

IN THE COUNTY COURT OF LANCASTER COUNTY NEBRASKA

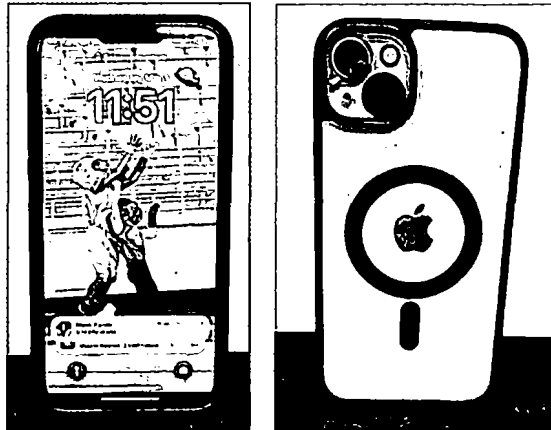
STATE OF NEBRASKA)
) SS
COUNTY OF LANCASTER)

CR24-1

RETURN AND INVENTORY
NSP24014027

Investigator John Lukesh #342, being first duly sworn, deposes and says that, on May 9, 2024, I served the within warrant at 4600 Innovation Drive, 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:

The expected download of the blue iPhone, with in a protective case that is clear with black edges, as pictured below. The download has not yet been received by Investigator Lukesh; however, a return of this search warrant was completed to adhere to the ten-day requirement.



Said property was inventoried in the presence of the Investigator John Lukesh #342 and a copy of said Warrant and a receipt for said property was left with the Clerk of the Lancaster County Court.

LANCASTER COUNTY

2024 MAY -9 PM 2:51

CLERK OF THE
DISTRICT COURT

Dated this 9th day of May, 2024.

John Lukesh #342

Investigator John Lukesh #342
Nebraska State Patrol

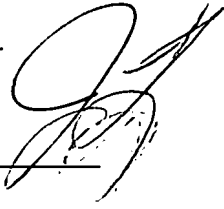


002176226D02

1
5

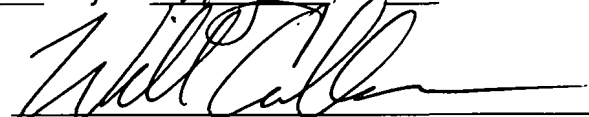
SUBSCRIBED AND SWORN TO before me this _____ day of _____, 20____.

~~_____~~
Lancaster County Judge



Warrant and inventory returned on this 9th day of May, 2024.

~~_____~~
Lancaster County Clerk



IN THE COUNTY COURT OF LANCASTER COUNTY NEBRASKA

STATE OF NEBRASKA)
) SS LANCASTER COUNTY **SEARCH WARRANT**
COUNTY OF LANCASTER) 2024 MAY -9 PM 2: 51 **NSP24014027**

CLERK OF THE
DISTRICT COURT

TO NEBRASKA STATE PATROL OFFICER: INVESTIGATOR JOHN LUKESH #342

This matter came on for hearing on the 1st day of May, 2024, upon the sworn application and affidavit for issuance of a search warrant of Investigator John Lukesh #342 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 John Lukesh #342 of the Nebraska State Patrol, dated the 1st day of May, 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 possession with intent to distribute-cocaine in violation of Nebraska State Statute 28-416.

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 4600 Innovation Drive, Lincoln, Lancaster County, Nebraska, more fully described in **Attachment B**, under the care, custody and control of Nebraska State Patrol Evidence Technician Angela Bell.

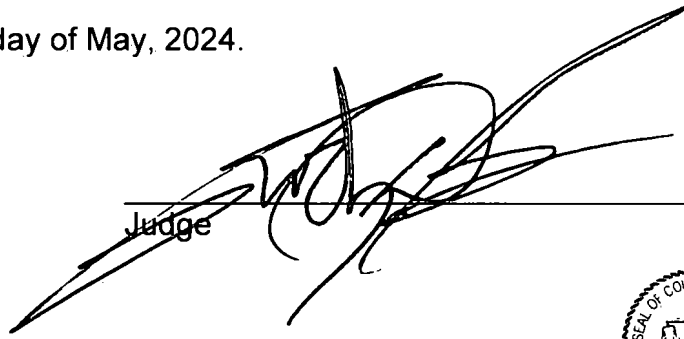
And, if found, to seize and deal with the same as provided by law, and to make return of this warrant to me within ten days after the date hereof.

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 DAY TIME HOURS.

