

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 10TH)
STREET, LINCOLN,)
LANCASTER COUNTY, NE)
Q2401153)

CR24-1

SEARCH WARRANT
RETURN

LANCASTER COUNTY
2024 FEB 16 PM 3:18
CLERK OF THE
DISTRICT COURT

STATE OF NEBRASKA)
COUNTY OF LANCASTER)

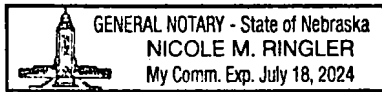
ss.

The undersigned states that he/she received the search warrant issued herein on the 24th day of January, 2024 and that he/she executed the same on the 24th day of January, 2024 and on the 15th day of February, 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 15 day of February, 2024.

Joanna Dimas
Inv. Joanna Dimas

SUBSCRIBED AND SWORN to before me this 15th day of February, 2024.



Nicole M. Ringler
Notary Public

C4000542



S

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)
10TH STREET, LINCOLN,)
LANCASTER COUNTY, NE)
Q2401153)

INVENTORY

CLERK OF THE
DISTRICT COURT

2024 FEB 16 PM 3:19

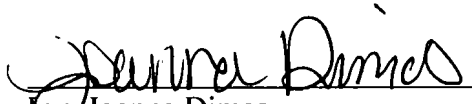
LANCASTER COUNTY

STATE OF NEBRASKA)
County of Lancaster) ss.
County of Lancaster)

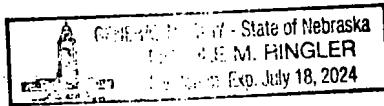
Inv. Joanna Dimas being first duly sworn upon oath, deposes and states the following is an inventory of property seized by virtue of the warrant issued herein:

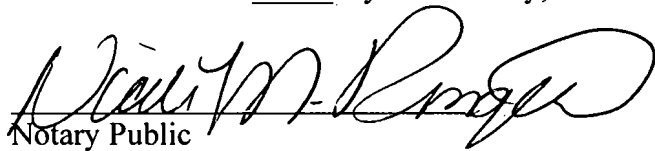
- Digital File Extraction

DATED this 15 day of February, 2024.


Inv Joanna Dimas

SUBSCRIBED AND SWORN to before me this 15th day of February, 2024.




Notary Public

C4000542

RECEIPT

The undersigned hereby acknowledges receipt of the following described property seized from 1 each, black Samsung Galaxy S10 in a black case, located in the Lincoln Police Property Evidence Unit at 575 South 10th, Lincoln, Lancaster County, NE, labeled with Property Number Q2401153 labeled with Case Number C4000542:

Digital File Extraction

LANCASTER COUNTY
2024 FEB 16 PM 3:19
CLERK OF THE
DISTRICT COURT

DATED this 15 day of February, 2024.



Law Enforcement Officer



WITNESS

C4000542

IN THE COUNTY OF LANCASTER COUNTY, NEBRASKA

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

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

WHEREAS, Joanna Dimas, 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 1 each, black Samsung Galaxy S10 in a black case, located in the Lincoln Police Property Evidence Unit at 575 South 10th, Lincoln, Lancaster County, NE, labeled with Property Number Q2401153 labeled with Case Number C4000542, Lincoln, Lancaster County, Nebraska, for the following items:

- 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 sexual assault of a child and incest, 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 sexual assault of a child and incest;

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 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 or co-conspirators to a certain screen name, handle, email address, Social media identity, etc.;

h. Records showing a relationship with victim, location, 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 sexual assault of a child and incest;

l. Evidence of purchases, such as items used in planning or carrying out sexual assault of a child, incest or tampering with witnesses;

m. Internet research history conducted while planning, executing, or covering up sexual assault of a child and incest;

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 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; 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.

Your AFFLIANT 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 24th day of January, 2024



JUDGE OF THE COUNTY COURT

Laurie J Teresh
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)

Joanna Dimas, being first duly sworn upon oath deposes and states that she is an Investigator for the Lancaster County Sheriff's Office, Lancaster County, Nebraska. AFFIANT further states he is currently involved in the investigation of 1st degree sexual assault of a child, witness tampering and incest with a child under the age of 18 occurring at 630 Maple St, Hickman, 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 to be searched for digital evidence are particularly described as:

a. 1 each, black Samsung Galaxy S10 in a black case, located in the Lincoln Police Property Evidence Unit at 575 South 10th, Lincoln, Lancaster County, NE, labeled with Property Number Q2401153 labeled with Case Number C4000542;

The items to be searched are currently located at the Lincoln Police Department Property Unit, 575 South 10th, Lincoln, Lancaster County, State of Nebraska. The item 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 January 19th, 2024, the Sheriff's Office received DHHS intake #0104404. Joshua Brokering was self-reporting that he was engaging in an

LANCASTER COUNTY
2024 FEB 16 PM 3:19
CLERK OF THE
DISTRICT COURT

inappropriate physical relationship with his adopted daughter, a 12-year-old female furthermore known by her initials of B.A.

