IN THE UNITED STATES COURT OF APPEALS
FOR THE ARMED FORCES

UNITED STATES, Appellant v. Private (E-1) **JUSTIN M. GURCZYNSKI** United States Army, Appellee	) APPELLANT'S REPLY BRIEF)) Crim. App. Dkt. No. 20160402)) USCA Dkt. No. 17-0139/AR)) Tried at Fort Leavenworth, Kansas,) on 25 April 2016, before a general) court-martial, convened by) Commander, Headquarters, United) States Army Combined Arms Center) and Fort Leavenworth, Colonel) Jeffery R. Nance, presiding.)

SAMUEL E. LANDES
Captain, Judge Advocate
Branch Chief
Government Appellate Division
U.S. Army Legal Services Agency
9275 Gunston Road
Fort Belvoir, VA 22060
(703) 693-0783
samuel.e.landes.mil@mail.mil
U.S.C.A.A.F. Bar No. 36626

A.G. COURIE III
Lieutenant Colonel, Judge Advocate
Deputy Chief, Government
Appellate Division
U.S.C.A.A.F. Bar No. 36422

MARK H. SYDENHAM
Colonel, Judge Advocate
Chief, Government Appellate
Division
U.S.C.A.A.F. Bar No 34432

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

Index

Table of Cases, Statutes, and Other Authorities

United States Supreme Court

United States Court of Appeals for the Armed Forces/Court of Military Appeals

Service Courts

United States Courts of Appeals

Other Statutes, Materials and Regulations

IN THE UNITED STATES COURT OF APPEALS
FOR THE ARMED FORCES

UNITED STATES, Appellant v. Private (E-1) **JUSTIN M. GURCZYNSKI** United States Army, Appellee	APPELLANT'S REPLY BRIEF Crim. App. Dkt. No. 20160402 USCA Dkt. No. 17-0139/AR Tried at Fort Leavenworth, Kansas, on 25 April 2016, before a general court-martial, convened by Commander, Headquarters, United States Army Combined Arms Center and Fort Leavenworth, Colonel Jeffery R. Nance, presiding.

Statement of Statutory Jurisdiction

The United States Army Court of Criminal Appeals (Army Court) reviewed this case pursuant to Article 62, Uniform Code of Military Justice, 10 U.S.C. § 862 (2012) [hereinafter UCMJ]. The statutory basis for this Court's jurisdiction is found in Article 67(a)(2), UCMJ, which mandates review in "all cases reviewed by a Court of Criminal Appeals which the Judge Advocate General orders sent to the Court of Appeals for the Armed Forces for review." UCMJ art. 67(a)(2).

Statement of the Case

Appellee was charged with two specifications of possession of child pornography in violation of Article 134, UCMJ. (JA 6). On May 13, 2016, the military judge suppressed the evidence of child pornography found on Appellee's

thumb drive based on a purported violation of the Fourth Amendment. (JA 166-71). On June 22, 2016, the Government appealed the military judge's ruling under Article 62, UCMJ. On September 6, 2016, the Army Court denied the appeal. *United States v. Gurczynski*, ARMY MISC 20160402, 2016 CCA LEXIS 541 (A. Ct. Crim. App. Sep. 6, 2016) (unpublished). On October 6, 2016, the Government requested reconsideration en banc. The Army Court denied the Government's request for reconsideration on October 24, 2016. (JA 5). The Judge Advocate General then certified this case to this Court.

Statement of Facts

On December 19, 2012, the Criminal Investigative Command (CID) office at the Presidio of Monterey initiated an investigation into Appellee based on an allegation that he had committed an abusive sexual contact on a child, DB, who was under the age of 16. (JA 59). Appellee was interviewed and admitted to having befriended DB through the social networking website, Facebook. (JA 60).

On January 14, 2014, a United States magistrate judge issued a search warrant for Appellee's off-post residence. (JA 67). The magistrate judge incorporated the affidavit of the CID agent in the warrant. (JA 67). The affidavit requested a search warrant for the "cellular device, personal computers, and associated peripheral digital media storage devices" of Appellee. (JA 68).

The search warrant authorized CID agents to search Appellee's digital media devices for evidence of violations of the UCMJ for attempted aggravated sexual assault of a child, indecent acts with a child, attempted sexual abuse of a child, abusive sexual contact with a child, child endangerment, and other offenses related to these allegations. (JA 66, 68). The military judge found that the warrant authorized the CID agents to search Appellee's digital media devices "for evidence that [Appellee] used those devices to access on line [sic] mediums to communicate with [DB] in order to 'engage in indecent acts with a child and to plan and execute a meeting with [DB] where [Appellee] ultimately engaged in additional indecent acts and sexual contacts with the child.'" (JA 166) (quoting from the warrant). The search warrant authorized the agents to search for evidence that he used digital media devices between September 1, 2007, and December 28, 2011, to maintain contact with DB and to discuss with DB and with others the crimes that had been committed. (JA 68).

