ARTICLE:

The 2013 Salzburg Workshop on Cyber Investigations: **Digital Evidence and Investigatory Protocols**

By **Tommy Umberg** and **Cherrie Warden**

This article has been developed from a paper originally prepared for the 2013 Salzburg Workshop on Cyber Investigations under the supervision of Professors Laurel E. Fletcher, Chris Hoofnagle, Eric Stover, and Jennifer Urban.

Abstract

The purpose of this paper is to assist the Office of the Prosecutor ("OTP") at the International Criminal Court ("ICC") by discussing cyber investigation protocols that enable the strategic mobilization and acquisition of digital evidence.

This paper discusses cyber investigation protocols relevant to three types of digital evidence: data that is stored on a physical device; data that is not stored on a device that an investigator is able to have physical access to or is accessible online; and data that is stored in servers and held privately by a service provider. The first section addresses how an investigator might acquire and authenticate physical devices that may have evidentiary value. The protocols demonstrate methods that reduce the risk of inadmissibility and manipulation. The second section addresses situations where the investigator obtains evidence from a device other than the original, for instance, a video that is posted on a publicly available website, and is available as a download from a server. Since this type of digital evidence is not forensically acquired, this section aims to illustrate how investigators can determine its reliability. Additionally, this section explains how prosecutors might authenticate such evidence by corroboration or testimony. The third section turns to data held by service providers that is not available without their cooperation. This data may be acquired by a direct request from a prosecutor. For United States service providers, the U.S. Stored Communications Act ("SCA") sets forth procedures for domestic law enforcement access to this data. It is silent on foreign law enforcement access. The Mutual Legal Assistance Treaties ("MLAT") process addresses foreign law enforcement access to this data; however, this process is lengthy and may be subject to other legal requirements, such as dual criminality. Please note that protocols in all three sections are based on standards that reflect the current technological landscape and therefore should be updated when necessary. Furthermore, the basic procedures discussed here are derived from lengthy treatments of forensic analysis in source documents. In all three types of investigations, situational factors arise in which deviation from the protocols discussed is appropriate. Therefore, each investigation will need to employ specific procedures that are dependent on the context.

Introduction

Cyber investigation protocols help investigators gather digital evidence in a forensically valid way. This paper presents the existing landscape, presents challenges and opportunities, as well as provides a framework to aid prosecutors in establishing greater integrity of digital evidence in cyber investigations.

Digital evidence is "data that is created, manipulated, stored or communicated by any device, computer or computer system or transmitted over a communication system, that is relevant to the proceeding."[1] For purposes of this paper, digital evidence is divided into three categories. The first category includes data that an investigator acquires from a physical device such as a hard drive or wireless telephone. The second category includes data stored on a server, and accessible from an online service via a computer or smartphone. For example, a video that is stored in a publicly available online service, such as YouTube, or evidence sent by e-mail to an investigator from the scene of a crime fall within the second category. The third category includes evidentiary data held by a service provider, and not otherwise

[1] Stephen Mason, editor, *International Electronic Evidence* (British Institute of International and Comparative Law, 2008); for other definitions, see Burkhard Schaffer and Stephen Mason, 'The characteristics of electronic evidence in digital format' Chapter 2, 27 in Stephen Mason, gen ed, *Electronic Evidence* (3rd edn, LexisNexis Butterworths, 2012) and George L. Paul, *Foundations of Digital Evidence* (American Bar Association, 2008), 23-24.

available. E-mail messages held by a service such as Gmail or Yahoo! Mail and photographs held in a cloud storage service such as Dropbox are each examples of this category of data.

The protocols illustrate digital evidence practices employed by investigators throughout the international community; however, this paper does not claim to set out minimum standards required to gather evidence or to offer precise procedures for how the ICC will evaluate different forms of digital evidence. Individual investigations are context and fact-specific, thus they may be affected by limitations on resources as well as unique factors that affect the particular situation an investigator may find themselves in. The purpose of this paper was to set out the basic procedures in order to provide some foundational information to aid the workshop discussion in Salzburg and the ICC's efforts in further developing its cyber investigation practices. Finally, the entirety of relevant investigative practices cannot be summarized in a treatment of this length.

Evidentiary protocols for devices in the possession of investigators

This section addresses situations for investigators who encounter or directly obtain a physical device, such as a hard drive, that may have evidentiary value. The handling of the device can affect the admissibility of the evidence extracted from the device and its probative value. A consideration of the protocols described below will enhance the veracity of the evidence.

