

AO 91 (Rev. 11/11) Criminal Complaint

UNITED STATES DISTRICT COURT

for the

Middle District of Florida

United States of America
v.

MATTHEW C. GRAZIOTTI

Defendant(s)

Case No.

6:14-mj- 1381

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 2012 to on or about July 14, 2014 in the county of Volusia in the Middle District of Florida, the defendant(s) violated:

<i>Code Section</i>	<i>Offense Description</i>
18 U.S.C. § 2252A 18 U.S.C. § 2251	Distribution, Receipt and Possession of Child Pornography. Production of Child Pornography.

This criminal complaint is based on these facts:

Continued on the attached sheet.

Alyson Samuels
Complainant's signature

Alyson Samuels, Special Agent
Printed name and title

Sworn to before me and signed in my presence.

Date: 7/14/14

Gregory J. Kelly
Judge's signature

City and state: Orlando, Florida

Gregory J. Kelly, United States Magistrate Judge
Printed name and title

STATE OF FLORIDA

CASE NO. 6:14-mj-

1381

COUNTY OF ORANGE

AFFIDAVIT IN SUPPORT OF CRIMINAL COMPLAINT

I, Alyson Samuels, being duly sworn, do hereby depose and state as follows:

1. I have been employed as a Special Agent (SA) with the Federal Bureau of Investigation (FBI) for the past 11 years. I am currently assigned to the FBI Jacksonville Division, Daytona Beach Resident Agency.

2. The statements contained in this affidavit are based on my experience and background as a law enforcement officer, including my experience with the Federal Bureau of Investigation (FBI), and information provided by other Special Agents (SAs) and task force officers of the FBI familiar with this case.

3. I have received specialized training in the investigations of sex crimes, child exploitation, child pornography and computer crimes. I have participated in investigations of persons suspected of violating federal child pornography laws, including 18 U.S.C. § 2252A. I have also participated in various training courses for the investigation and enforcement of federal child pornography laws in which computers are used as the means for receiving, transmitting, and storing child pornography. Additionally, I have participated in the execution of search warrants involving searches and seizures of computers, computer equipment, software and electronically stored information.

4. This affidavit is submitted in support of an application for the issuance of a criminal complaint and arrest warrant for the residence of Matthew C. Graziotti (Graziotti). As set forth in more detail below, I believe there is probable cause that Graziotti

distributed, received and possessed child pornography, that is, sexually explicit images of minors, in interstate commerce, in violation of 18 U.S.C. § 2252A. I also believe there is probable cause that Graziotti knowingly used, persuaded, enticed or coerced a minor to engage in sexually explicit conduct for the purpose of producing a visual depiction of such conduct using materials that had been mailed, transported or shipped in interstate or foreign commerce, in violation of 18 U.S.C. § 2251(a).

5. I make this affidavit from personal knowledge based on my participation in this investigation, information from other criminal investigators, information from law enforcement officers, information from agency reports, and the review of documents provided to me by these witnesses and law enforcement officers. Because this affidavit is being submitted for the limited purpose of seeking a criminal complaint, I have not set forth each and every fact learned during the course of this investigation.

STATUTORY AUTHORITY

6. Title 18, United States Code, Sections 2252A(a)(2) and (a)(5), prohibit a person from knowingly transporting, distributing, receiving, or possessing any child pornography, as defined in 18 U.S.C. § 2256(8), using any means or facility of interstate commerce, or in or affecting interstate commerce, or that was produced using materials that have been mailed, shipped or transported in or affecting interstate or foreign commerce. Title 18, United States Code, Section 2251(a) prohibits a person from knowingly using, persuading, inducing, enticing or coercing a minor to engage in sexually explicit conduct for the purpose of producing a visual depiction of such conduct using materials that have been mailed, shipped or transported in or affecting interstate or foreign commerce.

DEFINITIONS

7. The following definitions apply to this Affidavit:

a. "Child Pornography," as used herein, includes the definition in 18 U.S.C. § 2256(8), which defines child pornography as any 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).

b. "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).

c. "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).

PEER TO PEER (P2P) FILE SHARING

8. A growing phenomenon on the Internet is peer to peer file sharing (hereinafter "P2P"). P2P file sharing is a method of communication available to Internet users through the use of special software. The software is designed to allow users to trade digital files over the Internet.

