WORKING PAPER

DIGITAL EVIDENCE: INVESTIGATORY PROTOCOLS

SALZBURG WORKSHOP ON CYBERINVESTIGATIONS

This paper was prepared by Tommy Umberg '15 and Cherrie Warden '15, students from the International Human Rights Law Clinic and the Samuelson Law, Technology & Public Policy Clinic at the University of California, Berkeley, School of Law, under the supervision of Professors Laurel E. Fletcher, Chris Jay Hoofnagle, Eric Stover, and Jennifer M. Urban

October 2013

Table of Contents

I. Introduction 1

II. Evidentiary Protocols for Devices Possessed by Investigators 2

A. Acquisition 2

i. Discovery of a Powered-Off Device 3

ii. Discovery of a Powered-On Device 4

B. Authentication 5

C. Conclusion 6

III. Evidentiary Protocols for Digital Evidence Not Recovered from a Device 6

A. General Authentication Techniques 7

B. Sri Lanka Case Study 7

C. Conclusion 9

IV. Evidentiary Protocols for Digital Evidence Stored with Service Providers 9

A. Acquisition and Preservation 9

B. Authentication and Chain of Custody 10

C. Procedure on How to Request Service Provider Data 11

D. Mutual Legal Assistance Treaties and Joint Investigation Teams 12

V. Conclusion 12

VI. Appendices I-VI 14

Abstract

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

This paper discusses cyberinvestigation protocols relevant to three types of digital evidence: data that is on a device; data that is not on a device or is accessible online; and data that is held privately by a service provider. The first section addresses how an investigator should 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 independent of a physical device, for instance, a video that is posted on a publicly available website. Since this type of digital evidence is not forensically acquired, this section aims to help investigators 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 context-dependent.

I. Introduction

Cyberinvestigation 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 strengthening linkage evidence in cyberinvestigations.

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, we have divided "digital evidence" into three categories. The first category includes data that an investigator acquires from a physical device such as a hard drive or wireless phone. The second category includes data divorced from a device, but accessible from an online service. For example, a video that is stored in a publicly available online service, such as YouTube, or evidence emailed to an investigator from the scene

[1] STEPHEN MASON, BRITISH INSTITUTE OF INTERNATIONAL AND COMPARATIVE LAW, INTERNATIONAL ELECTRONIC EVIDENCE (2008).

of a crime. The third category includes evidentiary data held by a service provider, and not otherwise available. Email 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 resource limitations as well as situational factors. As such, this paper sets out the basic procedures in order to provide some foundational information to aid the workshop discussion and the ICC's efforts in further developing its cyberinvestigation practices. Finally, the entirety of relevant investigative practices cannot be summarized in a treatment of this length.

II. Evidentiary Protocols for Devices Possessed by 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 affects admissibility of evidence and its probative value. Consideration of the described protocols 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")[3] practice guides for computer-based electronic evidence. These guidelines were chosen because they are based upon current technologies and are referenced throughout the cyberinvestigation community; however, the guidelines should be updated as new technologies emerge.

A. 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 evidence.

---

[2] US DEPARTMENT OF JUSTICE, FORENSIC EXAMINATION OF DIGITAL EVIDENCE: A GUIDE FOR LAW ENFORCEMENT, (2012), *available at* https://www.ncjrs.gov/pdffiles1/nij/199408.pdf.

[3] ASSOCIATION OF CHIEF POLICE OFFICERS, GOOD PRACTICE GUIDE FOR COMPUTER-BASED ELECTRONIC EVIDENCE, (2003), *available at* http://www.7safe.com/electronic_evidence/ACPO_guidelines_computer_evidence.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 317 (2013).

