

Case Studies

INFORMATION IN THIS CHAPTER:

- A day in the life of a cybercriminal
- The life and casework of a cyber investigator
- Testifying to your work

INTRODUCTION

In theory, investigations should succeed as planned and expected. However, in practice, theory is only the starting point for real-life situations requiring creative solutions to obstacles. A review of case studies provides a means to show theory and practical applications in real-life case scenarios, with both positive and negative results. A thorough examination of one case for a targeted study goes well beyond this book due to the amount of information any single case possesses, but we can use many examples to reinforce investigative concepts.

In order to give examples showing how successful concepts in this book have been applied in real life, this chapter will show a collection of briefed examples across a wide range of case studies. Keep in mind that there is more than one solution to any single problem you will encounter and certainly more solutions that can be given in this chapter.

And as some examples are clearly criminal investigations where the availability of demanding evidence through search warrants exists, civil cases allow for evidence to be gathered without warrants, such as electronic evidence owned by a business and used by an employee. Whichever type of case you have, use the resources and legal authority available to secure the evidence. Sometimes you can just ask for it; other times, you may need a judge to order it.

CONTENTS

Introduction.....	225
A Day in the Life of a Cybercriminal.....	226
Backdating Documents...	226
False Names and Disposable Email Accounts.....	229
Evidence Leads to More Evidence.....	230
Searching for All the Bad Things.....	231
Scenario—Threatening Blog Posts.....	233
Making the Wrong Kind of Friends Online ...	234
A Break in the Case, Otherwise Known as a Suspect's Mistake	235
Altered Evidence and Spoliation.....	237
Spoofed Call Harassment.....	240
Disgruntled Employee Steals and Deletes Employer's Data.....	242
Missing Evidence	245
Bomb Threats by Email.....	246
ID the Suspect.....	247
Online Extortion.....	249
Placing Suspect at a Location.....	250

<i>Placing the Suspect in the Office at a Specific Location</i>	251
<i>Stolen Property</i>	252
<i>IP Addresses Aren't Enough</i>	253
<i>Planted Evidence</i>	254
The Life and Casework of a Cyber Investigator	255
<i>Technical Knowledge and Skills</i>	256
<i>This Case is Different from That Case</i>	257
Testifying to Your Work	258
Summary	259
Bibliography	260

The specific examples come with disclaimers. Depending upon the type of operating system and even the version of an operating system, certain artifacts will not exist or be recoverable. Depending upon the actions of the suspect, artifacts that existed at one point may not exist after being overwritten by other data. Even depending upon the forensic application used, some artifacts may be incapable of being recovered. So, a statement that electronic evidence *may* be recovered in a specific situation literally means maybe, because it depends on other factors. Usually, the answer as to if a forensic artifact of evidence can be recovered is simply, it depends.

A DAY IN THE LIFE OF A CYBERCRIMINAL

The scenarios given in each following section are fictional, but much of the content has been taken from cases I've worked. Each scenario has a referenced case ("Case in Point") for a real-life example of a high profile case. Most of these can be found online through open source or court records to read detailed information on investigative methods used.

As an investigation can be comprised of one independent incident or a multitude of crimes over a period of time, utilizing different operating systems and versions of operating systems, your investigation processes and methods will need to flow with your evidence. Some of the investigative tips discussed in this chapter will work with some cases, others won't.

Backdating documents

Scenario: A business purchase agreement document in PDF format is alleged to have been altered to benefit one party in the agreement. Certain verbiage is claimed to have been changed as has the date of the agreement. Both the plaintiff and defendant claim their version of the document is accurate and the other document version being a manipulated copy.

Investigative Tips: Antedating is creating files with intentionally inaccurate time stamps. A common antedating action is backdating of electronic documents. Backdating documents is changing the date of a document, such as a business

CASE IN POINT

Paul D. Ceglia v Mark Elliot Zuckerberg, and Facebook Inc., 2012

This case hinged on the authenticity of a contract between Ceglia and Zuckerberg as it related to the development of Facebook. A forensic analysis was conducted resulting in conclusions that electronic documents and emails were manipulated and backdated.

contract creation date changed to an earlier date to gain a benefit. The benefit could be to cover knowledge of a crime or to benefit financially in a business dispute. Another example of backdating could be to create a suicide message after the fact, using a computer in an attempt to cover a murder. The printed date on a document is easy to manipulate and difficult to validate. The electronic time stamp is a different story.

Firstly, examining the metadata of an electronic file gives a baseline of information, whether or not the dates and times are authentic. Each copy or version of the documents under investigation will need the metadata extracted for comparison to create a historical timeline for each document.

In any document backdating investigation, being able to examine the machine on which the document was created may be the most beneficial source of information. Secondary items of evidence that the document may have been copied onto or emailed are also important as comparisons.

Documents which have been emailed as attachments create a credible source of information in the email headers. A document showing a creation date after an email date would be suspect as being modified. This example would be easy of course, but more important is building the timeline of historical relevance for the documents using all available information, including email header time stamps.

One method of manipulating document time stamps is through the use of software intended for altering metadata. Whether used for legitimate file management or nefarious purposes, these applications enable computer users with average skills to manipulate the time stamps on electronic files. One such example is seen in [Figure 11.1](#), showing the dialog box for *Stexbar*, an open source extension for Windows Explorer. This particular extension can be downloaded from <http://code.google.com/p/stexbar/> and easily installed. Once installed, computer users can change the metadata time stamps on any file by right clicking the file, choosing "properties," and selecting the TimeStamps tab to alter the metadata.

If the evidence in question is a file absent its respective computer on which it was created, validating the time stamps is problematic. More information is needed to validate the metadata. By examining the computing system, recovering time stamp information from the Master File Table (MFT), which will contain the time stamp of when the last modification of the file occurred ("Entry Modified"), when the file's attributes have changed, along with information on other actions affecting the evidence file.

