CHAPTER

Internet and e-mail

8

"The Internet is the crime scene of the 21st Century."
— Manhattan District Attorney Cyrus Vance, Jr.

INFORMATION IN THIS CHAPTER:

- Overview of the Internet and How It Works
- How Web Browsers Work and the Evidence They Can Create
- E-Mail Function and Forensics
- Chat and Social Networking Evidence

INTRODUCTION

In the beginning, the Internet was a little-known tool used by a few academics and the military. Today, it's truly a tool for the masses. We can order pizza, pay bills, look up a phone number, and take a class. For many of us, it is hard to imagine life without it. For examiners, its use can leave significant pieces of evidence scattered around that can persist for a long, long time. Web browsing, chat, e-mail, and social networking are just some of the technologies that we must understand in terms of how they're used, how they work, and where they leave traces.

INTERNET OVERVIEW

We'll begin with a quick introduction to the technology involved in getting your favorite web page to appear on your computer screen. Perhaps the best way is to track the process from start to finish. It all begins when someone enters a web address or Uniform Resource Locator (URL) into the address bar of a browser. A URL comprises three parts: the host, the domain name, and the file name. Let's use http://www.digitalforensics.com as an example.

In our example, "http" or Hypertext Transfer Protocol (HTTP) is the protocol used on the Internet to browse and interact with websites and the like. A protocol is nothing more than an agreed-upon way for devices to communicate with one another. Next is the domain name, "digital forensics" in this instance. Last is the Top Level Domain (TLD), ".com." It's called a TLD because it is at the top of the hierarchy that makes up the Internet's domain name system. Other TLDs include .org, .edu, and .net, just to name a few.

The browser, using the HTTP protocol, sends a "get" request to the web server hosting www.digitalforensics.com. A browser is an application that is used to view and access content on the Internet. There are several browsers to choose from; the most common are Microsoft's Internet Explorer, Mozilla's Firefox, and Google's Chrome.

After hitting Enter, the first order of business is to convert the domain name into an Internet Protocol (IP) address. The Internet functions with IP addresses. It can't do anything with the domain name itself. The domain name is for us, making it easier to remember the location of a website. A Domain Name Server (DNS) is responsible for mapping domain names to specific IP addresses. After the DNS makes the conversion, the request is then sent on to the server that's hosting the website. After receiving the request, the server returns the requested web page and associated content.

A web page has several components. The first is the Hypertext Markup Language (HTML) document. This contains quite a bit of information, including directions for how the page should be rendered (displayed) by the browser, content, and more. It also contains file names for subcomponents of the web page such as images. It's important to note that HTML is not a programming language.

There are two types of web pages: static and dynamic. A static web page is one that is prebuilt. Its content, layout, etc., are predetermined. A dynamic page, however, is built "on the fly." It doesn't exist until it's called. The page is built from different pieces drawn from databases. Amazon is a great example of a dynamic website. My Amazon page will very likely be different from your page. The books and so on that appear on my page are based on my shopping and buying habits. All this information is stored in a database, along with elements like book images, descriptions, and so on. When I logon to Amazon, the server sends the items that are standard for everyone (like the Amazon logo), along with the content targeted to me.

When interacting with a website, it's important to understand where certain things are occurring. This can be especially important from a forensics perspective because it can tell you where you should be looking for a given artifact. Actions can occur on either the client side or the server side. JavaScript (no relation to the Java programming language) is a client-side technology. It's used for things such as rollovers on a navigation bar. The code that makes that work is downloaded and run on the local machine. Server-side actions are just the opposite and are used when there is a need to send information to another computer (like my custom content at Amazon).

ADDITIONAL RESOURCES

WEB TECHNOLOGY

Today's web is a complex place using many different technologies to make it run. Understanding how these work, even at a rudimentary level, will be very helpful. The w3 Schools website is a great source of introductory material on many of these technologies. The site includes reference material, lessons, quizzes, tutorials, and more: http://www.w3schools.com/.

