

Digital Evidence

Major Jacqueline J. DeGaine*

*It's impossible to move, to live, to operate at any level without leaving traces, bits, seemingly meaningless fragments of personal information.*¹

I. Introduction

At 2000 on Tuesday night, Captain (CPT) Jones uses her iPhone to send CPT Smith a text message in an attempt to confirm the meeting place for Wednesday's Physical Training (PT) session. Receiving the text message, CPT Smith replies, confirming that Wednesday's PT session will start at 0615 with group stretching at the bottom of Birch Hill. To ensure that she knows her way to Birch Hill, CPT Smith conducts a quick search on her tablet's google maps app, and also uses her vehicle's Global Positioning System (GPS) the next morning. After a grueling run up and down Birch Hill, CPT Jones logs on to her Facebook account and posts a picture of the spectacular view of the snowcapped mountains from the top of the hill, with the caption, "[t]he weather is beautiful, wish you were here."

A short time later CPT Jones arrives at her office. While drinking her coffee she checks her work e-mail account and her electronic calendar to prepare for the day ahead. After reading her e-mail messages, CPT Jones listens to her voicemail messages from Charlie Company Commander, CPT Harper, and U.S. Army Criminal Investigation Command (CID), Special Agent (SA) Zimmerman. She immediately returns their phone calls and learns that CID has initiated an investigation into a Soldier named Specialist (SPC) John Doe, for suspected possession of child pornography. Specialist Doe's roommate, SPC Green, reported seeing digital images of suspected child pornography when he borrowed SPC Doe's laptop computer. When CID searched SPC Doe's barracks room, agents seized the laptop, a cell phone, and several thumbdrives. While interviewing witnesses later that day, CID agents learned that, in addition to possession of child pornography, SPC Doe is also suspected of communicating with underage minors via an AOL chat room. One of the witnesses told the agents that SPC Doe also has a stack of compact discs (CDs) and thumbdrives in a gym bag in the trunk of his vehicle.²

As shown through a typical day in the life of a trial counsel, CPT Jones, technology and digital evidence have become part of everyday life.³ Text messages, cell phone calls, social media postings, voicemails, digital photos, electronic calendars, and other forms of digital media are used to assist with a myriad of daily activities, both personal and professional in nature. "Unfortunately, those who commit crimes have not missed the information revolution. Criminals use mobile phones, laptop computers, and network servers in the course of committing their crimes."⁴ Several months after CPT Jones's initial notification of SPC Doe's case, she will represent the United States in the court-martial against SPC Doe. At trial, CPT Jones will use digital evidence and a digital evidence expert to further the government's case-in-chief against SPC Doe.

This article serves as a blueprint for military justice practitioners to use while advising personnel collecting digital evidence; in analyzing and evaluating collection procedures in preparation for trial; and in presenting digital evidence at trial. Part II discusses the background and definition of digital evidence before transitioning into a brief discussion of the Fourth Amendment and statutes applicable to digital evidence collection. Next, Part III outlines collection procedures with and without a search authorization, as well as collection procedures involving third party service providers by means of compelled and voluntary disclosure. The final part focuses on evidentiary issues leading up to and during trial.

II. Background and Definition

A. Background

"Although computers have existed for more than 60 years, it has been only since the late 1980s, as computers have proliferated in businesses, homes, and government agencies, that digital evidence has been used to solve crimes and prosecute offenders."⁵ The earliest crimes involving

* Judge Advocate, U.S. Army. Presently assigned as Chief, Administrative Law, 1st Sustainment Command (Theater), Afghanistan. This article was submitted in partial completion of the Master of Laws requirements of the 61st Judge Advocate Officer Graduate Course.

¹ *William Gibson Quotes*, BRAINYQUOTE, http://www.brainyquote.com/quotes/authors/w/william_gibson.html (last visited July 16, 2013). William Ford Gibson is an "American-Canadian writer of science fiction who was the leader of the genre's cyberpunk movement." (emphasis removed). *William Gibson*, ENCYCLOPAEDIA BRITANNICA, <http://www.britannica.com/EBchecked/topic/233297/William-Gibson> (last visited Mar. 12, 2013).

² EOGHAN CASEY, *DIGITAL EVIDENCE AND COMPUTER CRIME: FORENSIC SCIENCE, COMPUTERS, AND THE INTERNET* 76-77 (3d ed. 2011) (providing a loosely adapted scenario).

³ OFFICE OF LEGAL EDUC., EXEC. OFFICE FOR U.S. ATTORNEYS *COMPUTER CRIME & INTELLECTUAL PROPERTY. SEC. CRIM. DIV., U.S. DEP'T OF JUSTICE, SEARCHING AND SEIZING COMPUTERS AND OBTAINING ELECTRONIC EVIDENCE IN CRIMINAL INVESTIGATIONS*, at ix (3d ed. 2009) [hereinafter *SEARCHING AND SEIZING COMPUTERS*].

⁴ *Id.*

computers involved computer theft, computer destruction, and unauthorized computer access.⁶ Later, computer-related crime developed into the use of computers to commit fraud; and in the 1990s, the accessibility of computers led to additional types of crime including child pornography.⁷ Today computer crimes continue to grow exponentially and are considered “among the fastest growing crimes in our society.”⁸

Because digital devices and computer crime have evolved and infiltrated society, they have increasingly become a part of daily litigation.⁹ “Electronic records such as computer network logs, email [sic], word processing files, and image files increasingly provide the government with important (and sometimes essential) evidence in criminal cases.”¹⁰ Military justice practitioners, like CPT Jones, frequently rely on digital evidence in a variety of types of trials.¹¹ In addition to child pornography cases, practitioners may find digital evidence useful in cases of child abuse, homicide, domestic violence, assault, fraud, larceny, harassment, stalking, or drug-related crimes.¹² “Indeed,

virtually every class of crime can involve some form of digital evidence.”¹³

B. Digital Evidence Defined

Due to its increased importance in investigations and increased use at trial, litigators on both sides of the bar should first have a basic understanding of the definition of digital evidence and potential sources of digital evidence.¹⁴ “Digital evidence is information and data of value to an investigation that is stored on, received, or transmitted by an electronic device. This evidence is acquired when data or electronic devices are seized and secured for examination.”¹⁵ Digital evidence can be found on a number of electronic devices including hard drives, laptop computers, desktop computers, servers, telephone systems, wireless communication systems, the Internet, and mobile devices.¹⁶

C. Fourth Amendment and Applicable Statutes

One of the main sources of law that governs the area of digital evidence is the Fourth Amendment.¹⁷ To properly handle these digital evidence cases, litigators should re-familiarize themselves with the basics of the Fourth Amendment during the investigation and while preparing for trial. The Fourth Amendment provides:

The right of the people to be secure in their persons, houses, papers, and effects, against unreasonable searches and seizures, shall not be violated, and no warrants shall issue, but upon probable cause,¹⁸ supported by oath or affirmation, and particularly describing the place to be searched, and the persons or things to be seized.¹⁹

⁵ NAT’L INST. OF JUSTICE, U.S. DEP’T OF JUSTICE, DIGITAL EVIDENCE IN THE COURTROOM: A GUIDE FOR LAW ENFORCEMENT AND PROSECUTORS, at xi (2007) [hereinafter PROSECUTORS], available at <https://www.ncjrs.gov/pdffiles1/nij/211314.pdf>.

⁶ CASEY, *supra* note 2, at 65.

⁷ *Id.* at 65–66.

⁸ U.S. DEP’T OF ARMY, FIELD MANUAL 3-19.13, LAW ENFORCEMENT INVESTIGATIONS para. 11 (10 Jan. 2005) [hereinafter FM 3-19.13].

⁹ See CASEY, *supra* note 2, at 38–39.

By now it is well known that attorneys and police are encountering progressively more digital evidence in their work. Less obviously, computer security professionals and military decision makers are concerned with digital evidence. An increasing number of organizations are faced with the necessity of collecting evidence on their networks in response to incidents such as computer intrusions, fraud, intellectual property theft, sexual harassment, and even violent crimes.

Id.

¹⁰ SEARCHING AND SEIZING COMPUTERS, *supra* note 3; see also MARIE-HELEN MARAS, COMPUTER FORENSICS: CYBERCRIMINALS LAWS AND EVIDENCE 5 (Megan R. Turner et al. eds., 2012).

¹¹ Survey of Former and Current Chiefs of Military Justice (Nov. 2012) [hereinafter Survey] (received responses from four former and current chiefs of military justice recounting their experiences at various Army installations) (unpublished responses) (on file with author).

¹² See U.S. SECRET SERV., U.S. DEP’T OF HOMELAND SECURITY, BEST PRACTICES FOR SEIZING ELECTRONIC EVIDENCE v.3: A POCKET GUIDE FOR FIRST RESPONDERS 13–15 (2007) [hereinafter SECRET SERV. BEST PRACTICES], available at <https://www.ncjrs.gov/APP/publications/Abstract.aspx?id=239359>; see also PROSECUTORS, *supra* note 5, at xi (“Once the province of ‘computer crime’ cases such as hacking, digital evidence is now found in every crime category.”); see also CASEY, *supra* note 2, at 35–36.

¹³ SEARCHING AND SEIZING COMPUTERS, *supra* note 3, at ix.

¹⁴ “[N]o attorney can avoid the . . . task of understanding the law applicable to litigating with ESI [(electronically stored information)], as that law is developing, evolving, and maturing.” MARIAN K. RIEDY ET AL., LITIGATING WITH ELECTRONICALLY STORED INFORMATION 3 (2007).

¹⁵ NAT’L INST. OF JUSTICE, U.S. DEP’T OF JUSTICE, ELECTRONIC CRIME SCENE INVESTIGATION: A GUIDE FOR FIRST RESPONDERS, at ix (2008) [hereinafter FIRST RESPONDERS], available at <http://www.nij.gov/pubs-sum/219941.htm>. There are several other definitions of “digital evidence.” See CASEY, *supra* note 2, at 36–37.

