UNITED STATES DISTRICT COURT

for the

District of Alaska

United States of America)
v.)
GREG SALARD) Case No. 1:14-MJ-00029-LCL
)
)
)

Defendant(s)

CRIMINAL COMPLAINT

I, the complainant in this case, state that the following is true to the best of my knowledge and belief.

On or about the date(s) of June 5, and October 15, 2014 in the county of _____ in the _____ District of Alaska, the defendant(s) violated:

Code Section	*Offense Description*
18 USC § 2252(a)(2) & (b)(1)	Distribution of Child Pornography
18 U.S.C. § 2252(a)(4)(B) & (b)(2)	Possession of Child Pornography

This criminal complaint is based on these facts:

See attached affidavit.

☑ Continued on the attached sheet.

Sworn by phone/Signature to be faxed
Complainant's signature

ANTHONY PETERSON, Special Agent, FBI
Printed name and title

Sworn to before me ~~and signed in my presence.~~ by phone, with court recording.

Date: 10/16/2014 3:06 pm.

Redacted Signature
Judge's signature

City and state: Anchorage, Alaska

DEBORAH M. SMITH, U.S. Magistrate Judge
Printed name and title

IN THE UNITED STATES DISTRICT COURT
FOR THE DISTRICT OF ALASKA

IN THE MATTER OF THE ARREST OF	)	Case No. 1:14-MJ-00029-LCL
	)	
GREG SALARD	)	
	)	
	)	
	)	

AFFIDAVIT IN SUPPORT OF AN APPLICATION FOR AN ARREST WARRANT

I, **ANTHONY PETERSON**, being first duly sworn, hereby depose and state as follows:

INTRODUCTION AND AGENT BACKGROUND

1. I make this affidavit in support of an application for an arrest warrant for GREG SALARD, residing at 3362 Zimovia, Wrangell, Alaska (hereinafter "SUBJECT"). An investigation has revealed that the SUBJECT has received and distributed, and possessed visual depiction of minors engaged in sexually explicit conduct in violation of Title 18, United States Code, Sections 2252(a)(2) and 2252(a)(4)(B).

2. I am a Special Agent (SA) with the Federal Bureau of Investigation (FBI), and have been since June 2010. In this assignment I have investigated a number of violations of the United States Code. For the past several years, I have investigated crimes against children, including but not limited to, internet crimes

against children; online enticement of children; child pornography possession, receipt, and distribution; and the commercial sexual exploitation of children. Further, I have conducted and participated in a large number of search warrants, arrest warrants, and interviews of people involved in crimes against children. I have also attended training specific to the use of computers in the commission of crimes against children.

3. I have attended the following computer based training with an emphasis in online investigations involving the trafficking of child pornography: Introduction to Internet Investigations, February 2011; Digital Extraction Technician, September 2013; Forensic Tool Kit Boot Camp, September, 2013; Innocent Images Online Basic Training Program, April 2014; Basic Networking, May 2014; Peer to Peer Investigations, May 2014; and Peer to Peer Investigations and Downloading, September 2014.

4. This affidavit is made in support of an arrest warrant for GREG SALARD, 3362 Zimovia, Wrangell, Alaska. Based on my investigation, there is probable cause to believe that the SUBJECT has violated 18 U.S.C. §§ 2252(a)(2) (receipt or distribution of any visual depiction of a minor engaged in sexually explicit conduct), and 18 U.S.C. §§ 2252(a)(4)(B)(possession of any visual depiction of a minor engaged in sexually explicit conduct and possession of child pornography).

5. I am familiar with the information contained in this affidavit based upon the investigation I have conducted, which included conversations with law enforcement officers and others, and the review of reports, database records, and other acquired evidence.

6. Because I submit this affidavit for the limited purpose of securing an arrest warrant, I have not included each and every fact known to me or the government. I have only included those facts necessary to establish probable cause to believe that GREG SALARD, 3362 Zimovia, Wrangell, Alaska, has violated 18 U.S.C. §§ 2252(a)(2), and 2252(a)(4)(B).

RELEVANT STATUTES

7. The relevant statutes are as follows:

a. 18 U.S.C. §§ 2252(a)(2) and (b)(1) provide, in relevant part, that any person who knowingly receives, or distributes, any visual depiction using any means or facility of interstate or foreign commerce or that has been transported in or affecting interstate or foreign commerce, or which contains materials which have been transported in or affecting interstate or foreign commerce, by any means including by computer, or knowingly reproduces any visual depiction for distribution using any means or facility of interstate or foreign commerce or in or affecting interstate or foreign commerce, if the producing of such visual depiction involves the use of a minor engaging in sexually explicit

conduct and such visual depiction is of such conduct, or any person who attempts to do so, shall be guilty of a federal offense.

b. 18 U.S.C. §§ 2252(a)(4)(B) and (b)(2) provide, in relevant part, that any person who knowingly possesses, or knowingly accesses with intent to view any visual depiction that has been transported using any means or facility of interstate or foreign commerce or in or affecting interstate or foreign commerce, or which was produced using materials which have been so transported, by any means including by computer, if the producing of such visual depiction involves the use of a minor engaging in sexually explicit conduct and such visual depiction is of such conduct, or any person who attempts to do so, shall be guilty of a federal offense.