9. For this investigation, the FBI, during this undercover session utilized the P2P program, Gigatribe, a publicly available peer-to-peer file sharing program. To use Gigatribe, a user only has to download the free program and then select the folder(s) on their computer they want to share. Gigatribe allows file sharing through the peer to peer user and is limited to those users whom have been included in each other's private network. In order for a user to add someone to that user's private network, the requesting user must send an electronic "Invite" through Gigatribe. The receiving user will then receive a message that they have been invited by the requesting user. Prior to deciding whether to accept or refuse the Invite, a user can access the sender's "User Details" which is similar to a mini-profile. This contains user-generated information that is neither confirmed nor reviewed by Gigatribe.

10. Once a user accepts the Invite, that user is added to the requesting user's private network and generally allowed to access/download any files they are sharing. Likewise, that user can view/download the requesting user's shared files. Users can also password protect their files.

11. Users connect through the Gigatribe program and exchange files directly from one computer to another. Therefore, a downloaded file comes from a single user's computer and only that computer. The Gigatribe program offers a paid version (a/k/a

"Premium" or "Ultimate") which allows a user to download pieces of the same file from various people in their network (multi-source downloads). However, law enforcement mainly uses the free version of Gigatribe for the single source download component. In the case of some ID takeover accounts, law enforcement cannot avoid using the paid (multi-source download) version of Gigatribe. In those instances, each and every file transfer is monitored to ensure that the file is downloaded from only one source/ user. When downloading a file, the Gigatribe "Transfer Screen" renders a visual depiction of each file transfer. This includes the user(s) that the Gigatribe user is downloading from. In cases of multi-source downloads, the user can prevent any part of the file from being downloaded from any source except the subject.

12. After downloading and installing Gigatribe, a user specifically designates the folders they want to share with other users on their private network. Folders are not automatically shared by default. When viewing the shared folders of a target user, you are viewing the shared folder structure, folder names, file names, etc., exactly as it appears on the targeted user's computer.

13. Identification of a target is accomplished by way of a network protocol analyzer (NPA), commonly referred to as a "packet sniffer," which records and displays the Internet packet traffic between the undercover's computer and the target's computer. The undercover uses "CommView" which is kept running during the entire undercover session. Therefore, as the undercover downloads files from the target computer, CommView records the packet traffic and displays the corresponding IP address.

DETAILS OF THE INVESTIGATION

14. On May 19, 2014, FBI SA Kevin P. Matthews using a computer connected to the Internet, conducted an undercover online session using Gigatribe.

15. SA Matthews queried his network of "friends" and observed that the individual using the screen name "Enchanted_one" was logged into the network. SA Matthews saw that Enchanted_one was sharing two password protected file folders titled "HC" and "Vids." Enchanted_one also was sharing three folders titled "Boys Files," "boys" and "Girls" that were not password protected.

16. SA Matthews previewed the files in thumbnail view in the three folders that were not password protected. SA Matthews observed in these folders images depicting child pornography and video files with titles indicative of child pornography. SA Matthews downloaded approximately 141 child pornography images and six child pornography videos directly from Enchanted_one between approximately 10:08pm and 10:37pm Eastern Daylight Time (EDT). Most of these images showed the sexual abuse and exploitation of prepubescent children.

17. Enchanted_one initiated a chat session via the P2P software with SA Matthews. During this chat, SA Matthews asked Enchanted_one for his password. Enchanted_one responded that his password was "jura." SA Matthews used this password to review the contents in Enchanted_one's password protected shared folders. SA Matthews observed child pornography images and video files with titles indicative of child pornography in these folders. At that time, Enchanted_one's user profile showed that he had been a Gigatribe user since March 21, 2008.

18. SA Matthews used CommView to identify the Internet Protocol (IP) Address used by Enchanted_one as 97.103.221.10, registered to Time Warner Cable and assigned to Bright House Communications.

19. An administrative subpoena was served by the FBI on Bright House Network requesting subscriber information for the user assigned to the aforementioned IP address during the date and time the undercover session was conducted.

20. Neustar, a designated agent of Bright House Networks responded to the subpoena and provided that the subscriber was Matt Graziotti with a billing address of 3024 Mango Tree Drive, Edgewater, Florida 32141.