Changing the computer time before creating an electronic document is another method of antedating, as the metadata for the newly created electronic file will be based on the incorrect setting of the system. Antedating using more than

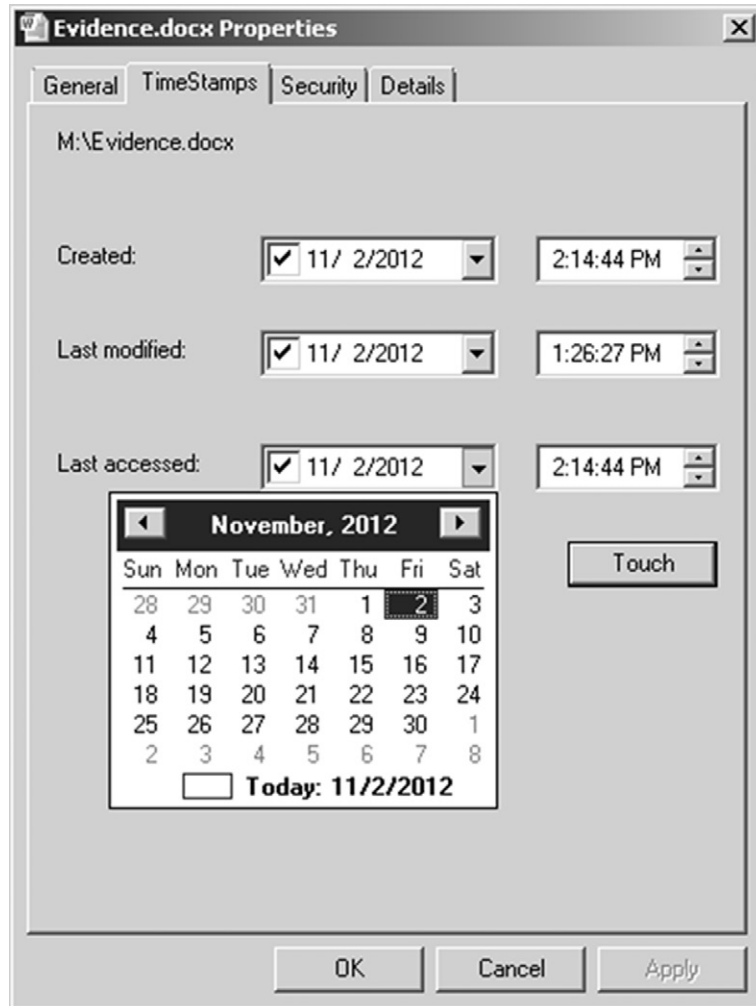


FIGURE 11.1 Stexbar, a Windows Explorer extension allowing an easy method of altering a file's time stamps.

one means only complicates an analysis. Once there is doubt to the validity of any file's time stamp, the computer system must be analyzed to correlate dates and times as well as determine if a suspect manipulated the system.

Internet web browsers are full of time stamped records from reliable sources such as from an Internet Service Provider or website. These can be compared to files on the system in relation to the evidence files. Event logs in Windows are also a great source of information to determine if antedating occurred,

such as the system logging a computer clock change. Other log files, like anti-virus program logs, may also have time stamps to help correlate activity on the system.

Generally, antedated documents are made with a substantial gap in the actual date and time compared to the altered date and time. For these situations, the differences are obvious. For situations where the time gap may be small, finding the differences requires attention to minute detail. Also, the time stamps of files do not change consistently. Depending upon how a file was copied or moved, will affect which time stamps are modified. Time stamps can be updated when extracted from a zip file, downloaded from the Internet, or moved to a folder when using the command line. Conversely, simply moving a file from one folder to another will not update the Create time.

The versions of software used to create a document give an indication if a file has been antedated. An example would be an evidence file, such as a Microsoft Word document which has been produced as authentic evidence in the file format of “.docx,” yet the claim is the document was created and not modified since the year 2001. The file format of the document is immediately questionable since it did not exist in 2001.

To antedate a file and make it appear credible, the suspect has to take into consideration the relation of the date chosen to backdate the file to the software and hardware used. Obviously, purchasing a new laptop in 2012, with the most current operating system and programs installed, will not be the best choice to create a file made to appear as if it were created in 2004. The file format type, metadata of the file, and system clock changes will each show any number of techniques to backdate the file.

When presented with a goal to validate time, you need to take into consideration the factors specific to the evidence in front of you. The operating system, the method of file creation and movement, log files, and even the printed documents need to be correlated for discrepancies. Without an authentic timeline of events, including accurate file time stamps, placing a suspect at the keyboard is an extremely difficult task. First things first; develop the time line, and then take the steps to identify possible suspects.

False names and disposable email accounts

Scenario: A victim has been receiving harassing and threatening emails from an unknown person. The names used in the emails are false names and the email accounts are commonly used, free webmail accounts.

Investigative Tips: This case includes great examples of suspect elimination. Interviews, polygraphs, and searches of computers and emails eliminated most potential suspects, leaving Bruce Ivins as the prime suspect. From the

CASE IN POINT**FBI Anthrax Investigation (Arredondo 2008)**

Doctor Bruce Ivins, a biodefense researcher at the US Army Medical Research Institute of Infectious Diseases was suspected of mailing anthrax contaminated letters causing five deaths and injury to dozens of more people. Ivins used disposable email accounts with false names during the time of the anthrax attacks. Although Ivins committed suicide before being charged, he was the primary suspect in these anthrax attacks in 2001.

elimination of suspects, focus on Ivins resulted in obtaining the evidence needed to determine he had to be the suspect in the murders.

Techniques used to gather information on Ivins comprised pen registers on email accounts and telephones, search warrants on his residence and cars, covert collection of his trash, and the installation of GPS devices on his vehicles. The pen registers, or trap-and-trace, allow for investigators to have near real-time information on phone numbers called/received and email addresses of correspondence, but without accessing the content of either voice or data.

Doctor Ivins sent anonymous emails days before the anthrax attacks with the warning of "WE HAVE THIS ANTHRAX. DEATH TO AMERICA. DEATH TO ISRAEL." Linking these emails to Doctor Ivins required a pen register which revealed additional email addresses related to the case. Additionally, an email address was linked to an online posting on Wikipedia.

