Obtaining and Admitting Electronic Evidence

In This Issue

November 2011
Volume 59
Number 6

United States
Department of Justice
Executive Office for
United States Attorneys
Washington, DC
20530

H. Marshall Jarrett
Director

Contributors' opinions and statements should not be considered an endorsement by EOUSA for any policy, program, or service.

The United States Attorneys' Bulletin is published pursuant to 28 CFR § 0.22(b).

The United States Attorneys' Bulletin is published bimonthly by the Executive Office for United States Attorneys, Office of Legal Education, 1620 Pendleton Street, Columbia, South Carolina 29201.

Managing Editor
Jim Donovan

Law Clerk
Carmel Matin

Internet Address
www.usdoj.gov/usao/reading_room/foiamanuals.html

Send article submissions and address changes to Managing Editor,
United States Attorneys' Bulletin,
National Advocacy Center,
Office of Legal Education,
1620 Pendleton Street,
Columbia, SC 29201.

Using Log Record Analysis to Show Internet and Computer Activity in Criminal Cases

Mark L. Krotoski
National Computer Hacking and Intellectual Property (CHIP) Program Coordinator
Computer Crime and Intellectual Property Section

Jason Passwaters
President of EdgePoint Forensics, LLC

I. What are log records? Why are they important?

Log record analysis is an underutilized area of expertise that can effectively be used in a variety of criminal investigations and trials. Log records essentially memorialize Internet communications and connections on various devices along the path of transmission. Because of the importance of Internet communications and activity, log records are rich in data and may contain significant evidence in many criminal cases. Common log records may include Web access or firewall log records.

Log records are useful because they record commands or other information transmitted through the Internet. For example, log records may show places visited on the Internet by indicating the click-by-click activity by a computer user. Log records may reveal identifying information, such as the type of operating system and browser that were used by the computer transmitting the request. This type of information is called "user-agent string" information and is discussed further below.

In many cases, log records can be important to show what activity took place on a computer or device even when the computer is no longer available, data on the computer was deleted, or malware was executed solely in Random Access Memory. While it certainly helps to use log records in conjunction with records from the computer, log records may reveal computer activity even without the original computer or its records because log records are external to the computer or device.

In addition to Internet activity, log records are also important in intrusion and botnet cases. Botnets are a collection of compromised computers connected to the Internet that were exploited through the use of malicious software. Log records can reveal connections to computers administering the botnet. For example, in the case of an HTTP-based (Hypertext Transfer Protocol) Command & Control (C&C) server used to administer a botnet, the C&C aspect is nothing more than a Webserver designed to help maintain and administer the botnet. All victim systems will check-in with the C&C server at regular intervals to the same resource or file that sits on the server. Each check-in causes a specific entry in the server's access logs. From the victim's perspective, the log records include significant information regarding the location of the victim, the size of the botnet, types of systems being targeted (for example, browser types, operating systems, etc.), and more. From the attacker's perspective, the log records may capture administrative activity including the Internet Protocol (IP) addresses used and information about the botnet owner's system.

A. Overview

This article reviews the use of log record analysis in criminal cases. Lessons learned from recent trials and investigations are shared. The issues discussed include answers to the following questions:

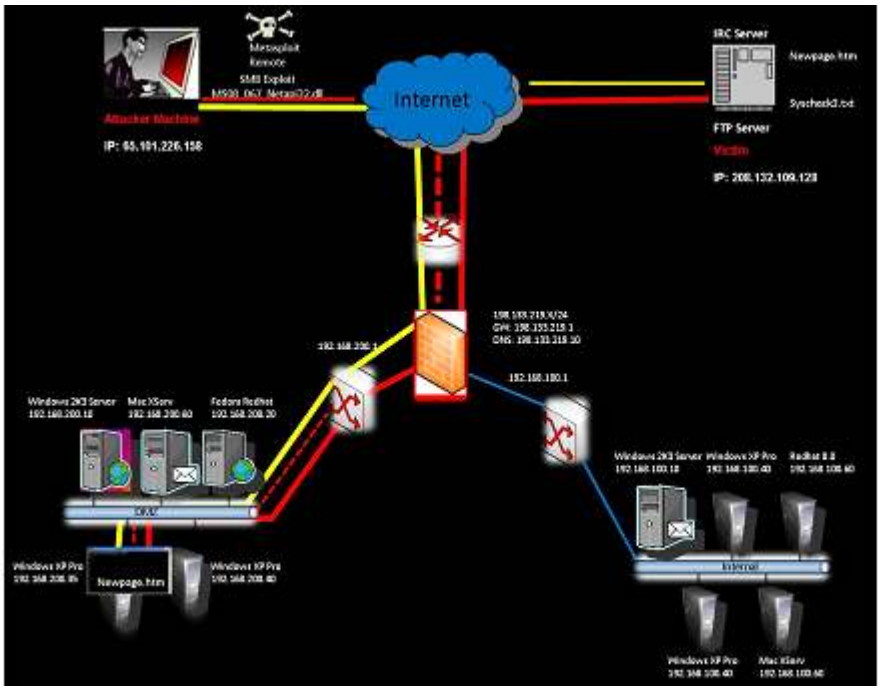
- What are log records and how are they created?
- How are log records retained and obtained through legal process?
- Can log records (like other electronic evidence) be manipulated?
- How does an analyst conduct log record analysis and what tools are used?
- What are some recent case examples in which log records were successfully used to provide information that was not readily available from other sources?

B. How are log records created?

To illustrate how log records are created and used in criminal cases, consider a hypothetical defendant who used a computer to commit an offense that targeted a victim computer or network. The conduct can be just about any offense involving a computer, such as an intrusion or unauthorized access (18 U.S.C. § 1030), misappropriating trade secret information (18 U.S.C. § 1832), wire fraud involving the transmission of an interstate communication (18 U.S.C. § 1343), or identity theft (18 U.S.C. § 1028). The transmission of information from the defendant's computer to the targeted victim computer will travel along a path on the Internet that involves dozens or more computers or devices. The figure below shows a simplified example of an internal network. At each system or device along the transmission path, logging records will record certain activity and events that may provide valuable evidence of the subject crime.

Hypothetical criminal scenario: An attacker exploits an unpatched vulnerability to gain unauthorized access to a company Web server. The firewall logs may provide an investigator with useful information about the activity. These records may contain artifacts that show the attacker's IP address, file names of any transferred data via FTP (File Transfer Protocol, used to exchange files over the Internet), attack and exploit signatures, and more. The various systems along the path, often obstructed from the view of the attacker, constantly log elements of the attack as it progresses. Each transmission or activity along the path creates new log records. This trail of information may provide useful leads for the investigation. These records can provide a time line of the unfolding events and be used to correlate the information on other log records or computers.

The figure and accompanying table below show a simplified network diagram of an intrusion into a corporate network. The PIX®/ASA (Private Internet eXchange/Adaptive Security Appliance) firewall, depicted as the brick wall at the center of the diagram, is a network security appliance that allows or denies network traffic based on certain rules set by an administrator. The log records created by these types of network devices are normally used to identify malicious activity or to locate and correct problems on a network. However, to an investigator these records may reveal a detailed account of network-level transactions much like an online personal bank account would have log records showing financial transactions and activity. The log entries contain detailed information about each connection that was denied or allowed by the device.



The transmissions involving the intruder and victim systems will pass through the firewall each time a connection is made. The following steps show a hypothetical scenario:

Step	Activity	Possible Log Information
1	Intruder scans for vulnerabilities	Scanning is easily identified in firewall logs as each TCP/UDP (Transmission Control Protocol / User Datagram Protocol) connection attempt is logged. The logs will show what services are being targeted, which IP addresses are being scanned, where (IP) the activity may be originating, etc.
2	Intruder attempts to exploit known vulnerability	The logs will show the exploitation of a known vulnerability. For example, if a user exploits an SMB (Server Message Block) vulnerability, the logs will capture the connection each time the exploit is attempted over Port 445.
3	Exploit causes internal host to retrieve files from remote FTP server	The logs will show the time of activity, filename, account used, IP address of the server or first proxy, size of file, etc.
4	Internal host connects to remote Internet Relay Chat (IRC) server	The logs will contain entries showing each unique IRC connection, the IP or first proxy for the connection, duration, total bytes transferred, time, etc.

Types of logging devices: What are examples of computers or devices that may log information? The types of devices along the transmission path will vary depending on the objective of the device or computer. For example, firewall log records may show, among other things, what IP addresses are trying to access the network, what internal systems they accessed, and the duration of the connection. Web Server Access Logs may include details about a visit to a Web site such as the pages or resources requested, the outcome of a request, the visitor's IP address, and click-by-click activity. Proxy server logs may confirm the source and destination of the computer user along with the activity. A network diagram may be useful to identify key devices that may contain useful log entries. Some common examples of devices and log records along the path include:

- Firewall Logs
- Web Server Access Logs
- Simple Mail Transfer Protocol / Internet Message Access Protocol Servers (email)
- FTP Servers (file transfer protocol)
- Proxy Server Logs
- Secure Shell Servers (remote access)
- Routers and Switches
- Chat Servers
- Intrusion Detection Systems
- DNS Servers (Domain Name System)
- Victim and Attacker Systems

Information collected in log entries: The type of information that may be retained in log records can vary depending on the role of the logging device. What are some examples of the type of information that may be recorded by logging activity? The excerpt below shows another example of Apache access logs from a Web server. The different fields have been numbered to identify the type of data that may be included in the log record.

No.	Field or Activity	Context/Notes
1	Requestor's Internet Protocol (IP) address	The user's IP address requesting information over the Internet or last connection computer (such as a proxy computer) In the example, the IP address is 218.1.111.50.
2	Identity and user id	The identity value and user id of the user requesting the resource at the Webserver. In the example, both values are empty. The identity check is turned off by default with the Apache server as the value is highly unreliable. The user id of the account associated with the request is blank in this case. This is normally due to the resource not requiring authentication in order to access it.
3	Date/Timestamp	Date and time of logged activity. The time zones in one set of logs may need to be normalized with different time zones used in other logs or on a computer. In the example, the date is March 13, 2005 and the time is 10:36:11 a.m.

4	HTTP (Hypertext Transfer Protocol) Method	The type of method may reveal the activity. For example, the "GET" method may be used to retrieve data; the "POST" method may be used to store data, send an email, or order a product. The example displays a GET method
5	Request URI	Indicates what was requested at the server The example shows a user has requested www.yahoo.com a number of times which indicates the user has visited the main Yahoo! page.
6	HTTP Protocol Version	This is the HTTP protocol version used by the client during the request. The example shows all clients utilized HTTP version 1.1 for each of the requests.
7	HTTP Status Code	Indicates how the server resolved the request—success, redirect, or error. For example, a 404 would indicate the requested resource was not found on this server. A 200 would indicate the request was fulfilled successfully by the Webserver. The example notes: 403 (Forbidden).
8	Total bytes transferred	The size of transferred files/data (for example, image or file) not including the HTTP response headers sent by the server. The example shows 1063 bytes were returned by the Webserver.
9	Referrer	Where the request originated, such as the Webpage or Uniform Resource Locator (URL) (for example, the referrer may show that the request came from Facebook) The example notes a blank referrer field indicating the field was purposely suppressed or the Uniform Resource Identifier (URI) was requested directly and not referred by another resource on the Internet.
10	User Agent String	The type of operating system, browser and other applications from the user's computer The example indicates the client had a user-agent string of "Mozilla/4.0 (compatible; MSIE 4.01; Windows 95)" revealing information about the Web browser and operation system.

As the illustration shows, log records contain a substantial amount of content that may be relevant in a criminal case. For example, the timing of key events over the Internet may be confirmed through log records, such as click-by-click activity. The log records may reveal identity information that connects the activity to user attributes, including the IP address used and the type of operating system, browser, and applications of the computer user. Logs are timestamp-centric, making them ideal for filling in time line gaps in an investigation.

Log records from different servers may use different formats or time zones. As explained in Part IV.B below, log records can be normalized to make them more readable and to focus on key events or activity.

II. Retaining and obtaining log records

A. Limited log record retention period

Log records are usually maintained for a very limited period. Each provider or company determines how long to retain its records. In past cases, many providers have maintained log records for only a few days. Other providers may retain the records for a week or so. Some providers may not log all events.

Because of the limited retention period for log records, it is useful to consider other places to find the same or similar data. For example, consider a scenario where a user from within a corporate network was suspected of sending sensitive company data to a remote storage site on the Internet. The Web access logs on the remote server may not be accessible. However, by analyzing the Domain Name Service (DNS) server logs, an investigator may be able to confirm the initial DNS request for the remote site. This identification would be important in both confirming the activity and developing a time line of events.

B. Legal process steps: identify, preserve, and collect

To obtain log records, three steps are recommended: (1) identify the types of records and where they are maintained; (2) preserve the records with the providers maintaining them; and (3) use legal process to collect the records.

There are a variety of common log records that a company may maintain. *See supra* Part I.B (listing examples). After identifying log records maintained by providers, as covered by the Electronic Communications and Privacy Act (ECPA), 18 U.S.C. §§ 2701–2712, the records should be preserved under 18 U.S.C. § 2703(f)(1) pending further legal process. This provision requires the provider to retain the requested records for 90 days. The government may renew the initial request for an additional 90 days. *Id.* § 2703(f)(2). The Computer Crime and Intellectual Property Section (CCIPS) has model preservation request letters, if needed. As a starting point, consider preserving the log records enumerated in Part I.B above.

After the records have been preserved, the next question is what legal process may be warranted? Part of the answer depends on whether the log records contain content. A § 2703(a) search warrant may be used to obtain content information. *See* 18 U.S.C. § 2703(a). Generally, "contents" under the ECPA, "when used with respect to any wire, oral, or electronic communication, includes any information concerning the substance, purport, or meaning of that communication[.]" 18 U.S.C. § 2510(8) (2010). For example, some courts have concluded that uniform resource locator (URL) or Web address information may include content. *See, e.g.*, *In re Pharmatrak, Inc.*, 329 F.3d 9, 16 (1st Cir. 2003) (noting that content is revealed when a search phrase "appear[s] in the URL").

While it may be possible to obtain non-content log records through a subpoena or § 2703(d) order, the use of a § 2703(a) search warrant, as a matter of prudence, provides the broadest legal basis to obtain log records, particularly if content is involved. CCIPS is available to assist in answering these legal questions. For more information, call 202-514-1026.

III. Can log records be manipulated?

When dealing with electronic evidence, one question that may arise is whether log records can be manipulated. While it is possible that log records, like other forms of electronic evidence, can be modified, it would be highly improbable that all the log records along the path of transmission could be altered because each of the devices creating log records would have to be compromised to some degree. There are simply too many records under the control of other entities that would have to be modified.

To illustrate, assume that our computer attacker made unauthorized access to a victim network or computer on the Internet. In doing so, the computer attacker connected through firewall, Web, mail, and proxy servers, only a few of the possible servers at which log records may be maintained. To manipulate information in a log record, the records at each server would have to be modified in a consistent manner. Information on the attacker's computer and victims' computers would have to be changed. Furthermore, each click on the Internet creates new log records along the path of transmission. These records would also have to be modified.

As the example shows, there are simply too many records to manipulate if an attacker or defendant intended to do so. Consequently, it is highly improbable that log records can be effectively manipulated for use in an investigation or in court. If an allegation was made that log records introduced in court could possibly have been manipulated, an analyst could compare other log records along the path. The claim could readily be rebutted by comparing information in other log records with those from the attacker or victim computers. This also provides a built-in check to demonstrate that the records have not been manipulated. If one log record was changed, it can be compared with records on the user's computer, the victim's computer, and other log records.

In court, questions concerning the trustworthiness of records normally go to the weight of the evidence and not to admissibility. One district court opinion generally placed this issue in perspective when dismissing a challenge to admit emails:

> The defendant argues that the trustworthiness of these e-mails cannot be demonstrated, particularly those e-mails that are embedded within e-mails as having been forwarded to or by others or as the previous e-mail to which a reply was sent. The Court rejects this as an argument against authentication of the e-mails. The defendant's argument is more appropriately directed to the weight the jury should give the evidence, not to its authenticity. While the defendant is correct that earlier e-mails that are included in a chain-either as ones that have been forwarded or to which another has replied-may be altered, this trait is not specific to e-mail evidence. It can be true of any piece of documentary evidence, such as a letter, a contract or an invoice. Indeed, fraud trials frequently center on altered paper documentation, which, through the use of techniques such as photocopies, white-out, or wholesale forgery, easily can be altered. The possibility of alteration does not and cannot be the basis for excluding e-mails as unidentified or unauthenticated as a matter of course, any more than it can be the rationale for excluding paper documents (and copies of those documents). We live in an age of technology and computer use where e-mail communication now is a normal and frequent fact for the majority of this nation's population, and is of particular importance in the professional world. The defendant is free to raise this issue with the jury and put on evidence that e-mails are capable of being altered before they are passed on. Absent specific evidence showing alteration, however, the Court will not exclude any embedded e-mails because of the mere possibility that it can be done.

United States v. Safavian, 435 F. Supp. 2d 36, 41 (D.D.C. 2006).

IV. Key steps in conducting log analysis

Five key steps are necessary to conduct log analysis: (1) data collection, (2) data normalization, (3) analysis, (4) correlation, and (5) report.

A. Data collection

The data collection phase involves assembling the log records and other computer records that will be used in the analysis. For example, log records may be obtained from a proxy, a victim company, or a social networking site such as Facebook. Moreover, information on a computer or hard drive, such as Internet activity records, may be used to correlate the activity reflected in the log records.

All best practices in traditional computer forensic evidence collection apply to the collection of log records as well. The integrity of the data is paramount, as it is with all evidence. Log records are no different, but the challenge lies in identifying records that may be helpful to the investigation prior to logs

being overwritten or deleted. The investigator must be able to call on expertise that expands past the computer hard drive and onto the greater network where valuable artifacts reside.

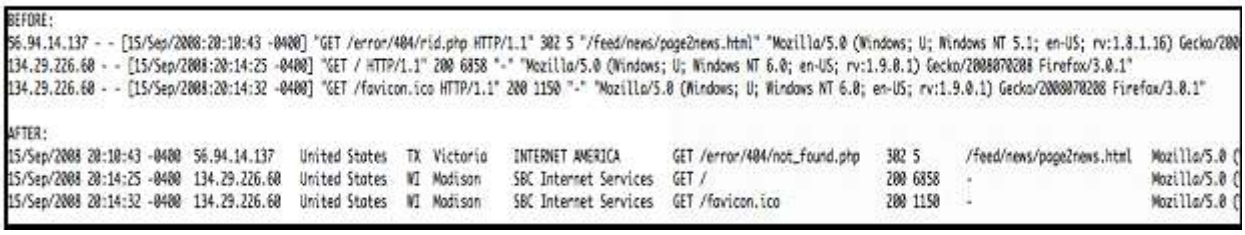
By gathering log records from different devices such as a Web server, proxy, or Internet Service Provider (ISP), the analyst can confirm and corroborate Internet activity. For example, the same request to visit an email provider such as Gmail may be reflected in the independent records of the Gmail Web server and proxy server. This type of confirmation in different records is important because events can be corroborated and it is very difficult to challenge or question the records once they have been confirmed by an independent source.

B. Data normalization

Data normalization is the process of parsing, filtering, and revealing additional metadata to facilitate the extraction of key information. For example, oftentimes data sets are taken from different time zones. The practice of synching all time-stamps into a single time zone is one part of the normalization process. Another step in normalization is revealing hidden metadata associated with the different fields found in the logs. For instance, IP addresses can be associated with the following metadata:

- Geographical location of IP addresses
- ISP information
- Association with known harmful activity (for example, spamming block lists)
- Organizational affiliation
- Derivative log data (such as an Internet company's unique naming convention for certain events)

Log analysis often involves very large data sets. Adding this data is essential in order for it to be leveraged and used across all data simultaneously. Some log tools may contain parsers that assist in the normalization process, but knowledge in a scripting language (such as PERL or Python, among others) and/or programming language is considered a necessity when processing large data sets. The graphic below illustrates the normalization of Apache Web access logs. Note the cleaner tab delimited format and the addition of metadata. This format makes it much easier to combine with other related and normalized data sets from other sources and sets the stage for inputting the data into analysis tools.



```
BEFORE:
56.94.14.137 - - [15/Sep/2008:20:10:43 -0400] "GET /error/404/rid.php HTTP/1.1" 302 5 "/feed/news/page2news.html" "Mozilla/5.0 (Windows; U; Windows NT 5.1; en-US; rv:1.8.1.16) Gecko/200
134.29.226.60 - - [15/Sep/2008:20:14:25 -0400] "GET / HTTP/1.1" 200 6858 "-" "Mozilla/5.0 (Windows; U; Windows NT 6.0; en-US; rv:1.9.0.1) Gecko/2008070208 Firefox/3.0.1"
134.29.226.60 - - [15/Sep/2008:20:14:32 -0400] "GET /favicon.ico HTTP/1.1" 200 1150 "-" "Mozilla/5.0 (Windows; U; Windows NT 6.0; en-US; rv:1.9.0.1) Gecko/2008070208 Firefox/3.0.1"

AFTER:
15/Sep/2008 20:10:43 -0400  56.94.14.137   United States  TX  Victoria   INTERNET AMERICA       GET /error/404/not_found.php  302 5     /feed/news/page2news.html  Mozilla/5.0 (
15/Sep/2008 20:14:25 -0400  134.29.226.60  United States  WI  Madison    SBC Internet Services  GET /                         200 6858  -                          Mozilla/5.0 (
15/Sep/2008 20:14:32 -0400  134.29.226.60  United States  WI  Madison    SBC Internet Services  GET /favicon.ico              200 1150  -                          Mozilla/5.0 (
```

The "after" portion of the record provides the information in a format that allows focus on key events or fields. For example, the first line of the lower portion of the illustration indicates the date and time of the activity (September 15, 2008 at 20:10:43), the IP address where the request came from, the geographic and ISP information related to the IP address, and the other Web access log fields covered previously.

C. Analysis

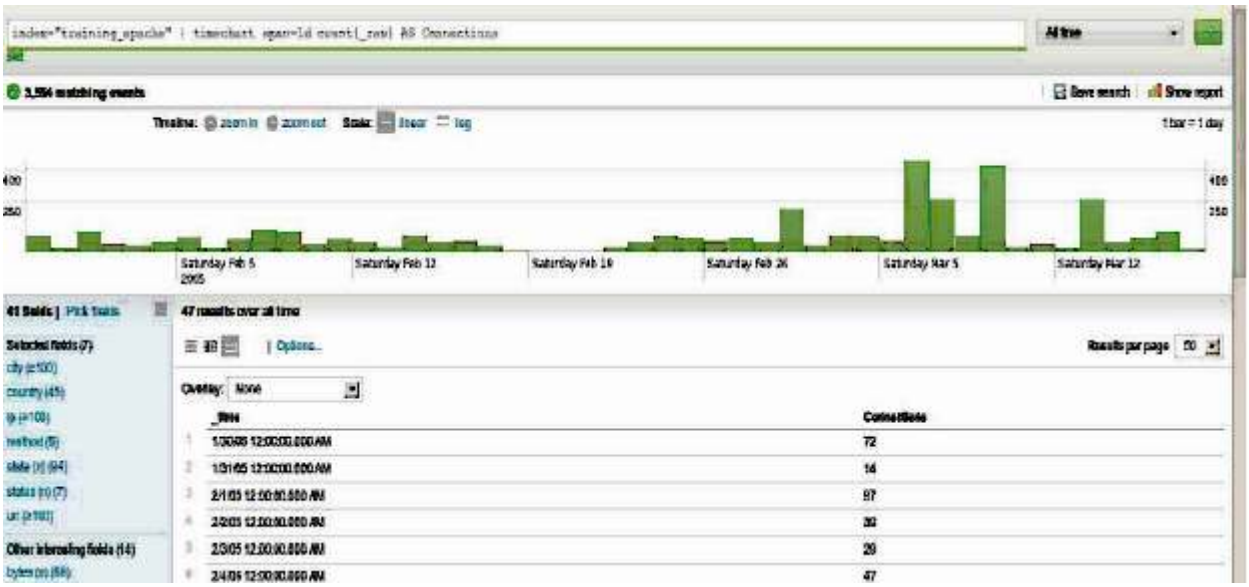
The analysis phase includes a review of the log entries in a manner that is relevant to the investigation and case. Log analysis often deals with large and disparate data sets that require a phased approach to analysis. It is important to understand the data being analyzed before digging deeper. A few of the many questions that may need to be answered at the front end are:

- What kind of systems conducted the logging? Firewalls, Webserver, etc.?
- What log format is being used?
- What fields are being logged and how are they defined?
- How do the different data sets relate to each other? Are they in the same network, same attacker or same victim data, etc.?

By using the time and date information—after normalizing different time zones on different log records—a time line of key events can be developed. The sequence of events may provide new leads for the investigation.

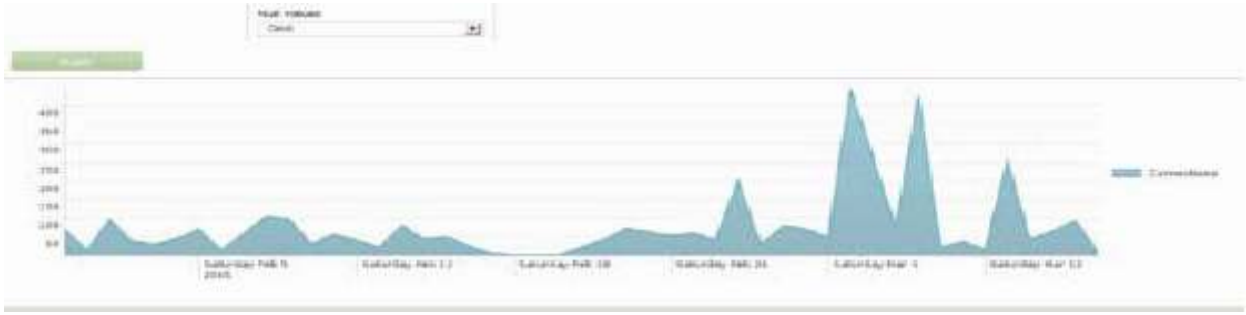
A "macro"-to-"micro" approach is generally useful for the analysis. Starting with general statistics allows the analyst to get to know the data. Accustoming one's self with the data in this way allows any unusual or suspicious activity to become more noticeable when deeper analysis begins later on. Beginning with a macro view on analysis will quickly identify the relevant issues, such as:

- Time period for an attack
- Type of attack
- Reconnaissance activity
- Automated vs. manual attack
- Signatures for known tools



The next step involves a deeper level of analysis of the log data. It is essential to use a tool that allows the analyst to mine through the data and interrogate it. Log records are time-stamp centric so any interactive time line-based tools will be helpful. The key to deeper analysis is not getting lost in the noise, as most log data will contain large amounts of unrelated data. The graphic below provides an example of

using an application named Splunk to conduct log analysis. The application allows the analyst to data mine, drill down, and interrogate the data very quickly. The time line allows information such as periods of high activity to stand out immediately.The image below indicates information from the "Show report" tool in the top right corner of the image above.



D. Correlation

The correlation phase involves the comparison and confirmation of common records or activity on different log records or computer records. For example, log records may show that a user initiated a request through a social networking site, used a proxy to conceal the user's source or origination point, and then made unauthorized access to a computer or network. Log records from the victim company (such as firewall logs) may be compared with log records from the proxy site and the social Internet site. This comparison may highlight useful investigative leads as patterns emerge and key events and relationships are identified. The comparison of the records may also provide corroboration of the Internet activity at trial. Independent log records from different companies may confirm the particular activity taking place through the connections.

A key aspect of the correlation phase is relating the different data sets to key elements of the investigation or other data sets. Artifacts found through analysis of the log records can often be correlated with those found on a victim or suspect system through traditional hard drive forensics. For example, Internet activity to specific Web sites can be correlated in both the browser history logs, such as the index.dat file in the case of Microsoft Internet Explorer, and the Web access logs found at the visited Web server.

E. Report

The report phase ensures that the analysis and conclusions are summarized and accompanied by the bases in support of the conclusions. The expert's report is used to prepare for the trial testimony and to satisfy the pretrial notice requirements of Rule 16(a)(1)(G) of the Federal Rules of Criminal Procedure. In civil cases, the expert disclosure requirements are mandated under Rule 26(a)(2) of the Federal Rules of Civil Procedure.