Furthermore, the documentation log should include a diagram or a photograph depicting the device's setup, including all 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 chain of custody leading to defense challenges. 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 powered on or off. A device in sleep mode or with a powered-off monitor may mislead the investigator in this determination.[7] To check if a computer is truly off, the investigator should switch the monitor on and move the mouse slightly. If there is no change in the screen, then the device may be powered off.[8]

i. Discovery of a Powered-Off Device

A powered-off device should be forensically imaged on site or in a forensic lab.[9] A forensic image ensures that analysts do not inadvertently alter data during the examination. Retaining an unaltered version strengthens the evidence's probative value by alleviating best evidence[10] concerns. 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 linkage between the

---

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

[7] US DEPARTMENT OF JUSTICE, ELECTRONIC CRIME SCENE INVESTIGATION: AN ON-THE-SCENE REFERENCE FOR FIRST RESPONDERS (2001), *available at* http://www.ncjrs.org.

[8] Id.

[9] For a detailed explanation of currently available tools for "forensic imaging" *See* PETER SOMMER, INFORMATION ASSURANCE ADVISORY COUNSEL, DIGITAL EVIDENCE, DIGITAL INVESTIGATIONS AND E-DISCLOSURE: A GUIDE TO FORENSIC READINESS FOR ORGANISATIONS, SECURITY ADVISERS AND LAWYERS 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

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

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. Proper ways to transport and store the equipment are discussed below.

ii. 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, two decisions exist. First, whether to immediately shut down the device 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 tradeoffs in both decisions.

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 devices' Random Access Memory (RAM), which may contain active programs and passwords.[15] Ultimately, investigators should consider whether the value of the recoverable volatile data outweigh the potential risk of diminishing the credibility of other anticipated evidence.

---

[12] *See* Prosecutor v. Karemera, et al. 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 encryption of evidence that was unrecoverable without the suspect's password).

[14] The general rule for mobile phones is to block remote alteration by placing the phone in a faraday bag, which is a radio frequency shielding cloth, or by switching it to "airplane" mode or its equivalent. *See* Eric Katz, A Field Test of Mobile Phone Shielding Devices 8 (Dec. 10, 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 (such as Apple iPhone's "Find My Phone") require mobile devices to be quickly isolated from the network to prevent the user from destroying data. On the other hand, network isolation can trigger data destruction. For instance, Blackberry devices will automatically wipe 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.

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 target device's operating system.[16] It is generally advocated to pull 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 original hard drive.[17] However, some operating systems can be damaged by immediate power failure and should be shut down through the regular internal shut down commands. To aid in making this decision, appendix V lists operating systems and their corresponding preferred shut down method.

Once the device is shut down, it should be forensically imaged.

B. Authentication

Authentication demonstrates that the investigation has not altered the digital evidence. The authentication process seeks to determine that the forensic image is an exact replica of the original device in question. Even a slight difference between the forensic image and the original will have a deleterious affect on the evidence's ultimate probative value.[18]

Typically, investigators authenticate evidence originating from a hard drive through an electronic fingerprinting process.[19] 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.[20] 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.[21]

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.[22] Also dust, smoke, sand, water, oil, and extreme humidity are harmful to electronic equipment.[23] Moreover, transporting digital evidence

---

[16] See Appendix IV for recommendations based on specific operating systems.
[17] ROBERT MOORE, CYBERCRIME: INVESTIGATING HIGH-TECHNOLOGY COMPUTER CRIME 215 (2010).
[18] *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).
[19] The most common tools for this are MD5 and SHA.
[20] Some forensic software, such as EnCase, can perform both the forensic imaging and digital fingerprinting process simultaneously.
[21] SOMMER, *supra* note 8 at 33.
[22] ASSOCIATE CHIEF POLICE OFFICERS, *supra* note 3 at 12.
[23] Id.

in the trunk of a police car is not recommended because of high temperatures and close proximity to other electronic communication equipment.[24]

C. Conclusion

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.

III. Evidentiary Protocols for Digital Evidence Not Recovered from a Device

Investigators sometimes obtain evidence that is divorced from a device or its creator. This may include a video emailed to an investigator or stored upon some publicly available internet service.