DEFINITIONS

8. The following terms are relevant to this affidavit in support of this application for an arrest warrant:

a. *Child Erotica:* The term "child erotica" means any material relating to minors that serves a sexual purpose for a given individual, including fantasy writings, letters, diaries, books, sexual aids, souvenirs, toys, costumes, drawings, and images or videos of minors that are not sexually explicit.

b. *Child Pornography:* The term "child pornography" is defined at 18 U.S.C. § 2256(8). It consists of visual depiction of sexually explicit conduct where (a) the production of the visual depiction involved the use of a minor engaged in sexually explicit conduct, (b) the visual depiction is a digital image, computer image, or computer-generated image that is, or is indistinguishable from, that of a minor engaged in sexually explicit conduct, or (c) the visual depiction has been created, adapted, or modified to appear that an identifiable minor is engaged in sexually explicit conduct), as well as any visual depiction, the production of which involves the use of a minor engaged in sexually explicit conduct. *See* 18 U.S.C. §§ 2252 and 2256(2), (8).

c. *Minor:* The term "minor" means any person under the age of eighteen years. *See* 18 U.S.C. § 2256(1).

d. *Sexually Explicit Conduct:* The term "sexually explicit conduct" means actual or simulated (a) sexual intercourse, including genital-genital, oral-genital, or oral-anal, whether between persons of the same or opposite sex; (b) bestiality; (c) masturbation; (d) sadistic or masochistic abuse; or (e) lascivious exhibition of the genitals or pubic area of any persons. *See* 18 U.S.C. § 2256(2).

e. *Visual Depictions:* "Visual depictions" include undeveloped film and videotape, and data stored on computer disk or by electronic means,

which is capable of conversion into a visual image. *See* 18 U.S.C. § 2256(5).

9. The following technical terms are relevant to my affidavit in support of this application for an arrest warrant.

a. As part of my training, I have become familiar with the Internet (also commonly known as the World Wide Web), which is a global network of computers[1] and other electronic devices that communicate with each other using various means, including standard telephone lines, high-speed telecommunications links (e.g., copper and fiber optic cable), and wireless transmissions including cellular networks and satellite. Due to the structure of the Internet, connections between computers on the Internet routinely cross state and international borders, even when the computers communicating with each other are in the same state. Individuals and entities use the Internet to gain access to a wide variety of information; to send information to, and receive information from, other individuals; to conduct commercial transactions; and to communicate via electronic mail ("e-mail").

[1] The term "computer" is defined by 18 U.S.C. § 1030 (e) (1) to mean "an electronic, magnetic, optical, electrochemical, or other high speed data processing device performing logical, arithmetic, or storage functions, and includes any data storage facility or communications facility directly related to or operating in conjunction with such device, but such term does not include an automated typewriter or typesetter, a portable hand held calculator, or other similar device."

b. Set forth below are some definitions of technical terms, used throughout this Affidavit, and in Attachments A and B, hereto, pertaining to the Internet and computers more generally.

i. *Client/Server Computing*: Computers on the Internet are identified by the type of function they perform. A computer that provides resources for other computers on the Internet is known as a server. Servers are known by the types of service they provide; that is, how they are configured. For example, a web server is a machine that is configured to provide web pages to other computers requesting them. A client computer is a computer on the Internet that is configured to request information from a server configured to perform a particular function. For example, if a computer is configured to browse web pages and has web page browsing software installed, it is considered a web client.

ii. *Compressed file*: A "compressed file" is a file that has been reduced in size through a compression algorithm to save disk space. The act of compressing a file will make it unreadable to most programs until the file is uncompressed.

iii. *Computer system and related peripherals, and computer media*: As used in this Affidavit, the terms "computer system and

related peripherals, and computer media" refer to tapes, cassettes, cartridges, streaming tape, commercial software and hardware, computer disks, disk drives, monitors, computer printers, modems, tape drives, disk application programs, data disks, system disk operating systems, magnetic media floppy disks, hardware and software operating manuals, tape systems and hard drives and other computer-related operation equipment, digital cameras, scanners, in addition to computer photographs, and other visual depictions of such graphic interchange formats, including but not limited to, JPG, GIF, TIF, AVI, and MPEG.

iv. *Digital device*: A "digital device" includes any electronic system or device capable of storing and/or processing data in digital form, including central processing units; desktop, laptop or notebook computers; tablets, internet-capable cellular phones (smart phones), or personal digital assistants; wireless communication devices such as telephone paging devices, beepers, and mobile telephones; peripheral input/output devices such as keyboards, printers, scanners, plotters, monitors, and drives intended for removable media; related communications devices such as modems, cables, and connections; storage media

such as hard disk drives, flash drives, thumb drives, floppy disks, compact disks, DVDs, magnetic tapes, and memory chips; and security devices.