These protocols are a compilation of the U.S. Department of Justice[2] and the Association of Chief Police Officers ("ACPO") *Good Practice Guide for Digital Evidence*.[3] These guidelines were chosen because they are based upon current technologies and are referenced throughout the cyber investigation community; however, the guidelines should be updated as new technologies emerge.

Acquisition

To maximize the integrity of an investigation, the investigator should identify the device, determine its setup, and make a forensic copy of the data. Investigators should document their actions by keeping a log that describes persons who handled the evidence, actions taken which could potentially alter the evidence, and the physical storage of the evidence from the point of discovery to its introduction. Capturing the entire process on video[4] is highly recommended.[5] Thorough documentation of the acquisition process will aid in establishing the chain of custody and the overall credibility of the evidence.

Furthermore, the documentation log should include a diagram or a photograph depicting the device's setup, including all the cables and ports, so it may be reassembled if necessary. If disassembling the device for relocation, all items should have signed exhibit labels attached. Failure to do so may create difficulties with the chain of custody, leading to challenges by the defense. Additionally, it is common for individuals to keep their passwords in written form and in close proximity to their computer; therefore investigators should search surrounding areas and document all potentially valuable pieces of evidence. Upon discovery,[6] the investigator should determine whether the device is likely to hold evidence. Furthermore, the investigator should consider removing the device from any network due to the possibility that the owner might be able to obtain access to it remotely.[7] However, this should be balanced against the possibility of losing evidentiary value, and protocols can depend on whether the device is powered on or off.[8]

Discovery of a powered-off device

A powered-off device should be forensically imaged on site or in a forensic laboratory.[9] A forensic image

[2] US Department of Justice, *Forensic Examination of Digital Evidence: A Guide for Law Enforcement*, (April 2004), available at https://www.ncjrs.gov/pdffiles1/nij/199408.pdf .

[3] Association of Chief Police Officers, *Good Practice Guide for Digital Evidence*, Version 5 (October 2011; published 2012), available at http://www.acpo.police.uk/documents/crime/2011/201110-cba-digital-evidence-v5.pdf .

[4] If possible, disable audio component because conversations or reactions by investigators may become an issue during trial.

[5] Marjie T. Britz, *Computer Forensics and Cyber Crime: An Introduction* (3rd edn, Prentice Hall, 2013), 317.

[6] Storage drives may be located on a wired or wireless network, thus a thorough search will aim to trace the physical wired network and search for wireless links to network storage. Furthermore, if available, investigators should always consider seizing any back-ups of the data.

[7] *Good Practice Guide for Digital Evidence*, 30-31.

[8] *Good Practice Guide for Digital Evidence*, 30-31.

[9] For a detailed explanation of currently available tools for "forensic imaging" See Peter Sommer, *Digital Evidence, Digital Investigations and E-Disclosure: A guide to Forensic Readiness for Organisations*,

ensures that analysts do not inadvertently alter data during the examination. Retaining an unaltered version strengthens the evidence's probative value by alleviating concerns over best evidence.[10] Ideally, an image of the entire device should be made, however, partial or selective file copying may be considered as an alternative when the amount of data to be imaged makes complete copies impracticable.

As part of the forensic imaging process, the investigator should compare the internal clock of the device in its BIOS against the actual time. Often, the internal clock differs from the actual date and time causing file metadata[11] to be inaccurate. Information regarding the difference between the internal clock and the actual time is useful in authentication of the evidence, establishing its chain of custody, and may aid in creating a link between the defendant and the evidence.[12] To establish the accurate metadata time stamps, examiners can photograph the computer time in the BIOS screen next to an external clock. At this point the hard drive and its forensic copy should be brought to a secure location for examination and analysis. Methods to transport and store the equipment are discussed below.

Discovery of a powered-on device

A powered-on device presents special challenges. If the device has encryption, powering it off may cause volumes to automatically encrypt such that investigators can never recover the data.[13] An inexperienced investigator who discovers a hard drive should leave it on until the appropriate personnel arrive to assess the situation. Once the investigator arrives, they have to decide whether to shut down the device immediately, or gather evidence prior to doing so. Second, whether it is more prudent to shut down the device by pulling the power cord or by internal commands. This section discusses the issues in a broad context.

