

UNITED STATES DISTRICT COURT

for the

District of South Carolina

United States of America

v.

BRANDON D. GRESSETTE

Case No.

2:15mj122

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 May 2015 through July 2015 in the county of Berkeley in the District of South Carolina, the defendant(s) violated:

Code Section 18 U.S.C. Section 2422(b) Offense Description Use of an Interstate Commerce Facility to Coerce and Entice a Minor

This criminal complaint is based on these facts:

See attached affidavit.

Continued on the attached sheet.

Gerrick E. Munoz, FBI Special Agent (Signature)

Gerrick E. Munoz, FBI Special Agent (Printed name and title)

Sworn to before me and signed in my presence.

Date: October 22, 2015

Bristow Marchant, United States Magistrate Judge (Signature)

City and state: Charleston, South Carolina

Bristow Marchant, United States Magistrate Judge (Printed name and title)

IN THE UNITED STATES DISTRICT COURT
DISTRICT OF SOUTH CAROLINA
CHARLESTON DIVISION

AFFIDAVIT IN SUPPORT OF CRIMINAL COMPLAINT

Gerrick E. Munoz being duly sworn, deposes and states as follows:

INTRODUCTION

1. Affiant is a Special Agent with the Federal Bureau of Investigation (FBI), United States Department of Justice, and has served in that capacity since September 1998. Affiant has been assigned to investigate violent crimes against children violations in the Charleston, South Carolina, area since June 2015. As a case agent, Affiant has participated in several search warrants and interviews in child pornography investigations. Through Affiant's training, education, and experience, Affiant has become generally familiar with the manner in which child pornographers solicit minors into making nude pictures and videos of themselves. As part of Affiant's duties as an FBI Special Agent, Affiant has participated in investigations involving the use of undercover online Agents and surreptitious takeovers of child pornography networks.

2. Affiant is an investigative or law enforcement officer of the United States within the meaning of Title 18, United States Code, Section 2510(7), that is, an officer of the United States who is empowered by law to conduct investigations of, and make arrests for, the offense enumerated in Title 18, United States Code, Section 2422(b), which is known as Use of an Interstate Commerce Facility to Coerce and Entice a Minor. That section provides in relevant part: "Whoever, using the mail or any facility or means of interstate or foreign commerce, or within the special maritime and territorial jurisdiction of the United States knowingly persuades, induces,



entices, or coerces any individual who has not attained the age of 18 years, to engage in prostitution or any sexual activity for which any person can be charged with a criminal offense, or attempts to do so, shall be [guilty of a crime]....”

3. The statements in this affidavit are based in part on information and reports provided by other FBI Special Agents; written reports about this and other investigations that I have received, directly or indirectly, from other law enforcement agents; information gathered from the service of administrative subpoenas; the results of physical and electronic surveillance conducted by federal agents; independent investigation and analysis by FBI agents/analysts and computer forensic professionals; and my experience, training and background as a Special Agent with the FBI. Since this affidavit is being submitted for the limited purpose of securing an arrest warrant, I have not included each and every fact known to me concerning this investigation. I have set forth only the facts that I believe are necessary to establish probable cause to believe that Brandon D. Gressette committed the offense of Use of an Interstate Commerce Facility to Coerce and Entice a Minor, in violation of Title 18, United States Code, Section 2422(b).

STATEMENT OF PROBABLE CAUSE

Investigation of Website A

4. On January 22, 2015, the FBI arrested a subject (hereinafter “S1”) on charges related to his use of a website that facilitated the sexual abuse of minors and the production and trafficking of child pornography. Following his arrest, S1 consented to being interviewed by law enforcement agents. During the interview, S1 admitted to accessing, using, and sharing child pornography to that website. S1 also alerted agents to the existence of another website used by individuals to help facilitate the enticement of minors to engage in sexually explicit conduct via web camera (this

website is known to law enforcement and has been identified. It will hereinafter be referred to as “WEBSITE A”). S1 told investigators that he was a member of WEBSITE A.

5. S1 subsequently consented to allow the FBI to assume his online identity on the site. Between the dates of January 26, 2015 and March 11, 2015, an Under Cover Law Enforcement Officer (UCA) logged into WEBSITE A on various dates and times and was able to observe the activities of members of WEBSITE A. When going to the site, the UCA had to log in using a specific name and password. Once logged in, the UCA observed that the site’s main page functioned as a chat room. The right side of the page listed the members who were logged into the site at the time and the main page was a continuously running chat. In the chat section, the UCA observed that the users posted links in the forum to publicly available websites where children used live webcams, such as, but not limited to: Kik, YouNow (YN), YouTube, Chateen (CT), Condorchat (CC), and mylol.¹

6. At the bottom of the homepage of WEBSITE A, there were several tabs that appeared to represent different “tools” the members could use to target specific people chatting on YouNow. One of the tabs labeled “Vault” appeared to be a listing of files stored on www.mega.co.nz, a free cloud storage site that offers encryption, with the encryption key only known to the up-loader, not to the site administrators. The UCA noted that several of the files available in the Vault appeared to be child pornography.

7. One of the files the UCA viewed in the Vault appeared to be a composite of images from a video file that depicted a prepubescent girl exposing her vagina and spreading her labia as a close up to the camera.

