IN THE UNITED STATES COURT OF APPEALS
FOR THE ARMED FORCES

U N I T E D S T A T E S,	)	FINAL BRIEF ON BEHALF OF
	)	APPELLANT
	)	
v.	)	
	)	Crim. App. Dkt. No. 20090446
Specialist (E-4)	)	
MATTHEW J. McCLAIN,	)	
United States Army,	)	USCA Dkt. No. 12-0099/AR
Appellant	)	

MATTHEW T. GRADY
Captain, Judge Advocate
Appellate Defense Counsel
Defense Appellate Division
U.S. Army Legal Services Agency
9275 Gunston Road
Fort Belvoir, Virginia 22060
(703) 693-0737
U.S.C.A.A.F. Bar No. 35092

RICHARD E. GORINI
Major, Judge Advocate
Branch Chief, Defense Appellate Division
U.S.C.A.A.F. Bar No. 35189

IMOGENE M. JAMISON
Lieutenant Colonel, Judge Advocate
Deputy Chief, Defense Appellate Division
U.S.C.A.A.F. Bar No. 32153

PATRICIA A. HAM
Colonel, Judge Advocate
Chief, Defense Appellate Division
U.S.C.A.A.F. Bar No. 31186

INDEX OF FINAL BRIEF ON BEHALF OF APPELLANT

TABLE OF CASES, STATUTES, AND OTHER AUTHORITIES

State Courts

Statutes

Uniform Code of Military Justice

Manual for Courts-Martial, United States, 2005 Edition

Other

Regulations and Publications

IN THE UNITED STATES COURT OF APPEALS
FOR THE ARMED FORCES

UNITED STATES, Appellee	) FINAL BRIEF ON BEHALF OF APPELLANT
v.	) Crim. App. Dkt. No. 20090446
	) USCA Dkt. No. 12-0099/AR
Specialist (E-4) **Matthew J. McClain,** United States Army Appellant	)

TO THE JUDGES OF THE UNITED STATES COURT OF APPEALS
FOR THE ARMED FORCES:

Introduction and Summary of Argument

Military Rule of Evidence 701 provides that "witness' testimony in the form of opinions or inferences is limited to those opinions or inferences that are . . . (c) not based in scientific, technical, or other specialized knowledge within the scope of Rule 702." The military judge abused his discretion when he allowed Special Agent ["SA"] Sean Devinny to testify as a lay witness under M.R.E. 701 concerning matters that were scientific, technical, and specialized in nature. SA Devinny's testimony on SHA1 values[1] served as the sole link between the video files found in appellant's Internet Protocol ["IP"]

---

[1] SA Devinny testified that a SHA1 value is a "32 alphanumeric string that is a digital signature of any file that you apply the algorithm to." (JA. at 90.)

address[2] and the allegedly matching video files SA Devinny found available on the gnutella network.[3] Even assuming the military judge did not abuse his discretion in admitting SA Devinny's expert testimony, the evidence remains legally insufficient to support appellant's conviction for knowingly possessing child pornography. Despite his training and experience, SA Devinny could not personally download or view any of the video files the government alleged SPC Matthew McClain possessed even though he attempted to do so. (JA. at 247.)

Issue Presented

WHETHER THE EVIDENCE IS LEGALLY SUFFICIENT TO SUPPORT APPELLANT'S CONVICTION OF POSSESSING CHILD PORNOGRAPHY.

Statement of Statutory Jurisdiction

The Army Court of Criminal Appeals ["Army Court"] had jurisdiction over this matter pursuant to Article 66, Uniform Code of Military Justice ["UCMJ"]; 10 U.S.C. § 866 (2008). This Honorable Court has jurisdiction over this matter under Article 67(a)(3), UCMJ; 10 U.S.C. § 867(a)(3) (2008).

---

[2] An IP address "is a numerical label assigned to each device (e.g., computer, printer) participating in a computer network" and "serves two principal functions: host or network interface identification and location addressing." http://en.wikipedia.org/wiki/IP_address (last visited Oct. 19, 2011).

