COUNTY OF LARIMER )

) SS IN THE COMBINED COURT

STATE OF COLORADO )

**SEALED**

**AFFIDAVIT FOR SEARCH WARRANT**

Before the Honorable \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

Judge / Magistrate

Affiant, LEO NAME, a commissioned law enforcement officer, being duly sworn, deposes and states that I have probable cause to believe that data stored within, on, or upon the equipment capable of storing electronic data identified or described as:

**YOUR DEVICE HERE, EXAMPLE (Multiple devices may be listed):**

A Dell computer with a serial number of 1234567. This computer is currently located at 2221 Timberline Rd (Fort Collins Police Services) logged into evidence as item number FC145-1 under case number 13-1234

Computer system: make, model, s/n, description.

# of floppy disks

# of CD’s

There is now located there within or upon:

The following data stored in the device, relevant to the criminal activity described in the affidavit, which is incorporated by reference, and possible prosecution of CRIMINAL OFFENSE(S) perpetrated against NAME OF VICTIM OR LOCATION [IF APPLICABLE] (hereinafter “Subject Offense(s)”):

REVIEW THE LISTED CATEGORIES OF DATA, PLEASE REMOVE ANY CATAGORIES NOT SUPPORTED BY THE FACTS CONTAINED IN YOUR AFFIDAVIT

1. Data which tends to show possession, dominion and control over said equipment, including device and system ownership information (telephone number, ESN number, serial number, IMEI, IMSI, CCID);
2. Evidence of software that may allow others to control a device, such as viruses, Trojan horses, and other forms of malicious software, as well as evidence of the presence or absence of security software designed to detect malicious software;
3. Evidence of the lack of such malicious software;
4. Evidence of counter-forensic programs (and associated data) that are designed to eliminate data from the device;
5. Passwords, encryption keys, codes, and/or other devices or information that may be necessary to access the device and its contents;
6. Date/time, language, and other settings preferences to include wireless local area network setting(s), Bluetooth settings to include device name(s), hotspot SSID (name), and MAC address and connection dates and times to the device;
7. Address books, contact lists, names, and lists of names and addresses of individuals who may have been contacted by use of the device or by other means for the purpose of committing violations of the Subject Offense(s);
8. Records, documents, invoices and materials that concern any accounts with an Internet Service Provider pertaining to Subject Offense(s);
9. Records, documents, invoices and materials, in any format or medium, that concern e-mail accounts, online storage, or other remote computer storage pertaining to Subject Offense(s);
10. Records of Internet activity, including Internet Protocol addresses, firewall logs, transactions with Internet hosting providers, co-located computer systems, cloud computing services, caches, browser history and cookies, “bookmarked” or “favorite” web pages, search terms that the user entered into any Internet search engine, and records of user-typed web addresses pertaining to Offense(s) or that show who used, owned, possessed, or controlled the device;
11. Voicemail messages, text messages, MMS messages, Emails whether stored, received, or deleted as they pertain to pertaining to Offense(s), including username(s) and account information;
12. Photographs or images stored, sent, received or deleted, or documents containing photographs or images pertaining to Subject Offense(s);
13. Videos stored, sent, received or deleted pertaining to Subject Offense(s);
14. Notes, documents, records, or correspondence, pertaining to Subject Offense(s);
15. Electronic files, data, videos, and communications, including related metadata and location data, stored, sent, received or deleted from social media applications such as Facebook, Snapchat, Instagram, Twitter and/or any other third party programs or applications located on the device pertaining to Offense(s);
16. Global position system (GPS) data and any other geolocation data pertaining to Subject Offense(s);
17. Records of internet activity, including internet protocol (IP) addresses and Port IDs, firewall logs, transactions with internet hosting providers, co-located computer systems, cloud computing services, caches, browser history and cookies, “bookmarked” or “favorite” web pages, search terms that the user entered into any internet search engine, and records of user-typed web addresses that show who used, owned, possessed, or controlled the device(s) pertaining to Offense(s);

Items ITEMS LIMITED BY DATE are limited to data with created, accessed or modified dates between DATE OF INTEREST through DATE OF INTEREST.

\*\*NOTE: Descriptions of the data, information, functions or services listed above are contained in Attachment A, which is incorporated herein by reference.

Further, I have probable cause to believe that the requested items constitutes property which are designed or intended for use as a means of committing a criminal offense, or which are or have been used as a means of committing a criminal offense, or the possession of which is illegal, or which would be material evidence in a subsequent criminal prosecution in this state, another state, or federal court, or the seizure of which is expressly required, authorized, or permitted by a statute of this state or the United States. **OPTIONAL LANGUAGE IF APPROPRIATE (add or delete):** or that would aid in the detection of the whereabouts of or in the apprehension of a person for whom a lawful arrest order is outstanding.

