

IN THE COUNTY COURT OF LANCASTER COUNTY NEBRASKA

STATE OF NEBRASKA)
) SS
COUNTY OF LANCASTER)

RETURN AND INVENTORY
NSP23036206

CR241

Investigator Justin Davis, being first duly sworn, deposes and says that, on June 11, 2024, I served the within warrant at 5018 South 48th Street, Lincoln, Lancaster County, Nebraska and made a diligent search for the property described therein at the place, or person, mentioned therein, and seized and am in possession of the following described property, to-wit:

SEE ATTACHED INVENTORY FORM

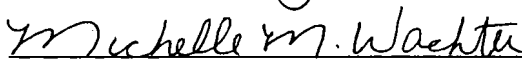
Said property was inventoried in the presence of Investigator Justin Davis and a copy of said Warrant and a receipt for said property was left at the residence.

Dated this 11th day of JUNE, 2024.


Inv. Justin Davis, Nebraska State Patrol

SUBSCRIBED AND SWORN TO before me this 11 day of June, 2024.




Notary

LANCASTER COUNTY
2024 JUN 11 PM 2:59
CLERK OF THE
DISTRICT COURT



254

NSP23036206

NEBRASKA STATE PATROL

Inventory of Vehicles, Dwellings or Buildings

Date 06/11/24 Charge/Reason Search Warrant Time 0635

Location Inventory Made 5018 S. 48th St. Lincoln NE

Vehicle: Make _____ Color _____ Year _____ Body Style _____

License: State _____ Number _____ VIN _____

Owner: _____ Address _____

Driver: _____ Address _____

No.	Item	No.	Item
1	Desktop Computer (Tower)		
2	USB Drive (unknown size)		
3	USB Drive (unknown size)		
4	Hard Drive (320 GB)		
5	Hard Drive (500 GB)		
6	Hard Drive (2TB)		
7	Cell Phone (Motorola Edge)		

LANCASTER COUNTY
CLERK OF THE
DISTRICT COURT
2024 JUN 11 PM 3:00

As provided in Nebraska Statute 60-4,110, this vehicle has been impounded for ten (10) days because the driver's license has been suspended, revoked, or impounded. The driver or an innocent interested person may obtain an administrative review of this impound by calling NSP Troop Area Office at _____

Copy received by Left At Residence

Witnesses:

N. Trantram #238
Signature of Officer

IN THE COUNTY COURT OF LANCASTER COUNTY NEBRASKA

STATE OF NEBRASKA)
) SS
COUNTY OF LANCASTER)

SEARCH WARRANT
NSP23036206

LANCASTER COUNTY
2024 JUN 11 PM 3:00
CLERK OF THE
DISTRICT COURT

TO NEBRASKA STATE PATROL OFFICER: INVESTIGATOR JUSTIN DAVIS

This matter came on for hearing on the 10 day of June, 2024, upon the sworn application and affidavit for issuance of a search warrant of Investigator Justin Davis 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 based upon the sworn affidavit and application for issuance of a search warrant of Investigator Justin Davis of the Nebraska State Patrol, dated the 10 day of June, 2024, that there is probable cause to believe that 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 visual depictions of sexually explicit conduct which would depict children as one of its participants or portrayed observers in violation of Nebraska State Statutes 28-813.01, 28-1463.03, and 28-1463.05.

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 5018 South 48th Street, Lincoln, Lancaster County, Nebraska, more fully described in **Attachment B**.

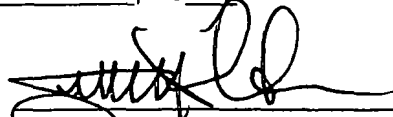
And, if found, to seize and deal with the same as provided by law, and to make return of this warrant to me within ten days after the date hereof.

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 ten days after the date thereof.