v. *Domain Name*: "Domain names" are common, easy to remember names associated with an internet protocol address (defined below). For example, a domain name of "www.usdoj.gov" refers to the internet protocol address of 149.101.1.32.

vi. *Hash value*: A "hash value" is a mathematical algorithm generated against data to produce a numeric value that is representative of that data. A hash value may be run on media to find the precise data from which the value was generated. Hash values cannot be used to find other data. The term "SHA-1" or "SHA-1 hash" refers to a type of hash value that may be given to a computer file. The SHA-1 is a cryptographic hash function designed by the United States National Security Agency and is a United States Federal Information Processing Standard. SHA stands for "secure hash algorithm." SHA-1 hash value is the standard for unique identifying numbers. It is computationally infeasible for two files with different content to have the same hash values. I am unaware of any instance in

which two files have been naturally assigned the same SHA-1 hash value.

vii. *Image or copy*: An "image or copy" is an accurate reproduction of information contained on an original physical item, independent of the electronic storage device. "Imaging" or "copying" maintains contents, but attributes may change during the reproduction.

viii. *Internet Service Providers (ISPs) and the Storage of ISP Records*: Internet Service Providers 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, cellular networks, dedicated circuits, or satellite-based subscription. ISPs typically charge a fee based upon the type of connection and volume of data, called bandwidth, which 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 and can access the Internet. ISPs maintain business and other records ("ISP records") pertaining to their subscribers (regardless of whether those subscribers are individuals or entities). These records may include account application information, subscriber and billing information, account access information (often times in the form of log files), e-mail communications, information concerning content uploaded and/or stored on or via the ISP's servers, and other information, which may be stored both in computer data format and in written or printed record format. ISPs reserve and/or maintain computer disk storage space on their computer system for their subscribers' use. This service by ISPs allows for both temporary and long-term storage of electronic communications and many other types of electronic data and files. Typically, e-mail that has not been opened by an ISP customer is stored temporarily by an ISP incident to the transmission of that e-mail to the intended recipient, usually within an area known as the home directory. Such temporary, incidental storage is

defined by statute as "electronic storage." *See* 18 U.S.C. § 2510 (15). A service provider that is available to the public and provides storage facilities after an electronic communication has been transmitted and opened by the recipient, or provides other long-term storage services to the public for electronic data and files, is defined by statute as providing a "remote computing service." *See* 18 U.S.C. § 2711(2).

ix. *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 four numbers separated by a period, and each number is a whole number between 0 and 254. 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. Some ISP's employ dynamic IP addressing, that is they allocate any unused IP addresses 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. On the other hand, some ISP's, 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. Absent some break in service, static IP addresses generally do not change over a period of time, and typically remain assigned to a specific computer.

x. *Log files*: "Log files" are records automatically produced by computer programs to document electronic events that occur on computers. Computer programs can record a wide range of events including remote access, file transfers, logon/logoff times, and system errors. Logs are often named based on the types of information they contain. For example, web logs contain specific information about when a web site was accessed by remote computers; access logs list specific information about when a computer was accessed from a remote location; and file transfer

logs list detailed information concerning files that are remotely transferred.

xi. *Malicious Software ("malware")*: Software designed to infiltrate a computer without the owner's informed consent is called "malicious software" or "malware." The expression is a general term used by computer professionals to mean a variety of forms of hostile, intrusive, or annoying software or program code. Software is considered malware based on the perceived intent of the creator rather than any particular features. Malware includes computer viruses, worms, Trojan horses, most rootkits, spyware, dishonest adware, crimeware, and other malicious and unwanted software.

xii. *Metadata*: "Metadata" are data contained in a file that is not usually associated with the content of a file but is often associated with the properties of the application or device that created that file. For example, a digital camera photograph often has hidden data that contains information identifying the camera that manufactured it and the date the image was taken.

xiii. *Steganography*: "Steganography" is the art and science of communicating in a way that hides the existence of the communication. Within the computer world, it can be used to

hide a file inside another. For example, a child pornography image can be hidden inside another graphic image file, audio file, or other file format.

xiv. *Trace Route*: A "trace route" is an Internet debugging tool used to document the list of inter-connected computers between two computers on the Internet. A trace route will list the names and IP addresses of computers that provide the physical link between two computers on the Internet. Trace routes are useful tools to help geographically identify where a computer on the Internet is physically located, and usually includes information about the registered owner of computers on the Internet.

xv. *Uniform Resource Locator (URL)*: A "uniform resource locator" is the address of a resource or file located on the Internet. It is also called a "domain name."