Report writing for the technical analyst can be as challenging as the analysis itself. The ability to convey technical analysis and conclusions to non-technical audiences is required in forensic log analysis as it is with most forensic disciplines. The forensic report will focus on and summarize the primary opinions and bases in support of the forensic conclusions.

The Rule 16(a)(1)(G) pretrial notice obligation in criminal cases expressly provides:

> At the defendant's request, the government must give to the defendant a written summary of any testimony that the government intends to use under Rules 702, 703, or 705 of the

> Federal Rules of Evidence during its case-in-chief at trial. If the government requests discovery under subdivision (b)(1)(C)(ii) and the defendant complies, the government
>
> must, at the defendant's request, give to the defendant a written summary of testimony that the government intends to use under Rules 702, 703, or 705 of the Federal Rules of Evidence as evidence at trial on the issue of the defendant's mental condition. The summary provided under this subparagraph must describe the witness's opinions, the bases and reasons for those opinions, and the witness's qualifications.

FED. R. CIV. P. 16(a)(1)(G).

The log analyst's report will indicate, among other things, what media or log records were used in the analysis. Identifying information such as an IP address or user-agent information may be provided about the particular computer user. Conclusions about the user's activities such as the transfer of data, sites visited, or other communications may also be included. A time line of key events may be useful in the report as well. If the computer user's hard drive indicates that information was deleted, the log records may reveal what transmissions were made by the computer. Other relevant details for the case will also be summarized. Because of the technical nature of log records, it is helpful to include graphics and tables that may summarize the information and opinions. In supporting the conclusions, the log records may provide a unique chance to highlight the corroboration of the identified activities based on confirmation of log records obtained from different companies. Another key area in the report may be confirming events identified in a forensic review on the user's laptop with information from the log records that were created external and independent of the laptop. In addition to fulfilling the pretrial notification requirements, a well-written report will focus on the key issues to be presented at trial.

V. Recent case examples

The usefulness of log records in investigations and criminal cases can be highlighted by considering some scenarios from recent cases. While log records may assist in confirming a wide variety of activity taking place on the Internet, four examples are noted: (1) email account activity; (2) posting and deleting content on the Internet; (3) unique identifying information about the user; and (4) interstate commerce activity.

A. Email account activity

Log records may reveal specific activity in an email account such as the places that were visited in the account or whether any email was sent during a particular visit. Other common records from an email provider, such as IP connection logs that reveal the IP address connected to the account by date and time or basic account subscriber information associated with the account, will not contain this information.

Consider a scenario where a user sends a message from a Web-based email service such as Gmail, Hotmail, or Yahoo!. The Web access logs will capture this activity albeit in a somewhat non-understandable format to the average observer. The two entries below show a visitor navigating to the "compose" function of a Web-based email service and then subsequently sending an email. Note that some fields from the log have not been included for the sake of brevity.

IP Address	Status Code	HTTP Method	Uniform Resource Identifier (URI)
113.23.10.11	200	GET	http://us.mc1100.mail.yahoo.com/mc/compose?..
113.23.10.11	200	POST	http://us.mc1100.mail.yahoo.com/mc/compose?...

The fields in this scenario are defined as follows:

- IP Address: IP where the request originated
- Status Code: The outcome of the request. In this case "200" indicates the Web server successfully resolved the request.
- HTTP Method: The HTTP method sent to the Web server. The GET request is the initial "click" on the "compose" link on the page. The POST request is the "click" of the "send" button on the page.
- URI: The Web server's content or resource that has been requested by the user. In this case it is the part of the site that allows a user to compose and send an email.

This information from the log records shows that the particular user visited an email account and composed and sent a message. While this evidence is external to the user's computer, it may be important to confirm records and activities on the user's computer if it is seized or available in the investigation.

B. Posting and deleting content on the Internet

Analysis of the access logs can also confirm a user's activity to post or delete information in an account. Considering how content is shared on the Internet is helpful to better understand the way such confirmation works. The nature of the Web revolves around dynamic content that is often provided by the end users sitting behind a computer. Usually, requests are sent back and forth between systems without any direct interaction from the user. Social networking sites have created an environment that allows easy sharing of content across the Web. Each time content is shared or requests are sent, the receiving servers generate a specific log entry in different logs across numerous networks. These logs can tell us what was requested, from what resource or page the request was generated, details about the system requesting the resource, and the outcome of the request. Facebook is one of the more popular social networking sites with nearly 700 million active users. If requested and received, the Web access logs can essentially retrace a user's activity on the site. The actual content of a posting may not be determined through the logs themselves but the action of posting, deleting, or logging in/out can be confirmed through analysis of the access logs.

The table below contains some of the fields that would be found in access logs related to Facebook activity. Note that other data would be mixed in with a large amount of noise. The order of log entries can be summarized as such:

- A user navigates to Facebook.com and logs into an account.
- The user hovers over a link for Facebook ID 123456 from their home page.
- The user navigates to the home page of Facebook ID 123456.
- The user posts comments to the home page of Facebook ID 123456.
- The user deletes comments from the home page of Facebook ID 123456.
- The user logs out of their Facebook account while on the home page of Facebook ID 123456.

HTTP Method	HTTP Status	Request URI	Referer	Description
GET	200	/	–	User navigates to facebook.com. Lack of referrer indicates user likely entered URI into browser.
POST	302	/login.php?login_attempt=1	https://www.facebook.com/index.php	User logs into account and is redirected upon sending username and password. Referer shows user logged in from main facebook.com page.
GET	200	/home.php	https://www.facebook.com/index.php	User is sent to the home page associated with their account.
GET	200	/ajax/hovercard/user.php?id=123456	https://www.facebook.com/home.php	User hovers over a Facebook user's account link. The facebook user's Facebook ID is 123456.
GET	200	/joesmith	https://www.facebook.com/home.php	User navigates to Facebook user Joe Smith's page. This coincides with previous Facebook id of 123456.
POST	200	/ajax/updatestatus.php?_a=1	https://www.facebook.com/joesmith	User enters text and posts comment to home page of Facebook ID 123456 (Joe Smith).
POST	200	/ajax/minifeed.php	https://www.facebook.com/joesmith	User deletes text from home page of Facebook ID 123456 (Joe Smith).
POST	302	/logout.php	https://www.facebook.com/joesmith	User logs out of Facebook account and is redirected. The referrer field shows the user logged out while on the homepage of Facebook ID 123456 (Joe Smith).
GET	200	/index.php	https://www.facebook.com/joesmith	User goes to main Facebook page. Referer shows user came from home page of Facebook ID 123456 (Joe Smith).

A number of the fields that would have been logged have been redacted but these entries illustrate some of the artifacts that can be identified.

C. Unique identifiers

One recurring issue in investigations and cases is identifying the computer user behind the activity. Log records may contain useful information about the computer user. This article has addressed how the IP address may be identified in the log records. However, the identification information in those log records can indicate even more about the particular user.

For example, log entries often contain information that correlates directly to the hardware and/or software of the requesting system. The user-agent string is one such example that provides information related to the browser type/version, the operating system, and other third-party plug-ins or applications. It is normally logged at the Web Server in the Web access logs. An example is shown below:

```
Mozilla/5.0 (BlackBerry; U; BlackBerry 9800; zh-TW) AppleWebKit/534.8+ (KHTML, like Gecko)
Version/6.0.0.448 Mobile Safari/534.8+
```

This user-agent string tells us the following details about the visitors:

- The user is visiting with a BlackBerry with Blackberry OS version 6.0.0.448.
- The user's client is localized for a "Chinese-Taiwan" language setting (zh-TW).

- AppleWebKit build 534.8
- The KHTML layout engine is used.
- A Safari-based mobile browser is used.

All of this information can be corroborated through traditional mobile device forensics or other elements of the investigation. It should be noted that it is trivial to spoof the user-agent string since other information related to the investigation may be considered when determining the credibility of the information contained in the user-agent string.

D. Interstate commerce

Many offenses contain an interstate commerce element. For example, wire fraud under 18 U.S.C. § 1343 requires a transmission in interstate or foreign commerce; interstate transportation of stolen property under 18 U.S.C. § 2314 includes proof of the transfer and transmission or transport across state lines or abroad; unauthorized access to information in a protected computer under 18 U.S.C. § 1030(e)(2)(B) requires that the computer was "used in or affecting interstate or foreign commerce or communication"; and some identity theft offenses under 18 U.S.C. § 1028(a), (c)(3)(A) mandate proof that "the production, transfer, possession, or use prohibited by this section is in or affects interstate or foreign commerce, including the transfer of a document by electronic means[.]" *See, e.g., United States v. Wittig*, 575 F.3d 1085, 1093 (10th Cir. 2009) (holding that one of the three elements the government must prove to establish wire fraud is "an interstate wire communication"); *United States v. Klopf*, 423 F.3d 1228, 1239 (11th Cir. 2005) ("[W]e now hold that the government must prove only a minimal nexus with interstate commerce in a § 1028(a) prosecution to satisfy the 'in or affects interstate or foreign commerce' requirement[.]"); *see generally United States v. MacEwan*, 445 F.3d 237, 245 (3d Cir. 2006) ("[T]he Internet is an instrumentality and channel of interstate commerce[.]"). In addressing this element of proof, log records may contain information that can be used to establish interstate or foreign commerce.

Advertisement revenue is a major part of the Internet. Log records may include information about advertisements on the Internet site that can be used to show interstate commerce. The log records may also confirm that the transmission was in interstate commerce.

Most major sites will subject visitors to numerous third-party ads that are hosted throughout the world on different servers. A single visit to cnn.com may generate well over 150 unique requests. Many of these requests are directed to third-party advertisement sites on different systems. Each access log at the different servers will correlate with the original request for cnn.com through the referrer field. This correlation identifies how the visitor arrived at the requested advertisement. For example, each entry would have a referrer of "www.cnn.com" from the same IP address that would have been observed in the access logs at the point the user visited www.cnn.com.

Analysis of log data will likely highlight other unknown datasets that can be brought into the investigation. For example, if the logs identify intellectual property being sent out to a public FTP server, one may move quickly to have the FTP server logs preserved at the remote system. This data would corroborate all data transfer from point A to point B. Moreover, one could use DNS records to establish a time line of activity to specific sites. These logs could lead to a request to preserve all Web access logs at certain sites within a specific time period key to an investigation.

VI. Conclusion

As these examples demonstrate, log records can provide useful and key evidence during the course of investigation or for trial. Few other types of records are comparable to log records' usefulness. As one of the unique benefits, log records are external to the computers that are used, and it is highly

unlikely that all of the log records in the path of communication can be successfully manipulated. Any claims of manipulation can be checked by referring to other log entries recording the same events or by correlating the log records with other evidence. Log records can also be used to fill in gaps in the evidence either where records have been deleted or where records are otherwise unavailable. In this way, log records may provide a full or at least more complete picture of the activity. Log records are useful to establish a time line of key events or, where possible, the click-by-click activity in an account. Log records can provide important identification information about the user of the computer behind the activity under investigation. Log entries may confirm whether one or more persons had access to an account during a particular period. Given the importance of log records and their limited retention, it is essential that they be identified and preserved early in the investigation.❖

ABOUT THE AUTHORS

❑**Mark L. Krotoski**, a federal prosecutor since 1995, has served as National Computer Hacking and Intellectual Property (CHIP) Program Coordinator at the Computer Crime and Intellectual Property Section in the Criminal Division for almost four years.✠

❑**Jason Passwaters** currently serves as the President of EdgePoint Forensics, LLC. He has been asked to assist with a number of federal cases involving network data and log analysis. His experience includes network data analysis for the Department of Defense during his service as a United States Marine and in support of other federal law enforcement cases.✠

The views expressed in the article are those of the authors and not of the agencies for which they have served.

Using Historical Cell Site Analysis Evidence in Criminal Trials

Thomas A. O'Malley
Assistant United States Attorney
Computer Hacking and Intellectual Property (CHIP) Coordinator
Identity Theft Coordinator
Western District of North Carolina

I. Introduction

In real estate, "location, location, location" describes the most important factors in determining the value of real property. In a criminal jury trial, establishing a defendant's location during the commission of the crimes charged in the indictment is equally important to the jury's determination of whether a defendant is guilty of those crimes.

Eyewitness testimony and physical evidence traditionally have been and continue to be the primary methods of proving a defendant's location at times and places relevant to the charged offenses. This type of testimony is referred to in this article as "defendant location evidence." Oftentimes, cases that go to trial involve little if any physical evidence, such as fingerprints or DNA, and eyewitness testimony is routinely challenged by the defense on grounds of reliability and credibility. Defense attorneys typically cross-examine victims and lay witnesses testifying about defendant location evidence based on their varying abilities to accurately perceive, record, and recall such evidence. Confidential informants and accomplice witnesses, on the other hand, are routinely attacked on their credibility. Law enforcement witnesses are often confronted with one or both of these defense tactics that are designed to raise jurors' doubts about defendant location evidence.

Today, traditional defendant location evidence may be supplemented with historical cell site analysis (CSA) evidence in cases where one or more cellular phones can be connected to defendants, co-conspirators, accomplices, victims, or witnesses at times and places relevant to the charged offenses. CSA evidence is considered "historical" in nature because the records used in the analysis are historical records of completed cell phone calls and transmitted text messages. Historical CSA evidence involves using historical call detail records (CDRs) to identify the location and pattern of movements over time of relevant cell phones 1) within mapped radio frequency (RF) areas, 2) relative to geographically-fixed cell towers, and 3) at fixed points in time. Narrowing the geographic location of cell phones to unique cell tower sectors at specific times is useful in establishing the proximity of identified cell phones relative to crime scenes and other relevant locations along with movement patterns of the cell phones.

Historical cell site analysis evidence can, for example, establish that a cell phone connected to an armed robbery defendant was used within specific cell tower sectors located in the general vicinity of banks victimized by a serial masked robber at or near the times of the robberies, along with pre-robbery movement of the cell phone towards the banks and post-robbery movement away from the banks and towards the defendant's residence or some other safe haven. Historical CSA evidence also can be used to corroborate the testimony of an accomplice getaway driver, bystander witness, or victim. The nature of the science and precision of the technology underlying historical CSA evidence is such that attacks on this type of evidence are usually limited to issues regarding the identities of persons using the cell phones

at the relevant times and the cell phones' location within recorded cell sites, some of which may be near or include known crime scenes or other relevant locations.

This article discusses the use of historical CSA evidence at trial with expert witnesses, such as the members of the Federal Bureau of Investigation's Cellular Analysis Survey Team (CAST), an experienced, specially-trained group of experts in this field. To fully understand why historical CSA evidence is reliable, accurate, and useful in criminal trials, this article begins with a review of the science, technology, and network architecture underlying wireless cellular communications ("cellular communications") (Part II) and the explosive growth and ubiquity of cell phones and cell usage in the 21st century (Part III). Next, this article will cover the pre-trial preparation necessary for presentation of historical CSA evidence at trial, including the use of qualified experts (Part IV), historical CSA evidence (Part V), and federal discovery and evidentiary rules applicable to historical CSA evidence (Part VI).

II. Science, technology, and network architecture for cellular communications

A. Discovery and research of the RF spectrum

The science of wireless communications is over 150 years old. Beginning in the mid-nineteenth century, Scottish physicist and mathematician James Clerk Maxwell theorized an electromagnetic spectrum containing invisible electromagnetic waves of energy (radiant energy) extending below known infrared light (where radio waves are found) and above known visible and ultraviolet light. Decades later, German physicist Heinrich Rudolph Hertz verified Maxwell's theory through experimentation when Hertz discharged a spark that traversed a gap between two unconnected points.

Scientific research of electromagnetic waves established that these waves are a repetitious series of waves with peaks and valleys. The entire wave pattern before its repetition is called a "cycle" and the number of cycles a wave repeats itself in one second is referred to as "frequency." Electromagnetic waves within the RF spectrum are measured in Hertz (Hz) units, named after Heinrich Hertz. A Hertz (Hz) unit is defined as the number of times an electromagnetic wave oscillates in one second. A kilohertz (kHz) is 1,000 cycles per second, a megahertz (MHz) is one million cycles per second and a giga-hertz (GHz) is one billion cycles per second. RF spectrum consists of all the electromagnetic waves operating at frequencies between 3 kHz (3,000 Hz) and 300 GHz (300 billion Hz) and has a finite capacity to transmit radio signals.

Maxwell's and Hertz' scientific works served as the foundation for Italian inventor Gugliemo Marconi's development of wireless telegraphy equipment that earned Marconi the 1909 Nobel Prize in Physics. Before the nineteenth century ended, Marconi had developed hardware that he used to wirelessly transmit one-way Morse code messages over a distance of several miles and, in 1901, across the Atlantic Ocean. Reginald Fessenden, a naturalized United States citizen from Canada, improved on Marconi's work when he wirelessly transmitted and received two-way transatlantic Morse code messages in January 1906. By the end of that year, Fessenden demonstrated the "[w]ireless transmission of speech over a distance somewhat greater than ten miles . . . [to] a number of persons invited to witness demonstration of a new system of wireless telephony." John Grant, *Experiments and Results in Wireless Telephony*, THE AM. TEL. JOURNAL 49-51 (Jan. 26, 1907).

Marconi was one of the first wireless inventors to successfully commercialize his work. On a fateful night in April 1912, Marconi's equipment and his radio operators transmitted and received Morse code distress messages between transatlantic passenger ships, resulting in the *Carpathia*'s rescue of 705 *Titanic* passengers from the frigid Atlantic Ocean. The scientific and technical achievements of Maxwell, Hertz, Marconi, and Fessenden ushered in an era of wireless communications, including radio transmissions, commercial radio and television broadcasts, satellite transmissions, mobile

communications, and hand-held telephone communications. Today the invisible "airwaves" of the electromagnetic spectrum wirelessly carry an increasing volume of voices, text, photographs, music, movies, and other data transmitted and received through the air between separate hardware devices located throughout the world.

B. Management of RF spectrum use

The RF spectrum range (3 kHz to 300 GHz) lacks the capacity to handle unlimited, interference-free wireless communications. Radio waves can be set to different frequencies by adjusting the oscillation, thus enabling partitioning to accommodate more users and multiple wireless communications on different frequencies. More efficient use of the RF spectrum's capacity has also been achieved through new technological advances. However, RF spectrum remains a finite natural resource that must be managed to meet growing demand for interference-free wireless communications for consumers, businesses, national defense, public safety, transportation, and entertainment and news broadcasts.

In the United States, two separate federal government agencies regulate, allocate, and manage RF spectrum based on the identity of the RF spectrum user. RF use by federal agencies is handled by the National Telecommunications and Information Administration, an agency in the United States Department of Commerce. The Federal Communications Commission (FCC), an independent agency of the United States government, is responsible for regulating, allocating, and managing RF spectrum use by non-federal government agencies and private parties, including commercial cellular communications providers (cell providers).

Cell providers cannot operate in the United States without being licensed by the FCC. In this highly-regulated industry, cell providers offering mobile telecommunications service to the general public must acquire rights to use certain frequencies in specific geographic regions throughout the country. Beginning in 1993, the FCC's use of auctions to award licenses for the rights to use RF spectrum "spurred the marketing of new technologies and the building of transmission capacity to meet growing demand." Thomas Duesterberg & Peter Pitsch, *Wireless Services, Spectrum Auctions and Competition in Modern Telecommunications*, OUTLOOK 7 (1997).

C. Architecture and components of cellular mobile phone networks for communications using RF spectrum

Architecture of cellular mobile phone networks: Marconi's successful commercialization of wireless communications in the early 20th century precipitated the profitable business of wireless communications that has evolved into today's multibillion-dollar cellular mobile phone industry. From its inception, all two-way wireless communication systems have required a network of antennas to transmit and receive radio signals to and from fixed or portable communication devices. In 1947, Bell Lab engineers proposed a cellular architecture consisting of a network of directional antennas positioned at three corners of hexagonal cells to transmit and receive radio signals in three directions to three adjacent cells for use in vehicle-based mobile phone communications. This cellular network was not developed when it was first envisioned because of a lack of technology and frequency allocation by the FCC.

In the decades that followed, new technologies, government-allocated RF spectrum, and the prospect of financial profits spurred development of today's cellular mobile phone network (cellular network). The cellular network built in the United States consists of a honeycomb grid of hexagonal cells covering the land area for wireless communication services, with directional antennas positioned at three cell corners to transmit and receive wireless communications with wireless devices located in range of RF transmissions from any of the fixed directional antennas. *See infra* Figure 1. The cellular network design utilizes RF spectrum more efficiently by reusing frequencies (frequency reuse) in other non-adjacent cells

without co-channel interference. It also enables "handover" of wireless telephone communications to/from antennas servicing adjacent cells so that wireless mobile phone users can talk without interruption as they travel throughout the cellular network.

Basic components of cellular mobile phone networks: A cellular network is composed of four basic components: 1) Base Transceiver Stations (BTS), known as "cell towers" and "cell sites"; 2) mobile stations (MS), known as "cell phones" and "mobile phones"; 3) Mobile Switching Center (MSC); and, for connection to wired telephones, 4) Public Switched Telephone Network (PSTN).

Base Transceiver Stations constitute the first component. Cellular networks typically use directional antennas that radiate greater power in one or more directions for increased performance to transmit and receive signals while reducing interference from unwanted sources. Directional antennas in cellular networks are usually mounted and positioned on the cell towers to radiate in separate sectors facing different directions. A "cell sector" refers to a specific sector emanating from a cell tower.

The number of sectors around a cell tower may vary by cellular provider or region serviced. The most prevalent configuration, however, is three separate 120-degree, pie-shaped arcs connected to form a circle of 360-degree coverage around the cell tower. *See infra* Figures 2 and 3. Additional equipment on cell towers and in enclosures at tower bases further enables wireless communications with cell telephones and relay of communications back to the telecommunication network—known as "backhaul"—that connects with other wireless and wire-based networks. Cell tower location and properly working equipment are essential to the operational performance of the cellular networks.

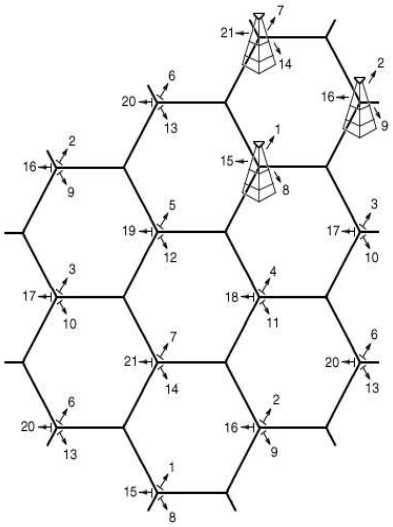


Figure 1. Hexagonal cellular network with three-sector directional antennas.

The second component is the mobile station. The mobile station in a cellular network is more commonly known as a "cell phone" or "mobile phone." In essence, it is a wireless telephone that transmits to and receives from cell towers audio, text, and data. In order to communicate with a cellular provider's cell towers, a cell phone must be programmed with one of several channel-access technologies that match the channel-access technology used by a cellular provider in its network. The most widely used channel-access technologies that are implemented by providers in the United States are Code Division Multiple Access (CDMA) and Global System for Mobile communications (GSM). Other channel-access technologies in the United States include Universal Mobile Telecommunications System (UMTS) and Integrated Digital Enhanced Network (iDEN). The type of channel-access technology that a cell phone uses to connect to a provider's cellular network is irrelevant to conducting an historical cell site analysis, because call detail records (CDRs), discussed below, are generated for telephone calls and text messages relayed between cell towers and cell phones using any channel-access technology.

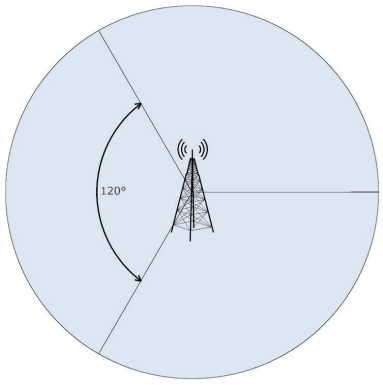


Figure 2. Cell tower with three 120° sectors.

Delivery of private telephone calls and text messages requires the cellular network to deliver these private communications to a single, uniquely identifiable cell phone associated with a cellular subscriber who is billed for the cell

phone usage. Cell phones must also be uniquely identifiable to prevent cell phone usage fraud known as "cloning." Cell phone cloning involves the duplication of phone identifiers for the purpose stealing call minutes or text/data usage that is fraudulently billed to a legitimate cell phone subscriber. Since the late 1990s, cell phone manufacturers and providers have deployed authentication systems that have nearly eliminated cell phone cloning fraud.

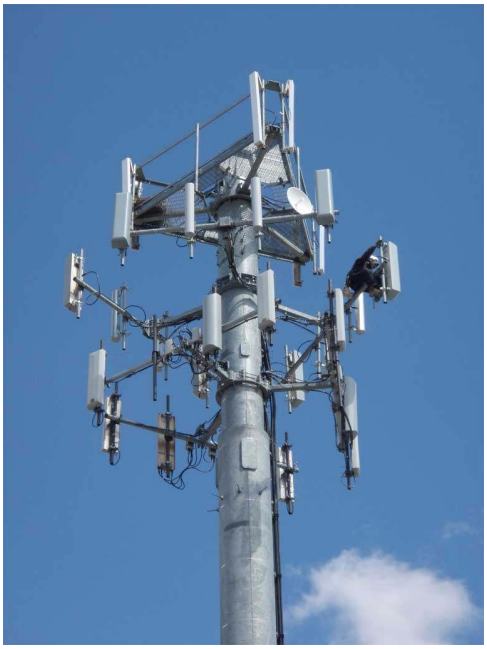


Figure 3. Cell tower with directional antennas facing three separate sectors.

Cell phones in a cellular network are identified by unique ten-digit telephone numbers assigned under the North American Numbering Plan (NANP), the same format used to assign numbers to traditional wired telephones located at residential and business addresses. Developed by AT&T in 1947 to simplify and facilitate direct dialing of long-distance telephone calls, NANP telephone numbers are ten-digit numbers consisting of a three-digit Numbering Plan Area (NPA) code, commonly called an area code, followed by a seven-digit local telephone number unique to each area code. Cell phones are further identified in a cellular network by one or more other identifiers. The most common cell phone identifiers include: an electronic serial number (ESN), a unique identification number embedded on a cell phone microchip by the cell phone manufacturer for use in a CDMA network; a mobile equipment identifier, a globally unique number "burned" into newer cell phones used in CDMA network after available ESN numbers were exhausted in 2008; an International Mobile Equipment Identifier (IMEI), a globally unique number "burned" into cell phones used in a GSM or iDEN network; an International Mobile Subscriber Identity (IMSI), a unique number burned into a removable security identity module (SIM) card that identifies a cell phone subscriber used in GSM and UMTS networks; a Mobile Subscriber Integrated Services Digital Network Number (MSISDN), a number uniquely identifying a subscription in a GSM or UMTS network that is the telephone number of a SIM card; and a Mobile Identification Number (MIN), a unique provider-assigned number for each cell phone in the cellular provider's network.

The third component of a cellular network is the Mobile Switching Center. The MSC is the brains of the cellular network. It routes voice calls, text/SMS (short message service) messages, and data between wire-based telephones and between cell phones, whether on the provider's cellular network of another provider's cellular network. The MSC also routes connections to the Internet for the growing "smart phone" market. Among other tasks, the MSC handles end-to-end connections and mobile handover for uninterrupted calls as cell phone users travel through the cellular network. The MSC also interacts with various servers that contain databases to authenticate cell phones and to ensure that cell phones attempting to use the provider's cellular network are authorized to do so and are associated with a paying subscriber's account.

A Base Station Subsystem (BSS) handles cell phone traffic and signaling between cell phones, cell towers, and the MSC. The BSS is composed of Base Transceiver Stations (BTS), discussed above, equipped to transmit and receive radio signals and to encrypt and decrypt communications. The BSS is also composed of Base Station Controllers (BSC) that allocate radio channels and control RF power levels in BTSs and manage "handover" of calls between cell towers as cell phone users travel throughout the cellular network.

The fourth component is the Public Switched Telephone Network. The PSTN is the global network of public circuit-switched telephone networks through which calls are routed with switching equipment for wired telephone service on a local, regional, national, and international level. Telephone calls on the PSTN are routed to and received from consumers served by wired telephones, commonly known as landline phones. Together, the PSTN and MSC enable mobile phone users and wired telephone users to communicate with each other. *See infra* Figure 4.