Following the trail of evidence on Wikipedia led to information obtained where Ivins communicated with others with an email having his real name in the name field of the email. Other emails believed to be owned by Ivins were identified, where Ivins was sending emails to himself, between email accounts.

The investigation of a single email address may lead to another email or to the identification of an online account with accurate user name information. The inclusion of IP address verification in your investigations is an important aspect if the IP addresses can be traced to an actual physical location. Otherwise, the investigative means will be to trace and follow emails through online sources such as online bulletin boards and forums to eventually end at the legitimate information of your suspect.

Evidence leads to more evidence

During the collection of storage media at a search warrant related to a gang shooting, a smartphone is seized. There are several computer systems to be examined and only one forensic examiner. Where do you start?

CASE IN POINT

State of Wisconsin v Brian Pierick, 2010

During a search warrant executed at a residence, two iPhones were seized along with other items. An analysis of the iPhones recovered sexually explicit chat messages with juveniles. Coupled with child pornography discovered on seized computers, investigators continued the investigation to obtain even more evidence of these crimes, including postings on Craigslist that were pertinent to the case.

Investigative Tips: The forensic examiner starts the first forensic examination first. Ideally, the first examination is the one that cries for attention as a priority. In one case, this could be the laptop. In another case, it may be the smartphone or a flash drive. All things being equal, the smartphone may be a good piece of evidence to search your examinations.

As in the case in point above, investigators not only examined the iPhones, but requested the call detail records which helped to identify victims. The analysis of mobile devices such as smartphones can yield a wealth of evidence and much of that evidence can place a suspect at any one location that has been either logged by GPS on the phone or through cell tower records. Being able to create a historical location and movement of a suspect helps prove or disprove alibis. It also helps to potentially identify locations where additional evidence may exist.

Although smartphones capable of geolocation through GPS logging or by embedding EXIF data in photos are incredible items of evidence for suspect locations, laptops may contain some of the same location information, as they are almost as portable as a smartphone.

As shown throughout this book, the combination of investigative techniques and forensic processes helps place the suspect at a location and behind a keyboard, but these same processes help find clues and lead to additional evidence and victim identification. Of course, there is always the question of how much effort to place in an investigation when there is enough evidence to prove an allegation in a legal hearing, but when unidentified victims exist, sometimes you should consider going the extra ten yards. The victims will appreciate your effort.

Searching for all the bad things

Scenario: The suspect is alleged to have planned the murder of his ex-wife to end paying alimony. After his arrest and search warrant of his home, a computer is seized for examination. The goal is to determine if evidence of the

CASE IN POINT

The people of the state of illinois v steven zirko, 2009

In this case, Steven Zirko was charged with first degree murders of two persons and the solicitation of murder. A forensic examination of Internet activity on Zirko's computer revealed evidence directly related to his charges. Internet searches for "killer," "nitrous oxide," "unconscious," "hire a hitman," and "hire plus mercenary" were performed by a computer user. Websites visited included www.hireahitman.com and www.gunshows.usa.com.florida.

The investigation showed that this computer belonged to the Zirko and he was not traveling during this activity on the computer. Considering the content of the websites visited, the search words used, and the timing of use, these items were determined to show intent and motive to commit the crimes and that it was Zirko that typed the search terms.

crime exists on the computer and determine if the electronic evidence can be tied to the suspect.

Investigative Tips: Intent, motivation, opportunity, and knowledge. Each of these constitutes factors to help identify a suspect. Typed URLs are clearly indicative of intent to at least view specific websites of interest. Typed search terms to find websites of interest also show intent. Other Internet and browsing activity which can show knowledge and intent includes bookmarking webpages, printing or saving webpages, and numerous revisits to specific webpages. Creating a timeline of Internet history can show determination to research a topic or attempts to find contraband online.

However, Internet history by itself doesn't have much weight as evidence unless it is tied to a suspect. Other than a computer belonging to a suspect, a process of elimination still needs to occur to narrow the list of suspects. A single family residence where a single person lives helps narrow the list of suspects having access to a computer. Multi-family homes and computers accessed by any person in a common area increase the amount of data to examine and decrease the ability to tie specific actions to a single person.

A method to help determine a specific user's activity on a computer is to examine another computer or device that the suspect has access. This can be an Internet enabled smartphone or work computer. Potentially, the Internet history on all devices will be comparable with each other. A suspect can be more easily placed at a job location than somewhere outside the workplace. Within the workplace, access to an assigned computer reduces the chance that only the suspect uses his assigned computer. Given a suspect can be placed at his work, on his computer where the same Internet bookmarks and searches were

conducted as on his home computer, his home use of the computer can be inferred.

So even as the intent of Internet searches is very relevant to an investigation, the searches of one computer at a work location, which mirror the searches of another computer at a home location, may effectively place that suspect behind both computers.

Scenario—threatening blog posts

A suspect has been making anonymous threatening posts on an Internet blog against specific persons. The posts are clearly death threats, yet the suspect is obviously using a false name. Depending upon how the suspect posted to the blog will determine the odds of being able to identify the suspect.

Investigative Tips: IP addresses can be gold in your investigation. Although to obtain the actual physical address requires law enforcement authority, being able to securely identify a physical address along with the subscriber of the Internet account is hard evidence to defend against.

Cybercriminals have become to know that their home IP address is not the Internet connection to use when committing a crime. Suspects that are unaware falsely believe that signing up for a free and anonymous webmail account means they are anonymous to the world. This can lead to the suspect creating evidence on a regular basis, such as posting comments on blogs, from their home, blissfully unaware that every log in and post is logged and waiting for an investigator to obtain.

But before you are too confident with IP addresses, there is still work needed to make sure you have the right suspect when based on any IP address. This additional work means you must do as much as reasonably necessary to ensure you are right, because if you are wrong based on erroneous information, nothing goes right.

CASE IN POINT

US District Court v Clifton Dwayne Brooks, 2012

Clifton Dwayne Brooks posted comments on an Internet blog threatening to kill Maricopa County Sheriff Joe Arpaio. Investigators sent emergency requests to the blog hosting company, Google Incorporated. Google responded with the email address blog poster, and afterward in response to a search warrant, provided the IP address used of the blog poster.