¹⁶ See CASEY, *supra* note 2, at 36–38. see also SECRET SERV. BEST PRACTICES, *supra* note 12, at 13–15.

¹⁷ SEARCHING AND SEIZING COMPUTERS, *supra* note 3, at ix.

¹⁸ Probable cause is determined by examining the “totality of the circumstances.” *Illinois v. Gates*, 462 U.S. 213 (1982).

¹⁹ U.S. CONST. amend. XIV.

In addition to the limits established by the Fourth Amendment, the legislative branch has established additional limits on digital evidence collection through the development of various statutes.²⁰ These statutes include the Wiretap Act,²¹ the Pen/Trap Statute,²² and the Electronic Communications Privacy Act (ECPA)/Stored Communications Act (SCA).²³ “[These statutes] are in large part a reaction to Supreme Court decisions interpreting the Fourth Amendment and are, broadly speaking, designed to provide more protections to individuals.”²⁴ The Wiretap Act governs interception and disclosure of electronic communications, including interception and disclosure by persons involved with investigations;²⁵ the Pen/Trap Statute²⁶ governs devices used to identify phone numbers;²⁷ and the ECPA/SCA governs access to stored electronic communications.²⁸ The ECPA/SCA will be discussed in further detail in Part III.B of this primer.

III. Digital Evidence Collection Procedures²⁹

In consideration of the Fourth Amendment and the statutes listed above, there are a variety of ways for military investigators to lawfully obtain digital evidence.³⁰ Digital evidence is unique because it consists of virtual information and thus may exist in more than one location: in the possession of the accused and in the possession of a third party, namely the service providers. This part will cover collection procedures for both.

A. Digital Evidence from the Accused

The most obvious and common way to obtain evidence directly from the accused is through the use of a search warrant,³¹ or what is referred to in the Uniform Code of Military Justice (UCMJ) as a “search authorization.”³² A commander can authorize the search of an area or person over which he has control.³³ For example, using the hypothetical fact pattern above, SPC Doe’s company commander can authorize a probable cause search of SPC Doe’s room and SPC Doe’s vehicle assuming, as in this case, he has reason to believe that the vehicle and room contain evidence of the crimes of which SPC Doe is suspected.³⁴ Higher level commanders have a broader range of authority regarding searches because they have control over larger areas and more Soldiers than do lower level commanders.³⁵

²⁰ THOMAS K. CLANCY, CYBER CRIME AND DIGITAL EVIDENCE: MATERIALS AND CASES 12–13 (2011); PROSECUTORS, *supra* note 5, at 1.

²¹ 18 U.S.C. §§ 2510–2522 (2011) (also known as the “Wiretap Act”); CLANCY, *supra* note 20, at 12–13.

²² 18 U.S.C. §§ 3121–3127 (also known as the “Pen/Trap Statute”); CLANCY, *supra* note 20, at 12–13.

²³ 18 U.S.C. §§ 2701–2711 (also known as the “Stored Communications Act” (SCA) and more recently as the “Electronic Communications Privacy Act” (ECPA)); CLANCY, *supra* note 20, at 12–13.

²⁴ CLANCY, *supra* note 20, at 257.

²⁵ *See id.* at 12.

²⁶ A “pen register” is (“[a] device that decodes or records electronic impulses, allowing outgoing numbers from a telephone to be identified.”) (emphasis removed) *Pen Register Definition*, FREE DICTIONARY BY FARLEX, <http://legal-dictionary.thefreedictionary.com/Pen+Register> (last visited Mar. 9, 2013). A “trap and trace device” is “a device or process which captures the incoming electronic or other impulses which identify the originating number or other dialing, routing, addressing and signaling information . . . provided . . . such information shall not include the contents of any communication.” *Trap and Trace Device Definition*, FREE DICTIONARY BY FARLEX, <http://encyclopedia.thefreedictionary.com/trap+and+trace> (last visited May 20, 2013) (quoting 18 U.S.C. § 3127(4)) (emphasis removed).

²⁷ *See* CLANCY, *supra* note 20, at 12.

²⁸ *Id.*

²⁹ The Computer Crime Investigation Unit (CCIU) and the U.S. Army Criminal Investigation Laboratory (USACIL) located at Fort Gillem, Georgia, are integral to the Army’s mission in combating computer crimes. Both offer training and support to the U.S. Army Criminal Investigation Command (CID) field offices and can be useful in helping attorneys address technical questions with respect to computer investigations. FM 3-19.13, *supra* note 8, para. 11; *see also* U.S. Army Criminal Investigation Laboratory, U.S. ARMY CRIMINAL INVESTIGATION COMMAND, <http://www.cid.army.mil/usacil.html> (last visited May 20, 2013).

³⁰ Presentation by Keith Lyon, Cal. Deputy Attorney Gen., E-Evidence: Getting it and Using it (Sept. 19, 2012) [hereinafter Lyon Presentation] (on file with author).

³¹ *Id.*; *see also* MANUAL FOR COURTS-MARTIAL, UNITED STATES, MIL. R. EVID. 315 (2012) [hereinafter MCM]. *See also* MARAS, *supra* note 10, at 81.

³² MCM, *supra* note 31, MIL. R. EVID. 315.

³³ *Id.* MIL. R. EVID. 315(d).

³⁴ *Id.*

³⁵ 2 CRIMINAL LAW DEP’T., THE JUDGE ADVOCATE GEN.’S LEGAL CTR. & SCH., U.S. ARMY, CRIMINAL LAW DESKBOOK, at N-15 (2012) [hereinafter DESKBOOK], available at http://www.loc.gov/rr/frd/Military_Law/pdf/Crim-Law-Deskbook-8-3-12_Vol-2.pdf.

In addition to commanders, military magistrates³⁶ can authorize on-post searches,³⁷ while United States magistrate judges³⁸ and civilian judges can authorize off-post searches.³⁹ As a practice tip, military practitioners must remember that in spite of their on-post search authority, neither commanders nor military magistrates may authorize off-post searches of a Soldier's quarters.⁴⁰ Before seeking a commander's search authorization, trial counsel must understand the following prerequisites for a commander to authorize a search.

1. Search Authorization

A request for search authorization⁴¹ should include information provided under oath⁴² describing the offense being investigated, the items being searched for, the location where the search is being conducted, and an explanation as to why the items are believed to be at the stated location at the stated time.⁴³ In other words, the request for search authorization must articulate a basis for probable cause and must articulate with "particularity" the items to be seized and the places to be searched.⁴⁴

³⁶ U.S. DEP'T OF ARMY, REG. 27-10, MILITARY JUSTICE para. 8-1 (3 Oct. 2011) [hereinafter AR 27-10] (noting the establishment of the Army Military Magistrate Program) ("A military magistrate is a JA[(judge advocate)] empowered . . . to issue search, seizure, and apprehension authorizations on probable cause.").

³⁷ U.S. ARMY TRIAL JUDICIARY, STANDING OPERATING PROCEDURES FOR MILITARY MAGISTRATES 8 (Mar. 2012) [hereinafter SOP FOR MAGISTRATES] (citing *United States v. Rogers*, 388 F.Supp. 298 (E.D. Va. 1975) and *United States v. Reppert*, 76 F. Supp. 2d 185 (D. Conn 1999) (explaining in *Reppert* that, "property leased by the Government in the civilian community to house sailors and their families [is] under 'military control'")); *see also* MCM, *supra* note 31, MIL. R. EVID. 315(d).

³⁸ *See generally* 28 U.S.C. §§ 631–639 (2011) (Terms of appointment and powers of U.S. magistrate judges).

³⁹ MCM, *supra* note 31, MIL. R. EVID. 315(d); SOP FOR MAGISTRATES, *supra* note 37, at 8.

⁴⁰ MCM, *supra* note 31, MIL. R. EVID. 315(d); SOP FOR MAGISTRATES, *supra* note 37, at 8.

⁴¹ U.S. Dep't of Army, DA Form 3744, Affidavit Supporting Request for Authorization to Search and Seize or Apprehend (Sept. 2002) [hereinafter DA Form 3744].

⁴² AR 27-10, *supra* note 36, para. 8-8(a) ("Information provided in support of the request for authorization may be sworn or unsworn. The fact that sworn information is generally more credible and often entitled to greater weight than information not given under oath should be considered."); *see also* SOP FOR MAGISTRATES, *supra* note 37, at 5.

⁴³ SOP FOR MAGISTRATES, *supra* note 37, at 5 (explaining that while there are rare instances in which the sworn statements can be oral, written sworn statements are a better practice).

⁴⁴ MARAS, *supra* note 10, at 81.

There are additional issues to consider when establishing particularity, including "whether the seizable property is the computer *hardware* or merely the *information* that the hardware contains."⁴⁵ If authorities plan to seize the computer equipment based upon its physical nature, the "courts have often found fairly generic descriptions of the items . . . sufficient."⁴⁶ "Of course, if computer equipment has been stolen and that specific equipment is the object of the search, it [must] be described with sufficient particularity to identify it."⁴⁷

When investigators want to search or seize computer items because of the information that may be stored on those items, a different technique may be necessary.⁴⁸ Instead of the *hardware* being described with particularity, the *content* should be described with particularity.⁴⁹

With regard to the accusations against SPC Doe, investigators want to search SPC Doe's computer and digital devices because of the potential information that may be stored on them. Therefore, a proper authorization may grant permission for law enforcement personnel to search "for all information, in whatever form found, to include records, documents, and materials, whether electronic or physical, related to the offenses previously described."⁵⁰ In this case, the authorization should also include language authorizing a search of the seized digital media for "evidence of ownership and control" of the information relevant to the crime.⁵¹

While CID and the military police (MP) oftentimes independently determine what evidence they are looking for during an investigation, trial counsel should proactively examine the investigative file to see if there is any additional evidence relevant to the investigation. The sooner that the trial counsel can examine the file, the sooner she will discover any missing pieces of evidence in the case and work to secure pieces of evidence before they disappear or are compromised. If a trial counsel examines the file and

⁴⁵ SEARCHING AND SEIZING COMPUTERS, *supra* note 3, at 70; CLANCY, *supra* note 20, at 109–10.