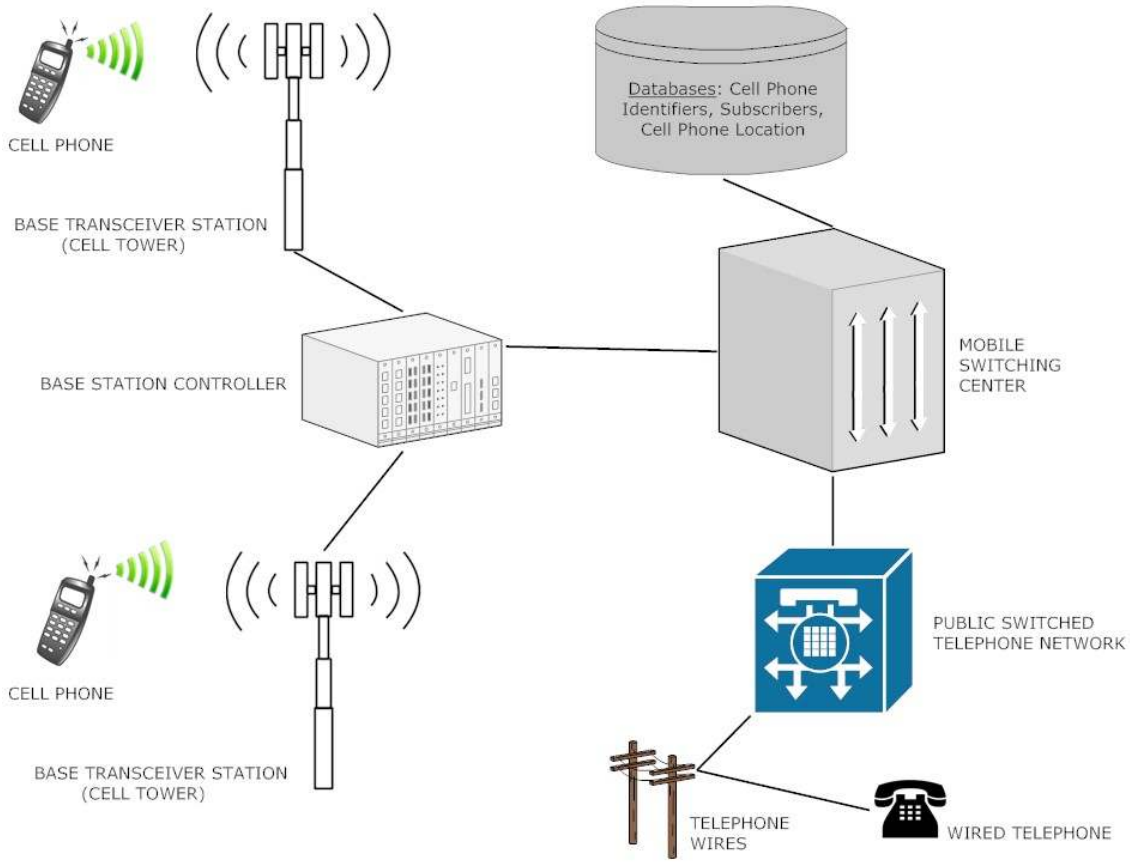


Figure 4. Main component of cellular mobile phone network and connection between MSC and PSTN

III. The cellular mobile phone industry in the United States

A. Evolution of cell phones and cell phone usage

Motorola researcher and executive Martin Cooper, while walking in Manhattan with a 2.2 pound mobile phone in his hand, called his rival at Bell Labs on April 3, 1973 to inform him that Motorola had just won the race to build the world's first hand-held mobile cell phone. Motorola spent another ten years and $100 million before its hand-held cell phone reached the market for commercial use. The DynaTAC cell phone that Motorola sold to consumers in 1983 weighed one pound, measured 9.5 inches tall, took ten hours to recharge, provided less than sixty minutes of talk time, and retailed for $3,995 ($9,054 in 2011 dollars).

In addition to the phone cost, mobile phone service plans in 1984 were $22 per month, plus 22 to 38 cents per minute depending on the time of day, plus $25 per month for long-distance access and an

additional 27 to 45 cents per long-distance minute. Motorola's "Brick," as it was known, was a status symbol of the rich who could afford the phone and the hefty costs of monthly phone service.

Today numerous cell phone providers compete to offer consumers free palm-sized cell phones with quick-recharge batteries that provide at least six hours of talk time and days of stand-by time in exchange for a two-year service contract. A typical service plan accompanying a free cell phone now costs less than $80 per month for 900 weekday call minutes, unlimited nighttime and weekend call minutes, free nationwide long-distance minutes, and unlimited text messages. The dramatic evolution of cell phone equipment and, more importantly, drastic price reductions for cell phones and cell phone service plans, have driven explosive growth in cell phone ownership, usage, and coverage throughout the United States and the world.

The spectacular growth of cell phones and cell phone usage has made cell phones ubiquitous; and ubiquity is what makes historical cell site analysis such an important investigative tool that may yield valuable evidence in a criminal case. According to statistics published by the CTIA–The Wireless Association, the number of cell phone subscribers in the United States has increased from 28.1 million in 1995 to 327.6 million in June 2011, 103.9 percent of the nation's population. Significantly, an increasing percentage of households, 29.7 percent in June 2011, are considered "wireless only" with at least one cell phone and no wired telephone in the household. Cell phone usage has increased from 31.5 billion call minutes in 1995 to 2.2 trillion call minutes in June 2011, or an average of 6 billion call minutes per day. Text messages exchanged between cell phone users has increased from 57.2 billion in 2005 to 2.1 trillion in June 2011, or an average of 5.7 billion text messages per day. As of June 2011, cell providers have installed over 250,000 cell towers to handle increased cell phone usage and consumer demand for wider and better wireless coverage.

B. Types of companies providing cell phone services

Two types of entities provide cell phone services in the United States: mobile network operators (MNO) and mobile virtual network operators (MVNO). MNOs own RF spectrum licenses obtained from the FCC for specific frequencies within specific areas throughout the United States. MNOs also build and own their infrastructure to provide cell phone services on their licensed frequencies. The United States currently has four nation-wide MNO's and over 100 regional and local MNO and MVNOs.

Unlike MNOs, MVNOs providing cell phone services do not own RF spectrum licenses. While many MVNOs do not have their own infrastructure to support their cell phone services, some do. MVNOs operate on licensed frequencies through business agreements with MNOs owning licenses by purchasing minutes of use (MOU) from MNOs and reselling MOUs to the MVNO's customers. An MNO that does not have spectrum licenses in certain regions of the country may operate in those regions as an MVNO.

C. Recordkeeping for business and maintenance

American consumers paid $160 billion in 2010 for wireless phone services. Cell providers earn their share of this multibillion-dollar revenue stream from consumer use of voice-call airtime minutes, text messaging, and, more recently, data transmissions from the Internet. To remain competitive, cell providers must insure that consumers are billed and pay for wireless services that the cell providers deliver to their customers. In order to retain their paying customers, cell providers must deliver wide, high-quality, reliable wireless coverage to their customers or risk losing them to competitors.

Cell providers collect and use mobile phone location information for various service and operational purposes. These include ensuring that customers have a wireless signal to complete a call, transferring a wireless call across a highly diverse and complex network as mobile users move in and out of geographic areas covered by radio antennas throughout the cellular network, maximizing network

capacity and efficiency to reduce operational costs, reducing the number of "dropped" calls, and providing their customers with high-quality wireless services. The business requirements to earn and collect revenue from wireless services and the need to retain customers through broad, reliable, quality wireless coverage necessitates collection and storage of real-time, accurate, detailed wireless usage data. Cell providers collect, record, and temporarily store this necessary billing data to obtain their share of consumer revenue that also may be shared with other business entities involved in providing wireless services, such as another cellular provider or an SMS messaging service. To ensure wide, continuous, reliable wireless coverage, cell providers monitor wireless systems operations 24/7 and field-test their engineered wireless coverage, adding new cell towers when and where they may be required. For these reasons, cell providers generate call detail records with cell tower/sector (cell site) information for every cell phone call and text transmissions throughout the cellular network.

IV. Pre-trial preparation for presentation of historical CSA evidence at trial

Advanced planning is required to use historical cell site analysis evidence in a criminal trial. Call detail records with cell tower location information for relevant cell phones should be preserved as soon as possible and acquired from MNO or MVNO cell providers that service the relevant cell phones. Cell tower location data/maps maintained by these respective cell providers to operate their own cellular networks must also be acquired to plot relevant cell tower locations on a map generated with widely-available mapping software. Finally, it will be useful to recruit a qualified witness to conduct an historical cell site analysis, prepare a report of the historical cell site analysis for discovery purposes, and comply with the requirements of Federal Rule of Evidence 702 and legal precedent for presentation of trial testimony based on scientific, technical, or other specialized knowledge.

A. Records required for historical cell site analysis

Call detail records: Historical cell site analysis begins with collection of CDRs for cell phones identified as relevant to a criminal investigation or trial. CDRs may be obtained from cell providers only pursuant to compulsory legal process. CDRs contain the necessary data to conduct an historical cell site analysis, including dates, times, and cell tower/sector locations (cell sites) for cell phone calls and text messages. *See infra* Part V.A.

Preservation of CDRs by cell providers should be requested as soon as possible. Cell providers retain CDRs containing cell site information for short time periods, ranging from six to eighteen months, depending on the cell provider and its business needs for cell site call and text data. CDRs with cell site information may be preserved pending issuance of legal process to compel production of CDRs for a period of 90 days pursuant to a preservation request made to a cell provider, which preservation may be extended for an additional 90-day period upon a renewal request. *See* 18 U.S.C. § 2703(f)(1) and(2) (2010).

Under the Electronic Communications and Privacy Act (ECPA), 18 U.S.C. §§ 2510–2522, cell providers must be served with either a court order issued pursuant to 18 U.S.C. §2703(d) or a § 2703(c) search warrant to compel production of CDRs containing cell site information. *See* 18 U.S.C. § 2703(c)(1)(A), (B) (2010). In the case of a cooperating witness or victim subscriber, CDRs may be obtained with the subscriber's consent. *See id.* § 2703(c)(1). For on-going criminal investigations, a § 2703(c) search warrant or a combined § 2703(d) court order and pen register order, 18 U.S.C. § 3121–1327, known as a "hybrid" order, may be used to collect prospective CDRs containing cell site information. For more information on collecting CDRs with cell site information, see CCIPS Online, available to federal prosecutors on the Department of Justice, Computer Crime and Intellectual Property Section (CCIPS) Intranet Web site.

Cell tower data and maps: Cell providers engineer and build their cellular network infrastructure of cell towers to provide wide, reliable, and efficient wireless service to their customers. In order to insure optimal cellular network operation, cell providers maintain records regarding cell tower/sector location to enable them to identify, locate, and repair any malfunctioning cell towers, perform ongoing cell tower maintenance, and install additional nearby cell towers to fill any wireless coverage gaps.

Cell tower data/map records contain the geographical locations of the cell towers in the cell provider's cellular network, recorded by longitude and latitude, and cell tower/sector information, including the number of cell sectors for each cell tower and the directional orientation of cell tower sectors for all cell towers in the cell provider's cellular network. No ECPA-required process is available for acquiring these records because these records relate to the cellular network and not to individual subscribers. Depending on the cell provider, these records may be obtained through an informal request, administrative subpoena issued by an appropriate law enforcement agency, or trial subpoena. However, consideration should be given to acquiring such records so that they are admissible in evidence. *See* FED. R. EVID. 803(6) and 902(11).

B. Qualified trial witness under Federal Rule of Evidence 702

Historical cell site analysis evidence may be presented through a witness who is qualified "as an expert by knowledge, skill, experience, training, or education" if the witness' testimony will be offered in the form of an opinion or otherwise and such testimony is based on sufficient facts or data and is the product of reliable principles and methods that the witness has reliably applied to the facts of the case. *See* FED. R. EVID. 702. In addition to Rule 702 expert testimony on historical cell site analysis, non-expert summary testimony involving historical cell site analysis may be offered where such testimony is limited to presentation of summary maps, charts, or other demonstrative summary exhibits based on evidence admitted at trial without offering any expert opinions.

FBI'S Cellular Analysis Survey Team (CAST) experts: CAST is a highly-qualified group of federal law enforcement agents who are experts in the field of historical cell site analysis. The Federal Bureau of Investigation (FBI) created CAST when it discovered that historical cell site analysis was a valuable investigative tool that could help identify criminal suspects and the general location of both suspects and crime victims at fixed points in time. Successful results achieved by CAST have included identification and arrests of violent felons, including murder suspects, and the rescue of kidnapping and child abduction victims. Recognizing its success in using historical cell site analysis to help solve crimes, the FBI has extended CAST's historical cell site analysis expertise to the courtroom for significant criminal cases.

CAST presently consists of nineteen FBI Special Agents stationed around the country who have received extensive specialized training in historical cell site analysis. The specialized training for CAST experts includes an intense four-week training course on various case scenarios, cellular technology, software mapping tools, and the use of industry-standard RF signal detection equipment and software (JDSU platform) to measure and map the actual RF coverage footprint within a particular cell tower sector. CAST experts also are certified to provide specialized training to federal and state law enforcement agents on the subject of historical cell site analysis in criminal investigations.

Recent demand for CAST experts has far exceeded the current resources of the CAST unit. For this reason, CAST must prioritize requests for trial assistance by giving precedence to cases involving murder, kidnapping, and other significant FBI investigations, especially those involving violent crimes. Once these priority cases have been addressed, remaining CAST resources are then made available to assist with major cases of other federal and state law enforcement agencies. The limited availability of

CAST experts often will require that prosecutors locate other qualified experts to provide trial testimony on historical cell site analysis evidence.

Specially-trained law enforcement experts: A law enforcement agent who has received specialized training in historical cell site analysis provided by CAST or by any other qualified training program should be able to qualify as a Rule 702 expert to testify on the subject of historical cell site analysis. The advantage of using specially-trained law enforcement agents rather than a cell provider witness is that law enforcement witnesses can combine their training and street experience in both historical cell site analysis and law enforcement investigations, including any crime-specific training and experience relevant to the case, such as violent crime. Law enforcement expert witnesses often are also more readily available for investigative consultation and trial preparation, including preparation of demonstrative exhibits for graphic presentation of historical CSA evidence to a jury.

Cell provider employee experts: In addition to CAST experts and specially-trained law enforcement witnesses, a cell provider employee who is knowledgeable about the cell provider's cellular network, CDRs, and the basic science or technology underlying historical cell site analysis should be eligible to qualify as a Rule 702 expert, subject to their degree of training and experience in this field. Certainly, an engineer or cellular network technician familiar with the cell provider's network and CDRs should qualify as a Rule 702 expert. Cell provider records custodians, however, may lack the requisite training and experience to testify as Rule 702 experts. Some cell provider records custodians may have sufficient training and experience to testify about cell tower locations and cell tower sectors, particularly where such information is recorded in the CDRs or other business records that the records custodian produces at trial. Unlike law enforcement experts, cell provider experts may not be willing to devote any of their time or resources to prepare demonstrative trial exhibits.

Non-expert summary witness: A lack of available resources and time constraints for impending trials may preclude the use of a Rule 702 expert witness to present detailed historical cell site analysis evidence at trial. In such cases, an argument can be made that summary testimony limited to charts or maps based on evidence admitted during trial should be admissible through non-expert testimony. For example, a trial court may permit a witness not offering Rule 702 opinion testimony to testify about maps plotted with locations of a cell provider's cell towers based on business records, crime scene specifics, and CDR information admitted into evidence. *See, e.g.*, *United States v. Sanchez*, 586 F.3d 918, 929 (11th Cir. 2009) (CDR summary portrayed on accurate maps were properly admitted through testimony of detective who reviewed CDRs and did not violate Sixth Amendment Confrontation Clause where such summary evidence was not offered through cell provider's records custodian), *cert. denied*, 130 S.Ct. 1926 (2010).

Limited, non-expert summary testimony regarding cell tower locations and cell phone transmissions recorded in the CDRs should be admissible because the ubiquity of cell phones today means that most, if not all, jurors, judges, and attorneys have cell phones, have observed cell phone towers, know that the quality of their cell phone call reception depends, at least in part, on their proximity to cell towers, and that their cell phones work practically everywhere that they travel in the United States. Additionally, plotting tower locations in relation to crime scenes on accurate, readily-available computer mapping software can be accomplished easily through the input of the longitude and latitude of cell towers identified in a cell provider's business records. This input results in a graphic summary of the geographical location of cell towers on a map that can be easily verified, along with any other CDR data admitted into evidence.

Consideration should be give to restricting testimony by a non-expert summary witness to mapped crime scenes and cell tower locations, along with corresponding CDR information admitted into evidence—such as dates, times, connecting telephone numbers, and incoming/outgoing communications. Any additional testimony further explaining details about cellular communications, such as cell sectors, the

number and direction of cell tower sectors for each cell tower, and depictions of the directional orientation and reach of cell tower sectors on a map, arguably may require that the testifying witness be qualified as a Rule 702 expert. Such testimony could be considered the type of information that triggers Rule 702 requirements because it is often learned only through specialized knowledge, skill, experience, training, or education. In many cases, unless a cell provider's records custodian or technician testifies at trial about the number, orientation, and reach of the cell provider's cell tower sectors for specific towers, it will be appropriate to comply with Rule 702 and its concomitant discovery requirement if any testimony will be offered to explain cell tower sectors around a cell tower.

V. Historical cell site analysis evidence

Historical cell site analysis evidence involves identifying the location of relevant cell phones (1) within mapped RF areas, (2) relative to geographically-fixed cell towers, and (3) at fixed points in time. This analysis begins with reviewing CDRs, cell tower locations, and cell sector orientation to identify relevant voice call or SMS (text) message connections in relation to crime scenes or any other relevant locations, along with relevant patterns of movement in connection with these locations. Relevant voice call or text connections are then overlaid on mapping software depicting relevant cell towers and sectors along with locations relevant to the case.

A. Call detail records

Historical call detail records are a cell provider's business records of a particular cell phone's location and communication activity over time within the cell provider's network. CDRs contain accurate date, time, and location information for cell phones and, unlike a witness' memory, are not prone to impeachment based on their accuracy, reliability, or bias. Additional information available in CDRs includes the telephone number of the wireless or wire-based phone connecting with the relevant cell phone, whether the voice calls or text messages were incoming or outgoing, the duration of voice calls, and the cell tower and cell tower sectors at the beginning and end of voice calls or when text messages are sent or received. Cell tower and cell sector information may be coded in CDRs, that is, the CDRs may contain numbers or letters that are not recognizable geographic coordinates. Where cell site data is coded in the CDRs, care should be exercised to ensure that the records custodian witness is knowledgeable about converting the coded cell site data to geographic coordinates of the cell towers recorded in the CDRs, or that the records custodian produces at trial the cell provider's records to enable a non-expert summary witness to identify geographic location of the cell towers identified in the CDRs. CAST experts and most other qualified expert witnesses have the requisite training and experience to decode the CDR cell tower codes of various cell providers into geographical locations for relevant cell towers. As experts, they may rely on their knowledge gained from working with cell providers to convert the coded CDR cell site data to geographic locations without the need to enter the cell provider's decoding records into evidence. *See* FED. R. EVID. 703.

Cell tower and cell sector information for a particular cell phone is recorded in CDRs at the time (1) a voice call is initially connected, (2) a voice call is terminated, (3) a connection is made with the voice mail message service to leave or retrieve a voice message, (4) a text message is sent, and (5) a text message is delivered, which may be different than the time that the cell phone user reads the text message. CDRs do not record "handover" cell towers/cell sectors through which a cell phone travels during a voice call unless a particular cell tower/sector is the originating or terminating point of a voice call.

A cell phone that is switched on and operational will register with a nearby cell tower so that the cellular network knows its location to enable immediate access to the cellular network to send or receive voice calls or text messages. Typically, the strongest signal received by a cell phone is the closest tower or

one that is in direct line of sight of a cell phone. The cell tower with the strongest signal to a cell phone is known as the "servicing" tower that sends and receives voice calls and text messages to the cell phone. A cell phone also monitors and measures signals from nearby cell towers. As a cell phone moves through the cellular network, the cell provider's Base Station Controllers and MSC monitor, control, and manage "handover" of the cell phone to other servicing cell towers/sectors to enable uninterrupted voice calls on the cell phone. Cell tower/sector information for the constantly-monitored location of a cell phone during "handover" activity is not recorded in CDRs. Only the cell tower/sector information for the call or message activity listed above is recorded in CDRs.

B. Cell tower locations and sector orientation

Cell providers maintain business and operational records containing the geographical location and cell sector orientation for all cell towers in their cellular network. The number of sectors for cell towers, cell sector identifiers, and cell sector orientation vary by cell providers. Cell tower records contain the longitude and latitude of each cell tower in the cell provider's cellular network, along with the number, direction, and orientation of the sectors around a cell tower. For example, cell tower/sector records may reflect that three sectors are associated with a provider's cell towers, identified by numbers (for example, 1, 2 and 3) or other identifiers (for example, alpha, beta, and gamma). The records for such towers will reflect the angle of coverage, typically 120° for each sector of a three-sector tower. Finally, the records will reflect sector orientation for the cell provider's three-sector towers, which may be oriented north at 0° for sector 1, southeast at 120° for sector 2, and southwest at 240° for sector 3.

The radius of RF signals around a cell tower can vary considerably, but many towers have a radius of several hundred meters to several miles. For example, a cell tower located in an urban environment typically covers a smaller RF area than a cell tower located in a rural setting. The RF coverage difference between urban and rural cell towers is attributable in part to fewer buildings in rural areas that can affect RF coverage, lower cell phone user density in rural areas, different levels of broadcast wattage (power) of a cell tower, and proximity of a cell tower to neighboring cell towers. Thus, a cell tower located in a high-density urban setting often will have a shorter coverage range while a cell tower located in a low-density rural setting will have a longer coverage range.

C. RF mapping

Radio frequency mapping is used in historical cell site analysis to graphically depict relevant cell towers and cells sectors based on CDR information. RF mapping is prepared with commonly-available software mapping tools, such as Google Earth or MS MapPoint, that allow for exact plotting of cell towers and sectors by longitudinal, latitudinal, and directional orientation of sectors.

Cell sectors are typically drawn to reflect seamless cellular coverage that cell providers furnish to their users within their cellular network, including some overlapped coverage with nearby cell tower sectors. Mapping the directional orientation and angle of coverage of cell tower sectors is based on the cell provider's business records and mapping of the range of cell tower sectors is based on the cell provider's planned and engineered RF coverage and basic principles of wireless communication. *See infra* Figure 5. Actual RF coverage may be available from some cell providers who measure actual RF coverage within certain cell sectors and maintain business records of actual RF coverage measured for those cell sectors. Otherwise, industry-standard equipment and software must be used by trained individuals to measure and record the actual RF coverage footprint within a particular cell sector.

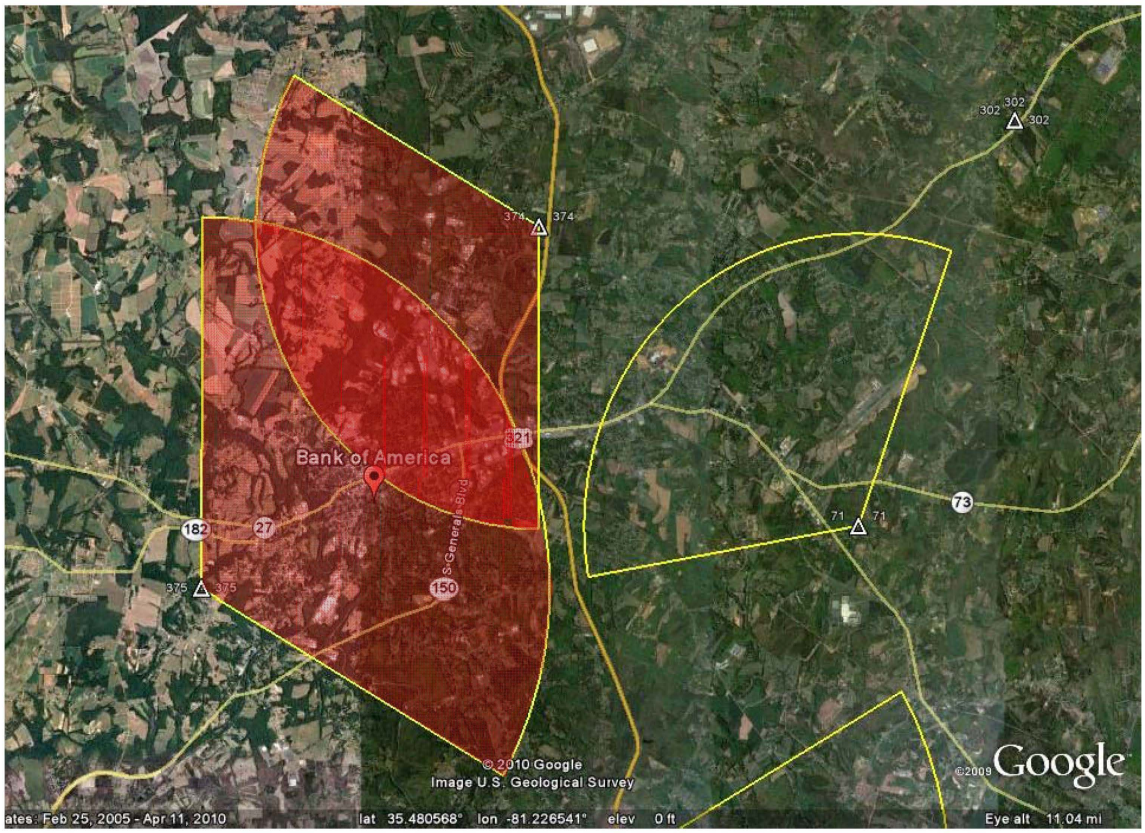


Figure 5. Mapped RF coverage of cell tower sectors and bank robbery location

D. JDSU drive test

As part of their extensive training, CAST experts have ready access to and have been certified to use industry-standard RF mapping equipment and software to map the actual RF coverage footprint within a particular cell sector. The equipment and software, known as the JDSU Drive Test Wireless Optimization Platform, is used by CAST experts and is the same RF measuring platform used by cell providers to map the actual RF coverage within particular cell tower sectors. Cell providers use RF coverage measurements to adjust directional antennas on their cell towers and to add new cell towers for improved wireless coverage in their cellular network.

A JDSU drive test of a particular cell sector, which can take several hours, usually is unnecessary for the vast majority of cell sectors identified in the CDRs. In most cases, location of a cell phone within various cell tower sectors at specific times on specific dates is sufficient to demonstrate a cell phone's proximity to relevant locations identified in the case and patterns of movement. In some cases, such as one where a witness observed a suspected bank robber talking on a cell phone in a bank parking lot moments before the robbery, it may be beneficial to narrow and confirm the location of the defendant's cell phone within the actual mapped RF coverage area of the cell sector that includes the bank, rather than locating the cell phone simply within the larger engineered area of the cell sector. *See infra* Figure 6. JDSU drive-test data is voluminous and easily summarized in a mapped footprint of the RF signal within a cell sector,

subject to the requirements of Federal Rules of Evidence 703 (facts and data of type reasonably relied on by experts in the field need not be admissible in evidence), 705 (expert opinion and inferences admissible without first testifying to underlying facts or data and disclosure may be required on cross-examination), and 1006 (voluminous writings, recordings not subject to convenient examination in court may be submitted in summary form; originals or duplicates of such voluminous evidence must be made available for examination or copying by other party, and produced in court if so ordered).