The IP address resolved to Comcast as the Internet Service Provider, who provided investigators with the physical address of their customer, Clifton Brooks.

Making the wrong kind of friends online

An unknown suspect attempts to lure children online for sexual exploitation by offering to be their friend. The only information about the suspect available a social networking user name given to you by a victim's mother.

Investigative Tips: Anonymous tips are like birthday presents. You never really know what is inside until you open it. But unlike a birthday present, an anonymous tip, if credible, can yield great cases. Rather than considering an anonymous tip as a nuisance, consider it a potential goldmine of a case, where you may be able to save a victim and prevent others from becoming a victim.

In this instance, the anonymous tip gave enough information to identify a person, but not enough information to constitute a crime. The investigation uncovered the criminal evidence because the investigator took an active, online undercover role. Forensic analysis doesn't usually come into play with an online investigation until physical electronic evidence is identified and seized.

A sexual predator case conducted through online chatting can be completed against a suspect without going beyond the evidence of the single online crime under investigation. However, by examining all of the suspect's electronic devices, past victims may be identified as well as any possible conspirators. Previously convicted sex offenders with Internet enable smartphones may even have created geolocation evidence on these devices by visiting areas ordered off limits by a court, such as playgrounds.

An investigation is not over until the investigator says it is over. Sometimes, investigators may close a case as soon as there is enough to bring charges so as to move on to the next case. Granted, some cases may only need limited evidence to succeed, but other cases, particularly where there are human

CASE IN POINT

US District Court, Eastern District of Wisconsin v Harry J Janikowski, 2009

Investigators received an anonymous letter with information that Harry Janikowski was involved in child molestation. All details in the anonymous letter were confirmed except for the child molestation allegations. To prove or disprove the allegations, investigators searched online for Janikowski on the MySpace website. Janikowski had a MySpace account and his photo on the MySpace user page matched his driver's license photo obtained from the Department of Transportation.

An undercover online conversation with Janikowski was initiated by an investigator that assumed the role of an underage boy. Chats and instant messages culminated in the probable cause in Janikowski's intention to meet the undercover officer to perform a sexual act. He was subsequently arrested.

victims, such as human trafficking investigations. It may be worth the extra effort during a forensic analysis in attempts to uncover more crimes and victims, just to make sure you do a good job for the victims that otherwise would have been ignored.

A break in the case, otherwise known as a suspect's mistake

Scenario: Suspect uses an anonymous email account to send a harassing email to an ex-girlfriend. The suspect attaches a word processing document stating numerous threats. After sending the email, the suspect learns about metadata and regrets his email.

Investigative Tips: There are investigations that cannot be solved. No amount of resources will do it. No amount of investigative skill will do it. No software or hardware will do it. These types of investigations just can't be cracked no matter how much effort is expended. That doesn't mean you stop trying.

There is a solution and that solution resides in your suspect's actions. Eventually, all suspects will make a mistake. Many of these mistakes go unnoticed, sometimes for 31 years. However, the astute investigator will have an ear to the ground in the event that a mistake is caught at some point. These mistakes are the "breaks in the case" that are unexpected and powerful. An example of metadata from a common document file is seen in [Figure 11.2](#). If the information in the metadata in this deleted file is accurate, then you would have the name of the suspect and potentially the name of his workplace, or at least the owning business of the computer used.

One search warrant in which I participated involved the seizure of a huge safe on the top floor of a multi-story home. The safe contained evidence and

CASE IN POINT

State of Kansas v Dennis Rader, 2005

Dennis Rader, also known as the "BTK Strangler" or "Bind, Torture, Kill," eluded law enforcement for 31 years. Rader murdered 10 people between the years of 1974 and 1991 and sent anonymous letters to the media and law enforcement detailing the murders he committed.

In one of his last anonymous letters, Radar mailed a computer floppy disk to the media which contained his usual message to the police. However, he had also created and deleted another document on the floppy using a computer at his church. Radar would later learn that the metadata in the deleted file was recovered by law enforcement and traced directly to him by name. In mere minutes, 31 years of anonymity as a serial murderer unraveled as BTK was identified as the President of Christ Lutheran Church. Mere minutes. Mere metadata. A 31-year-old case broke wide open in minutes because of metadata.

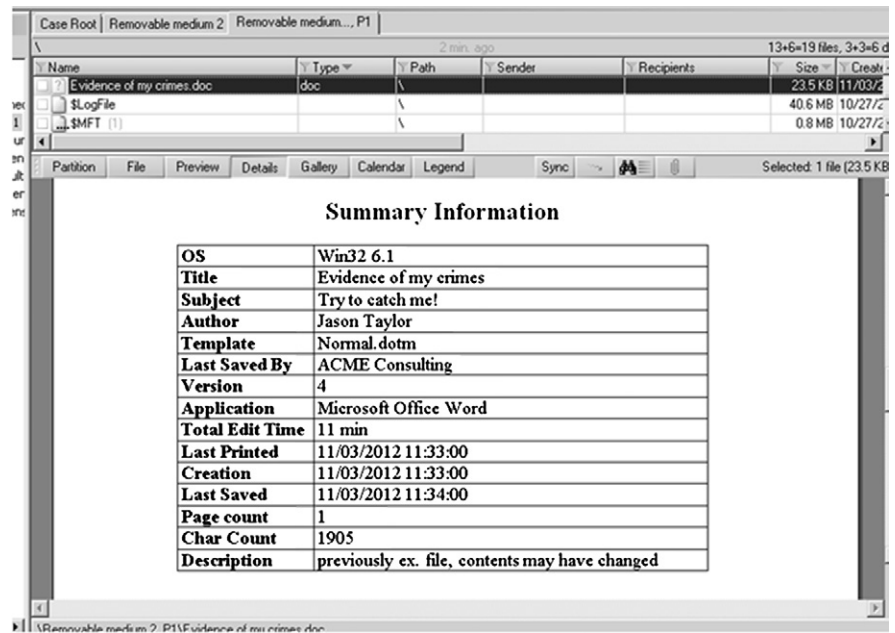


FIGURE 11.2 Metadata recovered from a deleted Microsoft Word document.

proceeds of crimes and was subject to seizure in the search warrant. Of course, the suspect did not cooperate or give us the combination to the safe. The result was a gaggle of cops dragging one of the heaviest items I've ever had to move down more than one flight of stairs and into the back of a truck. Shortly after loading the safe into a truck, the combination to the safe was found on a scrap of paper, lying on the kitchen table. It would have been nice to find that scrap of paper earlier, but at least the safe didn't have to be forced open with even more labor.

