phones and/or digital media, digital information can be generated, received and/or stored in an unlimited number of locations on the computer, computer equipment, cellular phone or digital media's, including, internal memory, external memory, removable memories, installed/un-installed software/applications, social media applications, cloud storage accounts, and email accounts.

Your affiant knows from training and experience that searches and seizures of evidence from computers, computer equipment, cellular phones, and digital media require agents to seize all items (hardware, software, passwords and instructions) to be processed later by a qualified computer expert in a laboratory or other controlled environment. Computer storage media which can be accessed by digital media to store or retrieve data can store the equivalent of thousands of pages of information. This storage medium includes: flash memory cards, compact flash cards and other similar storage medium, USB mini storage devices, micro hard drives, external hard drives, internal hard drives, and optical or mechanical storage.

Your affiant knows from training and experience that searching computers, computer equipment, cellular phones, and digital media for criminal evidence requires experience in the computer field and a properly controlled environment in order to protect the integrity of the evidence and recover even "hidden", erased, compressed, password-protected, or encrypted files. Since computer evidence is extremely vulnerable to tampering or destruction (from external sources or from destructive code imbedded in the system as a "booby trap"), the controlled environment of a laboratory is essential to its complete and accurate analysis.

Your affiant and experts have found through prior investigations, experience, and research that persons that utilize computers, computer equipment, cellular phones, and digital media almost always save information which can be forensically collected to identify the user and or other persons that may have come into contact with a specific piece of digital media, computer, computer equipment, and cellular phone.

Your affiant knows from training, experience, and research that computers used to access the Internet usually contain files, logs (including Internet Protocol Addresses) or file remnants which would tend to show ownership and use of the computer as well as ownership and use of Internet service accounts, including, social media accounts, email accounts, and cloud storage accounts, used for the Internet access and correspondence related to a criminal investigation as required by Nebraska State Statute 29-1401 (in-custody death).

Your affiant knows from training, experience, and research that mobile devices, including cellular phones, can be linked to social media accounts, email accounts, and cloud storage accounts, which enable the mobile device to manage the social media account, email account, and cloud storage account and upload digital data such as text, videos, and photographs.

Your affiant knows from training, experience, research, and general knowledge and use that individuals store digital data on their computers, computer equipment, cellular phones, and digital media. A summary, including, these storage locations, including, phone books, contacts, friends list, friends, recent calls, call history, maps, location services, global positioning system (GPS), emails, calendars, applications, messages, voicemails, photographs, videos, voice memos, Internet history, social media accounts, and cloud storage accounts, are described as follows. The following is a non-exclusive list for searching and seizing the items listed in **Attachment A**.

1. Phone Books/Contacts/Friends List/Friends - Your affiant knows that individuals use these types of contacts, in addition to legitimate purposes, to store phone numbers, names, and other information such as addresses, email addresses, instant messenger contact name(s), home and work addresses, and other information for contacting the corresponding individuals. Your affiant knows that this information is invaluable during the course of an investigation to establish conspirators, co-conspirators, and witnesses. Your affiant knows that contact information can be linked, synced and associated with other lists or databases of the computer, computer equipment, cellular phone or digital media, to include, photographs, videos, emails, social networking accounts and cloud storage accounts.
2. Recent Calls/Call History - Your affiant knows that individuals can use recent calls and call history on a computer, computer equipment, cellular phone or digital media, in addition to legitimate purposes, to store phone numbers, names, and other information such as email addresses, instant messenger contact name(s), and other information for contacting the corresponding individuals. Your affiant knows that this information is invaluable during the course of an investigation to establish conspirators, co-conspirators, and witnesses. Your affiant knows that recent calls and call history information can be linked, synced and associated with other lists or databases of the computer, computer equipment, cellular phone or digital media, to include, photographs, videos, emails, text messaging, picture messaging, social networking accounts and cloud storage accounts. You affiant knows that the call history can contain detailed records for dialed/sent calls and received calls. Your affiant knows that these records can be compared to subpoenaed records from telecommunication providers, and the call history may provide additional information that cannot be provided by a telecommunications provider.
3. Maps/Location Services/GPS - Your affiant knows that individuals use maps, location services, and GPS (factory installed and user installed), in addition to legitimate purposes, to identify, locate and document travel histories and points of interest on the computer,