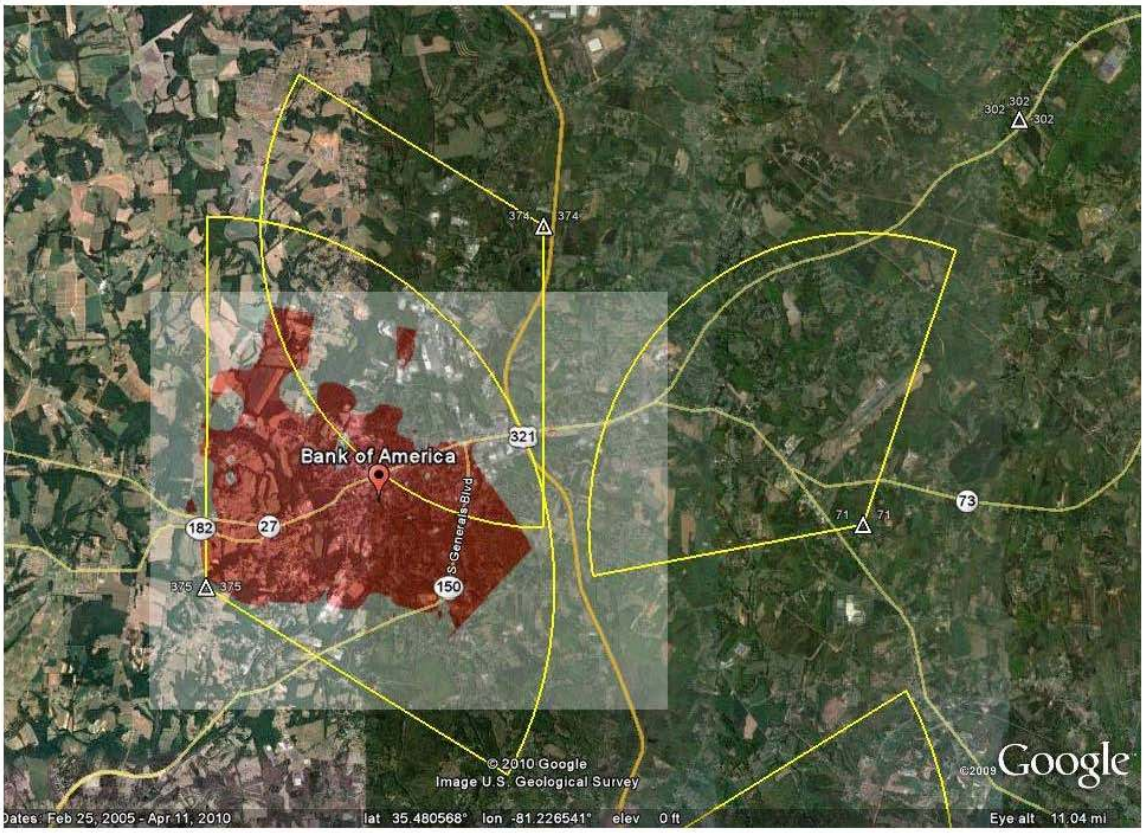


Figure 6. Mapped actual RF coverage of cell tower sectors and bank robbery location based on JDSU drive test

VI. Discovery and evidentiary rules applicable to historical cell site analysis evidence

Historical cell site analysis evidence is based on "scientific, technical, or other specialized knowledge . . . ." *See* FED. R. EVID. 702. This distinction regarding the nature of such evidence and other types of evidence implicates specific discovery and evidentiary rules. Compliance with these discovery and evidentiary rules is essential to error-free admission of historical cell site analysis evidence at trial. Failure to comply with these rules can result in the exclusion of such evidence at trial or, if admitted, reversible error on appeal. *See, e.g.*, *Wilder v. Maryland*, 191 Md. App. 319, 368-69 (Md. Ct. Spec. App. 2010) (conviction reversed where detective's testimony regarding historical cell site analysis was offered

as lay opinion testimony rather than expert testimony based on detective's specialized training and experience and prosecution failed to comply with concomitant discovery requirement for expert witnesses).

A. Discovery requirements

Rule 16(a)(1)(G) of the Federal Rules of Criminal Procedure requires that the government provide to the defense, at the defendant's request, "a written summary of any testimony that the government intends to use under [Fed. R. Evid.] 702 [testimony by expert], 703 [bases of expert's opinion testimony] or 705 [disclosure of facts or data underlying expert opinion] . . . during its case-in-chief at trial." FED. R. CRIM. P. 16(a)(1)(G). The written summary required by this rule "must describe the witness's opinions, the bases and reasons for those opinions, and the witnesses qualifications." *Id.*

CAST experts are familiar with this discovery requirement and routinely prepare reports that comply with Rule 16(a)(1)(G), along with resumes of their extensive qualifications. A CAST expert report typically includes the following:

- The methodology used in conducting the historical cell site analysis
- The mapping of cell tower locations based on cell provider records
- The orientation of cell sectors for the cell provider's cell towers
- The methodology and assumptions in drawing cell sector coverage
- The methodology and equipment (JDSU drive test) used to measure and map actual RF signal coverage within certain cell sectors, if applicable
- The conclusions regarding cell phone location in cell sites and call activity patterns as reflected in CDRs for individual calls or text messaging.

Other qualified experts who may be called to testify about historical cell site analysis evidence should be directed to prepare a similar report regarding their anticipated testimony. Any expert reports must be provided in discovery pursuant to Rule 16(a)(1)(F) prior to trial pursuant to the rules and local practice of the trial court. Additional summary expert reports prepared under Rule 16(a)(1)(G) based on a defense request for a written summary of expert testimony also must be delivered to the defense prior to trial pursuant to the rules and local practice of the trial court. Failure to comply with these discovery requirement for written expert witness reports and expert summaries within time frames established by the trial court may result in the exclusion of the expert witness at trial.

Rule 16 imposes other discovery obligations for historical cell site analysis evidence in addition to written expert summaries. Rule 16(a)(1)(E) requires that the defense, upon request, be permitted to inspect and copy certain physical and tangible objects that the government intends to use in its case-in-chief at trial. Thus, CDRs, cell tower data/maps, and any other records acquired from the cell provider in advance of trial must be made available to the defense within the time frame established by the trial court. *See* FED. R. CRIM. P. 16(a)(1)(E); FED. R. EVID. 1006.

Once it is determined that a case will proceed to trial, the historical cell site analysis expert may prepare demonstrative or summary exhibits to graphically illustrate the historical CSA evidence to the jury. Once prepared, any such demonstrative or summary exhibits relating to historical cell site analysis evidence must also be made available to the defense in advance of the trial within the time frame established by the trial court. FED. R. CRIM. P. 16(a)(1)(E); FED. R. EVID. 1006. Such exhibits may include interactive PowerPoint presentations, mapped depictions of CDR activity, or movie clips depicting time-sequenced CDR activity. CAST experts are extremely adept at preparing such powerful demonstrative

exhibits to visually depict their testimony to jurors and can prepare such exhibits in advance of trial, subject to their workload and timing of the prosecutor's pre-trial request for demonstrative exhibits.

B. Evidentiary requirements

Records of regularly-conducted business activity for historical cell site analysis: CDRs must be introduced into evidence through a records custodian employed by the cell provider, unless the parties stipulate to their admissibility. Consideration should be given to introduction of relevant cell tower data/maps through a cell provider's records custodian or other qualified witness employed by the cell provider, such as a cell tower technician. If cell tower data/maps for multiple areas are voluminous, they may be presented in a summary exhibit under Federal Rule of Evidence 1006, which also requires that such evidence be made available to the defense for examination, copying, and, if ordered, production in court. *See* FED. R. EVID. 1006. Additionally, a qualified expert may be permitted to testify as to opinions based on a particular cell provider's cell tower data without such data being admitted into evidence if the trial court finds that it is the type of data reasonably relied on by experts in this particular field. *See* FED. R. EVID. 703, 705. CAST experts are qualified experts based on their training and experience with several major cell providers and their weekly contact with various cell providers regarding the providers' cell tower networks.

Rule 803(6) of the Federal Rules of Evidence governs the admissibility of a cell provider's CDRs and cell tower data/maps through a cell provider's records custodian or other qualified witness. These records qualify as business records and should be admitted into evidence as an exception to the hearsay rule. *See* FED. R. EVID. 802, 803(6). Any defense argument to the contrary simply ignores the fact that cell providers collect and maintain CDRs and cell tower location data in the course of their regularly-conducted business activity for the purpose of maintaining a reliable, operational cellular network and collecting their share of the billions of dollars in revenue from cell phone users.

In *United States v. Sanchez*, 586 F.3d 918, 927-29 (11th Cir. 2009), the Eleventh Circuit rejected several defense arguments that CDRs in that case were admitted erroneously into evidence. The records custodian for the cell provider in *Sanchez*, MetroPCS, testified that MetroPCS's cell towers stored information for two or three days that included tower i/d switch, cell sector id, caller's cell phone number, call date/time, telephone number dialed, and call duration. The MetroPCS information subsequently was transmitted to a third-party contractor, Verisign, for database storage. Depending on MetroPCS's business needs, Verisign continued to store this database information for six months. MetroPCS had and used software to retrieve the Verisign-stored data that had originated from MetroPCS's cellular network. Based on this testimony, the trial court admitted into evidence CDRs that were produced and offered through the MetroPCS records custodian.

The defense argument that admission of the CDRs under Rule 803(6) should have been through a records custodian from the third-party storage contractor was found by the *Sanchez* court to be frivolous. *Id.* at 928-29. The court also rejected the defense argument that the stored CDR database was not a MetroPCS record, finding that the replicated database information stored by the third-party contractor initially had been collected and recorded by MetroPCS cell towers and that MetroPCS relied on the stored database to maintain its cell towers and reconcile its cell phone billing. A third defense attack on the CDRs, that MetroPCS's extraction of CDRs from Verisign's database was not a reliable indicator of information contained in Verisigns's CDR database, was rejected based on the lack of any showing that the MetroPCS information-extracting software was defective or manipulatable. *Id.* at 929.

CDRs and cell tower data/maps also may be introduced into evidence through certification of a records custodian or other qualified witness pursuant to Federal Rule of Evidence 902(11) without violating the Confrontation Clause. *See United States Yeley-Davis*, 632 F.3d 673 (10th Cir.) (certified cell

phone records admitted into evidence pursuant to cell provider's certification under Rule 902(11) did not violate Sixth Amendment's Confrontation Clause), *cert. denied*, 131 S.Ct. 2172 (2011); *see also Sanchez*, 586 F.3d at 529 (rejecting "patently frivolous" defense argument that presentation of summary records through detective rather than cell provider's records custodian deprived defendant of Sixth Amendment right to cross-examine the records custodian).

Caution should be exercised in admitting CDRs into evidence through Rule 902(11) certification or by stipulation if cell site data is coded in a cell provider's CDRs. A Rule 702 expert may testify about decoded cell tower locations made known to the expert by the applicable cell provider because the tower locations are the type of facts and data reasonably relied upon in the field of historical cell site analysis. *See* FED. R. EVID. 703. However, if a non-expert summary witness will be called to testify about mapped cell tower locations based on such CDRs, consideration should be given to admitting cell provider records at trial to enable decoding of the cell tower locations listed in the CDRs into identifiable geographic locations. Such evidence may consist of additional business records produced by the cell provider's records custodian that decodes the CDR cell site data into geographic locations, or testimony from the cell provider's records custodian with knowledge or records to decode the cell tower locations, which also may include cell sector information.

Expert witness testimony - Federal Rule of Evidence 702, *Daubert*, and *Kumho Tire*:

Expert testimony is admissible at trial pursuant to FED. R. EVID. 702 that provides:

> If scientific, technical, or other specialized knowledge will assist the trier of fact to understand the evidence or to determine a fact in issue, a witness qualified as an expert by knowledge, skill, experience, training, or education, may testify thereto in the form of an opinion or otherwise, if (1) the testimony is based upon sufficient facts or data, (2) the testimony is the product of reliable principles and methods, and (3) the witness has applied the principles and methods reliably to the facts of the case.

FED. R. EVID. 702. Beginning in1993, the Supreme Court provided trial courts with guidance on admission of expert evidence at trial.

In *Daubert v. Merrell Dow Pharm., Inc.*, 509 U.S. 579 (1993), the Supreme Court established a two-prong test for the admissibility of scientific evidence. The first prong rejected the widely used "general acceptance" test enunciated in *Frye v. United States*, 293 Fed.1013 (App. D.C. 1923), decided half a century before the Federal Rules of Evidence were adopted, in favor of a more flexible standard that reviews the scientific validity and reliability of the evidence. The second prong, sometimes referred to as the "relevancy" requirement, simply reiterated that scientific testimony or evidence must assist the trier of fact to be admissible. *See Maryland Cas. Co. v. Therm-O-Disc, Inc.*, 137 F.3d 780, 783 (4th Cir. 1998) (finding that *Daubert* replaced the stricter "general acceptance" test of *Frye* with a requirement that the proffered testimony merely be reliable and helpful and that trial court's role is "that of a 'gatekeeper' who should exercise broad discretion in admitting scientific testimony"), citing *Daubert*, 509 U.S. at 579.

The Supreme Court in *Daubert* listed four non-exclusive factors that are helpful to determine the reliability of scientific testimony: (1) whether the scientific theory or technique can be (and has been) tested; (2) whether the theory or technique has been subjected to peer review and publication; (3) whether a particular technique has a known potential rate of error; and (4) whether the theory or technique is generally accepted in the relevant scientific community. *Daubert*, 509 U.S. at 593-95. The Court noted that these factors do not constitute a "definitive checklist or test," and that "[m]any factors will bear on the inquiry" that involves "a preliminary assessment of whether the reasoning or methodology underlying the testimony is scientifically valid and of whether that reasoning or methodology properly can be applied to the facts in issue." *Id.* at 592-93. The inquiry to be undertaken by a trial court is "a flexible one" focusing

on the "principles and methodology" employed by the expert, not on the conclusions reached. *Id.* at 594-95. Expert testimony, like all other admissible evidence, is subject to testing by "[v]igorous cross-examination, presentation of contrary evidence, and careful instruction on the burden of proof." *Id.* at 596.

In *Kumho Tire Co., Ltd.* v. *Carmichael*, 526 U.S. 137 (1999), the Supreme Court extended the *Daubert* test to include expert testimony involving technical and other specialized knowledge. *Kumho Tire*, 526 U.S. at 141. The Court held that a trial court "may consider one or more of the specific factors that *Daubert* mentioned when doing so will help determine that testimony's reliability." *Id.* The Court again noted that a trial court considering the admissibility of expert testimony exercises a gatekeeping function to assess whether the proffered evidence is sufficiently reliable and relevant. *Id.*

Kumho Tire also made clear that a trial court is not required to conduct a pretrial hearing based on a *Daubert* challenge. *Id.* at 152. A trial court has considerable latitude in deciding whether or when special briefing or other proceedings are needed to investigate challenged reliability of proposed expert testimony. *Id.* at 152-53. Pretrial evidentiary hearings are particularly unnecessary when expert testimony is based on well-established principles. *See, e.g.*, *United States v. Beasley*, 495 F.3d 142, 150 (4th Cir. 2007) (no abuse of discretion where narcotics agent testified as an expert witness regarding conversion of powder cocaine into crack cocaine without pre-trial *Daubert* hearing).

Historical cell site analysis evidence is clearly admissible at trial through a qualified expert witness pursuant to Rule 702, *Daubert*, and *Kumho Tire*. It is evidence that is based on valid, reliable, scientific, technical, and specialized knowledge that will assist the jury in understanding the evidence and determining facts in issue. Specifically, various locations of cell phones associated with the users on specific dates and at specific times relative to the relevant places and events in the case will be of assistance to the jury. The *Daubert* analysis is satisfied because (1) the scientific theory underlying cell phone communications is over 150 years old, the technology for cellular communication on a hand-held cell phone is almost 40 years old, and the scientific theory and technology have been tested for decades in the multibillion-dollar wireless communications industry, (2) the theory and techniques involved in cell phone communications have been subjected to peer review and publication for decades, (3) the nature of cell phone communications in a wireless cellular network are such that no rate of error exists when a cell phone makes a connection within a cell tower sector and can be easily tested by making a cell phone call and inspecting the corresponding CDR information, and (4) the scientific theory and techniques in wireless cellular communications are generally accepted in the relevant scientific community of wireless communications. *See Daubert*, 509 U.S. at 593-95. Finally, a witness who has gained expertise in historical cell site analysis through experience, training, or education may testify as an expert witness regarding the technical and specialized knowledge aspects of historical cell site analysis pursuant to Rule 702 and *Kumho Tire*.

VII. Conclusion

Historical cell site analysis evidence has become an important investigative tool in recent years for law enforcement agencies. In an age when Americans use cell phones for 11.7 billion call minutes and text messages every day, historical cell site analysis may provide valuable evidence in a criminal trial. Call detail records for cell phones can establish the exact dates, times, and general locations of cell phones relative to the longitude and latitude of geographically-fixed cell towers when cell phones are used to initiate, receive, or terminate a voice call or send or receive text messages. Geo-locating cell phones associated with defendants, accomplices, witnesses, or victims can establish cell phone movement patterns and proximity to crime scenes or other relevant locations.

Presentation of historical cell site analysis evidence at trial requires advance planning. First, CDRs that cell providers retain for short time periods, ranging from six to eighteen months, must be preserved as

soon as possible and collected from cell providers with appropriate legal process. Second, a qualified expert should be recruited to conduct the historical cell site analysis, prepare a written report, and prepare demonstrative trial exhibits that will be helpful in explaining historical CSA evidence to a jury. Third, all records, reports, underlying facts, and data for the expert's opinions and demonstrative trial exhibits must be made available for copying and inspection by the defense during discovery in advance of trial, pursuant to Federal Rule of Criminal Procedure 16, local court orders, and standard practice. Finally, it may be appropriate in cases where the trial court is not familiar with this type of evidence to file a motion in limine or trial brief regarding historical cell site analysis so that the trial court is familiar with the admissibility of CDRs and other business records of cell providers and expert testimony on historical cell site analysis evidence under Federal Rule of Evidence 702, *Daubert*, and *Kumho Tire*.❖

ABOUT THE AUTHOR

❑**Thomas A. O'Malley** currently is the Computer Hacking and Intellectual Property (CHIP) Coordinator and Identity Theft Coordinator for the United States Attorney's Office in the Western District of North Carolina. He served as the district's Lead OCDETF Attorney and Deputy Criminal Chief (2005 - 2009) following his transfer from the United States Attorney's Office in the Southern District of Florida (1986 - 2004), where he served as a Deputy Criminal Chief in the Fort Lauderdale and West Palm Beach branch offices (2000 - 2004). He began his prosecutorial career as a state prosecutor in 1980 and has conducted over 175 jury trials. Mr. O'Malley serves regularly as an instructor for the Department of Justice's Basic and Intermediate Trial Advocacy Programs at the National Advocacy Center. ✠

Compelling Online Providers to Produce Evidence Under ECPA

Josh Goldfoot
Senior Counsel
Computer Crime and Intellectual Property Section

This article is adapted from Chapter 3 of Searching and Seizing Computers and Obtaining Electronic Evidence in Criminal Investigations, 115-48 (3d ed. 2009).

I. Introduction

Much evidence of Internet use and communication is located online. This means that Internet companies, such as mail providers, social networking sites, and Internet Service Providers, have copies of the evidence on their servers. The government, as part of a law enforcement investigation, may compel those providers to produce that evidence. However, a federal law, the Electronic Communications Privacy Act (ECPA), 18 U.S.C. §§ 2701-2712, restricts the government's ability to do so.

Whenever agents or prosecutors seek stored email, account records, or subscriber information from an Internet company such as an ISP or a social networking site, they must comply with ECPA. It sets forth a system of statutory privacy rights for customers and subscribers of computer network service providers. Section 2703 creates a code of criminal procedure that federal and state law enforcement officers must follow to compel disclosure of stored communications from network service providers. Section 2702 regulates voluntary disclosure by network service providers of customer communications and records to both government and non-government entities.

To assist agents and prosecutors in complying with ECPA, the Computer Crimes and Intellectual Property Section has collected advice and go-bys on an Intranet site, CCIPS Online, available at http://dojnet.doj.gov/criminal/ccips/online. That site contains go-bys for complying with ECPA, including preservation letters and ECPA search warrants specialized for email, social networking sites, cell phones, and other applications. For monthly updates about ECPA and other electronic evidence issues, federal prosecutors and agents may subscribe to the CCIPS Electronic Evidence Newsletter by emailing ccips.tips@usdoj.gov.

II. Preservation

In general, no law regulates how long network service providers must retain account records in the United States. Some providers retain records for months, others for hours, and others not at all. As a result, some evidence may be destroyed or lost before law enforcement can obtain the appropriate legal order compelling disclosure. For example, suppose that a crime occurs on Day 1 but agents do not learn of the crime until Day 28. They begin work on a search warrant on Day 29 and obtain the warrant on Day 32, only to learn that the network service provider deleted the records in the ordinary course of business on Day 30. To minimize the risk that evidence will be lost, ECPA permits the government to direct providers to "freeze" stored records and communications pursuant to § 2703(f). Specifically, § 2703(f)(1) states:

> A provider of wire or electronic communication services or a remote computing service, upon the request of a governmental entity, shall take all necessary steps to preserve

> records and other evidence in its possession pending the issuance of a court order or other process.

18 U.S.C. § 2703(f)(1) (2010).

There is no legally prescribed format for § 2703(f) requests. While a simple phone call should be adequate, a fax or an email is a safer practice because it both provides a paper record and guards against misunderstanding. Upon receipt of the government's request, the provider must retain the records for 90 days, renewable for another 90-day period upon a government request. *See* 18 U.S.C. § 2703(f)(2) (2010). A sample preservation letter is available on CCIPS Online.

Agents who send § 2703(f) letters to network service providers should be aware of two limitations. First, § 2703(f) letters should not be used prospectively to order providers to preserve records not yet created. If agents want providers to record information about future electronic communications, they should comply with the Pen Register and Trap and Trace Act, 18 U.S.C. §§ 3121-3127 and the Wiretap Act, 18 U.S.C. §§ 2510-2522.

A second limitation of § 2703(f) is that some providers may be unable to effectively comply with § 2703(f) requests or may be unable to comply without taking actions that could potentially alert a suspect. In such a situation, the agent must weigh the benefit of preservation against the risk of alerting the subscriber. The key here is effective communication; agents should communicate with the network service provider before ordering the provider to take steps that may have unintended adverse effects.

III. Appropriate process for non-content information

A. Basic subscriber and session information listed in § 2703(c)(2)

Section 2703(c)(2) lists the categories of basic subscriber and session information:

> (A) name; (B) address; (C) local and long distance telephone connection records, or records of session times and durations; (D) length of service (including start date) and types of service utilized; (E) telephone or instrument number or other subscriber number or identity, including any temporarily assigned network address; and (F) means and source of payment for such service (including any credit card or bank account number)[.]

18 U.S.C. § 2703(c)(2) (2010).

In general, the items in this list relate to the identity of a subscriber, his relationship with his service provider, and his basic session connection records. In the Internet context, "any temporarily assigned network address" includes the IP address used by a customer for a particular session. For example, for a Webmail service, the IP address used by a customer accessing his email account constitutes a "temporarily assigned network address." This list does not include other, more extensive transaction-related records, such as logging information revealing the email addresses of persons with whom a customer corresponded.

ECPA permits the government to compel disclosure of the basic subscriber and session information using a subpoena. Investigators may use any federal or state grand jury or trial subpoena or an administrative subpoena authorized by a federal or state statute. *See id.* A sample subpoena is available on CCIPS Online. Of course, evidence obtained in response to a federal grand jury subpoena must be protected from disclosure pursuant to FED. R. CRIM. P. 6(e).

B. Records or other information pertaining to a customer or subscriber

Section 2703(c)(1) covers a second type of information, "a record or other information pertaining to a subscriber to or customer of such service (not including the contents of communications)." This provision provides a catch-all category that includes all records that are not contents, including basic subscriber and session information described in the previous section. As one court explained, "a record means something stored or archived [and t]he term information is synonymous with data." *In re Applications of United States*, 509 F. Supp. 2d 76, 80 (D. Mass. 2007).

Common examples of "record[s] . . . pertaining to a subscriber" include transactional records, such as account logs that record account usage; cell-site data for cellular telephone calls; and email addresses of other individuals with whom the account holder has corresponded. *See* H.R. Rep. No. 103-827, at 10, 17, 31 (1994), reprinted in 1994 U.S.C.C.A.N. 3489, 3490, 3497, 3511. *See also In re Applications of the United States*, 509 F. Supp. 2d 76, 80 (D. Mass. 2007) (historical cell-site information falls within scope of § 2703(c)(1)); *Hill v. MCI WorldCom Communications, Inc.*, 120 F. Supp. 2d 1194, 1195 (S.D. Iowa 2000) (concluding that the "names, addresses, and phone numbers of parties . . . called" constituted "a record or other information pertaining to a subscriber or customer of such service," not contents, for a telephone account); *Jessup-Morgan v. America Online, Inc.*, 20 F. Supp. 2d 1105, 1108 (E.D. Mich. 1998) (holding that a customer's identification information is a "record or other information pertaining to a subscriber" rather than contents); *United States v. Allen*, 53 M.J. 402, 409 (C.A.A.F. 2000) (concluding that "a log identifying the date, time, user, and detailed internet address of sites accessed" by a user constituted a "record or other information pertaining to a subscriber or customer of such service" under ECPA).

According to the legislative history of the 1994 amendments to § 2703(c), the purpose of separating the basic subscriber and session information from other non-content records was to distinguish basic subscriber and session information from more revealing transactional information that could contain a "person's entire on-line profile." H.R. Rep. No. 103-827, at 17, 31-32 (1994), reprinted in 1994 U.S.C.C.A.N. 3489, 3497, 3511-12.

Agents need a § 2703(d) court order to obtain most account logs and most transactional records. Agents who obtain a court order under § 2703(d) may obtain basic subscriber information as well as all "record[s] or other information pertaining to a subscriber to or customer of such service (not including the contents of communications [held by providers of electronic communications service and remote computing service]) . . . ." 18 U.S.C. § 2703(c)(1) (2010). A court order authorized by § 2703(d) may be issued by any federal magistrate, district court, or equivalent state court judge. *See* 18 U.S.C. §§ 2703(d), 2711(3) (2010).

To obtain such an order,

> the governmental entity [must] offer[] specific and articulable facts showing that there are reasonable grounds to believe that the contents of a wire or electronic communication, or the records or other information sought, are relevant and material to an ongoing criminal investigation.

18 U.S.C. § 2703(d) (2010).

This standard does not permit law enforcement merely to certify that it has specific and articulable facts that would satisfy such a showing. Rather, the government must actually offer those facts to the court in the application for the order. *See United States v. Kennedy*, 81 F. Supp. 2d 1103, 1109-10 (D. Kan. 2000) (concluding that a conclusory application for a 2703(d) order "did not meet the requirements of the statute"). As the Tenth Circuit has noted, the "specific and articulable facts" standard of 2703(d) "derives

from the Supreme Court's decision in [*Terry v. Ohio*, 392 U.S. 1 (1968)]." *United States v. Perrine*, 518 F.3d 1196, 1202 (10th Cir. 2008).

As a practical matter, a short factual summary of the investigation and the role that the records will serve in advancing the investigation should satisfy this criterion. A more in-depth explanation may be necessary in particularly complex cases. Sample § 2703(d) order applications are available on CCIPS Online.

Section 2703(d) orders that are issued by federal courts have effect outside the district of the issuing court. ECPA permits a judge to enter § 2703(d) orders compelling providers to disclose information even if the judge does not sit in the district in which the information is stored. *See* 18 U.S.C. § 2703(d) (2010) (stating that "any court that is a court of competent jurisdiction" may issue a 2703(d) order) (emphasis added); *id.* § 2711(3) (stating that the term " 'court of competent jurisdiction' has the meaning assigned by section 3127, and includes any Federal court within that definition, without geographical limitation"); 18 U.S.C. § 3127(2) (2010) (defining "court of competent jurisdiction").

IV. Appropriate process for content of communications stored with providers

The contents of a network account are the actual files (including email) stored in the account. *See* 18 U.S.C. § 2510(8) (2010) ("'contents,' when used with respect to any wire, oral, or electronic communication, includes any information concerning the substance, purport, or meaning of that communication"). For example, stored emails or voice mails are "contents," as are word processing files stored in employee network accounts. The subject lines of emails are also contents. *Cf. Brown v. Waddell*, 50 F.3d 285, 292 (4th Cir. 1995) (noting that numerical pager messages allow "an unlimited range of number-coded substantive messages" in the course of holding that the interception of pager messages requires compliance with Title III).

A. Search warrants

Investigators can obtain everything associated with an account with a search warrant. ECPA does not require the government to notify the customer or subscriber when it obtains information from a provider using a search warrant.

