IN THE SECOND DISTRICT COURT - FARMINGTON DEPARTMENT

IN AND FOR DAVIS COUNTY, STATE OF UTAH

AFFIDAVIT FOR SEARCH WARRANT

STATE OF UTAH)
:ss
County of Davis)

The undersigned affiant, Investigator BRENT JASON BAGGS of Davis County Attorney's Office, upon an oath or written affidavit subscribed under criminal penalty, declares:

That your affiant has reason to believe:

THAT

On the premises known as [redacted] Syracuse, UT 84075,

On the person(s) described as: Benjamin Alyk, DOB 11/28/1997. SSN [redacted];

In the City of Syracuse, County of Davis, State of Utah, there is now certain property or evidence described as:

A. Computer Hardware
Computer hardware consists of all equipment that can receive, capture, collect, analyze, create, display, convert, store, conceal, or transmit electronic, digital, magnetic, or similar computer impulses or data. Hardware includes any data-processing device (including but not limited to central processing units, internal and peripheral storage devices such as fixed disks, external hard drives, floppy disk drives and diskettes, digital cameras, web cams, scanners, Bernoulli drives and other memory storage devices, cell phones and other electronic communication and/or storage devices), peripheral input/output devices (including but not limited to keyboards, printers, video display monitors, and related communication devices such as cables and connections), and any devices, mechanisms, or parts that can be used to restrict access to computer hardware (including but not limited to physical keys and locks).
B. Computer Software

Computer software is digital information that can be interpreted by a computer and any of its related components to direct the way they work. Software is stored in electronic, magnetic, or other digital forms. It commonly includes programs to run operating systems, applications, and utilities.

C. Documentation

Computer-related documentation consists of written, recorded, printed, or electronically stored material that explains or illustrates how to configure or use computer hardware, software, or other related items.

D. Passwords and Data Security Devices

Computer passwords and other data security devices are designed to restrict access to or hide computer software, documentation, or data. Data security devices may consist of hardware, software, or other programming code(s). A password (a string of alpha numeric characters) usually operates a sort of digital key to “unlock” particular data security devices. Data security hardware may include encryption devices, chips, and circuit boards. Data security software of digital code may include programming code that creates “test” keys or “hot” keys that perform certain pre-set security functions when touched. Data security software or code may also encrypt, compress, hide, or “booby-trap” protected data to make it inaccessible or unusable and may reverse the process to restore the data.

E. Any and all images of child pornography as defined under Utah Code §76-5b-103, et seq. and related data.

F. Any and all notes, documents, records, or correspondence pertaining to child pornography as defined under Utah Code §76-5b-103, et seq.

G. Any and all address books, names, lists of names and addresses, e-mail addresses, or other electronically stored lists of individuals whom there is reasonable basis to believe have been contacted by use of a computer for the purpose of distributing child pornography, and any and all diary entries regarding the collection, distribution, or manufacturing of child pornography as defined under Utah Code §76-5b-103, et seq.

H. Any and all correspondence identifying persons transmitting, through interstate commerce including by United States Mail or by computer, any visual depictions of minors engaged in sexually explicit conduct as defined under Utah Code §76-5b-103, et seq.

I. Any and all records, documents, invoices, and materials that concern any accounts with peer-to-peer networks or any other Internet Service Provider that may have been used to facilitate access to the Internet in the commission of the above-mentioned crimes.

J. Any and all address books, mailing lists, supplier lists, mailing address labels, e-mail addresses or other electronically stored lists, documents, and records pertaining to the preparation, purchase, and acquisition of names or the lists of names to be used in connection with the purchase, sale, trade, or transmission, through interstate commerce, including by United States Mail or by computer, of any visual depiction of minors engaged in sexually explicit conduct, as defined under Utah Code §76-5b-103, et seq.

K. Any and all address books, names, lists of names and addresses, and any e-mail addresses or other electronically stored lists of minors visually depicted while engaged in sexually explicit conduct, as defined under Utah Code §76-5b-103, et seq.
L. Any and all diary or notebook entries, notebooks, notes, e-mail addresses or other electronically stored lists, and records reflecting personal contact and other activities with minors visually depicted while engaged in sexually explicit conduct, as defined under Utah Code §76-5b-103, et seq.
M. Any of the items described in paragraphs A through L, above, that are stored in the form of magnetic or electronic coding on computer systems or on media capable of being read by a computer with the aid of computer-related equipment, including but not limited to floppy diskettes, fixed hard disks, removable hard disk cartridges, software, or memory in any form.
N. Motion picture films and video cassettes and film that may contain child pornography, including but not limited to VHS, Beta, 8MM and 35 MM, and any devices for recording depictions of child pornography.
O. Books, magazines, or photographs containing visual depictions of child pornography or any printed material from the computer hardware modalities listed above.
P. Any safes, hidden or concealed compartments, caches, or other locations where the above-mentioned items could be secreted.
Q. Any part of the premises including rooms, separate storage areas, furniture and files that could be used to store, conceal, hold, or contain any of the above-described items.

The search of any computer media obtained through the execution of this warrant shall be conducted as in accordance with the strategy outlined in the affidavit, described below and the search and seizure of any and all computers, electronic communication systems and storage devices, including any and all digital content contained thereon, and all of the following evidence is authorized, as it relates to a violation(s) of Utah Code Section 76-5b-201.

Searches for physical or digital evidence authorized in the warrant may be conducted using any of the computer search tools described in the affidavit, both on-site or subsequently off-site, as necessary, in addition to or in lieu of a full forensic search, or a forensic image may be created, if deemed necessary and appropriate, in order to locate and retrieve the evidence described in the affidavit and warrant. If write-blocking software cannot be used, then the appropriate search tools will be used.

If a write-blocking device is not used, all actions taken will be documented so that they can be verified by a forensic computer examiner at the Intermountain West Regional Computer Forensic Laboratory (“IWRCFL”), if necessary.

Law enforcement will maintain all original evidence in a secure environment.

and that said property or evidence:

Was unlawfully acquired or is unlawfully possessed;

has been used or is possessed for the purpose of being used to commit or conceal the commission of an offense; or

is evidence of illegal conduct.

