AO 91 (Rev. 08/09) Criminal Complaint

UNITED STATES DISTRICT COURT

for the

District of New Mexico

United States of America
v.
Juan Larry Barela

Defendant(s)

Case No. 10-2767MJ

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 July 25, 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: ______

Judge's signature

City and state: Las Cruces, New Mexico

Printed name and title

AFFIDAVIT SUPPORTING COMPLAINT ON JUAN LARRY BARELA

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 Unites 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 on the Gnutella network.

A) Background:

Affiant learned the following facts and information from Special Agent Anthony Manfredi on September 15, 2010 while assisting with a search warrant at 6015 Ledesma Drive, Las Cruces, New Mexico:

1. In July 2007, the New Mexico State Police, Online Predator Unit began working an Internet undercover operation to identify persons using peer-to-peer (P2P) software on the Internet to traffic in child pornography. Peer-to-peer networks are frequently used in the trading of child sexual abuse images.

2. While examining P2P file sharing networks computer users can choose to install publicly available software that facilitates the trading of images. The software, when installed, allows the user to search for pictures, movies and other digital files by entering text as search terms. That text search is sent to an ultra-peer. An ultra-peer is an index server that handles requests, examines submitted text searches and routes the requests to peers that it knows about that may have a file that matches the submitting peer's request. A file list is then sent back to the requesting user who can choose to download files from peers who possess at least a portion of the file.

3. Search results presented to the user allow the user to select a file and then receive that file from other users around the world. These users can receive the selected file from numerous sources at once. The software can balance the network load and recover from network failures by accepting pieces of the file from different users and then reassembling the file on the local computer. Software on the P2P network works at the request of a peer to another peer.

Other users of the network can not upload or push a file to another computer on the network. A file can only be transferred once a request has been made from the originating computer.

4. P2P networks can only succeed in reassembling the file from different parts if the parts all come from the same original file. Multiple persons sharing one file can deliver different pieces of that file to the local software and the local software can insure that a complete and exact copy can be made from the parts. Special Agent Anthony Manfredi has been able to confirm from use of the software that different copies of the same file can be named differently.

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. Special Agent Anthony Manfredi knows that 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. This method has proven to be extremely reliable, working just like software used by end users around the world in locating and downloading precise files. Once the download of child pornography is initiated an Agent receives a list of download candidates that are participating in the possession, receipt and/or distribution of child sexual exploitation images. This feature allows an Agent to conduct undercover operations that involve images of child sexual abuse being traded on peer-to-peer networks.

10. Internet computers identify each other by an Internet Protocol or IP address. Affiant knows that these IP addresses can assist law enforcement in finding a particular computer on the Internet. These IP addresses lead the law enforcement officer to a particular Internet service provider or company (ISP). Given the date and time the IP address was used, an ISP can typically identify the account holder by name and physical address.

11. Special Agent Anthony Manfredi learned that searching on a peer-to-peer network as described above results in your Affiant receiving a list of IP addresses identifying locations where a computer has P2P software installed and individual files have been reported as available for download with a specific digital signature (SHA1).

12. These computers are referred to as a download candidate. A download candidate is a computer that was reported by an ultra-peer as a source for the file listed by SHA1 value. In almost every known case the download candidate serves those files to P2P users across the Internet. Computers from throughout the world can download files from download candidates without regard to geographic location. The files located on P2P download candidates are quickly available throughout the world due to the distributed sharing model of P2P networks.

13. Shareaza LE is a modified version of the free downloadable Shareaza Gnutella client software. It has been modified for law enforcement to meet the stringent investigative requirements of these cases. Shareaza LE will only download files from a single source – the target IP, while the public version will download from many sources. Shareaza LE will log all activity and transactions that occur while connected to the target IP. Shareaza LE will monitor several IPs and when they appear online, attempt to browse the shared folder, compare the hash values of the files in the shared folder to the Peer to Peer hash database, and download any suspected child sexual abuse image files.

14. Shareaza LE adheres to the common Gnutella protocols and functions exactly the same way as the free public version. 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.

15. Special Agent Anthony Manfredi has validated Shareaza LE by conducting investigations manually using publicly available Gnutella clients and compared the results with the automated Shareaza LE process and found the results to be exactly the same.

16. Special Agent Anthony Manfredi knows that Detective Wiltse, with the Salem, Oregon Police Department has created an automated software application named GnuWatch, which sends Gnutella-based network messages to computers offering to distribute child pornography. These computers, or peers, are ones previously identified by investigative methods listed above, as well

as automated software tools such as Peer Spectre. GnuWatch sends messages to these peers, requesting to download the files they are advertising for distribution as well as a request to view the contents of their shared directory. These Gnutella-based network messages are open-source and widely documented on the Internet. Sergeant Matt Pilon has validated this software by sending similar requests to the same peer computers using publicly available file-sharing software. After doing so, Sergeant Pilon confirmed the peer computers responded to messages sent from GnuWatch in the same way as with publicly available file-sharing software.