Your Affiant knows that Health and Human Services employee Katherine Lantis and Deputy Uzzell, an employee of the Lancaster County Sheriff's Office, currently assigned to the Patrol Division, arrived at 630 Maple St, Hickman, Lancaster County, Nebraska. and spoke with Joshua's wife, Dorothy Brokering. Your Affiant knows that Dorothy told Deputy Uzzell on the night of January 18th, 2024, Joshua took her to that he had inappropriately touched B.A. Dorothy told Katherine Lantis that Josh had taken her out to his office, an outbuilding behind the residence, and stated he was having an inappropriate relationship with B.A. for approximately a week and a half. Dorothy said that Joshua did not provide her further details. Dorothy said that she had warned Joshua to be careful with B.A., due to her history of sexual abuse as well as ADHD and attachment issues. Dorothy had witnessed Joshua snuggling on the couch with B.A. and would have to remind him to give her more space. Dorothy said that Joshua had a hard time with this due to his naivety and having been sheltered.

B.A. has an 11-year-old brother, furthermore, known by his initials of P.A. On January 15th, 2024, P.A. had been playing at a neighbor's home and returned to his residence with a friend to play 'Fortnite'. P.A. could not find B.A. or Joshua. P.A. was looking for Joshua to get permission to play and heard the downstairs shower on. P.A. said that he could hear a "moaning sound" coming from the bathroom. P.A. described the moaning as someone not being hurt and knew it was sexual. P.A. thought it was B.A. and then believed Joshua and B.A. were in the shower having sex. P.A. felt uncomfortable and flustered. B.A. then came out of the bathroom with wet hair and Joshua exited the bathroom behind her. P.A. ran to his grandmother, Cheryl Brokering's, home several houses down and told her what he had witnessed. Cheryl then called Joshua and Joshua said that he had been sleeping. Joshua then arrived at Cheryl's home and said that he had actually been in the furnace room. P.A. told Joshua that he knew he was lying as he had seen them standing by the bathroom together and told Joshua that he had heard moaning. Cheryl and Joshua then decided they would not tell Dorothy because it was best for the family, and they needed to keep the family together. Cheryl and Joshua told the children this was what they must do.

During an interview at BraveBe Child Advocacy Center, B.A. stated that Joshua had first started with just hugging her. Joshua started to come into B.A.'s room and lay on her bed and talk about her friends and church. This progressed to back rubs and then Joshua began to remove her shirt for a backrub then her bra and then eventually progressed to them both being naked together. Joshua would touch B.A.'s breasts and vagina. B.A. said this made her feel scared and that she hated it. B.A. would try to push Joshua's hands away or tell him that he needed to go away so she could go to bed. When Joshua would lay in her bed naked with her, she could feel his leg hair poking her and his chest against her. B.A. tried to scoot away but Joshua would follow and hold her against him with his hand over her stomach. Eventually Joshua began to digitally penetrate B.A.'s vagina. Joshua usually came into B.A.'s room at night to molest her. Another time B.A. went out to Joshua's office in the outbuilding to ask for chocolate. B.A. stayed in the office on the couch to use B.A.'s phone to text a friend and Joshua touched her breasts and digitally penetrated her vagina on this couch. The last time was when P.A. found Joshua and P.A. in the shower. P.A. stated that Joshua had told her to go take a shower since she hadn't. B.A. went into the laundry room and when she turned around Joshua was there. Joshua then took B.A. into the shower and digitally penetrated her vagina. B.A. told Joshua not to and he said to be quiet because he thought P.A. might be home and he didn't want to get caught. After P.A. saw Joshua and B.A. and ran away Joshua told B.A. that they needed to come up with a plan to keep the secret. B.A. Joshua suggested that he say he was in the furnace room scooping kitty litter or was asleep. B.A. told him she did not think that would work because P.A. had heard and seen what was happening. After these things happened B.A. said that she had to wash all of her bedding since Joshua had been on them. B.A. has been sleeping on the floor because she is uncomfortable with being in her bed since Joshua began to molest her. B.A. said that Joshua digitally penetrated her vagina 5 or 6 times before he was caught by P.A. B.A. drew a layout of her home and the outbuilding and detailed her bedroom, the downstairs bathroom and the outbuilding where Joshua has his home office as the places where he molested her.