Determining the ownership and host of a particular domain name can become relevant in a criminal or civil case. A search query known as a "whois" can help you identify some of the individuals and/or companies associated with a given domain name. A whois search can tell you the registrant, when the domain was created, the administrative contact, and the technical contact. The contact information typically provides a name, address, and phone number. Most, if not all, domain name registrars now offer private registration. Any whois search for a domain name with private registration will typically get the registrar's contact information, rather than that of the actual owner (Network Solutions, LLC, 2011). If you'd like to give this a try, visit one of the sites offering the whois service. Network Solutions is one: http://www.networksolutions.com/whois/index.jsp.

PEER-TO-PEER (P2P)

Peer-to-Peer (P2P) is used primarily as a means to share files. A major portion of the traffic on a P2P network is pirated music and movies, as well as child pornography. P2P differs from a client/server network in that computers on a P2P network can serve both roles (client and server). Gnutella is one of the major systems or architectures used in P2P networks.

MORE ADVANCED

GNUTELLA REQUESTS

On a P2P network, what stops a file request from propagating forever? There is actually a built-in mechanism in the information packets. In each packet, there is a Time To Live (TTL) value that is set to decrease by one every time it is delivered to another node on the network. Once that number hits 0, the packet is stopped.

To get started with a P2P network, users must first download and install a P2P client such as KaZaA, Frostwire, GigaTribe, or eMule. Typically, users then create a "shared" directory containing files they want to make available to others. To find files of interest to download, users normally enter search term(s) for the file or files they want. If the search is successful, the software returns a list of computers that have the requested file(s). Lastly, the files are downloaded to a directory of the user's choosing or to the default location specified by the client. P2P networks use HTTP to transfer files.

Nodes on a Gnutella fall into two categories. Nodes that have the required bandwidth as well as the uptime (time on the network) are classified as Ultrapeers. Those that don't are known as leafs. Ultrapeers perform some additional duties such as searching, indexing, and facilitating connections.

THE INDEX.DAT FILE

The INDEX.DAT is a binary, container-like file that is used by Microsoft's Internet Explorer (MSIE). The INDEX.DAT file holds quite a bit of value for forensic

examiners. There are multiple INDEX.DAT files on a system. The INDEX.DAT tracks several pieces of information regarding the URLs visited, the number of visits, and so on. These files are hidden from the user and must be viewed using a tool of some sort. Both FTK and EnCase are able to decipher INDEX.DAT files. MSIE has three directories: History, Cookies, and Temporary Internet Files. INDEX.DAT files are used to track the information and contents of each directory (Casey, 2009).

WEB BROWSERS—INTERNET EXPLORER

Web browsers are an indispensable part of the overall computing experience and serve as our "vehicles" on the "Information Superhighway" known as the World Wide Web. Although there are multiple browsers on the market, Microsoft's Internet Explorer is far and away the most widely used. Other browsers (for the PC) also getting some traction are Mozilla's Firefox and Google's Chrome. On Macintosh computers, Safari is king, with Firefox getting some use there as well. At their foundation, these applications function in much the same way. For instance, all of them use some sort of caching system. They also have mechanisms to deal with cookies, Internet history, typed URLs, bookmarks, and more. They differ in the details. Space does not permit an exhaustive look at all the browsers and the details of their inner workings. Instead, we'll focus on some of the common functions as they work in MSIE, the overwhelming market leader.

COOKIES

A cookie is a small text file that is deposited on a user's computer by a web server. Cookies can serve a variety of purposes. They can be used to track sessions and remember a user's preferences for a particular website. Amazon.com is a great example. When you return to the site, you are normally greeted with a "Hello, Susan," as well as customized recommendations based on your buying and browsing history. That level of individualization is made possible through cookies.

Cookies can provide valuable evidence and are tracked in a single INDEX.DAT file. They can contain Uniform Resource Locators (URLs), dates and times, user names, and more. Deciphering cookies can be a challenge, as they aren't normally written in the clear. Fortunately for us, tools are available to get this done. It's critical to note that the existence of a web address in a cookie is not necessarily proof that the suspect actually visited that site (Casey, 2009).