Encrypted data that may contain evidence is even more difficult to by pass than a locked safe. If a dictionary attacks doesn't open the files quickly, then the possibility of bypassing the encryption is low. [Figure 11.3](#) shows a spreadsheet from Mandylin Research Labs to obtain time estimates to by pass a password using brute force. In [Figure 11.3](#), the example shows that based on the complexity of this password, it could take over 182,000,000h to break.

The point in this example is not to discourage trying, but rather to encourage not giving up as you never know when the break (i.e. suspect's mistake) will occur. Perhaps the password chosen by the suspect in an evidence document is the same password you found written on a scrap piece of paper on the kitchen table. You just never know where or when you will find the break in your case.

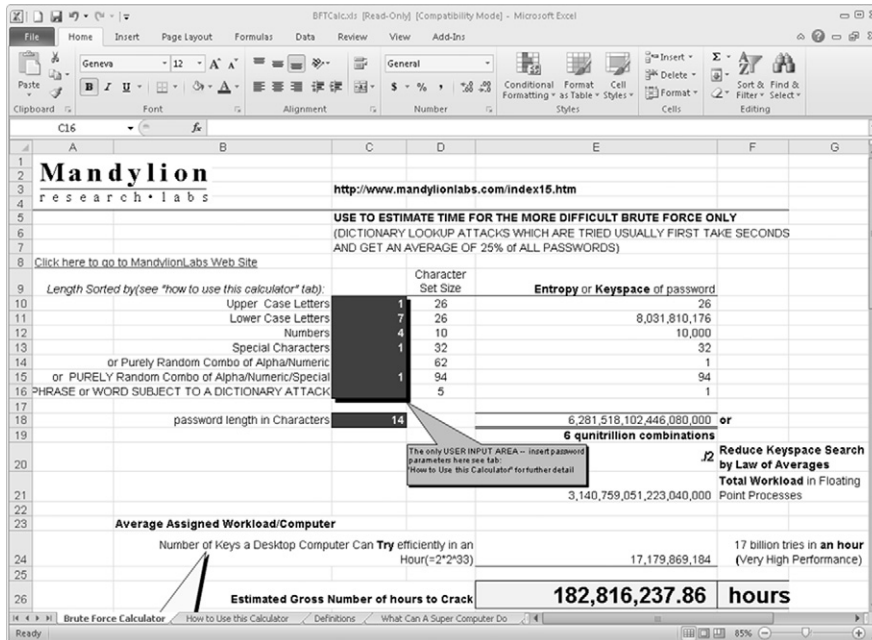


FIGURE 11.3 Spreadsheet calculator for brute force attacks, by Mandylion Research Labs, <http://www.mandylionlabs.com/>.

Breaks from the suspect may seem to be too good to be true. As in the BTK case, investigators believed that the BTK Killer may have been intentionally leading law enforcement on a wild goose chase, because the name “Dennis Radar” and the name of the church were in the metadata of a deleted document. The document even contained the word “encase,” which investigators thought was a reference to the forensic software program. The investigators thought BTK was taunting them through false leads. Surprisingly, “encase” ended up only being a misspelling for “in case.” Mistakes by the suspect are the best kind of mistakes to find.

Altered evidence and spoliation

Electronic evidence in the form of word processing documents which were submitted by a party in litigation is alleged to have been altered. Altered electronic evidence has become a common claim with the ability to determine the changes becoming more difficult. How do you know if an email has been altered? What about a text document?

Investigative Tips: All evidence needs to be validated for authenticity. The weight given in legal hearings depends upon the veracity of the evidence.

CASE IN POINT

Odom v Microsoft and Best Buy, 2006

The Odom v Microsoft and Best Buy litigation primarily focused on Internet access offered to customers in which the customers were automatically billed for Internet service without their consent. One of the most surprising aspects of this case involved the altering of electronic evidence by an attorney for Best Buy. The attorney, Timothy Block, admitted to altering documents prior to producing the documents in discovery to benefit Best Buy.

Many electronic files can be quickly validated through hash comparisons. An example seen in Figure 11.4 shows two files with different file names, yet their hash values are identical. If one file is known to be valid, perhaps an original evidence file, any file matching the hash values would also be a valid and unaltered copy of the original file.

Alternatively, Figure 11.5 shows two files with the same file name but having different hash values. If there were a claim that both of these files are the same original files, it would be apparent that one of the files has been modified.

The screenshot shows the HashMyFiles application window. The menu bar includes File, Edit, View, Options, and Help. The toolbar contains icons for file operations. The main area displays a table with the following data:

Filename	MDS	SHA1	CRC32
Not evidence.docx	d41d8cd98f00b204e9800998ecf8427e	da39a3ee5e6b4b0d3255bfef95601890afd80709	
Evidence.docx	d41d8cd98f00b204e9800998ecf8427e	da39a3ee5e6b4b0d3255bfef95601890afd80709	

The status bar at the bottom indicates "2 file(s)" and "NirSoft Freeware. http://www.nirsoft.n".

FIGURE 11.4 Two files with different file names, but having the same hash value, indicating the contents of the files are identical.

