

LPD Case Number: C3-084481

IN THE COUNTY COURT OF LANCASTER COUNTY, NEBRASKA

CR24-1

IN THE MATTER OF THE SEARCH WARRANT
OF THE DESCRIBED PREMISES OF
575 SOUTH 10TH STREET
LINCOLN, LANCASTER COUNTY, NEBRASKA

SEARCH WARRANT RETURN

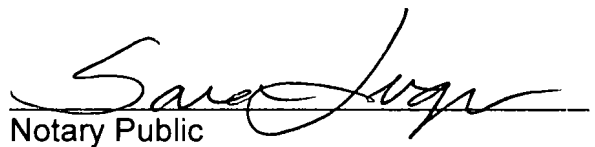
STATE OF NEBRASKA)
)
) ss.
COUNTY OF LANCASTER)

The undersigned states that he received the Search Warrant issued herein on the 11th day of June, 2024, and that he executed the same on the 11th day of June, 2024, by seizing the property described in the Inventory filed herein and by delivering a copy of the Search Warrant for the said property at the place from which the property is taken.



Robert Norton, #1443

SUBSCRIBED to in my presence and sworn to before me this 13th day of June, 2024.


Notary Public

LANCASTER COUNTY
2024 JUN 14 PM 2:54
CLERK OF THE
DISTRICT COURT



002176444D02

Warrant Return & Inventory

Page 1



#261

INVENTORY

IN THE COUNTY COURT OF LANCASTER COUNTY, NEBRASKA

IN THE MATTER OF THE SEARCH WARRANT
OF THE DESCRIBED PREMISES OF
575 SOUTH 10TH STREET
LINCOLN, LANCASTER COUNTY, NEBRASKA

STATE OF NEBRASKA)
)
COUNTY OF LANCASTER)

ss.

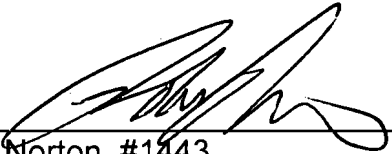
INVENTORY OF PROPERTY
SEIZED BY VIRTUE OF THE
SEARCH WARRANT ISSUED HEREIN

Robert Norton, being first duly sworn on oath, deposes and says the following is an inventory of the property seized by virtue of the Search Warrant issued herein:

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


Digital extraction from Samsung Galaxy smartphone, Serial # RFCT908FZ5V

Inventory made in the presence of John Donahue, #715.



Robert Norton, #1443

SUBSCRIBED to in my presence and sworn to before me this 13th day of June, 2024.



Notary Public

LANCASTER COUNTY
2024 JUN 14 PM 2:54
CLERK OF THE
DISTRICT COURT



RECEIPT

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

-digital extraction from Samsung Galaxy smartphone, Serial # **RFCT908FZ5V**

LANCASTER COUNTY
2024 JUN 14 PM 2:55
CLERK OF THE
DISTRICT COURT

DATED this 11th day of June, 2024.

 1443

Law Enforcement Officer

 # 715

WITNESS

IN THE COUNTY OF LANCASTER COUNTY, NEBRASKA

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

TO: Robert Norton, a Police Officer with the Lincoln Police Departments Special Victims Unit, Lancaster County, Nebraska, and any and all law enforcement officers.

WHEREAS, Robert Norton, 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 for the following items:

a. 1 each, Samsung Galaxy, located in the Lincoln Police Department Electronic Evidence Unit at 605 South 10th Street, Lincoln, Lancaster County, NE, labeled with Property Number Q2321189 labeled with Case Number C3-084481;

Evidence to be searched for includes:

- a. Evidence of use of the device to communicate with others about the above-listed crime(s), chat sessions, instant messages, text messages, internet usage, and other similar digital communications;
- b. Photographs, images, videos, documents, and related data created, accessed, read, modified, received, stored, sent, moved, deleted or otherwise manipulated;
- c. Evidence of use of the device to conduct internet searches relating to above listed crime(s);
- d. 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;

LANCASTER COUNTY
2024 JUN 14 PM 2:55
CLERK OF THE DISTRICT COURT

e. 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, and similar data;

f. Records showing a relationship with victim(s), location(s), other suspects, etc.;

g. Names, nicknames, account ID's, phone numbers, or addresses of specific persons;

h. Records showing a relationships to particular areas or locations.;

i. Photographs, images, videos, documents that contain or are evidence of above listed crime(s);

j. Evidence of purchases, such as items used in planning or carrying out above listed crimes(s);

k. Internet research history conducted while planning, executing, or covering up to commit above listed crimes(s);

l. Any live and deleted user attribution data including user 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;

m. 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;

n. 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;