Agents who obtain a search warrant under § 2703 may obtain any content or non-content information pertaining to an account by obtaining a search warrant "issued using the procedures described in" FED. R. CRIM. P. 41; 18 U.S.C. § 2703(a) (2010).

Search warrants issued under § 2703 have several noteworthy procedural features. First, as mentioned earlier, although most search warrants obtained under Rule 41 are limited to "a search of property . . . within . . . the district" of the authorizing magistrate judge, search warrants under § 2703 may be issued by a federal "court with jurisdiction over the offense under investigation," even for records held in another district. *See United States v. Berkos*, 543 F.3d 392, 396-98 (7th Cir. 2008); *In re Search of Yahoo, Inc.*, 2007 WL 1539971, at *6 (D. Ariz. May 21, 2007); *In re Search Warrant*, 2005 WL 3844032, at *5-6 (M.D. Fla. Feb. 13, 2006) ("Congress intended 'jurisdiction' to mean something akin to territorial jurisdiction."). State courts may also issue warrants under § 2703 but the statute does not give these warrants effect outside the limits of the courts' territorial jurisdiction. Second, obtaining a search warrant obviates the need to give notice to the subscriber. *See* 18 U.S.C. § 2703(b)(1)(A) (2010); FED. R. CRIM. P. 41(f)(1)(C).

Third, investigators ordinarily do not themselves search through the provider's computers in search of the materials described in the warrant. Instead, investigators serve the warrant on the provider as they would a subpoena and the provider produces the material specified in the warrant. *See* 18 U.S.C.

§ 2703(g) (2010) (stating that the presence of an officer is not required for service or execution of a § 2703 warrant); *United States v. Bach*, 310 F.3d 1063, 1068 (8th Cir. 2002) (finding search of email by ISP without presence of law enforcement did not violate Fourth Amendment).

Fourth, a two-step process is often used to obtain the content of communications under a § 2703 warrant. Initially, the warrant directs the service provider to produce all email from within the specified account or accounts. The warrant also authorizes law enforcement to review the information produced to identify and copy information that falls within the scope of the particularized "items to be seized" under the warrant.

Otherwise, as a practical matter, § 2703 search warrants are obtained much like Rule 41 search warrants. As with a typical Rule 41 warrant, investigators must draft an affidavit and a proposed warrant that complies with Rule 41.

CCIPS Online contains go-bys for search warrants tailored to several specific applications, including email accounts, social networking sites, Web site hosting, and cell phones.

B. Content without a search warrant

ECPA divides contents into two categories: (1) contents in "electronic storage" held by a provider of electronic communication service and (2) contents stored by a remote computing service. (Contents that fall outside of these two categories are not protected by ECPA.) The distinction is important because ECPA requires law enforcement to obtain a warrant to compel production of contents in "electronic storage" in an electronic communication service for less than 181 days but allows the use of a subpoena or 2703(d) order to compel production of other contents. When a subpoena or § 2703(d) order is used to obtain contents, ECPA requires either prior notice to the subscriber or customer or complying with the delayed notice provisions of § 2705.

Prosecutors who endorse the use of process other than a warrant to obtain the contents of communications, however, should be aware of *United States v. Warshak*, 631 F.3d 266 (6th Cir. 2010). In *Warshak*, the Sixth Circuit held, as a constitutional matter, that "[t]he government may not compel a commercial ISP to turn over the contents of a subscriber's emails without first obtaining a warrant based on probable cause" and "to the extent that [ECPA] purports to permit the government to obtain such emails warrantlessly, [ECPA] is unconstitutional." *Id.* at 288. Many providers have informed the Department that, because of *Warshak*, they will refuse to provide content without search warrants. Prosecutors who are considering the use of a subpoena or a § 2703(d) order to obtain the contents of communications from a commercial ISP are encouraged to consult with CCIPS.

V. Orders not to disclose the existence of a warrant, subpoena, or court order

Section § 2705(b) states:

> A governmental entity acting under section 2703, when it is not required to notify the subscriber or customer under section 2703(b)(1), or to the extent that it may delay such notice pursuant to subsection (a) of this section, may apply to a court for an order commanding a provider of electronic communications service or remote computing service to whom a warrant, subpoena, or court order is directed, for such period as the court deems appropriate, not to notify any other person of the existence of the warrant, subpoena, or court order. The court shall enter such an order if it determines that there is reason to believe that notification of the existence of the warrant, subpoena, or court order will result in--

(1) endangering the life or physical safety of an individual;

(2) flight from prosecution;

(3) destruction of or tampering with evidence;

(4) intimidation of potential witnesses; or

(5) otherwise seriously jeopardizing an investigation or unduly delaying a trial.

18 U.S.C. § 2705(b) (2010).

This language permits agents to apply for a court order directing network service providers not to disclose the existence of legal process whenever the government itself has no legal duty to notify the customer or subscriber of the process. If the relevant process is a § 2703(d) order or § 2703 warrant, agents can simply include appropriate language in the application and proposed order or warrant. If agents instead seek to compel the disclosure of information using a subpoena, they must apply separately for this order. A sample § 2705(b) application is available on CCIPS Online.

VI. Reimbursement

When a government entity obtains information pursuant to ECPA, the network provider may be entitled to reimbursement for its reasonable costs incurred in supplying the information.

In general, persons and entities are not entitled to reimbursement for complying with federal legal process unless there is specific federal statutory authorization. However, in many (but not all) circumstances, ECPA requires government entities obtaining the contents of communications, records, or other information pursuant to ECPA to reimburse the disclosing person or entity. *See* 18 U.S.C. § 2706 (2010).

Section 2706 generally obligates government entities "obtaining the contents of communications, records, or other information under section 2702, 2703, or 2704" to pay the service provider "a fee for reimbursement for such costs as are reasonably necessary and which have been directly incurred in searching for, assembling, reproducing, or otherwise providing such information." *Id.* § 2706(a). Significantly, this section only requires reimbursement when the government actually obtains communication content, records, or other information. Thus, the government is not required to pay for costs incurred by a provider in responding to a § 2703(f) preservation letter unless the government later obtains the preserved records.

The amount of the fee required under § 2706(a) "shall be as mutually agreed by the governmental entity and the person or entity providing the information or, in the absence of agreement, shall be as determined by the court . . . ." *Id.* § 2706(b). In practice, if the service provider seeks what appears to be unreasonably high reimbursement costs, the government should demand a detailed accounting of costs incurred by activity. A cost accounting will help ensure that the provider is not seeking reimbursement for indirect costs or activities that were not reasonably necessary to the production.

In addition, ECPA contains a reimbursement exception that precludes reimbursement in specific circumstances. The reimbursement requirement "does not apply with respect to records or other information maintained by a communications common carrier that relate to telephone toll records and telephone listings obtained under section 2703" unless a court determines that the information sought by the government is "unusually voluminous" or "caused an undue burden on the provider." *Id.* § 2706(c).

VII. Remedies

ECPA does not provide a suppression remedy. *See* 18 U.S.C. § 2708 (2010) ("The [damages] remedies and sanctions described in this chapter are the only judicial remedies and sanctions for nonconstitutional violations of this chapter."). Accordingly, nonconstitutional violations of ECPA do not result in suppression of the evidence. *See United States v. Perrine*, 518 F.3d 1196, 1202 (10th Cir. 2008) ("[V]iolations of the ECPA do not warrant exclusion of evidence."); *United States v. Steiger*, 318 F.3d 1039, 1049 (11th Cir. 2003); *United States v. Smith*, 155 F.3d 1051, 1056 (9th Cir. 1998) ("[T]he Stored Communications Act expressly rules out exclusion as a remedy . . . .").❖

ABOUT THE AUTHOR

❑**Josh Goldfoot** is Senior Counsel with the Computer Crime and Intellectual Property (CCIP) Section where he has worked since 2005. He prosecutes criminal cases involving computer crime and provides legal advice about electronic evidence and computer search issues. His prior publications, all in a personal capacity, include: *The Physical Computer and the Fourth Amendment*, 16 BERKELEY J. CRIM. L. 112 (2011) (discussing computer search and seizure law); *A Declaration of the Dependence of Cyberspace*, 32 COLUM. J.L. & ARTS 365 (2009) (with Alex Kozinski) (discussing federal law's reach on the cyberspace community); *Method of Shape Recognition Using Postulated Lines*, U.S. Patent No. 7,418,136 B2 (filed Mar. 30, 2004) (issued Aug. 26, 2008); *Antitrust Implications of Internet Administration*, 84 VA. L. REV. 909 (1998) (discussing antitrust laws' application to parties' disputes involving the internet).✠

Admissibility of Forensic Cell Phone Evidence

Timothy M. O'Shea
Assistant United States Attorney
Western District of Wisconsin

James Darnell
Special Agent
Criminal Investigative Division
United States Secret Service

I. Introduction

At 3 p.m., an undercover officer receives a call, recognizes the defendant's cell phone number, and speaks to him. A second officer watches the defendant place the call and arrests him moments later, recovering the phone. The officers give the phone to the forensic examiner who advises that the cell phone's call logs show no outgoing calls during the afternoon in question. The cellular service provider records support the examiner and state that no records of outgoing calls were made on the phone the entire afternoon. If the call records are not in the phone's call logs or with the provider, where is the evidence?

While cell phone evidence may be crucial to a case, the evidence may not be where it is expected to be and it may take time to develop the evidence and understand its admissibility. This article is divided into two parts—a primer on cell phone forensics and technical issues and a discussion of evidentiary issues. The first section relies on a resource that prosecutors wanting to introduce cell phone evidence should become familiar with, the Prosecutor's Initial Reference List for Cell Phone Evidence (PIRL-Cell Phones), *available at* http://dojnet.doj.gov/criminal/ccips/online/lab.htm. The second section, which addresses evidentiary and Constitutional issues in admitting cell phone evidence at trial, relies on Chapter 5 of the SEARCHING AND SEIZING COMPUTERS AND OBTAINING ELECTRONIC EVIDENCE IN CRIMINAL INVESTIGATIONS MANUAL (3rd ed. Office of Legal Education 2009), *available at* http://www.cybercrime.gov/ssmanual/.

II. Cell phone forensics

Today's cell phones often hold information similar to that held in computers. Cell phones may contain key evidence that may be difficult or impossible to obtain elsewhere. For example, while cellular providers typically retain text messages for a very short time (forty-eight hours or less), a forensic examiner may find weeks or months of text messages in a cell phone. This information can serve as the backbone of a time line of significant case events. On the other hand, a great deal of information relating to cell phone use will be found—sometimes exclusively—at the cell phone service provider or at a third party service provider like Google. In this way, cell phone evidence is an introduction to "cloud computing," where information that is accessed, used, and manipulated by a device is stored outside of the device itself.

Before addressing information stored outside the phone, it is important to understand the unique forensic challenges that cell phones present. In this context, "forensics" typically refers to extracting information from cell phones using repeatable and verifiable processes. Due to the way cell phones work,

the traditional forensic view of not inducing a change to the phone is rarely possible. Instead, an examiner's goal is typically to avoid changing user data while extracting information and documenting changes to the cell phone resulting from the forensic process.

The complexity of cell phones means, at present, that no one forensic tool can "do it all." To illustrate this point, cell phones are contrasted with computers. Today, a relatively small number of computer operating systems are widely used. For example, eighty-three percent of computers sold last year used some version of the Windows operating system. It follows that, in general, forensic tool makers have designed reliable tools to extract, verify, and analyze the information contained within computers employing widely-used operating systems.

Unlike computers with a limited number of operating systems, there are presently at least nine cell phone operating systems available (Symbian, Android, Apple iOS, Blackberry OS, Windows Mobile, webOS, Bada, MeeGo, and Maemo). Furthermore, cell phone variety multiplies exponentially when one moves beyond operating systems to the many different cell phone manufacturers, then to the numerous models each manufacturer offers, then to the options within those models, and finally to the applications or "apps" offered by third parties. For example, as of late last year, there were approximately 300,000 apps for the iPhone, 100,000 apps for the Android phone, and 15,000 apps for Blackberry available.

Unsurprisingly, forensic tool designers struggle to develop tools to analyze the many types of cell phones. Likewise, prosecutors, courts, and juries must understand that an examiner will often use several forensic tools to extract different types of information from a single phone and that some tools work better than others in obtaining information from certain phones.

Another contrast between computer and cell phone examinations is that a "hash" is typically not created in connection with the examination of cell phones. With computer analyses, an "acquisition hash" is foundational to both the exam and the admissibility of the results. Because the examiner works on a copy of the extracted information and not on the seized computer or hard drive itself, the "hash" serves as a "digital fingerprint" and verifies that the examiner is examining an exact copy. A forensic hash program applies an algorithm to generate a unique alpha-numerical identifier called a "hash" to a set of data (for example, all the information on a hard drive). After acquiring the information from the original, the examiner verifies that the copy has the same "hash" value as the original. If the data is changed even a little (such as adding or deleting a comma), the "hash" changes. From a prosecutor's perspective, the acquisition hash simply confirms that the duplicate set of data that is examined is an exact copy of the original source data.

In contrast, given the way cell phone memory works and the present limitations of many of the forensic tools used to analyze cell phones, an acquisition hash is not typically created when examining a cell phone. It follows, therefore, that the examiner must use other means to verify the information. For example, the examiner may simply turn on the phone and navigate to the data by hand after using the forensic tool (forensics by thumb) to compare what is seen with what was extracted and reported by the tool. Also, where two forensic tools can be used to obtain information from a phone, the examiner may use both tools and then compare to see whether the forensic results match. If the results do not match, it does not necessarily mean that the tools—or the examiner—are ineffective. The disparity should be explored before trial.

A. Three levels of sophistication in cell phone examinations

Depending on the make and model of a cell phone, the forensic examiner's level of training, and the tools available to the examiner, there are three general levels of sophistication in the forensic examination of a cell phone. At the most basic level, an examiner may process a phone by taking pictures

of the phone screen while scrolling through the relevant information. This method is often used when information on the phone must be documented immediately.

The second level of sophistication involves forensic tools that enable examiners to recover from most cell phones identifiable "objects," such as pictures, call logs, text messages, and contact lists. Still within this category, but using somewhat more sophisticated tools that look at the contents of a cell phone after the contents have been put in a logical order by the phone's operating system, examiners can recover from some phones directory trees, folders, and files beyond the "objects" that simpler tools recognize. These tools produce a "logical" file system recovery. Deleted information is typically not recovered with this process.

At the third level of sophistication, examiners use "physical recovery" processes. At this level, forensic tool support is typically both limited and expensive. Furthermore, this type of examination requires an experienced examiner with access to sophisticated processing tools. For example, an examiner at this level may have to physically remove (desolder) the data storage chips within the phone and read the information stored within the chip through a chip programmer. This "chip off" process is often a last resort and is typically used only when a phone has been damaged to such an extent that other processes do not work. At present, only three known United States federal law enforcement labs attempt the "chip off" process described here. When a cell phone is acquired using this method, the acquisition hash process described above can be applied to the extracted file.

B. Relevant cell phone evidence may be found outside the cell phone.

In addition to data or evidence found on a cell phone through a forensic examination, additional evidence relating to cell phone use may be obtained outside the cell phone. This information may corroborate evidence on the phone or fill in gaps in the evidence if information on the phone was deleted. A person may synchronize his phone with a computer or use third party services (for example, Google) that result in relevant information, such as text messages, email, voice mail, transcribed voice mails, and Internet search terms being stored outside of the phone itself.

If the defendant in the introductory paragraph called the undercover officer using voice over Internet protocol (VoIP), such as Google Voice, Skype, or Rebtel, evidence relating to the call would be found within the phone's Internet history rather than within the call logs and with the VoIP provider, not the cell service provider.

Historical location information: Our hypothetical defendant's call record is a good example of how cell phone evidence may turn up in unexpected places. However, historical location evidence best illustrates how information can be found both within and outside the phone. A cell phone provider will maintain for a time cell tower records that indicate the cell tower through which a call was channeled. Because cell phones typically communicate through cell towers that are proximate to the phone, these "tower records" give an approximate location of a phone during a call. In addition, cell towers are typically divided into three sectors, each representing 120 degrees of a 360 degree spectrum.

The specific cell tower sector that the cell phone call was channeled through further approximates the cell phone's location. Finally, when a cell phone moves during a call, the call may channel through multiple towers and sectors, thus indicating the direction that the cell phone user moved during the call. However, cell tower information is described as "approximate" for good reason. In rural areas, for example, cell tower information can describe an area covering more than twenty square miles.

Enhanced 911 (E911): More specific information can be obtained from the provider or the phone itself when the E911 system is activated. The Federal Communications Commission's Enhanced 911 initiative requires cell phone providers to be able to pinpoint a user's location so that emergency

responders can find the caller in a crisis. Cell phone providers use three basic processes to comply with the E911 initiative. One process involves analysis of network connection signal strength and the angle that the signal arrives at individual elements within a cell tower. The second process uses Global Positioning System (GPS) chips built into the phone. The third process, employed by some carriers, involves "Network Assisted GPS location" where tower information and GPS data are used together to locate the phone.

GPS: In addition, an examiner may recover historical location information on the phone in several ways, including the use of stored GPS coordinates of the phone or information indicating to which cell towers the phone connected. Furthermore, photographs taken with some cell phones, such as an iPhone or a BlackBerry, may contain GPS location data stored within the image metadata.

Applications: Finally, application providers may also have location information. If one searches for a restaurant using a smart phone app, such as Urbanspoon or Zagat Mobile, the application will use the GPS built into the phone and provide restaurant choices physically proximate to the phone. This type of information may be on the phone in the Internet history, in the phone's application files, or retained by the application provider.

For more detailed information describing the types of information associated with cell phones and how to preserve and obtain cell phone information stored at cellular service and third party providers, see the PIRL-Cell Phones link at http://dojnet.doj.gov/criminal/ccips/online/lab.htm.

III. Evidentiary issues

After a successful examination and investigation, the prosecutor will confront a number of issues in admitting evidence relating to cell phones at trial. *See generally* Chapter 5 of the SEARCHING AND SEIZING COMPUTERS AND OBTAINING ELECTRONIC EVIDENCE IN CRIMINAL INVESTIGATIONS MANUAL (3rd ed. Office of Legal Education 2009) at http://www.cybercrime.gov/ssmanual/. Prosecutors involved with searching, seizing, and introducing computer evidence should keep this manual handy. This section will refer both to cell phone and computer information for two reasons: (1) the same evidentiary considerations apply to both types of information; and (2) as described above, a great deal of information relating to cell phones will be found in computers at the cellular provider or at third-party service providers.

Once an investigator has recovered relevant data associated with a cell phone, a prosecutor preparing to use the information at trial must determine whether the data was created as a result of a process, such as the cell tower records described above; whether it is hearsay, for example, a text message containing an assertion; or whether the information is "mixed" hearsay and process-created information, such as an assertion in an email and the header information associated with the email. This sorting-out process requires a review of both hearsay and foundational evidentiary standards.

Hearsay is "a statement, other than one made by the declarant while testifying at the trial or hearing, offered in evidence to prove the truth of the matter asserted." FED. R. EVID. 801(c). The rule provides that "[a] '*statement*' is (1) an oral or written assertion or (2) nonverbal conduct *of a person*, if it is intended by the person as an assertion." *Id.* 801(a) (emphasis added). The Federal Rules of Evidence do not define the term "assertion." However, courts have held that "the term has the connotation of a positive declaration." *Lexington Ins. Co. v. W. Pa. Hosp.*, 423 F.3d 318, 330 (3d Cir. 2005); *United States v. Lewis*, 902 F.2d 1176, 1179 (5th Cir. 1990).

Many courts have categorically determined that computer records are admissible under Federal Rule of Evidence 803(6), the hearsay exception for "records of regularly conducted activity," more commonly known as the "business records" exception, without first asking whether the records contain hearsay at all. *See, e.g.*, *United States v. Yeley-Davis*, 632 F.3d 673, 678 (10th Cir. 2011) (holding that cell phone tower records are admissible as business records under FED. R. EVID. 803(6)); *Haag v.*

United States, 485 F.3d 1, 3 (1st Cir. 2007) (Internal Revenue Service's computerized records containing notification letters sent to taxpayers following filing of tax lien were admissible under the business records exception to the hearsay doctrine); *United States v. Fujii*, 301 F.3d 535, 539 (7th Cir. 2002) (computer data compiled and presented in computer printouts prepared specifically for trial is admissible, even though the printouts themselves are not kept in the ordinary course of business).

The "business records" foundation has superficial appeal to litigants: it is easy, familiar, and electronically-produced information is often reliable for the same reasons that business records are. The problem, however, with failing to adequately consider whether the information involves a person's "assertion" is that prosecutors are unnecessarily pulled into Confrontation Clause disputes under *Crawford v. Washington*, 541 U.S. 36 (2004), and its progeny. *See, e.g.*, *Yeley-Davis*, 632 F.3d at 678. More about *Crawford* and electronically-produced information appears below.

Some courts, however, recognized that many computer records result from a process, are not "statements" of a person at all, and thus are not hearsay. *See United States v. Lamons*, 532 F.3d 1251, 1262-64 (11th Cir. 2008) (automatically-generated telephone call records are not statements of a person and are thus not hearsay); *United States v. Washington*, 498 F.3d 225, 230-31 (4th Cir. 2007) (printed result of computer-based test was not the statement of a person and thus would not be excluded as hearsay); *United States v. Hamilton*, 413 F.3d 1138, 1142-43 (10th Cir. 2005) (computer-generated header information was not hearsay and no statement or declarant was involved within the meaning of Rule 801); *United States v. Khorozian*, 333 F.3d 498, 506 (3d Cir. 2003) (information provided by a machine is not hearsay); *State v. Kandutsch*, 2011 WL 2820791 at *11 (Wis. July 19, 2011) ("A record created as a result of a computerized or mechanical process cannot lie. It cannot forget or misunderstand. Although data may be lost or garbled as a result of some malfunction, such a malfunction would go to the weight of the evidence, not to its admissibility."). Note, however, that the process used to create information—especially those aspects of a process relying on people—may be legitimate cross-examination fodder. *See Bullcoming v. New Mexico*, 131 S. Ct. 2705, 2711 (2011).

Information relating to cell phones can be divided into three categories. The first category includes non-hearsay information that is created by a process not involving a human assertion, such as telephone toll records, cell tower information, email header information, and GPS data. Although human input triggers some of these processes (for example, dialing a phone number), such conduct is a command to a system, not an assertion, and thus is not hearsay. *United States v. Bellomo*, 176 F.3d 580, 586 (2d Cir. 1999) ("Statements offered as evidence of commands . . . are not hearsay."). The second category involves hearsay records that contain assertions by a human being, such as the content of a voice mail or text message. The third category involves mixed hearsay and non-hearsay records that combine the first two categories and include emails containing both content and header information or a file containing both written text and file creation, last written, and last access dates. After determining the category that the information falls into, prosecutors must lay the appropriate foundation. For a more extensive analysis of the various foundations for hearsay exceptions, see Chapter 5, SEARCHING AND SEIZING COMPUTERS AND OBTAINING ELECTRONIC EVIDENCE IN CRIMINAL INVESTIGATIONS MANUAL (3rd ed. Office of Legal Education 2009).

A. Confrontation Clause

In *Crawford v. Washington*, 541 U.S. 36, 68 (2004), the Supreme Court held that the Confrontation Clause of the Sixth Amendment bars the government from introducing pre-trial "testimonial statements" of an unavailable witness unless the defendant had a prior opportunity to cross examine the declarant. The *Crawford* Court declined to define "testimonial statements," but the Court has subsequently held that when a statement's "primary purpose" is to establish or prove "past events potentially relevant to later criminal prosecution," it is "testimonial" and thus implicates the Sixth Amendment. *See Davis v.*

Washington, 547 U.S. 813, 822 (2006); *Michigan v. Bryant*, 131 S.Ct. 1143, 1155 (2011); *see also Bullcoming v. New Mexico*, 131 S. Ct. 2705, 2713 (2011).

Although Confrontation Clause analysis is distinct from hearsay analysis, records that are the output of a computer-generated process do not implicate the Confrontation Clause for the same reason that computer-generated records are not hearsay: these records simply are not statements of persons. *See United States v. Lamons*, 532 F.3d 1251, 1262-64 (11th Cir. 2008). It is important, however, not to oversimplify the analysis. As noted above, statements that are "testimonial" implicate the Sixth Amendment. *See Bullcoming*, 131 S. Ct. at 2713. In line with this reasoning, the Court has held that an analyst's certification of the results of a gas chromatograph report concerning the percentage of alcohol in a blood sample, as in *Bullcoming*, or a lab result stating that a particular substance was cocaine, as in *Melendez-Diaz v. Massachusetts*, 129 S.Ct. 2527 (2009), are prepared for the "primary purpose" of criminal prosecution and thus implicate the Sixth Amendment. While the underlying data may not implicate the Confrontation Clause, the examiner's report that is prepared for prosecution does.

A necessary but obvious point is that information created or triggered by a cell phone user is not typically "testimonial" because it is not made for the primary purpose of prosecution. For example, cell tower records are created while calls are routed; text messages are used to communicate information; and GPS data results from geo-locating a device. The Supreme Court in *Bullcoming*, however, made clear that criminal defendants have a Sixth Amendment right to confront forensic witnesses about the reliability of the witness and the processes employed. *Bullcoming*, 131 S. Ct. at 2714-15. It follows, therefore, that while the data itself may not implicate the Sixth Amendment, the defendant retains the right to confront the person who found and extracted the information.

B. Authentication

To introduce information from a cell phone, or any other source, the proponent must show that it is authentic. The proponent must offer evidence "sufficient to support a finding that the matter in question is what its proponent claims." FED. R. EVID. 901(a); *see United States v. Salcido*, 506 F.3d 729, 733 (9th Cir. 2007) (data from defendant's computer was properly introduced under Rule 901(a) based on "chain of custody"); *United States v. Meienberg*, 263 F.3d 1177, 1181 (10th Cir. 2001) (district court correctly found that sufficient evidence existed under Rule 901(a) to admit computer printout of firearms sold through defendant's business). The proponent need not prove beyond all doubt that the evidence is authentic and has not been altered. *United States v. Gagliardi*, 506 F.3d 140, 151 (2d Cir. 2007). Instead, authentication requirements are "threshold preliminary standard[s] to test the reliability of the evidence, subject to later review by an opponent's cross-examination." *Lorraine v. Markel Am. Ins. Co.*, 241 F.R.D. 534, 544 (D. Md. 2007). Once evidence has met this low admissibility threshold, it is up to the fact finder to evaluate what weight to give the evidence. *United States v. Ladd*, 885 F.2d 954, 956 (1st Cir. 1989).

Federal Rule of Evidence 901(b) offers a non-exhaustive list of authentication methods. Several are useful in cases involving cell phone information. For example, Rule 901(b)(1) provides that evidence may be authenticated by a person with knowledge "that a matter is what it is claimed to be." *See United States v. Gagliardi*, 506 F.3d 140, 151 (2d Cir. 2007) (witness and undercover agent sufficiently authenticated emails and chat log exhibits by testifying that the exhibits were accurate records of communications they had had with the defendant); *United States v. Kassimu*, 2006 WL 1880335, at *1 (5th Cir. Jul. 7, 2006) (district court correctly found that computer records were authenticated based on the Postal Inspector's description of the procedure employed to generate the records).

Rule 901(b)(3) allows authentication of the item where the trier of fact or an expert compares it "with specimens which have been authenticated." *See United States v. Safavian*, 435 F. Supp. 2d 36, 40 (D.D.C. 2006) (emails that were not clearly identifiable on their own could be authenticated by comparison

to other emails that had been independently authenticated). Rule 901(b)(4) indicates that evidence may be authenticated based on distinctive characteristics such as "contents, substance, internal patterns, or other distinctive characteristics." *See United States v. Siddiqui*, 235 F.3d 1318, 1322-23 (11th Cir. 2000) (email was appropriately authenticated based entirely on circumstantial evidence, including presence of the defendant's work email address, information in the email that the defendant was familiar with, and use of the defendant's nickname in the email).