Typically, the device that captured the evidence, i.e. 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.[25]

As opposed to the previous section, 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.[26] Thus, this section switches focus to techniques that prove that the proffered "divorced" evidence is what it purports to show, and thus authenticated.[27] Each individual case is unique and no universal practices can be applied to authenticating divorced evidence. However, an understanding of traditional approaches to authentication, coupled with the creativity to go beyond those approaches when untraditional situations present themselves, will increase the likelihood that valuable divorced evidence will be usable.

This section provides a non-exhaustive list of useful authentication techniques for divorced evidence, 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.

---

[24] ROBERT MOORE, CYBERCRIME: INVESTIGATING HIGH-TECHNOLOGY COMPUTER CRIME 223 (2010).
[25] *See* Prosecutor v. Karemera, et al. 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).
[26] If the evidence is in the public realm, i.e. YouTube, then see section IV (a) for discussion on acquisition.
[27] *See Prosecutor v. Popovic*, 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)

A. General Authentication Techniques

Prosecutors and investigators often employ general techniques that are applicable to a wide variety of evidence when authenticating divorced evidence. These techniques include use of witness testimony, internal factors such as metadata, and comparison with other independently authenticated evidence.

If the divorced evidence involves personal communication, courts typically prefer it be introduced through testimony of an individual who was a party to the communication.[28] This method affords the defendant an opportunity to cross-examine. If the witness is not available to deliver in-person testimony, then a written statement can still be beneficial for authentication.[29] For divorced evidence, this technique typically requires the investigator to trace back the origins of the evidence until someone can be ascertained who is knowledgeable of its contents or creation. For instance, if the evidence is a YouTube video, a request can be made to YouTube to identify the information of the subscriber who uploaded it.[30]

Additionally, divorced evidence's metadata may be used to assist in its authentication.[31] The use of metadata is helpful in many ways, but in the authentication context it is most helpful in tracing the evidence's origins to a party who can testify to its accuracy.

Lastly, if divorced evidence is similar enough to other independently authenticated evidence, courts may determine that the divorced evidence is also authenticated based on its similarities.[32]

B. Sri Lanka Case Study[33]

Often authentication is not suited for divorced evidence; therefore, an investigator must use unconventional methods. Authentication scenarios requiring creative maneuvering vary dramatically, and thus, advisable techniques must adapt. The following case study describes one such situation that called for creative approaches to authentication.

---

[28] US DEPARTMENT OF JUSTICE, OBTAINING AND ADMITTING ELECTRONIC EVIDENCE 58 (2011) *available at,* http://www.justice.gov/usao/eousa/foia_reading_room/usab5906.pdf

[29] *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 courts discretion will take this into account when determining probative value).

[30] For details on how to submit such a request see section IV (c).

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

[32] *See United States v. Safavian*, 435 F. Supp. 2d 36, 40 (D.D.C. 2006) (holding that email exchanges where authenticated based on their similarity to other previously authenticated emails between the same individuals).

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

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 private submission to a news agency.[34] 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.[35]

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 video's reliability, i.e., 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[36] to stabilize and enlarge vital parts of the footage. He concluded that there were no breaks in the film's continuity, indicating that the footage had not been edited or manipulated.

Subsequently, Alston 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 guns 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 fake 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.[37]

While none of the experts' findings independently proves beyond all doubt that the video is authentic, working in conjunction, they serve as compelling evidence of the video's authenticity. Upon publishing these findings, the international community pressed 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.[38] The results of the official investigation are pending.

The case study's methods 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 divorced evidence. Furthermore, the investigation's reliance upon

---

[34] Video can be viewed at http://www.liveleak.com/view?i=0a1_1311145191

[35] 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*, (Jan. 7, 2010), http://www.ohchr.org/EN/NewsEvents/Pages/DisplayNews.aspx?NewsID=9706&LangID=E.

[36] The exact software used was "Cognitech"

[37] Office of the High Commissioner, *supra* note 35

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

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.