The facts establishing grounds for issuance of a search warrant and showing probable cause to believe that they exist are as follows.

**PROABABLE CAUSE STATEMENT**

Tie the items you are searching for to the suspect, why do we believe a computer was used during the crime, etc

Use the two below paragraphs in your affidavit to explain why the search of computer equipment is not done at the scene.

Due to the nature and vulnerability of magnetic or digital data, it is necessary to seize media capable of storing magnetic data, and the computer, or what is commonly referred to as the CPU, meaning the computer case which contains the hard drive, motherboard and related hardware. It is necessary to remove these items from the scene and transport them to a controlled environment so a complete search of the items may be accomplished in such a way that the data it is protected, and unaltered.

Your affiant is aware that the current technology available for the downloading of data from digital devices such as cell phones, computers, or other mobile devices, does not allow the download of information only for a specific date range. Your affiant is also aware that the current technology available may not allow the downloading of only specific types of data, (e.g. pictures, messages, contacts, application data, etc.) as this data, including dates, may be in raw form, making it humanly unreadable without the use of specific software.  In light of that, the data from the digital device must be downloaded as completely as technologically possible. Once that download is completed, and the downloaded data is processed with specific software, a search of the data for a specific date range or specific type of data content is possible.

Your affiant is also aware that many times, there is only one opportunity to download the information from a digital device. Without obtaining all of the downloadable data from the cell phone, computer, or other mobile device, if additional information is learned later in the investigation, either by law enforcement, the District Attorney’s Office, or defense counsel, the same data that existed at the time of the initial download may no longer be available.  The only way to ensure preservation of all the downloadable data that existed at the time of the original download is to initially obtain all the downloadable data from the cell phone, computer, or other mobile device, and then preserve that data for any future searches.

Your affiant is requesting to obtain all of the downloadable data from the digital device(s). That data will be saved to preserve it in case additional review of the data is warranted and authorized by the courts at a later time. If a future search of the downloaded data from the device is necessary at a later time, additional applications will be made to the courts. At this time, the review of the data extracted from the device(s) will be for the date range and data authorized in the warrant.

***Further requests:***

1. Pursuant to Crim. P. 41 and §16-3-304(2), Your Affiant requests that this Court seal the affidavit and search warrant and court order for production of records until the filing of charges based on this law enforcement criminal investigation. The affidavit establishes grounds to believe that disclosure at this time of the affidavit and search warrant and court order for production of records would be contrary to the public interest. Such order for sealing does not apply to representatives of law enforcement agencies, and District Attorney’s Offices.

The executing law enforcement officer(s) may enlist the aid of a law enforcement computer forensic laboratory and/or certified digital evidence examiner(s) in the searching, viewing, photographing, recording, copying, forensic imaging, and analysis of any and all of the information described.

I believe the above facts to be true from official Fort Collins Police Services records, conversations with fellow officers, personal observations and interviews. I am a sworn police officer with Fort Collins Police Services. I have been trained at the State, and local levels with regard to my duties. I am authorized by law to execute search warrants in the State of Colorado.

# Affiant\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

# Dated \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_, 20\_\_\_at \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_am/pm.