Affiant believes the property and evidence described above is evidence of the crime or crimes of Section 76-5b-103 of the Utah Code includes the following definitions (relevant portions only):

(1) "Child pornography" means any visual depiction, including any live performance, photograph, film, video, picture, or computer or computer generated image or picture, whether made or produced by electronic, mechanical, or other means, of sexually explicit conduct, where:
(a) the production of the visual depiction involves the use of a minor engaging in sexually explicit conduct;
(b) the visual depiction is of a minor engaging in sexually explicit conduct; or
(c) the visual depiction has been created, adapted, or modified to appear that an identifiable minor is engaging in sexually explicit conduct.
(2) "Distribute" means the selling, exhibiting, displaying, wholesaling, retailing, providing, giving, granting admission to, or otherwise transferring or presenting child pornography . with or without consideration.
(3) "Identifiable minor" means a person:
(a)(i) who was a minor at the time the visual depiction was created, adapted, or modified; or
(ii) whose image as a minor was used in creating, adapting, or modifying the visual depiction; and
(b) who is recognizable as an actual person by the person's face, likeness, or other distinguishing characteristic, such as a birthmark, or other recognizable feature; and
(4) and (5) not relevant as pertain to vulnerable adults
(6) "Live performance" means any act, play, dance, pantomime, song, or other activity performed by live actors in person.
(7) "Minor" means a person younger than 18 years of age.
(8) "Nudity or partial nudity" means any state of dress or undress in which the human genitals, pubic region, buttocks, or the female breast, at a point below the top of the areola, is less than completely and opaquely covered.
(9) "Produce" means the photographing, filming, taping, directing, producing, creating, designing, or composing of child pornography or the securing or hiring of persons to engage in the production of child pornography…..
(10) "Sexually explicit conduct" means actual or simulated:
(a) sexual intercourse, including genital-genital, oral-genital, anal-genital, or oral-anal, whether between persons of the same or opposite sex;

(b) masturbation;
(c) bestiality;
(d) sadistic or masochistic activities;
(e) lascivious exhibition of the genitals or pubic area of any person;
(f) the visual depiction of nudity or partial nudity for the purpose of causing sexual arousal of any person;
(g) the fondling or touching of the genitals, pubic region, buttocks, or female breast; or
(h) the explicit representation of the defecation or urination functions.
(11) "Simulated sexually explicit conduct" means a feigned or pretended act of sexually explicit conduct which duplicates, within the perception of an average person, the appearance of an actual act of sexually explicit conduct.
(12) and (13) not relevant as pertain to vulnerable adults

Section 76-5b-201 of the Utah Code makes it a second degree felony to possess, view, distribute and/or produce child pornography. Section 76-5b-201 of the Utah Code states as follows:

Sexual exploitation of a minor - Offenses.
(1) A person is guilty of sexual exploitation of a minor:
(a) when the person:
(i) knowingly produces, possesses, or possesses with intent to distribute child pornography; or
(ii) intentionally distributes or views child pornography; or
(b) if the person is a minor's parent or legal guardian and knowingly consents to or permits that minor to be sexually exploited under Subsection (1)(a).
(2) Sexual exploitation of a minor is a felony of the second degree.
(3) It is a separate offense under this section:
(a) for each minor depicted, and if more than one minor is depicted in the child pornography in violation of this section, the depiction of each individual minor in the child pornography is a separate offense; and
(b) each time the same minor is depicted in different child pornography.
(4) It is an affirmative defense to a charge of violating this section that no person under 18 years of age was actually depicted in the visual depiction or used in producing or advertising the visual depiction.
(5) In proving a violation of this section in relation to an identifiable minor, proof of the identity of the identifiable minor is not required
(6) This section may not be construed to impose criminal or civil liability on:
(a) any entity or an employee, director, officer, or agent of an entity when acting within the scope of employment, for the good faith performance of:
(i) reporting or data preservation duties required under any federal or state law; or
(ii) implementing a policy of attempting to prevent the presence of child pornography on any tangible or intangible property, or of detecting and reporting the presence of child pornography on the property; or
(b) any law enforcement officer acting within the scope of a criminal investigation..

The facts to establish the grounds for issuance of a Search Warrant are:

I, Agent Brent Baggs am a certified peace officer in the State of Utah with 18 years of experience and have been employed as an Investigator with the Davis County Attorney's Office since April, 2014. Prior to that, I was employed as a Detective by the Syracuse City Police Department since July, 2006. I was assigned to the Davis Metro Narcotics Strike Force from 2006 to 2012. Prior to that, I was employed by the Ogden City Police Department and the Utah State Department of Corrections. I have attended training in numerous and varied aspects of law enforcement. As an ICAC TFO, I have attended training at the Intermountain West Regional Computer Forensic Laboratory in Salt Lake City, Utah, on ICAC Investigative Techniques, Peer to Peer sharing systems, osTriage, BitTorrent, and eMule. I have investigated many various crimes, to include homicide, sexual assault, child abuse, fraud, and others. I am currently assigned to the Internet Crimes Against Children Task Force (ICAC). The ICAC task force is a multi-jurisdictional task force comprised of local, state and federal law enforcement officers. The task force investigates internet crimes against children, including state and federal violations of laws, such as those dealing with enticement, child pornography and dealing harmful material to minors, and submits their investigations to state and/or federal entities for prosecution.

BACKGROUND REGARDING COMPUTERS, THE INTERNET, AND E-MAIL

1. The term a computer as used herein includes any electronic, magnetic, optical,
electrochemical, or other high speed data processing devices performing logical, arithmetic, or storage functions, and includes any data storage device or facility or electronic communication device or facility directly related to or operating in conjunction with such device. The term “computer” also includes cellular phones, iPods, Tablets, Smart phones, Personal Hand-Held Devices, iPads, electronic game devices or systems and other similar electronic communication or storage systems or devices.

2. The term “electronic communication system” or “electronic communication device” means any wire, radio, electromagnetic, photo-optical or photo-electronic facility or device for the transmission of wire or electronic communications and any computer facilities or related electronic equipment for the storage of such communications, including memory stick, memory cards or other items capable of electronic or digital storage.

3. Computers and computer technology (including electronic communication systems and devices and their technology) have revolutionized the way in which child pornography is produced, distributed, and utilized. They have also revolutionized the methods used by child pornography collectors to interact with each other and interact with and sexually exploit children. Computers serve

four functions in connection with child pornography: production; communication; distribution; and storage.

4. Child pornography formerly was produced using cameras and film (both still photography and movies). The photographs required darkroom facilities and a significant amount of skill in order to develop and reproduce the images. As a result, there were definable costs involved with the production of pornographic images. To distribute these on any scale also required significant resources. The photographs themselves were somewhat bulky and required secure storage to prevent their exposure to the public. The distribution of these wares was accomplished through a combination of personal contact, mailings, and telephone calls. Any reimbursement would follow these same paths.

5. Child pornographers can now produce both still and moving images directly from a camera, video camera, webcam or any electronic device with an imbedded camera which can convert the video into a format that is usable by computer programs. The output of the video camera or webcam can be stored, manipulated, transferred, or printed directly from the computer. The captured video image can be edited in ways very similar to those used to edit still images. The image can be lightened, darkened, cropped, and manipulated in a wide variety of ways. The producers of child pornography can also use a device known as a scanner to transfer photographs into a computer-readable format. In addition, with the use of cellular phones, child pornographers can take images and/or encourage others, including minors, to take images of themselves. Those images can then be transmitted through text messaging. Images can be sent from cellular phone to cellular phone as easily as placing a telephone call. Those images can also be sent to email accounts by using an electronic communication device, such as a cellular phone, that has Internet access. As a result of this technology, it is relatively inexpensive and technically easy to produce, store, and distribute child pornography. There is the added benefit to the child pornographer that this method of production does not leave as much evidence for law enforcement to discover as has been the case in the past.