⁴⁶ CLANCY, *supra* note 20, at 110 (citing *State v. Lehman*, 736 A.2d 256, 260–61 (Me. 1999)).

⁴⁷ *Id.* at 110–11; SEARCHING AND SEIZING COMPUTERS, *supra* note 3, at 71 ("Courts have . . . held that descriptions of hardware can satisfy the particularity requirement so long as the subsequent searches of the seized computer hardware appear reasonably likely to yield evidence of a crime . . .").

⁴⁸ *See generally* CLANCY, *supra* note 20, at 113 (explaining the "container approach" and the "special approach" for evidence collection).

⁴⁹ SEARCHING AND SEIZING COMPUTERS, *supra* note 3, at 72. *See generally* *infra* Appendix A.

⁵⁰ SOP FOR MAGISTRATES, *supra* note 37, at 10.

⁵¹ PROSECUTORS, *supra* note 5, at 10.

wants additional evidence, she should notify CID and request that the agent obtain the evidence pursuant to the original authorization or pursuant to an additional authorization if necessary.⁵²

If there is no authorization to search, there are specific exceptions that allow law enforcement personnel to search for evidence under certain conditions; the most common exceptions include consent, plain view, and exigent circumstances.⁵³

2. Consent

When an individual consents to a search, he permits law enforcement officials to search his person or his property.⁵⁴ If law enforcement personnel arrive on scene without authorization, they may seek permission to search the property from the person who owns, controls, or shares the property.⁵⁵ To be valid, consent must be deemed “voluntary”⁵⁶ when viewing the totality of circumstances.⁵⁷ The government’s burden of proof to show that consent existed is “clear and convincing evidence.”⁵⁸ While working with CID agents, trial counsel should encourage agents to obtain written consent during investigations because the language of the consent can help establish the voluntariness and scope of the consent.⁵⁹ “It is a good practice for agents to use written consent forms that state explicitly that the scope of consent includes consent to search computers and other electronic storage devices.”⁶⁰

If, however, the computer or particular files are password-protected with a password that the third party has not been given access to, the third party cannot consent to the search of the protected computer or its protected files.⁶¹ For instance, assuming that SPC Green had permission to use SPC Doe’s computer and assuming that SPC Doe’s computer and its files are not password-protected, SPC Green can consent to the search of his roommate’s computer.⁶² If, however, some of the files are password-protected, SPC Green can only give Special Agent (SA) Zimmerman limited consent to search those files that are not protected.⁶³ A better option is for SA Zimmerman to receive SPC Doe’s full consent to search the computer and all of its files.⁶⁴

3. Plain View

The plain view doctrine⁶⁵ provides that “[law enforcement officials] are acting within the scope of their authority, and . . . they have probable cause to believe the item is contraband or evidence of a crime.”⁶⁶ With respect to computer cases, plain view scenarios arise in one of two ways.⁶⁷ The first is when an officer lawfully searches an area and sees evidence of a crime left on an open computer screen, and the second is when investigators lawfully search a computer for evidence of one crime and find evidence regarding a different crime.⁶⁸

⁵² A new authorization is advised if there is a lapse in time from the original search because “the authorization should be executed within 10 days after the date of issue.” AR 27-10, *supra* note 36, para. 8-10.

⁵³ CASEY, *supra* note 2, at 87–88; *see also* Lyon Presentation, *supra* note 30.

⁵⁴ MCM, *supra* note 31, MIL. R. EVID. 314 (e).

⁵⁵ DAVID A. SCHLUETER, MILITARY CRIMINAL JUSTICE: PRACTICE AND PROCEDURE 257 (Ethan Shaw & Heidi Litman eds., 7th ed. 2008) (citing various cases). Military courts defer to an agent relying on a third party’s “apparent authority to provide consent.” *Id.* *See also* MARAS, *supra* note 10, at 85; *see also* CLANCY, *supra* note 20, at 152.

⁵⁶ DESKBOOK, *supra* note 35, at N-23 (referencing a number of cases, e.g., *Ohio v. Robinette*, 519 U.S. 33, 40 (1996)); *see also* *Schneckloth v. Bustamonte* 412 U.S. 218, 248 (1973).

⁵⁷ MCM, *supra* note 31, MIL. R. EVID. 314(e)(1) analysis, at A22-27 (“The basic rule for consent searches is taken from *Schneckloth v. Bustamonte*, 412 U.S. 218 (1973).”; *see also* MARAS, *supra* note 10, at 84.

⁵⁸ MCM, *supra* note 31, MIL. R. EVID. 314(e)(5).

⁵⁹ MARAS, *supra* note 10, at 86.

⁶⁰ SEARCHING AND SEIZING COMPUTERS, *supra* note 3, at 19. *See infra* Appendix B.

⁶¹ SCHLUETER, *supra* note 55, at 256–58; *see also* MARAS, *supra* note 10, at 86.

⁶² SCHLUETER, *supra* note 55, at 256–58; *see* *United States v. Rader*, 65 M.J. 30 (C.A.A.F. 2007); *see also* MARAS, *supra* note 10, at 86.

⁶³ MARAS, *supra* note 10, at 86.

⁶⁴ Sometimes obtaining consent is impractical because consent may alert an accused of a pending investigation and result in obstruction of evidence. FM 3-19.13, *supra* note 8, para. 11-13.

⁶⁵

[P]lain view doctrine n. the rule that a law enforcement officer may make a search and seizure without obtaining a search warrant if evidence of criminal activity or the product of a crime can be seen without entry or search. Example: a policeman stops a motorist for a minor traffic violation and can see in the car a pistol or a marijuana plant on the back seat, giving him ‘reasonable cause’ to enter the vehicle to make a search.

Plain View Doctrine Definition, FREE DICTIONARY BY FARLEX, <http://legal-dictionary.thefreedictionary.com/Plain+View+Doctrine> (last visited Feb. 28, 2013) (emphasis removed).

⁶⁶ *United States v. Washington*, No. 20100961 2011 WL 498325 (A. Ct. Crim. App. Feb. 8, 2011) (unpublished) (quoting *United States v. Fogg*, 52 M.J. 144 (C.A.A.F. 1999)).

⁶⁷ SEARCHING AND SEIZING COMPUTERS, *supra* note 3, at 34.

⁶⁸ *Id.* at 34.

While some courts differ in their application of the plain view doctrine to computer searches,⁶⁹ military courts have a fairly mainstream view regarding seizure of electronic evidence pursuant to the plain view doctrine. For instance in *United States v. Washington*, while searching for photos and videos of a specific rape victim, the agent found unrelated images of child pornography. The Army Court of Criminal Appeals (ACCA) found that the agent had proper authorization to open images during his search and that his discovery of evidence related to a different crime constituted plain view.⁷⁰

In the hypothetical case referenced in the introduction, SPC Green was not an “officer” or agent of the government, so his discovery did not constitute “plain view” of the suspected illegal content.⁷¹ Had the facts been different, the search and seizure may have been permissible pursuant to the plain view doctrine. If, for instance, a military police officer was called to the Soldiers’ barracks room to break up a fight between SPC Green and SPC Doe, and while breaking up the fight the officer saw SPC Doe’s computer screen displaying images of child pornography, he would not need a search authorization to further examine the image.⁷² However, it is advised that any further search of the computer files be pursuant to a search authorization based on the image in plain view.⁷³

⁶⁹ MARAS, *supra* note 10, at 87–88. In the past the 10th Circuit’s more restrictive application of the plain view doctrine has since been further clarified by developing case law. In subsequent cases, the 10th Circuit has noted that the more narrow caselaw was very fact specific. SEARCHING AND SEIZING COMPUTERS, *supra* note 3, at 36; *see also* DESKBOOK, *supra* note 35, at N-8. *See infra* Appendices C and D.

⁷⁰ *Washington*, 2011 WL 498325. In *Washington* the Court explains that the Supreme Court established three prongs that comprise the “plain view” test: (1) the officer must lawfully be on the premises, (2) the criminality of the evidence must be “immediately apparent,” and (3) “the officer must also have a lawful right of access to the object itself.” (citing *Horton v. California*, 496 U.S. 128, 136–37 (1990)); *see also* DESKBOOK, *supra* note 35, at N-8.

⁷¹ SEARCHING AND SEIZING COMPUTERS, *supra* note 3, at 34; *see also* MARAS, *supra* note 10, at 87.

⁷² An example of military case involving plain view is *United States v. Tanksley*, in which the accused was suspected of sexual offenses against minors. 54 M.J. 169 (C.A.A.F. 2000). The accused left an office document open on his computer and left the computer on. Later a judge advocate (JA) went to the accused’s office and found the open document that referenced the allegations against the accused. The JA printed the document and seized the disk that was inside the computer. In spite of the accused’s objection, the court allowed such seizure under the plain view doctrine, noting, “appellant forfeited any expectation of privacy he might have enjoyed by leaving the document in plain view on a computer screen in an unsecured room.” *Id.* at 172. The analysis by the court stresses that the seized document in this case was “exculpatory.” *Id.* Therefore there may be a different outcome with similar facts involving an “inculpatory” document. *Id.* *See also* SCHLUETER, *supra* note 55, at 254.

⁷³ The CID trains its agents that, “[i]f during the conduct of a search for one offense, evidence of an unrelated or different type of offense is identified, the scope of the search authorization must be expanded accordingly.” FM 3-19.13, *supra* note 8, para. 11-13.