# \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

# Judge/Magistrate

**ATTACHMENT A**

1. **Internet Service Providers (“ISPs”):** ISPs are commercial organizations that are in business to provide individuals and businesses access to the Internet. ISPs provide a range of functions for their customers including access to the Internet, web hosting, e-mail, remote storage, and co-location of computers and other communications equipment. ISPs can offer a range of options in providing access to the Internet including telephone based dial-up, broadband based access via digital subscriber line (DSL) or cable television, dedicated circuits, or satellite based subscription. ISPs typically charge a fee based upon the type of connection and volume of data, called bandwidth, that the connection supports. Many ISPs assign each subscriber an account name – a user name or screen name, an “e-mail address,” an e-mail mailbox, and a personal password selected by the subscriber. By using a computer equipped with a telephone or cable modem, the subscriber can establish communication with an ISP over a telephone line or through a cable system, and can access the Internet by using his or her account name and personal password.
2. **Internet Protocol Address (“IP Address”)**: Every computer or device on the Internet is referenced by a unique Internet Protocol address the same way every telephone has a unique telephone number. An IP address is a series of numbers separated by periods; an example of an IP address is 192.168.10.102. Each time an individual accesses the Internet, the computer from which that individual initiates access is assigned an IP address. A central authority provides each ISP a limited block of IP addresses for use by that ISP’s customers or subscribers. Most ISPs employ dynamic IP addressing, that is they allocate any unused IP address at the time of initiation of an Internet session each time a customer or subscriber accesses the Internet. A dynamic IP address is reserved by an ISP to be shared among a group of computers over a period of time. The ISP logs the date, time and duration of the Internet session for each IP address and can identify the user of that IP address for such a session from these records. Typically, users who sporadically access the Internet via a dial-up modem will be assigned an IP address from a pool of IP addresses for the duration of each dial-up session. Once the session ends, the IP address is available for the next dial-up customer. On the other hand, some ISPs, including most cable providers, employ static IP addressing, that is a customer or subscriber’s computer is assigned one IP address that is used to identify each and every Internet session initiated through that computer. In other words, a static IP address is an IP address that does not change over a period of time and is typically assigned to a specific computer. A modem is an electronic device that allows one computer to communicate with another.
3. **Digital Camera** is a camera that records pictures as digital picture files, rather than by using photographic film. Digital cameras use a variety of fixed and removable digital storage media to store their recorded images. Images can usually be retrieved by connecting the camera to a computer or by connecting the removable storage medium to a separate reader. Removable storage media includes various types of flash memory cards and miniature hard drives. Most digital cameras also include a screen for viewing the stored images. This storage media can contain any digital data, including data unrelated to photographs or videos such as texts, word processing documents, or web pages. If the camera is equipped with global positioning system (“GPS”) technology, that information may be recorded as metadata associated with the photographs and videos taken with that camera as well as other information such as the make and model of the camera and the date and time the image was created. Some cameras and removable storage media are now equipped with wireless capabilities, which allow for images and files to be uploaded from the camera or digital storage media directly to the Internet or to other digital storage devices or computers using a wired or wireless connection.
4. **Wireless telephone** (or mobile telephone, or cellular telephone) is a handheld wireless device used for voice and data communication through radio signals. These telephones send signals through networks of transmitter/receivers, enabling communication with other wireless telephones or traditional “land line” telephones. A wireless telephone usually contains a “call log,” which records the telephone number, date, and time of calls made to and from the phone. In addition to enabling voice communications, wireless telephones offer a broad range of capabilities. These capabilities include: storing names and phone numbers in electronic “address books;” sending, receiving, and storing text messages and e-mail; taking, sending, receiving, and storing still photographs and moving video; storing and playing back audio files; storing dates, appointments, and other information on personal calendars; and accessing and downloading information from the Internet including websites, social media sites, bulletin boards, file sharing, and other Internet sites. Wireless telephones often have a subscriber identity module or subscriber identification module (“SIM”), which is an integrated circuit that securely stores the International Mobile Subscriber Identity (“IMSI”) and the related key used to identify and authenticate subscribers on mobile telephone devices. A SIM is embedded into a removable “SIM card,” which can be transferred between different mobile devices. A SIM card contains a unique serial number (“ICCID”), IMSI, security authentication and ciphering information, temporary information related to the local network, a list of the services to which the user has access, and certain passwords. Most SIM cards will also store certain usage data, such as call history, text (“SMS”) messages, and phone book contacts. Wireless telephones may also be “smartphones,” such that they operate as personal computers capable of accessing the Internet. They may also include GPS technology for determining the location of the device. Such telephones may also contain removable storage media, such as a flash card—such devices can store any digital data, and can have the capacity to store many gigabytes of data. Some cellular telephones also have software, giving them the same capabilities as personal computers including accessing and editing word processing documents, spreadsheets, and presentations. Some cellular telephones also operate as a “tablet,” or mobile computer, and can contain software programs called applications. Those programs can perform different functions and save data associated with those functions, including use associated with the Internet.
5. **Personal digital assistant**, or PDA, is a handheld electronic device used for storing data (such as names, addresses, appointments or notes) and utilizing computer programs. Some PDAs also function as wireless communication devices and are used to access the Internet and send and receive e-mail. PDAs usually include a memory card or other removable storage media for storing data and a keyboard and/or touch screen for entering data. Removable storage media include various types of flash memory cards or miniature hard drives. This removable storage media can store any digital data. Most PDAs run computer software, giving them many of the same capabilities as personal computers. For example, PDA users can work with word-processing documents, spreadsheets, and presentations. PDAs may also include GPS technology for determining the location of the device.
6. **Tablet device** is a mobile computer, typically larger than a phone yet smaller than a notebook, that is primarily operated by touching the screen. Tablets function as wireless communication devices and can be used to access the Internet through cellular networks, 802.11 “wi-fi” networks, or otherwise. Tablets typically contain programs called applications (“apps”), which, like programs on a personal computer, perform different functions and save data associated with those functions. Apps can, for example, permit accessing the Web, sending and receiving e-mail, and participating in Internet social networks.
7. A hard disk drive (“HDD”), also known as a hard drive or hard disk, is a data storage device that consists of an external circuit board, external data, power connections, and internal glass, ceramic, or magnetically charged rotating metal platters that permanently store data even when powered off.  A solid-state drive (“SSD”), also known as a solid-state disk, is a data storage device that uses integrated circuit assemblies as memory to permanently store data instead of using rotating platters. Flash drives, flash cards, and thumb drives are digital storage devices that can connect to computers or other devices using the appropriate connection. CDs/DVDs are digital storage devices capable of storing large amounts of digital data—a user can store information onto a CD/DVD by “burning” digital data to the device using a computer CD/DVD drive. These devices are capable of storing any electronic information including images, videos, word processing documents, programs and software, and web pages.
8. **Computer Routers and Modems** are also used as instrumentalities of crimes involving computers both to operate the computer to commit criminal offenses involving the sexual exploitation of minors. Modems and routers can contain information about dates, IP addresses, MAC addresses, frequency, and computer(s) used to access the Internet, and some have separate digital storage capacity that allow them to connect to other devices and to store information similar to an external digital storage device like a flash card or thumb drive. In my training and experience, examining data stored on devices of this type can uncover, among other things, evidence that reveals or suggests who possessed or used the device or the computers and devices connected to it.
9. “**Computers**” or “**digital storage media**” or “**digital storage devices**” may be used interchangeably, and can include any physical object upon which computer data can be recorded as well as all types of electronic, magnetic, optical, electrochemical, or other high speed data processing devices capable of performing logical, arithmetic, or storage functions, including desktop and laptop computers, mobile phones, tablets, server computers, game consoles, network hardware, hard disk drives, RAM, floppy disks, flash memory, CDs, DVDs, and other magnetic or optical storage media.

