IN THE UNITED STATES DISTRICT COURT FOR THE
EASTERN DISTRICT OF VIRGINIA
Alexandria Division

UNITED STATES OF AMERICA	)	
	)	Criminal No. 1:13-CR-243
v.	)	
	)	The Honorable Anthony J. Trenga
SCOTT WAHL,	)	
	)	Trial: December 3, 2013
Defendant.	)	

GOVERNMENT'S PROPOSED FINDINGS OF FACT
AND CONCLUSIONS OF LAW

The United States, by and through Acting United States Attorney Dana J. Boente, and Assistant United States Attorneys Lindsay A. Kelly and Matthew Gardner, submit the following Proposed Findings of Fact and Conclusions of Law. The government anticipates that the evidence presented at trial will establish the following facts. Based on the applicable law, the government believes that the evidence will establish beyond a reasonable doubt that:

(1) On or about and between December 15, 2010, and September 6, 2012, in the Eastern District of Virginia, the Defendant, Scott Wahl, knowingly received child pornography, which was on a Fantom USB drive at Wahl's residence;

(2) On or about and between October 8, 2008, and September 6, 2012, in the Eastern District of Virginia, the Defendant, Scott Wahl, knowingly possessed child pornography, which was on a Buffalo USB drive and a Dell Inspiron laptop at Wahl's residence; and

(3) On or about and between September 6, 2012, and July 3, 2013, in the Eastern District of Virginia, the Defendant, Scott Wahl, knowingly altered and destroyed a Dell XPS laptop with the intent to impede, obstruct, and influence the Federal Bureau of Investigation ("FBI") investigation into his distribution, receipt, and possession of child pornography.

Proposed Findings of Fact

On three separate occasions in May, June, and July 2012, a specific computer using the Gnutella peer-to-peer network was observed by law enforcement sharing a large collection of suspected child pornography files over the Internet. (GX 7-9.) The computer was identifiable by its GUID, which is specific to a file-sharing program on a particular device, and was associated with two Internet Protocol ("IP") addresses during those three occasions. Both IP addresses were assigned by Verizon Communications, Inc. ("Verizon") to the Defendant, Scott Wahl, at the relevant times. In undercover investigative sessions on May 14, 2012, June 12, 2012, and July 20, 2012, FBI Special Agent ("Agent") Steve Miller connected to the computer via the Internet and downloaded several suspected child pornography files from the computer. Agent Miller submitted the files he had downloaded to the National Center for Missing and Exploited Children ("NCMEC") in Alexandria, Virginia, which confirmed that several of the files downloaded from the computer depicted sexual abuse against known and identified children. (Stipulation 2; *e.g.*, GX 36.)

On September 6, 2012, law enforcement executed a search warrant at the Wahl residence. Law enforcement previewed the computer equipment on-site for child pornography, and seized a number of items containing suspected or known child pornography, including the Dell Inspiron laptop, Buffalo USB drive, and Fantom USB drive – the latter two of which were seized from a locked safe that the Defendant had to open for law enforcement. Agent Miller submitted files from this computer equipment to NCMEC, which confirmed that several of the files on the Buffalo USB drive depicted sexual abuse against known and identified children. (Stipulation 2; GX 14, 15.)

Shortly after the agents arrived at the Wahl residence on September 6, 2012, Agent Miller also spoke with the Defendant in a recorded interview. The Defendant stated that he worked in the audio-video field, and the computer equipment at the Wahl residence was "geared towards that." When agents asked the Defendant to recount all computers in the house, the Defendant asked the agents to "explain what's going on." Agent Miller told the Defendant that law enforcement had downloaded child pornography from a computer using the IP address registered to the Defendant, and that the search warrant enabled agents to preview all computer equipment in the Defendant's home and seize any equipment containing child pornography. (GX 2.)

The Defendant stated to agents that his wireless internet access "was open for quite some time," and that he had only "closed it up . . . like within the last, I don't know, few days." (GX 2.) This statement was false, as Agent Miller had personally surveyed the wireless network at the Defendant's home on multiple occasions prior to the search, and always found it to be "locked down." When Agent Miller confronted the Defendant about this, the Defendant said "I dunno . . . there's a Netgear router that I don't think is password protected and I don't think I've ever had it password protected." (GX 2.)