6. A device known as a modem allows any computer to connect with another computer through the use of telephone, cable or wireless connections. Electronic contact can be made with literally millions of computers around the world. Also, wireless Internet access (WiFi) is available to consumers: sometimes the service is free; sometimes there is a charge for the service; public access may be available to consumers; private access may be available to consumers; the WiFi access may be secured or it may be unsecured. iPhones and other similar devices can also connect to the Internet through their service providers.

7. The Internet and its world wide web afford collectors of child pornography several different venues for obtaining, viewing and trading child pornography in a relatively secure and anonymous fashion. With a computer connected

to the Internet, an individual computer user can make electronic contact with millions of computers around the world. Many individual computer users and businesses obtain their access to the Internet through businesses known as Internet Service Providers (ISPs). ISPs provide their customers with access to the Internet using telephone, cable, or other telecommunications lines. ISPs also provide Internet e-mail accounts that allow users to communicate with other Internet users by sending and receiving electronic messages through the ISP's servers, remotely store electronic files on their customer's behalf, and may provide other services unique to each particular ISP. ISPs maintain records pertaining to the individuals, businesses, or organizations that have subscriber accounts with them. Those records may include identifying and billing information, account access information in the form of log files, e-mail transaction information, posting information, account application information, Internet Protocol (IP) addresses, and other information in both computer data format and in written record format.

8. Collectors and distributors of child pornography also use online resources to retrieve and store child pornography, including services offered by Internet Portals such as Yahoo and Hotmail, among others. The online services allow a user to set up an account with a remote computing service that provides e-mail services as well as electronic storage of computer files in a variety of formats. A user can set up an online storage account from any computer with access to the Internet. Evidence of such online storage of child pornography is often found on the user’s computer, even in cases where the child pornography evidence is not found on the computer; however, evidence of child pornography can be found on the user’s computer in most cases. Service providers are now offering “cloud storage” for customers. According to Wikipedia, “Cloud storage is a model of networked enterprise storage where data is stored in virtualized pools of storage which are generally hosted by third parties. Hosting companies operate large data centers, and people who require their data to be hosted buy or lease storage capacity from them. The data center operators, in the background, virtualize the resources according to the requirements of the customer and expose them as storage pools, which the customers can themselves use to store files or data objects. Physically, the resource may span across multiple servers and multiple locations. The safety of the files depends upon the hosting company, and on the applications that leverage the cloud storage”.

9. As is the case with most digital technology, communications by way of computer can be saved or stored on the computer used for these purposes. Storing this information can be intentional, i.e. by saving an e-mail as a file on the computer or saving the location of one’s favorite websites, for example “bookmarked” files. Digital information can also be retained unintentionally, e.g. traces of the path of an electronic communication may be automatically stored in many places such as temporary files or ISP client software. In addition to electronic communications, a computer user’s Internet activities generally leave traces or “footprints” in the web cache and history files of the browser used. A forensic

examiner often can recover evidence suggesting whether a computer contains peer to peer software, when the computer was sharing files, and some of the files which were uploaded or downloaded. Such information is often maintained indefinitely until overwritten by other data.

10. Some ISPs offer their subscribers the ability to communicate publicly or privately with each other in real time in the form of chat rooms. In addition to chat rooms that reside on many ISPs internal networks, these ISPs allow access to a larger external network of chat channels, one of which is called Internet Relay Chat (IRC), which is accessed through intermediary or client software. Contact with other users in either of these internal or external online formats can be very open or anonymous B in front of others who happen to be in the same room/channel at the same time or very private and personal in the form of person-to-person instant messages. Also, social networking sites including sites such as Facebook, MySpace, Twitter and others, allow for private and public communications by account holders with each other.

11. These communication structures are ideal for the child pornography collector. Having both open and anonymous communication capabilities allows a user to locate others of similar inclination and still maintain his or her anonymity. Once contact has been established, it is then possible to send text messages and graphic images to other trusted child pornography collectors. Moreover, the child pornography collector need not use the large service providers. Child pornography collectors can use standard Internet connections, such as those provided by government entities, organizations, and universities, to communicate with each other and to distribute pornography. These communication links allow contacts around the world as easily as calling next door. In addition, these communications can be quick, relatively secure, and as anonymous as desired. All of these advantages are well known and are the foundation of transactions between collectors of child pornography.

12. The ability to produce child pornography easily, reproduce it inexpensively, and market it anonymously (through e-mail) has drastically changed the method of distribution of child pornography. For example, child pornography can be transferred via e-mail to anyone with access to a computer and modem or other electronic communication device with Internet or email access. Because of the proliferation of commercial services that provide e-mail service, chat services, and easy access to the Internet, the computer is a preferred method of distributing child pornography materials.

13. The computer’s capability to store images in digital form makes it an ideal repository for child pornography. The size of the electronic storage media (commonly referred to as the hard drive) used in home computers has grown tremendously within the last several years. These drives can store thousands of images at very high resolution. A single compact disc can store hundreds

of images and thousands of pages of text. The capacities of the electronic storage devices/media used in home computers, cell phone and other electronic communication devices (including hard drives, flash memory, memory cards, memory sticks, thumb drives and other electronic storage devices) has grown tremendously within the last several years. Hard drives with the capacities of 500 gigabytes are not uncommon. These drives can store hundreds of thousands of images at very high resolution. Magnetic storage located in host computers adds another dimension to the equation. It is possible to use a video camera to capture an image, process that image in a computer with a video capture board, and save that image by storing it in another country. The user may also utilize “cloud storage”, as previously described. Once that is done, there is no readily apparent evidence at the scene of the crime, but evidence of the image capture and processing and even temporary image storage usually remains on the computer and the storage devices. With careful laboratory examination of electronic storage devices it is possible to recreate the evidence trail.

14. Searching computer systems and electronic storage devices may require a wide range of data analysis techniques. Criminals can mislabel or hide files to evade detection or take other steps to frustrate law enforcement searches. In light of these deceptions and attempts to evade, I request permission to use whatever data analysis techniques appear necessary to locate and retrieve evidence of child pornography.

LAW ENFORCEMENT TOOLS USED TO SEARCH COMPUTERS AND OTHER SEARCH TOOLS

15. Due to the varying types of digital evidence encountered, there are several search tools
available to ICAC agents for searching computers prior to or instead of submitting them for a full forensic search. Examples of these tools include: Image Scan, Knoppix, TUX4N6, osTriage, X-Ways, P2P Marshal, AD Registry viewer, AD Lab field mode, and Mac\Windows native search Utilities. When possible, digital evidence will be mounted behind hardware or software write-blocking devices, using the above mentioned tools, to preserve the integrity of the digital evidence being reviewed. Each of these tools allows investigators to view images and files on a computer.