¹ Kik is an instant messaging application for mobile devices that also allows users to share photos and videos. YouNow is a social networking site offering live streaming broadcasting capabilities. YouTube is a video-sharing website. Chateen and Condorchat are social networking sites utilizing live video and audio chat. And mylol is a teen dating site for teens in the US, Australia and the United Kingdom.

8. Another file viewed by the UCA in the Vault appeared to be a composite of images from a video file depicting a nude pubescent girl exposing her breasts and vagina and masturbating.

9. On February 27, 2015, the UCA logged into the site and attempted to access the Vault but received the following error message: "Sorry! Your access to the Vault has been revoked until you have a discussion with our entire team in our chat. Inactives do not deserve access to the Vault. Thanks for your understand and hope to see you soon to discuss this issue!" On March 11, 2015 the UCA was logged into the site when the administrator told the UCA that the UCA's access had been revoked due to the UCA continuing to attempt to access the Vault without contributing material to the site.

10. Open source searches revealed the IP address of the website to be hosted by OVH, a company located in Montreal, Quebec, Canada. On March 5, 2015, pursuant to a Mutual Legal Assistance request, members of the Royal Canadian Mounted Police (RCMP) provided the FBI with registration information for WEBSITE A. On March 11, 2015, the site was seized and taken down by the RCMP. An image of the server that hosted WEBSITE A was obtained by the RCMP and later provided to the FBI. A review of the image revealed various archive files and log files related to WEBSITE A, including but not limited to user login records and user chat records. OVH records provided the identifying information of the site administrator, (hereinafter "S2").

11. On April 15, 2015, the FBI executed a search warrant at the residence of S2. S2 consented to being interviewed by FBI agents. During the interview, S2 admitted to using WEBSITE A to facilitate the Specified Federal Offenses. S2 stated that WEBSITE A originally consisted of approximately 10-20 members, approximately 10 of which were still very active members. Members of the site were the people from other groups on the internet that were the most motivated to go out and get child pornography. S2 described WEBSITE A as a text chat room

where members would talk about getting children to self-produce images or videos of themselves engaging in sexually explicit conduct on social media via webcams, as explained in more detail in paragraph 13.

12. Upon reviewing the site and the UCA recordings of the site, law enforcement officers were able to determine several ways the members targeted and coerced children into self-producing images or videos of sexually explicit conduct. S2 confirmed that different members of the site had different rolls and/or techniques they each “specialized” in for the group. Such rolls and/or techniques are as follows:

a) Chatter: a member who would actually chat with children in social media, usually in a text-chat format, but sometimes using voice calling or text messaging.

b) Looping, also known as (aka) lewping: a term used to describe the process of pretending to be a minor child by showing a previously recorded webcam video and playing it as if it were a live-feed video. Members used this method to “prove” to minor children that they were also children. The method was used sparingly due to the chance the real minor child may request the member to conduct a specific action (like waving).

c) Linking: a member whose role was to find potential minor children engaging in, or willing to engage in sexually explicit conduct, and linking the minor child’s direct social media account information to the group. Often, linking also involved finding the child on multiple social media accounts, so the minor child could be contacted in multiple locations. Having multiple locations to contact the children was important to the members in case the child were to get kicked off a site for engaging in sexually explicit conduct. Many social media account services monitor, or have a reporting system, where users can report inappropriate conduct of other users.

13. Members of the site also used their own terms to describe their actions, as well as the children they were targeting. Examples of that specialized language include:

- (a) Bating/Bate: Short for masturbating/masturbate
- (b) Win: a term used to describe a video where the member was able to get the minor child to engage in sexually explicit activity, such as “bating”
- (c) Catfish: a term used to describe pretending to be someone you are not on the internet by creating false profiles. Members of this group that participated in chatting and looping would create profiles pretending to be minor children of the same age of the minor children they were targeting
- (d) Maxclock or Max Clock: A plus and minus system to describe the age of the minor children they were targeting, based off the 12 hours of the clock. For example, Maxclock +2 would make the child 14 years old. Maxclock -2 would make the child 10 years old
- (e) IRL: In Real Life
- (f) Banned: when a user of a social media account is kicked off the service for engaging in some conduct that was against the site’s rules, often sexually explicit activity
- (g) Pedro: a pedophile
- (h) Upping/Upped: to upload to the Vault (explained further in paragraph 15e)

14. The site had links and special tools designed by members to assist in finding children to engage in sexually explicit conduct for the purpose of producing images and videos of that conduct.

15. Examples of the tools, as described by S2 included:

- (a) Snapscan: YouNow offers users the ability to create still frame images of live broadcasts called “snapshots.” The Snapscan tool was created by members of WEBSITE A to pull

all the snapshots off YouNow servers, allowing WEBSITE A users to more efficiently determine whether a particular YouNow user was underage and likely to engage in sexually explicit activity.

(b) Pedrosan: a tool that allows members of WEBSITE A to put in the YouNow user name of any other like-minded individual (“pedros”) and the tool will then show all the children that individual has “liked” or “fanned”² previously.

(c) Mass Viewer (YNMV): a tool that allows members of WEBSITE A to add multiple filters, to include Number of Cams, Tags, Stars, and Location. After adding the filters, the tool shows all live broadcasts on YouNow that fit those criteria.

