

RECEIPT

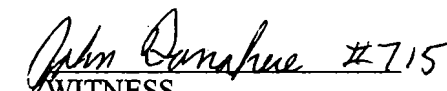
The undersigned hereby acknowledges receipt of the following described property seized from the Black Cricket smartphone, located in the Lincoln Police Property Evidence Unit at 575 South 10th Street, Lincoln, Lancaster County, Nebraska, labeled with Property Number Q2402758 and Case Number C4-012515

Full file system data extraction from phone narrowed to data between dates February 1, 2024, 0001 hrs to February 11, 2024, 1800 hrs

LANCASTER COUNTY
2024 FEB 26 PM 4:01
CLERK OF THE
DISTRICT COURT

DATED this 16th day of February, 2024

 #1187
Law Enforcement Officer

 #715
WITNESS

IN THE COUNTY OF LANCASTER COUNTY, NEBRASKA

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

TO: Christopher Champoux, a Investigator with the Lincoln Police Department, Lancaster County, Nebraska, and any and all law enforcement officers and agents thereof.

WHEREAS, Christopher Champoux has filed an Affidavit before the undersigned Judge of the County Court of Lancaster County, Nebraska, and said written Affidavit, having been duly considered, 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 places(s) listed in Attachment A to seize the listed property, as well as search the property for the digital evidence listed in Attachment B.

Law enforcement is authorized to seize the aforementioned items.

This search warrant shall be executed and returned within ten (10) days to a Clerk of the Lancaster District Court, Nebraska. In the event records are not received from within ten (10) days, law enforcement is authorized to return the search warrant within ten (10) days of receipt of the digital evidence.

Given under my hand and seal this 14th day of February, 2024.

Timothy C Phillips

Judge of the County Court
Timothy C Phillips

Printed Name of Judge



LANCASTER COUNTY
2024 FEB 26 PM 4:01
CLERK OF THE
DISTRICT COURT

ATTACHMENT A

Property to Be Searched

This warrant is directed to seize and search the following;

- Black Cricket smart phone located in the Lincoln Police Property Evidence Unit at 575 South 10th Street, Lincoln, Lancaster County, NE, labeled with Property Number Q2402758 and Case Number C4-012515.

129

ATTACHMENT B

Particular Things to be Seized

To the extent that the information described in Attachment A is within the possession, custody, or control of the Lincoln Police Department it is requested to search for and seize the following records for each item listed in Attachment A to include including any live and/or deleted data for the time frame of February 01, 2024 at 0001hours CDT/CST to February 11, 2024 at 1800 hours CDT/CST, specifically for the following items:

1. Device identifiers, information and configurations
2. User account information and any associated accounts on the device
3. Call logs
4. Contact lists
5. Short Message Service (SMS), Multimedia Messaging Service (MMS) messages and instant messages;
6. Chat messages from installed applications;
7. Email messages;
8. Installed applications and their corresponding accounts and data;
9. Images and associated metadata;
10. Videos and associated metadata;
11. Audio files, including voicemails, and associated metadata;
12. Document files and associated metadata;
13. Internet browsing history including bookmarks, searches, browser cookies and other associated cache files;
14. Location data to include cellular tower connections, GPS (Global Positioning System) fixes, waypoints, routes, tracks, maps, and associated metadata;
15. Wireless networks, Bluetooth, IP addresses, and synchronization connection history;
16. Memos and notes (typed and voice);
17. User dictionary;
18. Calendar information;
19. Passwords, keychains;
20. Databases and file systems;
21. Device activity logs and application usage logs;
22. Photographs of the device and any related information or data for this search warrant

In order to obtain and search the data from the aforementioned device:

TCP

1. Data may be obtained from the physical memory of the device itself as well as from any data storage devices housed within the device, specifically Secure Digital (SD) and Subscriber Identification Module (SIM) cards;
2. Data from the aforementioned cellular telephone may be searched from the device's active file system as well as unallocated space as to recover deleted data and file fragments;
3. Attempts will be made to obtain the cellular phone's data by only making unobtrusive revocable setting changes to permit the digital extraction of the data; however, if necessary, the device may require disassembly to obtain the desired data which may render the device inoperable;
4. Law enforcement is authorized to copy, forensically image, view, photograph, record and conduct forensic analysis of the data obtained from the aforementioned cellular telephone as well as any data storage devices within;
5. Law enforcement may enlist the aid of additional law enforcement officers or other third parties who are trained in conducting forensic analysis of the data in retrieving and analyzing the data. When files have been deleted, they can be potentially recovered later using forensic tools. Furthermore a person with familiarity with how cellphones work may, after examining the data, be able to draw conclusions about how the device was used, the purpose of its use, who used it, where and when;
6. Law enforcement or their agents may be required to examine every file and scan its contents briefly to determine whether it falls within the scope of the warrant. This is necessary as it is difficult to know prior to the search the level of technical ability of the device's user and data can be hidden, moved, encoded or mislabeled to evade detection;
7. Law enforcement will complete a timely search of the cellular telephone as failure to do so could result in the irrevocable loss of data due to accidental or intentional destruction. The device could be damaged, remotely erased or contain internal destructive mechanisms which could destroy the data.

IN THE COUNTY COURT OF LANCASTER COUNTY, NEBRASKA

LANCASTER COUNTY

2024 FEB 26 PM 4:01

CLERK OF THE DISTRICT COURT

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

Christopher Champoux, being first duly sworn upon oath deposes and states that he is an Investigator for the Lincoln Police Department, Lincoln, Lancaster County, Nebraska. AFFIANT states he is currently involved in the investigation of a Child Abuse, Statute 28-707, occurring on 02-11-2024, at 1708 S. 6th Street #2, Lincoln, Lancaster County Nebraska. AFFIANT has reviewed case reports regarding this investigation prepared by other involved Law Enforcement Officers.

Affiant's Background

Your affiant has been a police officer for the Lincoln Police Department since 1997. Since 2008, your Affiant has been investigating misdemeanor and felony crimes with the Lincoln Police Department to include homicide, child abuse, sexual assault, human trafficking, child enticement, and pornography. Your Affiant has training and experience in conducting criminal investigations.

This Affidavit is submitted in support of a search warrant. Since this Affidavit is being submitted for the limited purpose of securing a search warrant, your Affiant not set forth every fact known to me regarding this investigation. The statements contained in this Affidavit are based in part on the investigation that your Affiant has conducted, and information provided to your Affiant by other law enforcement officers verbally, and through written reports.

Case Facts

On 02-11-2024 at 12399hrs, Lincoln Police Officers and Lincoln Fire and Rescue Personnel were dispatched to 1708 S. 6th #2 on a report of a five year old child not breathing. Shortly thereafter, dispatch updated information to the responders identifying that there were five children suffering from excessive carbon monoxide exposure. Upon first responders arrival, the five children ages 3 weeks to 8 years , along with their mother, Ariel Arenas were found to be in medical distress and transported to an area hospital for treatment and evaluation.

Ariel Arenas reported to Lincoln Police Officers that she placed all five of her children

into her vehicle which was parked in the closed garage of her residence. Ariel Arenas stated she left the children in the running vehicle, in the closed garage for 30 to 60 minutes when she discovered her five year old had collapsed. Ariel Arenas then retrieved the unconscious child and went outside the garage yelling for help which resulted in neighbors calling 911. Ariel Arenas claimed she was unaware of the life-threatening situation she placed her children in by placing them in a running vehicle in a closed garage for 30 to 60 minutes.

While Ariel Arenas and her five children were receiving treatment at St. Elizabeths Hospital, a black Cricket Smartphone was located in the car seat of Ariel's 3 week old baby. This is the same car seat the 3 week old was seated in while in the running vehicle in the closed garage. This Cricket Smart phone was collected and tagged into Lincoln Police Property and Evidence unit under #Q2402758.

Based on your Affiants training and experience, carbon monoxide poisoning is a common method used in efforts to end one's life or the life of others. Investigator Champoux interviewed the father of two of Ariel's children, Efrain Izaguirre. Mr. Izaguirre advised Ariel has threatened on more than one occasion in the past to kill herself and her children. Officer Grell provided information received from Ariel Arenas that the carbon monoxide detectors were sounding an audible alarm inside the residence while the children were in the running car parked in the closed garage. Ariel Arenas reported that she then unplugged the carbon monoxide detectors.

Technical Information Regarding Cell Phones and Searches

Through your Affiant's training and past experience, and from information provided by Electronic Evidence Unit forensic examiners, your Affiant is aware that cellular telephone data can provide valuable insight for Child Abuse 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.

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 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.