xvi. *Web site Hosting*: "Web site hosting" provides the equipment and services required to host and maintain files for one or more web sites and to provide rapid Internet connections to those web sites. Most hosting is "shared," which means that multiple web sites of unrelated companies are on the same server in order to reduce associated costs. When a client develops a web site, the client needs a server and perhaps a web hosting company to host

it. "Dedicated hosting" means that the web hosting company provides all of the equipment and assumes all of the responsibility for technical support and maintenance of a web site. "Co-location" means a server is located at a dedicated hosting facility designed with special resources, such as a secure cage, regulated power, a dedicated Internet connection, online security and online technical support. Co-location facilities offer customers a secure place to physically house their hardware and equipment as opposed to keeping it in their offices or warehouses, where the potential for fire, theft, or vandalism is greater.

xvii. The terms "*records*" and "*information*" includes all forms of creation or storage, including any form of computer or electronic storage (such as hard disks or other media that can store data); any handmade form (such as writings, drawings or paintings); any mechanical form (such as printing or typing); and any photographic form (such as microfilm, microfiche, prints, slides, negatives, videotapes, motion pictures, or photocopies).

COMPUTERS AND CHILD PORNOGRAPHY

10. Based upon my knowledge, training, and experience in child exploitation and child pornography investigations, and the experience and training

of other law enforcement officers with whom I have had discussions, computers and computer technology have revolutionized the way in which child pornography is produced, distributed and utilized. Prior to the advent of computers and the Internet, child pornography was produced using cameras and film, resulting in either still photographs or 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 images 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 contacts, mailings, and telephone calls, and compensation for these wares would follow the same paths. More recently, through the use of computers and the Internet, distributors of child pornography use various distribution networks, including but not limited to, personal email contacts, file-sharing services, f- and list serves, and membership-based/subscription-based web sites to conduct business, allowing them to remain relatively anonymous.

11. The development of computers has also revolutionized the way in which child pornography collectors interact with each other, and sexually exploit children. Computers serve four basic functions in connection with child pornography: production, communication and distribution, and storage. More

specifically, the development of computers has changed the methods used by child pornography collectors in these ways:

a. Production: Producers of child pornography can now produce high resolution still and moving images directly from a common video or digital camera. In this day and age, these types of cameras have become ubiquitous, and are located on nearly every cell phone sold. Once taken, images and videos can be saved onto a computer or uploaded onto a website or attached to an email within seconds. While still on the camera or after being saved onto a computer or uploaded into a photo or video editing program, images can be edited in ways similar to how a photograph may be altered. Images can be lightened, darkened, cropped, or otherwise manipulated. Videos can be edited, or spliced together to create montages of abuse that can be several minutes to several hours long. As a result of this technology, it is relatively inexpensive and technically easy to produce, store, and distribute child pornography. In addition, there is an added benefit to the pornographer in that this method of production does not leave as large a trail for law enforcement to follow. In some cases, depending upon the sophistication of the producer, it may be virtually impossible to law enforcement to determine the source of a sexually explicit image.

b. Communication and Distribution: The Internet allows any computer to connect to another computer. By connecting to a host computer, electronic contact can be made to literally millions of computers around the world. In addition, the Internet allows users, while still maintaining anonymity, to easily locate (i) other individuals with similar interests in child pornography; and (ii) web sites that offer images of child pornography. Child pornography collectors can use standard Internet connections, such as those provided by businesses, universities, and government agencies, to communicate with each other and to distribute child pornography. These communication links allow contacts around the world as easily as calling next door. Additionally, these communications can be quick, relatively secure, and as anonymous as desired. All of these advantages, which promote anonymity for both the distributor and recipient, are well known and are the foundation of transactions between child pornography collectors over the Internet. Sometimes the only way to identify both parties and verify the transportation of child pornography over the Internet is to examine the recipient's computer to look for "footprints" of the web sites and images accessed by the recipient.

c. Storage: The computer's capability to store images in digital form makes it an ideal repository for child pornography. Moore's law

predicts that the number of transistors in a dense integrated double circuit doubles approximately every two years. In the computing world, this translates to a doubling of computer memory capacity roughly every 24 months. It is not uncommon to encounter hard drives with 1 terabyte or more of data. According to Apple, Inc., 1TB of data can hold approximately 2 million standard resolution photographs. If those images are in high-resolution format, the number decreases to 26,000. *See* http://www.dpreview.com/forums/thread/3467175. A 1TB drive can also hold 357 DVD quality movies. *See* http://wiki.answers.com/Q/How_many_standard_movies_can_be_stored_on_a_1TB_external_hard_drive. The size of the electronic storage media (commonly referred to as a hard drive) used in home computers has grown tremendously within the last several years. Hard drives with the capacity of 1 terabyte are not uncommon. These drives can store thousands of images at very high resolution. Storage options located outside the physical boundaries of a computer add another dimension to the equation. It is possible to use a video camera to capture an image, process that image in a computer, and save that image to the cloud or to a server located in another country. Once this is done, there may be no readily apparent evidence at the "scene of the crime." Only with careful laboratory examination of electronic storage

devices is it possible to recreate the evidence trail.

