

FILED
UNITED STATES DISTRICT COURT
DISTRICT OF NEW MEXICO

AO 91 (Rev. 08/09) Criminal Complaint

UNITED STATES DISTRICT COURT

10 OCT -7 PM 3:47

for the
District of New Mexico

CLERK - LAS CRUCES

United States of America
v.
David Rounbehler

Case No.

10-2634 MJ

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 April 30, 2010 in the county of Dona Ana in the
District of New Mexico, the defendant(s) violated:

| Code Section | Offense Description |
|-----------------------|--|
| 18 U.S.C. 2252(a)(2) | Knowingly receives, or distributes any visual depiction involving the sexual exploitation of minors. |
| 18 U.S.C. 2252 (a)(4) | Possession of child pornography |

This criminal complaint is based on these facts:

See attached affidavit

Continued on the attached sheet.

Complainant's signature

Stephani Mendoza, Special Agent

Printed name and title

Sworn to before me and signed in my presence.

Date: October 7, 2010

Judge's signature

KAREN B. MOLZEN
U.S. MAGISTRATE JUDGE

Printed name and title

City and state: Las Cruces, New Mexico

AFFIDAVIT SUPPORTING COMPLAINT ON DAVID ROUNBEHLER

1. Immigration and Customs Enforcement (ICE) Special Agents (SA) assigned to the Resident Agent in Charge (RAC) Las Cruces working in conjunction with the Las Cruces Police Department (LCPD) and the United States Marshal Service (USMS) are utilizing training received at the "Child Protection System" to identify Internet Protocol (IP) addresses that are actively downloading and uploading identified and known child pornography and videos in the Gnutella network.

LIMEWIRE AND THE GNUTELLA NETWORK

2. LimeWire is a peer-to-peer ("P2P") file sharing program that operates on the Gnutella network to both locate and share files. Gnutella is a network protocol – a standardized system of queries and responses that allows individual computers to speak with each other. LimeWire functions as a gateway to the Gnutella network, allowing individual computers to connect to and search other computers on the Gnutella network. If someone with LimeWire installed on their computer wants a file, he or she can download it directly from the computer that holds it. The process works as follows:
 - A. A user downloads LimeWire software onto his or her computer. The software makes connections through the Internet to Gnutella programs on other computers. Each computer acts as both a client and a server. Each computer can send and receive files. There is no central server.
 - B. The user then runs a search for whatever file he or she seeks. When a user searches the network, the search begins from his or her computer. LimeWire sends the search to the connected computers, and they forward the search along their connections. The search may come to a computer that has a match. The computer with the match then sends a message through the Internet back to the first computer.
 - C. LimeWire searches for files by their file name. For instance, if a computer sharing the file "Classical Music.mp3" gets a search for "classical", it's a match. The text inside documents isn't searched.

Text search can't extend into the audio or video content of media files. Individual users set the file names.

- D. Once the search results come back the user reviews LimeWire's list of search results and double clicks the desired file. LimeWire contacts the computers that have the file and begins downloading. Different parts of the file come may from different computers. LimeWire keeps trying to request file fragments until it can assemble the complete file.
- E. In order to access the Gnutella network using LimeWire, a user must have access to a computer which communicates through a modem connected to a telephone line or other high-speed telecommunications medium, with other computers on the network. A user must then download and install the LimeWire software. Once the software is installed, a user may determine which files he or she wants to share over the network. This is accomplished by placing files into a "shared" folder.

DETAILS OF INVESTIGATION

April 30, 2010: Las Cruces Police Department Officers download child pornographic images from an IP address associated with Defendant's residence

- 3. On April 30, 2010, an investigation began on a P2P network. A peer offering to participate in the trafficking of child pornography was discovered (digital files with SHA1 signatures previously identified as child pornography were available in the peer's shared file directory). The peer's IP address was identified as 71.228.108.205. Using the automated software application, at 4:53 p.m. (MST) a digital file was downloaded from the peer's shared file directory. The file was viewed by a Computer Forensic Officer working with the Las Cruces Police Department (the "Forensic Officer") and discovered it was a movie that showed a nude female, approximately two to three years of age, being vaginally raped by an adult male, using his penis.
- 4. Forensic Officers observed 12 additional digital files in this peer's shared file directory. The automated software application was in the

process of downloading a third file when the peer became unavailable on the P2P network. The application was, however, able to record the SHA1 signatures of all 14 files in this peer's shared file directory on that date. Using the SHA1 signatures of the 12 files not downloaded, the Forensic Officer was able to search the P2P network and download those exact files from other sources, in order to verify whether or not they were child pornography. The Forensic Officer was able to obtain the peer's IP address and information that it was assigned to a Comcast account in New Mexico.