In assessing whether to power-down or gather evidence, first, investigators must weigh whether a digital inspection will inadvertently alter evidence and raise authentication issues later.[14] Alternatively, some data may be destroyed or encrypted if the device is immediately shut down. Data at risk of being lost is stored in the Random Access Memory (RAM), which may contain active programs and passwords.[15] Ultimately, investigators should consider whether the value of the volatile data that is recoverable outweighs the potential risk of diminishing the credibility of other evidence that might be obtained.

If an investigator decides to gather evidence prior to shutting down the device, then the investigator should consider making the evidence visible on the screen and photographing it. All actions taken in the attempt to bring the relevant information onto the screen should be documented.

The recommended method for powering down the computer is dependent upon the operating system of the device. One author suggests removing the power cord or battery out of the device, rather than from the wall socket. This prevents the hard drive from performing shut down processes that may alter the

Security Advisers and Lawyers (Information Assurance Advisory Counsel, v3 March 2012), 40, available at http://www.iaac.org.uk/_media/DigitalInvestigations2012.pdf?goback=%2Egde_37008_member_157854004#%21 .

[10] "Best evidence" issues arise when the evidence submitted is a copy of an original and the original was accessible to the party proffering such evidence. Note that there is no concept of a digital 'original', for which see George L. Paul, *Foundations of Digital Evidence*, 48; Burkhard Schaffer and Stephen Mason, 'The characteristics of electronic evidence in digital format', 2.04; Stephen Mason, "Electronic evidence and the meaning of 'original'" *Amicus Curiae* The Journal of the Society for Advanced Legal Studies, Issue 79, Autumn 2009, 26-28, available from http://sas-space.sas.ac.uk/2565/

[11] "Metadata" is "data about data," and includes the dates and times the files were viewed or altered.

[12] See *Prosecutor v. Karemera and others*, Case No. IT-98-44-T, Judgment, 169-173, 205 (Int'l Crim. Trib. for Rwanda Feb. 2, 2012) (The date and time of a video of a rally submitted as evidence proved that the accused was in attendance).

[13] *In re Grand Jury Subpoena to Sebastien Boucher*, No. 2:06-mj-91, 2009 WL 424718 (D. Vt. 2009) (Investigators shut down a suspect's computer causing the encryption of evidence that was unrecoverable without the suspect's password).

[14] The general rule for mobile telephones is to block remote alteration by placing the telephone in a faraday bag, which is a radio frequency shielding cloth, or by switching it to "airplane" mode or its equivalent. See Eoghan Casey and Benjamin Turnbull, 'Digital Evidence on Mobile Devices' in Eoghan Casey, *Digital Evidence and Computer Crime* (3rd edn, Academic Press, 2011), available at http://booksite.elsevier.com/9780123742681/Chapter_20_Final.pdf ; Eric Katz, *A Field Test of Mobile Phone Shielding Devices* 8 (10 December 2010) (Ph.D dissertation, Purdue University) available at http://docs.lib.purdue.edu/cgi/viewcontent.cgi?article=1033&context=techmasters . However, mobile forensics is becoming more complex as security on mobile devices improves. New features allowing the user to remotely wipe data require mobile devices to be quickly isolated from the network to prevent the user from deleting data. On the other hand, by being disconnected from the network, data can be automatically deleted. For instance, Blackberry devices will automatically delete all data after being disconnected from the network for a certain number of days, thus requiring forensic analysis to occur shortly after the device is seized.

[15] Examples of "running processes" that are typically more valuable to investigations are, instant messaging conversations, financial statements, active remote data storage, or data encryption.

original hard drive.[16] However, some operating systems can be damaged by an immediate power failure and should be shut down through the regular internal shut down commands. Once the device is shut down, it should be forensically imaged.

Authentication

Authentication ensures that the evidence tendered establishes what it is offered to prove. In this context, it attempts to demonstrate that the investigation has not altered the digital evidence. Even a slight difference between the forensic image and the original will have a deleterious affect on the evidence's ultimate probative value.[17]

Typically, investigators authenticate evidence originating from a hard drive through an electronic fingerprinting process. In this process, the original hard drive is subjected to a "checksum" of its contents through a mathematical process that produces a result unique to the specific hard drive in its current state. The forensic image of the hard drive is subjected to the same fingerprinting test, with identical results between the original, which is exposed to the test early in the process, and the forensic image, which is exposed at a later stage, indicating with a high degree of probability that the two are truly identical.[18]

To improve the likelihood that the forensic image and the original hard drive are identical, investigators should pay attention to the transportation and storage of the device. As a general guideline, computer equipment should be stored at normal room temperature and free from magnetic influence such as radio receivers. Also dust, smoke, sand, water, oil, and extreme humidity are harmful to electronic equipment.[19] Moreover, transporting digital evidence in the trunk or boot of a police car is not recommended because of high temperatures and close proximity to other electronic communication equipment.[20]

In all cases, investigators should exercise diligence, carefully log their investigative actions, and document how the device is connected to other equipment. The principal investigation should be performed on a forensic copy of the device, rather than the original. Furthermore, every step of the forensic analysis conducted by the investigator should be capable of replication.