TEMPORARY INTERNET FILES, A.K.A. WEB CACHE

We are an impatient lot. As such, speed is vital to our Internet experiences. Today, web browsing is expected to be nearly indistinguishable from the applications running on our own machines. Web cache is one way that the browser makers shave some time off how long it takes to download information. Cache speeds things along

by reusing web page components like images, saving users from having to download objects more than once.

Microsoft's browser, Internet Explorer, refers to web cache as Temporary Internet Files (TIF). In Microsoft Internet Explorer, TIF is organized into subfolders bearing random eight-character names. They are organized using a collection of INDEX.DAT files. Each file in TIF has a corresponding date and time value associated with it. This includes a "last-checked" time, which is used by the browser to determine if a newer version exists on the server. If so, then it will download the newer version.

Users can view their TIF anytime using Windows Explorer. Inside the TIF folder, users will see a listing of its contents. Each item in the list will display an icon showing file type, file name, and the associated URL. It's important to understand that, in this instance, what the user sees is a virtualized representation of the content. The actual items are kept in the TIF subdirectories. The only file that is actually kept here is the INDEX.DAT that keeps tabs on where the files are located inside the various subdirectories.

Webmail evidence can also be found in TIF. Hotmail, AOL, and Yahoo! can all leave messages and/or inbox information that can prove useful. These items can be recognized by the file names. Here are some examples:

- Outlook web Access Messages—Read[#].htm
- AOL Messages—Msgview[#].htm
- Hotmail messages—getmsg[#].htm
- Yahoo!—ShowLetter[#].htm
- Outlook web Access Inbox—Main[#].htm
- AOL Inbox—Msglist[#].htm
- Hotmail Inbox—HoTMail[#].htm
- Yahoo!—ShowFolder.htm

Web cache can be used to determine both culpability and intent. Much of what's in web cache will be thumbnails (those small images) along with bits and pieces of web pages.

Image size can affect a case, particularly those involving child pornography. If the suspect images are composed entirely of small, cache-like images, then some prosecutors may be reluctant to file charges. The issue then becomes intent. Those images could have been downloaded automatically, without his consent. Images of such a small size can make for a much weaker case. Larger images—those not commonly found as part of a web page—are harder to explain away.

INTERNET HISTORY

Microsoft's Internet Explorer, the reigning king of browsers, keeps multiple historic user records. History is used to prevent a user from having to retype URLs into the address bar of the browser. The INDEX.DAT files track other details as well. For example, it tracks the number of times the site is visited, and the name of the file.

The Internet history is organized in multiple folders and INDEX.DAT files. There are three folders: Daily, Weekly, and Cumulative.

These folders use a naming convention based on a set prefix followed by a date range. For example, a folder covering the Internet history from October 1, 2011, to October 8, 2011, would look like this:

MSHist012011100120111008
MSHist01 – Folder name/prefix
2011 – Year (start)
1001 – Date (start)
2011 – Date (end)
1008 – Date (end)

People who have something to hide will often clear their histories on a frequent basis. This can be done manually by the user or automatically by the system. By default, the history is set to clear every twenty days. The user can change this to clear much faster than that. Using a tool that can read the registry, you can view this information here:

NTUSERS\Software Microsoft\Windows\CurrentVersion\Internet Settings\URL History

MORE ADVANCED

THE NTUSER.DAT FILE

The NTUSER.DAT file contains preference settings and individual information for each user profile. Browser history is part of this information. There is one NTUSER.DAT for each user profile on the system. Although technically a registry file, the NTUSER.DAT is located in the user folder. Note that we're talking about user "profiles" and not "users." Whether a specific person has been on the keyboard is a very difficult, if not impossible, determination to make. Just because a person has a profile on the machine does not mean their fingers were on the keyboard at any given moment.

If this value is set to less than the default of twenty days, this can be used to show that the defendant took proactive steps to remove potentially incriminating evidence.

INTERNET EXPLORER ARTIFACTS IN THE REGISTRY

As part of its everyday function, MSIE deposits artifacts in the registry. These items are stored particularly in the NTUSER.DAT hive. Here we can see if the browser stores passwords, along with the default search engine, the default search provider, and more.