PEER TO PEER FILE-SHARING

12. "Peer-to-peer file-sharing" ("P2P") is a method of communication available to Internet users through the use of special software. P2P file sharing is a method of communication available to Internet users through the use of special software programs. P2P file sharing programs allow groups of computers using the same file sharing network and protocols to transfer digital files from one computer system to another while connected to a network, usually on the Internet. A user first obtains the P2P software, which can be downloaded from the Internet; this software is also available through applications that can be downloaded and used on smart phones. There are multiple types of P2P file sharing networks on the Internet. Computers using the software are linked together through the Internet to form a network that allows for the sharing of digital files between users on the network.

13. In general, P2P software allows the user to set up files on a computer to be shared with others running compatible P2P software. A user obtains files by opening the P2P software on the user's computer, and conducting searches for files that are currently being shared on another user's computer, and by viewing the files that another user has made available. One of the advantages of P2P file-sharing is that multiple files may be downloaded in parallel. This means that the user can download more than one file at a time.

14. In general, P2P client software allows the user to set up file(s) on a computer to be shared on a P2P file sharing network with other users running compatible P2P client software. A user can also obtain files by opening the P2P client software on the user's computer and conducting a search for files that are of interest and currently being shared on a P2P file sharing network.

15. Some P2P file sharing networks are designed to allow users to download files and frequently provide enhanced capabilities to reward the sharing of files by providing reduced wait periods, higher user ratings, or other benefits. In some instances, users are not allowed to download files if they are not sharing files. Typically, settings within these programs control sharing thresholds.

16. Typically, during a default installation of a P2P client software program, settings are established which configure the host computer to share files. Depending upon the P2P client software used, a user may have the ability to reconfigure some of those settings during installation or after the installation has been completed. A setting establishes the location of one or more directories or folders whose contents (digital files) are made available for distribution to other P2P clients. In some clients, individual files can also be shared. In addition, a setting controls whether or not files are made available for distribution to other P2P clients. A setting also controls whether or not users will be able to share portions of a file while they are in the process of

downloading the entire file. This feature increases the efficiency of the network by putting more copies of file segments on the network for distribution.

17. Typically, files being shared by P2P clients are processed by the client software. As part of this processing, a hashed algorithm value is computed for each file and/or piece of a file being shared (dependent on the P2P file sharing network), which uniquely identifies it on the network. A file (or piece of a file) processed by this hash algorithm operation results in the creation of an associated hash value often referred to as a digital signature. Some hash algorithms provide a certainty exceeding 99.99 percent that two or more files with the same hash value are identical copies of the same file regardless of their file names. By using a hash algorithm to uniquely identify files on a P2P network, it improves the network efficiency.

18. Because of this users may receive a selected file from numerous sources by accepting segments of the same file from multiple clients and then reassembling the complete file on the local computer. This is referred to as multiple source downloads. The client program succeeds in reassembling the file from different sources only if all the segments came from exact copies of the same file. P2P file sharing networks use hash values to ensure exact copies of the same file are used during this process.

19. A P2P file transfer is assisted by reference to an Internet Protocol (IP) address. Third-party software is available to identify the IP address of the P2P

computer sending a file. Such software monitors and logs Internet and local network traffic.

FACTS IN SUPPORT OF PROBABLE CAUSE

Background of the Investigation

20. On May 19, 2014, I was working in an undercover capacity and connected to a P2P file-sharing program from an Internet-connected computer in the Juneau, Alaska office of the FBI. This P2P program identifies other computers on the network that are sharing image and video files of child pornography. By comparing SHA-1 hash values of previously identified images and videos of child pornography with the SHA-1 hash values of files available on the network, I was able to identify computers on the file-sharing network that I believed were offering files of minors engaged in sexually explicit conduct. On May 19, 2014, the P2P program identified a computer connected to the Internet through IP address 65.74.22.111 that was making suspected child pornography files available for others to download through the P2P network. *Downloads from IP Address 65.74.22.111*

21. On May 19, 2014, I began attempting to download files from 65.74.22.111 using the P2P program. I utilized a modified version of the P2P software that permitted law enforcement to conduct single-source downloads, that is downloads from a single IP address. I only attempted to download files that 65.74.22.111 was making available to the entire network.

22. On June 5, 2014, I observed that the P2P program on the computer using the IP address 65.74.22.111, reported its version as 2.2.7.3051 and its program nickname as anon_414a166f@Ares.

23. On June 5, 2014, SA Peterson conducted a query on the IP address 65.74.22.111 through the American Registry for Internet Numbers (ARIN). ARIN is a non-profit corporation headquartered in Chantilly, Virginia that manages the allocation of IP addresses. The Registry showed the IP was registered as of that date to ISP General Communications, Inc. (GCI), and was used in Wrangell, Alaska.

