IN THE COUNTY COURT OF LANCASTER COUNTY, NEBRASKA

IN THE MATTER OF THE SEARCH WARRANT FOR PROPERTY LOCATED IN THE LINCOLN POLICE DEPARTMENT PROPERTY UNIT, 575 SOUTH 10 TH STREET, LINCOLN, LANCASTER COUNTY, NE Q2406933)))))))	CD2H-1 SEARCH WARRANT RETURN	CLERK OF THE DISTRICT COURT	2024 HAY 21 PM 3: 12	LANCASTER COURTY
STATE OF NEBRASKA)					
COUNTY OF LANCASTER)	SS.				

The undersigned states that he/she received the search warrant issued herein on the 17th day of April, 2024 and that he/she executed the same on the 1st day of May, 2024 seized the property/person described in the inventory filed herein and by delivering a copy of the said order for said property/person at the place from which the property/person was taken.

DATE this $\frac{18}{100}$ day of May, 2024.

Deputy Shana Schendt

SUBSCRIBED AND SWORN to before me this 1/8 day of May, 2024.

C4002629

IN THE COUNTY COURT OF LANCASTER COUNTY, NEBRASKA

IN THE MATTER OF THE SEARCH WARRANT FOF PROPERTY LOCATED IN LINCOLN POLICE DEPAI PROPERTY UNIT, 575 SO 10 TH STREET, LINCOLN, LANCASTER COUNTY, N Q2406933	R I THE RTMENT DUTH)	INVENTORY	LANCASTER COURT 2024 MAY 21 PM 3: 13 CLERK OF THE DISTRICT COURT
STATE OF NEBRASKA)			
) ss.			
County of Lancaster	Y			

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

- One IPhone in black Otterbox case under property number Q2406933
 - o Images
 - o Locations
 - o Cell phone calls
 - o Text messages
 - o Videos

DATED this \(\sum_{\text{day}} \) day of May, 2024.

Debuty Shana Schend

SUBSCRIBED AND SWORN to before merthis 18 day of May, 2024.

Notary Publ

GENERAL NOTARY - State of Nebraska LYNN A. KEMPER My Comm. Exp. September 20, 2027

C4002629

RECEIPT

The undersigned hereby acknowledges receipt of the following described property seized from 575 S 10th Street Lincoln, Lancaster County, Nebraska 68508:

One IPhone in black Otterbox case under property report number Q2406933

Images
Locations
Cell phone calls
Text messages
Videos

LANCASTER COUNTY
2024 HAY 21 PM 3: 13
CLERK OF THE
CLERK OF THE
CLERK OF THE

DATED this day of May, 2024.

Shows Shows 402258

Law Enforcement Officer

WITNESS

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

WHEREAS, Shana Schendt, has filed an Affidavit before the undersigned Judge of the County Court of Lancaster County, Nebraska, a copy of which affidavit is attached hereto and made a part hereof; the court finds that the facts set forth in said Affidavit are true, and that those facts do constitute grounds and probable cause for the issuance of a Search Warrant.

THEREFORE, you are commanded to search the following device(s) in the custody of the Lincoln Police Department Property Unit, 575 South 10th, Lincoln, Lancaster County, Nebraska:

 Black Iphone in an Otterbox case, labeled with Property Number <u>Q2406933</u> and Case Number <u>C4002629</u>

Evidence to be searched for includes:

- Evidence of other accounts associated with this device including email addresses, social media accounts, messaging "app" accounts, and other accounts that may be accessed through the digital device that will aid in determining the possessor/user of the device(s);
- b. Evidence of use of the device to communicate with others about the aforementioned crime(s), via email, chat sessions, instant messages, text messages, app communications, social media, internet usage, and other similar digital communications;
- c. Photographs, images, videos, documents, and related data created, accessed, read, modified, received, stored, sent, moved, deleted or otherwise manipulated;
- d. Evidence of use of the device to conduct internet searches relating to the aforementioned crime(s);
- e. Information that can be used to calculate the position of the device, including location data; GPS satellite data; GPS coordinates for routes and destination queries; application data or usage information and related location information; IP logs or similar internet connection information; and images created, accessed or modified, together with their metadata and EXIF tags;
- f. Evidence of the identity of the person in possession of the device(s) and the associated times and dates. Such evidence may be found in digital communications, photos and video and associated metadata, IP logs, documents, social media activity, and similar data;