Evidentiary protocols for digital evidence recovered from a device not in the possession of the investigator

Investigators sometimes obtain evidence that is obtained from a device that is not in the possession of the investigator (such as data from a website that is stored on a server), or its creator. This may include a video sent by e-mail to an investigator or stored upon some publicly available internet service. Typically, the device that captured the evidence, that is the hard drive or camera, does not accompany it, and in some situations the evidence may be sent anonymously, thus creating concern over its origins. With the increase in access to cameras and other recording devices, this type of evidence can be extremely useful in linking suspects to crimes perpetrated on large groups or in public view.[21]

Evidence of this nature has few acquisition procedures because, by definition, it has already been either acquired by investigators or is in the public realm. Thus, this section switches focus to techniques that prove that the proffered evidence is what it purports to show, and thus authenticated.[22] Each case is unique, and no universal practices can be applied to authenticating evidence from such sources. However, an understanding of traditional approaches to

[16] Robert Moore, *Cybercrime: Investigating High-Technology Computer Crime* (2 nd edn, Anderson, 2010), 215.

[17] *Prosecutor v. Bemba Gombo*, Case No. ICC-01/05-01/08, 19 November 2010 (holding that minor authentication issues does not prohibit admission into evidence, but does affect its final probative value).

[18] Eoghan Casey, *Digital Evidence and Computer Crime*, 22-24.

[19] *Good Practice Guide for Digital Evidence*, Appendix C.

[20] Robert Moore, *Cybercrime: Investigating High-Technology Computer Crime,* 223.

[21] See *Prosecutor v. Karemera and others*, Case No. IT-98-44-T, Judgment, 169-173, 205 (Int'l Crim. Trib. for Rwanda Feb. 2, 2012) (Video evidence of rally and transcript of radio broadcast authenticated the date of the video and proved that the accused was in attendance); *Prosecutor v. Bagosora*, Case No. IT-98-41-T, Trial Judgment and Appeals Judgment, 2029-2031, 460 (Int'l Crim. Trib. for Rwanda Dec. 8, 2008; Dec. 14, 2011) (Video footage and transcript led the court to conclude that the accused was acting as Minister of Defense and exercised control over the army).

[22] See *Prosecutor v. Popovic and others, et al*., Case No. IT-05-88-T, Decision on Admissibility of Intercepted Communications, 4, 22, 26, 33-35 (Int'l Crim. Trib. for the Former Yugoslavia Dec. 7, 2007).

authentication, coupled with the creativity to go beyond those approaches when unusual situations present themselves, will increase the likelihood that such evidence can be used.

This section provides a non-exhaustive list of useful authentication techniques for evidence not take directly from a device, followed by a case study in which an investigation attempted to authenticate a video brought into the public realm through private submission to a news agency.

General authentication techniques

Prosecutors and investigators often employ general techniques that are applicable to a wide variety of evidence when authenticating evidence not taken directly from a device. These techniques include use of witness testimony, internal factors such as metadata, and comparison with other independently authenticated evidence.

If such evidence involves a personal communication, courts in the U.S. typically prefer it be introduced through testimony of an individual who was a party to the communication.[23] This method affords the defendant an opportunity to cross-examine the witness. If the witness is not available to give evidence, then a written statement can still be beneficial for the purposes of authentication.[24] For evidence not taken directly from a device, this technique usually requires the investigator to trace the origins of the evidence until a person can be identified that has knowledge of its contents or creation. For instance, if the evidence is a video available online, a request can be made to the host website to identify the information of the subscriber who uploaded it.