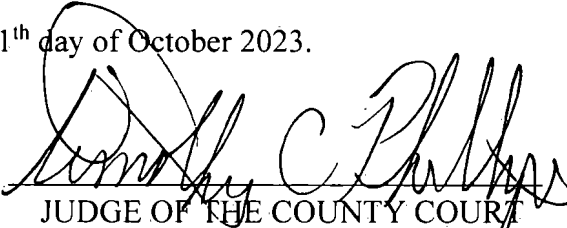
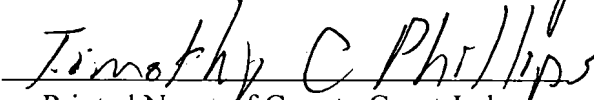
o. Any live and deleted passwords, password files, keys, encryption codes, or other information necessary to access the digital device, software or data stored on the digital device;

p. Any live and deleted records, documents, programs, applications, information, or materials created, modified, or stored in any form on the digital devices listed in this affidavit, that show the actual user(s) of the computers or

digital devices including web browser history; temporary Internet files; cookies, bookmarked or favorite web pages; MAC IDs and/or Internet Protocol addresses used by the computer, instant messages, text messages (SMS/MMS), application data and other electronic communications; address books; contact lists; records of social networking and online service usage; calendar entries, notes, journals, and any software that would allow others to control the digital device such as viruses, Trojan horses, malware, and other forms of malicious software.

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

Given under my hand and seal this 11th day of October 2023.


JUDGE OF THE COUNTY COURT

Printed Name of County Court Judge



IN THE COUNTY COURT OF LANCASTER COUNTY, NEBRASKA

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

Robert Norton, being first duly sworn upon oath deposes and states that he is a Investigator for the Lincoln Police Departments Special Victims Unit, Lancaster County, Nebraska. AFFIANT further states he is currently involved in the investigation of First-Degree Sexual Assault of a Child, Nebraska State Statute- 28-319, occurring at 401 'C' Street, Lincoln, 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:
(EXAMPLES)

a. 1 each, Samsung Galaxy, located in the Lincoln Police Department Electronic Evidence Unit at 605 South 10th Street, Lincoln, Lancaster County, NE, labeled with Property Number Q2321189 labeled with Case Number C3-084481;

The items to be searched are currently located at the Lincoln Police Department Electronic Evidence Unit, 605 South 10th, Lincoln, Lancaster County, State of Nebraska. The item(s) to be searched shall be delivered to the Electronic Evidence Unit located at 605 South 10th, Lincoln, Lancaster County, State of Nebraska for digital forensic processing and analysis. The Electronic Evidence Unit forensic examiners may designate additional forensic services, as they may deem necessary to complete the analysis. Once examination and analysis 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 September 20, 2023, Officer Schiefelbein #1686, a School Resource

LANCASTER COUNTY
2024 JUN 14 PM 2:55
CLERK OF THE
DISTRICT COURT

Officer for Lincoln Public Schools, was contacted by a middle school counselor after a 13-year-old female student (DOB: March 18, 2010), identified hereafter as 'L.A.', disclosed she had been sexually assaulted in the past. L.A. reported that her mother's fiancé, Daniel Ostiguin, a 28-year-old male with a date of birth of November 23, 1994, touched her privates. L.A. stated she never told her mother; however, told her 12 year old brother, 'J.A.'

Investigator Robert Norton of the Lincoln Police Departments Special Victims Unit, arranged for L.A. to be forensically interviewed. During the interview, L.A. described in detail how Daniel touched her inappropriately between the ages of 11 and 13 at their residence at 401 'C' Street in Lincoln, Lancaster County, Nebraska. L.A. said she was 11 years old the first time she was awakened by Daniel getting into bed with her. Daniel put his hand under L.A.'s clothing and touched L.A.'s thighs, stomach and vagina. L.A. described how Daniel used his fingers to manipulate a part of her vagina in between the labia. Daniel got up and left after L.A. refused to go to the bathroom with him when asked. L.A. disclosed how there were numerous other times in which Daniel entered her bedroom while she was sleeping and touched her butt, thigh's and stomach, on top of her clothes.