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

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

GIVEN under my hand this 10 day of June, 2024


Judge



ATTACHMENT A

ITEMS TO BE SEIZED AND SEARCHED

1. All visual depictions of sexually explicit conduct of sent and/or received files (including still images, videos, films or other recordings) or other computer graphic files which would depict children as one of its participants or portrayed observers.
2. Electronic copies of log files, including: 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 the possession, receipt or distribution of child pornography and/or visual depictions of sexually explicit conduct which would depict children as one of its participants or portrayed observers, or pertaining to an interest in child pornography and/or visual depictions of sexually explicit conduct which would depict children as one of its participants or portrayed observers 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

The location known as at the address of 5018 South 48th Street, Lincoln, Lancaster County, Nebraska is identified as follows:

The residence located at 5018 South 48th Street, Lincoln, Lancaster County, Nebraska is described as a single-family residence, with Light colored siding. On the mailbox are the numbers 5018. According to the Lancaster County Assessors website, the legal description is: SOUTH HAVEN HILLS, BLOCK 6, Lot 31. Any vehicles, outbuildings, campers on or adjacent to the aforementioned property that may be attributed to occupants of the home at the time of service may be searched along with the persons occupying the residence at the time of service.



IN THE COUNTY COURT OF LANCASTER COUNTY NEBRASKA

STATE OF NEBRASKA)
) SS
COUNTY OF LANCASTER)

**AFFIDAVIT AND APPLICATION
FOR ISSUANCE OF A
SEARCH WARRANT
NSP23036206**

LANCASTER COUNTY
CLERK OF THE DISTRICT COURT
2024 JUN 11 PM 3:00

10th day of JUNE, 2024, The complaint and affidavit of Investigator Justin Davis of the Nebraska State Patrol, on this day, who being first duly sworn, upon oath says:

Your affiant is a criminal investigator with 16 years of experience in law enforcement with the Nebraska State Patrol. He has completed 24 weeks of basic training at the Nebraska State Patrol Training Center in 2007/2008. Your affiant has attended several trainings since to include Internet Crimes Against Children Investigative Techniques in June 2011, EnCase® Computer Forensics I and II in July 2011 and February 2013, Fundamental of Cybercrime investigation in August 2011, Cell Phone Technology and Forensic Data Recovery by PATC Tech in January 2012, Internet Crimes Against Children Undercover Chat in May 2012, Peer to Peer data sharing in May 2012, the ARES Investigations training program, and the BitTorrent class in June 2020. Your affiant also attended in June 2023, the national Internet Crimes Against Children conference. He also attends annually in-service training provided by the Nebraska State Patrol. Your affiant also had the opportunity to observe and review numerous examples of child pornography in all forms and types of media including digital media. Your Affiant is a member of the Internet Crimes Against Children Taskforce. Your Affiant has attended training related to child exploitation including crimes involving computers used in the exploitation of children, including training related to the identification, collection, and preservation of computer related evidence.

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 visual depictions of sexually explicit conduct which would depict children as one of its participants or portrayed observers in violation of Nebraska State Statutes 28-813.01, 28-1463.03, and 28-1463.05.

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 5018 South 48th Street, Lincoln, Lancaster County, Nebraska more fully described in **Attachment B**.

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 Technical Crimes Division in Grand Island, Nebraska. 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, investigations involving the sexual exploitation of children, including child pornography and/or visual depictions of sexually explicit conduct which has a child as one of its participants or portrayed observers. I have also had the opportunity to observe and review examples of child pornography and/or visual depictions of sexually explicit conduct which has a child as one of

its participants or portrayed observers in all forms of media including computer media, as defined in Nebraska State Statute 28-813.01, 28-1463.03, and 28-1463.05

Based on the information set forth below, your affiant has probable cause to believe that evidence of visual depictions of sexually explicit conduct which would depict children as one of its participants or portrayed observers (28-813.01, 28-1463.03, and 28-1463.05) is located at the residence, more fully described in **Attachment B**.

I make this affidavit in support of an application for a search warrant of computers and/or digital devices/information/files, more fully described in **Attachment A**, contained within a residence, more fully described in **Attachment B**. There is probable cause to believe that the seizure of the 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 the possession of visual depictions of sexually explicit conduct which would depict children as one of its participants or portrayed observers in violation of Nebraska State Statutes 28-813.01, 28-1463.03, and 28-1463.05.