Additionally, the metadata may be used to assist in its authentication.[25] The use of metadata is helpful in many ways, but in the authentication context it is capable of tracing the origins of the evidence to a party who can testify to its accuracy. Finally, if such evidence is similar enough to other independently authenticated evidence, the courts may determine that the evidence is also authenticated based on its similarities.[26]

Sri Lanka case study[27]

Often authentication is not suited for evidence not taken directly from a device; therefore, an investigator must use unconventional methods. The following case study describes one such situation that called for creative approaches to the authentication of the evidence.

In August of 2009, during the Sri Lankan army's battle against the Liberation Tigers of Tamil Eelam, video footage purporting to show the execution of prisoners became public through the submission from a private source to a news agency.[28] No witnesses were willing to verify the video, nor was there any ancillary evidence to corroborate the video's authenticity. Furthermore, the Sri Lankan Government denied the allegations and labeled the video unreliable.[29]

Philip Alston, the UN special rapporteur on extrajudicial, summary or arbitrary executions, suspected that the video had evidentiary value and therefore sought to determine whether the video was authentic. Additionally, he set out to determine the reliability of the evidence, in that it depicted what it purported to show. To prove that the video was authentic, Alston sent the footage to a digital editing forensic expert. The expert used software (called "Cognitech") to stabilize and enlarge vital parts of the

[23] Mark L. Krotoski, "Effectively Using Electronic Evidence Before and at Trial", *United States Attorneys' Bulletin Obtaining and Admitting Electronic Evidence*, Volume 59, Number 6, (US Department of Justice, November 2011), 52-71, 58; available at http://www.justice.gov/usao/eousa/foia_reading_room/usab5906.pdf.

[24] *Prosecutor v. Dordevic*, Decision on Prosecution's Oral Motion for Admission of Evidence Tendered Through Witness Philip Coo, Case No. IT-05-87/1-T, (Int'l Crim. Trib. for the Former Yugoslavia Oct. 1, 2009) (Holding that it is desirable that digital documents be submitted into evidence via oral testimony, but not required because the court will take this into account when determining probative value).

[25] *Lorraine v. Markel*, 241 F.R.D. 534, 560 (D. Md. 2007) (stating that metadata can be a useful tool in authenticating digital evidence).

[26] In the U.S context, see *United States v. Safavian*, 435 F.Supp.2d 36, 40 (D.D.C. 2006) (holding that e-mail exchanges where authenticated based on their similarity to other previously authenticated e-mails between the same individuals); in the context of England and Wales, see *R v Mawji (Rizwan)* [2003] EWCA Crim 3067, [2003] All ER (D) 285 (Oct), discussed in Stephen Mason, *Electronic Evidence*, chapter 4.

[27] This section is predominantly compiled from *Deeming Sri Lanka Execution Video Authentic, UN Expert Calls for War Crimes Probe*, UN News Centre, 7 January 2010, http://www.un.org/apps/news/story.asp?NewsID=33423 .

[28] The video can be viewed at http://www.liveleak.com/view?i=0a1_1311145191 .

[29] Office of the High Commissioner for Human Rights, United Nations, *UN Expert Concludes that Sri Lankan Video is Authentic, Calls for an Independent War Crimes Investigation*, (7 January 2010), http://www.ohchr.org/EN/NewsEvents/Pages/DisplayNews.aspx?NewsID=9706&LangID=E .

footage. He concluded that there were no breaks in the film's continuity, indicating that the footage had not been edited or manipulated.

Alston subsequently sent the stabilized and enlarged footage to two other experts, a ballistic expert and a forensic pathologist. The ballistic expert sought to determine whether the weapons and bullets shot during the video were real. He concluded that the weapons in the video were AK-47s and thus conducted experiments by shooting live and imitation AK-47 ammunition. After comparing the tapes with the original video, he concluded that the recoil, the movement of the weapon and shooter, and the gasses emitted from the muzzle were consistent with the firing of live ammunition rather than blanks. The forensic pathologist analyzed the victims' body reactions and blood splatter from the video, and determined that both were consistent with "what would be expected" in a close range shooting.[30]

While none of the experts' findings independently proved beyond all doubt that the video was authentic, working in conjunction, they serve as compelling evidence of the authenticity of the video. Upon publishing these findings, the international community put pressure on the Sri Lankan Government to address the situation. In addition, Christof Heyns, a U.N. special rapporteur, stated at a press conference that the case should go to the next level of international investigation.[31] The results of the official investigation are pending at the time of writing.

The methods outlined above shed sufficient light upon the accuracy of the video to warrant an official investigation. If resources permit, then similar techniques should be employed to aid in the authentication for other evidence of a similar nature. Furthermore, the reliance upon a wide array of experts suggests that it is advantageous for an investigative body such as the OTP to pursue and maintain a large network of diverse experts.

