AO 91 (Rev. 11/11) Criminal Complaint

UNITED STATES DISTRICT COURT

for the

Eastern District of California

United States of America
v.
Adam Alan Henry

Case No. 1:13-mj-00237-SAB

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 2007 to September 2013 in the county of Stanislaus in the Eastern District of California, the defendant(s) violated:

Code Section	*Offense Description*
18 USC 2252(a)	Receipt/Distribution of Child Pornography

This criminal complaint is based on these facts:

See attached affidavit.

☑ Continued on the attached sheet.

Complainant's signature

SA Mark E. Lucas, FBI
Printed name and title

Sworn to before me and ~~signed in my presence~~ signed electronically pursuant to Fed.R.Crim. P. 4.1 and 4(d).

Date: **Nov 8, 2013**

Judge's signature

City and state: Fresno, California

Stanley A. Boone, United States Magistrate Judge
Printed name and title

UNITED STATES DISTRICT COURT
EASTERN DISTRICT OF CALIFORNIA
FRESNO, CALIFORNIA

INTRODUCTION

I, Mark Lucas, being duly sworn, depose and state:

1. I am a special agent with the Federal Bureau of Investigation (FBI), currently assigned to the Sacramento Division, Modesto Resident Agency. I have been assigned to the Sacramento Division since 2009. I have been employed by the FBI since 2008. As part of my daily duties as a special agent, I investigate criminal violations relating to child exploitation and child pornography including violations pertaining to the illegal production, distribution, receipt and possession of child pornography, in violation of 18 U.S.C. §§ 2251 and 2252. I have received training in the area of child pornography and child exploitation and as part of my duties have observed and reviewed numerous examples of child pornography and visual depictions of minors engaged in sexually explicit conduct (as defined in 18 U.S.C. § 2256) in all forms of media, including computer media.

2. The statements contained in this affidavit are based in part on information provided by other law enforcement officers with whom I have spoken or whose reports I have read, and upon my own experience and background. This affidavit is being presented in support of a criminal complaint charging Adam Henry with violating 18 U.S.C. § 2252(a)(2) - Receipt or Distribution of Child Pornography received and/or distributed from 2007 to September 2013. One source of information has been Detective Britton Moore, who is assigned to the Ceres Police Department (CPD) and Sacramento Valley High Technology Crimes Task Force (SVHTCTF), Sacramento Internet Crimes Against Children Task Force (ICAC), and the FBI Sacramento Child Exploitation Task Force. The following information was derived from investigation conducted by the Ceres Police Department and myself.

PEER TO PEER NETWORKS

3. Detective Moore has received training in peer-to-peer (P2P) child pornography investigations. During these courses, he learned how to conduct investigations to identify persons using P2P software on the internet to traffic child pornography. P2P networks are frequently used to trade child pornography and individuals can choose to install publicly-available software that facilitates the trading of still images and videos. The software, when installed, allows a user to search for pictures, movies and other digital files by entering words and phrases as search terms. Also during the installation process, the user has the option to maintain all the default settings or make specific changes. One default option is the installation of a shared folder on the computer so downloaded files will be available for the P2P network to access. The essence of a P2P network is the availability of computers with shared folders for others to access and share. In the normal use of the program, search terms are sent to an ultra peer (sometimes called a super node). An ultra peer or super node is a computer on the network that handles incoming requests and examines submitted file lists from other computers (peers) that it is connected to for files matching the search terms. These file lists are a compilation of files in the shared folder. A file

list is then sent back to the requesting computer. The user then can choose to download files from peers who possess at least a portion of the file.

4. Search results presented to the user allow the user to select a file from the list and then receive that file (or portions of that file) from other users (peers) from around the world. The software can balance the network load and recover from network failures by accepting portions of the requested file from different users (peers) and then reassembling the file on the local computer.

5. P2P networks (software) can only succeed in reassembling the requested file from different parts if the portions all come from the same original file or an exact copy of the original file. Multiple persons (peers) sharing one file can deliver different portions of that file to the local software and the local software can insure that a complete and exact copy can be made from all the parts. I have been able to confirm from use of this type of software that different copies of the same file can have different names.

EDONKEY NETWORK

6. The eDonkey network is a peer-to-peer file-sharing network and is also known as the eDonkey2000 file-sharing network, or eD2k. Users of this network can simultaneously provide files to users while downloading files from other users. The eDonkey network can be accessed by computers running several different client programs. These programs share common protocols for network access and file-sharing. The user interface, features, and configuration may vary between clients and versions of the same client.