For cell phone evidence resulting from an automated process, such as cell tower information or location data in a photograph, prosecutors will be required to provide an evidentiary foundation under Rule 901(b)(9) by introducing "[e]vidence describing a process or system used to produce a result and showing that the process or system produces an accurate result." In addition to the obvious benefit of getting the records into evidence, a developed foundation will explain how the cell phone information was created and how the examiner found the data, thereby enabling the finder of fact to understand the soundness and relevance of the information. Once a minimum standard of trustworthiness is established, questions regarding the accuracy of records "resulting from . . . the operation of [an automated] program" affect only the weight of the evidence, not its admissibility. *United States v. Catabran*, 836 F.2d 453, 458 (9th Cir. 1988); *see also United States v. Tank*, 200 F.3d 627, 630 (9th Cir. 2000) (where defendant in a child pornography case deleted portions of his Internet chat logs from a third person's hard drive, deletions went to the weight of the evidence, not to its admissibility).

To demonstrate authenticity for process-generated records, the proponent is required to introduce evidence that describes a process or a system used to produce a result and to show that the process or system produces an accurate result. How much detail the proponent must provide depends on the complexity or familiarity of the information. The foundations for many categories of cell phone information will not require the proponent to cover each point noted in the fairly comprehensive checklist below. It is important to note that some parts of the checklist are relevant to information obtained from the phone itself while other areas relate to information obtained from a cellular provider or a third-party provider.

This checklist, along with the PIRL-Cell phones guide at http://dojnet.doj.gov/criminal/ccips/online/lab.htm, and the suggested questions for a computer forensic examiner found at http://dojnet.doj.gov/criminal/ccips/online/Evidence%20Issues/Computer%20Forensic%20Examiner%20Sample%20Questions%20&%20Cross%20Issues.wpd, will facilitate trial preparation discussions between prosecutors and cell phone examiners. The checklist is adapted from Timothy M. O'Shea, *Thinking Outside the Business Records Box: Evidentiary Foundations for Computer Records*, 81 WIS. LAW. No. 2 (2008):

1. The improbability that the information has been substantively altered, including:
    - The chain of custody for the evidence
    - How changes in the information are recorded and how this information shows that the relevant information has not been substantively changed (It is important to note that the forensic review of cell phones almost always triggers some explainable change to the information stored therein.)
    - Whether a verification hash shows that the relevant information was unchanged
    - How the information was created
    - Whether the information was forensically-obtained and, if so, what tools were used in the examination
    - The reliability of the forensic tools

2. The completeness of the record:

    - How the information was created and stored
    - Processing—what the cell phone, computer, or program was asked to do
    - Output—how the information was retrieved from the cell phone (or from a computer at the cellular or third-party service provider)

3. The reliability of the programs and equipment:

    - Whether the program and equipment were used routinely
    - Absence of prior problems
    - Ability of hardware or software to detect errors
    - Whether the equipment was regularly checked
    - Whether the program and equipment produce a testable result
    - Whether the output is routinely verified:
        - automatically as part of the program,
        - by a complementary system that would not work if errors occurred in the program or equipment producing the information, or
        - by other external controls

4. The examiner's training and experience with forensic tools.

The last entry on this list merits further discussion. It is important to understand the examiner's training, proficiency, and ability to appropriately document the forensic process. While no universally recognized certification for cell phone examiners exists, the prosecutor and examiner should explore the following:

- The examiner's current curriculum vitae documenting relevant training and certifications (Although cell phones require different tools and knowledge, a significant overlap exists between cell phones and computers. It follows, therefore, that computer forensic training, experience, and certifications are appropriately discussed, disclosed under FED. R. CRIM. P. 16(a)(1)(G), and explored before the jury.)
- Whether competency tests were administered during training and whether the examiner passed those tests (It is important to note that many forensic tool vendors offer a certification class—typically followed by an exam of some sort—that focuses only on the vendor's tool.)
- The number of examinations performed by the examiner and whether the examiner has previously testified regarding the results of forensic examinations
- Whether the examiner has provided training in forensics or has written about a relevant topic
- Whether the examiner follows a Standard Operating Procedure, agency prescribed or not, during examinations and, if so, whether the examiner followed the procedure(s) in the case at hand

- Whether the examiner takes periodic proficiency exams and, if so, whether the exam results are available
- Whether the examiner participates in technical, peer, or administrative forensic reviews

C. Presentation

As indicated in the PIRL-Cell Phones list, there are at least seventeen categories of information relating to cell phones. *See* http://dojnet.doj.gov/criminal/ccips/online/lab.htm. Information critical to a prosecution may be found within each category. For example, with regard to a photographic image stored in a cell phone, a prosecutor may be interested in knowing when the image was taken, where it was taken (if the background is identifiable or if GPS data is embedded in metadata), what camera or device was used to take the picture, to whom the image was sent, and of course, who or what is depicted. Further, there are many effective ways to present information to the jury. Some prosecutors present evidence electronically and some print the relevant information and introduce it in three-ring binders. In light of the many types of information and the ways to present it, this article ends with a few fairly-universal observations about technical computer and cell phone testimony.

IV. Conclusion

While judges and juries are becoming increasingly technically savvy, cell phone and computer forensics are not generally well understood. It is important to spend enough time with the examiner to understand the process that the examiner employed and how the relevant information that you will use at trial was created and stored. One must also work with the examiner to sort out the best way to communicate the information to the jury. One productive technique is to ask the examiner to explain the technical information as if he were sitting at a kitchen table and talking to his least technical aunts and uncles. With the same hypothetical aunts and uncles in mind, explore with the examiner possible metaphors to help the judge and jury understand the evidence. For example, "GPS coordinates are like markings along a trail" or "a file system is like a card in a(n) (old school) library card catalogue." While many paths are available to admit and persuasively present electronic evidence, the important thing about the exercise is to craft questions and answers that help the judge and jury to genuinely understand the information rather than attempting to impress (but mystify) the finder of fact with technical jargon.❖

ABOUT THE AUTHORS

❑**Timothy M. O'Shea** has been an Assistant United States Attorney for the Western District of Wisconsin since 1991, Senior Litigation Counsel since 2002, and his district's Computer Hacking and Intellectual Property prosecutor since the inception of the program. As a general crimes prosecutor, Mr. O'Shea currently chairs the PIRL working group, regularly lectures at the National Advocacy Center, and has contributed to three manuals published by the Office of Legal Education: FEDERAL GRAND JURY PRACTICE (2008); SEARCHING AND SEIZING COMPUTERS AND OBTAINING ELECTRONIC EVIDENCE IN CRIMINAL INVESTIGATIONS (2009), and FEDERAL CRIMINAL DISCOVERY (2011).✠

❑**James Darnell** is a 12-year veteran of the United States Secret Service, having served in protective and investigative assignments in Las Vegas, Nevada, Washington, D.C., and Tulsa, Oklahoma. Mr. Darnell holds the position of Criminal Investigator/Special Agent, currently assigned to the Computer Forensics/Research & Development Branch of the Criminal Investigation Division (CID), where he administers the Service's Cell Phone Forensic Facility at the University of Tulsa. In this capacity, he provides training, examinations, and research in the area of embedded device forensics and oversees the United States Secret Service cell phone forensic program. Mr. Darnell is the Chairman of the Scientific Working Group on Digital Evidence and periodically instructs at the National Computer Forensics Institute and the Federal Law Enforcement Training Center.✠

Effectively Using Electronic Evidence Before and at Trial

Mark L. Krotoski
National Computer Hacking and Intellectual Property (CHIP) Program Coordinator
Computer Crime and Intellectual Property Section

I. Introduction

Electronic evidence provides unique information that may not otherwise be available in tangible form or from other sources. Compare, for example, a print-out of an electronic version of a document with a hard copy printout of the same record. The hard copy will provide information only about the content and any other visible information, such as handwritten notations. The electronic version, on the other hand, will provide the same content information generated by a computer as well as more information, including metadata (but not the handwriting). The electronic version captures many details that may otherwise be unavailable. Illustratively, the metadata—often referred to as data about data—from the electronic version may indicate the name of the title and author, the date it was created and last saved, the date of the last printed version, changes that were made, and more. Other electronic evidence may reveal activity on the computer before and after the key electronic document was drafted or sent. In many regards, the metadata provide insight and detail not only about the contents but also about what was transpiring at and around the time that the document was created.

Electronic evidence is now commonplace in both civil and criminal cases. When the civil procedure rules established new rules concerning "electronically stored information" in 2006, the advisory committee notes advised that "new sources of electronic data are constantly being created, such as instant and text messaging. Given the constant change in this area, it is important for lawyers to keep current on evolving technologies." FED. R. CIV. P. 34 advisory committee's note (2006).

Electronic evidence has become increasingly essential to investigate, build, and solve many criminal cases, regardless of type. In one case, for example, metadata from a document created by the defendant and sent anonymously was one key to solving the "bind, torture, and kill" series of gruesome murders after many years of investigation. *See generally* Monica Davey, *Computer Disk Led to Arrest in Killings, Pastor Says*, N.Y. TIMES, Mar. 2, 2005, http://www.nytimes.com/2005/03/02/national/02btk.html (reporting that information on the computer disk in the defendant's final mailing was used "to trace it back to a computer at Christ Lutheran Church" that the defendant "had used . . . a few weeks earlier"). In other criminal cases, electronic evidence has changed the case focus by revealing the primary co-conspirators or other participants and a fuller scope of the criminal activity.

This article uses recent case lessons to suggest practical steps on how to use electronic evidence effectively and efficiently during an investigation and at trial. First, the article highlights the importance of learning more about what electronic records are created in order to identify and use any evidentiary leads from this data that may be relevant to the case. The details in these records can provide significant information for the investigation. Second, the unique role of electronic evidence to test theories in the case will be noted. Finally, a five-part plan is suggested to enhance the early identification and use of electronic evidence in a criminal case, consisting of (1) investigation, (2) corroboration, (3) report, (4) admissibility, and (5) presentation phases.

II. Discovering what kinds of electronic records are available and how these records may advance the case

Electronic evidence or records come in many different types. When starting work in criminal cases involving the use of electronic evidence, it is helpful to consider and apply a basic understanding of these records to identify which ones may be useful for the case. At its core, electronic evidence is simply an event memorialized by a computer. This evidence reflects prior decisions made by someone else to record certain events on computers and on computer networks. The question becomes, what events and details are being recorded and how can they help the case?

This basic question helps to frame the issue and identify what records are created (on a laptop computer or on a computer network) and what information may be useful. While similar companies may create similar business or other records, they will not necessarily create the same ones. The details in these records can make an important difference in a case.

An understanding about why and how particular records are created and what information is collected can provide some useful evidence and possibly new leads in the case. For example, the records may provide identifiers about the individual making the transaction (such as Internet Protocol address, customer account information, or transactional history). The company and owner of the computer records may have collected customer account information when the account was first opened. A particular credit card may be linked to the account. Other identifiers may include username, company userid, and a history of files uploaded or transactions (that may provide new leads). This information may shed light on who was behind the transaction or may connect with other evidence in the case. Timestamp information often yields useful information for creating a time line or showing the sequence of unfolding events.

In working with another company's computer records (such as an Internet Service Provider or Internet company), some initial questions may help to focus on relevant events in the case and determine if the company or hard drive memorializes those events:

- Does your company make records of a particular event (online account access, online financial payment, or any other activity relevant to the case)?
- Where on the computer/system/network is this event recorded?

Once relevant records have been found, more refined questions may include:

- Who creates the information in the record (the user or computer)?
- How or when is the record created? (In other words, what is the triggering event for the creation of the record?)
- In how many places can a copy of this record or event be found? What related or companion records are created?
- How are the details on the record created? What is their significance? For example, account information may include data that is provided and updated over time.
- What is the business purpose for the records? Why is the information collected?

For example, an Internet site that allows visitors to post images may record information about the uploaded image for business purposes. The records about the image (including unique identifiers, attributes, and other metadata) may be used to match information on the defendant's computer to the image.

If interstate commerce must be established as an element of the offense, it may be necessary to show that a particular Internet communication crossed state lines. One question for an Internet Service Provider may concern identifying the location of a particular server handling a key Internet transaction on a particular day and time. If the server is in the same state as the prosecuting district, other theories or transactions may be needed to show interstate commerce. If the Internet Service Provider can show that the server handling the account or transaction was in another state, then interstate commerce is readily established.

Consider a forensic example involving possible deletions of data in a seized laptop. While the original file may no longer be available, other records such as a link file (or shortcut to a local file) may show that the computer was used to access certain named files. If Microsoft Windows was used, a "System Restore" process can restore the computer files to an earlier point. The process may be useful to show what programs or files were on a particular computer before significant changes (such as deletions) occurred.

Each of these forensic examples is driven by the needs of the case. These records may not be necessary or relevant in every case. However, by focusing on the key events and the types of records that may be made concerning the event, significant evidentiary leads may be identified. Moreover, related records may be found in multiple places. Recent cases underscore the importance of learning more about the electronic records that are created (either on a computer network or a computer) in advancing the investigation.

III. Testing case theories

From a prosecutor's perspective, one benefit of electronic evidence is that it may be used to test theories in the case, including theories offered by the defense. If certain events are alleged to have occurred, they can be verified by checking for the types of records that would have been created by the particular events.

One useful example comes from the child pornography prosecution in *United States v. Ganoe*, 538 F.3d 1117 (9th Cir. 2008), *cert. denied*, 129 S.Ct. 2037 (2009). Defendant Ganoe was charged with receipt and possession of child pornography. An investigation determined that a file sharing program (LimeWire) was used to share child pornography. A search warrant was obtained to seize a computer and evidence connected to a particular Internet Protocol address assigned to the defendant's residence. During the search, the defendant admitted that he had "inadvertently downloaded child pornography" and that the " 'bad stuff' could be found in the 'z' folder." *Ganoe*, 538 F.3d at 1119. After charges were filed, a computer forensics expert testified at trial that he located "72 pictures and videos depicting child pornography in a subfolder entitled 'z,' located within the iTunes folder." *Id.* at 1121. During the defense case, the defendant's sister, her boyfriend, and another friend testified that "a man named Ray Rodriguez" had resided at the residence "but vanished after" learning about the seized computer. *Id.* at 1121-22. The boyfriend testified that he "had personally observed Rodriguez search[ing] for and download[ing] child pornography on to the computer." *Id.* Rodriguez could not be found. The defendant also provided an alibi during the periods of the downloading of the child pornography.

How could the computer forensics address this trial defense? During rebuttal, the government recalled the forensic examiner who testified about the computer user's activity before and after the child pornography was downloaded. He told the jury that based on his examination "whoever was using the computer at the time the child pornography was downloaded had also accessed Ganoe's PayPal account, used Ganoe's American Express card, logged onto his email account, and sent emails to people associated with Ganoe, suggesting that it must have been Ganoe himself." *Id.* at 1122. The computer forensics provided further information about the computer user's activity.

In response, the defense provided surrebuttal testimony from the boyfriend who "testified that a list of passwords and user names for various password-protected websites was kept next to the computer, suggesting that anyone using the computer could have accessed these sites." *Id.* The jury convicted the defendant on two receipt counts and one possession count, but acquitted him on one receipt count. The convictions were affirmed on appeal. *Id.* at 1128.

The *Ganoe* case highlights how computer forensics helped respond to the defense claim that some other user was responsible for the child pornography found on the seized computer. Without further review of the electronic evidence, the jury would have been unaware of the activity on the computer. The case also highlights the ongoing need to use computer forensics to respond to specific issues in the case and the role of electronic evidence to test and verify case theories.

This principle may be applied to other cases to test case theories. If the events had occurred as the defense suggested, what records would be created? While the defense theory may be possible, how probable is it as measured against the electronic evidence and non-electronic evidence? A time line of key case events may also be useful to address these challenges.

IV. Five key phases

Five key phases enhance the identification and use of electronic evidence during an investigation and, if necessary, at trial. The five phases that follow the seizure or acquisition of the electronic evidence are (1) investigation, (2) corroboration, (3) report, (4) admissibility, and (5) presentation. These phases are interrelated and build on one another.

A. Investigation phase

The investigation phase identifies key evidence to further the investigation and prove the case. At this stage, forensic challenges may include the necessity to act quickly (before the defendant or conspirators leave the jurisdiction or country); to examine voluminous data and/or the limited time to review the seized data; and to identify, preserve, and collect electronic evidence from multiple sources before the retention period for the data expires.

During the investigative phase, electronic evidence generally falls into two broad categories: (1) computers or devices containing electronic evidence (such as hard drives or cell phones); and (2) electronic records (such as emails, chat, Paypal records) provided by a company maintaining the records, usually through legal process. This distinction is significant because records on a computer hard drive may fill gaps or corroborate electronic records created and maintained by other companies or at other locations. For example, the company may have information about the payment for a transaction and the information may include the Internet Protocol address and other identifiers. Evidence of the transaction may be found on the hard drive.

Key steps during the investigative phase include (1) using early triage steps to focus on key events and transactions, (2) identifying leads from both the forensic examiner and the agent, (3) addressing user attribution issues, (4) filling gaps in the evidence, and (5) proving events abroad.

Using early triage steps to focus on key events and transactions: Many cases now confront the challenge of dealing with voluminous data. Triage refers to steps that are essential to effectively and efficiently identify key evidence within the scope of a search warrant and consistent with the needs of the case. Given the lower costs of purchasing a hard drive with one or more terabytes of data (one terabyte is equivalent to 1,024 gigabytes), it is not uncommon for a hard drive to contain hundreds of thousands of files. One terabyte may contain "1,000 copies of the Encyclopedia Britannica." MEGABYTES, GIGABYTES, TERABYTES . . . WHAT ARE THEY?, http://www.whatsabyte.com/. Consequently, it is not humanly possible

to view each file. While not a substitute for a complete forensic examination, triage steps can identify key transactions or new leads that may be critical for the early phase and direction of the case.

More common triage tools and approaches are becoming available. The following basic triage example may be helpful. If a particular image or file is important to the case, a hash of the item, commonly referred to as a "digital fingerprint," *see infra* Part IV.D., can be used to search the data for a match. If a match is confirmed on some but not all seized hard drives, the disparity can prioritize the order that the media will be examined in the case.

While several common forensic tools and techniques may be available, they must be tailored to the case at hand. The forensic examination should address the specific needs of the case, just as other investigative techniques are adapted to the particular case. The same forensic examination is not required in every case. Some cases may merely require identification of key evidence (such as images or emails) on electronic media. Other cases may require more information about the history of these documents and how and when they were placed on the computer. The metadata may be important in some cases but not others.

Initial three-way discussion: One important practice that has proven effective is to encourage an initial three-way discussion between the examiner, agent, and prosecutor. This conversation will focus on the key evidence in the case. The agent will be able to identify key investigative leads and avenues external to the computer media. The prosecutor can address proof and other legal issues in the case. With this background and understanding, the examiner can identify relevant records and techniques that may produce key evidence. This three-way conversation will serve to bring an early focus to the case issues. If key evidence is identified early, the defense may entertain a pre-indictment resolution. If key evidence reveals that the case is larger (in scope and participants) than initially anticipated, then new investigative leads can be pursued. This three-way discussion ensures that the forensic review addresses the particular needs of the case. Some questions to ask during this early discussion may include:

- What are the primary transactions or events in the case? What records may confirm those transactions or events?
- How many participants were involved? Are there any co-conspirators? What are the roles of each participant/co-conspirator?
- What key documents, transactions, or evidence, such as a particular file, image, or email, may be found?
- What planning and preparation evidence can be located?
- What role did the laptop serve in the case? Was the laptop used as an instrumentality to commit the offense or does it store data related to the offense?
- Are there any financial or monetary ties to the computer?
- What are the anticipated defenses and the government's responses?

Finally, as the case advances and new leads are identified, it may be productive to renew the three-way discussion. For example, a particular file or image that may not have appeared significant early in the case may refocus the forensic examination and investigative steps later on. The discussion can focus on these emerging matters.

Identifying and using leads from both the forensic examiner and the agent: For this aspect, there are two key issues: (1) How can forensics help or guide the investigation? (2) How can the investigation help or guide the forensics?

Recent cases also demonstrate the benefits of exchanging information and sharing new leads between the examiner and investigator as the case advances. Each serves a unique role in the case. They do not operate in isolation. The examiner may locate additional information that fills gaps or provides new leads that may aid the investigators and that otherwise might not have been found. Investigators can identify key areas for the examiner to focus on within the scope of the search warrant. For example, the examiner may identify new email accounts that may have been unknown to the investigators. With this information, the investigators can use appropriate legal process to obtain the evidence related to the new accounts or leads. Alternatively, the examiner may reveal that a key document was the product of several drafts over a period of time or had contributions from others. These forensic details may otherwise be beyond the reach of the investigators.

This exchange of information may also benefit the examiner as investigators suggest key transactions, time periods, witness statements, or external events that the examiner may be able to corroborate on the computer media. The mutual benefits from this two-way exchange of information are not a one-time event. As more leads and evidence are gathered, it may be necessary for the forensic examiner or agents to review the evidence anew within the scope of the search warrant. For example, it may be that information about a key report or document resides on the laptop hard drive among 500,000 or more files. The report by itself may not seem significant early in the investigation. However, if the investigators learn that the defendant was aware of the report or document, it may be necessary for the examiner to review the hard drive again for this new evidence.

Addressing user attribution issues: One recurring issue is proving the defendant was the user of the computer during the offense or responsible for the key transactions in the case. The investigative phase can help address this issue. Some questions to consider may include:

- What electronic evidence tends to confirm who the user or owner of the seized computer was during the key events in the case?
- What indicia suggests who the author was of an email or chat message (e.g., nickname or other identification or familiarity with unique facts)?
- Can metadata provide information about the author of a file?
- What evidence external to the computer or email message provides information about the author?
- Can a pattern of access to customer accounts before and after a key event shed light about the computer user, such as Internet browsing history or access to accounts controlled by a specific person?
- Can the recipient of a message or electronic communication identify the author?

In a number of cases, early focus on user attribution issues has confirmed ownership and authorship issues.

Filling in gaps in the evidence: Electronic evidence has proven useful to identify gaps in the evidence. For example, in a series of email communications, perhaps only a few in the series will be found. During the investigative phase, it helps to consider how many places the same or comparable evidence may be found. In filling in evidence gaps, some useful questions to consider may include:

- How are the defendants communicating?
- What electronic records are being created?
- What computers or devices are being used?

- How many places can that electronic evidence be found (e.g. sender's computer, recipient's computer, Internet service provider records)?
- What process is necessary to obtain this evidence?

If evidentiary gaps are identified, it also helps to consider the role of the electronic evidence in the transaction or communication.

Proving events abroad: In cases involving international activities, electronic evidence is important to establish events abroad. Information from a computer or email and related communications have been used to establish a time line of key events that may have occurred outside of the United States.

For example, in some recent economic espionage cases under 18 U.S.C. § 1831 (involving the misappropriation of a trade secret with an intent to benefit a foreign government or foreign instrumentality), the seizure of the defendant's laptop and emails was instrumental to show the preparation, planning, misappropriation, and use of trade secrets in other countries. Without this information, the same information would have been more challenging for law enforcement to obtain. With this information, new leads and requests can be pursued with law enforcement partners in other countries under the 24/7 High Tech Crime Network (about 55 member countries provide a law enforcement point of contact, 24 hours a day, 7 days a week, to preserve evidence in a foreign country) and the Mutual Legal Assistance Treaties.

B. Corroboration phase

A related and significant phase concerns the identification of corroboration between the electronic evidence and external events (or non-electronic evidence). While this phase is certainly related to the prior investigative phase, given its significance, it is highlighted as a distinct area of focus. It also applies to each of the other key phases in using electronic evidence. Apart from the investigation, it can also be a key area at trial in presenting the evidence to the jury and rebutting defense claims. Once key events are identified by investigators external to the electronic media, the question becomes, can related evidence be found on the electronic media? Correspondingly, can evidence discovered through a forensic examination be confirmed by related external events?

Corroboration based on traditional investigative techniques: It is rare that electronic evidence alone can help prove all of the elements of the offense. More commonly, traditional investigative techniques will be used in conjunction with the forensic examination to prove the case. These tried and tested traditional investigative techniques may include:

- Witness interviews
- Physical evidence seized at a residence or company pursuant to a search warrant
- Surveillance
- Undercover activities
- Use of a confidential informant or cooperating witness
- Financial or transactions records ("follow the money" approach)
- Communication records (such as phone records) to show the relationship of key parties
- Confessions (partial or complete)

Evidence obtained under these traditional investigative approaches may be corroborated by electronic evidence such as email or chat.

Corroborating other electronic evidence: Corroboration is not restricted to electronic evidence and external events. A key corroborative area may involve corroborating electronic evidence with other electronic evidence. For example, if a key document is located on the defendant's laptop, the statements or

representations in the document may be corroborated by other evidence found on the computer. If the document recounts planning and preparation steps in a conspiracy, those steps may be confirmed by other computer activity or records. Also, a key document may have been shown to have been distributed to others. This chain of electronic evidence can strengthen the investigation and case presentation.

Corroboration benefits: At least four key benefits may result from the corroboration phase. First, the corroboration of external events with evidence from the laptop computer (or other electronic media) helps confirm the role and trace the activity under investigation directly to the computer user. This tracing may assist in answering who the computer user is.

Second, the corroboration strengthens the weight of the evidence and increases the chances of proving the case beyond a reasonable doubt. Information from external events may provide a fuller understanding about the electronic evidence. For example, witnesses may be able to testify about non-electronic events that preceded or followed the electronic transaction. The electronic record may have details or information that assists the witnesses in recalling the events. In building and presenting a strong case at trial, it helps to show the corroboration between the electronic evidence and external evidence. The linkage may help prove the case to the jury beyond a reasonable doubt. The fact-finder is also aided in considering the weight of the evidence presented at trial.

Third, the corroboration often removes issues in the case. For example, if the defense seeks to challenge the integrity of the electronic evidence records, it becomes harder to do so when independent confirmation of the event external to the electronic media is established. In one computer intrusion trial, the defense suggested that integrity questions concerning the collection of electronic evidence were an issue until the evidence presented showed that the same events on a company network were independently corroborated. *See generally United States v. Shea*, 493 F.3d 1110 (9th Cir. 2007) (logic bomb prosecution).

Fourth, the corroboration may resolve or prevent appellate issues after a trial. For example, the corroborated evidence may help to address a challenge to the admission of any particular evidence by showing that error was harmless under FED. R. EVID. 103(a) or was not plain error if no objection was lodged under FED. R. EVID. 103(d). If a challenge is raised to specific evidence, the corroborated evidence may show that any error was harmless or did not rise to the level of plain error.

C. Report phase

After key forensic evidence has been identified during the investigation phase and key external and electronic evidence have been corroborated, the prosecutor will need to decide whether the information requires expert testimony. If so, pretrial expert disclosure of the opinions and bases of the opinion will be needed if requested by the defense. This obligation arises from FED. R. CRIM. P. 16(a)(1)(G) that provides:

> At the defendant's request, the government must give to the defendant a written summary of any testimony that the government intends to use under Rules 702, 703, or 705 of the Federal Rules of Evidence during its case-in-chief at trial. . . . The summary provided under this subparagraph must describe the witness's opinions, the bases and reasons for those opinions, and the witness's qualifications.

Id.

While not all testimony concerning the admission of electronic evidence requires expert testimony, a substantial portion may. The threshold focus is determining whether expert testimony is needed and therefore whether a Rule 16 expert's summary report must be provided. If the testimony is deemed to

involve expert conclusions, the defense may seek to exclude the testimony altogether based on the non-compliance with the expert disclosure requirements or may request other appropriate sanctions.

Evaluating lay and expert testimony: Case law confirms that it is not always clear what aspects of the expert examination may constitute expert testimony. *See generally United States v. Hilario-Hilario*, 529 F.3d 65, 72 (1st Cir. 2008) ("There is no bright-line rule to separate lay opinion from expert witness testimony; circuits, and indeed decisions within a circuit, are often in some tension."); *United States v. Ayala-Pizarro*, 407 F.3d 25, 28 (1st Cir. 2005) ("The line between expert testimony under Fed. R. Evid. 702 . . . and lay opinion under Fed. R. Evid. 701 . . . is not easy to draw.") (citation omitted). Some forensic evidence may be introduced as lay testimony without any expertise.

Lay opinion testimony must be "rationally based on the perception of the witness[,]" which includes "the familiar requirement of first-hand knowledge or observation." FED. R. EVID. 701 advisory committee's notes. Under Rule 702, if "scientific, technical, or other specialized knowledge will assist the trier of fact," a qualified expert may testify "in the form of an opinion or otherwise . . . ." *Id.* The determinative factor is not whether the witness is an expert or lay witness but whether the proffered testimony is expert or lay testimony. Rule 701 "does not distinguish between expert and lay witnesses, but rather between expert and lay testimony." Consequently, "it is possible for the same witness to provide both lay and expert testimony in a single case." FED. R. EVID. 701 advisory committee's notes.