(d) Requests: members were able to put in requests for other members to target a specific child and later share the recording of the broadcast with them.

(e) Vault: a listing of encrypted compressed files stored on www.mega.co.nz. All members of WEBSITE A used the same password to encrypt the files and would share the recording of the videos they were able to find and/or produce. All members of WEBSITE A that contributed to the site were given the password to the Vault files. Nearly all files in the Vault contained child pornography.

16. A few days after WEBSITE A was taken down by the RCMP, S2 put the same site back up on a different IP address (hereinafter referred to as WEBSITE B), hosted by a company based out of the United Kingdom.

17. S2 provided the FBI with root access to the site and the FBI shut down the site on April 23, 2015. Prior to the shutdown, a review of the site revealed various archive files and log files related to WEBSITE B, including but not limited to user login records and user chat records.

Identification of user “samisbae”

² “Fanning” is the ability to have one user click a button to show another user that they are a “fan” of their broadcasts. The more fans a user has, the more status is given to them within the site.


18. On March 11, 2015, pursuant to a mutual legal assistance treaty request, the RCMP provided federal law enforcement officers with an image of the server seized from the OVH server hosting WEBSITE A. A review of those log files revealed IP address records, chat message records and login records. Amongst the various records, within the log files from this server, your affiant located IP addresses 24.211.84.210 and 172.9.112.133 for user "samisbae." Chat messages associated with these records were indicative of enticing children. The user Samisbae engaged in chat messages that included linking to outside social media accounts of girls, discussion of what he was able to get the girls to do on those accounts, and using the above mentioned tools offered on the site.

19. User Samisbae was observed to have been logged into WEBSITE A on multiple occasions between November 13, 2014 and February 16, 2015. Samisbae was observed to have been an active chatter, linker and looper, as well as a member that uploaded child pornography to the Vault.

20. On November 22, 2014, user Samisbae was viewed on WEBSITE A, using IP address 172.9.112.133, communicating with other site members. Samisbae engaged in a conversation with another WEBSITE A user (hereinafter referred to as S20, S24, and S32) and had the following conversation:

S20: [name redacted, hereinafter V1] [REDACTED]
 Samisbae: yea im skypeing her
 Samisbae: she is gonna call me when she gets off yn³
 Samisbae: any request for tonights how ?
 Samisbae: show
 S32: spanking
 S24: [REDACTED]
 S32: plz
 Samisbae: ok
 Samisbae: yea last video has lots of [REDACTED]
 S32: oh and [REDACTED] :P
 Samisbae: gonna either get her to [REDACTED] or [REDACTED]

3 YN is short for YouNow.

21. In the above communication, Samisbae is discussing chatting with a child on Skype once she logs off of YouNow. Samisbae is asking the other members if they have any requests of what he can get the child to do on camera while he is chatting with her and says that he is going to get her to 

22. On November 24 and 25th, 2014, user Samisbae was observed to have been on WEBSITE A, using IP address 172.9.112.133, communicating with other site members. Samisbae engaged in a conversation with S4 and two other WEBSITE A users (hereinafter referred to as S4 and S22) and had the following conversation:

Samisbae: new [V1] up in the vault
[...]
S22: girl loop right?
Samisbae: nope
S22: *u use
Samisbae: just voice
S22: dayum
S4: welcome to the club, sam. :D
S22: do you sound like a 13yo then?
Samisbae: I pose as 16 and yes im soft spoken
[...]
S22: so much bush tho ./ how old is she again?
Samisbae: shes 13 not to much bush

23. In the above communication Samisbae tells the other members that he uploaded a video of a specific child into the Vault. One of the other members asks Samisbae what method he uses in chatting, inquiring if he is a looper, to which Samisbae replies that he did not use a loop video, but pretends to be a 16 year old and talks to her using a soft-spoken voice. Samisbae also acknowledges that he knows the girl's age to be 13 years old.

24. Federal law enforcement officers were able to download a video that was uploaded to the Vault on the same date and time as mentioned in the chat by Samisbae. The video contained the



name V1 and depicted a nude pubescent female who appeared under the age of 16,

[REDACTED]

25. On December 20, 2014, Samisbae was observed to have been on WEBSITE A, using IP address 172.9.112.133, communicating with other site members about V1. Samisbae engaged in a conversation with WEBSITE A member hereinafter referred to as S19, and other members, and had the following conversation:

Samisbae: there should be lots of stuff from her this week, schools out

Samisbae:

Samisbae:

S19: what if her parents found out?

S19: are you anonymous?

Samisbae: yep fake amazon account , prepaid credit card using cash (wearing glasses and a hoody when I bought it

S19: nice, does she know?

Samisbae: here mom wont be home and she will be home from school for break.

26. In the above communication, Samisbae is telling the other members that he went to extensive measures to hide his identity to purchase and send a [REDACTED], to a minor child. He also gave the minor child instructions on how to hide the items from her mother.

27. On February 10, 2015, Samisbae was observed to have been on WEBSITE A, using IP address 24.211.84.210 and stated the following:

[REDACTED]

Samisbae: let me check the vault , ive been dealing with irl stuff for about a week , but im settled into my new house now

Samisbae: yea moved from my parents to a 3bed 2 bath with roommates :D freedom

28. In the above communication, Samisbae is describing accessing the Vault. He also is describing his real-life living situation and move from his parent's home, to a secondary residence with two roommates.