computer equipment, cellular phone or digital media. The documentation can occur via default installed mapping applications, computer, computer equipment, cellular phone or digital media operating system default settings, or user installed mapping applications. The mapping application or settings may be documented within the specific application and also documented, linked, synced or associated with the computer, computer equipment, cellular phone or digital media. Your affiant knows maps, location services, and GPS can contain a detailed location history of the computer, computer equipment, cellular phone or digital media. Your affiant knows individuals can manually save specific points of interest as a favorite location (such as their home) and can permanently or temporarily save recently visited locations. Your affiant knows that some computers, computer equipment, cellular phones or digital media will attach location services data to, include, photographs, videos, social media accounts, and cloud storage accounts. Your affiant knows that this information is invaluable during the course of an investigation to establish conspirators, co-conspirators, and witnesses. Your affiant knows that location services can contain a substantial amount of digital information and documentation regarding the location of a crime or a timeline history during the commission of one or several criminal acts. Your affiant knows location services data has been used in all aspects of criminal investigations to establish where conspirators, co-conspirators, and witnesses were located during an investigation.

4. **Emails** – Your affiant knows that individuals use email accounts, in addition to legitimate purposes, to send messages, store phone numbers, names, and other information such as addresses, email addresses, instant messenger contact name(s), home and work addresses, and other information for contacting the corresponding individuals. Your affiant knows that this information is invaluable during the course of an investigation to establish conspirators, co-conspirators, and witnesses. Your affiant knows that email accounts can be linked, synced and associated with other lists or databases of the computer, computer equipment, cellular phone or digital media, to include, photographs, videos, contact lists, social networking accounts and cloud storage accounts. Your affiant knows that individuals will create fake email accounts to avoid revealing their true identity during an investigation. Your affiant knows that emails can contain attachments, including photographs and videos, that are linked, synced, or associated with other lists or databases of the computer, computer equipment, cellular phone or digital media.
5. **Calendars** – Your affiant knows that individuals use calendars, in addition to legitimate purposes, to store meetings, appointments, scheduled tasks. The calendar meetings, appointments, and scheduled tasks can include identifying information such as phone numbers, names, and other information such as addresses, email addresses, instant messenger contact name(s), home and work addresses, and other information for contacting the corresponding individuals. Your affiant knows that this information is invaluable during the course of an investigation to establish conspirators, co-conspirators, and witnesses. Your affiant knows that calendars can be linked, synced and associated with other lists or databases of the computer, computer equipment, cellular phone or digital media, to include, photographs, videos, emails, contact lists, social networking accounts and cloud storage accounts. Your affiant knows that individuals can keep track of meetings, appointments, and scheduled tasks and document those activities in a calendar style database or application.
6. **Applications** – Your affiant knows that individuals use applications (factory installed and user installed), in addition to legitimate purposes, to communicate with individuals and store

digital data. The communication can occur via voice, text message, instant message, picture message, or video conference, and copies of the voice or text communication may be documented within the specific application and also documented, linked, synced or associated with the computer, computer equipment, cellular phone or digital media. Applications that store digital data, including, text, emails, photographs, videos, and emails, can be used to backup data located on the computer, computer equipment, cellular phone or digital media. Your affiant knows these backups can contain current and historical evidence of a crime. Applications interact with the computer, computer equipment, cellular phone or digital media and can be used to link, sync, or associate digital data with social media accounts and cloud storage accounts. Applications can be used to hide digital data, such as photographs, videos and text, to avoid detection during an investigation. Your affiant knows that this information is invaluable during the course of an investigation to establish conspirators, co-conspirators, and witnesses. Your affiant knows that messaging services within applications can contain a substantial amount of digital information and communication documentation.