For evidence that is recovered independently of a device or from some anonymous source, investigators must proceed on a case-by-case basis. Investigators dealing with such evidence may be able to employ traditional authentication techniques, but at times are required to develop creative strategies similar to those depicted in the Sri Lanka case study.

Evidentiary protocols for digital evidence stored with service providers

Acquisition and preservation

Often a private-sector provider of communications or other services holds relevant information to an investigation. When seeking this data, U.S. law enforcement officials may make a direct request to a service provider to acquire the user data. International law enforcement must make requests through either a Mutual Legal Assistance Treaty process or through letters rogatory. Furthermore, international law enforcement may be able to use the Joint Investigation Team ("JIT") process. These are discussed below.

Major service providers publish guides for investigators on how to request data, but as a first matter, it is important to identify the correct service provider to contact. This can be confusing, because even the unsophisticated can mask their internet protocol (IP) address or disguise the provenance of an e-mail. Investigators often begin an inquiry by examining available IP addresses of suspects. Investigators can run certain commands to try to reverse-trace the owner of an IP address. Similarly, e-mail headers can be carefully inspected to determine its route and origin.

The position in the United States

In the United States, the Stored Communications Act ("SCA") regulates access to stored electronic records, and this law limits government requests for user data. The SCA is a complex statute and this discussion aims to introduce the main contours of the Act. The SCA is section II of the Electronic Communications Privacy Act ("ECPA") and is codified at 18 U.S.C. 121 §§ 2701-2712. It addresses voluntary and compelled disclosure of stored wire and electronic communications.[32] The SCA is silent on applications for data made by foreign law enforcement officials, but it suggests that any domestic law enforcement personnel can make a request.

[30] Office of the High Commissioner for Human Rights, United Nations, *UN Expert Concludes that Sri Lankan Video is Authentic, Calls for an Independent War Crimes Investigation.*

[31] United Nations News Centre, United Nations, *Sri Lanka: UN Experts Calls on Government to Probe Executions Captured on Video*, (31 May 2011), http://www.un.org/apps/news/story.asp?NewsID=38564#.UkyDJLyTaFM .

[32] Stored Communications Act, 18 U.S.C. 121 §§ 2701-2712 (1986).

The status of the service provider is a significant determinant of legal protection for user data. If the service provider is a private provider, then it is exempt from many of the SCA obligations and therefore can voluntarily disclose non-content and content data to any person for any reason. If the service provider serves the public, then it is subject to the SCA and must comply with its rules that generally prohibit the disclosure of content. To determine the classification of a service provider as public or private, a prosecutor must consider whether the service provider affords service to the community at large.[33] A company that administers e-mail only for its employees is probably a private provider; whereas Google, Yahoo, or Microsoft mail are public providers.

There are two types of data categories: non-content and content data. Non-content data includes subscriber and traffic data; subscriber data[34] focuses on who owns the account whereas traffic data[35] focuses on who sent or received an e-mail. Content data includes the substance of an e-mail or telephone call such as subject lines or text in the body of an e-mail. As a general framework, subscriber data requires a subpoena that shows the request is relevant to an ongoing investigation; traffic non-content data requires a 2703(d) order which states "specific and articulable facts" linking the data request to an ongoing investigation; and content data such as e-mail content requires a 2703(c)(1) warrant.[36]

Importantly, a preservation request can be made under 2703(f) pending the court order.[37] For a 2703(f) request, a government entity need only send a request by facsimile transmission to the service provider to preserve all data in relation to the investigation. Finally, if a statutory exception applies, then public service providers may voluntarily disclose non-content and content data to the government.[38] For example, if exigent circumstances exist such as a kidnapping, then the government's request will fall within the statutory exemption.[39]

Authentication and chain of custody

Authentication refers to a legal concept that promotes the integrity of the trial process by ensuring tendered evidence establishes what it is offered to prove.[40] To ensure chain of custody and thus the admissibility of the service provider data, the recipient of the data should date the creation of the document, write the name of the client or individual being served, describe the evidence being held, describe the reason for the transfer from point A to point B, complete a list of each person who had physical control over the evidence, and provide appropriate space for individuals to sign when they receive and release the evidence.[41]

Procedure on how to request service provider data

Some major service providers such as Google and Facebook have corporate forms that require all data requests to be executed in the U.S.[42] To ensure investigators do not duplicate efforts and to assist in later stages of the legal process, investigators may consider completing a data acquisition request form for internal planning of the request from the service

[33] US Department of Justice, Executive Office for United States Attorneys, *Searching and Seizing Computers and Obtaining Electronic Evidence in Criminal Investigations*, 135.