4. Exigent Circumstances

A third commonly used exception to the search authorization is when law enforcement personnel are faced with “exigent circumstances.”⁷⁴ Searches under exigent circumstances still require probable cause,⁷⁵ but a warrant or search authorization is not required because obtaining the warrant under these circumstances could lead to imminent destruction of evidence⁷⁶ through physical damage to the computer or deletion of computer files.⁷⁷

For instance, adding some facts to the introductory fact pattern, authorities searched the room pursuant to a search authorization, but at the time that they had the authorization, had no reason to believe that there was evidence of a crime in the accused’s vehicle, and thus did not seek authorization to search the vehicle. While searching the room, authorities learned from a reliable witness⁷⁸ that the accused kept several digital video discs (DVDs) and CDs locked in the trunk of his car.

Now presume that nothing of evidentiary value was found during the course of the search of SPC Doe’s room. Special Agent Zimmerman asked SPC Doe if he could search his vehicle, and received written consent to search. During the search, SA Zimmerman asked if he could seize the CDs and DVDs that he found in a duffel bag in the trunk of SPC Doe’s vehicle, but SPC Doe refused. Special Agent Zimmerman believed that he did not have time to seek authorization to search the accused’s vehicle because he feared that if he left the scene to obtain authorization, the accused may destroy or alter the digital storage devices. Seizure in this case is most likely going to be found permissible due to exigent circumstances.⁷⁹ Practitioners should be aware that after a seizure of these digital storage devices, a best practice is for law enforcement personnel to obtain authorization to search the contents of the seized storage media.⁸⁰

⁷⁴ *See* CASEY, *supra* note 2, at 87–88.

⁷⁵ MCM, *supra* note 31, MIL. R. EVID. 315(g).

⁷⁶ SEARCHING AND SEIZING COMPUTERS, *supra* note 3, at 28. While there are other circumstances that may result in exigencies, a circumstance in which “the evidence is in imminent danger of destruction—is generally the most relevant in the context of computer searches.” *Id.*

⁷⁷ MARAS, *supra* note 10, at 84.

⁷⁸ MCM, *supra* note 31, MIL. R. EVID. 315(f)(3)(D).

⁷⁹ *See* MARAS, *supra* note 10, at 84.

⁸⁰ *Id.*; SEARCHING AND SEIZING COMPUTERS, *supra* note 3, at 30.

B. Digital Evidence from Third Parties—Service Providers

1. Introduction

Another factor that trial counsel must consider during an investigation is that sometimes the evidence or potential evidence is controlled not by the accused, but by service providers, including e-mail companies, phone companies, and financial institutions.⁸¹ As previously mentioned, “[w]henver investigators seek stored email [sic], account records, or subscriber information from . . . service providers, they must comply with the SCA/ECPA.”⁸² These stored e-mails may be retained by either electronic communication service providers or by remote computing service providers.⁸³ “An electronic communication service (‘ECS’) is ‘any service which provides to users . . . the ability to send or receive wire or electronic communications,’”⁸⁴ while “a remote computing service is provided by an off-site computer that stores or processes data for a customer.”⁸⁵

2. Compelled and Voluntary Disclosure

The government can seek information from public and non-public service providers⁸⁶ through two different means: compelled disclosure, regulated by 18 U.S.C. § 2703, and voluntary disclosure, regulated by 18 U.S.C. § 2702.⁸⁷ The government can compel disclosure of information in five ways: (1) through use of a subpoena; (2) through use of a subpoena with notice; (3) with a § 2703 (d) court order; (4) with a § 2703 court order with notice; and (5) through use of search warrant.⁸⁸

These five options for compelled disclosure provide access to different types of content and non-content information.⁸⁹ A subpoena without notice to the subscriber may compel service providers to release a limited amount of information regarding a customer’s identity and basic connection records.⁹⁰ A § 2703(d) court order may compel more detailed information than a subpoena would, including account activity logs with Internet Protocol (IP) addresses; contact lists; and cell-site location information.⁹¹ This mechanism will not usually compel disclosure of content information which is subject to additional protections.⁹² A subpoena or § 2703(d) court order with prior notice will usually compel “retrieved communications, unretrieved communications older than 180 days, and other files stored with a public provider.”⁹³ If prior notice is given to a subscriber, a § 2703 court order can also be used to compel “unretrieved communications older than 180 days.”⁹⁴

A search warrant will yield both content and non-content information associated with an account, without putting the subscriber of the account on notice of the content’s release, and consequently on notice of the investigation.⁹⁵ Reasons for proceeding with the first two options to obtain information from the internet service providers as opposed to the broader reaching warrant include the practical benefit that, “the legal threshold for issuing a subpoena is low,”⁹⁶ and the § 2703(d) standard is also lower than that required by a warrant.⁹⁷ It may be wisest to proceed in an investigation with a subpoena at the preliminary stages, followed by a search authorization when content-information is sought.

⁸¹ See Lyon Presentation, *supra* note 30.

⁸² CLANCY, *supra* note 20, at 269. One of the first steps of ensuring compliance with the ECPA/SCA is to determine whether the holder of the records qualifies as either an Electronic Communication Service (ECS) or a Remote Computing Service (RCS). SEARCHING AND SEIZING COMPUTERS, *supra* note 3, at 116; see generally Orin S. Kerr, *A User’s Guide to the Stored Communications Act—And a Legislator’s Guide to Amending It*, 72 GEO. WASH. L. REV. 1208 (2004).

⁸³ SEARCHING AND SEIZING COMPUTERS, *supra* note 3, at 117.

⁸⁴ *Id.*

⁸⁵ *Id.* at 119.

⁸⁶ *Id.* at 115–50.

⁸⁷ 18 U.S.C. §§ 2702, 2703 (2011); CLANCY, *supra* note 20, at 288–91. Anyone who “obtains, alters, or prevents authorized access” to protected communications can suffer criminal penalties. SEARCHING AND SEIZING COMPUTERS, *supra* note 3 at 115. See also Kerr, *supra* note 82, at 1218.

⁸⁸ SEARCHING AND SEIZING COMPUTERS, *supra* note 3, at 127; see also Kerr, *supra* 82, at 1218–19; see also Lyon Presentation, *supra* note 30.

⁸⁹ SEARCHING AND SEIZING COMPUTERS, *supra* note 3, at 127. “Content data are the spoken words in a conversation or the words written in a message (through either texting or e-mail).” MARAS, *supra* note 10, at 52 (emphasis omitted). “Non-content data include, but are not limited to, telephone numbers dialed, customer information (name and address), and e-mail addresses of the message sender and recipient.” *Id.*

⁹⁰ SEARCHING AND SEIZING COMPUTERS, *supra* note 3, at 128.

⁹¹ PROSECUTORS, *supra* note 5, at 4–5.

⁹² *Id.*

⁹³ *Id.* at 3, 5–6. SEARCHING AND SEIZING COMPUTERS, *supra* note 3, at 128–33. “NOTE: Because providers may use different terms to describe the types of data they hold, it is advisable to consult with each provider on its preferred language” PROSECUTORS, *supra* note 5, at 3.

⁹⁴ PROSECUTORS, *supra* note 5, at 5.

⁹⁵ SEARCHING AND SEIZING COMPUTERS, *supra* note 3, at 133.

⁹⁶ *Id.* at 128 (referencing *United States v. Morton Salt Co.*, 338 U.S. 632, 642–43 (1950)).

⁹⁷ *Id.*

As a practical matter trial counsel may conserve time and resources by becoming familiar with the major internet service providers' basic requirements to see what each company requires for release of information because § 2702 voluntary disclosure may yield positive results without compelling the companies to disclose the requested information.⁹⁸

3. Additional Considerations

In cases where notice will likely adversely affect an investigation, and in cases where notice will endanger an individual's life or safety, notice of disclosure may be delayed.⁹⁹ In instances involving subpoenas, a supervisor must certify in writing that notice will result in an "adverse result,"¹⁰⁰ while in instances involving a § 2703(d) court order, delayed notice requires permission from the court.¹⁰¹ When permitted, notice will be delayed for ninety days.¹⁰²

Trial counsel and investigators should consider options to preserve evidence while gathering records from service providers, so that it is not lost or manipulated during the course of the investigation. One way to preserve evidence is through the use of an order to service providers to "freeze" existing records and information.¹⁰³ The "SCA permits the government to direct providers to 'freeze' stored records and communications that contain content and non-content information, pursuant to 18 U.S.C. § 2703(f)."¹⁰⁴ Another way to preserve evidence is through a court order prohibiting the service provider from disclosing "existence of a warrant, subpoena, or court order," in accordance with 18 U.S.C. § 2705(b).¹⁰⁵ This tool can be used when notification will endanger someone's life or safety; cause the suspect to flee; compromise the evidence; result in witness intimidation; or seriously jeopardize an investigation.¹⁰⁶

Because SPC Doe is aware of the investigation against him, investigators should consider that he might take steps to

⁹⁸ See *id.* at 135, 139.

⁹⁹ 18 U.S.C. § 2705(a) (2011); PROSECUTORS, *supra* note 5, at 6.

¹⁰⁰ 18 U.S.C. § 2705(a)(1)(B); PROSECUTORS, *supra* note 5, at 6.

¹⁰¹ 18 U.S.C. § 2705(a)(1)(A); PROSECUTORS, *supra* note 5, at 6.

¹⁰² 18 U.S.C. § 2705(a)(1); PROSECUTORS, *supra* note 5, at 6.

¹⁰³ SEARCHING AND SEIZING COMPUTERS, *supra* note 3, at 139. CLANCY, *supra* note 20, at 304.

¹⁰⁴ 18 U.S.C. § 2703(f); SEARCHING AND SEIZING COMPUTERS, *supra* note 3, at 139; see also Lyon Presentation, *supra* note 30.