29. S2 described Samisbae as a member of the site whose role was to be a chatter. S2 also thought Samisbae was a member of another similar site that was used to sexually exploit children. S2 believed Samisbae could have hands-on offenses with children.

30. IP address 172.9.112.133 is controlled by AT&T. Law enforcement officers sent an administrative subpoena to AT&T for information concerning the location of the digital device that used the IP addresses 172.9.112.133 on 2/3/2015 at 17:19:39 and between 11/13/2014 1:36:11AM and 1/28/2015 9:28:29 PM. Documents provided in response to that subpoena indicated that this IP address was statically assigned and subscribed to by [REDACTED] [REDACTED], Summerville, SC 29483 starting 2/25/2014 through at least 6/17/2015.

31. IP address 24.211.84.210 is controlled by Time Warner Cable. Law enforcement officers sent an administrative subpoena to Time Warner for information concerning the location of the digital device that used the IP addresses 24.211.84.210 on 2/7/2015 at 1:39:00PM EST, and on 2/15/2015 at 5:01:00 AM EST. Documents provided in response to that subpoena indicated that this IP address was assigned to Time Warner subscribed to by [REDACTED] at [REDACTED] [REDACTED], Summerville, SC 29483- [REDACTED]. Records indicate service began on 2/6/2015 through at least 5/1/2015.

32. Open source record checks identified a common resident of both addresses in Summerville to be Brandon Gressette. Gressette appears to have moved from the [REDACTED] [REDACTED] address,

his [REDACTED], residence, to the [REDACTED] address prior to March 2015. This information is consistent with chat communications described in paragraph 27 regarding Samisbae's living arrangements.

33. A South Carolina Department of Motor Vehicles check for Brandon Gressette identified the following information:

Name: Brandon D. Gressette

DOB: [REDACTED] 1984

Address: [REDACTED] Summerville, SC 29483

Vehicles:

(a) 2003 Nissan Altima, license tag #JUH587

(b) 2005 Chevrolet Cavalier, license tag #KNW345

34. A surveillance of the target residence conducted on October 8, 2015 revealed that a silver Nissan Altima, South Carolina tag #JUH587 that is registered to Brandon D. Gressette was parked in the driveway. A white male matching the description of Brandon Gressette exited the residence at 7:24am and then entered the Nissan Altima.

Execution of Federal Search Warrant at [REDACTED]

35. On October 15, 2015, a search warrant signed by United States Magistrate Judge Mary Gordon Baker was executed by FBI agents at [REDACTED], Summerville, SC 29483. The search warrant was to recover evidence in the above-described child pornography investigation of which one of the subjects of the case is a person using the user ID "samisbae".

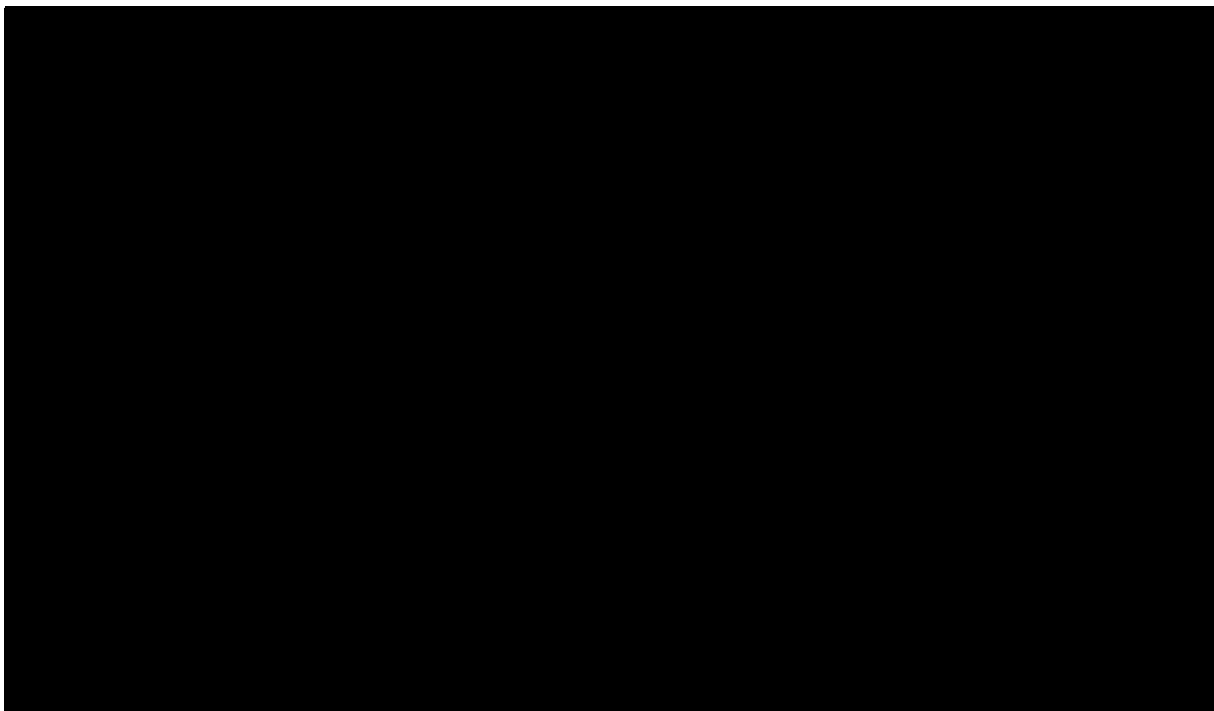
Interview of Brandon D. Gressette at Search Location