- g. Records linking the suspect(s), co-conspirator(s), victim(s), and/or witness(es) to a certain screen name, handle, email address, social media identity, etc.;
- h. Records showing a relationship with suspect(s), co-conspirator(s), victim(s), witness(es), and/or location(s), etc.;
 - i. Names, nicknames, account ID's, phone numbers, or addresses of specific persons;
- j. Records showing a relationships to particular areas or locations associated with the aforementioned crime(s);
- k. Photographs, images, videos, documents that contain or are evidence of the aforementioned crime(s);
- 1. Evidence of purchases, such as items used in planning or facilitating the aforementioned crime(s);
- m. Internet research history conducted while planning, executing, or covering up the aforementioned crime(s);
- n. Any live and deleted user attribution data including user accounts, e-mail accounts, passwords, PIN codes, patterns, account names, user names, screen names, remote data storage accounts, documents, files, calendars, metadata, recycle bin files, and any other information and evidence that may demonstrate attribution to a particular user or users;
- o. Any live and deleted applications, programs, or software, used to facilitate the creation, storage, display, or transmission of digital visual recordings and the logs and data associated with the applications, programs or software, and any device backup files;
- p. Any live and deleted audio or visual recording files including files bearing file extensions jpg, jpeg, png, gif, tif, wav, aiff, mp3, mp4, avi, mpg, mpeg, flv, mp4, mov, and wmv along with any descriptive metadata within or associated with the visual recording files, which may include date and time the recording was created, the device used to create the recording and location the recording was made;
- q. Any live and deleted passwords, password files, keys, encryption codes, or other information necessary to access the digital device, software or data stored on the digital device;
- r. Any live and deleted records, documents, programs, applications, information, or materials created, modified, or stored in any form on the digital device(s) listed in this affidavit, that show the actual user(s) of the computers or digital devices including web browser history; temporary Internet files; cookies, bookmarked or favorite web pages; e-mail addresses used from the computer; MAC IDs and/or Internet Protocol addresses used by the computer; e-mails, instant messages, text messages (SMS/MMS), application data and other electronic communications; address books; contact lists; records of social networking and online service usage; calendar entries, notes, journals, and any software that would allow others to control the digital device such as viruses, Trojan horses, malware, and other forms of malicious software.
 - s. Requesting data for the above listed information from 4-2-2024 to 4-9-2024.

This Court, being duly advised that the examination of digital devices is a lengthy process requiring special steps to ensure the integrity of the electronic evidence, finds it may not be possible to complete a return for the Court within the 10 days normally required by the Court.

Given under my hand and seal this 17 day of April, 2024.

JUDGE OF THE COUNTY COURT

Printed Name of County Court Judge

IN THE COUNTY COURT OF LANCASTER COUNTY, NEBRASKA)24 MAY 2	ANCAS.
STATE OF NEBRASKA)	PH PH	TER CC
) ss. AFFIDAVIT FOR SEARCH WARRANT COUNTY OF LANCASTER)	<u>မှ</u> - ၁	LINU

Shana Schendt, being first duly sworn upon oath deposes and states that she is a Deputy Sheriff for the Lancaster County Sheriff's Office, Lancaster County, Nebraska. AFFIANT further states she is currently involved in the investigation of Possession of Controlled Substance (28-416(3)) and Tampering with Evidence (28-922), occurring near 19100 Block of S 96th Street, Lancaster County, Nebraska. As part of the investigation, AFFIANT has consulted with other involved law enforcement and reviewed case reports. AFFIANT states as follows:

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

One black Apple Iphone in an Otterbox phone case located in the Electronic Evidence Unit at 605 S. 10th Street, Lincoln, Lancaster County, Nebraska and labeled with the Property Report number Q2406933 and case number C4002629.