The screenshot shows the HashMyFiles application window. The menu bar includes File, Edit, View, Options, and Help. The toolbar contains icons for file operations. The main area displays a table with the following data:

Filename	MDS	SHA1	CRC32
Evidence.docx	d41d8cd98f00b204e9800998ecf8427e	da39a3ee5e6b4b0d3255bfef95601890afd80709	
Evidence.docx	6b7f4c2ffbcf4f1413a2cf0ef6ecf4aa	fec349c02f847deb421dc931861dbb0ce3954d9d	

The status bar at the bottom indicates "2 file(s)" and "NirSoft Freeware. http://www.nir".

FIGURE 11.5 Two files with the same file names, but having different hash values, indicating the contents are not identical.

Finding the discrepancies or modifications of an electronic file can only be accomplished if there is a comparison to be made with the original file. Using [Figure 11.5](#) as an example, given that the file having the MD5 hash value of `d41d8cd98f00b204e9800998ecf8427e` is the original, and where the second file is the alleged altered file, a visual inspection of both files should be able to determine the modifications. However, when only file exists, proving the file to be unaltered is more than problematic, it is virtually impossible.

In this situation of having a single file to verify as original and unaltered evidence, an analysis would only be able to show when the file was modified over time, but the actual modifications won't be known. Even if the document has "track changed" enabled, which logs changes to a document, that would only capture changes that were tracked, as there may be more untracked and unknown changes.

As a side note to hash values, in [Figure 11.5](#), the hash values are completely different, even though the only difference between the two sample files is a single period added to the text. Any modification, no matter how minor, results in a drastic different hash value.

The importance in validating files in relation to the identification of a suspect that may have altered a file is that the embedded metadata will be a key point of focus and avenue for case leads. As a file is created, copied, modified, and otherwise touched, the file and system metadata will generally be updated.

Having the dates and times of these updates should give rise to you that the updates occurred on some computer system. This may be on one or more computers even if the file existed on a flash drive. At some point, the flash drive was connected to a computer system, where evidence on a system may show link files to the file. Each of these instances of access to the file is an opportunity to create a list of possible suspects having access to those systems in use at each updated metadata fields.

In the Microsoft Windows operating systems, Volume Shadow Copies may provide an examiner with a string of previous versions of a document, in which the modifications between each version can be determined. Although not every change may have been incrementally saved by the Volume Shadow Service, such as if the file was saved to a flash drive, any previous versions that can be found will allow to find some of the modifications made.

Where a single file will determine the outcome of an investigation or have a dramatic effect on the case, the importance of 'getting it right' cannot be overstated. Such would be the case of a single file, modified by someone in a business office, where many persons had common access to the evidence file before it was known to be evidence. Finding the suspect that altered the evidence file may be simple if you were at the location close to the time of occurrence.

Interviews of the employees would be easier as most would remember their whereabouts in the office within the last few days. Some may be able to tell you exactly where other employees were in the office, even point the suspect out directly.

But what if you are called in a year later? How about 2 or more years later? What would be the odds employees remembering their whereabouts on a Monday in July 2 years earlier? To identify a suspect at this point requires more than a forensic analysis of a computer. It will probably require an investigation into work schedules, lunch schedules, backup tapes, phone call logs, and anything else to place everyone somewhere during the time of the file being altered.

Potentially you may even need to examine the hard drive of a copy machine and maybe place a person at the copy machine based on what was copied at the time the evidence file was being modified. When a company's livelihood is at stake or a person's career is at risk, leave no stone unturned. If you can't place a suspect at the scene, you might be able to place everyone else at a location, and those you can't place, just made your list of possible suspects.

Spoofer call harassment

Scenario: An unidentified suspect continually calls a victim with harassing phone calls. The caller's phone number changes constantly. The phone numbers appear to be fake, or spoofed, numbers. Where do you start?

Investigative Tips: Spoofed calls that are criminal acts, such as conveying threats or harassment, have a devastating effect on the victims. As anonymous as it may feel to the victim, there are actions you can take to help identify the suspect, as long as legal authority exists to demand records.

CASE IN POINT

United States District Court, Western District of Washington at Tacoma v Daniel Christopher Leonard, 2010

A victim was receiving harassing phone calls from a spoofed telephone number. Investigators searched the Internet for spoofing services and discovered the service that was used to spoof these calls. This was based on the victim's phone number existing in the spoofing services logs. A search warrant to the spoofing service provided billing records and call logs related to the victim's phone number. Information provided included the suspect's billing information, date of the account being created, address, and a log of every call made. In this case, there were a total of 1566 calls made.

A spoofed call requires Internet access at some point to at least create an account. This will be important later in the case during a forensic analysis of any seized computer system or smartphone. Although there are free services to spoof phone calls, many of these limit the length of the spoofed call to a few minutes or less, and may only allow one call to be made. Therefore, where there are many spoofed calls being made, the assumption is that an account has been created, a credit used, and at least one legitimate phone number used for the spoofed calls.

As mentioned, at least one legitimate phone number is needed to make a spoofed call. The legitimate phone number, whether it is a landline or cell phone, calls the target and the spoofing service changes the number seen on the target's Caller ID. The evidence trail includes the calling logs maintained by the spoofing service, the credit card information used to purchase the service, the IP addresses recorded to access the spoofing service website, and the call detail records of the suspect's phone used. The call detail records and cell phone itself may provide geolocation records too.

The obstacles placing a suspect with the spoofing phone are only as difficult as the suspect makes it. If the suspect is unaware of the records kept by the spoofing service, and creates an account online using a home computer, their own credit card, and their personal cell phone or landline, the investigation will be fairly quick and easy. The amount of electronic evidence generated across third party providers such as the Internet Service Provider, phone service provider, and credit card service coupled with a forensic examination of the suspect's computer and phone should yield more than enough evidence to close the case with charges. The methods of placing a suspect at specific locations with specific electronic devices fall right in place with this type of electronic communication crime just as it does with an online crime.

However, each step the suspect takes to hide his identity creates extreme difficulty in identifying the suspect. As Internet access is needed to create an account with a spoofing service, public Internet terminals could be used to avoid the suspect disclosing his home or work IP address. Pre-paid credit cards can be used to purchase the spoofing service, thereby avoiding his true name being used. A pre-paid credit cell phone would allow a method where the suspect could dispose of the phone on a regular basis and replace with another. None of these actions require the suspect to use accurate personal information.