On January 24, 2014, the CID agents executed the search warrant and seized twenty-eight digital media devices from Appellee's home, including the thumb drive and external hard drive where child pornography was found. (JA 65, 74-76). The CID office at the Presidio of Monterey sent the evidence to the CID office at Joint Base Lewis-McChord (JBLM) for assistance in conducting the digital forensic exam. (JA 77).

The digital forensic examiner (DFE), Special Agent CJP, from the JBLM CID office, testified that he received the federal search warrant along with the evidence and conducted the digital forensic exam. (JA 13, 15). When the DFE examined Appellee's thumb drive, he used the software Encase, which showed him all the different files on the device. (JA 17). The software permits the user to select between "text view" and "picture view." (JA 18-19). In "picture view," an image preview of the highlighted file is displayed in the bottom pane of the user's screen. (JA 19). In this case, the DFE selected "picture view," so an image of each file was displayed in the bottom portion of his screen. (JA 19).[1] There were no folders on the thumb drive, so "as soon at the image loaded into [the DFE's] software, you know, the files read through the devices, it's right there on the screen." (JA 18). The DFE did not have to click into any folders or files to observe the file names and an image of the files. (JA 18-20). Based on this initial viewing of the file names and images of the files, the DFE "almost immediately" observed that the thumb drive contained child pornography. (JA 19).

In examining the hard drive, the DFE limited his search to areas where there would be communications between the subject and a young victim, such as programs, applications, databases, and images. (JA 21). He stated that he included

[1] For the purpose of graphic illustration, Encase training materials depicting "picture view" are provided in the appendix.

images in his search because, "[f]rom [his] experience people tend to screen shot things, make copies of it and it'll show up as an image." (JA 22). As it turns out, in this case, Appellee had a program set up on his computer to "automatically create screen shots every 30 minutes." (JA 22, 104). In those screen shot images, the DFE found evidence of communications between the victim and Appellee. (JA 22, 104). When the trial counsel asked the DFE if there were any areas that he would not look into or would exclude when searching for communications with a minor, he responded, "Not much, to be honest with you. Communications are—you know, can be found pretty much anywhere." (JA 23).

The military judge found that the Government had a "valid warrant based upon probable cause to search for communications (which could include shared photos) between [Appellee and DB]." (JA 169). The military judge acknowledged that the "communications were alleged to have occurred via various electronic communication devices." (JA 169). The military judge stated that these communications could include photographs, "and even child pornography, if such child pornography were part of a communication or possible communication" to DB. (JA 170). However, the military judge held that the DD Form 2922 from the Presidio of Monterey that requested a search for child pornography improperly expanded the scope of the warrant and the resulting search. (JA 170). The military

judge did not address the plain view doctrine, which operates as an exception to the Fourth Amendment's prohibition against unreasonable searches and seizures.

Issue Presented

WHETHER THE MIILITARY JUDGE ERRED IN SUPPRESSING EVIDENCE OF CHILD PORNOGRAPHY A DIGITAL FORENSIC EXAMINER DISCOVERED DURING A SEARCH FOR APPELLEE'S COMMUNICATIONS WITH A CHILD VICTIM.

Argument

A. Fourth Amendment search and seizure doctrine is not discretionary for the military judge.

In addressing the standard of review, Appellee first notes that under the applicable "abuse of discretion" standard this Court considers findings of fact for clear error and conclusions of law de novo. (Appellee's Br. 12). But Appellee continues:

> However, "[t]he abuse of discretion standard calls for more than a mere difference of opinion. The challenged action must be arbitrary, fanciful, clearly unreasonable, or clearly erroneous." [*United States v. Ayala*, 43 M.J. 296, 298 (C.A.A.F. 1995)]. "Further, the abuse of discretion standard of review recognizes that a judge has a range of choices and will not be reversed so long as the decision remains within that range." *United States v. Mott*, 72 M.J. 319, 329 (C.A.A.F. 2013) (quoting *United States v. Gore*, 60 M.J. 178, 187 (C.A.A.F. 2004)).

(*Id.*) (some explanatory parentheticals omitted).