A few case examples illustrate the differences between lay and expert testimony but also highlight the challenge for courts and attorneys in drawing a distinction. In a bank fraud case, an FBI financial analyst with 23 years of experience testified about a company's financial and business records. The analyst noted that the "expertise and the use of computer software" made review of the records "more efficient" in arriving at the conclusions. Was the government required to provide a pretrial expert summary report for this testimony? The Eleventh Circuit held that the testimony was proper lay testimony under Rule 701:

> Contrary to Appellants' contention, the government was not required to certify [FBI financial analyst] Odom as an expert witness and comply with [Federal] Rule [of Criminal Procedure] 16(a) with respect to Odom's testimony. To prepare for his testimony, Odom simply added and subtracted numbers from a long catalogue of MCC records, and then compared those numbers in a straightforward fashion. As Odom himself explained at trial, while his expertise and the use of computer software may have made him more efficient at reviewing MCC's records, his review itself was within the capacity of any reasonable lay person.

United States v. Hamaker, 455 F.3d 1316, 1331-32 (11th Cir. 2006) (footnote omitted). Alternatively, even if pretrial expert disclosure was required under FED. R. CRIM. P. 16, the defense effectively had notice about the analyst's testimony. *Id.* at 1332.

In a comparable vein, some federal investigative agencies rely on agents to use common forensic tools to identify evidence on seized computer media. The agent may not be a "forensic expert" in the classic sense. Many of the findings by the agent may be admitted through lay testimony.

Consider a related scenario. Can lay testimony be used to present forensic evidence by "running commercially-available software, obtaining results, and reciting them[?]" *United States v. Ganier*, 468 F.3d 920, 925 (6th Cir. 2006). In *Ganier*, forensic software was used to generate reports "display[ing] a heading, a string of words and symbols, date and time, and a list of words" based on "three different types of searches performed with particular search terms at particular times." *Id.* at 926. On the eve of trial, the defense filed a motion to exclude this testimony because it did not receive pretrial disclosure of the expert testimony. The trial court granted the motion in limine, excluding the expert testimony for non-compliance

with FED. R. CRIM. P. 16(a)(1)(G). The government appealed the exclusion of evidence. The Sixth Circuit agreed that expert testimony was implicated:

> The average layperson today may be able to interpret the outputs of popular software programs as easily as he or she interprets everyday vernacular, but the interpretation [the witness] needed to apply to make sense of the software reports is more similar to the specialized knowledge police officers use to interpret slang and code words used by drug dealers . . . [and the] knowledge and familiarity with computers and the particular forensic software [was] well beyond that of the average layperson.

Id. The fact that the government failed to provide pretrial notice of this expert testimony did not mandate exclusion of the evidence, particularly where no bad faith was shown by the government. The case was remanded for further findings and determination on the appropriate remedy. *Id.* at 927-28.

While some may question the analysis in the *Ganier* case, the opinion does serve to highlight the challenge in distinguishing between lay testimony and expert testimony. These cases essentially teach that a continuum between lay and expert testimony exists. Some matters may clearly be on the lay testimony side of the continuum, such as the use of computer software to find records or basic review functions. On the expertise side, more advanced knowledge and training may be required to analyze the data for recovering deleted files, understanding the imaging process, and determining the operation of malware or the use of codes and commands.

Given these cases and the difficulty in discerning lay and expert testimony on some forensic issues, what recommendations can be made? If in doubt, a Rule 16 expert summary may be provided out of an abundance of caution. The disclosure may state that while the testimony of witness A is admissible independent of expert Rule 702, in the event the trial court concludes that Rule 702 applies, the following summary provides the opinions and bases in support of those opinions.

The expert report: One question concerns who should prepare the Rule 16(a)(1)(G) expert summary report. Some prosecutors prefer to prepare the summary after meeting with the forensic examiner. One benefit of this approach is that the prosecutor will carefully consider, in advance, exactly how and why the electronic evidence may be admitted at trial. If the prosecutor drafts the summary report, the examiner must be comfortable with the opinions and bases included in the summary disclosure.

It is more common, however, for the expert to author the Rule 16(a)(1)(G) report. The tradeoff is that forensic examiners may not be accustomed to preparing an effective report for trial. This distinction is important. Review of some recent forensic reports shows that they were not "trial ready." This review highlights some recurring problems. Under the rules, the report is a trial document, not a technical or academic paper.

Determining whether the report is "trial ready" is also an important aspect of the case. Generally, forensic examiners have received some training in report writing. However, not many examiners have had their opinions tested at trial or it may have been years since the examiner's last trial testimony. The experience in preparing the expert summary for trial is often limited. An effective report should reflect discussions and consultation with the prosecutor about case presentation issues. If the report fails to summarize the expert "testimony that the government intends to use . . . during its case-in-chief at trial," as required under Rule 16(a)(1)(G), then the forensic testimony may be subject to exclusion or other sanctions.

Recurring concerns: Two primary issues recur in expert reports authored by forensic examiners. First, the report may contain technical representations that are too difficult to follow or comprehend. The role of the expert at trial is not to impress the jury with technical expertise or specialized knowledge but to assist the fact-finder in understanding and deciding the contested facts. Rule 702 provides that an expert

witness may be permitted to testify regarding "scientific, technical, or other specialized knowledge" if such knowledge "*will assist the trier of fact* to understand the evidence or to determine a fact in issue . . . ." FED. R. EVID. 702 (emphasis added); *see also Daubert v. Merrell Dow Pharm., Inc.*, 509 U.S. 579, 592 (1993) ("[T]he trial judge must determine at the outset, pursuant to Rule 104(a), whether the expert is proposing to testify to (1) scientific knowledge that (2) will assist the trier of fact to understand or determine a fact in issue.") (footnotes omitted). If the jury cannot follow and understand the expert, then the expert will have failed in his primary objective to assist the jury in understanding the facts of the case. The expert's report should thus be written with the trial and jury comprehension objectives in mind.

A second recurring challenge is that the report may provide an unfocused presentation. Under FED. R. CRIM. P. 16(a)(1)(G), the summary report is a trial document summarizing expert testimony that the government will offer during its case-in-chief. Therefore, the report should clearly and succinctly summarize the evidence that the government intends to offer in its case-in-chief and present a focused summary of the primary conclusions and support for those conclusions.

Practice tips: In order to address these two primary recurring issues, some practical suggestions are offered. An informal discussion with the examiner about the key forensic conclusions and the bases supporting those conclusions is encouraged to focus on the central areas to present to the jury. This discussion may require a couple of meetings. For example, the examiner may be asked the following questions: What is your conclusion concerning a key aspect of the case, such as the location of key documents or images, the metadata on a particular document, or finding deleted fragments? What specific bases support that conclusion? How many bases support that conclusion? How does the conclusion square with anticipated cross-examination or the theory of the defense? Each primary conclusion can be reviewed and probed. This informal dialogue can be accompanied by simulated cross-examination. This oral preparation process often helps refine and focus the conclusions and the bases in support of those conclusions in the final written report. In addition, more bases may be identified during this exercise that will help reinforce the weight of the expert testimony.

Another important tool is the use of a forensic time line that highlights key case events identified during the forensic examination. The time line can be helpful for the examiner in drafting the report. It may also aid the jury in following the key events. The time line can also be used to corroborate other case evidence, both electronic and external.

D. Admissibility phase

Thus far, the investigation phase led to the identification of key electronic evidence, steps have been made to corroborate electronic evidence with external events, and a useful pretrial expert report under FED. R. CRIM. P. 16 has been completed. The fourth phase involves consideration of the admissibility issues concerning the electronic evidence. This phase will typically address hearsay, authentication, and duplicate issues.

Hearsay: In considering hearsay questions, the following questions may be asked:

- Who made the statement?
- Was the statement machine-generated?
- Is there a non-hearsay purpose to admit the statement or record?
- Do party admission rules (FED. R. EVID. 801(d)) apply?
- Do other hearsay exceptions apply (such as co-conspirator, business, and public records)?

Computer-generated information: Many key records that are generated by a computer will not present any hearsay issues. Hearsay is defined as "a statement, other than one made by the declarant while

testifying at the trial or hearing, offered in evidence to prove the truth of the matter asserted." FED. R. EVID. 801(c). A machine does not make a "statement" within the meaning of the rule.

It is important to distinguish between computer-generated records and computer-stored records. One useful case addressing this issue arose in the Tenth Circuit in *United States v. Hamilton*, 413 F.3d 1138 (10th Cir. 2005). The court in that case held that "header" information (including the screen name, subject of the posting, the date that the images were posted, and the individual's IP address) was not hearsay. There was no "person" making a statement. *Id.* at 1142-43.

Surprisingly, not many cases address this issue, perhaps because the conclusion is readily apparent. Some related cases add further support to the notion that machine-generated output does not create a statement for purposes of the hearsay rules. *See also United States v. Washington*, 498 F.3d 225, 231 (4th Cir. 2007) (machine-generated data used in a DUI case to determine whether a blood sample contained drugs or alcohol were not statements of the lab technicians and were not hearsay statements because they were not made by persons but rather by machines analyzing the sample; no Confrontation Clause issues), *cert. denied*, 129 S.Ct. 2856 (2009); *United States v. Khorozian*, 333 F.3d 498, 506 (3d Cir. 2003) (information automatically generated by fax machine is not hearsay because "nothing 'said' by a machine . . . is hearsay").

For some electronic evidence, a portion may include non-hearsay computer-generated information and other portions may include potential hearsay statements. For example, an email may include a statement typed by the user but transmission information (for example, the date and time that the message was sent) will be computer-generated.

Admissibility of the defendant's and participants' statements: The statements of the defendant contained in electronic evidence may be admitted as statements against a party-opponent. Under FED. R. EVID. 801(d), "[a] statement is not hearsay if . . . [t]he statement is offered against a party and is (A) the party's own statement, in either an individual or a representative capacity . . . ."

A number of cases recognized the application of this rule with regard to electronic evidence. *See, e.g., United States v. Burt*, 495 F.3d 733, 738 (7th Cir. 2007) (admitting portions of an online chat communication that represented defendant's writings as admissions by a party opponent under FED. R. EVID. 801(d)(2)); *United States v. Siddiqui*, 235 F.3d 1318, 1323 (11th Cir. 2000) (noting that the emails "sent by Siddiqui constitute admissions of a party pursuant to FED. R. EVID. 801(d)(2)(A)"); *United States v. Safavian*, 435 F. Supp. 2d 36, 43 (D.D.C. 2006) ("The [email] statements attributed directly to Mr. Safavian come in as admissions by a party opponent under Rule 801(d)(2)(A) of the Federal Rules of Evidence."); *In re Homestore.com, Inc. Sec. Litig.*, 347 F. Supp. 2d 769, 781 (C.D. Cal. 2004) (noting in a civil securities action, emails "written by a party are . . . admissible as non-hearsay under FED. R. EVID. 801(d)(2)"); *see also Sea-Land Serv., Inc. v. Lozen Int'l., LLC*, 285 F.3d 808, 821 (9th Cir. 2002) (company email copied and forwarded to another employee " 'manifested an adoption or belief in [the] truth' of the information contained in the original e-mail" admitted under Rule 801(d)(2)(B)).

The statements of other participants to the conversation may be admitted as non-hearsay to provide context to the communication. *See, e.g., Burt*, 495 F.3d at 738-39 (third party portion of chat was admissible as non-hearsay to provide context to the conversation); *United States v. Dupre*, 462 F.3d 131, 136-37 (2d Cir. 2006) (emails from investors demanding information about defendant's fraudulent scheme were not hearsay when offered to provide the context for the defendant's message sent in response and to rebut defendant's argument that she did not know the scheme was fraudulent; no Confrontation Clause issues arose because the statements were offered for a non-hearsay purpose).

Defendant's exculpatory statements: The defendant's own exculpatory statements remain another important point for consideration. The defendant may seek to admit some of his "exculpatory"

statements without testifying. Under the Federal Rules of Evidence, a defendant's statement is admissible only if offered against him; a defendant may not elicit his own prior statements. FED. R. EVID. 801(d)(2)(A); *see also United States v. Palow*, 777 F.2d 52, 56 (1st Cir. 1985) ("The requirement of Rule 801(d)(2)(A) that an admission be offered against a party is designed to exclude the introduction of self-serving statements by the party making them.").

Two useful cases have addressed this issue. *See United States v. McDaniel*, 398 F.3d 540, 544 (6th Cir. 2005); *United States v. Ortega*, 203 F.3d 675, 682 (9th Cir. 2000). In *McDaniel*, the Sixth Circuit noted:

> Turning to the testimony at issue in this case, it is clear that the district court correctly prohibited [defendant] McDaniel's counsel from eliciting testimony from Postal Inspector Locke regarding certain statements made by McDaniel. Whereas Rule 801(d)(2) authorized the Government to question Postal Inspector Locke on direct examination regarding statements made by McDaniel because of McDaniel's status as a party-opponent, any testimony by Postal Inspector Locke on cross-examination by McDaniel's counsel regarding additional statements made by McDaniel that had not already been introduced on direct examination would have constituted inadmissible hearsay that would have effectively allowed McDaniel to testify without being under oath, without cross-examination, and without direct scrutiny by the jury.

McDaniel, 398 F.3d at 545-46.

Of course the defendant is protected by the Fifth Amendment from being compelled to testify at trial. The *McDaniel* court cited with approval to *Ortega*, a case that provides a useful discussion of the reasons why the defendant's exclupatory statements are not admissible by the defense. *Ortega* involved drug and firearms charges. The Ninth Circuit held that the trial court correctly precluded the defendant from "eliciting his own exculpatory statements, which were made within a broader, inculpatory narrative." *Ortega*, 203 F.3d at 681. In the excluded oral statements, the defendant claimed that the guns and drugs found in his residence belonged to someone else. On appeal, the defendant argued that exclusion of the statements violated the rule of completeness, the Confrontation Clause, FED. R. EVID. 801(d)(1) (exception for recent fabrication), and FED. R. EVID. 807 (residual exception). In affirming the exclusion of the defendant's "non-self-inculpatory statements," the court explained:

> First, Ortega's non-self-inculpatory statements are inadmissible even if they were made contemporaneously with other self-inculpatory statements. The self-inculpatory statements, when offered by the government, are admissions by a party-opponent and are therefore not hearsay . . . but the non-self-inculpatory statements are inadmissible hearsay. . . . Second, the rule of completeness applies only to written and recorded statements. . . . Even if the rule of completeness did apply, exclusion of Ortega's exculpatory statements was proper because these statements would still have constituted inadmissible hearsay.

Id. at 682 (citations omitted); *see also United States v. Collicott*, 92 F.3d 973, 983 (9th Cir. 1996) (The rule of completeness under "Rule 106 does not compel admission of otherwise inadmissible hearsay evidence[.]") (citation omitted); *United States v. Dorrell*, 758 F.2d 427, 434-35 (9th Cir. 1985) (no violation of the rule of completeness where edited statement does not distort meaning of passage).

This precedent should assist in responding to efforts to admit the defendant's exculpatory statements without the defendant taking the stand and being subject to cross-examination.

Other hearsay exceptions: Other hearsay exceptions may be considered to admit statements contained in electronic evidence. Some examples include business and public records and co-conspirator statements, noted below, among others.

Business records: Computer business records provide a good example of this type of exception. The hearsay business records exception may apply to admit useful electronic records. One court noted that under FED. R. EVID. 803(6) "it is immaterial that the business record is maintained in a computer rather than in company books." *United States v. Catabran*, 836 F.2d 453, 457 (9th Cir. 1988). Another court explained that "computer data compilations are admissible as business records . . . if a proper foundation as to the reliability of the records is established." *United States v. Briscoe*, 896 F.2d 1476, 1494 (7th Cir. 1990); *see also Potamkin Cadillac Corp. v. B.R.I. Coverage Corp.*, 38 F.3d 627, 632 (2d Cir. 1994) ("A business record may include data stored electronically on computers and later printed out for presentation in court, so long as the 'original computer data compilation was prepared pursuant to a business duty in accordance with regular business practice.' ") (citation and internal quotations omitted).

The business records rule expressly applies to a "memorandum, report, record, or data compilation, in any form . . . ." FED. R. EVID. 803(6). The term "data compilation" is "used as broadly descriptive of any means of storing information other than the conventional words and figures in written or documentary form. It includes, but is by no means limited to, electronic computer storage." FED. R. EVID. 803(6) advisory committee notes; *see also Rosenberg v. Collins*, 624 F.2d 659, 665 (5th Cir. 1980) (admitting computer business records involving commodity trading activity and explaining that "[u]nder Rule 803(6), computer data compilations may be business records themselves, and should be treated as any other record of regularly conducted activity"). Computer business records can be computer-generated and/or stored on a computer.

Business records are admissible as a hearsay exception because they are considered to be reliable. *See, e.g.*, *Timberlake Constr. Co. v. U.S. Fidelity & Guar. Co.*, 71 F.3d 335, 341 (10th Cir. 1995) ("The rationale behind the business records exception is that such documents have a high degree of reliability because businesses have incentives to keep accurate records."); *United States v. Blackburn*, 992 F.2d 666, 670 (7th Cir. 1993) ("First, businesses depend on such records to conduct their own affairs; accordingly, the employees who generate them have a strong motive to be accurate and none to be deceitful. Second, routine and habitual patterns of creation lend reliability to business records.").

Many businesses use computers to create and maintain records that are admissible as business records. *See, e.g.*, *United States v. Salgado*, 250 F.3d 438, 452 (6th Cir. 2001) (telephone toll records); *Dyno Constr. Co. v. McWane, Inc.*, 198 F.3d 567, 576 (6th Cir. 1999) (Federal Express delivery records); *United States v. Cestnik*, 36 F.3d 904, 909-10 (10th Cir. 1994) (money transfer orders); *United States v. Loney*, 959 F.2d 1332, 1341-42 (5th Cir. 1992) (admitting frequent flier airline miles under FED. R. EVID. 803(6) and 1006).

Public records: Computer public records are another example of a hearsay exception that may be used to admit statements contained in electronic evidence. FED. R. EVID. 803(8) allows public records to be admitted as an exception to the rule excluding hearsay. Based on public duties in creating the records, public records are "unusually trustworthy sources of evidence." *Chesapeake & Del. Canal Co. v. United States*, 250 U.S. 123, 128-29 (1919); *see also United States v. Quezada*, 754 F.2d 1190, 1193 (5th Cir. 1985) ("Two principal reasons underlie this exception to the general rule excluding hearsay: the presumed trustworthiness of public documents prepared in the discharge of official functions, and the necessity of using such documents, due to the likelihood that a public official would have no independent memory of a particular action or entry where his duties require the constant repetition of routine tasks.") (footnote omitted).

Computer public records can also be computer-generated and/or stored on a computer. Many public records in the form of computer records have been admitted under FED. R. EVID. 803(8). *See, e.g.*, *United States v. Lopez-Moreno*, 420 F.3d 420, 437 (5th Cir. 2005) (Immigration agency's "computer records of the passengers' deportations are the type of public records that are admissible under Rule

803(8), and they are not the sort of investigative reports (i.e., police reports) that would be excluded under Rule 803(8)(B).") (citations omitted); *Malkin v. United States*, 243 F.3d 120, 123 (2d Cir. 2001) (where records in IRS computer files were admissible under Rule 803(8) after original IRS consent form extending limitations period was lost or destroyed); *Hughes v. United States*, 953 F.2d 531, 540 (9th Cir. 1992) (admitting computer-generated IRS Certificates of Assessments and Payments (Form 4340)).

Co-conspirator exception: Co-conspirator statements constitute another example of hearsay exceptions. These statements are admissible under FED. R. EVID. 801(d)(2)(E) against a party as non-hearsay. In appropriate circumstances, computer records have been admitted under this hearsay exception. For example, in *United States v. Moran*, 493 F.3d 1002, 1010-11 (9th Cir. 2007) (per curiam), a case involving a tax and fraud trial, Quickbooks financial records that were recovered from a co-defendant's computer were admissible as records in furtherance of conspiracy under Rule 801(d)(2)(E). The records were used to keep track of complex financial transactions that furthered the conspiracy and served to keep the co-conspirators abreast of the ongoing conspiracy activities.

Authentication issues: A second evidence issue concerning electronic evidence involves authentication. The foundational "requirement of authentication or identification as a condition precedent to admissibility is satisfied by evidence sufficient to support a finding that the matter in question is what its proponent claims." FED. R. EVID. 901(a). As Seventh Circuit Judge Richard Posner summarized, "Evidence that is not oral testimony must be shown to be what it purports to be rather than a forgery or other fabrication or an innocent misidentification. But there are no rigid rules, such as chain of custody, for authentication; all that is required is adequate evidence of genuineness." *United States v. Dawson*, 425 F.3d 389, 392-93 (7th Cir. 2005).

Most courts have recognized that the burden to authenticate is not a high one. *United States v. Gagliardi*, 506 F.3d 140, 151 (2d Cir. 2007) ("The bar for authentication of evidence is not particularly high.") (citation omitted). Once an exhibit is authenticated, the jury decides its genuineness and how much weight to give it. *McQueeney v. Wilmington Trust Co.*, 779 F.2d 916, 930 (3d Cir. 1985) (Once the prima facie standard is met, the opposing party may "argue that the documents are not genuine, or that they are somehow not worthy of great weight in the jury's deliberations."); *United States v. Caldwell*, 776 F.2d 989, 1002 (11th Cir. 1985) ("Once that prima facie showing has been made, the evidence should be admitted, although it remains for the trier of fact to appraise whether the proffered evidence is in fact what it purports to be.").

The failure to authenticate the electronic evidence can result in exclusion with fatal results. *See, e.g.*, *United States v. Baker*, 538 F.3d 324, 332-33 (5th Cir. 2008) (reversing distribution count based on plain error in admitting image printouts and report where "[n]o other witness or document in evidence vouches for the source, accuracy, or circumstances surrounding preparation of" the exhibits); *United States v. Jackson*, 208 F.3d 633, 637 (7th Cir. 2000) (Web posting excluded due to lack of authentication where defendant, a skilled computer user, failed to show that the postings were made by the groups allegedly responsible for them and not by him); *United States v. Jackson*, 488 F. Supp. 2d 866, 871 (D. Neb. 2007) ("chat" conversations excluded as not authenticated and not an accurate original or duplicate where an undercover agent cut-and-pasted without preserving the original).

Witness with knowledge: A common form of authenticating electronic evidence—used often for authenticating physical, non-electronic evidence—is the use of a witness with knowledge of the event or transaction. For example, for chat room log printouts, a witness can explain "how he created the logs" and that they "appeared to be an accurate representation of the chat room conversations . . . ." *United States v. Tank*, 200 F.3d 627, 630 (9th Cir. 2000). In *Tank*, the government made a prima facie showing of authenticity concerning chat room log printouts. A witness "explained how he created the logs with his computer and stated that the printouts, which did not contain the deleted material, appeared to be an

accurate representation of the chat room conversations among members of the Orchid Club." Another case, *United States v. Barlow*, 568 F.3d 215, 220 (5th Cir. 2009), also involved this form of authentication. In that case, online chats between the defendant and a person posing as a minor were authenticated by the witness's testimony that they were a full and fair reproduction of their year-long online "relationship." The witness "as the other participant in the year-long 'relationship,' had direct knowledge of the chats" and "could sufficiently authenticate the chat log presented at trial . . . ." In a similar manner, an undercover agent can testify about his participation in the communications. For example, in *United States v. Simpson*, 152 F.3d 1241, 1249-50 (10th Cir. 1998), an undercover FBI agent communicated with the defendant in a chat room devoted to child pornography. The agent testified about his Internet chat conversation with the defendant, an individual identified as "Stavron," who also gave the agent his name, his street address, and his email address.

Case agent based on investigation: A case agent may be able to authenticate electronic records obtained during the investigation, including those from computer media. The defendant in *United States v. Whitaker*, 127 F.3d 595 (7th Cir. 1997), was convicted of conspiring to distribute marijuana. A computer seized from his residence contained computer records of drug transactions and the drug business. The Seventh Circuit rejected the argument that the government was required to supply a witness with personal knowledge of the computer system and concluded that the computer printouts were sufficiently authenticated. The court held that the agent's testimony authenticated the computer printouts under Rule 901(a) where the computer was seized during the execution of a warrant, the agent was present when the computer records "were retrieved from the computer using the Microsoft Money program," and the agent "testified concerning his personal knowledge and his personal participation in obtaining the printouts." *Id.* at 601. The court in *United States v. Salcido*, 506 F.3d 729 (9th Cir. 2007) (per curiam), reviewed the conviction of a defendant who was prosecuted for the possession and receipt or distribution of material involving the sexual exploitation of minors. The court held that "the government properly authenticated the videos and images under Rule 901 by presenting detailed evidence as to the chain of custody, specifically how the images were retrieved from the defendant's computers." *Id.* at 733.

Unique or distinctive characteristics: Distinctive characteristics have also been used to authenticate electronic evidence under FED. R. EVID. 901(b)(4). Rule 901(b)(4) provides that distinctive characteristics may include "[a]ppearance, contents, substance, internal patterns, or other distinctive characteristics, taken in conjunction with circumstances." Courts have admitted email and chat communications that were authenticated by their distinctive characteristics. In *United States v. Siddiqui*, 235 F.3d 1318 (11th Cir. 2000), an email was authenticated by its content and context. The email included the email address and an automatic reply to sender. The messages themselves indicated knowledge of matter and used nicknames. Moreover, foreign deposition testimony concerning phone conversations after email messages were transmitted further authenticated the email. In *United States v. Safavian*, 435 F. Supp. 2d 36 (D.D.C. 2006), emails between defendant government official and a lobbyist were authenticated by distinctive characteristics. The characteristics included the email addresses that bore the sender's and recipient's names, the contents, and "the name of the sender or recipient in the bodies of the e-mail, in the signature blocks at the end of the e-mail, in the 'To:' and 'From:' headings, and by signature of the sender." *Id.* at 40.

Using hash values: Hash values are frequently used to authenticate electronic evidence from a hard drive that is examined to a particular file or document. Hash values are uniformly accepted as a "digital fingerprint." *See, e.g.*, *United States v. Finley*, 612 F.3d 998, 1000 (8th Cir. 2010) (noting Secure Hash Algorithm (SHA) "values are, in essence, unique digital fingerprints or signatures"); *United States v. Richardson*, 607 F.3d 357, 363 (4th Cir. 2010) (referring to a "hash value" as a digital fingerprint); *United States v. Henderson*, 595 F.3d 1198, 1199 (10th Cir. 2010) (same). A "hash value" or hash

algorithm provides another accepted method to authenticate an electronic document by distinctive means. The following excerpt explains what a hash value is:

> A unique numerical identifier that can be assigned to a file, a group of files, or a portion of a file, based on a standard mathematical algorithm applied to the characteristics of the data set. The most commonly used algorithms, known as MD5 and SHA, will generate numerical values so distinctive that the chance that any two data sets will have the same hash value, no matter how similar they appear, is less than one in one billion. "Hashing" is used to guarantee the authenticity of an original data set and can be used as a digital equivalent of the Bates stamp used in paper document production.

FED. JUDICIAL CTR., MANAGING DISCOVERY OF ELECTRONIC INFORMATION: A POCKET GUIDE FOR JUDGES, FEDERAL JUDICIAL CENTER, at 24 (2007) (quoted in *Lorraine v. Markel Am. Ins. Co.*, 241 F.R.D. 534, 546-47 (D. Md. 2007)).

Hash values are becoming commonly used to authenticate electronic evidence in court. *See, e.g.*, *Lorraine*, 241 F.R.D. at 546-47 ("Hash values can be inserted into original electronic documents when they are created to provide them with distinctive characteristics that will permit their authentication under Rule 901(b)(4)."); *Williams v. Sprint/United Mgmt. Co.*, 230 F.R.D. 640, 655 (D. Kan. 2005) ("This [hash value] method allows a large amount of data to be self-authenticating with a rather small hash mark, efficiently assuring that the original image has not been manipulated."); *see also United States v. Miknevich*, 638 F.3d 178, 181 (3d Cir. 2011) ("A SHA1 (or SHA–1) value is a mathematical algorithm that stands for Secured Hash Algorithim used to compute a condensed representation of a message or data file. Thus it can act like a fingerprint.").