IT IS FURTHER ORDERED, that the Nebraska State Patrol, Investigator John Lukesh #342, make return of this Search Warrant to me within ten days after the date hereof.

GIVEN under my hand this 1st day of May, 2024.



Judge

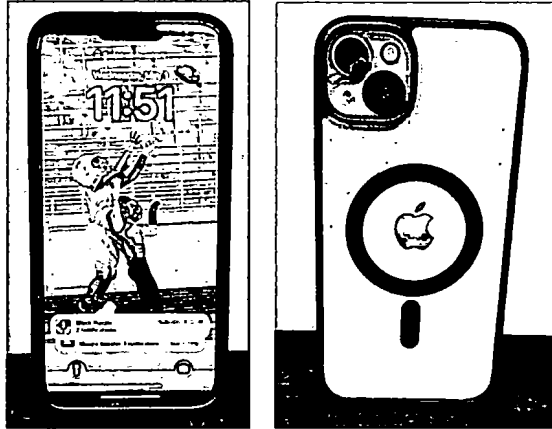


ATTACHMENT A

ITEMS TO BE SEIZED AND SEARCHED

Items:

- blue iPhone, with in a protective case that is clear with black edges, as pictured below.



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 possession with intent to distribute-cocaine, in violation of Nebraska State Statute 28-416.
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 possession with intent to distribute-cocaine, in violation of Nebraska State Statute 28-

416, or pertaining to an interest in possession with intent to distribute-cocaine, in violation of Nebraska State Statute 28-416 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 State Headquarters Office.

IN THE COUNTY COURT OF LANCASTER COUNTY NEBRASKA

STATE OF NEBRASKA
COUNTY OF LANCASTER

) LANCASTER COUNTY
) SS
) 2024 MAY -9 PM 2: 51

**AFFIDAVIT AND APPLICATION
FOR ISSUANCE OF A
SEARCH WARRANT
NSP24014027**

CLERK OF THE
DISTRICT COURT

The complaint and affidavit of Investigator John Lukesh 342, Nebraska State Patrol, on this 1st day of May, 2024, who being first duly sworn, upon oath says:

Your affiant is an Investigator with the Nebraska State Patrol and has been employed with this agency since July 2006. Your affiant has been in the Investigations Division since September 2019, serving as the Nebraska State Patrol's Pharmaceutical Diversion Investigator until October 2023, and is currently serving as a member of the Lincoln/Lancaster County Narcotics Task Force (LLCNTF). Your Affiant has been involved in and/or participated in several criminal and drug investigations to include general criminal violations, pharmaceutical diversion, and criminal conspiracy investigations. Your affiant has received over 200 hours of training from the Nebraska State Patrol and NHTSA in the identification and recognition of illegal drugs, including but not limited to marijuana, cocaine, methamphetamine, heroin, and other controlled substances. Your affiant was certified as a Drug Recognition Expert holding certification from 2014 to 2020 and has completed numerous drug evaluations on individuals impaired on illicit and pharmaceutical drugs. Your affiant has been case-specific deputized as an agent with the Federal Drug Enforcement Administration, to investigate cases involving national conspiracies of drug trafficking organizations. Your affiant has attended specialized training which dealt with the sale, concealment, storage, and transportation of drugs.

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 possession with intent to distribute-cocaine in violation of Nebraska State Statute 28-416.

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 4600 Innovation Drive, Lincoln, NE 68521, more fully described in **Attachment B**, under the care, custody and control of Nebraska State Patrol Evidence Technician Angela Bell.

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 Drug Division in Lincoln, 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 possession with intent to distribute-cocaine, as defined in Nebraska State Statute 28-416.

Based on the information set forth below, your affiant has probable cause to believe that evidence of possession with intent to distribute-cocaine, is located at the Nebraska State Patrol Headquarters Office, 4600 Innovation Drive, Lincoln, NE. 68521, 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 Nebraska State Patrol Headquarters Office, 4600 Innovation Drive, Lincoln, NE. 68521, 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 possession with intent to distribute-cocaine, in violation of Nebraska State Statute 28-416.

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 Statute 28-416.

On April 23, 2024, at approximately 1600 hours, Inv. J. Lukesh, #342, and Inv. J. Parsons, #69, were conducting surveillance near the apartment complex at 2310 C St., Lincoln, Lancaster County, Nebraska, to locate Matthew-Jon Kirkland, DOB 06/06/1985, for outstanding warrants out of Platte and Lancaster Counties in Nebraska. A subscriber inquiry on the utilities for this location was requested identifying Kirkland as the subject listed on the account, with a telephone number of 402-326-8732.