¹⁰⁵ 18 U.S.C. § 2705(b); SEARCHING AND SEIZING COMPUTERS, *supra* note 3, at 140–41. See also CLANCY, *supra* note 20, at 304.

¹⁰⁶ 18 U.S.C. § 2705(b); SEARCHING AND SEIZING COMPUTERS, *supra* note 3, at 141.

prevent the government from accessing information from his service providers. Therefore, the government should immediately contact his service providers and order them to freeze his records.¹⁰⁷ Then the government should also communicate with the service providers to learn about their requirements for release of the desired information.¹⁰⁸ Doing so may result in release of evidence that will assist as the investigation continues to develop. Finally, because the government will have additional time once the records are frozen, the government should issue a detailed search authorization to serve upon the service provider to gain any additional evidence desired.¹⁰⁹

IV. Using Digital Evidence in Court

In addition to being familiar with definitions, and the rules and practice of obtaining digital evidence, military practitioners must be familiar with rules surrounding the use of digital evidence in the courtroom. Authentication, hearsay, and expert issues oftentimes arise in digital evidence cases.

A. Authentication

As in using any form of evidence in court, counsel introducing evidence must first show that the evidence is relevant¹¹⁰ and must then authenticate the evidence in accordance with Military Rule of Evidence (MRE) 901¹¹¹ to show that the evidence is reliable.¹¹² To authenticate an

¹⁰⁷ 18 U.S.C. § 2703(f); SEARCHING AND SEIZING COMPUTERS, *supra* note 3, at 139; Lyon Presentation, *supra* note 30.

¹⁰⁸ SEARCHING AND SEIZING COMPUTERS, *supra* note 3.

¹⁰⁹ See Lyon Presentation, *supra* note 30.

¹¹⁰ "Relevant evidence" means evidence having any tendency to make the existence of any fact that is of consequence to the determination of the action more probable or less probable than it would be without the evidence." MCM, *supra* note 31, MIL. R. EVID. 401.

¹¹¹ "The requirement of authentication or identification as a condition precedent to admissibility is satisfied by evidence sufficient to support a finding that the matter in question is what its proponent claims." *Id.* MIL. R. EVID. 901.

¹¹² RIEDY ET AL., *supra* note 14, at 188.

Authentication means satisfying the court that (a) the contents of the record have remained unchanged, (b) that the information in the record does in fact originate from its purported source, whether human or machine, and (c) that extraneous information such as the apparent date of the record is accurate. As with paper records, the necessary degree of authentication may be proved through oral and circumstantial evidence, if available, or via technological features in the system or the record.

exhibit, a witness must convey “personal knowledge”¹¹³ of the exhibit. Keep in mind that authentication does not proffer the content of the document to be true, but instead confirms that the document is what the offering party claims it to be.¹¹⁴

1. Digital Storage Devices

With respect to SPC Doe’s case, to authenticate thumbdrive #3 taken from SPC Doe’s barracks room, SA Zimmerman testifies that he recognizes thumbdrive #3 as the thumbdrive he collected from SPC Doe’s room. He testifies that on X date he collected an orange, 16-gigabyte Memorex thumbdrive from barracks room #214 and placed it into a brown paper bag that he labeled “Thumbdrive #3, RAZ” in black marker before securing it in the evidence locker. He testifies that he recognizes the paper bag and the handwriting on the bag as his own, that he wrote the words on the bag, and that “RAZ” are his initials. He also testifies that the orange thumbdrive and the paper bag appear the same as they did on the day that he collected the evidence, save for the fact that the tape used to secure the bag on which he wrote his initials was ripped.

While SA Zimmerman is a skilled CID agent, he lacks knowledge in the area of digital forensic examinations. Therefore a digital forensic examiner, SA Gonzalez, is called to authenticate the photographs and videos that SA Gonzalez found on the thumbdrive during his forensic examination. Special Agent Gonzalez testifies that on X date he met with SA Zimmerman and retrieved a paper bag marked with the initials “RAZ,” both agents properly documenting the exchange of evidence on the chain of custody document. Special Agent Gonzales testifies that he took the bag to the digital examination room where he carefully opened the bag, breaking the tape marked “RAZ.” He testifies that he used Acmenats software to conduct his forensic examination and that in the midst of the examination he discovered images containing what he believes is child pornography. He verifies the images that the prosecutor displays on the projection screen as those images that he found during his examination of the thumbdrive and confirms that they are in the same condition as the images that he saw on the date of the forensic examination.¹¹⁵

CASEY, *supra* note 2, at 50–51 (quoting Chris Reed, *The Admissibility and Authentication of Computer Evidence—A Confusion of Issues*, 6 COMPUTER L. & SECURITY REV., no. 2, July–Aug. 1990, at 13–16).

¹¹³ PAUL R. RICE, ELECTRONIC EVIDENCE: LAW AND PRACTICE 336 (David Sluis, 2d ed. 2008).

¹¹⁴ Lyon Presentation, *supra* note 30 (citing *City of Vista v. Sutro & Co.*, 52 Cal. App. 4th 401, 411–12 (1997)).

¹¹⁵ See DAVID A. SCHLUETER ET AL., MILITARY EVIDENTIARY FOUNDATIONS 153 (Ethan Shaw et al. eds., 4th ed. 2010).

2. E-mails and Text Messages

Authentication of e-mails and text messages may be established through “personal knowledge and circumstantial indicia of authenticity” by a witness testifying as to sending or receiving the communication.¹¹⁶ Other avenues that may establish authenticity of text messages or e-mail include a witness’s familiarity with the following: a particular e-mail address from where the communication was sent; little-known information contained in the e-mail; or a “communication’s storage and retrieval systems.”¹¹⁷ For instance, if neither the sender nor recipient of an e-mail is willing or able to testify about sending or receiving the e-mail, an employee of the service provider may be able to establish authenticity by testifying that an e-mail or text message was sent from one specific address to another specific address at a certain date and time.¹¹⁸

While an expert witness is not required to authenticate the digital storage devices, or even the digital evidence,¹¹⁹ one is oftentimes used to authenticate the digital evidence (contents on computer hard drives and electronic storage devices) because of his specialized knowledge and ability to convey that knowledge to a layperson¹²⁰ and because he can testify that a computer was in proper working condition.¹²¹

3. Digital Files

Digital files found on removable storage devices and computer hard drives must also be authenticated in court.¹²² This can be done through a “two-step process.”¹²³ First, a chain of custody must be established and then a “forensic identifier” or “hash value” is used to show that the evidence is what it is purported to be.¹²⁴ If using an expert in the authentication process, trial counsel must remember that “[t]he computer forensics investigator needs to be viewed as a credible witness to ensure that the validity and reliability of the electronic evidence and its handling are upheld in court.”¹²⁵ These expert witnesses generally are the experts

¹¹⁶ RIEDY ET AL., *supra* note 14, at 188.

¹¹⁷ *Id.* at 188–89. Lyon Presentation, *supra* note 30. See also PROSECUTORS, *supra* note 5, at 31.

¹¹⁸ RIEDY ET AL., *supra* note 14, at 189.

¹¹⁹ MARAS, *supra* note 10, at 330.

¹²⁰ See *id.* at 331.

¹²¹ See *id.*

¹²² RICE, *supra* note 113, at xx (“Litigation involving electronic evidence will involve the same evidentiary issues as litigation in other contexts.”).

¹²³ SEARCHING AND SEIZING COMPUTERS *supra* note 3, at 199.

¹²⁴ *Id.*

¹²⁵ MARAS, *supra* note 10, at 331.

who conduct the forensic examination of the computer and can testify about their involvement in the collection, analysis, and evaluation of the evidence.¹²⁶

One of the most common types of digital files used in military courts involves digital images of child pornography that the accused downloaded.¹²⁷ To authenticate these images, the trial counsel must introduce the witnesses involved in collecting the evidence to establish a chain of custody.¹²⁸ To demonstrate reliability, “[e]ach person in the chain of custody should testify that he or she did not access or change the images.”¹²⁹

4. Chat Logs

With respect to internet relay chats (IRCs), trial counsel can authenticate the chat logs by presenting evidence about how the logs were created, that the logs are an accurate representation of the chat room conversations, and by further linking the parties involved to the screen names used during the conversation.¹³⁰ In *United States v. Tank*, the 9th Circuit found the chat logs were admissible because (1) a witness testified explaining the process he used to create chat logs with his computer and confirmed that the proposed chat log printouts were an accurate representation of the chat room conversations, (2) the accused admitted to using the screen name, and (3) others corroborated that the accused used the screen name.¹³¹ In SPC Doe’s case, the victim can confirm the details about the chats and can confirm the accuracy of the chat conversation while other means will likely need to be used to confirm SPC Doe’s link to the user name. For instance the service provider can testify that John Doe had an account registered with their company with user name X. Otherwise, an expert digital computer examiner may testify about the username being linked to SPC Doe’s computer.¹³²

¹²⁶ *Id.* at 325.

¹²⁷ Survey, *supra* note 11.

¹²⁸ RICE, *supra* note 113, at 361.

¹²⁹ *Id.*

¹³⁰ Lyon Presentation, *supra* note 30 (citing *United States v. Tank*, 200 F.3d 627 (9th Cir. 2000)).

¹³¹ *Tank*, 200 F.3d 627.

¹³² In military cases the CID agent responsible for collecting the evidence will usually first testify about collecting the computer and or other digital storage devices, before the expert digital forensic examiner. The digital forensic examiner is oftentimes a CID agent with specialized training in this area.