7. The eDonkey network uses MD4 root hash values to improve network efficiency. Users may receive a selected file from numerous sources by accepting segments of the file from multiple users and then reassembling the complete file on the local computer. The client program succeeds in reassembling the file from different sources only if all the segments came from exact copies of the same file. The network uses MD4 root hash values to ensure exact copies of the same file are used during this process.

INTERNET PROTOCOL (IP) ADDRESSES

8. I know from my training that networked computers identify each other by an internet protocol (IP) address. These IP addresses can assist law enforcement investigators in finding a particular computer on the internet. These IP addresses can help lead a law enforcement investigator to a particular Internet Service Provider (ISP) or Electronic Service Provider (ESP). Given the date and time an IP address was used, an ISP or ESP can often provide the name and physical address associated with the account holder.

GLOBAL UNIQUE IDENTIFIER (GUID)

9. P2P software may display the Globally Unique Identifier (GUID) identification of the P2P software programs offering to share files on the network or internet. A GUID is a random alphanumeric set of characters used in software programs, and a GUID is produced when some

P2P programs are installed on a computer. While each generated GUID is not guaranteed to be unique, the total number of GUIDs is so large that the probability of the same alphanumeric characters being generated twice is very small. When comparing GUIDs, an investigator can determine with a high degree of certainty that two or more different IP addresses that are associated with the same GUID are associated with the same computer.

10. By using publicly-available computer programs on the internet, it is possible to determine the geographical location of an IP address based on latitude and longitude information. This can give a general location in a particular city which can assist an investigator in determining legal jurisdiction. Also, with similarly available software on the internet, it is possible to determine which ISP/ESP owns the range of IP addresses related to a suspect IP address.

INVESTIGATIVE TOOLS

11. **Child Protection System** is a data collection system. Using this system Detective Moore was able to identify offenders in his region (Stanislaus County). It uses an automated software application called Peer Spectre and other similar types of software applications that search the Gnutella network, and other open source networks, for files using known child pornography search terms. These software applications identify computers at IP addresses that have files in their shared folder with hash values that match a database of suspected and known child pornography hash values. The software reads reported download candidates and logs the IP address, date, time, hash values, and filenames for each individual computer in the same way every time. The information gathered by Peer Spectre is uploaded to the Child Protection System, enabling investigators to query that data at any time.

12. **Shareaza LE** is a modified version of the free downloadable Shareaza P2P client software. It has been modified for law enforcement to meet stringent investigative requirements. Shareaza LE will only download files from a single source, the target IP address, while the public version will download files from many sources. Shareaza LE will log all activity and transactions that occur while connected to the target IP address. Shareaza LE can monitor several IP addresses, and when they come online, it will attempt to browse the shared folder, compare the SHA1 hash values of the files in the shared folder and then download any known child pornography files. Shareaza LE adheres to the common P2P protocols and functions the same way as the free public version (with the exception previously listed). Shareaza LE has no additional browsing or downloading capabilities over and above the free public version. In fact, Shareaza LE takes much longer to download files because of the single source limitation.

FACTS AND BACKGROUND

13. On September 10, 2013, using the Child Protection System, Detective Moore checked recent activity for IP addresses in Stanislaus County. He located an IP address of 71.94.43.84 that was on the "Recent Locates" for Stanislaus County. This means that the user of this IP address had recently downloaded known child pornography files, using the Gnutella network and/or the eDonkey network. Detective Moore initiated an investigation of the computer associated with that IP address (71.94.43.84).

14. CPS was reporting IP address 71.94.43.84, with the GUID of D818E0BE1217E24AB6279F5405912C90, as a source of files containing child pornography. Detective Moore focused his investigation on this IP address/GUID and launched the IP Address/GUID into ShareazaLE. The ShareazaLE program was able to initiate a "Browse Host" for IP address (71.94.43.84) which was displaying as a download candidate for at least 24 files containing child pornography.

15. The GUID D818E0BE1217E24AB6279F5405912C90 had been associated with this IP address (71.94.43.84) for several months. CPS was reporting activity for this IP address and GUID between the time frame of June 13th, 2013, and September 9th, 2013.