To the extent Appellee's articulation of the standard of review suggests that military judges have a range of choices on questions of constitutional law it is in error. Even when reviewing a military judge's decision for an abuse of discretion, this Court reviews a military judge's conclusions of law de novo. *United States v. Piren*, 74 M.J. 24, 27 (C.A.A.F. 2015) (citing *United States v. Gallagher*, 66 M.J. 250, 253 (C.A.A.F. 2008)). That is because the scope of Appellee's Fourth Amendment rights is a question of constitutional law, and questions of constitutional law are reviewed de novo. *United States v. Castillo*, 74 M.J. 160, 165 (C.A.A.F. 2015). Thus, the military judge's findings of historical fact—such as what the warrant authorized and where on the thumb drive the DFE searched—are reviewed for clear error, but the application of Fourth Amendment doctrine to those historical facts is reviewed de novo. *See United States v. Melanson*, 51 M.J. 1, 2 (C.A.A.F. 2000) (citing *United States v. Owens*, 51 M.J. 204, 209 (C.A.A.F. 1999)) ("When an accused contests personal jurisdiction on appeal, we review that question of law *de novo*, accepting the military judge's findings of historical facts unless they are clearly erroneous or unsupported in the record."). Appellee's formulation, mixing de novo review with a "range of choices," is inconsistent to the extent it applies to questions of law. Fourth Amendment doctrine is not discretionary for the military judge.

Instead, the "range of choices" test applies only to a military judge's factfinding, or to questions truly dedicated to a military judge's discretion, such as the choice among remedies, *see United States v. Stellato*, 74 M.J. 473, 488 (C.A.A.F. 2015), or whether to give a non-mandatory instruction, *see United States v. Taylor*, 53 M.J. 195, 199 (C.A.A.F. 2000). The case relied upon by Appellee, *Mott*, involved whether the accused waived his rights "knowingly," a state-of-mind question of fact. *See Ayala*, 69 M.J. at 65 (holding that the question of what was a commander's "primary purpose"—that is, what was his state of mind—is a question of fact reviewed de novo). The case the *Mott* court relied upon in selecting the "range of choices" standard of review, *Gore*, like *Stellato*, dealt with a military judge's choice among remedies. *Gore*, 60 M.J. at 187.

Thus, where the military judge's decision involves factfinding, this Court grants him substantial deference, and accepts his findings of fact unless they are clearly erroneous. *United States v. Cossio*, 64 M.J. 254, 256 (C.A.A.F. 2007). Where the military judge's decision involves matters within his discretion, he chooses from within a reasonable range of choices, and this Court will not reverse unless his choice is outside of that range, such that it is "arbitrary, fanciful, clearly unreasonable, or clearly erroneous." *Ayala*, 43 M.J. at 298. But, where the question is one of constitutional law, the military judge's conclusions of law—which is to say his application of the law to the facts—are reviewed de novo.

Piren, 74 M.J. at 27; *Castillo*, 74 M.J. at 165; *accord United States v. Burgess*, 576 F.3d 1078, 1087 (10th Cir. 2009) (quoting *United States v. Grimmett*, 439 F.3d 1263, 1268 (10th Cir. 2006)) ("'The ultimate question of reasonableness under the Fourth Amendment is a legal conclusion that we review de novo.'"). While the trial court is better situated to decide questions of fact and make discretionary decisions, this Court is best situated to decide questions of law.

Here, the military judge made findings of historical fact about what the warrant stated and what the DFE did during the search. To the extent those findings of fact are not clearly erroneous, this Court is bound by them. But the military judge also made conclusions of law, applying or ignoring Fourth Amendment doctrine to the facts he found. The Fourth Amendment does not provide him a "range of choices" from which to choose; the facts either constitute a violation of Appellee's Fourth Amendment rights or they do not. This Court owes the military judge no deference on that question.

B. The DFE was authorized to view all the files on the thumb drive.

Appellee relies heavily on the trial counsel's assertions of fact in his filings and argument in the trial court in asserting that the DFE relied solely on file names, rather than on file names *and* the picture view, in determining that what he was looking at was child pornography. (Appellee's Br. 6, 8-10, 36-37). This argument is factually incorrect and misses the point. "The averments of counsel during

motions practice and oral argument may be informative, but they are not evidence." *United States v. Warner*, 62 M.J. 114, 124 (C.A.A.F. 2005) (citing *United States v. Loving*, 41 M.J. 213, 138 (C.A.A.F. 1994)). Putting aside counsel's argument, then, the unrebutted evidence was that the DFE opened the thumb drive in "picture view," meaning that an image preview of each file was displayed on his screen. (JA 17-19).