C. Conclusion

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 divorced 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.

IV. Evidentiary Protocols for Digital Evidence Stored with Service Providers

A. 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 may make a direct request to a service provider to acquire user data. International law enforcement must "domesticate" requests through either a Mutual Legal Assistance Treaty (MLAT) process or through "letters rogatory".[39] Furthermore, international law enforcement may be able to use the Joint Investigation Team ("JIT") process. These are discussed below in section IV(D).

Major service providers publish guides for investigators on how to request data,[40] 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 IP address or disguise the provenance of an email.

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, email headers can be carefully inspected to determine its route and origin.

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.[41] Furthermore, the SCA is silent on foreign law enforcement, but it suggests that any domestic law enforcement personnel can trigger a request.[42]

---

[39] Letters rogatory are the "customary method of obtaining judicial assistance from abroad in the absence of a treaty or executive agreement." http://travel.state.gov/law/judicial/judicial_683.html

[40] Apps. I-V.

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

[42] United States Department of Labor, *Wage and Hour Division*, http://www.dol.gov/whd/regs/compliance/web/SCA_FAQ.htm, (last visited Oct. 10, 2013) (Furthermore, as discussed in *Digital Evidence and the American Servicemembers' Protection Act*, ASPA does not appear to directly apply to private entities).

The status of the service provider is a key determinant of legal protection for user data. If the service provider is a non-public provider, then it is exempt from many 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 SCA and must comply with its rules generally prohibiting disclosure of content. To determine the classification of a service provider as public or non-public, a prosecutor should ask whether the service provider affords service to the community at large.[43] A company that administers email only for its employees is most likely 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[44] focuses on who owns the account whereas traffic data[45] focuses on who sent or received an email. Content data includes the actual substance of an email or telephone call such as subject lines or text in the body of an email. 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 email content requires a 2703(c)(1) warrant.[46]

Importantly, a preservation request can be made under 2703(f) pending the court order.[47] For a 2703(f) request, a government entity need only send a fax requesting the service provider to preserve all data in relation to the investigation.

Lastly, if a statutory exception is applicable, then public service providers may voluntarily disclose non-content and content data to the government.[48] For example, if exigent circumstances exist such as a kidnapping, then the government's request will fall within the statutory exemption.[49]

B. 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.[50] To ensure chain of custody

---

[43] US DEPARTMENT OF JUSTICE, EXECUTIVE OFFICE FOR UNITED STATES ATTORNEYS, SEARCHING AND SEIZING COMPUTERS AND OBTAINING ELECTRONIC EVIDENCE IN CRIMINAL INVESTIGATIONS 135

[44] 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

[45] 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.

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

[47] Id. at 18 U.S.C. 121 §§ 2703(f)

[48] Id.

[49] Stored Communications Act, 18 U.S.C. 121 §§ 2702(5) (1986).

[50] *See* Prosecutor v. Popovic, et al., 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).

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.[51]

C. Procedure on How to Request Service Provider Data [52]

Some major service providers such as Google and Facebook have corporate forms that require all data requests to be executed in the U.S. 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 provider.[53] 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 divorced from a device, the location, and any other reasonable information.[54] Furthermore, many service providers publish a guide for law enforcement investigators with forms for data requests and specific information about procedures. These guides can be obtained by contacting the specific service provider's legal office, searching online, or looking at the Electronic Frontier Foundation's page that stores these documents.[55] Comcast is one of many service providers that provide step-by-step data acquisition guidelines as outlined below.

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, email address, street address, phone 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.[56] 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.

---

[51] Erik Laykin, INVESTIGATIVE COMPUTER FORENSICS 76-69, 83-85 (2013).
[52] COMCAST, LAW ENFORCEMENT GUIDE, http://cryptome.org/isp-spy/comcast-spy.pdf
[53] Erik Laykin, INVESTIGATIVE COMPUTER FORENSICS (2013).
[54] Erik Laykin, INVESTIGATIVE COMPUTER FORENSICS (2013).
[55] Electronic Frontier Foundation, https://www.eff.org
[56] Interview with Chris Hoofnagle, Director, Information Privacy Programs, Berkeley Center for Law & Technology (Oct. 1, 2013).