The Electronic Evidence Unit forensic examiners may designate additional forensic services, as they may deem necessary to complete the analysis. Once examination and analysis has been completed, the listed evidence shall be returned to the Lincoln Police Department Property Unit, where it will be held until any final disposition by the Court

Facts:

On 4-7-2024, I was driving eastbound on Hickman Road approaching 82nd St. I observed a white Chrysler Town & Country (NE: ABP326) making a right turn, onto Hickman Road from 82nd Street. The vehicle had been northbound on 82nd, prior to turning eastbound on Hickman Rd. When the vehicle completed the turn, I observed it to enter into the westbound lane, making an improper turn. I continued to follow the vehicle and observed the vehicle to be driving above the 55 MPH speed limit. I activated my front radar unit and observed the speed of the vehicle to be traveling 65mph. The vehicle continued on to turn south on 96th St. After turning, I observed the vehicle to cross the center line. I initiated a traffic stop with the vehicle and approached the driver's side. Upon approaching the vehicle, I observed two male occupants seated in the front. Both male occupants kept their hands on their knees and did not look my way, but appeared to be evading eye contact. The driver informed me through the window he was unable to roll his window down so I requested he open the door. The driver complied and was informed the reason for the stop was speed and making an improper turn.

The driver identified himself through a Nebraska driver's license as Anthony Smith Ir and claimed he had just visited a friend near 91st and Olive Creek Rd, but was heading back to Omaha. I questioned Smith if he was heading back to Omaha, then why was he turning to continue South toward Olive Creek Rd. Through out conversation, Smith stated he was visiting his friend, Elizabeth Foley, who just moved to the residence. I am familiar with Elizabeth Foley as being a known associate to Clinton Hummer, who resides at 9105 Olive Creek Road. Hummer and Foley have both previously found to be in possession of methamphetamines. This address has also been observed to have various vehicles coming and leaving throughout the night, which is believed to be related to possible drug activity. Hummer was charged with possession of controlled substance numerous times, most recently being 2-7-2024.

Smith claimed they were going to pull over to get directions. I requested Smith to exit the vehicle for the duration of the traffic stop. When Smith stepped out, I asked if he had any weapons on his person. Smith began reaching in his pockets and I instructed him to remove them. I asked Smith if I could conduct a pat search for weapons. Smith appeared very nervous when he replied that I could and then admitted he had a marijuana pipe in his front right pocket. A pink pipe containing marijuana residue was located inside his front pocket. I asked Smith if he had any other contraband in his vehicle, he stated if he does, then it is not his and he does not know about it.

When asked if I could search the vehicle, Smith stated he would rather I not, but I would not find anything anyways so he did not care. I informed Smith I would be searching the vehicle anyways because a pipe was located on his person, which would have also been inside the vehicle. During my contact with Smith, it should be noted he appeared very jittery and his speech was rapid.

I contacted the front passenger, Cedric Schuman. Schuman stated he was unaware of any contraband that may be inside the vehicle. Schuman appeared very nervous and evaded several of my questions regarding his relationship with Smith and their whereabouts this evening. I located a small green sandwich bag with a pipe containing a white substance in between my patrol vehicle and the suspect vehicle on the ground. I informed Schuman that my patrol car would have been recording and it would have shown if he was the one who threw it from the vehicle. Schuman admitted to throwing the bag from the vehicle, but stated it was Smith's and he did this at the request of Smith because the driver's side window was inoperable.

A bag containing a white powder substance was also located a few feet north of my patrol unit. Schuman also admitted to throwing it out the window. During the vehicle search, a small yellow bag containing foils were located in between the driver's seat and the middle console. An open Coors light can was located directly behind the driver's seat. A pretest showed the pipe and the white substance positive for amphetamines/methamphetamines. The bag of suspected meth weighed 19 grams with the evidence bag it was placed in.

Smith agreed to participate in standardized field sobriety maneuvers. I asked Smith if he had any medical conditions. Smith claimed to have back problems and mentioned he has been depressed. Smith states he sometimes takes medications for depression, but had not today. Smith states he usually wears glasses, but mostly for reading. Smith displayed signs of impairment during the testing and at 2329 hours, after a fifteen minute deprivation period, Smith submitted to a preliminary breath test, which displayed .000g/210L.

At 2343 hours, Smith was placed into custody and transported to ADF. Once there Smith was read his post arrest chemical advisement, and a second 15 minute observation period was began at 0040 hours. At 0057 hours, Smith provided a breath sample into Datamaster #300401 of .000BAC. Smith refused to undergo an evaluation with a drug recognition expert and refused to provide a urine sample at 0058 hours. Smith stated he wished to speak with a lawyer and would no longer be answering questions.