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 violation of Nebraska State Statutes 28-813.01, 28-1463.03, and 28-1463.05.

Computers and computer technology have revolutionized the way in which individuals interested in child pornography and/or visual depictions of sexually explicit conduct which has a child as one of its participants or portrayed observers interact with each other. Child pornography and/or visual depictions of sexually explicit conduct which has a child as one of its participants or portrayed observers formerly was produced using cameras and film (either still photography or movies). There were definable costs involved with the production of pornographic images. To distribute these images on any scale required significant resources. The distribution of these wares was accomplished through a combination of personal contacts, mailings, and telephone calls.

The development of computers, computer equipment, cellular phones, and digital media has changed this; computers, computer equipment, cellular phones, and digital media serve five functions in connection with child pornography and/or visual depictions of sexually explicit conduct which has a child as one of its participants or portrayed observers: production, communication, distribution, storage, and viewing.

Individuals involved with child pornography and/or visual depictions of sexually explicit conduct which has a child as one of its participants or portrayed observers can now transfer photographs from a camera onto a computer readable format with a device known as a scanner. With the advent of computers, computer equipment, cellular phones, and digital media, the images can now be transferred directly onto a computer. A device known as a modem allows any computers, computer equipment, cellular phones, and digital media to connect to another computer through the use of telephone, cable, or wireless connection. Electronic contact can be made to literally millions of computers around the world.

The computer's ability to store images in digital form makes the computer itself an ideal repository for child pornography and/or visual depictions of sexually explicit conduct which has a child

as one of its participants or portrayed observers. The size of the electronic storage media (commonly referred to as the hard drive) used in home computers has grown tremendously within the last several years. These drives can store hundreds of thousands of images at very high resolution.

The Internet and its World Wide Web protocol afford collectors of child pornography and/or visual depictions of sexually explicit conduct which has a child as one of its participants or portrayed observers several different venues for obtaining, viewing and trading child pornography and/or visual depictions of sexually explicit conduct which has a child as one of its participants or portrayed observers in a relatively secure and anonymous fashion.

Collectors and distributors of child pornography and/or visual depictions of sexually explicit conduct which has a child as one of its participants or portrayed observers also use online resources to retrieve and store child pornography and/or visual depictions of sexually explicit conduct which has a child as one of its participants or portrayed observers, including services offered by electronic service providers such as Yahoo, MSN, and AOL and Peer-2-Peer (P2P) services (Limewire, Bearshare, Shareaza, BitTorrent, eMule, Gnutella, Ares). The online services allow a user to set up an account with a remote computing service and/or electronic service provider that provides email services as well as electronic storage of computer files in a variety of formats. Programs also provide a similar nexus to share their files to millions of subscribers. Users can also set up online storage accounts from any computers, computer equipment, cellular phones, and digital media with access to the Internet. Evidence of such online storage of child pornography and/or visual depictions of sexually explicit conduct which has a child as one of its participants or portrayed observers is often found on the user's computer.

As is the case with most digital technology, communications by way of computers, computer equipment, cellular phones, and digital media can be saved or stored on the computer used for these purposes. Storing this information can be intentional, such as saving an email as a file on the computers, computer equipment, cellular phones, and digital media or saving the location of one's favorite websites in "bookmarked" files. Digital information can also be retained unintentionally indicating the path and traces of an electronic communication, and may be automatically stored in many places, such as temporary files or electronic service provider client software, and other types of electronic service provider technologies. In addition to electronic communications, a computer user's Internet activities generally leave traces or "footprints" in the web cache and history files of the browser used. A forensic examiner can often recover evidence which shows that computers, computer equipment, cellular phones, and digital media contains software, such as P2P software, when the computer was sharing files, and even some of the files which were uploaded or downloaded. Such information may be maintained indefinitely until overwritten by other data.