On a cellular telephone, data can be created in a matter of moments because most operations can be performed almost instantly, which would be relevant to the incident being investigated. The data can be created intentionally or accidentally by the user, or automatically by the device itself as a part of its regular functioning. Your Affiant seeks to complete a comprehensive and unbiased examination of the data on the device for information which could aid in the investigation; seeking only prescribed information would jeopardize the completeness of the search as it is typically unknown how the cellular telephone was used or the technical ability and intent of the user before the device has been examined.

Your Affiant knows 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. Data generally is stored on the physical memory of the device, but also can be stored on removable storage devices such as Secure Digital (SD) and Subscriber Identification Module (SIM) cards. A forensic examiner may be able to recover information deleted by the user throughout the working life span of the device.

The following are examples of how types of data on digital devices can assist investigators. A full, all inclusive list would be impossible due to the ever increasing development of digital devices and their applications.

1. Phone information, configurations, calendar events, notes and user account information which can be used to identify or confirm who owns or was using a cellular telephone. Because of their small size, cellular telephones can easily be passed from one person. As such it is necessary to document evidence that reveals or suggests who possessed or used the device. This evidence is akin to the search for venue items when executing a search warrant at a residence.
2. Call logs can establish familiarity between people involved in an incident. These records are consistently stamped with dates and times which can be significant regarding the reconstruction of the timeline of events regarding an investigation. Associated contact lists stored in the device can provide names to correspond with voice calls as well as other forms of communication. Voicemails can indicate the purpose of the phone call when the phone call was not answered. This information can also be invaluable to establish conspirators, witnesses and suspect information.
3. Communication records from SMS and MMS messaging, chats, instant messages and e-mails can provide invaluable insight to establish an individual's level of culpability and knowledge regarding an investigated incident. It is not uncommon for users to send and receive dozens and even hundreds of messages a day which document the person's activities and can aid in completing an investigation.
4. Data from associated supplemental software applications (apps), both standard and manually installed, stored on the cellular telephone can demonstrate the user's association with investigated people, locations and events. Cellular telephones have the ability to run apps which allow them to increase their functionality. Common programs include social media applications such as Facebook and Twitter as well as messaging applications Snapchat and Facebook Messenger to name a few. These applications are increasingly used as alternative methods for users to communicate from the standard messaging service as they offer additional functionality. Many of these applications are able to determine the user's geographic location which can be instrumental to completing an investigation.
5. Media files such as images, videos, audio and documents provide first-hand documentation of actions regarding an event. Additionally, files can contain embedded metadata that show additional information which is valuable to investigators such as when and where the file was created. Cellular telephones have the ability to create, store and exchange media with other devices and computers.

6. Internet browsing history including bookmarks, browser cookies and other associated cache files stored on cellular telephones can demonstrate the planning or desire to participate in a crime by documenting the viewing of websites associated with the incident.
7. Cellular tower connections, GPS data, wireless networks, Bluetooth and synchronization logs can associate the cellular telephone with being in proximity of a location or other digital devices. Viewing this data can demonstrate that the device, and thus also its user, was in a location associated with an incident.
8. The user dictionary on a phone contains user generated entries such as names and uncommon words. The presence of these records can demonstrate familiarity with the crime being investigated.
9. Device generated files and data, wholly apart from user-generated files and data, contains electronic evidence pertaining to virtually all actions taken on the digital device, often without any conscious action by the user. This data is stored in multiple databases within a file system, which are determined by the application creating the data. This data includes logs of device use; records of the creation, modification, deletion, and/or sending of files; uses of the internet, such as uses of social media websites and internet searches/browsing; 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 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 the warrant authorizes for seizure, and to assist in securing such evidence. For the technical reasons described, the digital evidence listed above shall be submitted to the Electronic Evidence Unit located at 605 South 10th Street, Lincoln, Lancaster County, State of Nebraska for digital forensic processing and analysis.

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 digital devices are constantly changing system data on the device as programmed by their manufacturer. Additionally, your Affiant knows that searching the digital device itself would irreversibly alter data and/or evidence on the device. To search a device for evidence, the commonly accepted best practice of digital forensics is to utilize forensic software to obtain an extraction of the data on the device. Attempts will be made to obtain the devices data by only making unobtrusive revocable changes to the system settings to permit the digital extraction of the data. If necessary, the device may require disassembly to obtain the desired data which may render the device inoperable. These processes do not change or alter any of the user data stored on the device. The extraction is then searched using analysis software to locate, identify, and seize the evidence authorized by this warrant. The device and the image are then preserved in evidence.