The Defendant initially feigned ignorance of file-sharing programs, asking whether "iTunes" was a file-sharing program. After Agent Miller explained that he was referring to peer-to-peer programs like "the old Napster," the Defendant admitted being familiar with those programs, but denied having any of those programs on his computer equipment. (GX 2.)

Near the end of the interview, the Defendant angrily asked the agents, "When are you done? When are you out of my house?" Agent Miller explained that it would depend on the computer equipment in the house, and the time needed to preview that equipment. When asked, again, how many computers were in the house, the Defendant said, slowly and quietly, "I have

three computers . . . I think. This is a little overwhelming, with all of you in my house." The Defendant then added, more confidently, "So, preview away. I don't think there's anything on any of it." Though it was obviously at the forefront of his mind during this portion of the interview, the Defendant did not disclose to agents that his primary laptop computer, the Dell XPS, which he had left at a client's house in Florida, was *en route* back to Virginia. (GX 2.)

For roughly two weeks at the end of August 2012, the Defendant resided in Florida, next door to the home of his clients Deena and Barber Dick. The Defendant installs complex electronic systems, including audio/visual controls and surveillance systems, and was assisting the Dicks with projects at their new home. Deena Dick personally observed the Defendant using his laptop "all day, every day" as part of his work. At no time did Ms. Dick see the laptop malfunction, see the Defendant unscrew or otherwise work on the laptop, or hear the Defendant complain that the laptop was not working properly. When the Defendant left the Dicks' residence to return to Virginia, he mistakenly left the laptop behind. Ms. Dick agreed to ship the laptop back to him. Ms. Dick packaged the laptop herself, and – while she cannot recall exactly what packing materials she used – is confident that she wrapped the laptop and fit it securely inside the shipping box.

Shortly after law enforcement left the Wahl residence on September 6, 2012, Ms. Dick received a text message from the Defendant asking for the tracking number of the package containing the Dell XPS laptop. Ms. Dick advised that she had sent the package from her friend's dental office, for arrival in Virginia that afternoon, and could get the tracking number if needed. Two hours later, the Defendant asked for the tracking number. Ms. Dick called the dental office, then replied that her contact was at lunch. Over the next hour and forty minutes, the Defendant sent four (4) more texts asking if the contact had returned from lunch. Finally, at

2:54 p.m., Ms. Dick provided the tracking number and informed the Defendant that the laptop was on the truck for delivery. (GX 21.) According to UPS records, the Dell XPS laptop was delivered to the Defendant at almost that exact time, 2:51 p.m. (GX 20.) At 6:41 p.m., Ms. Dick asked the Defendant if he had received the laptop, and he replied "Yup thank you so much." The Defendant did not tell Ms. Dick that the laptop had arrived damaged, or had been packaged improperly. Indeed, the next correspondence between the Defendant and Ms. Dick was more than two (2) weeks later, when Ms. Dick asked the Defendant what time he planned to arrive at her house the next day. (GX 21.)

On July 3, 2013, the Defendant turned over what was left of the Dell XPS laptop to the FBI, and made an unsolicited statement to agents that he had attempted to fix the computer, but was unable to. In fact, sometime between his receipt of the laptop on September 6, 2012, and his provision of the laptop shell to FBI on July 3, 2013, the Defendant destroyed the Dell XPS laptop. The Defendant did not just remove and dispose of the computer's hard drive (where child pornography would most likely be recovered from). The defendant also removed and disposed of the Random Access Memory ("RAM"), which is the temporary memory utilized by a computer during operating sessions; disconnected the wiring for the wireless Local Access Network ("LAN") card, which enables the computer to connect to wireless networks; removed and disposed of the computer's power supply; and altered the wiring associated with the computer's power supply, which prevented law enforcement from restarting the computer using a new battery. (GX 1.) As a result, law enforcement was not only unable to recover the child pornography housed on the Dell XPS laptop, they were also unable to obtain information tying the Dell XPS laptop to the IP addresses assigned to the Wahl residence, or to the GUID observed sharing child pornography from those IP addresses.