At approximately 1617, hours Inv. Lukesh observed an individual matching Kirkland's physical description exit the front door of the apartment complex who was contacted by investigators and ultimately identified verbally as Matthew-Jon Kirkland. Kirkland was detained pending confirmation of arrest warrants. Once warrants were confirmed, Kirkland was advised he was under arrest.

Inv. Lukesh conducted a search of Kirkland's person and located, amongst other items, two (2) yellow plastic bags which appeared to be twisted off from grocery sacks and contained a white powdery substance (bag #1: 2.3 grams and bag #2: 3.9 grams). Kirkland verbally confirmed this substance to be cocaine. Inv. Lukesh continued the search and located an Apple iPhone, which he confirmed as his personal cell phone with associated number 402-326-8732. Inv. Lukesh placed Kirkland's phone in airplane mode at this time.

Inv. Lukesh read Miranda Rights to Kirkland, who acknowledged that he understood and would waive, agreeing to questioning. Kirkland confirmed he had approximately one-half ounce of marijuana on the ground by a television stand in his apartment along with another, what he described as, approximately nine (9) grams of cocaine in a cabinet in the kitchen of his apartment.

At 1711 hours, Kirkland consented to search of his apartment. This was documented on a Nebraska State Patrol Permission to Search Consent Form which Kirkland did sign at 1711 hours on April 23, 2024. Additional evidentiary items seized from Kirkland's apartment during this consent search were: a black/pink gas mask bong; an additional 7.6 grams of cocaine; a green/black scale found in the kitchen; a black scale in the kitchen cupboard; a green tray with the image of "Mario" (from Mario Bros.) which had cocaine residue on it; 7.8 grams (total weight) of marijuana between a blunt that weighed 1.8 grams, a package that weighed 5.1 grams, and a white plastic bag containing .9 grams of marijuana; a scratch ticket with two \$1 bills with cocaine residue; and LES bill for 2310 C St., Apt. 1, addressed to Kirkland.

At 1735 hours, Kirkland was transported to the Lancaster County Jail for possession with intent to distribute-cocaine in violation of Nebraska State Statute 28-416. Upon completion of the booking process, Investigator Lukesh Mirandized Kirkland, who agreed to waive his rights and participate with the interview. Kirkland stated during this interview that he utilized his personal cell phone with associated number 402-326-8732 to place a phone call to his source to purchase cocaine and marijuana. Kirkland stated at approximately 1345 hours – 1430 hours, on April 23, 2024, Kirkland's source arrived at his apartment and sold him one-half ounce of cocaine for \$625.00 and one-half ounce of marijuana for \$65.00.

Inv. Lukesh asked Kirkland for consent to search cell phone with associated number 402-326-8732 during the mirandized interview at the Lancaster County Jail which he denied. Upon completion of the interview, Inv. Lukesh transported Kirkland's cell phone to the Nebraska State Patrol Headquarters Office, 4600 Innovation Drive, Lincoln, Lancaster County, Nebraska, where it was placed in an evidence locker equipped with a iPhone charging cable to maintain constant power to the device.

Through you affiant's training and past experience, you affiant is aware that cellular telephone data can provide valuable insight for narcotics distribution/ trafficking investigations. Cellular telephones are used by the general public for communication, access to and sharing of information, research, socialization, entertainment, mapping, shopping, note taking and other functionality. Your affiant is aware from training and experience that individuals involved in criminal activity (specifically narcotics distribution/trafficking) utilize cellular telephones for the aforementioned purposes and additionally as a tool for facilitating criminal activity, specifically the sale and trafficking of illegal drugs. The data contained in cellular telephones seized in narcotics investigations can provided a wealth of information that can assist investigators in determining culpability of criminal participants, identifying co-conspirators and determining the scope, hierarchy and operational methods of drug trafficking organizations. This data also assists investigators with identifying sources of controlled substances, trafficking routes and financial information related to the sale of illegal drugs. As such, a cellular telephone possessed by criminal participants can serve both as an instrument for committing crime as well as a storage medium for evidence of the crime.

Your affiant has personally been involved, or has knowledge of, numerous narcotics-related investigations. These investigations span the entire spectrum of drug related crime; ranging from investigation of street level narcotic users to domestic and international drug trafficking organizations operating between eastern Nebraska and the southern United States/ Mexico border. From experience in these investigations, your affiant is aware that cellular telephones and cellular web-based applications are used in nearly all drug related cases by criminal participants to plan, organize and facilitate criminal activities, specifically to include drug transactions.