The computer forensics investigator has one of two roles in a . . . proceeding—as a technical witness or as an expert witness. As a technical witness, an individual can testify only as to the facts of the case, evidence, and procedures used. . . . as an expert witness, the individual can provide an opinion based

B. Hearsay

Another concern with proffering digital evidence in the courtroom is hearsay. “Digital evidence might not be admitted if it contains hearsay because the speaker or author of the evidence is not present in court to verify its truthfulness.”¹³³ An important practice tip is that computer-generated¹³⁴ evidence, such as “the login record of an ISP [(internet service provider)], automated telephone call records, and automatic teller receipts” are not hearsay “because they are not the statement of a person.”¹³⁵ In SPC Doe’s case, the chat logs, even after proper authentication, cannot be used to prove the truth of the contents in the chat logs. If the chat logs note, “it was wonderful meeting with you, Minor T, on 12 August 2012,” that content cannot be used to show that there was a meeting between Minor T and SPC Doe, but can be used to establish that SPC Doe had computer contact with Minor T.

When evaluating evidence for trial, a prosecutor should attempt to anticipate evidentiary problems and anticipate solutions. There are a number of exceptions that can be considered with respect to hearsay,¹³⁶ but the business records exception is the most common exception with

on the investigation conducted and the observations he or she made.

MARAS, *supra* note 10, at 335.

¹³³ CASEY, *supra* note 2, at 95. “Hearsay” is an out-of-court statement offered for the truth of the matter asserted. MCM, *supra* note 31, MIL. R. EVID. 801.

[I]n a prosecution for credit fraud, computer printouts related to the defendant’s account, kept by the collections department of the credit card company, would meet the core definition of hearsay because they would be offered to prove the truth of their contents. On the other hand, in a prosecution for online solicitation of a minor, the reply e-mails from the victim, if introduced simply to show contact between the defendant and victim rather than for the truth of their contents, would not meet the core definition of hearsay. They would be relevant for the fact that the defendant received them, not for what they say.

PROSECUTORS, *supra* note 5, at 29.

¹³⁴ “Computer-generated evidence consists of the direct output of computer programs.” PROSECUTORS, *supra* note 5, at 30.

¹³⁵ *Id.* at 30. If a computer-generated document is considered hearsay, some exceptions that should be considered include present-sense impression, Military Rule of Evidence (MRE) 803(1); public records, MRE 803(8); and residual exception, MRE 807. *Id.* at 36–37 (referencing federal rules of evidence as opposed to the military rules of evidence). See also CASEY, *supra* note 2, at 96–97. See also RIEDY ET AL., *supra* note 14, at 206 (noting the argument that there is “human activity . . . behind . . . the computer-generated data”).

¹³⁶ MCM, *supra* note 31, MIL. R. EVID. 803, 804; see also PROSECUTORS, *supra* note 5, at 29.

respect to “computer-stored”¹³⁷ records.¹³⁸ This exception requires that the proponent lay a foundation, establishing the trustworthiness of the records¹³⁹ by showing that they were kept in the ordinary course of business and that the regular practice of the business was to generate the evidence in question.¹⁴⁰

V. Conclusion

The world of digital evidence will continue to evolve and develop along with the evolution and development of new electronic devices, storage options, and storage capabilities.¹⁴¹ Practitioners must arm themselves with information necessary to litigate their current cases, and must continue to stay informed as new technology emerges.¹⁴² With the advent of new technology, law will change to reflect emerging issues that will affect evidence collection phase, pre-trial preparation, and trial.¹⁴³

After properly researching the Fourth Amendment, exceptions to the Fourth Amendment, statutes applicable to digital evidence, and rules for courts-martial, CPT Jones confidently represented the United States in its case against SPC John Doe. Her knowledge and preparation were evident when the court found SPC Doe guilty of all charges and specifications. Following the close of court, CPT Jones left the courtroom and listened to her voicemail messages. She had two messages; one from a company commander who suspects his Soldier of misconduct and one from a CID agent who is planning to interview the suspect.

¹³⁷ “Computer-stored” records are human-generated documents that are electronically stored. PROSECUTORS, *supra* note 5, at 30.

¹³⁸ *Id.* at 31.

¹³⁹ *Id.*

¹⁴⁰ MCM, *supra* note 31, MIL. R. EVID. 803(6).

¹⁴¹ See RIEDY ET AL., *supra* note 14, at 3–4.

¹⁴² *See id.*

¹⁴³ *See id.* See also RICE, *supra* note 113, at 492–94.

Appendix F

Sample Premises Computer Search Warrant Affidavit

This form may be used when a warrant is sought to allow agents to enter a premises and remove computers or electronic media from the premises. In this document, “[[” marks indicate places that must be customized for each affidavit. Fill out your district’s AO 93 Search Warrant form without any reference to computers; your agents are simply searching a premises for items particularly described in the affidavit’s attachment. Consider incorporating the affidavit by reference. See Chapter 2 for a detailed discussion of issues involved in drafting computer search warrants.

UNITED STATES DISTRICT COURT
FOR THE [DISTRICT]

_____)
In the Matter of the Search of) Case No.
[[Premises Address]])
_____)

AFFIDAVIT IN SUPPORT OF AN APPLICATION
UNDER RULE 41 FOR A WARRANT TO SEARCH AND SEIZE

I, [[AGENT NAME]], being first duly sworn, hereby depose and state as follows:

INTRODUCTION AND AGENT BACKGROUND

1. I make this affidavit in support of an application under Rule 41 of the Federal Rules of Criminal Procedure for a warrant to search the premises known as [[PREMISES ADDRESS]], hereinafter “PREMISES,” for certain things particularly described in Attachment A.

¹⁴³ SEARCHING AND SEIZING COMPUTERS, *supra* note 3, app. F.

2. I am a [[TITLE]] with the [[AGENCY]], and have been since [[DATE]]. [[DESCRIBE TRAINING AND EXPERIENCE INCLUDING EXPERTISE WITH COMPUTERS]].

3. This affidavit is intended to show only that there is sufficient probable cause for the requested warrant and does not set forth all of my knowledge about this matter.

PROBABLE CAUSE

4. [[Give facts that establish probable cause to believe that evidence, fruits, or contraband can be found on each computer that will be searched and/or seized, or to believe that the computers may be seized as contraband or instrumentalities.]]

TECHNICAL TERMS

5. [[THIS SECTION MIGHT BE UNNECESSARY; DEFINE ONLY TECHNICAL TERMS AS NECESSARY TO SUPPORT PROBABLE CAUSE.]] Based on my training and experience, I use the following technical terms to convey the following meanings:

a. IP Address: The Internet Protocol address (or simply “IP address”) is a unique numeric address used by computers on the Internet. An IP address looks like a series of four numbers, each in the range 0-255, separated by periods (e.g., 121.56.97.178). Every computer attached to the Internet computer must be assigned an IP address so that Internet traffic sent from and directed to that computer may be directed properly from its source to its destination. Most Internet service providers control a range of IP addresses. Some computers have static—that is, long-term—IP addresses, while other computers have dynamic—that is, frequently changed—IP addresses.

b. Internet: The Internet is a global network of computers and other electronic devices that communicate with each other. Due to the structure of the Internet, connections between devices on the Internet often cross state and international borders, even when the devices communicating with each other are in the same state.

COMPUTERS AND ELECTRONIC STORAGE

6. As described above and in Attachment A, this application seeks permission to search and seize records that might be found on the PREMISES, in whatever form they are found. I submit that if a computer or electronic

medium is found on the premises, there is probable cause to believe those records will be stored in that computer or electronic medium, for at least the following reasons:

a. Based on my knowledge, training, and experience, I know that computer files or remnants of such files can be recovered months or even years after they have been downloaded onto a hard drive, deleted or viewed via the Internet. Electronic files downloaded to a hard drive can be stored for years at little or no cost. Even when files have been deleted, they can be recovered months or years later using readily available forensics tools. This is so because when a person “deletes” a file on a home computer, the data contained in the file does not actually disappear; rather, that data remains on the hard drive until it is overwritten by new data.

b. Therefore, deleted files, or remnants of deleted files, may reside in free space or slack space—that is, in space on the hard drive that is not currently being used by an active file—for long periods of time before they are overwritten. In addition, a computer’s operating system may also keep a record of deleted data in a “swap” or “recovery” file.

c. Similarly, files that have been viewed via the Internet are typically automatically downloaded into a temporary Internet directory or “cache.” The browser often maintains a fixed amount of hard drive space devoted to these files, and the files are only overwritten as they are replaced with more recently viewed Internet pages or if a user takes steps to delete them.

d. [[FOR CHILD PORNOGRAPHY CASES]] I know from training and experience that child pornographers generally prefer to store images of child pornography in electronic form as computer files. The computer’s ability to store images in digital form makes a computer an ideal repository for pornography. A small portable disk or computer hard drive can contain many child pornography images. The images can be easily sent to or received from other computer users over the Internet. Further, both individual files of child pornography and the disks that contain the files can be mislabeled or hidden to evade detection. In my training and experience, individuals who view child pornography typically maintain their collections for many years and keep and collect items containing child pornography over long periods of time; in fact, they rarely, if ever, dispose of their sexually explicit materials.

e. [[FOR BUSINESS SEARCH CASES]] Based on actual inspection of [[spreadsheets, financial records, invoices]], I am aware that computer

equipment was used to generate, store, and print documents used in the [[tax evasion, money laundering, drug trafficking, etc.]] scheme. There is reason to believe that there is a computer system currently located on the PREMISES.

7. [[FOR CHILD PORNOGRAPHY OR OTHER CONTRABAND CASES]] In this case, the warrant application requests permission to search and seize [[images of child pornography, including those that may be stored on a computer]]. These things constitute both evidence of crime and contraband. This affidavit also requests permission to seize the computer hardware and electronic media that may contain those things if it becomes necessary for reasons of practicality to remove the hardware and conduct a search off-site. [[In this case, computer hardware that was used to store child pornography is a container for evidence, a container for contraband, and also itself an instrumentality of the crime under investigation.]]