Appellee seeks to avoid this evidence by asserting that the military judge found otherwise. (Appellee's Br. 10). The military judge wrote, "During the course of the exam, [the DFE] . . . saw several file names of videos normally associated with child pornography . . . ." (JA 167). Appellee thus relies on an unreasonable negative implication to suggest that the military judge found as a matter of fact that the DFE did not *also* rely on the picture view. The force of a negative implication depends on the circumstances. A sign on a storefront that reads "No Dogs Allowed" should be read to also exclude monkeys, since it is apparent that the sign's author sought to highlight only those animals most likely to be brought inside. So too a sign that reads "No Shirt, No Shoes, No Service" should not be read to allow the service of customers wearing a shirt and shoes but not pants. *See United States v. Robinson*, 28 M.J. 481, 483 n.* (C.M.A. 1989) (citing *Sullivan v. Hudson*, 490 U.S. 877 (1989)). Here, the military judge failed to consider and grapple with the evidence that the DFE used picture view. Therefore,

Appellee's desired negative implication—that because the military judge did not mention image previews, he affirmatively found that the DFE did not use image previews—is not reasonable under these circumstances.

In any event, even if the military judge did find that the DFE relied only on the file names, this Court should set aside his ruling for three reasons. First, such a finding would be clearly erroneous. To the extent the military judge relied on the arguments of counsel instead of the evidence (as Appellee suggests), he clearly erred, because the arguments of counsel are not evidence under *Warner*. The DFE's testimony that he used picture view was unrebutted by the defense. The defense did not put on contrary evidence or suggest that the DFE should not be believed. If the military judge found that the DFE did not use picture view, he clearly erred.

Second, even without picture view, the file names and the DFE's experience alone sufficiently made the contraband nature of the files "immediately apparent." *See Horton v. California*, 496 U.S. 128, 136 (1990). One example illustrates the tenor of these file names: "P101-Webcam - 12Yo Boy Get Sucked-Bibcam-Webcamboy -Fxg Older Brother Sucks Off His Preteen Bro Till He Orgasms And His Whole Body Jerks- Gay Pedo Pthc.avi." (JA 111). With or without an image preview, the file names made the contraband nature of the files "immediately

apparent." While the DFE's experience was surely helpful in determining that the files were contraband, it was hardly necessary.

Finally, the DFE was authorized to open and look at each of the files with or without an incriminating file name or an image preview. When a warrant authorizes a search for certain documents among comingled documents, "it is certain that some innocuous documents will be examined, at least cursorily, in order to determine whether they are, in fact, among those papers authorized to be seized." *Andresen v. Maryland*, 427 U.S. 463, 483 n.111 (1976). Thus, the Fourth Amendment permits a "brief perusal of documents in plain view in order to determine whether probable cause exists for their seizure under the warrant." *United States v. Heldt*, 668 F.2d 1238, 1267 (D.C. Cir. 1981). In the digital realm, because of the immense amount of comingled data, there may not be a substitute for a brief physical examination of many, if not all, of the files. *Burgess*, 576 F.3d at 1094.

Here, the warrant authorized the DFE to search for communications. (JA 166). The thumb drive included both files that showed communications with the victim and files that did not fit that description. (JA 94-112). The DFE testified that, to search for communications, he would have to look everywhere on the thumb drive because there was no place a communication could not be. (JA 23). *See United States v. Mann*, 592 F.3d 779, 782-83 (7th Cir. 2010) (noting that

images "could be essentially anywhere on the computer."). The thumb drive had no folders, so all of the files displayed at once and the DFE did not have to do any "digging." (JA 18, 21). Under *Andresen* and *Burgess*, the warrant thus authorized the DFE to briefly peruse each file on the drive to determine if it constituted a communication with the victim. Thus, with or without incriminating file names or image previews, the DFE did not run afoul of the Fourth Amendment when he opened the files on the thumb drive. Accordingly, this Court should set aside the military judge's ruling.

C. The discovery of evidence in plain view need not be inadvertent.

Both the military judge and Appellee devote substantial attention to whether the DFE knowingly looked for child pornography because of the search request provided by CID. The implied legal test they use is whether the DFE discovered the child pornography files purposely or inadvertently. Under Appellee's view, the plain view doctrine does not apply if the DFE wanted or expected to find child pornography on the thumb drive. Accordingly, both Appellee and the military judge considered dispositive the fact that CID requested a search for child pornography. Under the view of the military judge and Appellee, therefore, the

focus is on the agent's subjective state of mind, not on the objective scope of the search he in fact conducted.[2]

This is simply not the law. For a warrantless seizure of evidence to be authorized by the plain view doctrine, three requirements must be met: (1) the officer must not have violated the Fourth Amendment in arriving at the place at which the item of evidence could be plainly viewed; (2) the item's incriminating nature must be immediately apparent; and (3) the officer must have lawful access to the item of evidence plainly seen. *Horton*, 496 U.S. at 136-37. *Horton* is foundational for providing these three requirements, but the issue in the case was whether there was a fourth requirement, inadvertency:

> In this case we revisit . . . [w]hether the warrantless seizure of evidence of crime in plain view is prohibited by the Fourth Amendment if the discovery of the evidence was not inadvertent. We conclude that even though inadvertence is a characteristic of most legitimate "plain view" seizures, it is not a necessary condition.