36. During the execution of the search warrant at [REDACTED], Summerville, SC 29483 on October 15, 2015, Brandon D. Gressette was found at the residence. Gressette was read

his Miranda Rights. Gressette then waived his Miranda Rights, signed an advice of rights Form FD-395, and agreed to be interviewed by FBI agents at the search location. Gressette also gave consent for the agents to access and control his email accounts and social media accounts. Gressette was interviewed by FBI agents. During the interview, Gressette provided the following information:

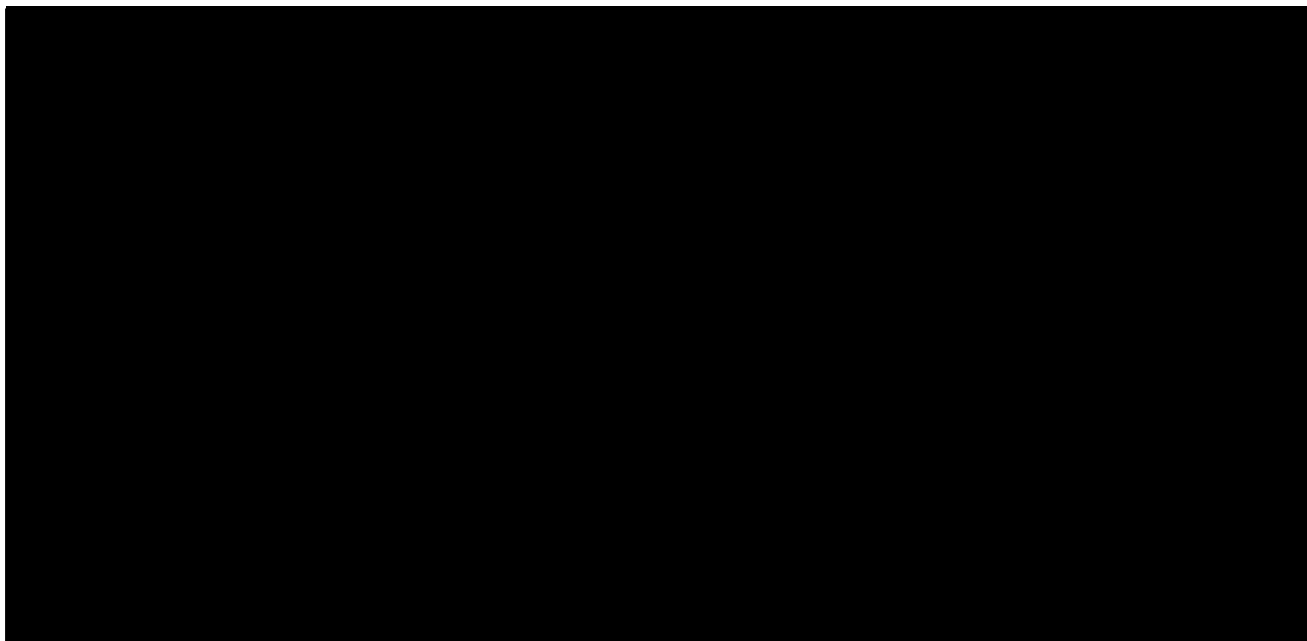
Gressette removed his hard drive from his computer, put it in the bathtub and turned the water on when he noticed law enforcement outside the residence. Gressette advised that he was told to do this by other child pornography users on the websites he visited. He did this hoping that it would erase all of the data on his hard drive that contained child pornography. Gressette admitted to using the names samisbae, sam, noah, and Brandon. Gressette would talk to young girls in chat rooms such as mylol, younow and on Skype⁵ with the intention of getting them to post nude photographs and videos. Some of Gressette's accounts are "samisbae" on mylol, "sam.r16" on Skype, "sam19bae" on Skype and "samr16" on younow. Gressette would also try to talk the young girls into performing certain sexual acts on the videos. Gressette would then record the videos and then post them in a place called the "Vault" in Website A where other people could then go to view the videos. During the summer of 2015, Gressette met a young girl named [REDACTED] in a chat room while he was posing as a young boy and began talking to her on a regular basis. Gressette would ask [REDACTED] to send him nude photos and videos, and he would ask her to perform sexual acts such as [REDACTED] [REDACTED] on Skype. And he requested that she [REDACTED] on Skype. [REDACTED]

⁵ Skype is a voice-over-Internet Protocol service and communication based social network that allows users to communicate with peers by voice, video, and instant messaging over the Internet. Through my training and experience I am aware of numerous applications that allow a user to capture the contents of their screen or video streams (such as Skype video sessions) and save those to a video file on the user's computer.