Not surprisingly, none of the computer equipment seized from the Wahl residence matched the GUID that was seen sharing large numbers of child pornography files over the Gnutella network. Nonetheless, law enforcement recovered significant evidence of the Defendant's child pornography activities from that equipment.

First, on the Dell Inspiron laptop, which was seized from a common area of the Wahl residence (GX 3), the search term history indicates that a user of this computer sought out child pornography on the Internet, by typing in phrases associated with child pornography such as "Lola," "Lolita," and "13y." (GX 29.) The Internet Explorer activity history confirms that a user of this computer visited websites that contain child pornography, and viewed Temporary Internet File ("TIF") images of child pornography that are saved on the computer. (GX 30, 28.) Later on, the user switched to InPrivate browsing, which does not track full browsing information. Search terms used during InPrivate browsing sessions likewise confirm that the user was seeking out child pornography. (GX 33.) Child pornography files were also found in unallocated clusters of the Dell Inspiron laptop, which is where files go once they are "permanently" deleted by the user, but not yet overwritten by new files or programs.

The user seeking out child pornography on the Dell Inspiron laptop was undoubtedly the Defendant. For example, the Defendant is interested in the unsolved disappearance of Maura Murray, a young woman who had a car accident on a New Hampshire highway in February 2004, and was never seen again. The Defendant claims to have spent time at the accident site in New Hampshire on multiple occasions, recorded a video retracing the route of Ms. Murray's last drive, and posted the video to YouTube under the moniker "Human1666." (GX 44-46.) The Defendant also claims to have met with Ms. Murray's family members in Boston, and has had at least one long telephone call with one of those relatives. (GX 44, 47.)

Forensic analysis of activity on the Dell Inspiron laptop reveals that, during the early morning hours of February 9, 2012, the Defendant first viewed a news report of Ms. Murray's disappearance on YouTube, then viewed a photograph of Ms. Murray he had saved in a folder hierarchy named "Maura Murray/Pictures of Maura", then viewed a suspected adult pornography file. After viewing that file, the Defendant clicked on a "Needs to be sorted" folder on an external hard drive, then viewed a child pornography file titled as the "gangbang" of a 13-year-old child. Forensic analysis indicates that the child pornography was accessed through an external Western Digital My Passport hard drive. A Western Digital My Passport drive was seized from the Wahl residence, from the locked safe that also contained the Fantom USB and Buffalo USB drives (both of which primarily housed pornography, as explained below) (GX 4-6), but was damaged and could not be forensically accessed. After viewing the child pornography, the Defendant then did a Google search for blogs about Maura Murray, and visited the website http://mauramurray.blogspot.com. (GX 41.)

Second, a forensic review of the Buffalo USB drive, which was recovered from the locked safe in the Wahl home (GX 4-6), confirms that the Defendant uses this hard drive to backup files and photographs, and store pornography. The Defendant methodically categorized the pornography on the Buffalo USB drive through an extensive set of folders that accurately describe the folder's contents, such as "scat" and "shemale." (GX 26, 26A.) The active child pornography images and videos on this drive were recovered from two places: the root drive (meaning that the child pornography was not in a named folder), and the recycle bin (which is not deleted and can be easily accessed and/or restored by the user). (GX 23, 24.) Through forensic analysis, law enforcement was also able to reconstruct many child pornography videos

that had been "permanently" deleted, by utilizing a program that recombines snippets of the same file scattered on the hard drive as separate unallocated clusters. (GX 16.)

The child pornography files on the Buffalo USB drive, too, were undoubtedly possessed by the Defendant. The dated child pornography files on the root drive were all placed onto that drive between October 2007 and April 2009. In 2007, the Defendant's oldest child was only seven (7) years old, and his younger children were not yet born. Moreover, some child pornography images recovered from this device overlap with child pornography images being distributed from the GUID associated with the Wahl's IP addresses. Many images of child pornography are released as numbered "series" under a specific moniker. In June 2012, Agent Miller observed that GUID sharing images 8, 10, and 12 from the "Nadya" series, and images 9, 17, and 25 from the "Tori" series. (GX 8, 10.) Other numbered images from the "Nadya" and "Tori" series were on the Buffalo USB drive seized from the Wahl residence, confirming that the Defendant had a particular interest in those series, collected images from those series, and was the person responsible for sharing images from those series on the Gnutella network. (GX 37.)