16. osTriage is a program that allows agents to search for images and videos saved on a
computer system. This program is designed to run on a "live" computer. This program will detect files using keyword searches and file value matches of the files on the drive of the computer. This program also detects encryption, virtualization, registry files, mapped network drives, Internet history, and passwords stored in the Internet browsers. osTriage writes nothing to the computer being scanned (short of an entry in the registry for the USB device from which osTriage is run). This

tool has been validated by the FBI. It was previously known as “zSearch”. Utah ICAC Task Force agents are trained on how to use this search tool and have used it successfully in their investigations since 2010.

17. TUX4N6 is a program that allows agents to view saved images, videos and browse files saved on the computer hard drive. Using this program, ICAC agents can save selected images and videos that are found on memory devices connected to the computer being searched. TUX4N6 allows agents to search for files by file extensions, type of files, and keywords. TUX4N6 does not change data on a computer hard drive. TUX4N6 was validated by the National White Collar Crime Center (NW3C), most recently in a report dated November 2, 2011, of testing which occurred the latter part of 2010 and early part of 2011. Many Utah ICAC Task Force agents have been trained on how to use this search tool and have used it successfully in their investigations since 2011.

18. Image Scan is a program that allows agents to view images, videos, and browse files saved on the computer hard drive. Using this program, agents can save the images and videos that are found to a memory device. Image-Scan does not change data on a computer hard drive. Utah ICAC Task Force agents have been trained on using this tool and have used it successfully in investigations for many years. This tool has been validated by the FBI.

19. Knoppix is a program that allows agents to view saved images, videos, and browse files. Using this program, agents can save the images and videos that are found to a memory device. Knoppix allows agents to search for files by file extension and keywords. Knoppix does not change data on a computer hard drive. Utah ICAC Task Force agents have been trained on how to use this search tool and have used it successfully for many years. Knoppix was developed by Linux consultant Klaus Knopper. It was originally released for use back in 2000 and updated with the latest version having been released in September, 2011. It is also the one of the first search tools taught by Fox Valley Technical College in training ICAC courses.

20. X-Ways is a program that allows agents to view saved images, videos and browse files saved on digital pieces of evidence. Using this program, ICAC agents can mount various digital mediums or images and save selected images and videos that are found within the items mounted. X-Ways traverses the file system of the mounted items, creating an inventory of the data located. Using a filtering process, X-Ways allows agents to search for files by name, file extensions, file type, keywords, registry data, peer to peer activity, among other file variables pertinent to the nature of the search warrant. X-Ways is a useful tool in producing a customized view of the evidence being searched, allowing agents to efficiently locate and save pertinent suspect data, which can be included in an “on site” generated report if necessary. X-Ways does not change data on the items mounted for review. X-Ways is a widely used tool among various law enforcement

agencies and forensic specialist who have been trained in it use. Any evidence found can also be recovered from the target computer in a forensically sound manner. X-Ways Forensics contains advanced capabilities not found in other forensic tools to include searching for files using file names, hash values, file metadata and keywords. This program optionally performs file format specific and statistical encryption tests that can determine whether encryption is being used on a computer. If encryption is suspected and it is determined a live system analysis is needed, X-Ways Forensics can be run on a live computer system, which may result in minor changes, being made to the system. In addition to reviewing a computer, agents may also make a forensic image and conduct a full forensic analysis of a drive by using X-Ways Forensics if warranted (i.e. disk encryption is found for example). It will not change a forensic image file such as an E01 or other image format; however, if a physical hard drive is mounted with X-Ways, without write protection, minor changes could occur to the drive. X-Ways Forensics has been tested and validated for use by the FBI in January 2009. It is currently being utilized at the Intermountain Western Regional computer Laboratory (IWRCFL) and Salt Lake City FBI field office. Utah ICAC Task Force agents are trained on how to use this forensic tool and have used it successfully in their investigations since 2012.

21. P2P Marshal is a program written by Architecture Technology Corporation to target specific computer peer-to-peer file sharing activity. This tool allows ICAC agents to preview a computer's file system as it relates to specific peer-to-peer files sharing activity. Once a computer hard drive or hard drive image is mounted P2P Marshal will automatically traverse the mounted data looking for known peer-to-peer file sharing programs. P2P Marshal supports the following clients: Ares, BitTorrent, FrostWire, Kazaa, LimeWire, µTorrent, Azereus Vuze (Azereus 3+) and Kazaa. P2P Marshal will inventory digital data associated with the use of any supported peer-to-peer file sharing program and parse it out in a reviewable format. P2P Marshal will locate associated images, videos or other data files used in any detected peer-to-peer file sharing activity. Other digital artifacts, if located, will include IP addresses used to conduct file sharing, the computer user or users involved in the file sharing, files shared, the location of the shared files and the dates and times the files were being shared.

22. AD Registry Viewer is an Access Data product written for the specific purpose of previewing computer registry information and activity. ICAC agents can use this tool to locate registry artifacts describing various types of computer activity or information. AD Registry Viewer can provide useful registry information such as current operating system time zone, date and times of key registry values.

23. AD Lab field mode is a search preview process developed by Access Data for efficiently previewing digital data on site or out in the field. ICAC agents using AD Lab's field mode feature can mount various types of digital mediums or images. Once mounted, the files within the items are traversed and parsed out into

viewable categories such as images, videos, email data, registry files, encrypted files, documents, recycle bin files, and executable file types. AD Lab field mode provides a live search process, enabling ICAC agent to search for suspect file items using relevant search terms. AD Lab field mode also allows agents to use a file filter process to efficiently narrow down results pertinent to the case. The filtering process can includes or excludes files to be reviewed by using filtering values such as creation and or modification date and time, file size, file type, file owner and file status. Relevant data can be saved and imported into an “on site” generated preview report to include useful registry information.

24. Windows Search Utility is a default program inside of the Windows operating system, on a computer using Windows, which allows agents to search for text, images, videos, and other files saved on the computer. The search can be used to find files by name, a word or phrase, and last modified time. There are other features to assist in the search such as: the file is marked as hidden or case sensitive and the search will be conducted through system folders and subfolders. Windows Search Utility does run ‘live’ on a Windows computer so there is a possibility of changing date and time information on saved files on the computer hard drive. Because a write-blocking device cannot be used on this default program, the agent must document the steps taken when using this search program.

25. Mac Search Utility, Spotlight, is a native search program inside of the Mac operating system, which allows agents to search for text, images, videos, and other files saved on the computer. The search can be used to find files by name, a word or phrase, and last modified time. There are other features to assist in the search such as: the file is marked as hidden or case sensitive and the search will be conducted through system folders and subfolders. Spot Light Search Utility does run ‘live’ on a Mac computer so there is a possibility of changing date and time information on saved files on the computer hard drive. Because a write-blocking device cannot be used on this native program, the agent must document the steps taken when using this search program.