[3] Gnutella network refers to a decentralized computer network that operates over the internet. It essentially links other users together for individual, private file sharing. (JA. at 29.)

Statement of the Case

On May 18-19, 2009, a military judge sitting as a general court-martial tried appellant. Contrary to his pleas, the military judge convicted appellant of possessing child pornography and distributing visual depictions of minors engaging in sexually explicit conduct to internet users, in violation of clause two of Article 134, UCMJ; 10 U.S.C. § 934 (2008).[4] The military judge sentenced appellant to reduction to Private (E-1), confinement for fourteen months, and a bad-conduct discharge. (JA. at 355.) The convening authority reduced appellant's period of confinement to thirteen months, but otherwise approved the adjudged sentence. (JA. at 375.)

The Army Court affirmed the finding of guilty as to Specification 1 of the Charge (possessing child pornography) and the sentence on August 19, 2011. (JA. at 1-6.) However, the Army Court set aside Specification 2 of the Charge (distributing visual depictions of children engaging in sexually explicit conduct) and dismissed it because it found the evidence legally and factually insufficient. *United States v. McClain*, 2011 WL 4371302, slip op. 3-5 (Army Ct. Crim. App. Aug. 21, 2011) (JA. at 3-5.) Appellant petitioned this Court for review on October 13, 2011, and moved for leave to file the supplement separately

---

[4] Appellant was found not guilty of conduct "prejudicial to good order and discipline" regarding both offenses. (JA. at 353-54.)

from the petition. This Court granted that motion on October 14, 2011, and ordered appellant to submit the supplement by November 2, 2011.

Appellant filed the supplement to his petition with this Court on October 24, 2011, and this Court granted appellant's petition for review on December 20, 2011. This Court ordered briefs filed under Rule 25 of this Court's rules and procedures. On January 10, 2012, appellant moved for an extension of time to file his final brief. This Court granted that motion on January 10, 2012, and ordered appellant to file his final brief by January 27, 2012.

Statement of Facts

In March, 2008, SA Devinny of the Naval Criminal Investigative Services conducted an undercover operation targeting Navy personnel who may have been distributing child pornography over the Internet. (JA. at 28.) As part of his investigation, SA Devinny found a total of fourteen video files from the Limewire[5] share folder of the IP address 72.130.203.222. (JA. at 247.) This IP address was registered to appellant. (JA at 362.) SA Devinny only downloaded three files from this IP address, despite attempting to download more. (JA. at 247-49.)

---

[5] Limewire is part of the gnutella network, which is "a network that operates over the internet and it is a network that links computers to each other for file sharing." (JA. at 29.)

First, SA Devinny downloaded a video file titled "Fucking my little sis in the ass (illegal preteen)." (JA. at 257.) SA Devinny "believed" that this file constituted adult pornography. (JA. at 250.) Appellant was not charged with possessing this video and a review of the video indicated that the woman shown in this file appears to be over the age of eighteen. (JA. at 376.)

Second, SA Devinny downloaded a video file titled "Collection 1-rape (illegal preteen)." (JA. at 257.) SA Devinny agreed that this file could have contained adult pornography. (JA. at 250.) Appellant was not charged with possessing this video and a review of this short, low-quality one minute video indicated that the sex organs were not readily apparent and ages are difficult to determine. (JA at 376.) SA Devinny exclusively downloaded these two video files from the IP address registered to appellant. (JA. at 257.)

Third, SA Devinny downloaded "over 90 percent" of a video file titled "_little girls mix (lolitas-preteens-reelkiddymov-r@ygold-hussyfans-underage-girls-children-pedofilia-pthc-ptsc-xxx-sexy).mpeg" from appellant's IP address. (JA. at 232, 245, and 367.) SA Devinny downloaded the file from users in addition to appellant because this procedure helps increase the download speed of a file. (JA. at 79.) SA Devinny attempted to exclusively download this video file from appellant's IP address

using "isolation" procedures, but he was unable to do so. (JA. at 116-18.) Appellant was not charged with possessing this video. (JA. at 7-9.) SA Devinny never personally downloaded or viewed any of the remaining eleven video files in the share folder of appellant's IP address, including all four videos the government charged appellant with possessing. (JA. at 249.)