D. Mutual Legal Assistance Treaties and Joint Investigation Teams

Mutual Legal Assistance Treaties ("MLATs") and letters rogatory allow international evidence exchanges in criminal procedures.[57] 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.[58] 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 requesting country's law. 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.[59] This trend demands strengthened transnational cooperation between competent authorities.[60] A JIT is an investigation team established for a specified time period, based on an agreement between two or more European Union ("E.U.") member states and/or competent authorities. If all parties are in agreement, then non-E.U. members may participate in a JIT.[61]

V. Conclusion

This brief paper has set forth strategies to acquire and authenticate digital evidence in a forensically valid manner. Careful cyberinvestigations can strengthen the prosecutions' case as well as provide linkage evidence connecting the accused to the alleged crime. Digital evidence acquisition is fundamental in all investigations within a modern law enforcement environment.

---

[57] U.S. DEPARTMENT OF STATE, BUREAU OF INTERNATIONAL NARCOTICS AND LAW ENFORCEMENT AFFAIRS, INTERNATIONAL NARCOTICS CONTROL STRATEGY REPORT (Mar. 7, 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).

[58] GOOGLE, TRANSPARENCY REPORT, n.d., *available at* http://www.google.com/transparencyreport/userdatarequests/legalprocess/#how_does_google_respond

[59] EUROPEAN COMMISSION: JOINT INVESTIGATION TEAMS, *available at* http://ec.europa.eu/dgs/home-affairs/what-we-do/policies/police-cooperation/jit/index_en.htm

[60] *Id*. (It is unclear whether "authorities" means states or may include international criminal tribunals.)

[61] EUROPOL, JOINT INVESTIGATION TEAMS, 2013, *available at* https://www.europol.europa.eu/content/page/joint-investigation-teams-989

The collection of digital evidence is the "rule rather than the exception" in current investigations.[62]

Two key themes dominate each procedure: First, the goal 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. This paper addresses data that is already in the possession of the OTP. Therefore, further points of discussion are warranted.

- What investments in training and equipment are necessary to enhance evidence gathering in a forensically valid way as well as increase the probative value of the evidence?

- Given the burdens of the MLAT and letters rogatory processes, should the ICC seek U.S. provider data on European servers or the JIT process?

[62] INTERNATIONAL CRIMINAL COURT, DIGITAL EVIDENCE REPORT, Oct. 2013

VI. Appendices I-VI

I. Sample Preservation Request Letter
II. Sample Language for Subpoenas, 2703(d) Court Orders, and Search Warrants
III. Sample Consent to Search Form
IV. List of Operating System and Preferred Methods
V. Electronic Frontier Foundation Law Enforcement Guide Overview

Appendix I: Sample Preservation Request Letter[63]

This letter serves as a formal request for the preservation of records and other evidence pursuant to 18 U.S.C. § 2703(f) pending further legal process. For the Yahoo! subscriber ID [*INSERT ID, email address, Group name, Flickr NSID, Flickr URL, or Profile URL*], you are hereby requested to preserve, for a period of 90 days, the records described below currently in your possession.

This request applies only retrospectively. It does not in any way obligate Yahoo! to capture and preserve new information that arises after the date of this request. This preservation request specifically applies to all records and other evidence relating to the subscriber(s), customer(s), account holder(s), or other entity(ies) associated with the subscriber(s) identified above, including, without limitation, [*include as may be relevant*]:

- Subscriber names, user names, screen names, or other identities;
- Mailing addresses, residential addresses, business addresses, email addresses, telephone numbers, and other contact information;
- Billing records;
- Information about length of service and the types of services the subscriber(s) or customer(s) used;
- Any other identifying information, whether such records are in electronic or other form;
- Connection logs and records of user activity for the subscriber(s) identified above, including log-in history and records identifying sent and received communications;
- All communications stored in the account(s) of the subscriber(s) identified above; and
- All files that are controlled by user accounts associated with the subscriber(s) identified above. At this time we are expecting to obtain formal legal process within 90 days. We acknowledge that if we do not serve legal process upon you in the next 90 days and do not request a 90-day extension, the preserved information may no longer be available.