Third, a forensic review of the Fantom USB drive, which was the third drive recovered from the locked safe at the Wahl residence (GX 4-6), confirms that the Defendant used that drive solely to store pornography downloaded from the Internet. Although no active program capable of accessing the Gnutella network was found on the electronic equipment seized from the Wahl residence, the Buffalo USB drive contained an executable file for Limewire – a peer-to-peer software program used to access the Gnutella network. Since an executable file cannot be run locally, the Defendant would have had to install the Limewire program on some device before he could access the Gnutella network. And the evidence is clear that he did so: the child pornography on the Fantom USB hard drive was located in a folder named "Downloads from

Limewire." Likewise, the Buffalo USB drive contained several "T-files," in which Limewire places a "T" before the file name to indicate that a file is in the process of being downloaded, with names indicative of child pornography. The Buffalo USB drive also contained folders named "Stills from Limewire" and "Downloads from Limewire."

Conclusions of Law

I. Receipt of Child Pornography

Count 1 of the Superseding Indictment charges that, on or about and between December 15, 2010, and September 6, 2012, in the Eastern District of Virginia, the Defendant, Scott Wahl, knowingly received child pornography. The government has specified that the child pornography charged in this count was on the Fantom USB drive seized from the locked safe in the Wahl residence.

To sustain its burden of proof for receipt of child pornography, the government must prove the following four (4) essential elements beyond a reasonable doubt:

(1) The defendant received computer files that contained child pornography;

(2) The defendant did so knowingly;

(3) The child pornography had been mailed or shipped or transported in interstate or foreign commerce by any means, including by computer; and

(4) At the time of such receipt, the defendant believed that the material constituted or contained child pornography.

See United States v. Yu, 411 Fed. Appx. 559, 563 n.6 (4th Cir. 2010).

First, two of the three videos identified as child pornography on the Fantom USB drive, and displayed at trial, clearly depict prepubescent children being sexually abused. (GX 17.) As the factfinder, the Court is entitled to conclude that these files depict actual children, without the aid of expert testimony. *See United States v. Salcido*, 506 F.3d 729, 733-34 (9th Cir. 2007) ("We

agree with every other circuit that has ruled on the issue that expert testimony is not required for the government to establish that the images depicted an actual minor."); *United States v. Irving*, 452 F.3d 110, 121–22 (2d Cir. 2006) (rejecting claim that the government must present extrinsic evidence to prove the reality of children in video images); *United States v. Deaton*, 328 F.3d 454, 455 (8th Cir. 2003) (per curiam) (affirming conviction based solely on child pornography images, and noting that Eighth Circuit upholds "a jury's conclusion that real children were depicted even where the images themselves were the only evidence the government presented on the subject").

Here, as in the above-cited cases, there is no question that the acts depicted – which include two prepubescent girls being penetrated digitally and with objects, in the vagina and anus, and engaging in oral sex – constitute child pornography. *See* 18 U.S.C. § 2256(8)(A) (defining "child pornography" to include depictions of "a minor engaging in sexually explicit conduct"); *id.* § 2256(2)(A) (defining "sexually explicit conduct" to include "actual or simulated (i) sexual intercourse, including genital-genital, oral-genital, anal-genital, or oral-anal, whether between persons of the same or opposite sex; . . . (iii) masturbation; . . . or (v) lascivious exhibition of the genitals or public area of any person."); *see, e.g.*, *United States v. Overton*, 573 F.3d 679, 687-88, (9th Cir. 2009) (affirming district court's determination, as factfinder during bench trial, that photographs of children depicted "sexually explicit conduct").

The forensic evidence also shows that the Defendant downloaded the child pornography videos on the Fantom USB drive between December 15, 2010, and September 6, 2012. The "last written" dates for the child pornography videos, which represent the last time that the video was produced or edited, fall within that date range. And the "created on" dates, which represent the dates those videos were saved on the Fantom USB drive, are within that date range as well. (GX 25.) Thus, because the child pornography videos on the Fantom USB drive were created in their

current form during the charged date range, and saved on the Fantom USB drive within the charged date range, the Defendant necessarily received those child pornography videos within the charged date range.