Id. at 130.

As the Court further explained:

> [E]ven handed law enforcement is best achieved by the application of objective standards of conduct, rather than standards that depend upon the subjective state of mind of the officer. The fact that an officer is interested in an item of evidence and fully expects to find it in the course of a search should not invalidate its seizure if the search is

[2] While this was the military judge's focus, he failed to consider the plain view doctrine at all.

> confined to an area and duration by the terms of a warrant or a valid exception to the warrant requirement.

Id. at 138.

So, for example, the limits of where an officer may discover evidence in plain view during a search of a car are defined by where in the car probable cause supports a search for the evidence in question. Thus, "probable cause to believe that undocumented aliens are being transported in a van will not justify a warrantless search of a suitcase." *Id.* at 140-41. The limit of the search warrant and the first *Horton* requirement—that the officer did not violate the Fourth Amendment in arriving at the place where the evidence could be plainly seen—operate to constrain an agent's ability to put evidence into plain view. But the inquiry is entirely objective, focused on where the officer in fact searched, not on what he thought he would find. In *Horton*, for instance, the searching officer had a warrant to search for three rings in a house, but fully expected to find certain weapons in the house as well, and did. *Id.* at 141. Because the expectation of finding weapons did not expand the scope of where the officer *in fact* searched, there was no Fourth Amendment violation. *Id.* at 141-42.

Lower courts have had little trouble applying these principles to searches of digital media. *See United States v. Williams*, 592 F.3d 511 (4th Cir. 2010). In *Williams*, agents obtained a warrant to search the defendant's digital media for harassing messages. *Id.* at 515-16. A search of one item made agents suspicious

that the defendant possessed child pornography in his other media, the agents hoped to find child pornography on that media, and in fact did so. *Id.* at 516. The court held that each of the *Horton* requirements was met. First, the warrant allowed the officer to open the media, and so made him lawfully present at the "place" from which evidence was viewed. *Id.* at 522. Second, under the *Andresen-Burgess* line of cases, the officer was authorized to briefly open and review each file on the media in his search for the evidence of harassing communications, and so had lawful access to the media. *Id.* Third, having opened the files to conduct the *Andresen* review, the contraband nature of the files was immediately apparent. *Id.* Thus, the court held, the files were seized in plain view. *Id.* The court dismissed concerns that the agents were hoping to find child pornography because there is no "inadvertence" requirement. *Id.* at 523 (rejecting *United States v. Carey*, 172 F.3d 1268 (10th Cir. 1999)). *See also Mann*, 592 F.3d at 786 (holding that a detective who was searching for images of voyeurism that could have been "essentially anywhere" on the computer properly seized images of child pornography discovered during the course of the search).

Here, the search was like the one in *Williams*, and so plain view applies. First, the DFE had a search warrant to search the thumb drive for communications with the victim. As the DFE testified, consistent with *Mann*, there is nowhere on the thumb drive a communication could *not* be, so he was authorized to search the

entire drive and, in any event, there were no folders or subfolders to "dig" through. (JA 18, 21, 23). Thus, the DFE did not violate the Fourth Amendment in arriving at the "place" at which the evidence could be plainly viewed. Whether or not the DFE hoped, wished, or expected to find child pornography subjectively, objectively, his search in fact conformed to the limits of the warrant, because the warrant authorized a search of the entire thumb drive. Second, the DFE had lawful access to the files because he was authorized to conduct an *Andresen* examination of each file. Because the communications were commingled with other files, the DFE was authorized to open each to conduct a cursory review. Third, the DFE testified that the child pornography's contraband nature was immediately apparent to him. Thus, the plain view exception to the warrant requirement applied, and the DFE did not violate the Fourth Amendment by seizing the child pornography. Accordingly, this Court should set aside the military judge's ruling suppressing it.

D. The discovery of evidence of previously unknown crimes during a lawful search does not prevent the continued execution of that search.

Appellee suggests that the DFE was required to obtain a new warrant once he discovered the child pornography, relying primarily on language from *Burgess*. (Appellee's Br. 30-31). The court in that case stated, "[A]s our cases seem to require, [the searching agent] immediately closed the gallery view when he observed a possible criminal violation outside the scope of the warrant's search authorization and did not renew the search until he obtained a new warrant."