COUNTY OF LARIMER )

) SS IN THE COMBINED COURT

STATE OF COLORADO )

**SEALED**

**SEARCH WARRANT**

## BEFORE THE HONORABLE \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

Judge / Magistrate

TO: ANY PEACE OFFICER AUTHORIZED BY LAW TO EXECUTE SEARCH WARRANTS IN THE COUNTY OF LARIMER AND STATE OF COLORADO.

The court, upon review of a sworn affidavit filed by LEO NAME, a commissioned police officer, in support of the issuance of this search warrant, hereby commands you to search the following described property, namely:

**YOUR DEVICE HERE, EXAMPLE (Multiple devices may be listed):**

A Dell computer with a serial number of 1234567. This computer is currently located at 2221 Timberline Rd (Fort Collins Police Services) logged into evidence as item number FC145-1 under case number 13-1234

Computer system: make, model, s/n, description.

# of floppy disks

# of CD’s

And to Seize:

The following data stored in the device, relevant to the criminal activity described in the affidavit, which is incorporated by reference, and possible prosecution of CRIMINAL OFFENSE(S) perpetrated against NAME OF VICTIM OR LOCATION [IF APPLICABLE] (hereinafter “Subject Offense(s)”):

REVIEW THE LISTED CATEGORIES OF DATA, PLEASE REMOVE ANY CATAGORIES NOT SUPPORTED BY THE FACTS CONTAINED IN YOUR AFFIDAVIT