A phenomenon on the Internet is peer to peer file sharing (hereinafter, "P2P"). P2P file sharing is a method of communication available to Internet users through the use of publically available software. The software is designed to allow users to trade digital files through a worldwide network that is formed by linking computers together. There are several P2P networks currently operating. There are several different software applications that can be used to access these networks but these applications operate in essentially the same manner.

To access the P2P networks, a user first obtains the P2P software, which can be downloaded from the Internet. This software is used exclusively for the purpose of sharing digital files. When the P2P software is installed on a computer, the user is directed to specify a "shared" folder. All files placed in that user's "shared" folder are available to anyone on the P2P Network for download. Most P2P software gives each user a rating based on the number of files he/she is contributing to the

network. This rating affects the user's ability to download files. The more files a user is sharing, the greater his/her ability is to download files. This rating system is intended to encourage users to "share" their files, thus propagating the P2P network. However, a user is not required to share files to utilize the P2P network.

A user obtains files by conducting keyword searches of the P2P network. When a user initially logs onto the P2P network, a list of the files that the user is sharing is transmitted to the network. The P2P software then matches files in these file lists to keyword search requests from other users. A user looking to download files simply conducts a keyword search. The results of the keyword search are displayed and the user then selects file(s) which he/she wants to download. The download of a file is achieved through a direct connection between the computer requesting the file and the computer(s) hosting the file. Once a file has been downloaded, it is stored in the area previously designated by the user and will remain there until moved or deleted. Most of the P2P software applications keep logs of each download event. Often times a forensic examiner, using these logs, can determine the IP address from which a particular file was obtained.

Your Affiant knows from training and experience that search results presented to the user allow the user to select a file and then receive that file from other users around the world. These users can receive the selected files from numerous sources at once, or a user can select to receive a file from only one source. By selecting numerous sources, the software can balance the network load and recover from network failures by accepting pieces of the file from different users and then reassembling the file on the local computer.

Your Affiant knows that P2P networks can only succeed in reassembling the file from different parts if the parts all come from the same original file. Your Affiant knows that multiple persons sharing one file can deliver different pieces of that file to the local software and the local software can insure that a complete and exact copy can be made from the parts.

A person interested in sharing child pornography and/or visual depictions of sexually explicit conduct which has a child as one of its participants or portrayed observers with others in the P2P network, need only place those files in his/her "shared" folder(s). Those child pornography and/or visual depictions of sexually explicit conduct which has a child as one of its participants or portrayed observers files are then available to all users of the P2P network for download regardless of their physical location.

A person interested in obtaining child pornography and/or visual depictions of sexually explicit conduct which has a child as one of its participants or portrayed observers can open the P2P application on his/her computer and conduct a keyword search for files using a term such as "preteen sex." The keyword search would return results of files being shared on the P2P network that match the term "preteen sex." The user can then select files from the search results and those files can be downloaded directly from the computer(s) sharing those files.

There are instances in which a user selects a file from the keyword search results and is unable to immediately begin downloading a file. In this case, the P2P program sends a "push request" to an ultra peer. A "push request", also known as a "push proxy", is a method used in the Gnutella network and many other P2P protocols. The protocol is used in P2P clients such as Limewire, Shareaza and many more. The push request is sent through the ultra peer to another client. This push request asks the other client to push the file to the original user requesting the file. For example, if "user A" selects a file to download from "user B", but "user B" is not accepting incoming connections, "user A" would then send a "push request" to the ultra peer requesting "user

B" to push the file to "user A". This push request is part of the P2P protocol that allows a user to download a file from one specific user.

One of the advantages of P2P file sharing is that multiple files may be downloaded in parallel. This means that the user can download more than one file at a time. In the event a push proxy is not used, a user may download parts of one file from more than one source computer at a time. For example, a user downloading an image file may actually receive parts of the image from multiple computers. The advantage of this is that it reduces the time it takes to download the file.