Burgess, 576 F.3d at 1094-95. However, the law does not require such a procedure, for two reasons. First, the *Burgess* language is dicta. The agent in that case chose to seek a new warrant, so the court was not faced with the question of whether the continued execution of the search would have been permissible had he not done so. Not only is the language dicta, it is weak dicta ("as our cases *seem* to require . . . ."). Even the Seventh Circuit, which believes that seeking a new warrant would be the preferable practice, does not hold that the Fourth Amendment is violated if agents continue the original search without a new warrant. *Mann*, 592 F.3d at 786 (acknowledging *Burgess* but holding that the Fourth Amendment was not violated when a detective continued a search for images of voyeurism after finding child pornography).

Second, Appellee's approach is inconsistent with Fourth Amendment jurisprudence. Appellee's privacy rights are protected by the requirement that any search be justified by either a warrant or an established exception to the warrant requirement. *Katz v. United States*, 389 U.S. 347, 357 (1967). Here, agents sought and obtained a warrant to search for communications with the victim. The justification for that warrant was not dependent on whether the DFE discovered evidence of other crimes as well. The DFE was entitled to execute the warrant by searching in any place on the thumb drive where communications with the victim could be found. As the DFE explained, communications could be found anywhere

on the thumb drive, so he was entitled to search the entire thumb drive. That he also found child pornography in plain view on the thumb drive—whether inadvertently or not—does not extinguish the warrant to search for communications, and so does not affect the reasonableness of the search. Instead, like in *Williams* and *Mann*, the DFE was permitted to continue the execution of the original search warrant, collecting along the way other evidence subject to the plain view exception, and was not required to stop the execution of the search for communications to seek a warrant to search for child pornography.

Consider the seizure of a terrorist's cell phone following a domestic attack. Assume agents seek and obtain a warrant to search the contents of the phone for contacts with terrorist organizations, or that knowledge of these organizations is so important to national security and the prevention of future attacks that exigent circumstances justify a warrantless search for terrorist contacts. Pursuant to this justification, agents determine that evidence of contact with terrorist organizations could be found anywhere on the phone, and examine the contents of the phone with the *Andresen* procedure, briefly examining each file to determine if it constitutes evidence of contacts with a terrorist organization. By the tenth of 100 files to be examined in this manner, agents see what is obviously child pornography. Must the search for terrorist contacts within the remaining ninety files halt while agents obtain a warrant to also search for child pornography?

Under Appellee's view, the agents must choose between pausing the original search and the suppression of any child pornography they might find. Nothing in the Supreme Court's Fourth Amendment jurisprudence supports this result. Instead, like in *Williams* and *Mann*, the agents, supported by the original justification for the search, may continue the search, seizing evidence of other crimes they discover when permitted by the plain view doctrine. The result in the digital realm in this instance is not different from the result in the physical realm. In *Horton*, the detective had a warrant for jewelry but found weapons. If he was required to halt the search for jewelry in order to obtain a new warrant for weapons, the Court would have mentioned it.

To be sure, an agent who wishes to search in an area *not* supported by the original justification for the search must rely on a new warrant or warrant exception. For example, suppose an agent obtains a warrant to search a device for malicious software that can be deployed to harm other computers. The agent knows that the software she is looking for is at least 1,000 megabytes in size. During the search, she comes across a folder that, based on information provided by her forensic software, apparently contains a total of only 1 megabyte worth of data. Because the object of the search could not possibly be in the folder, if the agent wishes to search within the folder, she must obtain a new warrant or rely on an exception to the warrant requirement. *Cf. Horton*, 496 U.S. at 140-41

(explaining that justification to search a van for illegal immigrants will not constitute justification to search a briefcase found within the van). Similarly, an agent with an authorization to search for photographs taken during a given date must obtain a new warrant to search for photographs taken on a different date. *See United States v. Osorio*, 66 M.J. 632, 636-37 (A.F. Ct. Crim. App. 2008).[3] Lastly, if the agent's software identifies certain files already known to law enforcement, indicating that they cannot possibly be the files sought by the warrant, the agent must obtain a new warrant to search those files. *See Mann*, 592 F.3d at 786 (holding that a detective was not authorized to examine files that forensic software indicated were known child pornography during a search for recently made images of voyeurism).