But this does not mean the case is impossible. Besides hoping for a break caused by the suspect, the same methods of identifying the physical phone being used and the IP address logged by the spoofing service provider apply. Call detail records of a pre-paid cell phone still yield information with other numbers that may have been called which were not spoofed. Perhaps the suspect called

home using his disposable phone, or perhaps the cell tower records give a geo-location that may help identify the suspect.

Once a list of possible suspects is developed, placing the list of suspects at locations as calls have been made will be helpful in reducing the list of suspects. Potentially, the victims in these cases have met the suspect at one or more points in their life, either as friends, acquaintances, or in passing.

Disgruntled employee steals and deletes employer's data

Scenario: An employee, unhappy with his current employer, decides to copy company information consisting of client files and confidential product information onto an external USB hard drive. After he steals the information, he proceeds to delete folders from the company server. A few months after leaving his company, the former employee starts his own business using the stolen information.

Investigative Tips: Intellectual property (IP) theft by employees is a serious threat to any business. The security of information by an organization requires that employees be able to access the information needed to perform their duties, while at the same time, the employer has no option but to trust the information not be stolen. Non-disclosure agreements, employment agreements, and promises do not prevent the theft of IP as it only helps litigate the damage afterwards.

If a suspect has not already been caught with stolen IP, the first course of action is to determine which data has been stolen, when it was stolen, and which persons had access during those times. Many large or high tech companies secure confidential data through a series of safeguards. One safeguard could be allowing the fewest persons necessary to have access to the data. Another safeguard is requiring a series of secure logins to access the data, which every login is recorded with as much detail as possible.

In cases where the company employs a high level of security, identifying those employees with access requires a review of the logs showing access to the files.

CASE IN POINT

United States of America v Biswamohan Pani, 2008

Biswamohan Pani was an employee at Intel. While working for Intel, he gave a resignation notice and while on leave from Intel, obtained a job at AMD, a competing manufacturer of computer chips. Having access to both AMD and Intel at the same time, Pani copied electronic files from Intel to an external hard drive. Pani's intention was to use the stolen files to benefit his new position at AMD.

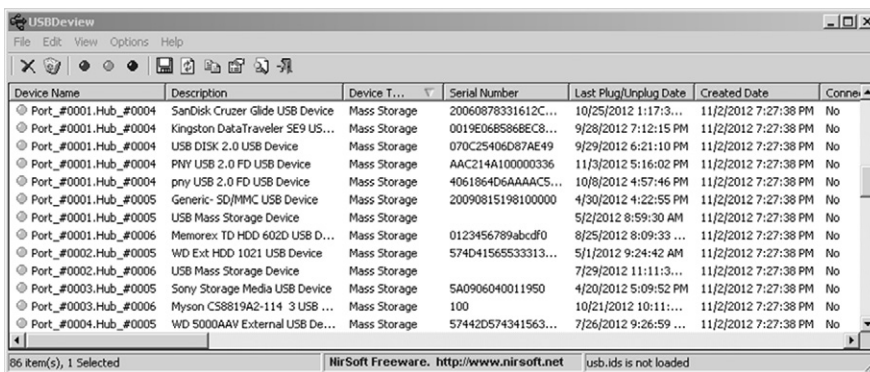
Files in question that were accessed can be collected in order to create a hash database and listing of the files. This list and database can be compared against any storage media devices of possible suspects for matches of identical or near identical files.

In companies where computer security is not as secure requires more hands on effort. In an office in which an employee can access multiple computer systems and access file servers that do not require individual login credentials requires additional work beyond the examination of the computer systems. The suspect that does not want to use their assigned workstation most likely will use an external hard drive or USB flash drive to copy files using another employee's computer. This could also be in an attempt to frame someone else for IP theft.

Since files can easily be copied onto a flash drive, leaving no visible trace by an average computer user, obtaining a list of all USB device information from suspected computers is paramount to start developing leads.

Collecting information about any attached USB storage devices across a broad spectrum of computers allows you to build a timeline of device travel across the computers. As an example, a suspect using his own flash drive to copy files by connecting the flash drive to a co-workers computer leaves traces of that activity on the co-workers computer. One of the artifact traces is the serial number of the flash drive. It would be expected that the suspect would have connected that same USB device in his own assigned workstation or his personally owned computer before copying the files and certainly after copying the files.

Figure 11.6 shows a collection of information about USB devices obtained from a computer system. If a different computer system showed any of the



Device Name	Description	Device T...	Serial Number	Last Plug/Unplug Date	Created Date	Conne...
Port_#0001.Hub_#0004	SanDisk Cruzer Glide USB Device	Mass Storage	20060878331612C...	10/25/2012 1:17:3...	11/2/2012 7:27:38 PM	No
Port_#0001.Hub_#0004	Kingston DataTraveler SE9 US...	Mass Storage	0019E0685868EC8...	9/28/2012 7:12:15 PM	11/2/2012 7:27:38 PM	No
Port_#0001.Hub_#0004	USB DISK 2.0 USB Device	Mass Storage	070C25406D87AE49	9/29/2012 6:21:10 PM	11/2/2012 7:27:38 PM	No
Port_#0001.Hub_#0004	PNV USB 2.0 FD USB Device	Mass Storage	AAC214A100000336	11/3/2012 5:16:02 PM	11/2/2012 7:27:38 PM	No
Port_#0001.Hub_#0004	pry USB 2.0 FD USB Device	Mass Storage	4061864D6AAAAC5...	10/8/2012 4:57:46 PM	11/2/2012 7:27:38 PM	No
Port_#0001.Hub_#0005	Generic - SD/MMC USB Device	Mass Storage	20090815198100000	4/30/2012 4:22:55 PM	11/2/2012 7:27:38 PM	No
Port_#0001.Hub_#0005	USB Mass Storage Device	Mass Storage		5/2/2012 8:59:30 AM	11/2/2012 7:27:38 PM	No
Port_#0001.Hub_#0006	Memorex TD HDD 602D USB D...	Mass Storage	0123456789abcd0	8/25/2012 8:09:33 ...	11/2/2012 7:27:38 PM	No
Port_#0002.Hub_#0005	WD Ext HDD 1021 USB Device	Mass Storage	574D41565533313...	5/1/2012 9:24:42 AM	11/2/2012 7:27:38 PM	No
Port_#0002.Hub_#0006	USB Mass Storage Device	Mass Storage		7/29/2012 11:11:3...	11/2/2012 7:27:38 PM	No
Port_#0003.Hub_#0005	Sony Storage Media USB Device	Mass Storage	5A0906040011950	4/20/2012 5:09:52 PM	11/2/2012 7:27:38 PM	No
Port_#0003.Hub_#0006	Myson CS8819A2-114 3 USB ...	Mass Storage	100	10/21/2012 10:11:...	11/2/2012 7:27:38 PM	No
Port_#0004.Hub_#0005	WD 5000AAV External USB De...	Mass Storage	57442D574341563...	7/26/2012 9:26:59 ...	11/2/2012 7:27:38 PM	No