Appellant was subsequently charged with possessing four video files containing child pornography in violation of 18 U.S.C. §2252A. (JA. at 7.) Prior to trial, appellant asked the military judge "to make appropriate evidentiary rulings regarding the scope and nature of testimony permitted to be elicited from government witnesses." (JA at 12-15.) Specifically, appellant moved to preclude SA Devinny "from rendering any opinion as to any files, images, or videos that he downloaded on 11 March 2008." (JA at 12.) Appellant felt that SA Devinny did not qualify as an expert witness, and that he would offer opinions "generally prohibited under [M.R.E.] 701." (JA at 14.) The government responded and stated that they had no intention of offering SA Devinny as an expert. (JA at 16-17.) Instead, the government argued that SA Devinny should be allowed to give testimony "concerning the Limewire network, peer-to-peer downloading, general computer knowledge, and the methods of his investigation." (JA at 17.)

During the Article 39(a), UCMJ, session on appellant's motion, appellant clarified his position as to why he filed a motion in limine to limit expert testimony, stating that he did so:

> [T]o limit opinion testimony, sir, because the defense didn't want to be in a position where if we were in trial, and having to stand up and object to what we believe was improper lay opinion testimony, basically the witness going into an area that's only reserved for experts . . . [t]hat's why we filed the motion, sir, so that we could hash this out prior to being in the case-in-chief, the merits portion.

(JA. at 168.) The military judge then engaged in the following colloquy with trial counsel:

> MJ: Government, do you intend to offer - I think we are left with Devinny - to testify about any area beyond mere lay testimony?
>
> TC: I intend to offer him on SHA1 values and what they are.
>
> MJ: Is that lay opinion testimony?
>
> TC: I believe it could be for Agent Devinny based on his personal knowledge and experience.
>
> MJ: Is it not based on scientific, technical or other specialized knowledge within the scope of 702? Referring under 701(c).
>
> TC: Yes, sir.
>
> MJ: Because if it is not, Counsel, then couldn't a doctor just come in and lay testify about performing surgery? Couldn't a DNA specialist, because it's within their

common knowledge, come in and testify about their lay opinion about DNA evidence?

TC: Yes, sir.

MJ: So do you, Trial Counsel, intend to offer testimony from Agent Devinny under M.R.E. 702?

TC: No.

> MJ: Okay. So your response to the defense motion in limine is I've got no expert testimony.
>
> TC: Yes, Your Honor.

(JA. at 168-69.)

SA Devinny testified during this Article 39(a), UCMJ, session that SHA1 values are used in peer-to-peer software applications to distinguish files from one another. (JA. at 65.) In fact, SA Devinny testified that SHA1 values were "developed originally by the NSA in conjunction with the National Institute of Standards and Technology to develop a file encryption method to transfer financial information." (JA. at 91.) SA Devinny continued:

> So if I transfer a file to you over the internet, I can calculate the SHA1 value before I sent it and then when you get it, you can calculate the SHA1 value and we can ensure then that the files is [sic] in its same form from when it is sent from me to when you receive it by comparing our SHA1 values. So it was established for that reason and its accuracy has been computed mathematically that the chance of two different files sharing the same SHA1 value is calculated as 1 in 9.2 quintillion and

> that's trillion, quadrillion, quintillion. So it's said to be many times more accurate than DNA - then a result that you will get in DNA and it is the fingerprint or digital signature of a file, an electronic file.

(JA. at 91.) SA Devinny clarified that if one changed the pixel on a movie, the SHA1 value for the file would change. (JA. at 91.)