16. Detective Moore noted the filenames associated with IP address 71.94.43.84. Each of the filenames contained terms that he recognized, through his training and experience, to be consistent with child pornography. Detective Moore compared the SHA1 hash values and/or eDonkey hash values reported as available from this IP address (71.94.43.84) to files with the same hash value recovered in previous investigations and concluded that the files depicted minors engaged in sexually explicit conduct.

17. Detective Moore also determined that the IP address, 71.94.43.84, belonged to Charter Communications.

18. On September 11, 2013, a state search warrant was issued by the Honorable Dawna Reeves of the Stanislaus County Superior Court, to be served at Charter Communications for the subscriber information records related to this investigation. The search warrant was for subscriber information records for IP address 71.94.43.84 within the time in which the above IP address (71.94.43.84) was believed to have been associated with peer-to-peer file-sharing software and the receipt and/or distribution of child pornography files.

19. On September 18, 2013, Charter Communications communicated that IP address 71.94.43.84 had been assigned to Lock-n-Stitch during the times that Detective Moore's investigation showed that child pornography files were being made available for sharing. The response from Charter Communications also showed that the IP address was a static IP address, meaning it had been indefinitely assigned to Lock-N-Stich.

SEARCH WARRANT AT LOCK-N-STITCH

20. On September 19, 2013, a search warrant was issued by the Honorable Timothy Salter, Judge of the Stanislaus County Superior Court, to be served at LOCK-N-STITCH, 1015 S. Soderquist Rd. Turlock CA 95380 for computers and other digital media devices.

21. Ceres Police Officers served the search warrant at Lock-N-Stitch and conducted an onsite preview of computers they encountered. Two computers were located inside of the Information Technology (IT) Office. Detective Moore located a computer on a desk along the north wall. This computer was powered on and the screen was locked with a password. The user account that was logged on was "Adam Henry". The owner of the company informed Detective Moore the IT manager for the business was Adam Henry and that he had full and exclusive control of

the entire company's network and computers. He also told Detective Moore there were no other employees with access to that computer. Further there were no other employees assigned to the IT department other than Adam Henry.

22. There were two hard drives located inside of the computer tower. During an onsite preview of the hard drives, detectives located the peer-to-peer program, Shareaza. Detective Moore conducted a forensic analysis of the hard drives. On the hard drive containing the operating system, Detective Moore located numerous child pornography videos under the user account "Adam Henry". These files were located under the peer-to-peer folder structure, specifically the "Incomplete" folder.

23. One of the files viewed was:
btih_MTBDWWNPJTPOTKDZWVBKNO7IOFH3OJ7U.partial

This was a portion of a larger digital video approximately 41:30 minutes in length. This file was approximately 503MB in size. The viewable portion of this video depicted a white, female child approximately 8 years of age and a white male adult. There were several scenes of this video which were viewable. These scenes depicted the child completely nude and placing her mouth on the adult male's erect penis and performing oral copulation. Another scene depicted the adult male inserting his erect penis into her anus and sodomizing her.

24. There was also a folder titled "Shareaza" on the root of the drive, which did not contain any files. Detective Moore suspected this may have been where the user had directed that the completed files be stored. The fact that the folder was empty led Detective Moore to believe Henry (the suspected computer user) had emptied the folder by moving the files to another device and most likely taken the files to a different location such as his home.

25. The owner of Lock-N-Stitch provided Henry's home address as XXXX Burman Dr. Turlock Ca 95XXX.

SEARCH WARRANT AT ADAM HENRY'S RESIDENCE

26. On September 19, 2013, at approximately 1933 hours, a search warrant was issued by the Honorable Timothy Salter, Judge of the Stanislaus County Superior Court, to be served at XXXX Burman Dr, Turlock Ca 95XXX for computers and other digital media devices. Henry was located, and he agreed to go to his residence and to show investigators where he stored the files that he had acquired by using peer-to-peer programs. Henry was transported by Ceres PD to his residence where he showed investigators a Netgear media storage device. Henry explained there would be files shared through peer-to-peer programs stored on that device. Henry logged on to a computer located in his living room and accessed the Netgear media storage device using his password "Stitch@11". Detective Moore opened one of the video files and observed child pornography. He then collected the computer and associated hard drives as evidence.