26. Internet Evidence Finder (IEF) is a digital forensic product designed by Magnet Forensics, targeting internet related activity and the various associated digital artifacts on a computer system or mobile device. IEF will search a targeted piece of digital medium or forensic image file, parsing data into reviewable categories associated with cloud artifacts, instant messaging, media files, mobile backups, P2P file sharing, social networking, webmail applications, web related activity, web page recovery, native phone apps, mobile device third party apps and Xbox data.

27. RECON is a digital forensics suite designed by Sumuri forensics, targeting MAC OS X (Mac computer operating systems). Recon is designed to run on both a live system, as well as, being capable of mounting a physical piece

of digital medium or forensic image file and categorizing recovered data into reviewable sections for review. Recon has the ability to traverse through the Mac file system, locating artifacts of interest to include but not limited to, media files, documents, network activity, cloud storage, virtual machines, destructive processes, mobile backups, email data, apple mail, apple notes, apple maps, file origination, password recovery, messaging activity and conduct timeline analysis. Recon is also capable of forensically imaging system memory during a live system acquisition and can be used to image targeted digital storage devices.

28. Lantern4 is a digital forensic product developed by Katana forensics. This utility is designed to image analyze and report items of interest associated with Mac computers and iOS devices. Lantern4 has the ability to conduct multiple device acquisitions within one case file, a feature unique to their item link analysis piece. The program will conduct logical and physical extractions of iOS devices. Other capabilities include but are not limited to acquisitions of Macs, password recovery, importation of call detail records, plist viewer, file signature analysis, global and local keyword searching, file system viewer, parses 30 plus third party applications, conducts hash set analysis and acquires all versions of Kik Messenger data with images.

29. Utah ICAC Task Force agents are responsible for maintaining the integrity of the evidence and content contained on the computer and digital media. Agents will document all activity while working on a computer and digital media by maintaining a log of the agent's activity. This documentation will allow verification by the Intermountain West Region Computer Laboratory (IWRCFL), if necessary.

30. A hardware and/or software write-blocking device is used, except in rare cases, to
prevent any "writes" from the operating system to original evidence attached to the computer system. Although it would always be preferred, a write-blocking device may not always be feasible. Some examples are:
• Image Scan, Knoppix, and TUX4N6 all run off a Compact Disc. If the suspect computer doesn't have an operational disc drive, these programs will not work.
• Image Scan will not run if the USB ports are not functioning in the suspect computer.
• If the agent doesn't have a portable write-blocking device and the knowledge to remove a hard drive, or the computer has multiple hard drives, the only option is a Windows Search, in the above examples.
• Computers have evolved to the point that a single CPU can run virtual machines (VM) within partitions. If a machine is running VM and it is turned off and rebooted, there is a chance of not seeing the evidence. If a machine is running, agents must look at it to see how a machine is configured.
• Encrypted hard drives are not readable without a password. If a machine is running and shut off to use the agent's tools, the drive cannot be read without the password, even at the IWRCFL.

• If a machine has a NAS (Network Attached Storage), it may not be seen by agents' software. The agents may have to look at configurations while a machine is running. If a NAS is present, agents may have to look at it without shutting the system down.
•As stated above, Windows Search Utility does not allow the use of a write-blocking device.
All actions taken by the agents will be documented so that the actions can be verified, if necessary, by the IWRCFL.

31. A forensic image can also be created of the data on seized electronic storage devices to
be searched. A forensic image is a bit for bit copy of the original evidence created using specialized software, approved for use by the National White Collar Crime Center, an ICAC Task Force approved training agency. The forensic image can be verified to exactly match the original evidence and verified by hash values. A search can also be conducted on a forensic image. Specialized training is required to create a forensic image. Many agents on our ICAC team have received this training from NW3C, called Basic Data Recovery and Acquisition (BDRA) and the advanced course called Intermediate data Recovery and Analysis (IDRA). This training consists of a series of classroom presentations and hands-on reinforcement in protecting and preserving electronic evidence. IDRA is a 3 ½ -day course that covers the forensic examination of Windows based operating systems on FAT file system.

32. Cell phones can be searched by agents manually, or by agents having specialized training in forensics tools, including Cellebrite, or can be submitted to the IWRCFL for a full forensics search.

INTRODUCTION REGARDING PREFERENTIAL SEXUAL OFFENDERS AND THE INTERNET

33. Based upon my experience and discussions with other law enforcement officers and from training I have received, I have learned that there are many types of sex offenders. Some of these offenders have a primary sexual interest in children and are often referred to as pedophiles. Sex offenders receive sexual gratification from actual contact with children and/or from fantasy involving children, through the use of photographs, digital images, and/or videos that can be stored on computer hard drives, floppy disks, flash memory, other electronic storage devices, optical compact discs (CDs), and on digital versatile discs (DVDs).

34. Kenneth V. Lanning, M.S., is a noted expert in the area of sexual exploitation of children. He is a retired FBI agent and has been involved in the professional study of the criminal aspects of deviant sexual behavior since 1973, later specializing in the sexual victimization of children in 1981. He has

lectured before and trained thousands of law enforcement officers and criminal justice professionals. He authored “Child Molesters: a Behavioral Analysis for Professionals Investigating the Sexual Exploitation of Children”, the fifth edition being published in 2010 by the National Center for Missing and Exploited Children (NCMEC manual). He is a founding member of the Board of Directors of the American Professional Society on the Abuse of Children (APSAC). He has testified before the US Senate and House of Representatives and he has testified as an expert in state as well as federal courts. He has published articles for law enforcement and professional journals, written book chapters, authored monographs and been project manager for research in the areas of child molesters, child pornography, child sexual exploitation and abductions.

35. In the NCMEC manual, Mr. Lanning has found that sex offenders often collect sexually explicit material consisting of photographs, video tapes, books, slides, and digital images and videos which they use for their own sexual gratification and fantasy and to show children in an attempt to lower the child's inhibitions. They also maintain their collections for indefinite periods and prefer to maintain them in close proximity so that they may be readily accessed. Sex offenders often hide their collections amongst legitimate files and/or other non-illicit images or videos.

36. Mr. Lanning has described a certain type of sex offender as a “preferential sex offender” who has a paraphilia (deviant sexual need) such as pedophilia, voyeurism or sadism and whose behavior is focused, compulsive, need-driven, persistent and primarily fantasy-driven. This type of sex offender includes those who molest children as well as those who collect, view or distribute child pornography. Mr. Lanning has found this type of sex offender is more likely to retain corroborative evidence. Collecting this type of material may help the preferential sex offender to satisfy, deal with or reinforce their compulsive, persistent sexual fantasies. Collecting may also fulfill important needs for validation. Collecting and trading with others also serves to justify or rationalize their behavior and gives them value and legitimacy.