Second, the evidence will establish beyond a reasonable doubt that the Defendant knowingly received child pornography. The forensic evidence shows that the Defendant searched for child pornography using Internet Explorer on the Dell Inspiron laptop. (GX 40.) The browsing history of the Dell Inspiron laptop shows that the Defendant actively searched for child pornography by typing in well-known search terms for child pornography, such as "Lola," "Lolita," and "13 y." (GX 29, 40.) The browsing history and TIF images show that the Defendant used the Dell Inspiron laptop to visit websites that hosted child pornography, and to view images of child pornography. (GX 28, 40.) In short, the Defendant necessarily knew he was receiving child pornography files because he actively sought out child pornography on the Internet. *See, e.g., United States v. Pruitt*, 638 F.3d 763, 766-767 (11th Cir. 2011) ("Evidence that a person has sought out — searched for — child pornography on the internet and has a computer containing child-pornography images — whether in the hard drive, cache, or unallocated spaces — can count as circumstantial evidence that a person has 'knowingly receive[d]' child pornography."). The location of the Fantom USB drive, the Buffalo USB drive, and the Western Digital My Passport drive – in a locked safe that the Defendant had to open for law enforcement – is further evidence that the Defendant knew that the drives contained child pornography. The Defendant's lies to law enforcement about his familiarity with and use of file-sharing programs – despite evidence on numerous pieces of electronic equipment that he was an active Limewire user, and lies about the unprotected status of his wireless network – despite Agent Miller's observation

that the wireless network at the house was always "locked down," likewise show knowledge, and consciousness of guilt. (GX 2.)

Third, the child pornography was necessarily transported in interstate commerce because the Defendant sought it out via the Internet. *See, e.g., United States v. Ellyson*, 326 F.3d 522, 533 (4th Cir. 2003) ("[P]roof of transmission of pornography over the Internet . . . satisfies the interstate commerce element of the offense [of possession of child pornography]."); *United States v. White*, 2 Fed. Appx. 295, 298 (4th Cir. 2001) ("Transmission of [child pornography] by means of the Internet is tantamount to moving [child pornography] across state lines and thus constitutes transportation in interstate commerce."). *See also United States v. Winkler*, 639 F.3d 692, 700-01 (5th Cir. 2011) (finding interstate commerce nexus satisfied where child pornography videos were obtained from a website); *United States v. MacEwan*, 445 F.3d 237 (3rd Cir. 2006) ("[W]e conclude that because of the very interstate nature of the Internet, once a user submits a connection request to a website server or an image is transmitted from the website server back to the user, the data has traveled in interstate commerce.").

The investigation in this case began when the FBI determined that two IP addresses registered to the Defendant were sharing large numbers of child pornography files on the Gnutella network between May and July 2012. (GX 7-9.) The forensic evidence confirmed that the Defendant used Limewire to download and collect child pornography. On both the Buffalo USB and Fantom USB drives, the Defendant created folders called "Downloads from Limewire." (GX 26A, 27A.) Indeed, the child pornography videos on the Fantom USB drive were stored in the "Downloads from Limewire" folder. (GX 25.) The evidence will show that the Defendant methodically and accurately named and sorted folders on his hard drives. Thus, the presence of

child pornography videos in a "Limewire" folder on the Fantom USB drive confirms the means by which the Defendant obtained the files.

Other forensic evidence confirms that the Defendant's use of Limewire to collect child pornography. For example, a Limewire executable file and Limewire "T" files (indicating downloads in process) were located on the Buffalo USB drive. The "T" files had names that were consistent with child pornography. In addition, different numbered child pornography images from the "Nadya" and "Tori" series were found on the Buffalo USB drive and available for sharing by the GUID associated with the Defendant's residence. (GX 10, 37.) This confirms that the Defendant, and no one else, was the person collecting and sharing "Nadya" and "Tori" images over the Gnutella network.

Fourth, the evidence establishing that the Defendant sought out child pornography on the Internet and moved child pornography files on the Fantom USB drive from their download locations to a "Limewire" folder—especially when one considers the video titles and content—proves beyond a reasonable doubt that, at the time of receipt, the Defendant knew that the files found on the Fantom USB drive were child pornography.