17.The P2P software may display the Globally Unique Identifier (GUID) identification number of computers offering to share files on the network. A Globally Unique Identifier or GUID is a pseudo-random number used in software applications. This GUID number is produced when some P2P software applications are installed on a computer. While each generated GUID is not guaranteed to be unique, the total number of unique keys is so large that the probability of the same number being generated twice is very small. When comparing these GUIDs, your Affiant can quickly determine with a high degree of certainty that two different IP addresses that are associated with the same GUID are associated with the same computer.

18.Cooperating police agencies pool their information to assist in identifying criminal conduct and build probable cause to further criminal investigations. With this pooled information police get a better understanding of the global information available about a suspect that resides in their area of jurisdiction. This information is valuable when trying to regionalize a suspect to a certain jurisdiction, given the global scope of the Internet. Investigators from around the world gather and log information, which can be used by an investigator to build probable cause on one specific case.

19.Special Agent Anthony Manfredi has learned that by examining a list of IP addresses an Agent can locate computers that are reported to be in New Mexico. By comparison of the SHA1 digital signatures your Affiant can conclude that a computer, originating from an IP address known to be in New Mexico, has P2P software installed on it and contains images of child sexual abuse. With this information a request can be made to the Internet service provider to identify the specific physical address related to the use of P2P software in the exchange of images of child sexual abuse.

20. Special Agent Anthony Manfredi is aware that numerous search warrants have been executed in the State of New Mexico and throughout the United States using the above method of investigation. This method has proven to be extremely reliable in determining the location of computers that were involved in the P2P-facilitated trading of child sexual abuse images. Special Agent Anthony Manfredi has been involved in many of those search warrants and that the above listed method of investigation, almost every case was verified through the following means:

21. Evidence of child sexual exploitation was found on the computer.

22. If no images of child sexual exploitation were found on the computer, interviews of persons using those computers verified that images and or materials of child sexual abuse had been present at one time but had been deleted or the computer with the images of child sexual abuse had been removed from the premises.

23. Images moved from computer and stored on other media.

B) Current Investigation

1. The current investigation involves activity in reference to IP address 76.113.88.162 which occurred on the following date and time:
   a) July 25, 2010 at 07:30 GMT

2. The following was learned from Sergeant Matt Pilon and Agent Anthony Manfredi of the New Mexico State Police Online Predator Unit.
   a) Sergeant Pilon utilized software configured to search the Gnutella network for IP address/computers which were offering to share or possess, at least in part, files known to law enforcement that contain images/videos of child sexual abuse.
   b) Upon reviewing the logs within the Law Enforcement version

of the peer to peer software, Sergeant Pilon noted this activity occurring on each of the above mentioned dates.

c) Sergeant Pilon noted that a computer utilizing IP address of 76.113.88.162 was offering to participate in the trafficking of child sexual abuse images.

d) Sergeant Pilon was also able to determine that the IP address was assigned to the Internet service provider (ISP) Comcast Communications within New Mexico. In addition to the IP address, he also noted and identified a specific GUID (2944E28727A9A628E114357DD72C8800) that was associated with the above IP address.

e) Sergeant Pilon noted that from these logs on each of the above mentioned dates and times, a computer utilizing IP Address **76.113.88.162** was seen with files containing SHA 1 values which have been previously identified as depicting images of child sexual abuse.

f) Agent Manfredi reviewed these file lists and noted that there were numerous files on the listings.

g) Agent Manfredi also noticed the overwhelming majority of the file names were pornographic in nature and many appeared to be directly referencing underage children. A few of these file names were listed as:

   1. Kids-Boy&Girl-13-real child porn!!!(illegal preteen underage Lolita kiddy incest little girl rape anal cum sex l.jpg
   2. Candy-058-001_preteen teensex childfugga r%40ygold bd-company kdquality ptsc pthc new newer tori 9yo sandra fucked raped abused forced daughter torture cum lsm lsn 5yo 5yo 7yo .jpg
   3. Jailbait girls too young for sex but too hot and horny to resist even family males are targets of their lust Real incest13.jpg

h) Agent Anthony Manfredi examined a copy of some of the files listed on the logs which included their filenames, and SHA values. After examining these files, Affiant noted the following information for a file seen on July 25, 2010:

SHA VALUE:
ICYAZPJY7DWR2MBKEYNKPWV3LOG2HA5H
FILE NAME:
Kids Teens Women (Porno-Lolitas-Preteens-Reelkiddymov-R@Ygold-Hussyfans-

Underage-Girls-Children-PedofiliaPthc-Ptsc-Xxx-Sexy)01.jpg
DESCRIPTION: An adult male is shown forcing his erect penis into the vagina of a prepubescent female child that may be as young as 10 years old.