21. Your affiant conducted a search on Florida's Driver and Vehicle Information Database finding that Matthew C. Graziotti lives at 3024 Mango Tree Drive, Edgewater, Florida. In addition, on July 8, 2014, law enforcement officers observed Graziotti outside the residence. An Internet search revealed that Graziotti teaches 5th grade at a private school in South Daytona, Florida, and is the Director of the school's summer day camp program. Graziotti coaches middle school boys' sports programs. Graziotti formerly worked as a youth pastor at a church in Edgewater, Florida.

22. Your affiant reviewed the downloaded files from SA Matthew's undercover session and believes, based on my training and experience, that the three below listed files downloaded on May 19, 2014, from Enchanted_one are child pornography as defined in 18 U.S.C. § 2256. The following table provides information regarding those files:

DOWNLOADED FILES	DATE/TIME	CONTRIBUTING IP ADDRESS	DESCRIPTION
!Carlos4	05/19/2014 10:06 pm to 10:37 pm EDT	97.103.221.10	Approximately 4 year old boy holding his shirt up with one hand, to expose his penis, as his underwear and pants are around his ankles while he holds an adult's erect penis in his other hand.
0_13507800_1182611556	05/19/2014 10:06 pm to 10:37 pm EDT	97.103.221.10	Approximately 8 year old girl shown naked wearing a dog collar lying on her stomach while she is strapped down to a work out bench.
Adam and Anthony BB2	05/19/2014 10:06 pm to 10:37 pm EDT	97.103.221.10	Two approximately 9 year old boys lying on top of each other. Each boy has their head in the other boy's groin area and the other boy's penis in their mouth.

23. On July 11, 2014, the Honorable Magistrate Judge David A. Baker authorized the issuance of a search warrant for the residence of Matthew C. Graziotti.

24. On July 14, 2014, agents executed the search warrant at Graziotti's residence and determined that Graziotti lived alone at the residence. Graziotti's 10 year-old son was also present at the residence.

25. When agents entered the residence, they located an HP laptop computer in the living room. A forensic examiner determined that the computer's user was "Matt" with a computer name of "Matt's-computer."

26. The forensic examiner determined that Gigatribe was installed and running on the computer. The program was actively uploading and downloading files with names indicative of child pornography. The examiner looked at the Gigatribe downloads folder and determined that there were 8,761 images in the folder, many of which depicted the sexual abuse and exploitation of prepubescent males. One of the files, titled "7615676igp.jpg," depicts an adult woman with her mouth on a prepubescent boy's penis. The Gigatribe user account name was Enchanted_one. The user had 267 contacts on

Gigatribe, categorized by names such as "1teens," "cut off," "female," "no share," "nshare some," "other friends-trust," and "others."

27. The forensic examiner also determined that there was a folder entitled "personally known" on the hard drive of the HP laptop computer. That folder contained 41 subfolders titled with boys' names.

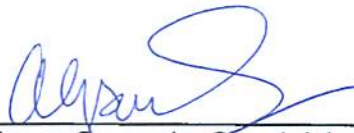
28. One of those folder's bearing the name of a boy contained a picture of Graziotti licking a prepubescent's boy's naked penis. The boy appears to be asleep on the couch in Graziotti's living room. The picture was created on or about June 30, 2012 with a Canon Powershot SX1301S camera. Agents located the camera in Graziotti's residence. The camera was manufactured in China.

29. Another folder titled with the name of another boy contains a picture of a 10 year-old boy asleep on Graziotti's couch in his living room. The picture depicts an individual pulling the child's shorts up and exposing his naked penis and scrotum. The picture was created on or about May 2, 2014 with a Nikon Cool Pix S9700 camera. Agents located the camera in Graziotti's residence. The camera was manufactured in Indonesia.

CONCLUSION

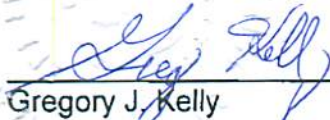
30. Based on the above, I have probable cause to believe that Matthew C. Graziotti knowingly produced, distributed, received and possessed child pornography that was produced using materials that were mailed, shipped or transported in interstate and foreign commerce, and using a facility of interstate commerce, in violation of 18 U.S.C. §§ 2252A(a)(2), (a)(5) and 2251(a).

Affiant further sayeth naught.



Alyson Samuels, Special Agent
Federal Bureau of Investigation

Sworn to and subscribed before me
this 14 th day of July, 2014.



Gregory J. Kelly
United States Magistrate Judge