The item(s) has/have been stored in a manner in which its/their contents are, to the extent material to this investigation, in substantially the same state as they were when the device(s) first came into the possession of the Lincoln Police Department.

The item(s) to be searched shall be delivered to the Electronic Evidence Unit located at 605 South 10th Street, 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 or pursuant to Neb. Rev. Stat. §29-820.

Your Affiant requests authorization to search for and seize the listed items in Attachment B, hereby attached and incorporated by reference.

This search warrant shall be executed and returned within ten (10) days to a Clerk of the Lancaster District Court, Nebraska. In the event records are not received from within ten (10) days, your Affiant requests authorization to return the search warrant within ten (10) days of receipt of the records.

Further AFFIANT saith not;

Dated this 14 day of February, 2024

CCC

Christopher Champoux AFFIANT

SUBSCRIBED to in my presence and sworn to before me this 14th day of February, 2024.

Timothy C Phillips
Judge of the County Court

Timothy C Phillips
Printed Name of Judge



ATTACHMENT A

Property to Be Searched

This warrant is directed to seize and search the following;

- Black Cricket smart phone located in the Lincoln Police Property Evidence Unit at 575 South 10th Street, Lincoln, Lancaster County, NE, labeled with Property Number Q2402758 and Case Number C4-012515.

128

ATTACHMENT B

Particular Things to be Seized

To the extent that the information described in Attachment A is within the possession, custody, or control of the Lincoln Police Department it is requested to search for and seize the following records for each item listed in Attachment A to include including any live and/or deleted data for the time frame of February 01, 2024 at 0001hours CDT/CST to February 11, 2024 at 1800 hours CDT/CST, specifically for the following items:

1. Device identifiers, information and configurations
2. User account information and any associated accounts on the device
3. Call logs
4. Contact lists
5. Short Message Service (SMS), Multimedia Messaging Service (MMS) messages and instant messages;
6. Chat messages from installed applications;
7. Email messages;
8. Installed applications and their corresponding accounts and data;
9. Images and associated metadata;
10. Videos and associated metadata;
11. Audio files, including voicemails, and associated metadata;
12. Document files and associated metadata;
13. Internet browsing history including bookmarks, searches, browser cookies and other associated cache files;
14. Location data to include cellular tower connections, GPS (Global Positioning System) fixes, waypoints, routes, tracks, maps, and associated metadata;
15. Wireless networks, Bluetooth, IP addresses, and synchronization connection history;
16. Memos and notes (typed and voice);
17. User dictionary;
18. Calendar information;
19. Passwords, keychains;
20. Databases and file systems;
21. Device activity logs and application usage logs;
22. Photographs of the device and any related information or data for this search warrant

In order to obtain and search the data from the aforementioned device:

1. Data may be obtained from the physical memory of the device itself as well as from any data storage devices housed within the device, specifically Secure Digital (SD) and Subscriber Identification Module (SIM) cards;
2. Data from the aforementioned cellular telephone may be searched from the device's active file system as well as unallocated space as to recover deleted data and file fragments;
3. Attempts will be made to obtain the cellular phone's data by only making unobtrusive revocable setting changes to permit the digital extraction of the data; however, if necessary, the device may require disassembly to obtain the desired data which may render the device inoperable;
4. Law enforcement is authorized to copy, forensically image, view, photograph, record and conduct forensic analysis of the data obtained from the aforementioned cellular telephone as well as any data storage devices within;
5. Law enforcement may enlist the aid of additional law enforcement officers or other third parties who are trained in conducting forensic analysis of the data in retrieving and analyzing the data. When files have been deleted, they can be potentially recovered later using forensic tools. Furthermore a person with familiarity with how cellphones work may, after examining the data, be able to draw conclusions about how the device was used, the purpose of its use, who used it, where and when;
6. Law enforcement or their agents may be required to examine every file and scan its contents briefly to determine whether it falls within the scope of the warrant. This is necessary as it is difficult to know prior to the search the level of technical ability of the device's user and data can be hidden, moved, encoded or mislabeled to evade detection;
7. Law enforcement will complete a timely search of the cellular telephone as failure to do so could result in the irrevocable loss of data due to accidental or intentional destruction. The device could be damaged, remotely erased or contain internal destructive mechanisms which could destroy the data.