The registry can also tell us what URLs have been typed right into the browser's address bar. These are listed from 1 to 25 with the lowest number being the most recent. Only twenty-five entries can be kept at a time. The entries are purged on a first-in/first-out basis. Figure 8.1 shows you what they look like through a forensic tool.

Here is the file path to this registry artifact:

Name	Type	Data
url1	REG_SZ	http://www.google.com/
url2	REG_SZ	http://www.fileshredder.com/
url3	REG_SZ	http://www.wikileaks.org/
url4	REG_SZ	http://hackernews.com/
url5	REG_SZ	http://www.hacker.com/
url6	REG_SZ	http://www.hacer.com/

FIGURE 8.1

Typed URLs as found in the Windows Registry. Graphic courtesy of Jonathan Sisson.

NTUSER\Software\Microsoft\Internet Explorer\Typed URLs

Remember, the registry is not human-readable in its native form. To examine it, you will need an appropriate tool. Some of these tools include Microsoft's RegEdit, Harlan Carvey's RegRipper, and AccessData's Registry Viewer.

CHAT CLIENTS

Chat applications are both popular and numerous. They are used for instant text-based communication. Popular applications include AOL Instant Messenger (AIM), Yahoo! Messenger, Windows Live Messenger, Trillian, Digsby, and many more. These clients can be used either to commit or to facilitate a variety of crimes. Pedophiles use these tools to solicit sex from minors or to distribute child pornography. Buyers and sellers use them to negotiate the sale and transfer of narcotics. The list can go on and on. Function varies from client to client as do the artifacts they leave behind. Function and residual evidence can also vary from version to version.

It's difficult to keep up with the rapid pace at which these clients change. Changes can result in artifacts moving or disappearing. Rather than get "down in the weeds" with each application and version, we'll talk in broad terms about what kind of artifacts are possible and how they can be used as evidence.

Not unlike other software, a chat client will leave artifacts of its installation. Paths and directories may vary somewhat. The presence or absence of these files and folders may help in proving or disproving that a specific client was used to communicate with a victim or accomplice.

Chat programs maintain a contact or "buddy" list. This list of screen names can be used to link individuals together, particularly if the other parties' screen names appear in the logs or on the drive. Screen names are often nonsensical, like "football-fan7878," and it can take some effort to connect them with specific people. Entering screen names as part of your keyword search can also be very helpful. To complicate matters further, users can have multiple screen names. Many times, these alternate identities assume a parent-child relationship with the primary identity.

Users can also choose to block people, preventing them from communicating with them. If this function is available, this setting should be tracked somewhere, potentially leaving relevant artifacts. Often clients will also maintain a list of recent chats.

Other preferences that are under user control include embedding the date time in the chat, selecting a custom icon or image, and enabling or disabling logging. Logging can serve as a tremendous source of evidence if it's enabled.

Normally, logging is turned off by default, requiring the user to activate that function. Logs typically record the chat conversations and/or other related information like connection details. Even if logging is turned off, the user can manually save that particular chat session if necessary. A major difference between having logging turned on and manually saving a session log is the location where the resulting file is saved. Auto-saved logs will normally go to a default location, whereas a destination will have to be selected for a manually saved log.

Another preference setting of interest involves the automatic acceptance of video calls, file transfers, real-time instant messages, and so on. By default, many of these features are disabled. This setting and the subsequent functionality can be used to prove that an image wasn't downloaded without consent. Suspects will have an uphill slog trying to get a jury to believe that they "had no idea" they were downloading child pornography through their chat clients when the settings prove that they had to agree to accept it.

Some chat/IM clients are now allowing users to associate a cell phone (or more than one) with their accounts. This allows them to have IM messages forwarded to their mobile phones. In this situation, the cell number, together with the account information, could be used to help connect that person to a particular screen name.