A P2P file transfer is assisted by reference to an Internet Protocol (IP) address. This address, expressed as four numbers separated by decimal points (IPv4), is unique to a particular internet connection during an online session. Newer IP addresses (IPv6) are expressed as eight groups of four hexadecimal digits with the groups being separated by colons. The IP address provides a unique location making it possible for data to be transferred between computers.

The computers that are linked together to form the P2P network are located throughout the world; therefore, the P2P network operates in interstate and foreign commerce. A person that includes child pornography and/or visual depictions of sexually explicit conduct which has a child as one of its participants or portrayed observers files in his/her "shared" folder is hosting child pornography and/or visual depictions of sexually explicit conduct which has a child as one of its participants or portrayed observers and therefore is in possession, promoting, presenting, and potentially distributing child pornography and/or visual depictions of sexually explicit conduct which has a child as one of its participants or portrayed observers. A person that hosts child pornography and/or visual depictions of sexually explicit conduct which has a child as one of its participants or portrayed observers in this manner is in violation of Nebraska State Statutes 28-813.01, 28-1463.03, and 28-1463.05. He/she is in possession, promoting, presenting, and potentially distributing child pornography and/or visual depictions of sexually explicit conduct which has a child as one of its participants or portrayed observers in interstate and foreign commerce by means of a computer.

Even though the P2P network links together computers all over the world and users can download files, it is not possible for one user to send or upload a file to another user of the P2P network. The software is designed only to allow files to be downloaded that have been selected. One does not have the ability to send files from his/her computer to another user's computer without their permission or knowledge. Therefore, it is not possible for one user to send or upload child pornography and/or visual depictions of sexually explicit conduct which has a child as one of its participants or portrayed observers files to another user's computer without his/her active participation. If a file is downloaded through the use of a push request, another user may send the file to a user but only if user requests the file be sent. Even with a use of a push request, a file is never sent to the user requesting the download unless the user has requested such download.

Your Affiant knows that cooperating police agencies accumulate their information to assist in identifying criminal conduct and build probable cause to further criminal investigations. With this accumulated information, police get a better understanding of the global information available about a suspect that resides in their area of jurisdiction. This information is valuable when trying to regionalize a suspect to a certain jurisdiction, given the global scope of the Internet. Investigators from around the world gather and log information, which can be used by an investigator to build probable cause on one specific case.

Your Affiant uses an automated system which reads the publicly available advertisements from computers that are identifying child pornography and/or visual depictions of sexually explicit conduct

which has a child as one of its participants or portrayed observers and/or child sexual abuse images or videos available for distribution in a consistent and reliable manner. The software reads these reported offers to participate in the sharing of child pornography and/or visual depictions of sexually explicit conduct which has a child as one of its participants or portrayed observers and reports the time, date, SHA-1 values and/or hash values, and filenames for each individual computer in the same way. Your Affiant has run search terms through the manual method described above and the automated system performs in the same way with matching results as the previous manual investigative techniques used in this operation to date. When using the manual method, Your Affiant connected to an Internet Protocol (IP) address using P2P software. Your Affiant requested, through P2P software, to browse the "Shared File" folder at that address. Your Affiant was given a listing of multiple files which were available advertisements from computers with child pornography and/or visual depictions of sexually explicit conduct which has a child as one of its participants or portrayed observers and/or child sexual abuse images or videos available for sharing. Your Affiant exported the multiple filenames and/or files with their respective SHA-1 values and/or hash values in the publicly available folder (also known as a "shared folder") and loaded them into software shared by the Child Exploitation Investigative Entities to ascertain if any identified child pornography and/or visual depictions of sexually explicit conduct which has a child as one of its participants or portrayed observers images and/or videos were present.

Your Affiant knows from training and experience that an investigator can review these details and identify a pattern of activity that links a single IP address to specific files of child pornography and/or visual depictions of sexually explicit conduct which has a child as one of its participants or portrayed observers with an extremely high degree of accuracy. The automated search process conducts and reports the search in the same manner that has previously been done by individual investigators. This search process does not report details that are not also discoverable by the general public using Internet available software.