37. I have learned that preferential sex offenders use computers to: a) correspond with like-minded individuals via e-mail, chats, bulletin boards, newsgroups, instant messages, file transfers and other means; b) store identifying information about child victims and identifying information about other individuals who share the same interests; and c) locate, view, download, collect and organize images of child pornography found through the Internet. Computers also afford individuals a degree of anonymity. Preferential sex offenders also print and save images of child pornography.

38. Mr. Lanning states that preferential sex offenders who collect sexually oriented pictures of minors do not separate themselves from their child pornography and/or child erotica for any prolonged time period. This behavior has

been documented by law enforcement officers involved in the investigation of child pornography throughout the United States. Preferential sex offenders typically retain their sexually explicit or suggestive materials for many years.

THE INVESTIGATION

39 . On February 7, 2018, I was assigned a follow up sex offense case that had come in through the Davis County Attorney's Office Juvenile Division. I contacted the subject's attorney, Todd Sessions, and scheduled an interview with his client, Benjamin Alyk.

40. On February 14, 2017, I interviewed Benjamin Alyk at Todd Session's office. Mr. Sessions was present during the interview.

41. Benjamin told me that at age 11 he encountered pornography for the first time. He stated that after that, at age 11-12, he received a Kindle for his birthday. He said that he discovered that the Kindle had a web browser and he began to look for porn.

42. Benjamin said that his parents operated an in-home daycare business out of their home, located a [redacted] in Syracuse, Utah. He said that he had observed a child from the daycare use the bathroom with the door open and he watched from his bedroom which made him curious. He said that he continued to look at internet porn and found a nudist website. He said that the website had pictures of children. He said that led him to discover an image sharing site where there were a community of pedophiles that were using the website to share links to cloud storage where you could find pictures and videos of child pornography. He said that the website security increased and they transitioned into sharing the material via email trading. He said that in order to obtain the material he would be asked to share child pornography. He said that he was around 14 – 15 years old at this time.

43. Benjamin stated that he then received a flip camera for his birthday. He said tha [redacted], ages 4 and 6, had come to stay at their house. He said that [redacted] didn't close the door when they used the restroom so he used his flip camera to capture video of them in the bathroom. He said that he created 3 videos of [redacted] during the time they stayed there. He said that he used those videos to trade for child pornography for a while, and then deleted them.

44. He said that he later received a Gopro camera for Christmas and discovered that he could control the camera remotely from an app on his phone. He said that he set the camera up in the bathroom, hidden under the closet door, to create videos of the daycare children. He said that he created videos of the children changing from their swimsuits into their clothes in the bathroom. He said that he

created 3-4 videos which he used to trade for child pornography. He said that he used those videos for 1-2 weeks before deleting them. Benjamin said that the first child he recorded with the Gopro was approximately age 5-6 at the time. The second child was approximately age 5-6. The third child was approximately age 4-5. The fourth child was approximately age 5. He confirmed that the videos taken were of the children either using the restroom or changing. He stated that the parents of the daycare children have not been notified about the creation of the videos. Benjamin said that he was around age 15-16 when he created these videos. He said that he used his Yahoo email account to share the videos. He said that he has since closed the email account. He said that he had traded the videos with approximately 5 other users and in return they would provide him with links to child pornography. This was done through the site Yandex. He said that he would originally meet the other users on imgsrc.ru. He described imagesource as a hotbed for this kind of activity. Benjamin confirmed that all of these acts occurred at his residence in Syracuse, Utah.

45. Benjamin said that he used the following devices to access imgsrc.ru:

Kindle
Ipod Touch
Droid Mini Smart Phone
Iphone
Desktop Computer

46. Benjamin said that he still has all of these devices with the exception of the Iphone, which had been traded in. Benjamin said that he also still has the GoPro and Flip camera mentioned above. Benjamin said that most of the time he would view the child pornography and delete it, other than a few times when he had downloaded the images to his desktop computer, then deleted them at a later time. He said that he gave the desktop computer to his parents after removing the hard drive, which he still has.

47. He said that continued to visit the image sharing site until around age 16-17 when he made the decision to stop viewing child pornography. Benjamin said after that he transitioned to only viewing adult pornography until the time that he left for his LDS Mission. Benjamin clarified that adult pornography would be classified as people 18 years and older.

48. He said that in December of 2016, while serving his mission in the Dominican Republic, he determined that he needed to report his past problems to his Missionary President, Mr. Nuckols. He said that Mr. Nuckols immediately sent him home. He said that once he arrived home, he went before a disciplinary council with the local church leaders. He said that he had disclosed all of the same details to the LDS church council and President Nuckols. He said that the church

had not made a report to law enforcement. He said that meeting took place in June of 2017.

49. Benjamin said that the daycare business that was primarily operated by his mother was no longer being operated at their residence, and said that his parents have limited knowledge of this case.

50. I Informed Benjamin that when you delete files from your computer equipment that it doesn't always mean that the files are completely gone. I asked Benjamin if he would be willing to turn the computer hard drive over to me to be destroyed. He stated that he would make arrangements to bring it to me. I spoke with Benjamin the following week and asked if I could also preview his camera equipment and the other devices that he mentioned during the interview in order to ensure that the files containing child pornography were completely removed. He stated that he would speak with his attorney and get back to me.

51. On March 15, 2018, I sent an email to Todd Sessions regarding Benjamin's camera and computer equipment in question. I did not receive a response from Mr. Sessions.

52. Based on the aforementioned information, I submit that there is probable cause to believe that Benjamin Alek at the residence located at [redacted] in Syracuse, Utah 84075, used a computer or computers to access the Internet to receive, possess, view and distribute material that depicts minors engaged in sexually explicit conduct, in violation of Utah Code Ann., ' 76-5b-103, et seq., and that probable cause exists to believe that a search of the residence, premises, vehicles at the residence, and out buildings, located at 524 W 2575 S in Syracuse, Utah 84075, for this data and related materials including emails which may be found in computers, electronic communication systems, and storage devices and media will yield evidence of violations of ' 76-5b-103 et seq., Utah Code Ann.