24. On June 5, 2014, I attempted to download through a P2P network a previously identified suspected child pornography video from a computer connected to the Internet using IP address 65.74.22.111. The child pornography video being requested was named "(pthc) dad and cumming in toddler.avi" and was identified by the unique Sha-1 value "W3WLH7SDVQ3DXGYCPILWY4OB2PUXRE6T." I know from my training and experience that "pthc" is an acronym for "pre-teen hard core," and is widely used on the Internet among individuals who possess, distribute, receive, and produce images of child pornography. This acronym may refer to child pornography images and videos that depict the extreme sexual abuse of children.

25. On June 5, 2014, at 08:48:11, my law enforcement computer established a connection with a computer located at 65.74.22.111. At 08:48:16, my law enforcement computer began downloading the file named "(pthc) dad and cumming in toddler.avi". At 08:52:02, the download was ended, and 632 kilobytes of

the 14.6 megabytes of this file were downloaded. That downloaded portion of the requested child pornography file is only15 seconds in length and is viewable. I viewed the downloaded portion of the video titled "(pthc) dad and cumming in toddler.avi" and saw that it showed an adult male rubbing his erect penis on the exposed vagina of a toddler. The child depicted in the video "(pthc) dad and cumming in toddler.avi" is prepubescent, and appears to be under four years of age; the child's face cannot be seen. I estimated the child's age by comparing her tiny body size to that of the adult male, and by her undeveloped physical appearance.

Identification of IP Address 65.74.22.111 and Its Link to the SUBJECT

26. On July 14, 2014, an administrative subpoena was issued to GCI requesting subscriber information for IP address 65.74.22.111, between the dates of May 19, 2014 and July 14, 2014.

27. On July 29, 2014, GCI provided the following subscriber information for IP address 65.74.22.111:

> Greg or Laura Salard
> Address: PO Box 1831, Wrangell, Alaska
> Physical Address: 3362 Zimovia, Wrangell, Alaska
> Active Date: February 17, 2009
> Services: Cable Modem
> Status: Active

28. I reviewed Alaska Department of Motor Vehicles (DMV) and Alaska Public Safety Information Network (APSIN) records for the SUBJECT and found

that those databases listed his mailing address as PO Box 1831, Wrangell, Alaska, and his residential address as 3.5 Mile Zimovia Highway, Wrangell, Alaska.

29. Alaska Airlines records show a reservation for a September 6, 2014, flight for the SUBJECT, purchased on Alaskaair.com by the SUBJECT using IP address 65.74.22.111.

30. United State Forest Service the SUBJECT lived at 3362 Zimovia, Wrangell, Alaska, and that there were no unsecured wireless signals emitting from that address.

31. On August 1, 2014, your affiant learned from USFS LEO Ault that Greg Salard was employed by Alaska Island Community Services, at the Wrangell Medical Center, as a Doctor. This information was confirmed by the Wrangell Medical Center's website that list Greg Salard, M.D. as practicing family medicine treating both adults and children. There was a picture of Greg Salard M.D. on the Wrangell Medical Center's website that matches the photo of Greg Salard that I received and reviewed from the State of Alaska DMV.

32. On October 1, 2014, I spoke to a customer service agent with GCI, who stated that addresses on accounts in rural Alaska are provided by the customer.

33. A search of the Accurint information database (a public records database that provides names, dates of birth, addresses, associates, telephone numbers, e-mail addresses, etc.) was conducted for the SUBJECT. The search listed his address as 3.5 Zimovia Highway, Wrangell, Alaska.

Subsequent Activity at IP Address 65.74.22.111

34. I know from my training and experience that "hussyfan" is a term used on the Internet among individuals who possess, distribute, receive, and produce images of child pornography. This term is often included in the names of image and video files that show minors engaged in sexually explicit conduct.

35. On October 1, 2014, at 11:49 AM, I used the search term "hussyfan" on a P2P network and identified the IP address 65.74.22.111 port 2466 as a download candidate for three video files of suspected child pornography. The file names being made available by the computer at IP address 65.74.22.111 were "(pthc) meikko special lolimania (rare file).avi", (pthc)(liluplanet((lordofthering) cristi_happy.avi" and "(muy chavita siendo violada(2).mpg." As explained above, "pthc" is a term commonly associated with child pornography. I am aware that the phrase "Muy chavita siendo violada" translated to English is "Very little girl being raped."