8. [[FOR CHILD PORNOGRAPHY PRODUCTION CASES]] I know from training and experience that it is common for child pornographers to use personal computers to produce both still and moving images. For example, a computer can have a camera built in, or can be connected to a camera and turn the video output into a form that is usable by computer programs. Alternatively, the pornographer can use a digital camera to take photographs or videos and load them directly onto the computer. The output of the camera can be stored, transferred or printed out directly from the computer. The producers of child pornography can also use a scanner to transfer photographs into a computer-readable format. All of these devices, as well as the computer, constitute instrumentalities of the crime.

9. [[FOR HACKING OR OTHER INSTRUMENTALITY CASES]] I know that when an individual uses a computer to [[obtain unauthorized access to a victim computer over the Internet]], the individual's computer will generally serve both as an instrumentality for committing the crime, and also as a storage device for evidence of the crime. The computer is an instrumentality of the crime because it is used as a means of committing the criminal offense. The computer is also likely to be a storage device for evidence of crime. From my training and experience, I believe that a computer used to commit a crime of this type may contain: data that is evidence of how the computer was used; data that was sent or received; notes as to how the criminal conduct was achieved; records of Internet discussions about the crime; and other records that indicate the nature of the offense.

10. [[FOR CASES WHERE A RESIDENCE SHARED WITH OTHERS IS SEARCHED]] Because several people share the PREMISES as a residence, it is possible that the PREMISES will contain computers that are predominantly used, and perhaps owned, by persons who are not suspected of a crime. If agents conducting the search nonetheless determine that it is possible that the things described in this warrant could be found on those computers, this application seeks permission to search and if necessary to seize those computers as well. It may be impossible to determine, on scene, which computers contain the things described in this warrant.

11. Based upon my knowledge, training and experience, I know that searching for information stored in computers often requires agents to seize most or all electronic storage devices to be searched later by a qualified computer expert in a laboratory or other controlled environment. This is often necessary to ensure the accuracy and completeness of such data, and to prevent the loss of the data either from accidental or intentional destruction. Additionally, to properly examine those storage devices in a laboratory setting, it is often necessary that some computer equipment, peripherals, instructions, and software be seized and examined in the laboratory setting. This is true because of the following:

a. The volume of evidence. Computer storage devices (like hard disks or CD-ROMs) can store the equivalent of millions of pages of information. Additionally, a suspect may try to conceal criminal evidence; he or she might store it in random order with deceptive file names. This may require searching authorities to peruse all the stored data to determine which particular files are evidence or instrumentalities of crime. This sorting process can take weeks or months, depending on the volume of data stored, and it would be impractical and invasive to attempt this kind of data search on-site.

b. Technical requirements. Searching computer systems for criminal evidence sometimes requires highly technical processes requiring expert skill and properly controlled environment. The vast array of computer hardware and software available requires even computer experts to specialize in some systems and applications, so it is difficult to know before a search which expert is qualified to analyze the system and its data. In any event, however, data search processes are exacting scientific procedures designed to protect the integrity of the evidence and to recover even "hidden," erased, compressed, password-protected, or encrypted files. Because computer evidence is vulnerable to inadvertent or intentional modification or destruction (both from external

sources or from destructive code imbedded in the system as a “booby trap”), a controlled environment may be necessary to complete an accurate analysis.

12. In light of these concerns, I hereby request the Court’s permission to seize the computer hardware (and associated peripherals) that are believed to contain some or all of the evidence described in the warrant, and to conduct an off-site search of the hardware for the evidence described, if, upon arriving at the scene, the agents executing the search conclude that it would be impractical to search the computer hardware on-site for this evidence.

13. Searching computer systems for the evidence described in Attachment A may require a range of data analysis techniques. In some cases, it is possible for agents and analysts to conduct carefully targeted searches that can locate evidence without requiring a time-consuming manual search through unrelated materials that may be commingled with criminal evidence. In other cases, however, such techniques may not yield the evidence described in the warrant. Criminals can mislabel or hide files and directories, encode communications to avoid using key words, attempt to delete files to evade detection, or take other steps designed to frustrate law enforcement searches for information. These steps may require agents and law enforcement or other analysts with appropriate expertise to conduct more extensive searches, such as scanning areas of the disk not allocated to listed files, or peruse every file briefly to determine whether it falls within the scope of the warrant. In light of these difficulties, the [[AGENCY]] intends to use whatever data analysis techniques appear necessary to locate and retrieve the evidence described in Attachment A.

14. [[INCLUDE THE FOLLOWING IF THERE IS A CONCERN ABOUT THE SEARCH UNREASONABLY IMPAIRING AN OPERATIONAL, OTHERWISE LEGAL BUSINESS]] I recognize that the Company is a functioning company with many employees, and that a seizure of the Company’s computers may have the unintended effect of limiting the Company’s ability to provide service to its legitimate customers. In response to these concerns, the agents who execute the search anticipate taking an incremental approach to minimize the inconvenience to the Company’s legitimate customers and to minimize the need to seize equipment and data. It is anticipated that, barring unexpected circumstances, this incremental approach will proceed as follows:

a. Upon arriving at the PREMISES, the agents will attempt to identify a system administrator of the network (or other knowledgeable employee) who will be willing to assist law enforcement by identifying, copying, and printing out paper and electronic copies of the things described in the warrant. The assistance of such an employee might allow agents to place less of a burden on the Company than would otherwise be necessary.

b. If the employees choose not to assist the agents, the agents decide that none are trustworthy, or for some other reason the agents cannot execute the warrant successfully without themselves examining the Company's computers, the agents will attempt to locate the things described in the warrant, and will attempt to make electronic copies of those things. This analysis will focus on things that may contain the evidence and information of the violations under investigation. In doing this, the agents might be able to copy only those things that are evidence of the offenses described herein, and provide only those things to the case agent. Circumstances might also require the agents to attempt to create an electronic "image" of those parts of the computer that are likely to store the things described in the warrant. Generally speaking, imaging is the taking of a complete electronic picture of the computer's data, including all hidden sectors and deleted files. Imaging a computer permits the agents to obtain an exact copy of the computer's stored data without actually seizing the computer hardware. The agents or qualified computer experts will then conduct an off-site search for the things described in the warrant from the "mirror image" copy at a later date. If the agents successfully image the Company's computers, the agents will not conduct any additional search or seizure of the Company's computers.

c. If imaging proves impractical, or even impossible for technical reasons, then the agents will seize those components of the Company's computer system that the agents believe must be seized to permit the agents to locate the things described in the warrant at an off-site location. The seized components will be removed from the PREMISES. If employees of the Company so request, the agents will, to the extent practicable, attempt to provide the employees with copies of data that may be necessary or important to the continuing function of the Company's legitimate business. If, after inspecting the computers, the analyst determines that some or all of this equipment is no longer necessary to retrieve and preserve the evidence, the government will return it within a reasonable time.

CONCLUSION

15. I submit that this affidavit supports probable cause for a warrant to search the PREMISES and seize the items described in Attachment A.

REQUEST FOR SEALING

[[IF APPROPRIATE: It is respectfully requested that this Court issue an order sealing, until further order of the Court, all papers submitted in support of this application, including the application and search warrant. I believe that sealing this document is necessary because the items and information to be seized are relevant to an ongoing investigation into the criminal organizations as not all of the targets of this investigation will be searched at this time. Based upon my training and experience, I have learned that, online criminals actively search for criminal affidavits and search warrants via the Internet and disseminate them to other online criminals as they deem appropriate, i.e., post them publicly online through the carding forums. Premature disclosure of the contents of this affidavit and related documents may have a significant and negative impact on the continuing investigation and may severely jeopardize its effectiveness.]]

Respectfully submitted,

[[AGENT NAME]]

Special Agent

[[AGENCY]]

Subscribed and sworn to before me on _____:

UNITED STATES MAGISTRATE JUDGE

ATTACHMENT A

1. All records relating to violations of the statutes listed on the warrant and involving [[SUSPECT]] since [[DATE]], including:

- a. [[IDENTIFY RECORDS SOUGHT WITH PARTICULARITY; EXAMPLES FOR A DRUG CASE FOLLOW]];
- b. lists of customers and related identifying information; types, amounts, and prices of drugs trafficked as well as dates, places, and amounts of specific transactions;
- c. any information related to sources of narcotic drugs (including names, addresses, phone numbers, or any other identifying information);
- d. any information recording [[SUSPECT]]'s schedule or travel from 2008 to the present;
- e. all bank records, checks, credit card bills, account information, and other financial records.

2. [[IF OFFENSE INVOLVED A COMPUTER AS AN INSTRUMENTALITY OR CONTAINER FOR CONTRABAND]] Any computers or electronic media that were or may have been used as a means to commit the offenses described on the warrant, including [[receiving images of child pornography over the Internet in violation of 18 U.S.C. § 2252A.]]

3. For any computer hard drive or other electronic media (hereinafter, "MEDIA") that is called for by this warrant, or that might contain things otherwise called for by this warrant:

- a. evidence of user attribution showing who used or owned the MEDIA at the time the things described in this warrant were created, edited, or deleted, such as logs, registry entries, saved usernames and passwords, documents, and browsing history;
- b. passwords, encryption keys, and other access devices that may be necessary to access the MEDIA;
- c. documentation and manuals that may be necessary to access the MEDIA or to conduct a forensic examination of the MEDIA.

4. [[IF CASE INVOLVED THE INTERNET]] Records and things evidencing the use of the Internet Protocol address [[e.g. 10.19.74.69]]

to communicate with [[e.g. Yahoo! mail servers or university mathematics department computers]], including:

- a. routers, modems, and network equipment used to connect computers to the Internet;
- b. records of Internet Protocol addresses used;
- c. records of Internet activity, including firewall logs, caches, browser history and cookies, “bookmarked” or “favorite” web pages, search terms that the user entered into any Internet search engine, and records of user-typed web addresses.