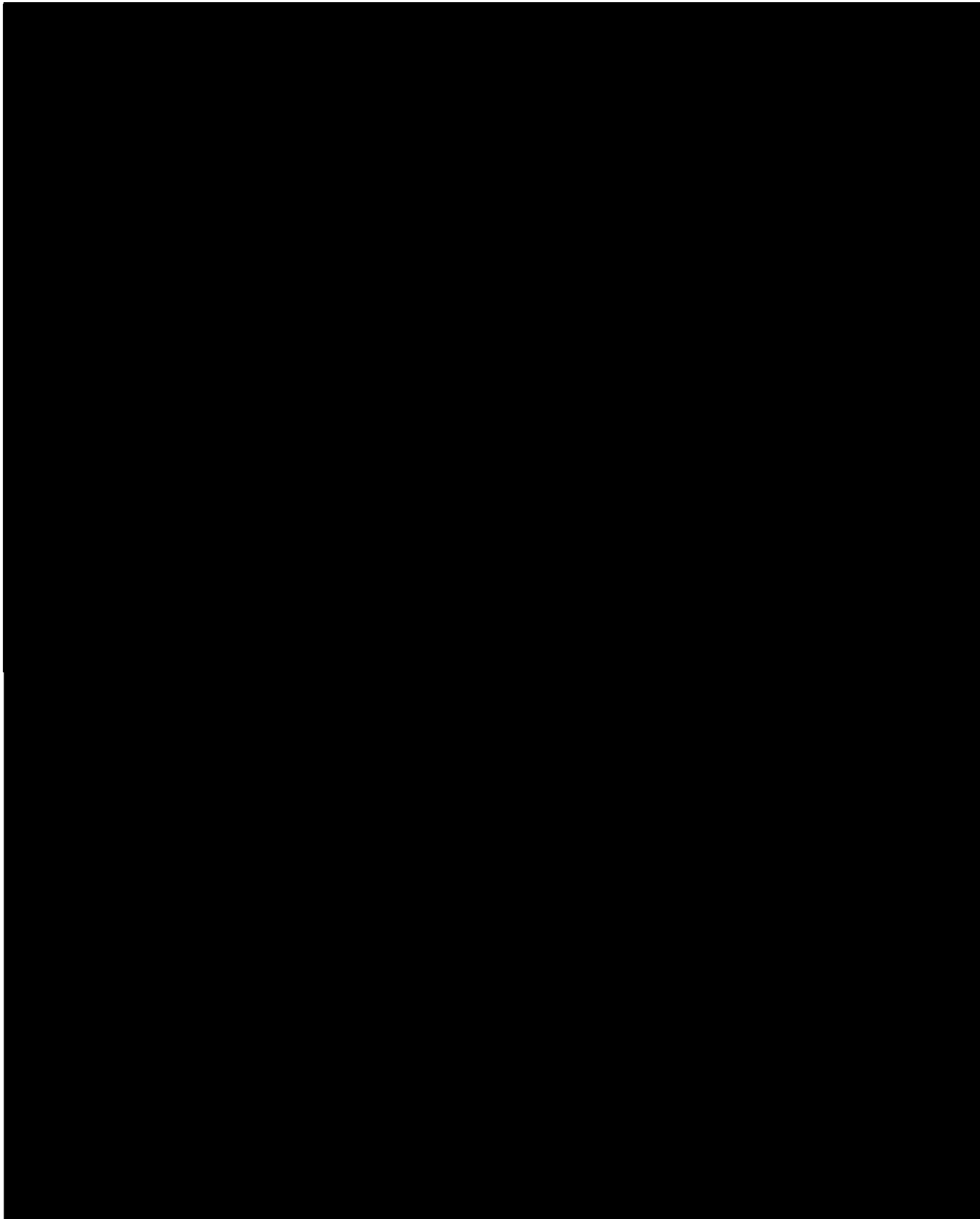


Review of Brandon D. Gressette's Computer Hard Drive and Cell Phone

37. During the execution of the search warrant at [REDACTED] [REDACTED] Summerville, SC 29483, several items were seized from Gressette, including his Toshiba hard drive, S/N Y2SVS9LPS that he had thrown in the bathtub. A Computer Analysis Response Team Agent (CART) was able to recover files on the hard drive. I reviewed several videos located on the hard drive that show minor females performing sexual acts, including the following the videos listed below:



A small, handwritten mark or signature is located in the bottom right corner of the page.



A small, handwritten mark or signature is located in the bottom right corner of the page, below the page number.