27. Upon a forensic review of the computers seized by Ceres PD, Detective Moore found 110 videos containing children engaged in sexually explicit conduct, as described in 18 USC 2256, that had been downloaded from the internet. In addition, multiple videos were found that appear

to have been produced by Henry using a hidden camera in his residence. One of the cameras appears to have been secreted in the bathroom of the residence where visitors to the residence were recorded while using the bathroom (more specifically a toilet and a shower). These videos were catalogued and sorted according to the victim's name on Henry's computer.

28. Three videos of a 14 year-old victim were found on the computer. The victim was identified by investigators and interviewed by Ceres PD. The video depicts the victim changing clothes in the bathroom of the residence and taking a shower showing the victim's nude body. The victim was shown clips of the video collected and stated that did not know that she was video recorded while showering.

29. Another recovered video depicts the victim and Angele Henry, trying on clothes in the main bedroom of the residence. During the video Angele Henry sets up and adjusts the camera prior to the victim entering the room. During the video, Angele coaxes the victim to remove her clothing while trying on a corset. While the victim appears to be apprehensive about changing clothes in front of her, Angele removes the victim's bra and positions the victim toward the camera. As this happens, the victim's breasts are exposed to the camera and Angele moves the victim's hair to maintain a line of sight of the victim's breasts.

30. It should be noted there was a child care business being operated out of the residence. Angele Henry lived at the residence with her two children from a previous relationship. One child was a 7 year-old boy and the other child was a 6 year-old girl. A records check confirmed that Adam Henry and his spouse (Angele) filed an application with the State of California to operate a family day care business. In addition to the children living at the residence, at least two other minor children were being cared for by Angele Henry.

31. Detective Moore and I reviewed the digital evidence recovered by CPD. I believe the following videos and images, among others, to be child pornography that Henry received, through the internet:

> Title: (~pthc center~)(opva)(2012) Asian cambodian SVAY001 (snd)_xvid.avi
> SHA1 Hash: 2NAOLFI7FUY7AV4U6I4U5OTGCY44SOGW

32. This file is a digital video approximately 21:25 minutes in length. This video shows four Asian female children approximately five to eight years old who are standing on what appears to be a bed. They are all told to undress until they are completely nude. Then a white adult male stands in between them and the children start masturbating the adult male's erect penis. They each take turns performing oral copulation on the adult male's penis. The adult male takes turns with the girls holding their ankles and hanging them upside down while they perform oral copulation on the adult male's erect penis. The next scene shows the adult male laying on his back, on what appears to be a bed. One of the children is performing oral copulation on the adult male's erect penis while he digitally penetrates another child's vagina. The video continues on with similar scenes of oral copulation, masturbation and digital penetration of the children's vaginas. The children have very small physical frames and do not appear to have any pubic hair. The children have no breast development. These children are notably smaller than the adult male.

Title: (Pthc) 12Yo Boy Turky Fuck Mother.avi
SHA1 HASH: 66OI6OXUTQ77PNVIARZ3NZ6RCJASNCGV

33. This file is a digital video approximately 17:17 minutes in length. The video shows a white female child approximately five years old. The video begins with the child lying on top of a naked white adult female and the two of them are kissing. A second white adult female is massaging and digitally penetrating the child's anus and vagina with her fingers. The next scene shows a white adult male now penetrating the child in the anus, while the child lies on top of the adult female. The next scene shows the child orally copulating an adult female's vagina. The next scene shows the two adult females and the child orally copulating the adult male's erect penis. The next scene shows the adult females performing orally copulating, masturbating, and digitally penetrating the child's vagina. The next scene shows the child lying on her back while the adult male rubs and penetrates the child's vagina and anus with his erect penis. The final scene shows the child seated in a bathtub and an adult female holding the child down while the adult male urinates on the child.

CONCLUSION

34. Based on the above information, it is my opinion that probable cause exists to believe that Adam Henry received and/or distributed child pornography between 2007 and September 2013 in Turlock, California in violation of 18 U.S.C. § 2252(a)(2).

Mark E. Lucas
Special Agent
Federal Bureau of Investigation

Approved as to form

/s/ David Gappa
David Gappa
Assistant United States Attorney

Affidavit submitted by email/pdf and attested to me as true and accurate by telephone consistent with Fed.R.Crim. P. 4.1 and 4(d) before me this 8th day of November, 2013.

THE HONORABLE STANLEY A. BOONE
United States Magistrate Judge