INTERNET RELAY CHAT

Commercial chat clients like Yahoo! and AOL are quite popular and in wide use. Two other chat clients are well worth exploring. These tools are arguably better suited for criminal activity. Internet Relay Chat (IRC) is one such tool. IRC is a large chat network that has little to no oversight as it is under the control of no one single entity. It affords its user near-total anonymity because there is no formal registration process. IRC is also free to use. The IRC network comprises many smaller networks, such as Undernet, IRCnet, and EFnet, just to name a few (Casey, 2011). IRC users create their own chat rooms or "channels." IRC attracts criminals with a wide range of interests looking to trade information or contraband. Network intrusion, identity theft, and child pornography represent some of the main criminal interests found on IRC.

IRC boasts some other features that make it attractive for criminals. Direct Client Connection (DCC) allows two users to connect directly from one machine to the other. In this mode ,the communication is totally private. This private traffic even avoids network servers, leaving no evidence for investigators to find.

"I SEEK YOU"

I Seek You (ICQ) is the second chat tool that warrants a closer look. ICQ came on the scene in 1996.

These numbers from ICQ give you an idea of just how popular this chat client is:

- More than 42 million active users
- More than 425 million downloads

- More than 1.1 billion messages sent and received every day
- Average ICQ user connected more than five hours per day
- 47% female and 53% male
- 80% of users between the ages of thirteen and twenty-nine
- Available in sixteen languages (ICQ)

Unlike IRC, ICQ does have a registration process. Users who register are assigned a User Identification Number (UIN). Communication on ICQ maintains a high level of privacy. One must be invited to be included into a conversation. ICQ does route traffic through centralized servers so some artifacts may exist there if that server can be found.

E-MAIL

Of all the potential sources of digital evidence, e-mail is one of the best. People often draft and send e-mail that they assume will never be read by anyone other than the intended recipient. These often-candid exchanges can (and have) come back to haunt the parties involved. It's also persistent, residing in multiple locations, making it harder to get rid of.

ACCESSING E-MAIL

E-mail is accessed and managed in one of two ways. The first is web-based e-mail such as Google's Gmail or Microsoft's Hotmail. These tools function through a web browser. The second is through an e-mail application (client). E-mail clients are specialized programs designed specifically for working with e-mail. Some applications also manage calendars, tasks, contacts, and more. Outlook and Windows Live Mail by Microsoft are two of the most popular e-mail clients on Windows systems. Outlook, the more robust of the two, is used primarily in the workplace or by power users. Windows Live Mail and its predecessor Outlook Express have much more limited functionality.

Outlook stores data in either a .pst or .ost file. Windows Live Mail stores individual messages as .eml files. Microsoft Outlook Express uses .dbx. Getting at the individual messages from inside these containers is a concern, but much less so now that several current tools handle these file types natively. Individual e-mail messages (.msg files) can be exported out and given to investigators or attorneys for review.

E-MAIL PROTOCOLS

E-mail uses multiple protocols to send and receive messages. Some of them are:

- Simple Mail Transfer Protocol (SMTP)—Used by e-mail clients to send e-mail and by servers to both send and receive.
- Post Office Protocol (POP)—Used by e-mail clients to receive e-mail messages.
- Internet Message Access Protocol (IMAP)—Two-way communication protocol used by clients to access e-mail on a server.

E-MAIL AS EVIDENCE

E-mail is widely used and people tend to be uninhibited in their e-mail messages, saying things they might never say otherwise. Thus, e-mail can provide us with a wealth of potential evidence. Some of those things include:

- Communications relevant to the case
- E-mail addresses
- IP addresses
- Dates and times

When investigating e-mail, it's important to realize that it could be found in a number of places. These include: the suspect's machine, any recipient's machine, a company server or backup media, a smartphone, a service provider, and any server that the message may have passed through on its way to its final destination. Like most web-based evidence, time is still a factor. Collecting that evidence sooner rather than later will give you a better chance of success.

The main components of an e-mail are the header, the body, and—potentially—attachments. Every e-mail message that's sent has a header. The header records information as the e-mail travels from the sender to the receiver. Think of it as a passport of sorts. At every stop (server) along the way, information is added to the header. The body of the e-mail is the message itself. Finally, any attachments are added. These include items such as images and user-created files such as documents, spreadsheets, and so on. Keeping the attachments connected with an associated e-mail message is very important from an evidentiary perspective.