SA Devinny testified at trial that he could view a file in a share folder if two conditions were met: (1) the other user was online with Limewire actively running and (2) the complete file was located in the other user's Limewire share folder. (JA. at 248.) Even though the four suspected contraband videos seemed to be located in the Limewire share folder of appellant's IP address, for some unknown reason, SA Devinny could not personally download or view them. (JA. at 247.) Nonetheless, SA Devinny opined that the four charged video files were located in appellant's share folder because he later found files with matching SHA1 values elsewhere in the gnutella network. (JA. at 214.)

Specifically, SA Devinny testified that he observed the *titles* of the charged video files pertaining to Specification 1 of the Charge in the share folder registered to appellant's IP address. (JA. at 209-10.) While SA Devinny was unable to personally view or download the four charged video files directly from appellant's IP address (JA. at 221), he testified

that he obtained copies of the files from the gnutella network because he "observed identical files as identified by the SHA1 values." (JA. at 211.) Appellant objected to this testimony at trial. (JA. at 211-12.) The military judge and the defense counsel then had the following colloquy:

> MJ: But what I think [SA Devinny's] saying is, 'I went out and got the - I did the same search terms, I pulled them down, and I thought they were the same item, because they had the same SHA number.' Is that not something within the collective ken of society?
>
> DC: That could be within the -
>
> MJ: Within a lay opinion.

(JA. at 213.) SA Devinny then re-stated that he "downloaded files with the identical SHA1 value." (JA. at 214.) Trial counsel reiterated this point again by asking SA Devinny if these files had the same SHA1 value, to which SA Devinny agreed. (JA. at 214.)

SA Devinny later testified that he re-named the video files on Pros. Ex. 1 according to their SHA1 values "so it'd be easier for [him to] determine which files were which." (JA. at 217.) Trial counsel and SA Devinny then discussed the charged videos by referring to their respective SHA1 values over the next 23 pages on the record. (JA. at 217-40.) During this span, the parties referred to the term SHA1 values approximately twenty-nine times. (JA. at 217-40.) In rebuttal during findings

argument, trial counsel argued that SA Devinny obtained the same files that were on the share folder of appellant's IP address because he found files of the "same size, same long name, [and] same SHA1 value." (JA. at 352.)

The other facts necessary for the disposition of the assigned errors are set forth in the argument below.

Issue Presented and Argument

WHETHER THE EVIDENCE IS LEGALLY SUFFICIENT TO SUPPORT APPELLANT'S CONVICTION OF POSSESSING CHILD PORNOGRAPHY.

1. Standard of Review

The standard of review for legal sufficiency is whether, when viewed in a light most favorable to the government, a rational fact-finder could have found all essential elements of the offense beyond a reasonable doubt. *United States v. Turner*, 25 M.J. 324, 325 (C.M.A. 1987) (citing *Jackson v. Virginia*, 443 U.S. 307 (1979)). When applying the test for legal sufficiency, this Court is "bound to draw every reasonable inference from the record in favor of the prosecution." *United States v. McGinty*, 38 M.J. 131, 132 (C.M.A. 1993) (*quoting United States v. Blocker*, 32 M.J. 281, 284 (C.M.A. 1991)). This Court reviews questions of legal sufficiency de novo as a question of law. *United States v. Hays*, 62 M.J. 158, 162 (C.A.A.F. 2005).

2. Military Rule of Evidence 701 Governs Lay Testimony at Courts-Martial

"Like other evidentiary rulings, a military judge's application of [M.R.E.] 701 is reviewed for an abuse of discretion." *United States v. Byrd*, 60 M.J. 4, 6 (C.A.A.F. 2004). "A trial judge's ruling is entitled to due deference." *Id.* (citations and internal quotation marks omitted). This Court should reverse the military judge's evidentiary ruling under an abuse of discretion standard "if the military judge's findings of fact are clearly erroneous or if his decision is influenced by an erroneous view of the law." *Id.* (citations and internal quotation marks omitted).