Your Affiant is aware that over fifty search warrants have been executed in the State of Nebraska and other jurisdictions within the United States by using the above method of investigation. This method has proven to be extremely reliable in determining the location of computers that were involved in the P2P facilitated trading of child pornography and/or visual depictions of sexually explicit conduct which has a child as one of its participants or portrayed observers. Your Affiant has been involved some of those search warrants either as the primary investigator, or assisting other investigators with their search warrant. Your Affiant advised that by using the above listed method of investigation; nearly every case was verified through the following means:

- a. Evidence of child pornography and/or visual depictions of sexually explicit conduct which has a child as one of its participants or portrayed observers.
- b. If no images and/or videos of child pornography and/or visual depictions of sexually explicit conduct which has a child as one of its participants or portrayed observers were found on the computer, interviews of persons using those computers verified that child pornography and/or visual depictions of sexually explicit conduct which has a child as one of its participants or portrayed observers had been present at one time but had been deleted or the computer with the child pornography and/or visual depictions of sexually explicit conduct which has a child as one of its participants or portrayed observers had been removed from the premises.
- c. Images and/or videos moved from computer and stored on other media

Below is a summary of the current investigation:

Peer to Peer (P2P) file sharing allows people using P2P software to download and share files with other P2P users using the same or compatible P2P software. P2P software is readily available on the Internet and often free to download. Internet connected devices such as computers, tablets and smartphones running P2P software form a P2P network that allow users on the network to share digital files. BitTorrent is one of many P2P networks. For a user to become part of the BitTorrent network, the user must first obtain BitTorrent software and install it on a device. When the BitTorrent software is running and the device is connected to the Internet, the user will be able to download files from other users on the network and share files from their device with other BitTorrent users. Users of the BitTorrent network wishing to share new content will use a BitTorrent program to create a "torrent" file for the file or group of files they wish to share. A torrent file is a small file that contains information about the file(s) and provides a method for a user to download the file(s) referenced in the torrent from other BitTorrent users. Torrent files are typically found as the result of keyword searches on Internet sites that host or link to them. Torrent files may be referenced by their "infohash", which uniquely identifies the torrent based on the file(s) associated with the torrent file.

To download file(s) from other users on the BitTorrent network, a user typically obtains a torrent file. The BitTorrent software processes the information in the torrent file and locates devices on the BitTorrent network sharing all or parts of the actual file(s) being sought. The download of the content referenced in the torrent is achieved after the requesting computer and the sharing computer(s) directly connect to each other through the Internet using the BitTorrent software.

On Sunday, October 8, 2023, I was conducting an online investigation on the BitTorrent network for offenders sharing visual depictions of sexually explicit conduct which would depict children as one of its participants or portrayed observers, commonly known as child pornography. An investigation was initiated for a device at IP address 140.228.180.251, because it was associated with a torrent with the infohash: 7c72a80e32e64c51efb12639ef650ce0939733db. This torrent file references 41 files, at least one of which was identified as being a file of investigative interest to child pornography investigations. Using a computer running investigative BitTorrent software, a direct connection was made to the device at IP address 140.228.180.251, hereinafter referred to as "Suspect Device". The Suspect Device reported it was using BitTorrent client software -qb4550-qBittorrent/4.5.5.

On Sunday, October 8, 2023, between 0316 hours CDT and 2001 hours CDT, a download was successfully completed of the following 3 file(s) that the device at IP address 140.228.180.251 was making available. The device at IP Address 140.228.180.251 was the sole candidate for each download, and as such, each file was downloaded directly from this IP Address.