Smith was cited and lodged on possession of controlled substance (28-416(3)) and cited for tampering with physical evidence, refusal to submit to test, possession of drug paraphernalia, speeding 6-10MPH over, improper turn, fail to stay in lane, and DUI -1st offense (AL7000383). Deputy Hicks placed Schuman into custody at 2359 hours and transported him to ADF where he was cited and lodged for possession of control substance (28-416(3)) and cited for tampering with physical evidence(AL7000382).

On the ride to jail, Schuman informed Deputy Hicks the drugs were initially hidden on Smith's person prior to Smith requesting Schuman to throw them out the window. Smith's cell phone that was located on his person, was confiscated for evidence and placed into a Faraday locker under property report number Q2406933. The suspected bag of meth and the pipe have been submitted to NSP lab for further testing.

It is believed the 19 grams of suspected meth located during this traffic stop is more than personal amount and is possibly involved in the sales of narcotics. Smith has no ties to the community, but admitted to leaving the residence 9105 Olive Creek Road, which is known to be a location of frequent drug and criminal activity.

Digital Storage Devices

Your AFFIANT knows from training and experience that digital media devices and related digital storage devices, such as cell phones, can be used to create, edit, delete, share, and store files and other data including, live and deleted documents, photographs, videos, electronic mail (e-mail), search history and other relevant user information.

Your AFFIANT also knows from training and experience that computers and mobile devices, such as cell phones, connected to the Internet, are used to search the World Wide Web for content

and such access can allow users to access and control data such as pictures, videos, documents, and other files.

Your AFFIANT also knows that such devices are often used to communicate and share data with other users and that such digital data can be transferred between various devices. Your AFFIANT knows that information associated with such data may show evidence of current, ongoing, future, and past criminal activity. Your AFFIANT knows that this type of information can be used to identify and locate potential victims, witnesses, and co-conspirators.

Your AFFIANT also knows that data associated with these devices can often include user attribution data that can help identify the person(s) who sent, received, created, viewed, modified, or otherwise had control over particular content.

Your AFFIANT knows from training and criminal investigation experience that individuals also use cellular telephones for the aforementioned purposes, and as a tool for facilitating criminal activity. The data contained on cellular telephones seized in investigations can provide a wealth of information that can assist investigators in determining identity and culpability of participants, including identifying those with knowledge of a criminal offense or identify those who have aided a criminal participant in the commission of a criminal offense. As such, a cellular telephone possessed by criminal participants can serve both as an instrument for committing crime as well as a storage medium for evidence of the crime, including communications to plan, execute, and otherwise document the commission of a crime. Cellular telephones contain location data that can assist in an investigation by both corroborating and disproving statements. Cellular telephones can also show any possible relationships between parties involved through past communications, location data, and contact information stored.

Your AFFIANT is aware from past criminal investigation experience of numerous instances where cellular telephones were used by criminal participants to communicate via voice, text messaging, social media or other communication applications; instances in which criminal participants utilized cellular telephones to photograph themselves, associates and coconspirators; instances in which cellular telephones were used by criminal participants to create videos of their criminal activity; instances where criminal participants have used cellular based internet applications to research crimes they have or intend to participate in; instances in which criminal participants have maintained notes within cellular telephones and instances in which criminal participants used global positioning, mapping and other location services to facilitate inperson meetings with co-conspirators or a victim;

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

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

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

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

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

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

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

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

Your AFFIANT knows the forensic examiner may also need the following items in order to conduct a thorough and accurate search of the devices: computer hardware, software, peripherals,

internal or external storage devices, power supplies, cables; internet connection and use information; security devices; software; manuals; and related material.

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

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

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

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

Your AFFIANT knows from my training and experience, and from information provided to me by Electronic Evidence Unit Personnel that it is necessary to search live and deleted data recovered from digital devices from the time when the device was first used through the time when the device was seized. This is specifically necessary to establish associations between a particular device and associated applications and files to a particular user (or users). This scope of time is necessary to identify potential inculpatory and exculpatory evidence during the planning, execution and post event activities of potential criminal activity. These activities may include communication, contact, calendar entries, pictures, videos, location information (including GPS, navigation, and maps), This scope of time is also necessary to determine accurate device date and time settings, including time zone changes, and allow for the analysis any associated data within a proper context. I know from my training and experience that it is important to understand events of a particular day and time in proper context that may exist before and to attribute particular users of a device and associated applications.