If the military judge abused his discretion, this Court must test for prejudice. *Id.* at 10. In assessing prejudice, the Court should weigh "(1) the strength of the Government's case, (2) the strength of the defense case, (3) the materiality of the evidence in question, and (4) the quality of the evidence in question." *Id.* (citation omitted). The government bears the burden of demonstrating "harmlessness" when a military judge abuses his or her discretion in making an evidentiary ruling involving M.R.E. 701. *Id.*

Military Rule of Evidence 701 provides the following:

> If the witness is not testifying as an expert, the witness' testimony in the form of opinions or inferences is limited to those opinions or inferences that are (a)

> rationally based on the perception of the witness, (b) helpful to a clear understanding of the witness' testimony or the determination of a fact in issue, and (c) not based in scientific, technical, or other specialized knowledge within the scope of Rule 702.

Military Rule of Evidence 701 "limits opinion testimony by lay witnesses." *Byrd*, 60 M.J. at 5. When interpreting the provisions of M.R.E. 701, guidance can be found in judicial interpretations of Federal Rule of Evidence ["F.R.E."] 701, since F.R.E. 701 is "the model for its military counterpart." *Byrd*, 60 M.J. at 6.

"It is the proponent of lay opinion testimony who must satisfy the rule's three foundation requirements." *United States v. Garcia*, 413 F.3d 201, 211 (2d Cir. 2005). First, F.R.E. 701 "requires lay opinion testimony to be based on the witness's personal perceptions" as the fact-finder must have "an accurate reproduction of the event at issue." *Id.* (citations and internal quotation marks omitted). Second, "[a] lay opinion may be received in evidence only if it is 'helpful' to the jury's 'clear understanding of the witness' testimony or the determination of a fact in issue.'" *Id.* at 213 (citation omitted). Third, lay testimony cannot be "based on scientific, technical, or other specialized knowledge." *Id.* at 215.

"[T]he distinction between lay and expert witness testimony is that lay testimony results from a process of reasoning

familiar in everyday life, while expert testimony results from a process of reasoning which can be mastered only by specialists in the field." *United States v. Throckmorton*, 269 Fed. Appx. 233, 235-36 (3d Cir. 2008). In assessing this third prong, "a court must focus on 'the reasoning process' by which a witness reached his proffered opinion." *Garcia*, 413 F.3d at 215. "If the opinion rests 'in any way' upon scientific, technical, or other specialized knowledge, its admissibility must be determined by reference to Rule 702, not Rule 701." *Id.*

3. SA Devinny's Testimony Concerning SHA1 Values Did Not Constitute Lay Testimony Under Military Rule of Evidence 701

The government failed to meet any of the three specified conditions for lay opinion testimony in appellant's case.

First, SA Devinny did not personally download or observe any of the contraband video files appellant was actually charged with possessing. Nonetheless, SA Devinny opined, based upon his "training and experience," that the other eleven files in the share folder of appellant's IP address would play and that they were not corrupt or infected with viruses. (JA. at 248.) The following colloquy between the military judge and SA Devinny illustrates the speculative nature of his opinion:

> MJ: Do you know if those files [referring to the eleven files the witness did not actually view] could play?
>
> WIT: Well what I do know, sir, is if there is a file in a share folder and it's located

> in the share folder and I can view it, and there are two things: number one, that the targeted IP address is online and his, in this case, the LimeWire account was actively running; and the complete file is located in that share folder, and I know that from my training and experience.

(JA. at 248.)