As used above, the terms “records” and “information” include all of the foregoing items of evidence in whatever form and by whatever means they may have been created or stored, including any form of computer or electronic storage (such as hard disks or other media that can store data); any handmade form (such as writing, drawing, painting); any mechanical form (such as printing or typing); and any photographic form (such as microfilm, microfiche, prints, slides, negatives, videotapes, motion pictures, photocopies).

Appendix B

Samples (1–4) of Consent to Search¹⁴⁴



SPECIAL REPORT / JAN. 07

Sample 1: Consent to Search

(Adapted from Maine Computer Crimes Task Force Consent-to-Search Form)

I hereby give my consent and permission for the items described below to be searched by law enforcement officer _____, and by any law enforcement officer of the _____ [insert name of task force or agency].

I hereby state that I myself have the authority and the ability to gain access to, possess, inspect, examine, and search the items described below.

I understand that I have the right to refuse to give my consent to search the items described below. I give my consent to this search voluntarily and as an act of my own free will, and not because of any threats, compulsion, promises, or inducements. I further state that no threats or promises have been made to compel or induce me to sign this consent form.

I understand that any items, images, documents, or other evidence discovered pursuant to a search of the items described below may be used as evidence in a court of law.

Items to be searched (description, serial numbers, etc.):

By signing this form, I hereby declare that I have read and understood its contents entirely.

Signature

Date

Witnessed by:

Witness/Law Enforcement Officer

Date

144 PROSECUTORS, supra note 5, at 66–69.

Sample 2: Consent to Search

I, _____, hereby consent to search of the following locations, vehicles, and articles by Agents of _____ *(insert name of task force or agency)* or other local, State, or Federal law enforcement personnel.

Home/Business Address(s)

1.) _____ 2.) _____

This consent extends to any and all yards, garages, carports, outbuildings, storage areas, sheds, trash containers, or mailboxes assigned to the above listed premises.

Initials

Vehicle(s)

Make/Model _____

Year/License _____

Make/Model _____

Year/License _____

I understand that this consent includes authorization to remove all computers, hard drives, and other electronic storage media (CDs, DVDs, floppy discs, Zip® discs, Jaz® cartridges, Smart Media Cards, Compact Flash, Memory Sticks, etc.) for examination offsite at a secure facility using appropriate tools and techniques.

Initials

This consent is freely and voluntarily given. I have not been coerced or threatened, nor have any promises been made regarding my cooperation in this investigation.

 Signature

 Date

 Witness/Law Enforcement Officer

 Date

Sample 3: Supplemental Consent to Search

To assist agents of the _____ *[insert name of task force or agency]*, or other local, State, or Federal law enforcement personnel with their search of computers, hard drives, and other electronic storage media seized with my consent, I am providing the following information:

Screen Saver/BIOS Password

Other Passwords/Username

Program/Service	Username	Password

Encryption Keys

Public Key	Private Key

Initials

Appendix C

Plain View in the Digital Context¹⁴⁵

PLAIN VIEW IN THE DIGITAL CONTEXT

“PURE” PLAIN VIEW [Majority View]

An agent can look at EVERY file on a computer when searching for evidence. This is “pure” plain view – any file on a computer is plainly viewable and can be opened.

United States v. Upham, 168 F.3d 532 (1st Cir. 1999)

United States v. Highbarger, 380 Fed. Appx. 127 (3rd Cir. 2010)(unpublished)

United States v. Williams, 592 F.3d 511 (4th Cir. 2010)

Warning: officers must conduct these searches with “care and respect for privacy.”

United States v. Mann, 592 F.3d 779 (7th Cir. 2010)

United States v. Miranda, 325 Fed. Appx. 858 (11th Cir. 2009)(unpublished)(per curiam)

United States v. Whaley, 415 Fed. Appx. 129 (11th Cir. 2011)(unpublished)(per curiam)

“PROCEED WITH CAUTION”

Subjective Intent Approach

Plain View does NOT apply when evidence indicates that the **subjective intent** of the agent was to uncover unauthorized evidence. Therefore, agents must have a purpose for opening each file. If the agent finds a file containing another criminal act, the agent must abide by the rules for **Stop & Ask**.

United States v. Carey, 172 F.3d 1268 (10th Cir. 1999)

United States v. Osorio, 66 M.J. 632 (A.F.C.C.A. 2008)

“[T]here must be specificity in the scope of the warrant which, in turn, mandates specificity in the process of conducting the search. Practitioners must generate specific warrants and search processes necessary to comply with that specificity and then, if they come across evidence of a different crime, stop their search and seek a new authorization.” *Id.* at 637.

“Stop & Ask” Approach

An agent can open any file **BUT** when he discovers something criminal which is outside of the scope of the warrant, he must **stop** and **ask** for a new warrant.

United States v. Lucas, 640 F.3d 168 (6th Cir. 2011)

United States v. Koch, 625 F.3d 470 (8th Cir. 2010)

United States v. Walsler, 275 F.3d 981 (10th Cir. 2001)

Search Protocols Approach

Agents need to have limitations on their search. Agents should follow protocols and tailor searches to the objective of the warrant.

In *Burgess*, the court set forth some protocols:

- (1) analyze the file structures first;
- (2) look at suspicious file folders;
- (3) use keyword searches to look for folders/files that would most likely contain objects of the search;
- (4) might be able to look into some or all folders/files in order to find objects.

United States v. Otero, 563 F.3d 1127 (10th Cir. 2009) (warrants must affirmatively limit searches)

United States v. Burgess, 576 F.3d 1078 (10th Cir. 2009) (the search must be tailored to meet allowed ends)

United States v. Washington, ARMY MISC 20100961 (A.C.C.A. 2011) (unpublished) (adopts *Burgess*-like factors: (1) the agent performing the search was clear as to what he was searching for; (2) the agent conducted his search in a way to avoid types of files not identified by the warrant by segregating only image files.)

¹⁴⁵ In-class Handout, Criminal Law Dep’t., The Judge Advocate Gen.’s Legal Ctr. & Sch., U.S. Army, Plain View in the Digital Context (2012–2013).

“PLAIN VIEW DOES NOT APPLY”

Prophylactic Approach

- (1) Reliance on PV is **waived**;
- (2) An independent 3rd party must review, segregate, and redact files first;
- (3) Warrants must disclose the risks of destruction of information and prior efforts to seize that information;
- (4) The government must disclose its search protocol and it must be designed to uncover **only** information for which it has probable cause;
- (5) The government must destroy or return evidence outside the scope of the warrant.

U.S. v. Comprehensive Drug Testing, Inc., 579 F.3d 989 (9th Cir. 2009) (en banc)

ALTERNATE ROUTES AROUND PLAIN VIEW

Some courts have used **Inevitable Discovery** or **Alternate Source** in order to support a search and avoid PV.

United States v. Crespo-Ríos, 645 F.3d 37, 42 (1st Cir. 2011) (**Inevitable Discovery**)

United States v. Stabile, 633 F.3d 219 (3rd Cir. 2011) (**Inevitable Discovery**) (routine police procedures would have inevitably led to discovery of CP files)

United States v. Wallace, 66 M.J. 5, 10 (C.A.A.F. 2008) (**Inevitable Discovery**)

Appendix D

Plain View Doctrine—Digital Context¹⁴⁶

PLAIN VIEW DOCTRINE – DIGITAL CONTEXT

1ST CIRCUIT:

- *United States v. Upham*, 168 F.3d 532 (1st Cir. 1999)
 - o A search warrant for image files on a computer gave authorization to police to search every file on the computer as well as deleted info.
 - o “[A] search of a computer and co-located disks is not inherently more intrusive than the physical search of an entire house for a weapon or drugs.” *Id.* at 535.
 - o The PC showing in the warrant must demonstrate a “sufficient chance of finding some needles in the computer haystack.” *Id.* at 535.
 - o Followed by *United States v. Burdulis*, 2011 U.S. Dist. LEXIS 53612
 - Search warrant of computer for a single image gave authorization to open every image file on the computer and all is admissible under PV.

2ND CIRCUIT:

3RD CIRCUIT:

- *United States v. Stabile*, 633 F.3d 219 (3rd Cir. 2011)
 - o Seized hard drives and have search warrant for evidence of financial crimes, discovered CP when opened video files on hard drive.
 - o Refuse to address if PV applies (*Id.* at 242)
 - o The court upholds the search on grounds of (1) independent source and (2) inevitable discovery – routine police procedures would have inevitably led to police discovering the CP files.
- *United States v. Highbarger*, 380 Fed. Appx. 127 (3rd Cir. 2010) (unpublished)
 - o Search warrant for all documents and records relating to drug offense.
 - o During search, police opened graphic files and discovered CP.
 - o Court upheld search under PV – authorization to search is not limited by the names/type of file – police had to open files to verify contents.

4TH CIRCUIT:

- *United States v. Williams*, 592 F.3d 511 (4th Cir. 2010)
 - o PV doctrine applies fully so long as there is a warrant to look for files on digital media relating to an offense (here it was harassing or threatening behavior) – the warrant implies that officers can open each file to determine what the file contains and then PV rules apply.
 - o “[T]he warrant impliedly authorized officers to open each file on the computer and view its contents, at least cursorily, to determine whether the file fell within the scope of the warrant’s authorization-i.e., whether it related to the designated Virginia crimes of making threats or computer harassment.” *Id.* at 522.
 - o “Once it is accepted that a computer search must, by implication, authorize at least a cursory review of each file on the computer, then the criteria for applying the plain-view exception are readily satisfied.” *Id.*
 - o Warning: officers must conduct these searches with “care and respect for privacy.” *Id.* at 523-24.

¹⁴⁶ In-class Handout, Criminal Law Dep’t., The Judge Advocate Gen.’s Legal Ctr. & Sch., U.S. Army, Plain View Doctrine—The Digital Context (2012).