Two (2) of three (3) files that was downloaded from the Suspect Device were:

- a. **File Name: 10 little boy.mp4**
Sha1 hash: Z5MB6NEOTGVYQ6PTOMYCF7JH7SUJ7KOZ
- b. **File name: 6 pedomom.mp4**
Sha1 hash: LLULZBKTXKBTEVSSK4TKY4JTEUGARMM7

Your Affiant knows that filenames do not always accurately depict the contents of the file. Your Affiant compared the following SHA-1 (Secure Hash Algorithm-1) values reported as residing at this IP address to files with the same SHA-1 recovered in previous investigations. A SHA-1 value is a popular one-way hash algorithm used to create digital signatures the value of a file that can be described as digital "DNA" for a specific file. SHA-1 algorithms statistically greatly exceed DNA

standards by providing 99.9999 percent certainty. Your Affiant and others that utilize this resource have never seen or heard of two completely different digital files have the same SHA-1 value. Your Affiant has had the opportunity to collect, share, and receive other SHA-1 values from "known" child pornography and/or visual depictions of sexually explicit conduct which has a child as one of its participants or portrayed observers images and/or videos and collected them for investigative purposes from other law enforcement officers around the world. The collection of SHA-1 values allows law enforcement to conduct a methodical comparison of files to identify child pornography and/or visual depictions of sexually explicit conduct which has a child as one of its participants or portrayed observers without actually viewing the images. Your Affiant noted the SHA-1 values associated with the files listed above to depict the listed conduct:

- a. **File Name: 10 little boy.mp4**
Sha1 hash: Z5MB6NEOTGVYQ6PTOMYCF7JH7SUJ7KOZ

This is a video file that depicts in the beginning of the video an Asian prepubescent male approximately 5 to 8 years of age naked and on a pillow with a flower pattern. Another person is using a purple-colored device and rubbing the child's penis. As the video continues it appears the child is inserting another male's penis in his mouth. There is lettering on the bottom of the screen that says, "how to buy this pack is shown at the end of the video". The video then depicts another scene where an adult female is using her mouth to suck on a prepubescent male's penis. The child in this scene is approximately 6 to 9 years of age. The video depicts more scenes with several children involved in sexual acts including penetration. The video appears to be intended to advertise 44 videos for the price of 40 EUR. The entire video is 3 minutes and 48 seconds in length.

- b. **File name: 6 pedomom.mp4**
Sha1 hash: LLULZBKTXKBTEVSSK4TKY4JTEUGARMM7

This is a video file that depicts in the beginning of the video a toddler male approximately 2 to 4 years of age laying on blue bedding and appears to be naked. An adult female with a mask on and red nail polish is using her mouth to suck on the child's penis. As the video continues it appears the video depicts more scenes with several prepubescent children, both male and female, involved in sexual acts including penetration with adult females. There is lettering on the bottom of the screen that says, "how to buy this pack is shown at the end of the video". The video appears to be intended to advertise 27 videos for the price of 30 EUR. The entire video is 3 minutes and 54 seconds in length.

On October 10, 2023, the Nebraska State Patrol requested a Lancaster County Attorney Subpoena for subscriber information from Allo Communications for the IP address 140.228.180.251 for 08-16-2023 at 2311 hours CDT to 10-09-2023 at 2012 hours CDT. On October 13, 2023, Allo Communications advised that the IP address was leased to the subscriber Melissa Stewart and had a service address of 5018 S 48th St, Lincoln, NE 68516. The phone number tied to the account was 4025253025 and an email address of melissa.stewart.ne@gmail.com. The additional contact for the account was Sunny Csuhta.

Investigator Davis noted that the device and user at IP address 140.228.180.251 has been on the BitTorrent network at several times between August 17, 2023, and March 24, 2024, making available several other info hashes available for download. Between August 17, 2023, and March 24, 2024, Investigator Davis has downloaded more than 2,000 files of visual depictions of sexually explicit conduct which would depict children as one of its participants or portrayed observers in violation of Nebraska State Statutes 28-813.01, 28-1463.03, and 28-1463.05 from IP address 140.228.180.251.