36. My investigation revealed that between February 01, 2014 and October 5, 2014, the IP address 65.74.22.111 has made available for download by other users of the P2P network at least 104 files containing suspected images and videos of child pornography, or parts of a series that contain suspected images and videos of child pornography. In addition to having previously been identified in other law enforcement investigations as possible images of child pornography, many of these files contained acronyms, words, or phrases that in my training and experience are consistent with images and videos of child pornography. Indeed,

many of the acronyms, words, and phrases used in these file names have been used in other files I have observed which I know show child pornography. Among the files being offered by the computer located at IP address 65.74.22.111 between February 2, 2014, and October 5, 2014, were the following:

a. "pthc daddy cum and lick daughter katy.mpg"

b. "(pthc) webcam – 5y &11y daughters show yours (1)[1](2).avi"

c. "pthc daddy cun and lick daughter katy.mpg"

d. "bibcam-kdv-pjk-pthc-rdv(42)(2)(3).mpeg"

e. "((hussyfan))pthc_colombia_girl_sexo infantile(3)(2).avi"

f. "pthc boy+man-11yo boy suck.mpg"

g. "pthc woman sucks little boy.avi"

h. "(pthc) webcam – 5y & 11y daughters show yours(1)[1](2).avi

Search of the Defendant's Residence

37. On October 10, 2014, I obtained a warrant to search the defendant's residence from United States Magistrate Judge Longenbaugh. Law enforcement officers executed this warrant on October 15, 2014. Prior to the execution of this search warrant the following observations were made on October 15, 2014 (all times noted are AKT):

a. At 8:10 a.m. (AKT), FBI Special Agent Matthew Judy observed Laura Salard leaving the residence of 3362 Zimovia, Wrangell, Alaska, in a 2003 Silver Subaru Forester with Alaska license plates.

b. At 10:31 a.m., a computer using the IP address 65.74.22.111 became a download candidate for the file "12 & 14 yo brasil adolescent boy and girl (0 04 26).avi." This file is a suspected file of child pornography.

38. At 10:39 a.m., USFS LEO Ault made a phone call to Greg Salard, 907-xxx-0361, this phone call was unanswered. One minute later, USFS LEO Ault and FBI SA Judy knocked on the SUBJECT's front door at 3362 Zimovia, Wrangell, Alaska; they received no answer. At 10:43 a.m., USFS LEO Ault made a second phone call to the SUBJECT; the SUBJECT answered and said that he could meet USFS LEO Ault at his front door in a few minutes.

39. At 10:45 a.m., SA Judy observed the SUBJECT walk through his living room wearing only a robe. After putting on his pants, the SUBJECT answered the front door of his residence and met with USFS LEO Ault and SA Judy at the entrance of his house. The suspect stated that he was the only one in the house.

40. SA Judy and USFS LEO Ault remained with the SUBJECT while other law enforcement agents entered the house. The SUBJECT was cooperative, but appeared nervous and was sweating profusely.

41. After entering the residence, I found an "Alienware" laptop computer in an upstairs common area with the inscription "BUILT FOR GREG A. SALARD, DESIGNED BY ALIENWARE" running a program named "CCLEANER64.EXE" I know this program to be a file-cleaner, that is, a type of software that can be used to completely wipe files from a computer's hard drive. The program showed that the

wipe was 35% complete. I stopped the program "CCLEANER64.EXE" and then began an on-scene preview of the computer using osTriage2.

42. An initial preliminary examination of the defendant's computers using osTriage2 showed the CCLEANER64.EXE program was started at 10:42:02 a.m. on October 15, 2014. I also observed that the Ares file-sharing program last connected on October 15, 2014, at 9:55:21 a.m., using Ares port number 2466. This is the same Ares port number observed on October 1, 2015, from the SUBJECT's IP address. I also located two files of child pornography on the computer. The images appeared to be the same, but were saved in different locations on the computer and are described as follows:

a. The first file was saved as c:\users\alien\appdata\roaming\real\rpds\content\images\115.jpg.

b. The second file was saved as c:\users\alien\appdata\roaming\real\rpds\content\images\45.jpg.

Both file show what appears to be a girl in her early teens exposing her vagina. The girl's age is estimated based on her face and body size.

43. Located on the couch next to the "Alienware" laptop was a detachable hard drive with what appeared to be a complete copy of the "Alienware" hard drive on it. The hard drive was named "Greg's computer 2014-10-12."

44. Law enforcement agents met with Laura Salard. During this interview, Laura Salard said that she has never heard of the program Ares and was

unaware of any peer-to-peer file sharing software. She also said that she very little computer knowledge, and that she rarely used her husband's computer.