5. P2P computer software has different methods to insure that two files are exactly the same. The method used by the P2P Operation described herein involves a compressed digital representation method called Secure Hash Algorithm Version 1 or SHA1. Your Affiant knows that the Secure Hash Algorithm (SHA) was developed by the National Institute of Standards and Technology (NIST), along with the National Security Agency (NSA), for use with the Digital Signature Standard (DSS) as specified within the Secure Hash Standard (SHS). The United States of America has adopted the SHA1 hash algorithm described herein as a Federal Information Processing Standard.
6. Digital files can be processed by this SHA1 standard resulting in a digital signature. By comparing these signatures your Affiant can conclude that two files are or are not identical with a precision that greatly exceeds 99.9999 percent certainty. Affiant knows through the computer forensic community that there has never been a documented occurrence of two different files being found on the Internet having different contents while sharing the same SHA1 value.
7. The P2P network investigated in this operation uses the SHA1 digital signature to verify the unique identity of individual files. Users attempting to trade files on a P2P file-sharing network can place files from their local computer in a shared file directory. If that user then starts the P2P software that local computer calculates the SHA1 signature for each shared file and provides that information to other users wishing to trade files.
8. Entering search terms in the P2P software results in a list of SHA1 digital signatures that an Agent can choose for download. By using

this type of search an Agent compares the offered SHA1 signatures with SHA1 signatures known to belong to movies or images of child pornography. An Agent confirms these SHA1 values as belonging to child pornography by examining the files from previous investigations with the matching SHA1 value. By watching these movies or viewing these images your Affiant is able to determine the exact file referenced by the given SHA1 value. Once a matching set of digital signatures is identified, an Agent can submit a download request for the file.

9. When installing the P2P software utilized by the peer, in the setup process, a user must click on a box titled indicating whether or not they wish to add files they download from P2P users to their Public Shared list. The user is also advised, in the setup process that files in their Public Shared list is shared with the world." Affiant viewed the aforementioned additional five digital files located by the Forensic Officer on the P2P network and observed the five of those files contained Child Pornography:
 - A. SHA1 3Y75 ... is a movie depicting an obviously young female, approximately five years of age, lying under a blanket, being sexually abused by an adult male (oral penetration, digital penetration, ejaculation on child).
 - B. SHA1 50WH ... is a still image of a female about 12 years old, posed in a sexual manner, with her breasts and genitals visible.
 - C. SHA1 IAEB... is a movie depicting a female under the age of 13 being sexually abused by an adult male who penetrates her vagina with his mouth, hand and penis.
 - D. SHA1 L6AE... is a movie depicting two females under the age of 16 years engaged in masturbation. Also seen is a male being masturbated by children and a male vaginally penetrating females under the age of 16, both with his fingers and penis.
 - E. SHA1 T6YL. .. is a movie depicting a nude, prepubescent female lying down, displaying her genitals. This female is also seen masturbating an adult male and rubbing his penis on her vagina.

10. Affiant learned the following from the Forensic Officer, Certified Computer Forensic Examiner:

- A. In order to be able to view the files offered for distribution in the Defendant's shared file folder on the P2P network on April 30, 2010, the Defendant had to have also been in possession of those files.
- B. Seven of those files were found to contain child pornography and have been described above.

11. A federal summons was obtained for the IP address 71.228.108.205 and served on Comcast. Comcast supplied the following account holder information pertaining to that IP address on April 30, 2010:

Subscriber Name: David Rounbehler
Service Address: 4305 Del Prado Way, Las Cruces, NM
Account status: active

On May 12, 2010, the IP address changed to 76.113.44.96. Property records verified David and Anna Rounbehler as the homeowners of 4305 Del Prado Way, Las Cruces, NM.

June 8, 2010: A search of Defendant's home and a statement by Defendant reveals: that child pornographic images were kept on Defendant's computers; that one of the child pornographic images downloaded on April 30 was stored on a flash drive found in Defendant's desk; and that Defendant admitted to searching for and possessing child pornographic images.

12. Affiant learned the following from a search warrant executed on the Defendant's residence, 4305 Del Prado Way, on June 8, 2010:

- A. The only residents of the address are David Rounbehler and his wife, Anna Rounbehler.
- B. There were three computers in the home.
 - i. HP laptop - using Comcast internet service

- ii. Sony Vaio Laptop - using Verizon internet service
- iii. A Dell Desktop computer

C. The Rounbehlers used Comcast as their Internet Service Provider and had Comcast change their service to a Voice Over IP system approximately one month prior (May 12 according to Comcast records).

13. Affiant learned the following from Las Cruces Police Department Detective Kacee Thatcher, regarding the interview with the Defendant on June 8, 2010:

- A. Several years ago, former co-workers told Defendant that child pornography could be accessed over the internet. Out of curiosity, the defendant began searching the internet for child pornography. He was able to find a significant number of these images, which surprised him because he did not know that five and six year olds could have sex, as the Defendant stated. The Defendant stated he found the images to be "amazing."
- B. The Defendant has been searching for, viewing and downloading still images and videos containing child pornography ever since. Approximately one month prior to the date of the interview with the Defendant, the defendant's wife caught him looking at images of child pornography on his Dell desktop computer. He quickly tried to remove the images from his screen, but the hard drive in his computer was so corrupt that it ran very slow and she was able to see the images. His wife became very angry with him and told him that he needed to permanently delete those images, as well as any others he had.
- C. The Defendant stated his wife, Anna, is a retired software engineer, so she was able to provide him with specific instructions on how to clean his hard drive. After following those instructions, his hard drive was still running very slowly, so he decided to replace the hard drive with a new one. The Defendant believed his old hard drive was running so poorly due to the viruses/Trojans he was inadvertently acquiring on his file-sharing (P2P) networks. The

Defendant stated that he has intentionally downloaded videos and images containing child pornography from file sharing networks. He has also intentionally searched for, accessed and viewed child pornography on the internet.