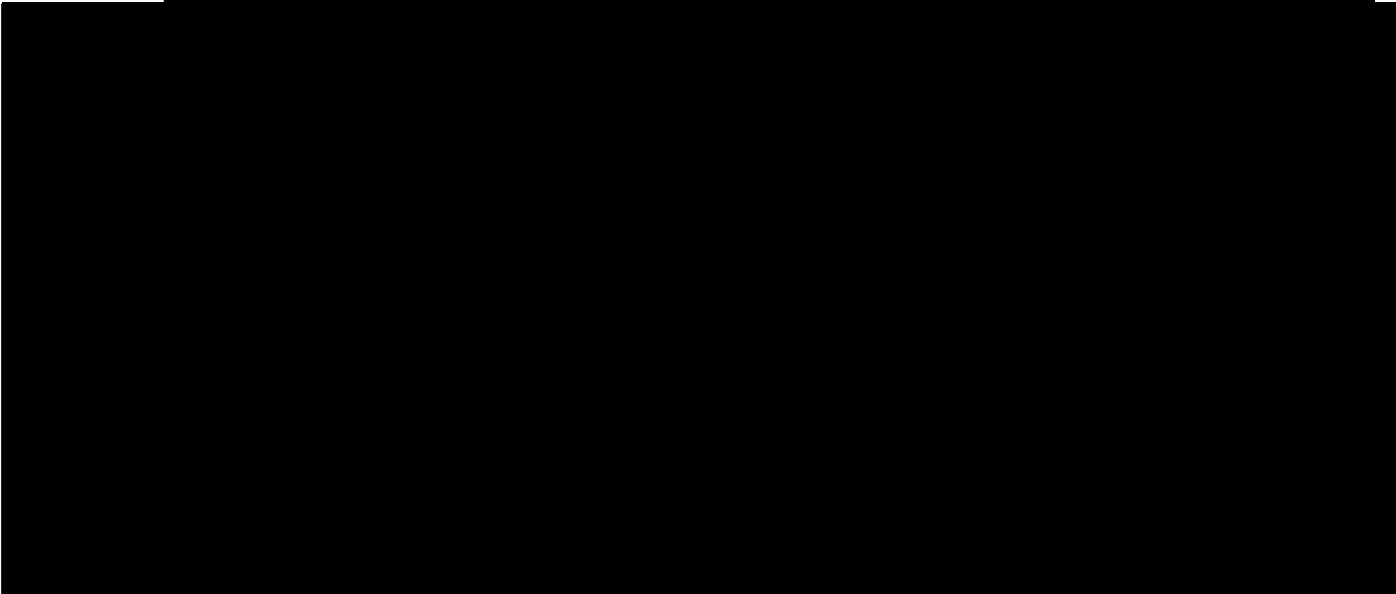
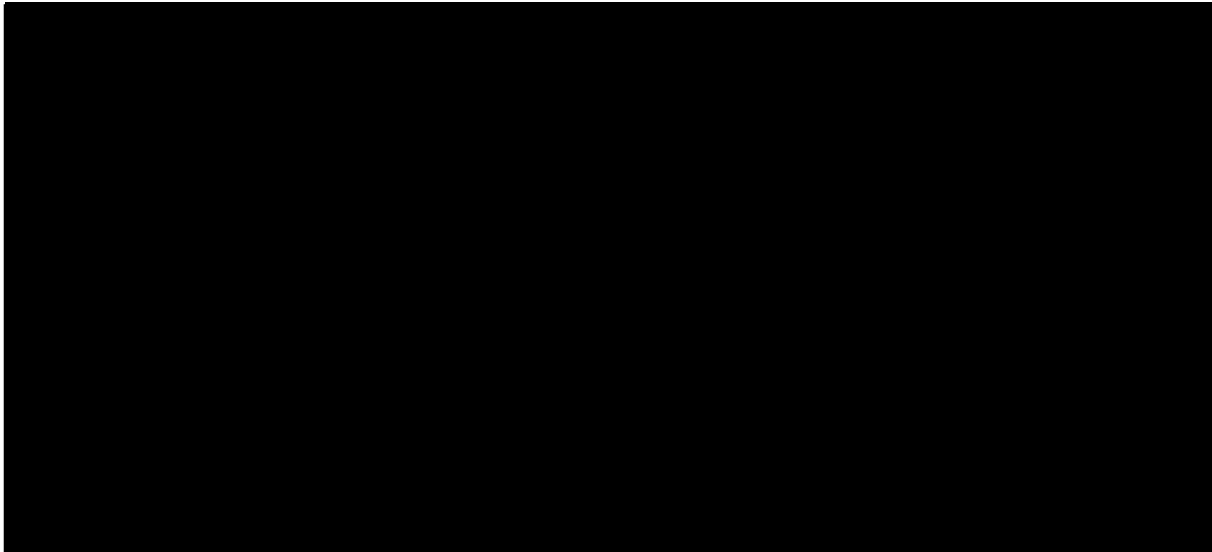