53. Based upon my knowledge, training, experience, and information received from other law enforcement officers, I know that searching and seizing information from computers, electronic devices and storage media often requires agents to seize most or all electronic storage devices (along with related peripherals) to be searched later by a qualified computer expert in a laboratory or other controlled environment. This is true because of the following:

a. The volume of evidence. Computer storage devices (like hard disks, diskettes, tapes, laser disks, thumb drives, removable storage devices, etc.) can store the equivalent of millions of pages of information. In addition, a suspect may try to conceal criminal evidence; he or she might store it in random order with deceptive file names. This may require searching authorities to examine all the stored data to determine which particular files are evidence of instrumentalities of crime. This sorting process can take weeks or months, depending on the

volume of data stored, and it would be impractical to attempt this kind of data search on site. Technical requirements. Searching computer systems for criminal evidence is a highly technical process requiring expert skill and a properly controlled environment. The vast array of computer hardware and software available requires even computer experts to specialize in some systems and applications, so it is difficult to know before a search which expert is qualified to analyze the system and its data. In any event, however, data search protocols are exacting scientific procedures designed to protect the integrity of the evidence and to recover even "hidden," erased, compressed, password-protected, or encrypted files. Since computer evidence is extremely vulnerable to inadvertent or intentional modification or destruction (both from external sources and from destructive codes imbedded in the system as a "booby trap"), a controlled environment is essential to its complete and accurate analysis.

b. Law enforcment utilizes programs as outlined in this affidavit under “LAW ENFORCEMENT TOOLS USED TO SEARCH COMPUTERS AND OTHER SEARCH TOOLS”. These investigatory programs and devices are used to find images on computer media, however, they do not have the capability of finding all images. For example, they cannot locate deleted images or images in unallocated space. They do have the capability of finding active images. As such, I request permission to use any of these tools, and/or a write-blocking device in an effort to determine if there are active images of child pornography on the suspect’s computer media. In the event that they do not manifest evidence in active files, there may nonetheless be images in deleted or unallocated space. I therefore request permission to search for and seize any of the evidence of crimes of sexual exploitation of minors referenced herein, irrespective of the results of running our search programs, and/or a write-blocking device. Permission is requested that the law enforcement agents also be allowed to make a forensic computer image of any hard drives found. Permission is also requested to search any and all items seized, including cell phones, electronic communication devices, other electronic devices which may contain data, including images, emails, accounts, communications, contacts, relating to the sexual exploitation of minors and storage media

WHEREFORE, your affiant prays that a Search Warrant be issued for the seizure of said items in the daytime.

I declare under criminal penalty of the State of Utah that the foregoing is true and correct.

Executed on: 4th day of April, 2018 @ 12:42 PM by /s/ BRENT JASON BAGGS

IN THE SECOND DISTRICT COURT - FARMINGTON DEPARTMENT

IN AND FOR DAVIS COUNTY, STATE OF UTAH

SEARCH WARRANT

No. 1805681

COUNTY OF DAVIS, STATE OF UTAH

To any peace officer in the State of Utah:

Proof by Affidavit made upon oath or written affirmation subscribed under criminal penalty of the State of Utah having been made to me by Investigator BRENT JASON BAGGS of Davis County Attorney's Office, this day, I am satisfied that there is probable cause to believe

THAT

On the premises known as [redacted] Syracuse, UT 84075,

On the person(s) of: Benjamin Alyk, DOB 11/28/1997. SSN[redacted];

In the City of Syracuse, County of Davis, State of Utah, there is now certain property or evidence described as:

A. Computer Hardware
Computer hardware consists of all equipment that can receive, capture, collect, analyze, create, display, convert, store, conceal, or transmit electronic, digital, magnetic, or similar computer impulses or data. Hardware includes any data-processing device (including but not limited to central processing units, internal and peripheral storage devices such as fixed disks, external hard drives, floppy disk drives and diskettes, digital cameras, web cams, scanners, Bernoulli drives and other memory storage devices, cell phones and other electronic communication and/or storage devices), peripheral input/output devices (including but not limited to keyboards, printers, video display monitors, and related communication devices such as cables and connections), and any devices, mechanisms, or parts that can be used to restrict access to computer hardware (including but not limited to physical keys and locks).
B. Computer Software

Computer software is digital information that can be interpreted by a computer and any of its related components to direct the way they work. Software is stored in electronic, magnetic, or other digital forms. It commonly includes programs to run operating systems, applications, and utilities.

C. Documentation

Computer-related documentation consists of written, recorded, printed, or electronically stored material that explains or illustrates how to configure or use computer hardware, software, or other related items.

D. Passwords and Data Security Devices

Computer passwords and other data security devices are designed to restrict access to or hide computer software, documentation, or data. Data security devices may consist of hardware, software, or other programming code(s). A password (a string of alpha numeric characters) usually operates a sort of digital key to “unlock” particular data security devices. Data security hardware may include encryption devices, chips, and circuit boards. Data security software of digital code may include programming code that creates “test” keys or “hot” keys that perform certain pre-set security functions when touched. Data security software or code may also encrypt, compress, hide, or “booby-trap” protected data to make it inaccessible or unusable and may reverse the process to restore the data.

E. Any and all images of child pornography as defined under Utah Code §76-5b-103, et seq. and related data.

F. Any and all notes, documents, records, or correspondence pertaining to child pornography as defined under Utah Code §76-5b-103, et seq.

G. Any and all address books, names, lists of names and addresses, e-mail addresses, or other electronically stored lists of individuals whom there is reasonable basis to believe have been contacted by use of a computer for the purpose of distributing child pornography, and any and all diary entries regarding the collection, distribution, or manufacturing of child pornography as defined under Utah Code §76-5b-103, et seq.

H. Any and all correspondence identifying persons transmitting, through interstate commerce including by United States Mail or by computer, any visual depictions of minors engaged in sexually explicit conduct as defined under Utah Code §76-5b-103, et seq.

I. Any and all records, documents, invoices, and materials that concern any accounts with peer-to-peer networks or any other Internet Service Provider that may have been used to facilitate access to the Internet in the commission of the above-mentioned crimes.

J. Any and all address books, mailing lists, supplier lists, mailing address labels, e-mail addresses or other electronically stored lists, documents, and records pertaining to the preparation, purchase, and acquisition of names or the lists of names to be used in connection with the purchase, sale, trade, or transmission, through interstate commerce, including by United States Mail or by computer, of any visual depiction of minors engaged in sexually explicit conduct, as defined under Utah Code §76-5b-103, et seq.

K. Any and all address books, names, lists of names and addresses, and any e-mail addresses or other electronically stored lists of minors visually depicted while engaged in sexually explicit conduct, as defined under Utah Code §76-5b-103, et seq.
L. Any and all diary or notebook entries, notebooks, notes, e-mail addresses or other electronically stored lists, and records reflecting personal contact and other activities with minors visually depicted while engaged in sexually explicit conduct, as defined under Utah Code §76-5b-103, et seq.
M. Any of the items described in paragraphs A through L, above, that are stored in the form of magnetic or electronic coding on computer systems or on media capable of being read by a computer with the aid of computer-related equipment, including but not limited to floppy diskettes, fixed hard disks, removable hard disk cartridges, software, or memory in any form.
N. Motion picture films and video cassettes and film that may contain child pornography, including but not limited to VHS, Beta, 8MM and 35 MM, and any devices for recording depictions of child pornography.
O. Books, magazines, or photographs containing visual depictions of child pornography or any printed material from the computer hardware modalities listed above.
P. Any safes, hidden or concealed compartments, caches, or other locations where the above-mentioned items could be secreted.
Q. Any part of the premises including rooms, separate storage areas, furniture and files that could be used to store, conceal, hold, or contain any of the above-described items.