Joshua was lodged at Lancaster County Adult Detention Facility. Joshua's phone was with him and was seized by the Sheriff's Office in reference to this investigation. Joshua denied consent to download his phone. Your Affiant knows that Joshua has been making phone calls from Lancaster County Adult Detention

Facility. In reviewing Joshua's jail calls, the call states that the call will be recorded and is subject to monitoring at any time. On January 22nd, 2024, at 4:53 PM Joshua contacts his wife, Dorothy. Joshua wants to know if he is able to go to his house, specifically his office, when the children are not there. On January 23rd, 2024, at 12:09 PM Joshua contacts his wife Dorothy and wants to see about asking the Judge for favors. Joshua wants to have access to his office when the children are not there and do house repairs. On January 23rd, 2024, at 3:47 PM, Joshua contacted his mother, Cheryl. Joshua is upset that he is being charged with incest since B.A. is his adopted daughter. Joshua states, 'I have a phone I bought as a replacement. It's the same exact phone. It's in my office if you want to go there at some point. Do you want to just make a mental note of where it is? Because I think I know of where exactly to tell you to get it.' Joshua asks Cheryl to ask Verizon if they can deactivate the SIM card on the device the Sheriff's office seized and if they can activate a new one on the same account. At 14:20 minutes Joshua continues, 'It is in the right set of lockers, ya know. There's two sets right? The right set, it's in the I think the middle door where all the food is. And I think it is on the middle-ish shelve on the left, I think it's like a cardboard box roughly the size of a phone, like an inch thick. You can just pop it open and see the phone right there.' At 15:28 minutes Joshua asks Cheryl to open his laptop screen so that he can access it remotely. Cheryl says that there is a 'laptop here' and Joshua says that is the laptop he uses for 'Email and Facebook and Stuff'. Joshua then tells Cheryl to grab the laptop, computer mouse, computer mouse charger, and backpack. Cheryl asks what the 'code to get in' is and Joshua says, '8888'.

On January 23rd, 2024, your Affiant and Investigators with the Lancaster County Sheriff's Office executed a search warrant at 630 Maple St, Hickman, Lancaster County, Nebraska. Pursuant to the warrant Investigators seized 7 cellular devices, including the device mentioned in Joshua's jail phone calls, and the Dell laptop discussed by Joshua on his jail phone call. Your Affiant observed multiple cameras throughout the residence, including a Ring camera system at the front door. Your Affiant observed a Wink camera system to be in place outside of B.A.'s bedroom pointing in the direction of the basement bathroom and in the kitchen of the home. A Wink camera was placed on the exterior of the pedestrian door to the outbuilding office and two cameras in place on the interior of the

office. This camera system is a Wifi based camera system that is accessed via an app on a cellular device.

On January 24th, 2024, your Affiant contacted Dorothy again. Dorothy stated that Joshua is the only one that has access to the camera system and that it is accessed through his cellular device. Dorothy stated that through the application on his cellular device Joshua can access and store video from the Wink system. Dorothy was unsure how long video was stored by the program without Joshua saving the video himself.

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 sexual assault, sexual assault of a child and witness tampering. Through your AFFIANT's training and past experience, your AFFIANT is aware that cellular telephone data can provide valuable insight for sexual assault, child sexual assault and

incest 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 1 each, black Samsung Galaxy S10 in a black case, located in the Lincoln Police Property Evidence Unit at 575 South 10th, Lincoln, Lancaster County, NE, labeled with Property Number Q2401153 labeled with Case Number C4000542 for the following items:

- 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 sexual assault of a child and incest, 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 sexual assault of a child and incest;
- 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 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 or co-conspirators to a certain screen name, handle, email address, Social media identity, etc.;
- h. Records showing a relationship with victim, location, 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 sexual assault of a child and incest;
- l. Evidence of purchases, such as items used in planning or carrying out sexual assault of a child, incest or tampering with witnesses;
- m. Internet research history conducted while planning, executing, or covering up sexual assault of a child and incest;
- 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 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; 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.

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 24 day of January, 2024.

Joanna Dimas
Joanna Dimas, AFFIANT

SUBSCRIBED to in my presence and sworn to before me this 24th day of January, 2024.

[Signature]
Judge of the County Court

Laure J Terrell
Printed Name of Judge