Between June 4, 2024, and June 10, 2024, Investigator Davis conducted surveillance on 5018 South 48th Street, Lincoln, Lancaster County, Nebraska. During surveillance Investigator Davis saw in the driveway a black 2008 Ford Explorer bearing Nebraska passenger plate ASA435, currently registered to Wyatt Ray Stewart at the address of 5018 South 48th Street, Lincoln, Lancaster County, Nebraska. This vehicle left the residence at 0644 hours CDT. Investigator Davis conducted a check of the Nebraska Criminal Justice Information System (NCJIS) and located a citation # AO29V0000389 from December 7, 2021, for Wyatt Stewart for speeding in Otoe County Nebraska. The address for Stewart was 5018 South 48th Street, Lincoln, NE. Investigator Davis also located in NCJIS a Melissa M. Stewart, DOB: 07-01-1975, that has a current Nebraska Operator's License with the address of 5018 South 48th Street, Lincoln, NE.

Taken together, the above information indicates that on October 8, 2023, a person knowingly was in possession of child pornography and/or visual depictions of sexually explicit conduct which has a child as one of its participants or portrayed observers in interstate and foreign commerce by means of a computer or electronic device.

Your Affiant viewed the files and noted the files were child pornography and/or visual depictions of sexually explicit conduct which has a child as one of its participants or portrayed observers as defined in Nebraska State Statutes 28-813.01, 28-1463.03, and 28-1463.05. The pornographic images and/or videos described herein were publicly advertised via the Internet to Your Affiant using the automated software, and those public advertisements originated from a cable modem inside the residence, more fully described in **Attachment B**.

Your affiant 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' involved with the possession of visual depictions of sexually explicit conduct which would depict children as one of its participants or portrayed observers (28-813.01, 28-1463.03, and 28-1463.05). 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 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 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 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 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 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 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 the criminal violation(s) previously mentioned in this affidavit.

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

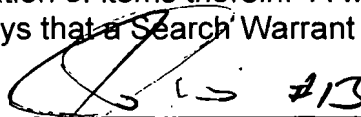
associated with a computer, computer equipment, cellular phone or digital media, and the operating system or applications of a computer, computer equipment, cellular phone or digital media device may not be known until the examination is conducted. Your affiant knows that individuals can change default 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 possession of visual depictions of sexually explicit conduct which would depict children as one of its participants or portrayed observers (28-813.01, 28-1463.03, and 28-1463.05).

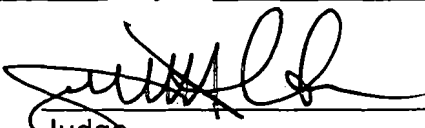
Your affiant is aware that the recovery of data by a computer forensic analyst takes significant time; much the way recovery of narcotics must later be forensically evaluated in a lab, computers, computer equipment, cellular phones or digital media will also undergo a similar process. For this reason, 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 ANYTIME search is requested. WHEREFORE, he prays that a Search Warrant may issue according to law.


Investigator Justin Davis
Nebraska State Patrol



SUBSCRIBED AND SWORN TO before me this 10 day of JUNE,
2024.


Judge

ATTACHMENT A

ITEMS TO BE SEIZED AND SEARCHED

1. All visual depictions of sexually explicit conduct of sent and/or received files (including still images, videos, films or other recordings) or other computer graphic files which would depict children as one of its participants or portrayed observers.
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 the possession, receipt or distribution of child pornography and/or visual depictions of sexually explicit conduct which would depict children as one of its participants or portrayed observers, or pertaining to an interest in child pornography and/or visual depictions of sexually explicit conduct which would depict children as one of its participants or portrayed observers 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

The location known as at the address of 5018 South 48th Street, Lincoln, Lancaster County, Nebraska is identified as follows:

The residence located at 5018 South 48th Street, Lincoln, Lancaster County, Nebraska is described as a single-family residence, with Light colored siding. On the mailbox are the numbers 5018. According to the Lancaster County Assessors website, the legal description is: SOUTH HAVEN HILLS, BLOCK 6, Lot 31. Any vehicles, outbuildings, campers on or adjacent to the aforementioned property that may be attributed to occupants of the home at the time of service may be searched along with the persons occupying the residence at the time of service.