7. **Messages** - Your affiant knows that individuals use message features and messaging accounts, in addition to legitimate purposes, to communicate with individuals. The message feature and/or message account can contain text and/or embedded photographs, videos, and voice memos. The message feature or message accounts can contain phone numbers, names, and other information such as addresses, email addresses, instant messenger contact name(s), home and work addresses, and other information for contacting corresponding individuals. Your affiant knows that this information is invaluable during the course of an investigation to establish conspirators, co-conspirators, and witnesses. Your affiant knows that message features and messaging accounts can be linked, synced and associated with other lists or databases of the computer, computer equipment, cellular phone or digital media, to include, photographs, videos, emails, calendars, applications, contact lists, social networking accounts and cloud storage accounts. Your affiant knows that individuals will use applications to communicate with conspirators, co-conspirators, and witnesses during an investigation to avoid using traditional short message service (SMS) or multimedia message service (MMS).
8. **Voicemails/Voice Memos** - Your affiant knows that individuals use voice features and voice messaging accounts, in addition to legitimate purposes, to communicate with individuals. The voice feature and/or voice message account can contain speech-to-text, audio, and voice memos. The voice feature and/or voice message accounts can contain phone numbers, names, and other information such as addresses, email addresses, instant messenger contact name(s), home and work addresses, and other information for contacting corresponding individuals. This information may be retained temporarily or indefinitely depending on the type of voice message service (visual voicemail or traditional voicemail), and this information may automatically be translated into a text file or similar file by use of an application. Your affiant knows that this information is invaluable during the course of an investigation to establish conspirators, co-conspirators, and witnesses. Your affiant knows that voice features and voice messaging accounts can be linked, synced and associated with other lists or databases of the computer, computer equipment, cellular phone or digital media, to include, photographs, videos, emails, calendars, applications, contact lists, social networking accounts and cloud storage accounts. Your affiant knows that individuals can send a voice message to another individual without actually calling the individual. Your affiant knows voice features and voice messaging accounts can store voice memos to document a conspirators, co-conspirators, and witnesses activities and

locations during criminal activity.

9. **Photographs/Videos** – Your affiant knows that individuals use photographs and videos, in addition to legitimate purposes, to communicate with individuals and to document several aspects of criminal activity. Photographs and videos can contain metadata and exif data that provide time, date, location and the type of computer, computer equipment, cellular phone or digital device used for the respective photograph and/or video. Your affiant knows that this information is invaluable during the course of an investigation to establish conspirators, co-conspirators, and witnesses. Your affiant knows that photographs and videos can be linked, synced and associated with other lists or databases of the computer, computer equipment, cellular phone or digital media, to include, photographs, videos, emails, calendars, applications, contact lists, social networking accounts and cloud storage accounts. Your affiant knows that individuals send/receive, upload/download photographs and videos to document activities of conspirators, co-conspirators, and witnesses. Your affiant knows that photographs and videos can link several conspirators, co-conspirators, and witnesses to criminal activity because those conspirators, co-conspirators, and witnesses are present in a photograph or video.
10. **Social Media Accounts/Cloud Storage Accounts** - Your affiant knows that individuals use social media accounts and/or cloud storage accounts, in addition to legitimate purposes, to communicate with individuals and store digital data. The communication can occur via voice, text message, instant message, picture message, emails, or video conference, and copies of the voice or text communication may be documented within the social media account and/or cloud storage account and also documented, linked, synced or associated with the computer, computer equipment, cellular phone or digital media. Social media accounts and/or cloud storage accounts can be accessed via a traditional computer setup via the Internet, mobile device such as a cellular phone or tablet, or an application installed on a computer, computer equipment, cellular phone or digital media. Social media accounts and/or cloud storage accounts can contain digital data, including, text, emails, contacts, calendars, photographs, videos, and emails, and can be used to backup data located on the computer, computer equipment, cellular phone or digital media. Social media accounts and/or cloud storage accounts can be linked, synced, or associated with one or several computers, computer equipment, cellular phones, and digital media. Several computers, computer equipment, cellular phones, and digital media can be synced with one or several social media accounts and/or cloud storage accounts to ensure all synced devices contain “updated” and/or “real-time” information, including, photographs, videos, emails, contact lists, voicemails, calendars, and applications. Your affiant knows that this information is invaluable during the course of an investigation to establish conspirators, co-conspirators, and witnesses. Your affiant knows that social media accounts and/or cloud storage accounts, with or without the use of an application, can be used to evade detection during an investigation by storing digital data in another location.
11. **Internet History** - Your affiant knows that individuals use web browsers and/or applications, in addition to legitimate purposes, to communicate with individuals, store digital data, and conduct online browsing and research. Using web browsers or applications to access the Internet creates an Internet history. As is the case with most digital technology, communications by way of computer, computer equipment, cellular phone or digital media can be saved or stored on the computer, computer equipment, cellular phone or digital media used for these purposes. Storing this information can be intentional, i.e., by saving an email as a file on the computer, computer equipment, cellular