However, where the agent searches only in places where the object of the warrant could be found, any evidence of other crimes discovered during the course of the search is admissible under the plain view exception, whether or not the agent subjectively expects to find the evidence, and no new warrant is necessary. As *Mann* recognizes, very often, a warrant for the search of certain files will authorize

---

[3] *Osorio*, as *Burgess* suggests, holds that an agent who discovers evidence of an unexpected crime must stop his search and wait for a new warrant. *Osorio*, 66 M.J. at 636. However, *Osorio* relied heavily on *Carey*, and both cases rather obviously ignore *Horton*'s explanation of the irrelevance of an agent's subjective intent. *See Williams*, 592 F.3d at 523 (criticizing *Carey* as inconsistent with *Horton*).

a search of all of the media, possibly putting into plain view either innocuous files or evidence of other crimes. But this is nothing new: a warrant to search for fingerprints or DNA evidence in a room will very often permit a search of every nook and cranny in that room, and may put into plain view everything in the room. However, an individual's primary privacy protection is the warrant requirement. As *Horton* recognized, so long as the agents adhere to the limits of the original search justification, no further privacy interest is violated by the seizure of other evidence seen in plain view. Here, the DFE was authorized to search for communications, and communications could have been found anywhere on the thumb drive, which had no folders. Accordingly, he searched everywhere on the thumb drive, and found child pornography. He did not violate the Fourth Amendment in arriving at the "place" at which he saw the child pornography in plain view, he had lawful access to it, and its contraband nature was immediately apparent. Accordingly, the military judge abused his discretion in suppressing the child pornography, and this Court should set aside his ruling.

Wherefore, the United States respectfully requests that this Honorable Court set aside the military judge's ruling suppressing evidence from Appellee's thumb drive.

for SAMUEL E. LANDES
Captain, U.S. Army
Branch Chief, Government
Appellate Division
U.S.C.A.A.F. Bar No. 36626

A.G. COURIE III
Lieutenant Colonel, Judge
Advocate
Deputy Chief, Government
Appellate Division
U.S.C.A.A.F. Bar No. 36422

MARK H. SYDENHAM
Colonel, Judge Advocate
Chief, Government Appellate
Division
U.S.C.A.A.F. Bar No 34432

CERTIFICATE OF COMPLIANCE WITH RULE 24

1. This brief complies with the type-volume limitation of Rule 24(c) because:

This brief contains 6,118 words.

2. This brief complies with the typeface and type style requirements of Rule 37 because:

This brief has been typewritten in 14-point font with proportional, Times New Roman typeface using Microsoft Word Version 2013.

A.G. COURIE III
Lieutenant Colonel, Judge Advocate
Attorney for Appellant
January 30, 2016

Appendix

Table Pane (Right Pane)

The table pane view displays the subfolders and files that are contained within the folder that is highlighted in the tree pane. Highlighting a folder in the tree pane affects the display in the right pane. Figure 12 shows "Star.Trek.Stories" folder highlighted in the Tree pane and the contents of this folder are displayed in the Table pane.

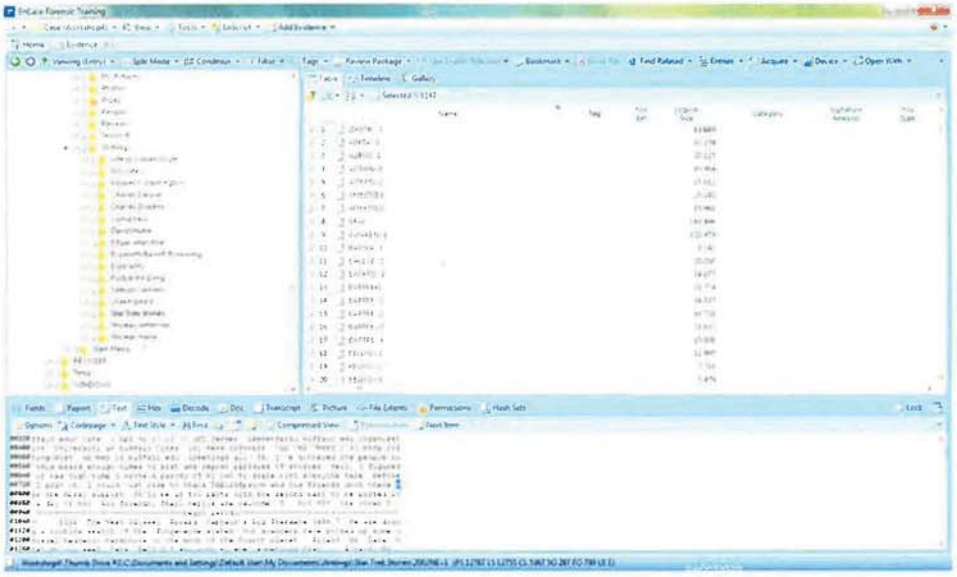

Figure 12. Tree view item chosen...table view displays contents of the chosen folder

View Pane (Bottom Pane)

The view pane displays the contents of the item selected in the table pane. The view pane has default settings that should be understood. The contents of a file are checked to see if it is an image that can be decoded internally. If so it will automatically switch to a picture of you in the bottom pane and display the image.