1. Data which tends to show possession, dominion and control over said equipment, including device and system ownership information (telephone number, ESN number, serial number, IMEI, IMSI, CCID);
2. Evidence of software that may allow others to control a device, such as viruses, Trojan horses, and other forms of malicious software, as well as evidence of the presence or absence of security software designed to detect malicious software;
3. Evidence of the lack of such malicious software;
4. Evidence of counter-forensic programs (and associated data) that are designed to eliminate data from the device;
5. Passwords, encryption keys, codes, and/or other devices or information that may be necessary to access the device and its contents;
6. Date/time, language, and other settings preferences to include wireless local area network setting(s), Bluetooth settings to include device name(s), hotspot SSID (name), and MAC address and connection dates and times to the device;
7. Address books, contact lists, names, and lists of names and addresses of individuals who may have been contacted by use of the device or by other means for the purpose of committing violations of the Subject Offense(s);
8. Records, documents, invoices and materials that concern any accounts with an Internet Service Provider pertaining to Subject Offense(s);
9. Records, documents, invoices and materials, in any format or medium, that concern e-mail accounts, online storage, or other remote computer storage pertaining to Subject Offense(s);
10. Records of Internet activity, including Internet Protocol addresses, firewall logs, transactions with Internet hosting providers, co-located computer systems, cloud computing services, caches, browser history and cookies, “bookmarked” or “favorite” web pages, search terms that the user entered into any Internet search engine, and records of user-typed web addresses pertaining to Offense(s) or that show who used, owned, possessed, or controlled the device;
11. Voicemail messages, text messages, MMS messages, Emails whether stored, received, or deleted as they pertain to pertaining to Offense(s), including username(s) and account information;
12. Photographs or images stored, sent, received or deleted, or documents containing photographs or images pertaining to Subject Offense(s);
13. Videos stored, sent, received or deleted pertaining to Subject Offense(s);
14. Notes, documents, records, or correspondence, pertaining to Subject Offense(s);
15. Electronic files, data, videos, and communications, including related metadata and location data, stored, sent, received or deleted from social media applications such as Facebook, Snapchat, Instagram, Twitter and/or any other third party programs or applications located on the device pertaining to Offense(s);
16. Global position system (GPS) data and any other geolocation data pertaining to Subject Offense(s);
17. Records of internet activity, including internet protocol (IP) addresses and Port IDs, firewall logs, transactions with internet hosting providers, co-located computer systems, cloud computing services, caches, browser history and cookies, “bookmarked” or “favorite” web pages, search terms that the user entered into any internet search engine, and records of user-typed web addresses that show who used, owned, possessed, or controlled the device(s) pertaining to Offense(s);

Items ITEMS LIMITED BY DATE are limited to data with created, accessed or modified dates between DATE OF INTEREST through DATE OF INTEREST

The court also hereby finds probable cause to believe that the requested items constitutes property which has been stolen or embezzled, or which are designed or intended for use as a means of committing a criminal offense, or which are or have been used as a means of committing a criminal offense, or the possession of which is illegal, or which would be material evidence in a subsequent criminal prosecution in this state, another state, or federal court, or the seizure of which is expressly required, authorized, or permitted by a statute of this state or the United States. **OPTIONAL LANGUAGE IF APPROPRIATE (add or delete):** or that would aid in the detection of the whereabouts of or in the apprehension of a person for whom a lawful arrest order is outstanding.

The grounds for this Search Warrant are set forth in the accompanying Affidavit for Search Warrant, a true and correct copy of which is attached hereto and is incorporated herein by reference. The Court being satisfied that grounds for the issuance of this Search warrant exist and that there is probable cause to believe that they exist.

Therefore you are commanded to execute and serve this warrant at any time within fourteen days from the date hereof, to search and seize theitems described herein. And to provide a copy of this search warrant to the person responsible for the equipment, and to make prompt return of this Search Warrant, to the undersigned Judge.

Therefore, any member of law enforcement agency or a designee, and/or a computer forensic lab, are commanded to:

* If not already in possession of the device, seize the aforementioned device within 14 days of the date this warrant is signed;
* Access the aforementioned device and view, copy and maintain the above described data contained therein;
* Use and employ such force as may reasonably be necessary in the performance of the duties described herein;
* The ability to use whatever means necessary to override any encryption or secure files encountered during the forensic examination of the phone, which may be destructive to the equipment. This could include having the item transferred to specialized forensic laboratories outside of the jurisdiction and/or the State of Colorado, if necessary.
* The ability to repair the device, replace the screen, replace the chassis, reconnect wires, or replace a battery. I also understand that it may be necessary to employ advanced forensic processes to bypass locked display screens and other data access restrictions. Advanced processes including potentially destructive and destructive processes such as gaining root and/or Super user level access, JTAG, ISP-JTAG and chip-off.
* The ability to enlist the aid of a law enforcement computer forensic laboratory and/or certified digital evidence examiner(s) in the searching, viewing, photographing, recording, copying, forensic imagining, and analysis of any and all of the information described.
* Deliver to the person from whom the property is taken a copy of this warrant together with a receipt for the property taken, or to leave a copy of the warrant and receipt at the place from which the property was taken;
* Make prompt return of this search warrant, accompanied by a written inventory describing the physical storage media that was seized or copied, to the undersigned judge.

IT IS FURTHER ORDERED:

1. That this Search Warrant and Order and application be **SEALED** until the filing of charges based on this law enforcement criminal investigation, that the identity of any target(s) of the underlying criminal investigation may be redacted from any copy of this Order to be served on any service provider or other person. After charges are filed, disclosure of this Search Warrant and Order and application is governed by Crim. P. 55.1.

Dated \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_, 20\_\_\_at \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_am/pm.

\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

Judge/Magistrate