45. I later conducted a more detailed examination of the hard drive from the SUBJECT's "Alienware" computer. The following deleted files were located:

a. __ARESTRA__(~pthc center~)(opva)(2012)mom and daughter(2).avi

b. __ARESTRA__(pthc)mom boy 10yr.avi

c. __ARESTRA__porno-mom – old sister and little kid.mpg

d. __ARESTRA__taboo – mom – father and daughter sex. Avi

e. __ARESTRA__pthc – 11yr mini's mom helps her get tied & double fuc'd.mpg

f. __ARESTRA__12yr fuck his mom.mpg

g. __ARESTRA__mom little boy fucks woman.mpg

h. 12 & 14 yo brasil adolescent boy and girl (0 04 26).avi

i. __ARESTRA__mom & friend catch son jerking off and help out.wmv

j. __ARESTRA__(pthc) mom boy 10yr.mpg

k. __ARESTRA__01(((kingpass))) st petersburg pthc – mom & 14 y old son 2.mpg

l. __ARESTRA__boy sucked by his mom.avi

m. __ARESTRA__(pthc)8yr mom rubbs daughter.mpg

n. __ARESTRA__!!!!new pthc daddy cum and lick k@ty-2(full very rare)(2.07)(b).avi

o. __ARESTRA__15 year old school girl lesbians (very cool)

p. __ARESTRA__xxx-nińa 9 ańos -video porno-146(2).mpg

q. __ARESTRA__(~pthc center~)(opva)(2012)buratino ra-07_new(4).avi

r. __ARESTRA__(~pthc center~)(opva)(2013)dolcemodz – star-011(2)(2).avi

s. __ARESTRA__!!(~pthc center~)(opva soft)(2014)tween twerk awesome ass 10yr girl youtube part 1.avi

t. __ARESTRA__!!(~pthc center~)(opva soft)(2014) playing with his dick 10yr boy youtube.avi

u. __ARESTRA__!!(~pthc center~)(opva soft)(2014) petlovergal 9yr girl panties and ass youtube.avi

v. __ARESTRA__!!(~pthc center~)(opva soft)(2014)jennifer 10yr girl bald pussy preview youtube.avi

w. __ARESTRA__!!(~pthc center~)(opva soft)(2014)finger fucking 10yr girl self and brother (kidcam)(unpublished).mpg

x. __ARESTRA__!!(~pthc center~)(opva soft)(2014)finger fucking 10yr girl self and brother (kidcam)(unpublished).avi

y. __ARESTRA__!!(~pthc center~)(opva soft)(2014)push it in sex play 9yr girl.avi

I have seen the term "ARESTRA" in other child pornography investigations included in file names of files I know to depict minors engaged in sexually explicit conduct.

CHARACTERISTICS OF CHILD PORNOGRAPHERS

46. My knowledge of preferential sex offenders and their characteristics is based on my experience as an FBI agent, and other training specific to child exploitation crimes and related computer storage I have received. Based upon such training and experience, as well as upon information provided to me by other law enforcement officers, I am aware of the following general characteristics of those who possess, view, receive, distribute, and produce child pornography, which may be exhibited in varying combinations:

a. Individuals who have a sexual interest in children or images of children may receive sexual gratification, stimulation, and satisfaction from contact with children, from fantasies they may have viewing children engaged in sexual activity or in sexually suggestive poses (such as in person, in photographs, or other visual media), or from literature describing such activity.

b. Individuals who have a sexual interest in children or images of children may collect sexually explicit or suggestive materials, in a variety of media, including photographs, magazines, motion pictures, videos, books, slides and/or drawings or other visual media.

Individuals who have a sexual interest in children or images of children often use these materials for their own sexual arousal and gratification. Further, they may use these materials to lower the inhibitions of children they are attempting to seduce, to arouse the selected child partner, or to demonstrate the desired sexual acts.

c. Individuals who have a sexual interest in children or images of children often maintain their collections in a safe, secure and private environment, such as a computer hard drive or separate digital media.

d. Individuals who have a sexual interest in children or images of children also may correspond with and/or meet others to share information and materials, and conceal such correspondence as they do their sexually explicit material. Individuals may often maintain lists of names, e-mail addresses or telephone numbers of individuals with whom they have been in contact, and who share the same interests in child pornography.

e. Individuals who have a sexual interest in children or images of children prefer not to be without their child pornography for any prolonged time period. This behavior has been documented by law enforcement officers involved in the investigation of child pornography throughout the world. The result is that individuals may travel with some or all of their collections, and that evidence of an individual's

interest in child pornography may be located in their vehicles. This is particularly true given the portable nature of many laptops computers, tablets, and storage devices that allow for easy transport between and individuals home and their ultimate destination.

CONCLUSION

1. I submit that this affidavit supports probable cause for an arrest warrant for GREG SALARD, 3362 Zimovia, Wrangell, Alaska. Based on my investigation, there is probable cause to believe that the SUBJECT has violated 18 U.S.C. §§ 2252(a)(2) (receipt or distribution of any visual depiction of a minor engaged in sexually explicit conduct), and 18 U.S.C. §§ 2252(a)(4)(B)(possession of any visual depiction of a minor engaged in sexually explicit conduct and possession of child pornography).

Respectfully submitted,

Sworn to by phone/Recorded by phone/Court record made

ANTHONY PETERSON
Special Agent
Federal Bureau of Investigation

Subscribed and sworn to before me on October 16, 2014. 3:06 pm

Redacted Signature

DEBORAH M. SMITH
United States Magistrate Judge
District of Alaska