Significantly, hash values are reproducible and can be verified. If one minor change is made, the hash value would result in a completely different number. Consider an example. The table below shows the hash value under two common versions for the same electronic text of the Declaration of Independence. Rows 1 and 2 show the hash value for the Declaration of Independence using two common hash value forms, known as MD5 and SHA-1, a longer alpha-numeric number. Rows 3 and 4 show the hash value result after one period was added to the text of the Declaration of Independence. Thus, Row 1 and Row 3 are the same text with Row 3 representing the text with the addition of one dot or period. As shown, a completely new and different hash value results from this minor change.

Declaration of Independence Text			
Row	*Text*	*Hash Value Form*	*Alpha-Numeric Hash Value*
1	Text	MD5	9b410f7b04070020949dca04b1323777
2	Text	SHA-1	fe3ff81814de9b201af9b7eccd3e9fa71d7a47c1
3	Text + Dot	MD5	64a31cf43f9e0fe17a1ed7f8d8e8f085
4	Text + Dot	SHA-1	dbec59860472bd08c3fda88934b27c3e86501bbc

In this way, hash values can be used to verify that one data set (for example, a hard drive, file, document, email, image, or other electronic communication) is the same as the data set to which it was compared. The same alpha-numeric hash value (or digital fingerprint) confirms that two data sets are the same and the evidence has not been altered or corrupted.

If different hash values are produced, then an issue is raised about an alteration to the data set. The probability of a random collision (two inputs with the same output) is 1 in 1,208,925,819,614,

629,174,706,176. The chances of winning the lottery multiple times in a row are more likely than the chances that two hash values match, a likelihood that readily satisfies a prima facie or comparable showing needed to authenticate a record. For this reason, the hash value may be useful to authenticate electronic evidence.

Computer-generated records: Rule 901(b)(9) applies to "[e]vidence describing a process or system used to produce a result . . . ." Computer records have been authenticated under this rule. In one case involving an insurance dispute brought by an insured and the primary insurer against an excess insurer, computer-generated summaries reflecting the insurance company's indemnity payments and loss adjustment expense payments for the insurance claims were admissible as a business record and authenticated under this rule. *U-Haul Int'l, Inc. v. Lumbermens Mut. Cas. Co.*, 576 F.3d 1040 (9th Cir. 2009). The claims manager, who "was familiar with the recordkeeping practices of the company, testified regarding the computer system used to compile and search the insurance claim records, and testified regarding the process of querying the computer system to create the summaries admitted at trial." *Id.* at 1045. The court held that it was not necessary for the computer programmer to testify to authenticate the computer-generated records as long as one with knowledge of the record system testified.

Comparisons: Another manner of authentication recognized in the rules is by comparison. *See* FED. R. EVID. 901(b)(3) ("Comparison by the trier of fact or by expert witnesses with specimens which have been authenticated."). In appropriate cases, this method has been used to authenticate emails. *See, e.g.*, *United States v. Safavian*, 435 F. Supp. 2d 36, 40-41 (D.D.C. 2006) (emails between defendant government official and lobbyist were authenticated by comparing email addresses, the use of the defendant's name, and his business).

Duplicates: A third evidence issue for electronic evidence involves the use of duplicates. The rules of evidence allow duplicates to be admitted as originals unless questions of genuineness or fairness arise. Specifically, FED. R. EVID. 1001(3) provides that an original is the writing or recording itself, a negative or print of a photograph or, "[i]f data are stored in a computer or similar device, any printout or other output readable by sight, shown to reflect the data accurately . . . ."

Under FED. R. EVID. 1001(4), a "duplicate" is "a counterpart produced by the same impression as the original, or from the same matrix, or by means of photography, including enlargements and miniatures, or by mechanical or electronic re-recording, or by chemical reproduction, or by other equivalent techniques which accurately reproduces the original." A duplicate is admissible to the same extent as an original unless a genuine question is raised as to the authenticity of the original or it would be unfair to admit the duplicate instead of the original under the circumstances. FED. R. EVID. 1003.

E. Presentation phase

At this point, key evidence has been identified during an effective investigation, corroborated with other electronic and external evidence, summarized in a forensics expert's report that is "trial ready," and is well-supported by admissibility theories under the rules of evidence. The fifth and final presentation phase focuses on whether the jury, as finders of fact, can follow and understand the electronic evidence.

Some electronic evidence can be highly technical. The output of a forensic examination can be important to prove issues in the case but may be difficult to present and comprehend at trial. While the technical forensic evidence discovered during an examination may be useful to obtain a plea agreement or as a reference in the factual basis for a plea agreement, a jury may not be able to follow this evidence. Because juries generally retain information better when obtained through visual senses, graphics can be an important tool in presenting the electronic evidence.

A fair amount of brainstorming may be involved in considering and developing appropriate graphics among trial team members. Many prosecuting offices have a litigation support specialist who can suggest fresh ideas and options in assisting in trial graphics. Some suggestions are noted below.

Network or computer diagrams: The context of the key exhibits can be easier to follow through a diagram that provides an overview. For example, the location of key events involving electronic evidence can be important to understand the sequence of events. Past criminal trials have used network diagrams or computer hard drive directories to highlight where certain events occurred. Generally, the diagrams do not have to be overly detailed because a basic understanding of the locations and the relationships can serve as an effective jury aid.

In one trial, a computer directory was used to show the different locations in which files were downloaded on the computer. Times were placed next to the files on the directory to indicate the download periods. Certain files had different colors to highlight subsequent deletions. In this manner, in one graphic, the jury was able to observe several key related and relevant events.

Avoiding complex matters: In reviewing the electronic evidence for the trial, a prosecutor will have to decide whether the data is useful as an exhibit or whether the expert can testify about the conclusion subject to cross-examination. Some exhibits are readily familiar or apparent to juries. Some examples will include email or other communications and online financial transactions. Other evidence will be inherently technical or complex. For example, the output or exhibit may contain lines of computer code that may be significant to the examiner but challenging for the jury to follow. If a tutorial is required to understand an exhibit, other graphic portrayals should be considered.

Summary tables: Electronic records from companies can appear to be congested for trial purposes. While this data may be useful for business recordkeeping purposes, it may be hard to focus on the relevant portions of the record. For example, Internet account access records may include some data that may not be necessary for the jury to see. In addressing this issue, recent trials have used summary tables highlighting only relevant fields. The data is the same as in the original with extraneous information extracted.

Time lines: Time lines have been used in recent trials to focus on key electronic evidence records. A time line can be based on a computer forensic examination or series of emails from a provider. One benefit of a time line is that the underlying exhibits can be admitted with the time line and the witness can testify about key events in the time line instead of each entry individually.

Summary: It is one matter to find and use electronic evidence as part of an investigation; it is quite another to use electronic records in a persuasive manner at trial in a criminal case. As the foregoing suggestions illustrate, special care should be taken to present this evidence to the jury in an understandable manner.

V. Conclusion

Electronic evidence takes many forms, including email, text message, screen shot, Internet activity, images, and more and this type of evidence is becoming more pervasive. The electronic evidence may be stored on many different types of media, such as hard drives, thumb drives, and cell phones. Electronic information can be maintained by information providers or companies, such as Internet Service Providers, financial institutions, and cell phone companies. Electronic evidence touches nearly every federal criminal case. This article has focused on some key phases and five distinct phases that may be worth considering to enhance the use of this evidence during an investigation and ultimately, if necessary, at trial.❖

ABOUT THE AUTHOR

❑**Mark L. Krotoski**, a federal prosecutor since 1995, has served as National Computer Hacking and Intellectual Property (CHIP) Program Coordinator at the Computer Crime and Intellectual Property Section in the Criminal Division for almost four years.✠

Recent Developments and Trends in Searching and Seizing Electronic Evidence

Howard W. Cox
Former Assistant Deputy Chief
Computer Crime and Intellectual Property Section

I. Introduction

Federal prosecutors are increasingly finding that electronic evidence is present in all cases. Traditionally, computer search and seizure issues were limited to child exploitation, computer crime, and identity theft cases. Today, criminals are using hand-held devices to stalk witnesses, using iPads to record proceeds of criminal activity, and tweeting and texting criminal communications on a broad range of devices. It is now a requirement that all federal prosecutors have a basic familiarity with where electronic evidence can be created and hidden and how to obtain it under the evolving requirements of the Fourth Amendment. The purpose of this article is to provide a brief overview of certain current issues in computer search and seizure relating to the Fourth Amendment and Rule 41 of the Federal Rules of Criminal Procedure. (Further information and training in this area may be found in three courses that CCIPS presents annually at the National Advocacy Center: Basic Cybercrimes, Complex Online Crimes, and Computer Forensics for Prosecutors.)

II. Search warrant protocols and plain view waivers

Some of the greater issues affecting applying for and executing Rule 41 warrants on computers came out in the litigation resulting in a fourth, and hopefully final, decision of the Ninth Circuit in *United States v. Comprehensive Drug Testing, Inc.* (*CDT IV*), 621 F.3d 1162 (9th Cir. 2010). While the lengthy litigation addressed numerous issues, at its core the case addressed two key issues: (1) whether the forensic manner in which the government searches a computer must be set forth in the warrant (search warrant protocols), and (2) whether the government must waive the plain view doctrine or use a filter team whenever it searches a computer via a warrant. An earlier Ninth Circuit opinion in the case mandated both protocols and a plain view waiver, but the 2010 opinion reduced this "mandate" to a concurring opinion. *United States v. Comprehensive Drug Testing, Inc.* (*CDT III*), 579 F.3d 989 (9th Cir. 2009).

The concerns in this area are based on certain judicial beliefs that computer searches are particularly intrusive and may involve the review of a large amount of sensitive personal data. A search warrant protocol is *ex ante* language in the warrant application that describes the forensic methodology that the forensic examiner anticipates using in conducting the post-seizure forensic examination. In the warrant application, the government sets forth, in a certain amount of detail, what kinds of forensic searches will or will not be conducted in order to carry out the court's search requirement. The purpose of these search protocols is to prevent government "rummaging" in computer files not directly related to the purpose of the warrant.

The wisdom of limiting the government's capability and methodology in this regard is of dubious practical and legal wisdom. For example, any Rule 41 search of a person's home for evidence of illegal drugs will automatically involve the examination of intimate personal spaces, such as night stands or

underwear drawers, where sensitive personal items will be seen but not seized. Courts have never suggested that an application for a home search warrant must set forth a search methodology; rather, courts seeks to ensure that the government's search methodology is "reasonable." For example, courts have not required an affiant to specify that he will first search the cupboards in the kitchen and then the knife drawer in the kitchen.

Similarly, the plain view waiver "requirement" was based on the theory that any computer search will involve the review of massive amounts of personal data unrelated to the search. In order to reduce this "unfairness," the government should be required to waive plain view if it is going to use a robust computer forensic methodology. (Again note that plain view waivers have never been considered to reduce similar issues that may arise in physical searches of night stands and underwear drawers.) *See* Orin S. Kerr, *Ex Ante Regulation of Computer Search & Seizure*, 96 VA. L. REV. 1241 (2010) (suggesting that judicially imposed *ex ante* conditions may be beyond the authority of courts); *see also United States v. Grubbs*, 547 U.S. 90 (2006); *Dalia v. United States*, 441 U.S. 238 (1979) (regarding the limited role of the judicial branch in the manner in which a lawful warrant is executed). In order to avoid waiver, the government would be required to create a filter team to conduct an independent review of the digital data. The filter team would provide to the prosecution team only that evidence that it determines to be within the scope of the warrant. Such teams place a significant burden on an already overloaded government forensic capability.

The original *CDT III* "mandate" for search warrant protocols and plain view waivers has been rejected by virtually every federal district and appellate court that has examined the issue outside of the Ninth Circuit, both before and after *CDT IV* was decided. *See United States v. Stabile*, 633 F.3d 219 (3d Cir. 2011) (decided after); *United States v. Mann*, 592 F.3d 779 (7th Cir. 2010) (decided after); *United States v. Williams*, 592 F.3d 511 (4th Cir. 2010) (decided after); *United States v. Burgess*, 576 F.3d 1078 (10th Cir. 2009) (decided after); *United States v. Khanani*, 502 F.3d 1281 (11th Cir. 2007) (decided before); *United States v. Grimmet*, 439 F.3d 1263 (10th Cir. 2006) (decided before); *United States v. McNamara-Harvey*, 2010 WL 3928529, at *2-4 (E.D. Pa. Oct. 5, 2010) (decided after); *United States v. D'Amico*, 734 F. Supp. 2d 321 (S.D.N.Y. 2010) (decided after); *United States v. Farlow*, 2009 WL 4728690, at *4-7 (D. Me. Dec. 3, 2009) (decided after); *United States v. Farlow*, 2009 WL 3163338, at *4-6 (D. Me. Sept. 29, 2009) (decided after); *United States v. Graziano*, 558 F. Supp. 2d 304 (E.D.N.Y. 2008) (decided before). Recognizing that incriminating digital evidence is not often filed under the "My Crimes" folder and that persons seeking to hide evidence of a crime have many opportunities to do so on a computer, most courts find that a computer search is "reasonable" if the warrant describes with particularity what evidence is being sought and the forensic examiner uses the warrant and available forensic tools to tailor a forensic examination to the crime under investigation and the electronic device being reviewed. *See, e.g.*, *United States v. Otero*, 563 F.3d 1127 (10th Cir. 2009) (where the forensic examiner's precision kept the scope of the warrant's execution within reasonable grounds).

Prior to the issuance of *CDT IV*, many district courts in the Ninth Circuit accepted arguments limiting the applicability of *CDT III*. These courts ruled that these requirements are not retroactive, *United States v. Sedaghaty*, 2010 WL 1490306, at *4 (D. Or. Apr. 13, 2010); *United States v. King*, 693 F. Supp. 2d 1200, 1227-29 (D. Haw. 2010); *United States v. Blake*, 2010 WL 702958, at *5-6 (E.D. Cal. Feb. 25, 2010), and do not apply to state warrants that subsequently lead to federal prosecutions, *Blake*, 2010 WL 702958, at *2-3. The one notable published exception to the uniform rejection of *CDT III* is the holding in *In re U.S.'s Application for a Search Warrant*, 2011 WL 991405 (W.D. Wash. Feb. 11, 2011). In that case, the magistrate judge ruled that search warrant protocols and waiver of plain view were mandated by the particularity and reasonability requirements of the Fourth Amendment. *Id.* at *4-5 (suggesting that because most computer searches will lead to the review of large amounts of data, the particularity requirements of the Fourth Amendment are automatically imperiled); *but see United States v.*

Bradley, 2011 WL 2565480, at *23-24 (11th Cir. June 29, 2011); *United States v. Simpson*, 2011 WL 721912, at *4-5 (N.D. Tex. Mar. 2, 2011) (rejecting a claim that the size of a data seizure, over 200 terabytes from a server farm, made the warrant lacking in particularity). To date, no other courts outside of the Western District of Washington have chosen to follow this decision.

While the implications of this holding in the Western District of Washington continue to be reviewed, certain relief may be available to prosecutors that confront *CDT III* issues in domestic terrorism cases under 18 U.S.C. § 2331. In most cases, a case may be prosecuted in one district but require the application for a Rule 41 warrant in order to obtain evidence in another district. If that other district is an adherent to *CDT III*, recent amendments to Rule 41 may be of assistance. Normally a Rule 41 warrant must be sought in the district in which the evidence is located. However, under Rule 41(b)(3), warrants for evidence relating to domestic or international terrorism can be sought before *any* magistrate judge.

III. Border searches of electronic devices

As populations become increasingly mobile and as digital devices capable of storing massive amounts of data become more ubiquitous, it is only natural to wonder how courts will address warrantless searches of digital devices at the border. While persons may be used to customs personnel having the authority to search luggage and other personal possessions at the border, *see generally* 8 U.S.C. § 1225 (2011); 19 U.S.C. §§ 482, 1581 (2010), certain groups are seeking to create greater privacy rights for digital devices at the border. While it may seem incongruous that a person would have greater privacy at the border in their thumb drive than in their dainty under things in their hand-held luggage, that is the position that has been asserted and prosecutors should be prepared to address warrantless searches of any digital device at the border.

First, some context is necessary. According to the Department of Homeland Security, between October 2008 and June 2010, 590 million entrances took place at the borders of the United States. Defendant's Memorandum of Law in Support of Motion to Dismiss at 16, *Abidor v. Napolitano*, No. 10 CV 4059 (E.D.N.Y. Jan. 28, 2011); *see also United States v. Abbouchi*, 502 F.3d 850, 855 (9th Cir. 2007) (recognizing that the government's search authority also extends to exit searches at the border). Of this number, 6,500 persons had their electric devices searched at the border; that is one person in every 90,000 travelers. Reply in Support of Motion to Dismiss at 2, *Abidor v. Napolitano*, No. 10 CV 4059 (E.D.N.Y. Mar. 30, 2011). The "search" may have ranged from asking the person to turn on his device and having customs personnel examine the "My Pictures" folder in the Windows directory to a full forensic review. Of the 6,500 border searches that were conducted during this time period, 220 digital devices were actually seized; that is one seizure for every 2.6 million travelers. Defendant's Memorandum of Law in Support of Motion to Dismiss at 16, *Abidor v. Napolitano*, No. 10 CV 4059 (E.D.N.Y. Jan. 28, 2011).

For the most part, courts recognize that suspicionless and warrantless searches of any digital device at the border are both reasonable and constitutional. *See, e.g.*, *United States v. Flores-Montano*, 541 U.S. 149, 155-56 (2004). Warrantless searches at the border based on the "reasonable suspicion" standard have usually been limited to searches of body cavities. *See, e.g.*, *United States v. Braks*, 842 F.2d 509, 512 (1st Cir. 1988). Border searches may also be based on warrants with probable cause. These traditional rules regarding searches of objects have also been applied to searches of digital media at the border. *See United States v. Arnold*, 523 F.3d 941, 944-48 (9th Cir. 2008); *United States v. Linarez-Delgado*, 259 F. App'x 506, 507-08 (3d Cir. 2007); *United States v. Ickes*, 393 F.3d 501, 503-06 (4th Cir. 2005).

The recent case of *United States v. Cotterman*, 637 F.3d 1068 (9th Cir. 2011), provides a graphic example of some of the problems with searching digital media at the border. The defendant and his wife sought to enter the United States at a small border crossing in Lukeville, Arizona. (Lukeville, Arizona is probably a lovely desert oasis, but, according to the 2000 Census, it has a population of thirty-five hearty

citizens. A more obscure point of legal entry into the United States is hard to imagine.) When Customs & Border Protection (CBP) inspectors ran their names through TECS, Cotterman's 15-year-old conviction for a child exploitation offense became known.

The inspectors then chose to send the Cottermans through a secondary border inspection. *See generally* 19 U.S.C. §§ 1433, 1582 (2010) (governing vehicle inspections at the border). Two laptops and three digital cameras were found in the Cotterman vehicle. Upon finding the digital devices and password-protected files on one of the laptops, CBP decided to ask for assistance from ICE agents that were stationed ninety miles away. (Most CBP officers do not have the technical equipment or forensic training to conduct even a limited forensic review of a computer at the border. Forensic reviews of digital devices are usually conducted by ICE agents.) Upon arrival in Lukeville, the ICE agents decided that the laptops and one of the digital cameras should be subjected to a forensic review. The Cottermans were told that their three devices would be subjected to a forensic inspection but that they were free to leave and could return later to pick up their devices. The ICE agents then left Lukeville with the devices and headed to the nearest ICE computer forensic facility, located in Tucson, Arizona, 150 miles away. The agents arrived in Tucson at 11 p.m. that Friday night, the night of the seizure. ICE forensic personnel commenced an examination of the media the next day. By Sunday, child pornography was found on Cotterman's laptop. ICE called Cotterman and gave him the opportunity to retrieve the other devices from the Tucson office and to have a quick chat with the agents regarding information on the remaining device. Rather than avail himself of this opportunity, Cotterman fled the country for Sydney, Australia. ICE agents were successful in cracking the password-protected files, a full forensic exam of the laptop was conducted, and numerous images of Cotterman abusing a small child were found. Cotterman was eventually indicted and extradited from Australia.

The district court ruled that while the agents had the authority to conduct a warrantless full examination of the laptop, such an examination had to be conducted at the Port of Entry in Lukeville. *United States v. Cotterman*, 2009 WL 465028, at *9 (D. Ariz. Feb. 24, 2009). The court explained that when the agents took the laptop to the nearest ICE forensic facility in Tucson, any governmental search away from the border had to be based on a reasonable suspicion standard. (As noted before, previous decisions applying the "reasonable suspicion" standard to border searches of items detained at the border had been limited to searches of body cavities). While this holding may have served as the impetus for the creation of a full computer forensic laboratory at every remote border crossing in the United States, calmer heads on the Ninth Circuit prevailed. On appeal, the court ruled that Cotterman did not have a reasonable expectation of privacy in his laptop or any other personal item when he crossed the border in Lukeville. *Cotterman*, 637 F.3d at 1077-78. Detaining his property at the border for a warrantless inspection was clearly within the government's authority. The court rejected the existence of any perceived right or heightened proof that the government must offer when property detained at the border is sent to another location to allow the government to conduct a more effective and efficient examination before it is allowed into the country. *Id.* at 1079. The court also ruled that the government exercised its inspection right in a reasonable manner and that it would be unreasonable to expect the government to have a fully equipped forensic station available at every remote border crossing. *Id.* at 1070. The court recognized that a forensic search of a computer may be as complex as the manner in which a person seeks to protect his data. *Id.* at 1081 ("It seems unlikely that every potential terrorist or purveyor of child pornography would label his or her contraband so that its incriminating nature is immediately recognizable, like 'Kiddie Porn' or 'Plot to Destroy America,' and place it in the middle of an unprotected computer desktop. Nor is it likely that a criminal or terrorist would go to the trouble of hiding and password protecting such a file, and then volunteer to identify and open it for inspection at the border."). Finally, the court rejected the argument that the government should have transported portable forensic equipment and examiners to Lukeville, rather than send the computer to Tucson. *Id.* at 1083.

IV. Second warrants and the subjective motivations of forensic examiners

While conducting a forensic examination of a computer for evidence of a crime set forth in a warrant, it is not uncommon for a computer forensic examiner to find evidence of a second crime. In these cases, it is traditional wisdom for forensic examiners to halt the examination and, based on the plain view doctrine, obtain a second warrant to search for evidence of the additional crime. *See, e.g.*, *United States v. Carey*, 172 F.3d 1268, 1276 (10th Cir. 1999). Some courts have ruled that this is not a hard and fast requirement, holding that as long as the forensic examiner continues with the methodology originally developed to seek evidence of the first crime, repeated discovery of evidence of other crimes remains within the scope of plain view and does not require a second warrant. *See United States v. Wells*, 2008 WL 2783264, at *4-6 (S.D. Iowa July 15, 2008); *United States v. Kearns*, 2006 WL 2668536, at *3-4 (N.D. Ga. Sept. 15, 2006). A new warrant would only be required when the examiner decides to commence a new forensic approach designed to find evidence of the second crime. *See United States v. Mann*, 592 F.3d 779 (7th Cir. 2010). For example, when a forensic examiner is reviewing a digital device for fraudulent check images, such a forensic review will often require a manual examination of every one of thousands of images on the device. *See, e.g.*, *United States v. Burgess*, 576 F.3d 1078, 1094 (10th Cir. 2009) ("[T]here may be no practical substitute for actually looking in many (perhaps all) folders and sometimes at the documents contained within those folders, and that is true whether the search is of computer files or physical files."). If the examiner sees multiple child pornography images in the course of this review, it can be successfully argued that all such images are within plain view because the examiner was going to have to review every image for evidence of check fraud. However, if after the first discovery of child pornography the examiner decides to run an image hash comparison tool specially designed to search for known child pornographic images, the search technique would be beyond the scope of the original warrant.

Recently, some defendants have sought to challenge this approach by seeking to impeach the motivation of the forensic examiner in conducting the original search. These advocates contend that the court should consider the subjective motivation of the examiner in conducting the original search; that is, even though the warrant was for check fraud, the examiner suspected that the target also possessed child pornography and crafted the check fraud search in a way to find evidence of the other crime as well. Courts have repeatedly rejected such approaches. In *United States v. Stabile*, 633 F.3d 219 (3d Cir. 2011), U.S. Secret Service agents and local police officers were investigating financial frauds committed by the defendant. Under a warrant authorizing a search of the defendant's hard drive for evidence of financial fraud, the examiner opened a computer folder thought to contain evidence of financial fraud and instead found evidence of child pornography. The defendant moved to suppress the contents of the folder because the examiner testified that, at the time he conducted the financial fraud review, he had suspicions that the defendant also possessed child pornography. The court ruled that the hopes and dreams of the investigator regarding finding evidence of other crimes were irrelevant. *Id.* at 240. The search was conducted in a reasonable manner to find evidence of the crime for which the warrant was issued and the child pornography images were within plain view.

The Third Circuit's holding in *Stabile*, rejecting as irrelevant the searcher's subjective motivation, was also followed by the Fourth Circuit in *United States v. Williams*, 592 F.3d 511 (4th Cir. 2010). In *Williams*, police were searching the defendant's hard drive, with a warrant, for evidence of sending threatening emails. A thorough forensic review also discovered evidence of child pornography under the plain view doctrine and the defendant argued that the review of the media for the original crime was too thorough. The defendant argued that in order to search for evidence of threatening emails, the government did not have to engage in the meticulous review of the media that was conducted here. The court rejected this argument and held that the warrant impliedly authorized officers to open every file on the computer and to review the file's contents to determine if it fell within the scope of the warrant. *Id.* at 525. The court also rejected Williams' argument that the plain view doctrine did not apply because the officer's original

purpose was to look for crimes outside the scope of the warrant and that any subsequent discovery of these crimes could not be "inadvertent." *Id*. at 523. The court ruled:

> This argument, however, cannot stand against the principle, well-established in Supreme Court jurisprudence, that the scope of a search conducted pursuant to a warrant is defined *objectively* by the terms of the warrant and the evidence sought, not by the *subjective* motivations of an officer. As the Court stated in *Horton*, "[t]he fact that an officer is interested in an [unauthorized] item of evidence and fully expects to find it in the course of a search should not invalidate its seizure if the search is confined in area and duration by the terms of a warrant or a valid exception to the warrant requirement." In that case, the Court *explicitly* rejected the very argument that Williams makes in this case, that unauthorized evidence must be suppressed because its discovery was not "inadvertent." As the *Horton* Court explained, "[E]ven though inadvertence is a characteristic of most legitimate 'plain view' seizures, it is not a necessary condition."

Id. at 523-24 (some internal citations omitted)

Williams also contains a good examination of the relationship between digital and physical searches. The warrant authorized a search of Williams' home for, *inter alia*, disks and "thumbnail drives" capable of storing data. In carrying out this search for the devices, agents opened a lockbox in his home and found a machine gun and silencer. The court ruled that because the digital devices covered by the warrant could be as small as a dime, the government properly opened the lock box in its quest for digital evidence and the machine gun and silencer were properly seen and examined as part of a legitimate safety procedure. *Id*. at 524-25.

V. Conclusion

As more and more prosecutors face issues regarding computer search and seizure, they must be prepared to address new technological and legal challenges. For the most part, federal courts have continued to rely on reasonability as the guiding principle in determining the appropriate computer search methodology. Prosecutors need to stay apprised of current computer forensic trends and techniques to ensure that the methodology utilized by the forensic examiner is indeed reasonable in light of the current state of the art and science of computer forensics.❖

ABOUT THE AUTHOR

❑**Howard W. Cox** is a former Assistant Deputy Chief of the Computer Crime and Intellectual Property (CCIP) Section of the Criminal Division of the United States Department of Justice and was responsible for supervising prosecutions of federal computer crimes throughout the United States. Prior to his work at the Department of Justice, Mr. Cox held a number of positions with the Office of Inspector General and was a trial attorney with the United States Army Judge Advocate General's Corps. He also served as Law Secretary to the Honorable Sherwin D. Lester in the Superior Court of New Jersey. He has written and taught extensively on matters relating to procurement and computer fraud as an adjunct Full Professor at George Washington University's Department of Forensic Science and as an instructor for the Government Audit Training Institute of the Graduate School.✠