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

The above does constitute grounds of probable cause for the issuance of a Search Warrant for black Apple Iphone in Otterbox case, Lincoln, Lancaster County, Nebraska, for the following items:

Evidence to be searched for includes:

- a. Evidence of other accounts associated with this device including email addresses, social media accounts, messaging "app" accounts, and other accounts that may be accessed through the digital device that will aid in determining the possessor/user of the device;
- b. Evidence of use of the device to communicate with others about the above-listed crime(s), via email, char sessions, instant messages, text messages, app communications, social media, internet usage, and other similar digital communications;
- c. Photographs, images, videos, documents, and related data created, accessed, read, modified, received, stored, sent, moved, deleted or otherwise manipulated;
 - d. Evidence of use of the device to conduct internet searches relating to above listed crime(s);
- e. Information that can be used to calculate the position of the device between the above dates, including location data; GPS satellite data; GPS coordinates for routes and destination queries between the above-listed dates; "app" data or usage information and related location information; IP logs or similar internet connection information, and images created, accessed or modified between the above-listed dates, together with their metadata and EXIF tags;
- f. Evidence of the identity of the person in possession of the device(s) and the associated times and dates. Such evidence may be found in digital communications, photos and video and associated metadata, IP logs, documents, social media activity, and similar data;
- g. Records linking the suspect(s), co-conspirators, victim(s), witness(es) to a certain screen name, handle, email address, Social media identity, etc.;
 - h. Records showing a relationship with victim(s), location(s), other suspects, etc.;
 - i. Names, nicknames, account ID's, phone numbers, or addresses of specific persons;
 - j. Records showing a relationships to particular areas or locations.;
- k. Photographs, images, videos, documents that contain or are evidence of above listed crime(s);
- l. Evidence of purchases, such as items used in planning or carrying out above listed crimes(s);
- m. Internet research history conducted while planning, executing, or covering up to commit above listed crimes(s);
- n. Any live and deleted user attribution data including user accounts, e-mail accounts, passwords, PIN codes, patterns, account names, user names, screen names, remote data storage accounts, documents, files, calendars, metadata, recycle bin files, and any other information and evidence that may demonstrate attribution to a particular user or users;
- o. Any live and deleted applications, programs, or software, used to facilitate the creation, storage, display, or transmission of digital visual recordings and the logs and data associated with the applications, programs or software, and any device backup files;
- p. Any live and deleted audio or visual recording files including files bearing file extensions jpg, jpeg, png, gif, tif, wav, aiff, mp3, mp4, avi, mpg, mpeg, flv, mp4, mov, and wmv along with any descriptive metadata within or associated with the visual recording files, which may include date and time the recording was created, the device used to create the recording and location the recording was made;

- q. Any live and deleted passwords, password files, keys, encryption codes, or other information necessary to access the digital device, software or data stored on the digital device;
- r. Any live and deleted records, documents, programs, applications, information, or materials created, modified, or stored in any form on the digital devises listed in this affidavit, that show the actual user(s) of the computers or digital devices including web browser history; temporary Internet files; cookies, bookmarked or favorite web pages; e-mail addresses used from the computer, MAC IDs and/or Internet Protocol addresses used by the computer; e-mails, instant messages, text messages (SMS/MMS), application data and other electronic communications; address books; contact lists; records of social networking and online service usage; calendar entries, notes, journals, and any software that would allow others to control the digital device such as viruses, Trojan horses, malware, and other forms of malicious software.
 - s. Requesting data for the above listed information from 4-2-2024 to 4-9-2024.

Your AFFIANT would also like to advise the court that the examination of digital devices is a lengthy process requiring special steps to ensure the integrity of the electronic evidence. Therefore, it may not be possible to complete a return for the court within the 10 days normally required by the court

Further AFFIANT saith not;

Dated this	17m day	of An	al	.2024ر
8	nanu	Sin	end	H
	na Schendt, Al		<u> </u>	

SUBSCRIBED to in my presence and swom to before me this 17 day of 2024.

ge of the County Court

Printed Name of Judge