According to this testimony, and assuming appellant had the "complete" files of the videos he was charged with possessing, SA Devinny should have been able to view the contraband files whenever appellant was online. Yet he was unable to do so and was not able to rule out the fact that the files could have been corrupt or contained viruses. (JA. at 248-49.) In sum, SA Devinny's testimony regarding the charged videos was based upon his training and experience, not on "personal perceptions." *Garcia*, 413 F.3d at 213. *See also Throckmorton*, 269 Fed. Appx. at 235-36 (holding that a law enforcement agent should not have been permitted to testify concerning "owe-sheets" since his opinion reflected his experience as a narcotics officer rather than facts discovered during the defendant's particular investigation); *see also Bank of China v. NBM LLC*, 359 F.3d 171, 181 (2d Cir. 2004) (acknowledging that testimony was erroneously admitted under F.R.E. 701 "because it was not based entirely on Huang's perceptions; the District Court abused its discretion to the extent it admitted the testimony based on Huang's experience and specialized knowledge in international banking.").

Second, SA Devinny's testimony did more than merely provide a summary of appellant's words and actions. Instead, SA Devinny's testimony included inferences that draw from the significance of SHA1 values. *See United States v. Oriedo*, 498 F.3d 593, 603 (7th Cir. 2007)(finding an agent's testimony erroneously admitted because it "was not limited to what he observed in the search or to other facts derived exclusively from this particular investigation; instead, [it] brought the wealth of his experience as a narcotics officer to bear on those observations and made connections for the jury based on that specialized knowledge."). *See generally United States v. Grinage*, 390 F.3d 746, 750 (2d Cir. 2004)(explaining that jurors were not "helped" under F.R.E. 701 by opinion testimony that told them what inferences to draw from the evidence).

Finally, the government did not demonstrate that SA Devinny's opinion testimony was informed by a "reasoning process familiar to the average person in everyday life rather than by scientific, technical, or other specialized knowledge." *Garcia*, 413 F.3d at 216. Knowledge regarding SHA1 values and their significance is hardly within the purview of an average person. Instead, information concerning SHA1 values reflects experience and training outside the ken of the average person. *See United States v. Cartier*, 543 F.3d 442, 446 (8th Cir. 2008) (identifying competing interpretations of hash values offered by

government and defense expert witnesses); *United States v. Hock Chee Koo*, 770 F.Supp.2d 1115, 1123 (D. Or. 2011) (noting that the defendant's expert witness explained "hash value" as "a series of numbers that acts as a digital fingerprint; when the hash value changes it means the content of a file has changed."); *United States v. Flinn*, 521 F.Supp.2d 1097, 1099 (E.D. Ca. 2007)(noting a computer forensic expert's testimony that images of actual child pornography are present if the hash values of the seized images matched a government database of known, real child pornography images). SA Devinny's testimony that the digital signature represented by a SHA1 value is more accurate than a DNA result demonstrates this principle. Much like forensic DNA evidence, SHA1 values are scientific, technical, or specialized within the meaning of M.R.E. 702.

Thus, this Court should follow *Garcia* and hold that "the foundation requirements of [M.R.E. 701] do not permit a law enforcement agent to testify to an opinion so based and formed if the agent's reasoning process depended, in whole or in part, on his specialized training and experience." 413 F.3d at 216. SA Devinny's testimony was not admissible under M.R.E. 701 and the "government was obliged to demonstrate its admissibility under [M.R.E.] 702 or forego its use." *Id.* at 217. "A holding to the contrary would encourage the Government to offer all kinds of specialized opinions without pausing first properly to

establish the required qualifications of their witnesses." *United States v. Figueroa-Lopez*, 125 F.3d 1241, 1246 (9th Cir. 1997). "Otherwise, a layperson witnessing the removal of a bullet from a heart during an autopsy could opine as to the cause of the decedent's death." *Id.*

The military judge has likely heard testimony similar to SA Devinny's in the past on unrelated cases. Nonetheless, "[a]s judges who have heard such testimony many times, we must not forget that *our* familiarity with it does not bring it within [F.R.E.] 701." *Id.* (emphasis in original). While the military judge evidently thought that information on hash values was "something within the collective ken of society," (JA. at 213), federal case law demonstrates it to be "scientific, technical, or other specialized knowledge" within the scope of M.R.E. 702.