A large amount of evidence gathering is conducted from the view pane. Here, the user can select various amounts of data and bookmark that information which can then be included in the report. The examiner can also select different formats from the tabs above the view pane. Depending upon which tab is chosen, sub-menus may or may not be present. Figure 13 shows the sub-menus for a Text tab view. Figure 14 shows the Picture tab view has no accompanying sub-menus. Figure 15 shows the both hex and text values in the view pane.

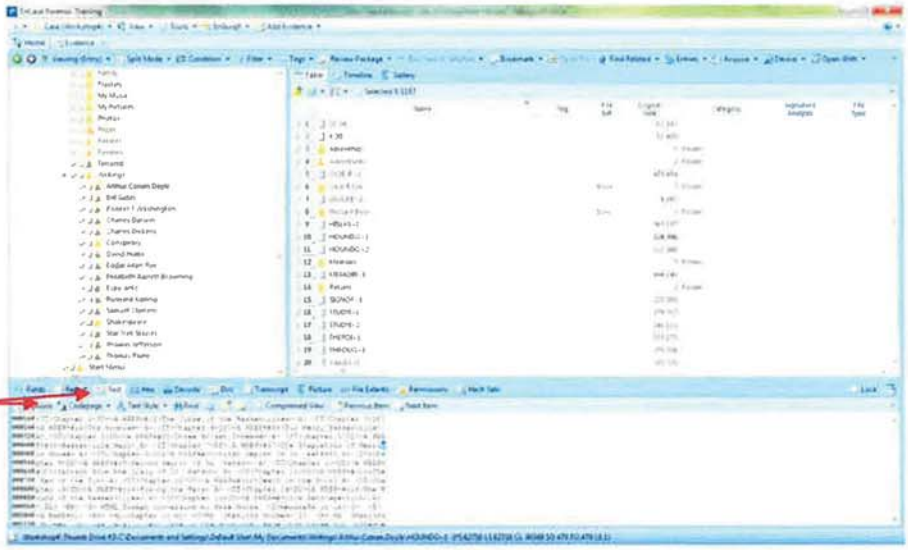

Figure 13. View pane with Text tab chosen (note the sub-menus).

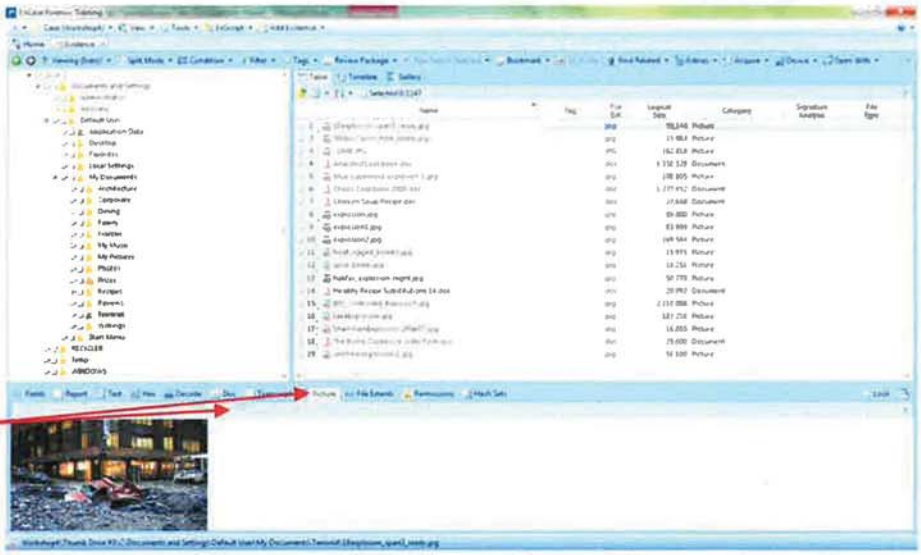

Figure 14. View pane with the Picture tab chosen (note no sub-menus).

CERTIFICATE OF FILING AND SERVICE

I certify that the foregoing reply brief in *United States v. Gurczynski*, Crim. App. Misc. Dkt. No. 20160402, USCA Dkt. No. 17-0139/AR, was electronically filed with the Court (efiling@armfor.uscourts.gov) on 30 January 2017 and contemporaneously served electronically on appellate defense counsel.

DANIEL L. MANN
Lead Paralegal Specialist
Office of The Judge Advocate General, United States Army
9275 Gunston Road
Fort Belvoir, VA 22060-5546
(703) 693-0822