E-MAIL—COVERING THE TRAIL

Especially savvy suspects may take steps to prevent someone from tracing a message back to them. For example, they could forge an e-mail (make it appear to be from someone else) or remove or modify the headers. Suspects could also create phony e-mail accounts.

Free software available on the Internet enables users to "spoof" an e-mail. Spoofing is the act of making an e-mail look as though it actually came from someone else or from a different location. There are services available that will remail (forward) messages, stripping out the identifying information before transmission. This is known as anonymous remailing. Many of these companies don't keep logs, further ensuring the privacy of their users.

ALERT!

SHARED E-MAIL ACCOUNTS

E-mail can be used to communicate even without being sent. This is done by creating an anonymous account, on Yahoo! for example, and sharing the login information. Users then simply create messages and deposit them in the "Drafts" folder for others to read. Once the message is read, it can be deleted. These accounts can be for one-time use, making them nearly impossible to trace or monitor. This is a popular practice

among terrorists. "One-time anonymous accounts are extremely difficult to monitor," said Richard Clarke, former U.S. counterterrorism czar (Frontline, January 25, 2005).

TRACING E-MAIL

Tracing an e-mail message is heavily reliant on logs. As we learned earlier, each server along the e-mail's path adds information to the message header. One of those bits of information is the Message ID. The message ID is a unique number assigned to the message by the e-mail server. Correlating the message ID with the server's logs is solid evidence that the message was received and sent by that particular machine. Again, the providers may purge those logs on a regular basis if they even keep them at all. Foreign providers will likely be very tough to deal with, making collection of this evidence that much harder.

READING E-MAIL HEADERS

The e-mail header provides a record of the path the message took from sender to receiver (assuming steps weren't taken to alter or remove it). E-mail headers should be read from the bottom to the top. Below is a sample e-mail header from a message I may have sent to legendary Pittsburgh Steelers linebacker Jack Lambert.

```
Delivered-To: Lambert58@gmail.com
Received: by 11.48.31.1 with SMTP1 id c2ct279nzg;
Fri, 25 Oct 2011 22:38:23 -0800 (PST)
Return-Path:
Received: from mail.emailprovider.com (mail.myisp.com
[12.34.567.890]) by mx.gmail.com with SMTP id
f27se846431anc.2011.10.25.22.38.19; Fri, 25 Oct 2011
22:38:23 -0800 (PST)
Message-ID: <20111025233819.47097.mail@mail.myisp.com>
Received: from [12.34.567.890] by mail.myisp.com via
HTTP; Fri, 25 Oct 2011 22:38:19 PST
Date: Fri, 25 Oct 2011 22:38:19 -0800 (PST)
From: John Sammons
Subject: Super Bowl
To: Jack Lambert
Delivered-To: Lambert58@gmail.com
The message recipient
Message-ID: <20111025233819.47097.mail@mail.myisp.com>
Received: from [12.34.567.890] by mail.myisp.com via HTTP;
Fri, 25 Oct 2011 22:38:19 PST
This the record of the message being sent through Jack Lambert's
email provider, mail.myisp.com.
Delivered-To: Lambert58@gmail.com
Received: by 11.48.31.1 with SMTP1 id c2ct279nzg; Fri, 25 Oct
2011 22:38:23 -0800 (PST)
Return-Path:
Received: from mail.emailprovider.com (mail.myisp.com
[12.34.567.890]) by mx.gmail.com with SMTP id f27se846431anc.
2011.10.25.22.38.19; Fri, 25 Oct 2011 22:38:23 -0800 (PST)
Finally,the message is transmitted from my email provider
to Jack's Gmail account, Lambert58@Gmail.com
```

Note the message ID, 20111025233819.47097.mail@mail.myisp.com. Remember, this is a unique number assigned by an e-mail server (Google, 2011).