II. Possession of Child Pornography

Count 2 of the Superseding Indictment charges that, on or about and between October 8, 2008, and September 6, 2012, in the Eastern District of Virginia, the Defendant, Scott Wahl, knowingly possessed child pornography. The government has specified that the child pornography charged in this count was on the Buffalo USB drive seized from the locked safe in the Wahl residence and the Dell Inspiron laptop seized from a public area of the Wahl residence.

To sustain its burden of proof on this charge, the government must prove the following three (3) essential elements beyond a reasonable doubt:

(1) The defendant possessed computer files that contained child pornography;

(2) The defendant did so knowingly; and

(3) The child pornography had been mailed or shipped or transported in interstate or foreign commerce by any means, including by computer.

See 18 U.S.C. § 2252(a)(4)(B); *United States v. Donton*, 266 Fed. Appx. 222, 224 (3rd Cir. 2008).

The Defendant has stipulated to elements 1 and 3 for this charge. Stipulation 2 provides:

> The United States and the Defendant, SCOTT WAHL, stipulate that six images and five videos, including Government Exhibit 36, and the images and videos shown at trial from Government Exhibits 14 and 15, were identified by the National Center for Missing and Exploited Children ("NCMEC") as depicting actual children under 18 years of age engaged in sexually explicit conduct that occurred outside the state of Virginia.

Government Exhibits 14 and 15 contain the child pornography from the Buffalo USB drive – one of the two pieces of equipment relating to the possession charge. Because those "known" child victims were abused outside the state of Virginia, the depictions of abuse were necessarily "mailed or shipped or transported in interstate or foreign commerce" to the Defendant in Virginia.[1]

Thus, the only disputed issue on Count 2 is whether the Defendant knowingly possessed child pornography. For all of the reasons articulated in Section I above – including the Defendant's Internet searches using common child pornography search terms, visits to websites housing child pornography, possession of child pornography in active and deleted spaces on multiple pieces of electronic equipment, and lies to law enforcement about his familiarity with and use of file-sharing programs – the evidence establishes the Defendant's knowledge beyond a reasonable doubt. This analysis applies equally to the child pornography files stored in active

[1] For the child pornography images on the Dell Inspiron laptop, which did not contain NCMEC-confirmed victims, the Court as factfinder can engage in the analysis outlined in Part I to conclude that the images depicted actual minors engaged in sexually explicit conduct. *See, e.g.*, *Overton*, 573 F.3d at 687-88; *Deaton*, 328 F.3d at 455.

space, as TIFs, and in unallocated clusters, as the Defendant at one time exercised dominion and control over all child pornography recovered from his computer equipment. *See, e.g., United States v. Tucker*, 305 F.3d 1193, 1204-05 (10th Cir. 2002) (affirming possession conviction where defendant "merely viewed [child pornography] on his Web browser," and then deleted images from cache file, because defendant understood that images viewed on websites were initially saved on computer).

III. Obstruction of Justice

Count 3 of the Superseding Indictment charges that, on or about and between September 6, 2012, and July 3, 2013, in the Eastern District of Virginia, the Defendant, Scott Wahl, knowingly altered and destroyed a Dell XPS laptop computer with the intent to impede, obstruct, and influence the FBI investigation into his distribution, receipt, and possession of child pornography.

To sustain its burden of proof on this charge, the government must prove the following three (3) essential elements beyond a reasonable doubt:

(1) The defendant altered, destroyed, mutilated, concealed, covered up, falsified, or made a false entry in any record, document, or tangible object;

(2) The defendant did so knowingly; and

(3) The defendant intended to impede, obstruct, or influence the investigation or proper administration of any matter within the jurisdiction of any department or agency of the United States or in relation to or contemplation of any such matter or case.

United States v. Powell, 680 F.3d 350, 356 (4th Cir. 2012).