phone or digital media or saving the location of one's favorite websites in, for example, "bookmarked" files. Digital information can also be retained unintentionally, e.g., traces of the path of an electronic communication may be automatically stored in many places (e.g., temporary files or Internet Service Provider client software, among others). In addition to electronic communications, a computer, computer equipment, cellular phone or digital media user's Internet activities generally leave traces or "footprints" in the web cache and history files of the browser and/or application used. A forensic examiner can often recover evidence which shows that a computer, computer equipment, cellular phone or digital media was used to share files, and even some of the files which were uploaded or downloaded. Such information may be maintained indefinitely until overwritten by other data. The Internet history can also contain information, including, account passwords, email addresses, and search terms. Your affiant knows that this information is invaluable during the course of an investigation to establish conspirators, co-conspirators, and witnesses.

Your affiant is aware that the above described storage locations are a brief summary indicating how any and all visual depictions of sent and/or received files are intricately linked, synced, and/or associated to a computer, computer equipment, cellular phone or digital media. Since this affidavit is being submitted for the limited purpose of securing a search warrant, your affiant has not described each and every storage location and how those locations link, sync, and/or associate to a computer, computer equipment, cellular phone or digital media. Computers, computer equipment, cellular phones or digital media have hundreds, if not thousands, of operating system specifications/versions and compatible applications. It is not feasible to define each operating system or application associated with a computer, computer equipment, cellular phone or digital media, and the operating system or applications of a computer, computer equipment, cellular phone or digital media device may not be known until the examination is conducted. Your affiant knows that individuals can change default storage locations and/or access preferences for digital data and/or applications, including, photographs, videos, emails, contact lists, social networking accounts and cloud storage accounts on the computer, computer equipment, cellular phone or digital media.

Your affiant knows that searching and seizing a computer, computer equipment, cellular phone or digital media is similar to searching and seizing a residence. Your affiant knows residences, include, doors, windows, rooms, closets, hidden spaces, attics and garages. When searching a residence for evidence of a crime, your affiant searches the entire residence, including known and unknown spaces within the residence, to seize all evidence of a crime. Searching a computer, computer equipment, cellular phone or digital media is a similar process. Any and all areas containing digital information on a computer, computer equipment, cellular phone or digital media needs to be thoroughly searched to seize any and all evidence of a crime. Just as evidence can be moved from room to room, or moved to hidden spaces or containers within a residence, digital evidence can be moved to different locations, folders, files, hidden/encrypted areas, and/or allocated/unallocated space of the computer, computer equipment, cellular phone or digital media. As set forth in this affidavit, any and all digital evidence is intricately linked, synced and/or associated with computers, computer equipment, cellular phones or digital media, and only upon the discovery of digital evidence can a determination be made to whether the digital evidence is relevant or irrelevant to the investigation relating to testimony, corroborating evidence, a potential exhibit in the form of documentary material or demonstrative evidence.

The above information has led the affiant to believe that probable cause exists to believe that the items listed in the to be seized section, more fully described in **Attachment A**, of the search warrant application are evidence of a criminal investigation as required by Nebraska State Statute 29-

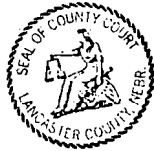
1401 (in-custody death).