Your affiant is aware of numerous instances where cellular telephones were used by criminal participants to communicate via voice, text messaging, social media or other communication applications; instances in which criminal participants utilized cellular telephones to photograph themselves, associates and co-conspirators with weapons and/or illegal narcotics; instances in which cellular telephones were used by criminal participants to create videos of their activity; instances where criminal participants to create videos of their criminal activity; instances where criminal participants have used cellular based internet applications to research crimes they have or intent to participate in; instances in which criminal participants have maintained notes, ledgers and customers lists in digital format within cellular telephones and instances in which criminal participants used global positioning, mapping and other location services to facilitate in-person meetings with co-conspirators.

Through your affiant's training and experience, your affiant knows that drug distribution organizations utilize trusted friends and members of their family to participate in a variety of capacities to assist with the organization. Your affiant knows through numerous investigations, when one party in an intimate relationship is involved in high volume drug distribution, the other partner commonly participates and benefits from the proceeds of that business. Your affiant is aware that homes where drugs are sold are commonly set up with security/surveillances equipment for the protection of all residents of the home while drug transactions are occurring. The security/surveillance systems commonly include exterior cameras to warn of imminent threats from rival criminal elements as well as law enforcement. The security/surveillance systems also commonly include interior cameras to cover areas of the residence where drugs and currency are stored and receivers and/or monitors for viewing real-time and past camera footage.

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 involved with possession with intent to distribute-cocaine, in violation of Nebraska State Statute 28-416. 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, 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 possession with intent to distribute-cocaine, in violation of Nebraska State Statute 28-416.

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.

From training and experience, your affiant knows that narcotic traffickers commonly use computers, computer equipment, cellular phones, and digital media to aid them in their criminal activities. This equipment includes telephonic paging devices, mobile/cellular telephones, speed dialers, answering machines, electronic telephone books, electronic date books, computers, computer memory disks, money counters, electronic surveillance equipment, eavesdropping equipment, police radio scanners, and portable communication devices. On electronic devices, particularly cellular phones, memory cards, and similar handheld devices, traffickers frequently maintain electronically stored records such as contact names and telephone numbers; calls placed, received or missed; text messages and e-mails; photographs and video; and information retrieved from the Internet, including social media accounts, cloud storage accounts and email accounts. It is also common for narcotic traffickers to subscribe to cellular phones in false names and addresses to covertly hide their true identity, with the effect of thwarting the ability of law enforcement to conduct electronic surveillance.

Your affiant is aware, that distances involved and frequently pressing time matters in drug trafficking often preclude direct, in person discussion and negotiation. Therefore, a narcotic distribution structure of any size will use computers, computer equipment, cellular phones, and digital media (voice and text) for the purpose of contacting sources and distributors from the top of the pyramid to the base of the pyramid and vice versa to discuss openly or in cryptic fashion the supply, cost, quality, distribution, transportation, or payments involved in marketing and distributing narcotics. Further, when a personal meeting between individuals involved in the drug distribution structure takes place, computers, computer equipment, cellular phones, and digital media will be used by the individuals for arranging and verifying the actual meetings.

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. Your 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 with intent to distribute-cocaine, in violation of Nebraska State Statute 28-416.

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.

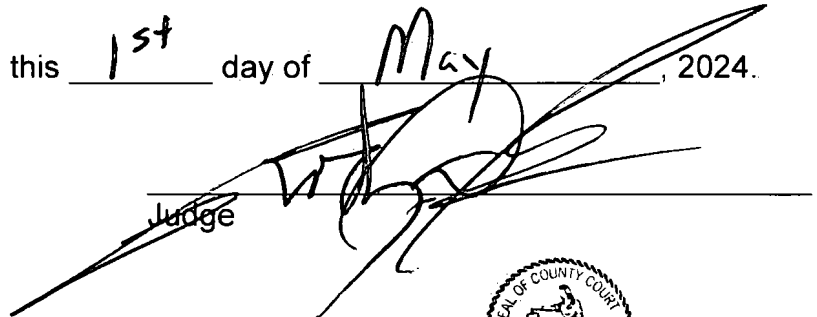
A warrant authorizing a day time search is requested.

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

 _____

Investigator John Lukesh #342
Nebraska State Patrol

SUBSCRIBED AND SWORN TO before me this 1st day of May, 2024.

 _____
Judge