[63] YAHOO!, COMPLIANCE GUIDE FOR LAW ENFORCEMENT 14, http://cryptome.org/isp-spy/yahoo-spy.pdf

Appendix II: Sample Language for Subpoenas, 2703(d) Court Orders, and Search Warrants[64]

Sample Subpoena Wording for Identification of a Yahoo! User

Any and all records regarding the identification of a user with the Yahoo! ID "_____" or Yahoo! email account "_____," to include name and address; Yahoo! email address; alternate email address; IP address and date and time of registration; account status; and log-in IP addresses associated with session times and dates.

Note: If Credit card numbers are sought, please identify any Yahoo! premium service used by the subscriber, if known, and insert: "credit card numbers used by the Yahoo! user to pay for Yahoo! premium services [or the name of the specific Yahoo! premium service used]."

Sample Subpoena Wording for Information About a Yahoo! Group and its Moderators

For the Yahoo! Group known as _____, email addresses for all moderators and members of the Group, the date the Group was created, the Group/List ID, and Group description.

Any and all records regarding the identification of the owners and/or moderators of the Yahoo! Group listed above, to include name and address; Yahoo! email address; alternate email address; IP address and date and time of registration; account status; and log-in IP addresses associated with session times and dates.

Sample Search Warrant Wording for Information Related to a Yahoo ID

Any and all information for Yahoo! ID "_____" or Yahoo! email account "_____," to include name and address; Yahoo! email address; alternate email address; IP address and date and time of registration; account status; and log-in IP addresses associated with session times and dates.
(If information related to email content is sought, add)

For the subscriber identified in Paragraph A above, the contents of any and all emails stored in the subscriber's Yahoo! account. [NOTE: Email content stored in domain-based email accounts hosted on Yahoo! or Flickr email must be requested explicitly.]
(If information is sought related to stored Yahoo! Briefcase files or Flickr photos, add)

Any and all contents of electronic files that the subscriber has stored in the subscriber's Briefcase and/or Flickr account.
(If Friends List information is sought, add)
Any and all Yahoo! IDs listed on the subscriber's Friends list.
(If information related to payments is sought, add)
Any and all methods of payment provided by the subscriber to Yahoo! for any premium services.

[64] YAHOO!, COMPLIANCE GUIDE FOR LAW ENFORCEMENT 15, http://cryptome.org/isp-spy/yahoo-spy.pdf

Sample Search Warrant Wording for Information about a Group and its contents

A. The identity of the moderators and members of the Yahoo! Group known as _____, including the date the Group was created, the Group ID, the dates that members joined the group, and the delivery options for the current members.

B. The current contents of the Files, Photos, Links, and Polls section of the Yahoo! Group known as _____ and the archived message posts, and all records relating to the activities of the Group members, as reflected in the Group Activity Log.

Appendix III: Sample Consent to Search Form[65]

(This request must be accompanied by a subpoena and a cover letter or fax bearing the official seal of the requesting agency)

I, _____ the account holder of the Yahoo! account with Yahoo! ID _____ understand that my account is being sought in connection with an official law enforcement investigation. As part of that investigation, I hereby grant my consent to authorize the following agency: _____, to receive, review, copy, and otherwise obtain access to all information of any kind held by Yahoo! relating to my accounts and any and all accounts that I have linked to the following Yahoo! ID _____, including but not limited to information about my identity, my online activities, and the contents of all electronic files or communications maintained by Yahoo! related to me or my ID.