At the conclusion of the forensic interview, Investigator Norton was present when L.A. completed a recorded phone call to Daniel, talking about her molestation by him and how she wants it to stop. Daniel apologized to L.A. and told her that it would not happen again. Daniel blamed his actions on depression and past incidents occurring in his childhood, when L.A. asked him why he touched her vagina. The recorded phone call was completed by L.A. calling Daniel's known phone number of 402-610-1728.

Investigator Norton interviewed L.A.'s 12-year-old brother, J.A. J.A. confirmed that L.A. told her a while ago that Daniel had sexually assaulted her while sleeping in the bedroom that they share. J.A. reported to witnessing Daniel enter their bedroom on numerous after being awakened, but didn't witness anything as he pretended to be asleep.

On September 20, 2023 at approx. 1800 hours, Daniel agreed to meet Investigator Norton at LPD Headquarters for an interview. Upon Daniel's arrival, Daniel called Investigator Norton from his phone number, 402-610-1728, to say he had arrived at the police station. Daniel waived his Miranda Rights and agreed to talk about the investigation without an attorney present. Daniel denied ever having sexual contact with L.A. He refused to consent to a forensic examination of his smartphone. Daniel's smartphone, a green Samsung Galaxy, was tagged into the Lincoln Police Department's Property Unit under property number Q2321189. Daniel was arrested and transported to jail.

On October 10, 2023, Investigator Norton contacted L.A. and spoke with her about her phone interactions with Daniel in the past. L.A. confirmed that she has had phone and text conversations with Daniel in the past. L.A. also said she believes Daniel has utilized his smartphone to take pictures of her siblings and herself in her bedroom before.

Because Daniel has awakened L.A. in the past while she was sleeping in her bed, your AFFIANT is concerned that Daniel has utilized his smartphone to record himself molesting L.A. Your AFFIANT has training and experience with past investigations in which perpetrators have used their smartphones to record molestations and record a victim in a state of undress.

Digital Storage Devices

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

Your AFFIANT also knows from training and experience that computers and mobile devices, such as cell phones, connected to the Internet, are used to search the World Wide Web for content and such access can allow users to access and control data such as pictures, videos, documents, and other files.

Your AFFIANT also knows that such devices are often used to communicate and share data with other users and that such digital data can be transferred between various devices. Your AFFIANT knows that information associated with such data may show evidence of current, on-going, future, and past criminal

activity. Your AFFIANT knows that this type of information can be used to identify and locate potential victims, witnesses, and co-conspirators.

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

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

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

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

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

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

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

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

Your AFFIANT knows, that, wholly apart from user-generated files and data, digital devices and media typically store, often without any conscious action by the user, electronic evidence pertaining to virtually all actions taken on the digital

device, and often information about the geographic location at which the device was turned on and/or used. This data includes logs of device use; records of the creation, modification, deletion, and/or sending of files; and uses of the internet, such as uses of social media websites and internet searches/browsing.

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

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

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

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

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

locate and identify that evidence whose seizure is authorized by this warrant. The unaltered device and the image are then preserved in evidence.

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

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

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

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

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

The above does constitute grounds of probable cause for the issuance of a Search Warrant for a Samsung Galaxy smartphone under property number Q2321189, at 605 South 10th Street, Lincoln, Lancaster County, Nebraska, for the following items:

Evidence to be searched for includes:

a. Evidence of use of the device to communicate with others about the above-listed crime(s), chat sessions, instant messages, text messages, internet usage, and other similar digital communications;

b. Photographs, images, videos, documents, and related data created, accessed, read, modified, received, stored, sent, moved, deleted or otherwise manipulated;

c. Evidence of use of the device to conduct internet searches relating to above listed crime(s);

d. 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;

e. 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, and similar data;

f. Records showing a relationship with victim(s), location(s), other suspects, etc.;

g. Names, nicknames, account ID’s, phone numbers, or addresses of specific persons;

h. Records showing a relationships to particular areas or locations.;

i. Photographs, images, videos, documents that contain or are evidence of above listed crime(s);

j. Evidence of purchases, such as items used in planning or carrying out above listed crimes(s);

k. Internet research history conducted while planning, executing, or covering up to commit above listed crimes(s);

l. Any live and deleted user attribution data including user 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;

m. 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;

n. 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;

o. 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;

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

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

Further AFFIANT saith not;

Dated this 11th day of October 2023.

Robert Norton 10/11/23
Robert Norton, AFFIANT

SUBSCRIBED to in my presence and sworn to before me this 11th day of
October, 2023.

Timothy C Phillips
Judge of the County Court
Timothy C Phillips
Printed Name of Judge