Your affiant is aware that the recovery of data by a computer forensic analyst takes significant time; much the way recovery of narcotics must later be forensically evaluated in a lab, computers, computer equipment, cellular phones or digital media will also undergo a similar process. For this reason, the "return" inventory will contain a list of only the tangible items recovered from the premises. Unless otherwise ordered by the Court, the return will not include evidence later examined by a forensic analyst.

During the course of the search, photographs of the searched premises and/or items may also be taken to record the condition thereof and/or the location of items therein.

A warrant authorizing a day time search is requested.

WHEREFORE, he prays that a Search Warrant may issue according to law.



#1
Investigator Jason Bauer
Nebraska State Patrol

SUBSCRIBED AND SWORN TO before me this 30th day of November, 2023.


Judge

ATTACHMENT A

ITEMS TO BE SEIZED AND SEARCHED

Items:

- #50: Winter Alen Samsung cell phone, IMEI:358997696318406

50	Collection Date: 10/24/2023 16:14	#50- Winter Alen Samsung cell phone	IMEI 358997696318406 Collected by: BAUER Location: WINTER ALEN
----	---	-------------------------------------	--



including:

1. All visual depictions of sent and/or received files (including still images, videos, films or other recordings) or other computer graphic files which are evidence of a criminal investigation as required by Nebraska State Statute 29-1401 (in-custody death).
2. Electronic copies of log files, to include: emails, instant messaging, audio, still images, video recordings, chat logs, social media data, and digital cloud data stored on or about computer hardware. Computer hardware, that is, all equipment which can collect, analyze, create, display, convert, store, conceal, or transmit electronic, magnetic, optical, or similar computer impulses or data. Any and all hardware/mechanisms used for the receipt or storage of the same, including: any computer system and related peripherals, including data processing devices and software (including central processing units; internal and peripheral storage devices such as fixed disks, hard drives, tape drives, disk drives, transistor-binary devices, magnetic media disks, external hard drives, floppy disk drives and diskettes, routers, computer compact disks, CD-ROMS, DVD, usb storage devices and flash memory storage devices, and other memory storage devices); peripheral input/output devices (including keyboards, printer, video display monitors, scanners, digital cameras, optical readers, recording equipment, RAM or ROM units, acoustic couplers, automatic dialers, speed dialers, programmable telephone dialing or signaling devices, electronic tone generating devices, and related communications devices such as modems, cables and connections), as well as any devices, mechanisms, or parts that can be used to restrict access to computer hardware (including physical keys and locks).
3. Cellular phones including any and all electronic data contained in cellular phone, including any names, co-conspirators, associates, phone numbers, addresses, contact information, data, text, messages, images, voice memos, photographs, videos, internet sites, internet access, documents, emails and email accounts, social media accounts, cloud storage accounts, or other information, ledgers, contained in the cellular phone internal, external or removable memory or memories, which includes any smart cards, SIM cards or flash cards.
4. Any and all computer passwords and other data security devices designed to restrict access to or hide computer software, documentation, or data. Data security devices may consist of hardware, software, or other programming code.
5. Any and all documents, records, emails, and internet history (in documentary or electronic form) pertaining to a criminal investigation as required by Nebraska State Statute 29-1401 (in-custody death) whether transmitted or received.
6. Any and all records, documents, invoices, notes and materials that pertain to accounts with any Internet Service Provider, including social media accounts, cloud storage accounts, and email accounts, as well as any and all records relating to the ownership or use of the computer hardware, digital device and/or digital media account.
7. Digital documents and records regarding the ownership and/or possession of the searched premises.
8. During the course of the search, photographs of the searched premises may also be taken to record the condition thereof and/or the location of items therein.

ATTACHMENT B

LOCATION TO BE SEARCHED

4600 Innovation Drive, Lincoln, Lancaster County, Nebraska is described as the NEBRASKA STATE PATROL Troop H Headquarters Office.