SOCIAL NETWORKING SITES

E-mail and social media have at least one thing in common: There seems to be almost nothing that people won't send, post, or tweet. The fact that everyone seems to be on Facebook, Twitter, LinkedIn, or some flavor of social media is not lost on law enforcement or prospective employers for that matter. Both groups routinely look to social media to learn more about suspects and prospective employees.

Social media evidence can be found in several places, including the suspect's computer and smartphone, and the provider's network. Getting evidence from the provider will require relatively quick action, along with a subpoena or search warrant. Remember, the provider only retains this information for a certain amount of time. At some point, the data you need will be purged without some legal intervention. All things considered, collecting the evidence from the provider might yield the best results.

Recovering evidence on the local machine can be a challenge. The page file (or swap space) is one location that could bear fruit. INDEX.DAT files also hold promise. Multiple artifacts can be found here. The confirmation e-mail (sent when the account is created) is found in the History.IE5(Index.dat file. The user's Facebook profile can be found on the local machine in a file named profile[#].htm. This is located in the Content.IE5 directories. The History.IE5(Index.dat file can hold Facebook friend searches.

ADDITIONAL RESOURCES

CASEY ANTHONY TRIAL TESTIMONY

The Casey Anthony trial garnered media attention across the country. Anthony was charged with murdering her young daughter Caylee. Digital forensics played a central role in the case, particularly regarding the searches for certain keywords such as "chloroform." The trial testimony in this case by computer forensic examiner Sgt. Kevin Stenger provides some insight expert testimony on browser forensics (Firefox, in this instance): http://www.myfoxorlando.com/dpp/news/060811-kevin-stenger-testifies

SUMMARY

The Internet functions in large part due to two protocols, specifically HTTP and TCP/IP. Another very common technology in wide use is or Hyper-text Markup Language (HTML). HTML is one of the primary languages used to construct web pages. In

digital forensics, evidence can be found within this code, so it behooves us as examiners to be able navigate through it to locate any existing evidence.

We also looked at how web pages are found and sent to browsers using Uniform Resource Locators (URLs) and Domain Name Servers (DNSs).

Peer-to-Peer (P2P) networks can be used to share not only pirated music and movies, but contraband such as child pornography as well.

This chapter also looked at several artifacts generated from Internet and e-mail usage. These includes such things as INDEX.DAT records, Temporary Internet Files (TIF), the NTUSER.DAT file, cookies, and e-mail headers. Tracing an e-mail back to its origin is no easy feat, as the identifying information can be forged or removed.

Chat clients and their associated logs are worth examining if found on a computer. Remember, logging may not be turned on by default.

IRC and ICQ are two modes of Internet communication that can't be ignored. These are two of the most popular ways for criminals (and others concerned with private communication) to help cover their trails.

Social networking is used worldwide today by a massive number of people. Social networking evidence can be found locally and remotely on a provider's network.

REFERENCES

Casey, E., 2009. Handbook of Digital Forensics and Investigation. Academic Press, Burlington, MA.

Casey, E., 2011. Digital Evidence and Computer Crime: Forensic Science. Computers and the Internet Academic Press, Waltham, MA.

E.I. du Pont de Nemours and Company v. Kolon Industries Inc., 2011. U.S. Dist. LEXIS 45888. E.D. Va. Retrieved from: <http://www.ca4.uscourts.gov/Opinions/Unpublished/121260.U.pdf> (accessed 09.16.11.).

Frontline. Retrieved from: <www.pbs.org/wgbh/pages/frontline/shows/front/special/tech-sidebar.html> (accessed 09.19.11.).

Google, 2011. Reading Full Email Headers. Retrieved from: <http://mail.google.com/support/bin/answer.py?hl=en&answer=29436> (accessed 11.10.11.).

http://www.nativeintelligence.com/ni-free/itsec-quips-05.asp.

Network Solutions LLC., 2011. WHOIS Behind That Domain Name? Retrieved from: <http://www.networksolutions.com/whois/index.jsp> (accessed 11.19.31.).

w3schools, 2011. HTML Introduction. Retrieved from: <http://www.w3schools.com/html/html_intro.asp> (accessed 11.10.13.).

http://www.nist.gov/.