[34] Subscriber data: the name and address associated with the account; usernames or screen names; session times and duration; IP addresses; means and source of payment; local and long distance telephone toll billing records; telephone number and type of service provided; and a temporarily assigned network address.

[35] Traffic data: Data that is not basic subscriber information or content specific. Some examples include log files, IP logs, and identities of e-mail correspondents.

[36] Stored Communications Act, 18 U.S.C. 121 §§ 2702-2703.

[37] Stored Communications Act, 18 U.S.C. 121 §§ 2703(f).

[38] Stored Communications Act, 18 U.S.C. 121 §§ 2703(f).

[39] Stored Communications Act, 18 U.S.C. 121 §§ 2702(5).

[40] See *Prosecutor v. Popovic and others*, Case No. IT-05-88-T, Decision on Admissibility of Intercepted Communications in Trial Chamber II, 4, 22, 26, 33-35 (Int'l Crim. Trib. for the Former Yugoslavia Dec. 7, 2007).

[41] Erik Laykin, *Investigative Computer Forensics: The Practical Guide for Lawyers, Accountants, Investigators, and Business Executives* (Wiley, 2013), 76-69, 83-85; Eoghan Casey, *Digital Evidence and Computer Crime*, 21-22; *Good Practice Guide for Digital Evidence*, 6.7.1.

[42] However, the Belgian police have challenged this requirement, requiring an ISP to provide data direct to the Belgian authorities when requested, for which see the translations of the various decisions in the Yahoo! case in Belgium (citations refer to the *Digital Evidence and Electronic Signature Law Review*) with commentaries written by Johan Vandendriessche: Corr. Dendermonde 2 maart 2009, onuitg. (Rechtbank van Eerste Aanleg te Dendermonde (The Court of First Instance in Dendermonde)), 8 (2011) 196 – 207; Gent 30 juni 2010, onuitg. (Hof van Beroep (The Court of Appeal in Ghent, third chamber, sitting in criminal matters)), 8 (2011) 208 – 215; Cass. 18 januari 2011, nr. P.10.1347.N (Hof van Cassatie (Court of Cassation of Belgium)), 8 (2011) 216 – 218; Brussel 12 oktober 2011, onuitg, Hof van Beroep te Brussel (The Court of Appeal in Brussels, thirteenth chamber, sitting in criminal matters), 9 (2012) 102 – 105; P. 11.1906.N/1 Hof van Cassatie – Cour de cassation (Court of Cassation of Belgium) (4 September 2012), 10 (2013) 155 – 157.

provider.[43] The request form should identify the evidence being sought; methodological information; the date and time of the acquisition; the individual who collected the data; whether it was from a physical device or not; the location, and any other reasonable information.[44] Furthermore, many service providers publish a guide for law enforcement investigators with forms for data requests and specific information about procedures. Comcast is one of many service providers that provide step-by-step data acquisition guidelines as outlined below.[45]

First, the requestor should verify that the IP address or e-mail address is registered to the service provider by using the reverse-trace mechanism. Second, the requestor should determine whether the data sought is subscriber, traffic, or content data and therefore whether it implicates a subpoena, 2703(d) order, or a 2703(c)(1) warrant respectively. Third, the requestors' inquiry should include the IP address, e-mail address, street address, telephone number and all other pertinent information that would allow the service provider to adequately respond. Fourth, the requestor should include the date and time of all incidents including seconds and time zone, i.e. 12 December 2007 @ 06:13:21 EST. Requestors should caution time synchronization stamps because if preserved inaccurately, then issues arise.[46] Fifth, the requestor should ensure that the required certifications and all applicable substantive and procedural requirements under the particular statutes or regulation authorizing the request have been satisfied. Sixth, the requestor should ensure that there is a complete explanation of the nature and circumstances of any potential serious injury or death to justify an emergency disclosure. Lastly, the requestor should ensure that all of the contact information is correct.