The search of any computer media obtained through the execution of this warrant shall be conducted as in accordance with the strategy outlined in the affidavit, described below and the search and seizure of any and all computers, electronic communication systems and storage devices, including any and all digital content contained thereon, and all of the following evidence is authorized, as it relates to a violation(s) of Utah Code Section 76-5b-201.

Searches for physical or digital evidence authorized in the warrant may be conducted using any of the computer search tools described in the affidavit, both on-site or subsequently off-site, as necessary, in addition to or in lieu of a full forensic search, or a forensic image may be created, if deemed necessary and appropriate, in order to locate and retrieve the evidence described in the affidavit and warrant. If write-blocking software cannot be used, then the appropriate search tools will be used.

If a write-blocking device is not used, all actions taken will be documented so that they can be verified by a forensic computer examiner at the Intermountain West Regional Computer Forensic Laboratory (“IWRCFL”), if necessary.

Law enforcement will maintain all original evidence in a secure environment.

and that said property or evidence:

Was unlawfully acquired or is unlawfully possessed;

has been used or is possessed for the purpose of being used to commit or conceal the commission of an offense; or

is evidence of illegal conduct.

Affiant believes the property and evidence described above is evidence of the crime or crimes of Section 76-5b-103 of the Utah Code includes the following definitions (relevant portions only):

(1) "Child pornography" means any visual depiction, including any live performance, photograph, film, video, picture, or computer or computer generated image or picture, whether made or produced by electronic, mechanical, or other means, of sexually explicit conduct, where:
(a) the production of the visual depiction involves the use of a minor engaging in sexually explicit conduct;
(b) the visual depiction is of a minor engaging in sexually explicit conduct; or
(c) the visual depiction has been created, adapted, or modified to appear that an identifiable minor is engaging in sexually explicit conduct.
(2) "Distribute" means the selling, exhibiting, displaying, wholesaling, retailing, providing, giving, granting admission to, or otherwise transferring or presenting child pornography . with or without consideration.
(3) "Identifiable minor" means a person:
(a)(i) who was a minor at the time the visual depiction was created, adapted, or modified; or
(ii) whose image as a minor was used in creating, adapting, or modifying the visual depiction; and
(b) who is recognizable as an actual person by the person's face, likeness, or other distinguishing characteristic, such as a birthmark, or other recognizable feature; and
(4) and (5) not relevant as pertain to vulnerable adults
(6) "Live performance" means any act, play, dance, pantomime, song, or other activity performed by live actors in person.
(7) "Minor" means a person younger than 18 years of age.
(8) "Nudity or partial nudity" means any state of dress or undress in which the human genitals, pubic region, buttocks, or the female breast, at a point below the top of the areola, is less than completely and opaquely covered.
(9) "Produce" means the photographing, filming, taping, directing, producing, creating, designing, or composing of child pornography or the securing or hiring of persons to engage in the production of child pornography…..
(10) "Sexually explicit conduct" means actual or simulated:
(a) sexual intercourse, including genital-genital, oral-genital, anal-genital, or oral-anal, whether between persons of the same or opposite sex;

(b) masturbation;
(c) bestiality;
(d) sadistic or masochistic activities;
(e) lascivious exhibition of the genitals or pubic area of any person;
(f) the visual depiction of nudity or partial nudity for the purpose of causing sexual arousal of any person;
(g) the fondling or touching of the genitals, pubic region, buttocks, or female breast; or
(h) the explicit representation of the defecation or urination functions.
(11) "Simulated sexually explicit conduct" means a feigned or pretended act of sexually explicit conduct which duplicates, within the perception of an average person, the appearance of an actual act of sexually explicit conduct.
(12) and (13) not relevant as pertain to vulnerable adults

Section 76-5b-201 of the Utah Code makes it a second degree felony to possess, view, distribute and/or produce child pornography. Section 76-5b-201 of the Utah Code states as follows:

Sexual exploitation of a minor - Offenses.
(1) A person is guilty of sexual exploitation of a minor:
(a) when the person:
(i) knowingly produces, possesses, or possesses with intent to distribute child pornography; or
(ii) intentionally distributes or views child pornography; or
(b) if the person is a minor's parent or legal guardian and knowingly consents to or permits that minor to be sexually exploited under Subsection (1)(a).
(2) Sexual exploitation of a minor is a felony of the second degree.
(3) It is a separate offense under this section:
(a) for each minor depicted, and if more than one minor is depicted in the child pornography in violation of this section, the depiction of each individual minor in the child pornography is a separate offense; and
(b) each time the same minor is depicted in different child pornography.
(4) It is an affirmative defense to a charge of violating this section that no person under 18 years of age was actually depicted in the visual depiction or used in producing or advertising the visual depiction.
(5) In proving a violation of this section in relation to an identifiable minor, proof of the identity of the identifiable minor is not required
(6) This section may not be construed to impose criminal or civil liability on:
(a) any entity or an employee, director, officer, or agent of an entity when acting within the scope of employment, for the good faith performance of:
(i) reporting or data preservation duties required under any federal or state law; or
(ii) implementing a policy of attempting to prevent the presence of child pornography on any tangible or intangible property, or of detecting and reporting the presence of child pornography on the property; or
(b) any law enforcement officer acting within the scope of a criminal investigation..

YOU ARE THEREFORE COMMANDED:

to make a search in the daytime of the above-named or described person, vehicle, item, and/or premises for the herein-above described property or evidence and if you find the same or any part thereof, retain such property in your custody subject to the direction of a prosecutor or an order of this Court.

Dated: 4th day of April, 2018 @ 12:57 PM /s/ MICHAEL G ALLPHIN
District Court Judge

RETURN TO SEARCH WARRANT

NO. 1805681

The personal property listed below or set out on the inventory attached hereto was taken from the person of Benjamin Alyk, DOB 11/28/1997. SSN [redacted], by virtue of a search warrant dated the 4th day of April, 2018, and issued by Magistrate MICHAEL G ALLPHIN of the SECOND DISTRICT COURT - FARMINGTON DEPARTMENT:

1. Black Motorola Cell phone
2. WD 1 TB Hard Drive
3. Seagate External Hard Drive
4. Seagate External Hard Drive
5. WD External Hard Drive
6. WD My Passport Hard Drive
7. Sandisk SSD Drive
8. Xmedia Hard Drive

I, Investigator BRENT JASON BAGGS of Davis County Attorney's Office, by whom this warrant was executed, do swear that the above listed or below attached inventory contains a true and detailed account of all the property taken by me under the warrant, on the 5th day of April, 2018.

All of the property taken by virtue of said warrant will be retained in my custody subject to the order of this Court or of any other court in which the offense in respect to which the property, or things taken, is triable.

I declare under criminal penalty of the State of Utah that the foregoing is true and correct.

Executed on: 5th day of April, 2018 @ 01:02 PM by /s/ BRENT JASON BAGGS