Pursuant to the consent I hereby request that the following specific information be provided:
_____
In connection with this authority to release information, I do hereby agree to hold harmless and do forever hold harmless Yahoo! for the disclosure of such information and do forever waive on my behalf, and on behalf of my heirs and assigns, any and all claims resulting from Yahoo!'s disclosure of any information related to my account pursuant to this authorization.
The following information should be used by Yahoo! to verify my identity:
Login name/Yahoo! ID Yahoo! email address Alternate email address Birthday (as indicated on this account) Answer to secret question

(Contact Yahoo! Compliance for secret question) City, state, and zip Gender
_____ Yahoo! user's signature
_____ Date

[65] YAHOO!, COMPLIANCE GUIDE FOR LAW ENFORCEMENT 17, http://cryptome.org/isp-spy/yahoo-spy.pdf

Appendix IV: List of Operating System and Preferred Methods

This chart displays the generally recommended shut down method based on the operating system employed by the target device. The list of operating systems is not exhaustive, but instead lists only the popular operating systems investigators are likely to find.[66]

Pull plug From device	**Traditional method via internal commands**
Windows Version 3.11	Windows 2000 Server
Windows 95	All Macintosh operating systems
Windows 98	Linux/Unix
Windows 2000	
Windows XP	

[66] ROBERT MOORE, CYBERCRIME: INVESTIGATING HIGH-TECHNOLOGY COMPUTER CRIME 212-17 (2010).

Appendix V. Electronic Frontier Foundation Law Enforcement Guide Overview
*Extracted from Electronic Frontier Foundation; Full version available at https://www.eff.org/files/EFF_Social_Network_Law_Enforcement_Guides-sprdsht.pdf

SOCIAL MEDIA—A Guide to the Law Enforcement Guides

Date	Facebook 2010
Date, length, link (if available) and other info	May 2010, 5 pages
How does Guide address Legal Process Requirements under Electronic Communications Privacy Act (ECPA)?	"we will provide records as required by law." (p.2)
How does site define and/or distinguish different types of user information	User ID number, email address, date/time account was created, most recent logins, registered mobile number (p. 4) "Expanded Subscriber Content (sometimes referred to as Neoprint)": Contact information, mini-feed, status update history, shares, notes, wall postings, friend listings (include friend IDs), group listings (including group member IDs), future and past events, video listings (p. 4)
What other info is available?	"User photos (sometimes referred to as User Photoprint)": User uploaded photos and photos tagged with user's name, group information, private messages (p. 4)
How does LE Guide address IP and other logs?	• IP logs contain same data as 2008/09 and also include Session Cookie -- HTTP cookie set by user session • Logs are often incomplete, but if available will be provided (p. 4)
How long is data generally retained? How long in reponse to preservation request?	90 days, but an extension can be made if necessary. "By default we will return data no older than 90 days prior to the date we receive the request." (p. 2)
Is content that has been changed or deleted by user (including private messages) still available?	If messages are retained by user, they are available (page 4)
Can law enforcement monitor user account without user knowledge?	Will normally disable account unless law enforcement clearly specify that doing so will hurt investigation (page 2)

Does site have exception for emergency disclosure?	Can provide upon answering 3 questions:Describe emergency? Provide ID of users involved? Provide location of evidence? (p. 5)
Does site charge law enforcement fees?	Does not say
What are the requirements to begin preserving records?	Request to preserve from law enforcement, with ID, name of agency, and contact info (p. 3)
Does site address fake accounts created by law enforcement?	Will "always disable accounts that supply false or misleading profile information or attempt to technically or socially circumvent site privacy measures." (p. 2)
Can user consent to data release?	Does not say
How will site deliver data?	Does not say
Other info?	"We are required to disable accounts engaged in illegal activity, even if that activity is brought to our attention through a request for records." (p.5)
Sample forms or sample language?	Emergency Disclosure Form