Mutual Legal Assistance Treaties and Joint Investigation Teams

Mutual Legal Assistance Treaties and letters rogatory allow international evidence exchanges in criminal procedures.[47] The MLAT process is initiated when a treaty facilitating the evidence exchange exists and the letters rogatory process is used when a treaty does not exist to facilitate the exchange between courts. MLATs are negotiated by the Department of State in cooperation with the Department of Justice.

Google is one service provider that specifies a MLAT framework as well as other diplomatic arrangements to assist foreign entities in their data requests.[48] Google states that non-U.S. agencies can work through the U.S. Department of Justice to gather evidence for legitimate investigations. Furthermore if United States law is implicated in the investigation, then "a U.S. agency may open its own investigation and provide non-U.S. investigators with evidence gathered." Google may provide data on a voluntary basis if the request is consistent with international norms, U.S. law, and the law of the requesting country. Given that an international agency goes through a diplomatic process, like MLAT, Google will divulge the same information to a non-U.S. agency, as it would produce if the request originated directly from a U.S. agency. The MLAT process takes significantly more time than that experienced by domestic law enforcement requesting data through the SCA.

Joint Investigation Teams ("JITs") are a response to the 21st century criminal landscape, which consists of highly mobile groups engaged in illegal activity across borders.[49] This trend demands strengthened transnational cooperation between competent authorities.[50] A JIT is an investigation team established for a specified time period, based on an agreement between two or more European Union member states and competent authorities. If all parties are in

[43] Erik Laykin, *Investigative Computer Forensics*, 78-79.

[44] Erik Laykin, *Investigative Computer Forensics*, 78-79.

[45] Comcast, *Law Enforcement Guide*, http://cryptome.org/isp-spy/comcast-spy.pdf .

[46] Interview with Chris Hoofnagle, Director, Information Privacy Programs, Berkeley Center for Law & Technology (1 October 2013).

[47] U.S. Department of State, Bureau of International Narcotics and Law Enforcement Affairs, *International Narcotics Control Strategy Report* (7 March 2012) (It is unclear whether and how the OTP can use the MLAT or letters rogatory processes. Furthermore, it is ambiguous whether parties to the Rome Statute should initiate the MLAT or letters rogatory processes).

[48] Google, *Transparency Report*, not dated, available at http://www.google.com/transparencyreport/userdatarequests/legalprocess/#how_does_google_respond .

[49] European Commission: Joint Investigation Teams, available at http://ec.europa.eu/dgs/home-affairs/what-we-do/policies/police-cooperation/jit/index_en.htm .

[50] European Commission: Joint Investigation Teams, (It is unclear whether "authorities" means states or may include international criminal tribunals).

agreement, then other states may participate in a JIT.[51]

Conclusion

This brief paper has set forth strategies to acquire and authenticate digital evidence in a forensically valid manner. Careful cyber investigations can strengthen the prosecutions' case as well as provide corroborating evidence connecting the accused to the alleged crime. The acquisition of digital evidence is fundamental in all investigations within a modern law enforcement environment. The collection of digital evidence is the "rule rather than the exception" in current investigations.[52] Two fundamental themes dominate each procedure: First, the objective of acquisition is to obtain an exact replica of the data to ensure validity and thus the highest probative value. Second, authenticity is critical and is attainable through corroboration or other means. It is suggested three further points of discussion are warranted. First, the nature of the investment in training and equipment that is necessary to enhance evidence gathering in a forensically valid way as well as increase the probative value of the evidence. Second, given the burdens of the MLAT and letters rogatory processes, it is to be considered whether the ICC should seek U.S. provider data on European servers, or via the JIT process. Third, the ICC may wish to consider the issue of novel scientific evidence, and whether a formal protocol is worth be considering in the future.

Thomas Umberg is currently a second year student at Berkeley School of Law. At Berkeley, Thomas has focused primarily on intellectual property and other technology related fields of law. Prior to attending law school, Thomas earned a bachelors degree in Economics from the University of California Santa Barbara.

Cherrie Warden is currently a second year student at Berkeley School of Law. At Berkeley, her area of interest includes international criminal law and the intersection of sexuality and culture, specifically victims of sexual violence. Cherrie has her Masters in Urban Education and Bachelors in International Studies and Criminology.

Cherriewarden@gmail.com

[51] Europol, Joint Investigation Teams, 2013, available at https://www.europol.europa.eu/content/page/joint-investigation-teams-989 .

[52] International Criminal Court, *Digital Evidence Report*, October 2013. This is an internal document circulated only within the ICC and the Human Rights Center at Berkeley.