4. The Erroneous Admission of SA Devinny's Expert Opinion Prejudiced Appellant and the Evidence is Legally Insufficient Even Considering SA Devinny's Inadmissible Testimony

Material prejudice to the substantial rights of appellant exists given the erroneous admission of SA Devinny's testimony on SHA1 values. But even assuming that the military judge properly admitted SA Devinny's testimony, the evidence remains legally insufficient to support a finding that appellant knowingly possessed videos containing child pornography given the following:

- SA Devinny never personally viewed, played, or downloaded any of the videos appellant was charged with possessing. Further, there is no indication that SA Devinny is a computer forensic examiner. Instead, it appears that SA Devinny is a regular case agent since he was "a special agent assigned to the general crimes division within the Naval Criminal Investigative Service" at the time of appellant's court-martial. (JA. at 27.)

- There is no evidence that the charged videos were even operable on appellant's computer because the government never seized the computer these contraband files were allegedly contained on. (JA. at 276.) Thus, the government never performed a computer forensic analysis of appellant's computer.

- Likewise, SA Devinny could not discount the possibility that the charged videos might not be operable on appellant's computer because of a virus or some other corruption within the file. (JA. at 248-49.)

- The government presented no evidence as to when appellant supposedly first downloaded the charged videos and when he last accessed them.

- The government presented no evidence that appellant purposely used specific search terms to locate filenames associated with child pornography.

- Similarly, the government presented no evidence showing that appellant affirmatively moved and categorized these videos, such as creating a separate folder titled "child pornography videos" and placing them in it.

- There is no evidence that appellant's computer was password protected or that appellant was the sole user of his computer.

- Appellant denied viewing, downloading, or attempting to download any child pornography at trial. (JA. at 313-14.) The government offered no evidence to rebut appellant's testimony in this regard.

"Possession" of child pornography "is not based upon unknown contingencies but must be knowing and conscious." *United States v. Navrestad*, 66 M.J. 262, 267 (C.A.A.F. 2008) (internal quotation marks and citation omitted). Too many "unknown contingencies" still exist in appellant's case even with SA Devinny's improperly admitted expert testimony. The evidence beyond SA Devinny's improperly admitted testimony (i.e., Prosecution Exhibits 2, 3, and 5) demonstrates the government's lack of investigation in this case. Prosecution Exhibit 5 simply stated that a certain IP address was registered to appellant. (JA. at 362.) Prosecution Exhibit 3 contained two fatal deficiencies. First, Prosecution Exhibit 3 does not establish that appellant knowingly possessed child pornography as required by 18 U.S.C. § 2252A(a)(5)(A). Appellant stated that he "saw what it was and never looked at them again." (JA. at 357.) Appellant's trial testimony supports this contention because he described how he believed that he had deleted the one video possibly containing a sixteen to eighteen year old girl when he clicked on the red X. (JA. at 310, 313, and 327.)

Second, Prosecution Exhibit 3 does not establish that the videos contained child pornography. Specifically, there is no mention of whether or how these videos depicted minors engaging in sexually explicit conduct as defined in 18 U.S.C. § 2256(2)(A). For example, there is no description as to the content of the videos. SA Marc Smith never defined child pornography to appellant nor reconciled the legal definition of child pornography under 18 U.S.C. § 2256(2)(A) with appellant's use of the term "underage porn." (JA. at 273-74.) While SA Smith may have showed appellant a copy of an NCIS investigative report (i.e., JA. at 364-74), this report was not admitted into evidence. Finally, SA Smith never showed the charged videos to appellant to ensure both parties were referring to the same videos. (JA. at 275.)

Ultimately, it was the quality and materiality of SA Devinny's improperly admitted expert testimony alone that could serve as the basis for appellant's conviction. SA Devinny essentially linked the videos found in appellant's share folder to contraband videos found off the gnutella network. SA Devinny would have been unable to do so without his training and experience in SHA1 values. (JA. at 33, 39, 46, 65, 95-96, 136, 150-51.) Stated differently, it is doubtful SA Devinny would opine that the files he recovered from the gnutella network would exactly match those found in appellant's share folder

based solely on the file title, file size, and file type. The government could only link appellant to contraband videos beyond a reasonable doubt by virtue of SA Devinny's expert testimony on SHA1 values. This testimony served as a key thrust during the trial counsel's rebuttal argument. (JA. at 352.)