i) Special Agent Anthony Manfredi concluded from specialized training and experience that the logged results indicated that a computer utilizing IP address 76.113.88.162 on the following date and time was receiving, possessing and/or distributing child sexual abuse images:
   1. July 25, 2010 at 07:30

j) The software can be configured to allow parts of the files to be shared even if the copy located at these listed IP addresses have not yet been completely downloaded.

k) Sergeant Pilon conducted an Internet search on the origin of the IP address 76.113.88.162 and found it to be issued to Comcast.

l) Working this as a joint investigation, Sergeant Pilon requested the assistance of Immigration & Custom Enforcement Special Agent, Christine Brital. Agent Brital completed a summons requesting the identification of the subscriber using the IP address 76.113.88.162 used on:
   1. 7/25/2010 at 07:30:37 GMT

m) On August 10, 2010, Comcast replied via facsimile. Special Agent Brital forwarded these results to Sergeant Pilon. The response indicated that one account had been accessing the IP address on the dates and times in question. The response contained the following information:

Subscriber Name:	Juan Barela Jr.
Account Status:	Active
Account Created:	06/08/10
Subscriber Address:	6015 Ledsma Dr Las Cruces NM 88005
Billing Address:	P.O. Box 92 Dona Ana, NM 88032-0092
Telephone Number:	575-644-4519
Type of Service:	Residential High Speed Internet Service
Account Number:	8497950580002800

n) Agent Manfredi interviewed Juan Barela on September 14, 2010, at approximately 1600 hrs during the execution of the search warrant.

o) Agent Manfredi learned the following during the interview:

1. Juan Barela confessed to downloading and possessing child pornography.
2. Barela also informed SA Manfredi he set up a peephole camera in the bathroom at his apartment in California. Barela videotaped his wife, sister-in-law and 15 year old niece on different occasions
3. He then transported the video to Las Cruces where agents found it in a backpack in Barela's bedroom during the execution of the search warrant on September 14th .
4. Juan Barela and his wife are currently separated due to other (not specific) videotapes Barela's wife found.
5. Juan Barela informed SA Manfredi there is a friend of his that resides in California that he used to watch peephole/child pornography videos with.
6. Juan Barela also used his friend's credit card to purchase different videos of child pornography.
7. Juan Barela has since moved to Las Cruces where he resides with his mother, father, sister and nephew.

3. Affiant learned the following from Officer Max Weir of the Las Cruces Police Departments Digital Evidence laboratory:

a) Officer Weir has extensive training in Digital Evidence and Computer Forensics.

b) Officer Weir assisted Agents with the search of the residence on 6015 Ledsma Dr. on September 14th 2010.

c) Officer Weir found in the bedroom identified as the defendant's , a laptop computer and an external USB harddrive.

d) Officer Weir used his equipment and training to pre-view the contents of the devices at the residence the day of the search warrant.

e) Officer Weir observed numerous video files and images of illegal nature on the Laptop and the external harddrive.

f) Officer Weir later conducted a forensic exam of the digital evidence and found the following:

1. The file named Kids Teens Women (Porno-Lolitas-Preteens-Reelkiddymov-R@Ygold-Hussyfans-Underage-Girls-Children-PedofiliaPthc-Ptsc-Xxx-Sexy)01.jpg was found on the External

Drive.

2. The file was located on on the "root" of the drive with several other illegal images.
3. The GUID identified by Sergeant Pilon was found on the Laptop computer, in what Officer Weir knows is a remnant of the configuration files for the Limewire file-sharing program which uses the Gnutella network.
4. The SHA value provided by Sergeant Pilon was found on the Laptop computer, in one of the configuration files for the Limewire program.
5. The laptop showed the external harddrive had been connected to the laptop.

g) He has software and training that enables him to trace the transmission of electronic files from his computer to the destination computer.

h) He used a function in the software to determine the routes the digital transmissions took to reach the suspects IP Address.

i) To "ping" the defendant's IP address, Officer Weir sent a series of digital signals, known as "packets" to the Defendant's IP address.

j) The packets pass through other computers known as nodes on the way to the destination IP address.

k) For each successive "hop" the information pertaining to the location of the node computer is returned to the computer used by Officer Weir.

l) That information showed the transmission traveling first through Albuquerque, New Mexico and then through either Dallas Texas, Denver Colorado, or Los Angeles California.

m) The test was performed numerous times and the results all showed that the information traveled to other states prior to returning to Las Cruces.

n) Based on these facts, a customer located in New Mexico would access servers outside of New Mexico when the Comcast subscriber uses their computer to access the internet.

Special Agent Stephani Mendoza

Sworn Before me this 22nd day of October
The Hon. Carmen E. Garza