D. Both the Defendant and his wife were concerned about any images that might still be readable on the old hard drive, so the Defendant drove a nail through the old hard drive and then threw it in the trash when he installed a new hard drive. About a month prior to this date, he purchased an HP laptop for himself. He does not have any file sharing networks on the new laptop. The Defendant stated he has not accessed child pornography on the new laptop but child pornography was found on the HP laptop. He utilizes a disk cleaning program on a daily basis and believes that his wife is probably checking his computer to see if he has anymore images containing child pornography.

E. In the past, the Defendant has used his Sony Vaio laptop as his primary computer, but when he purchased the new HP laptop, he gave the Sony Vaio to his wife. He used to have a file sharing network installed on the Sony laptop, but it was deleted long ago. He used to view child pornography on the Sony laptop, but believes he deleted all of those images. The Defendant has not used the new hard drive on the Dell desktop to view any pornography.

14. The Forensic Officers examined the Sony Vaio laptop computer seized from Defendant's home on June 8, 2010 and discovered that a wiping program had been run on the computer which had cleared out the internet cache and most active files. However, the computer also had Google desktop installed. Google desktop is an indexing program that creates a lists of all files on a computer, along with thumbnail photos of image files on the computer. Google desktop uses this index to quickly search for files on the computer. Even when an active file is deleted, remnants of the file – the file name, a thumbnail image, etc. – remain in the Google desktop index.

15. The Google desktop index of the Sony Vaio laptop computer showed that several hundred child pornographic images resided on that computer at one time.

16. The Forensic Officers also examined a small flash drive taken from the desk where Defendant was sitting when the search was executed. This flash drive contained evidence that file listed under the hash value beginning with SHA150WH . . . was stored on that flash drive at one time. In other words, the same image of a 12 year old female child that the Forensic Officer downloaded on April 30, 2010 was, at one time, stored on the flash drive found in Defendant's desk.

June 15, 2010: The State of New Mexico issues a warrant for Defendant's arrest; Defendant had already put his home up for sale and had moved to Massachusetts; Defendant is arrested by U.S. Marshal's and extradited to New Mexico.

17. Affiant learned a state arrest warrant was issued for David Rounbehler on July 15, 2010. When law enforcement went to the Rounbehler's residence the house was for sale. David and Anna Rounbehler listed their residence for sale on June 15, 2010 (seven (7) days after the execution of the search warrant). The Rounbehler's sold the furniture in their residence and moved to Boston, Massachusetts during the week of June 15, 2010. The Rounbehler's also replaced their cell phone numbers with new numbers. The Rounbehler's were located in Boston, Massachusetts by the United States Marshal Service (USMS) and David Rounbehler was arrested and extradited to Las Cruces, NM.

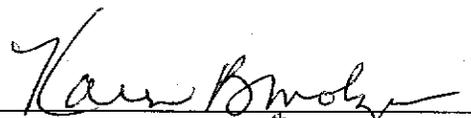
Forensic Officers determine that the images that Defendant distributed on April 30, 2010, and the computer equipment used to store and distribute those images, travelled in interstate and/or foreign commerce.

18. The Forensic Officer has software that enables him/her to trace the transmission of electronic files from his/her computer to the destination computer. The Forensic Officer has performed several tests, or "pings," to determine what route the digital transmissions took when travelling from the Forensic Officer's computer to the Defendant's IP address. To "ping" defendant's IP address, the Forensic Officer simply sent a series of digital signals, known as "packets" to Defendant's IP address. As the packets pass through the

internet, information pertaining to the path the packets take is returned to the Forensic Officer's computer. Each of these several "pings" showed the transmission traveling first through Albuquerque, New Mexico and then through either Dallas, Texas or Denver, Colorado. The packets then returned to Las Cruces and attempted to contact the defendant's IP address.

19. Your Affiant has also consulted with other law enforcement officers who have informed her that that Comcast subscribers in New Mexico utilize Dynamic Host Configuration Protocol (DHCP) and Domain name System (DNS) servers located in either Pennsylvania or Colorado. Based on this statement, a customer located in New Mexico would access a server outside of New Mexico when a Comcast subscriber uses their computer to access the Internet.
20. The Forensic Officer has also researched the manufacturing origin of the three computers taken from Defendant's residence, and which Defendant admitted to using to store child pornographic images. The Forensic Officer determined that all of those computers were manufactured in the Peoples Republic of China. The materials used to store, receive, and distribute the child pornographic images described above therefore travelled in interstate and foreign commerce when the computers travelled from the Peoples Republic of China to the United States and ultimately to Las Cruces, New Mexico.


Special Agent Stephani Mendoza


Sworn before me this 7th day of October
The Hon. Karen B. Molzen