"Where the erroneously admitted evidence goes to the heart of the case against the defendant, and the other evidence against the defendant is weak, we cannot conclude that the evidence was unimportant or was not a substantial factor in the jury's verdict." *Grinage*, 390 F.3d at 751. In addition, "[t]his was not a case where the prosecution presented a formidable array of admissible evidence and where the agent's inadmissible testimony was merely corroborative and cumulative." *Id.* at 752 (citation and internal quotation marks omitted). Instead, SA Devinny's expert link went to the crux of the government case and the admission of his testimony under M.R.E. 701 is not harmless because this Court cannot be certain that he would have been properly qualified under M.R.E. 702. There is nothing on the merits as to SA Devinny's training and experience conducting undercover computer operations involving child pornography. This is in keeping with the government's position that SA Devinny would not offer expert testimony at trial. *Cf. Figueroa-Lopez*, 125 F.3d at 1247 (finding that the witness would have been qualified to give expert testimony under F.R.E. 702

given his background and "the failure formally to go through the usual process-although an error-was clearly harmless.").

More importantly, a close examination of the government's case, even including SA Devinny's inadmissible testimony, demonstrates it to be legally insufficient. Even with SA Devinny's improper expert testimony, there are too many "unknown contingencies" at this point to show that appellant's possession was "knowing and conscious." Simply stated, the government never presented the charged videos as they exactly appeared on appellant's computer. This Court will never know if the charged videos were even operable on appellant's computer. Further, the government presented no evidence that appellant intentionally sought and repeatedly viewed the charged videos. At best, it appears that appellant inadvertently came across a video possibly containing a child, and then took actions he thought deleted the video from his computer. The government cannot rebut this testimony.

Conclusion

This Court should reverse the Army Court and find that SA Devinny's testimony was erroneously admitted against appellant. In addition, this Court should find the evidence to be legally insufficient even with SA Devinny's expert testimony. As such, the Charge should be dismissed with prejudice. *See Lockhart v. Nelson*, 488 U.S. 33, 39 (1988) (recognizing that when a defendant's conviction is reversed by an appellate court on the ground that the evidence was legally insufficient to sustain the jury's verdict, the Double Jeopardy Clause bars a retrial on the same charge).

MATTHEW T. GRADY
Captain, Judge Advocate
Appellate Defense Counsel
Defense Appellate Division
U.S. Army Legal Services Agency
9275 Gunston Road, #3206
Fort Belvoir, Virginia 22060
(703)693-0656
USCAAF No. 35092

RICHARD E. GORINI
Major, Judge Advocate
Branch Chief
Defense Appellate Division
USCAAF No. 35189

IMOGENE M. JAMISON
Lieutenant Colonel,
Judge Advocate
Deputy,
Defense Appellate Division
USCAAF No. 32153

PATRICIA A. HAM
Colonel, Judge Advocate
Chief,
Defense Appellate Division
USCAAF No. 31186

CERTIFICATE OF COMPLIANCE WITH RULE 24(d)

1. This brief complies with the type-volume limitation of Rule 24(c) because this brief contains 5,158 words.

2. This brief complies with the typeface and type style requirements of Rule 37 because this brief has been prepared in a monospaced typeface (12-point, Courier New font) using Microsoft Word, Version 2007 with no more than ten and a half inch characters per inch.

MATTHEW T. GRADY
Captain, Judge Advocate
Appellate Defense Counsel
Defense Appellate Division
U.S. Army Legal Services Agency
9275 Gunston Road
Fort Belvoir, Virginia 22060
(703)693-0656
USCAAF Bar No. 35092

(703) 893-0137