First, the evidence will establish beyond a reasonable doubt that the defendant altered and destroyed the Dell XPS laptop computer. Ms. Dick will testify that the laptop was fully assembled when she packaged and shipped it via UPS from Florida to Virginia. Upon receiving

the Dell XPS laptop (without complaint to Ms. Dick), the Defendant removed and disposed of the computer's hard drive, RAM, and power supply. The Defendant further disconnected the wiring connected to the LAN card, and altered the wiring associated with the computer's power supply. (GX 1.) These actions are inconsistent with attempts to repair a malfunctioning machine, and are instead evidence of a (successful) attempt to alter and destroy every piece of the laptop that contained relevant data or identifying information, and to prevent such information from being recovered through parts replacement. As a result of the Defendant's actions, law enforcement was not only unable to recover the child pornography housed on the Dell XPS laptop, they were also unable to obtain information tying the Dell XPS laptop to the IP addresses assigned to the Wahl residence, or to the GUID observed sharing child pornography from those IP addresses.

Second, the evidence proved beyond a reasonable doubt that the defendant altered and destroyed the Dell XPS laptop knowingly. The Defendant himself stated to FBI that he attempted to fix the machine, but was unable to – therefore admitting that he, and not someone else, altered the computer, and did so knowingly and voluntarily.

Third, the evidence showed beyond a reasonable doubt that the Defendant intended to impede and obstruct the FBI investigation into his receipt, distribution, and possession of child pornography. Agent Miller had explained to the Defendant that law enforcement had observed child pornography being shared on a file-sharing network, and had downloaded child pornography, from a computer associated with the Wahl residence. Agent Miller further explained to the Defendant that agents were authorized to search and seize computer equipment in the Wahl residence containing child pornography. The Defendant knew that the Dell XPS laptop – the laptop he used for most of his child pornography activity, which bore the GUID

observed by Agent Miller online – was not in Virginia, and was *en route* back to Virginia from Florida. The Defendant did not disclose the existence of the Dell XPS laptop to law enforcement.

Rather, shortly after the agents left the Wahl residence, the Defendant began his urgent attempts to locate the Dell XPS laptop. The laptop was delivered mere hours after law enforcement left the Wahl residence, and the Defendant confirmed receipt of the Dell XPS laptop to Ms. Dick that evening – without any indication that the laptop had been damaged or packed improperly. The Defendant, who installs and monitors elaborate electronics systems for a living, knew exactly which components of the laptop contained information that would be relevant to law enforcement's investigation. The Defendant methodically disassembled the computer, removed, and disposed of all items of interest to FBI: the hard drive, which contained files, programs, GUID, and information about Internet searches and browsing; and the RAM, which also contained data and activity information for the device. The Defendant did not stop there, however: he went on to alter the wiring connected to the power supply (and dispose of the existing power supply) to prevent law enforcement from attempting to obtain information from the machine by installing new RAM, a new hard drive, and a new power supply.

Conclusion

Based on the applicable law and the facts established by the evidence, the government will ask this Court to find the Defendant guilty of the three offenses charged in the Superseding Indictment.

Respectfully submitted,

Dana J. Boente
Acting United States Attorney

By: /s/

Lindsay A. Kelly
Matthew Gardner
Assistant United States Attorneys
Eastern District of Virginia
2100 Jamieson Avenue
Alexandria, VA 22314
Phone: (703) 299-3700
Fax: (703) 299-3981
Email: lindsay.a.kelly@usdoj.gov
Email: matthew.gardner@usdoj.gov

Date: November 27, 2013

CERTIFICATE OF SERVICE

I hereby certify that on this 27th day of November, 2013, I electronically filed the foregoing with the Clerk of Court using the CM/ECF system, which will send a notification of that electronic filling (NEF) to:

Mark Petrovich, Esq.
Petrovich and Walsh, P.L.C.
10605 Judicial Drive, Suite A-5
Fairfax, Virginia 22030
mp@pw-lawfirm.com

James Freeman
Kearney, Freeman, Fogarty & Joshi, PLLC
4085 Chain Bridge Road, Suite 500
Fairfax, Virginia 22030
Fax: 703-691-8380
Email: jfreeman@kffjlaw.com

Respectfully submitted,

Dana J. Boente
Acting United States Attorney

By: /s/
Lindsay Kelly
Assistant United States Attorney
Eastern District of Virginia
2100 Jamieson Avenue
Alexandria, VA 22314
Phone: (703) 299-3700
Fax: (703) 299-3981
Email: lindsay.a.kelly@usdoj.gov