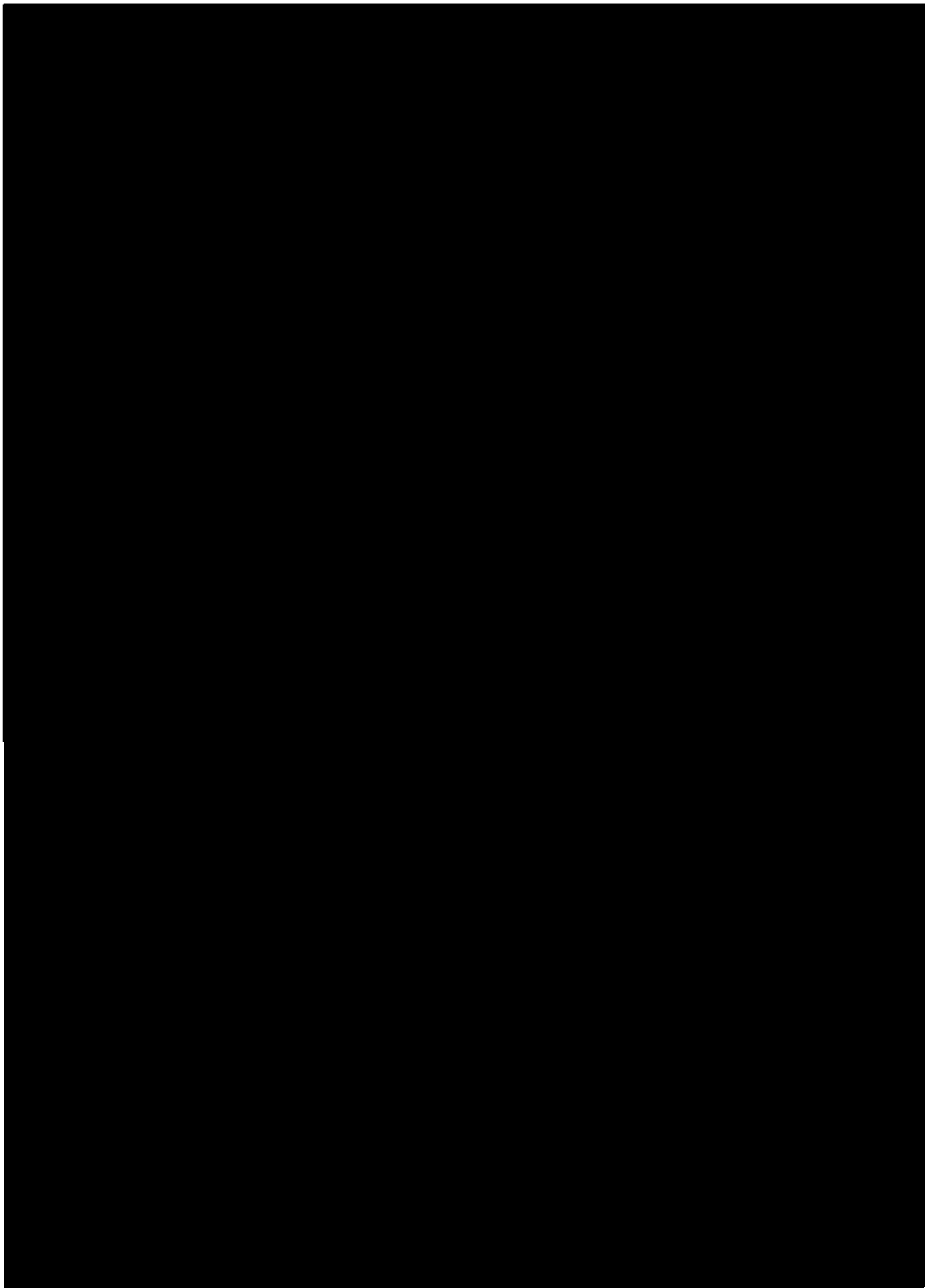
Interview of Minor Victim

38. On October 21, 2015, [REDACTED], 14 years old [REDACTED]

[REDACTED], SC [REDACTED], was interviewed at [REDACTED]

[REDACTED] SC and she provided the following information:





A small, handwritten mark or signature is located in the bottom right corner of the page, below the page number.

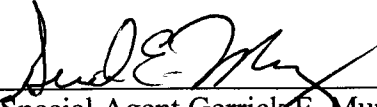


CONCLUSION

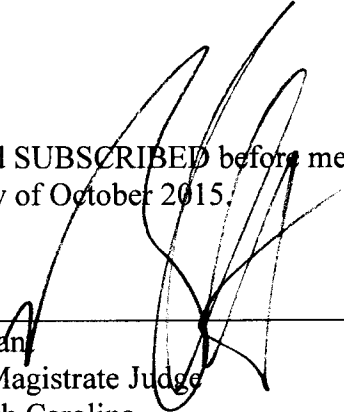
Therefore, based on the facts related above and my experience as a law enforcement officer, your Affiant believes that there is probable cause to believe that from in or around May 2015 through in or around July 2015, the defendant, Brandon D. Gressette, committed the offense of Use of an Interstate Commerce Facility to Coerce and Entice a Minor, in violation of Title 18, United States Code, Section 2422(b), in that he did the following: he communicated on the internet with a minor female for the purpose of meeting her to engage in sexually explicit conduct with her and then met with her at her residence and had sexual intercourse with her on more than one occasion, said sexual intercourse being a violation of South Carolina state law, namely, Criminal Sexual Conduct with a Minor, 2nd degree, in violation of S.C. Code of Laws, Section 16-3-655(B)(1); and he used the internet to instruct the same minor female to engage in sexually explicit conduct on a live internet video streaming service and he recorded those live video

A small, handwritten signature or mark is located in the bottom right corner of the page, consisting of a few cursive strokes.

streams, which is a violation of federal law, namely, Production of Child Pornography under Title 18, United States Code, Section 2251(a).


Special Agent Gerrick E. Munoz
Federal Bureau of Investigation

SWORN to and SUBSCRIBED before me
this 22 day of October 2015.


Bristow Marchant
United States Magistrate Judge
District of South Carolina