FIGURE 11.6 A list of USB devices collected using USBDeView, <http://www.Nirsoft.net>.

same devices, then those devices were connected to both systems. As the time stamps of connection are available, an analysis of the files created or accessed after the device being connected can show the files that may have been copied.

Visual depictions of USB activity across systems make an effective impact as to the suspect's physical actions as compared to a spreadsheet of the activity. Figure 11.7 shows a simple diagram of one USB flash drive connected to three computers and the files accessed. In this example, without explaining anything other than showing the movement of the flash drive, an assumption would be that Taylor connected his flash drive to Smith's workstation, copying files. About a half hour later, he then connected the flash drive to his computer and opened several files, probably to make sure the files copied correctly. Finally, later in the evening, he connected the same flash drive to his home computer, copying the files onto it.

This graphic strongly implies Taylor is the suspect and is probably correct. Effectively, Taylor has been placed at three different locations by mere use of his USB flash drive. If Taylor used this same flash drive across many other computers in the company, it would be that much more impactful as a graphic representation of his movements and activity.

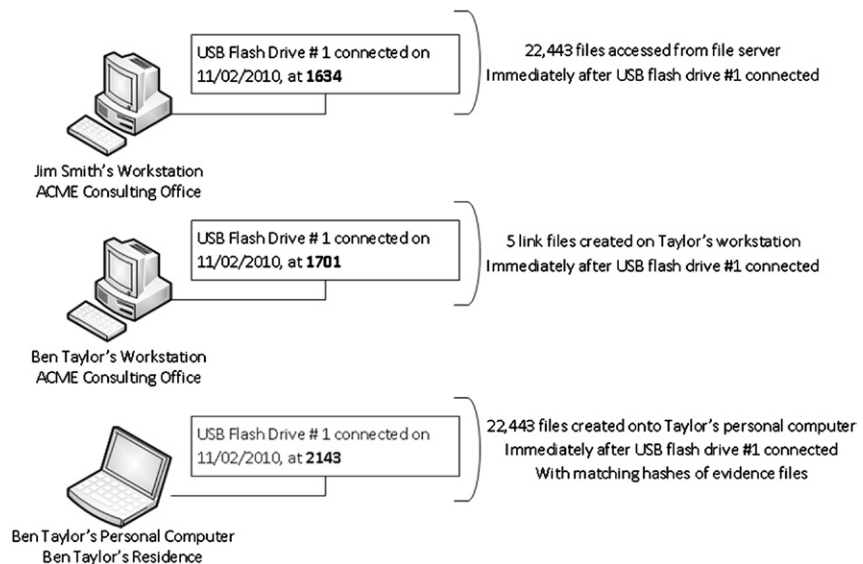


FIGURE 11.7 An easy-to-understand flow of historical USB history, as it was connected to three different computers.

Another method of IP theft includes the suspect emailing copies of files as attachments using web-based email to his own email or to others. Webmail evidence can be recovered from systems, but will not be as complete as having legal access to the webmail account through the provider. IP can also be copied by physically copying pages of paper, where the originals never leave the premises. Most modern copy machines have standard hard drives where images of each copy made are stored.

The forensic analysis of a copy machine hard drive could show IP being copied, such as computer-aided design (CAD) drawings, which may have had no reason to be copied by an employee. If CAD drawings were being copied, it can be suspected that these same drawings could have been stolen, causing an investigation into determining which employee was copying the drawings at that time. The goal then becomes placing the suspect at a copy machine, which could be more difficult than at a computer.

Missing evidence

Scenario: Suspect claims to have provided all electronic storage media, yet according to the forensic examiner, there are missing storage devices. Several devices that have been provided have never been connected to the suspect's computer and devices that have been connected were not produced. What is happening and how do you keep track?

Investigative Tips: At some point of every investigation, you have to get a handle on the evidence, insofar as counting the evidence you have on hand and the evidence that you should have, but either has not been found or produced yet. Beyond the electronic storage devices you have in your possession for examination, there most certainly will be references in your current evidence media that point to other devices relevant to your case.

As the previous case study showed, one computer system had information that many storage devices had been connected to it, any of which may contain

CASE IN POINT

Justin Lee Firestone v Hawker Beechcraft International Service Company, 2012

Defendants claimed the Plaintiff copied or removed confidential information from the Defendants' computer system. A forensic examination of the Plaintiff's assigned computer was conducted and between eight and twelve USB devices were discovered to have been connected to the computer. Upon request, the Plaintiff produced USB devices, but not all the devices that were found to have been connected to the computer.

evidence. Your list of evidence should include evidence which you do not have but has been discovered as attached devices, such as USB flash drives. These removable devices connect computers together and connect suspects to computers by sharing connections at different times. One flash drive, possessed by a suspect that has been shown to have been connected to multiple computers, shows a nexus between the suspect and all the systems by way of the flash drive connections. This also helps place a person at a specific location by date and time.

Almost by design, the hard drive you may be examining contains a listing of every device connected to that system. This includes the name, serial number, dates and times of connections, and a plethora of details to help you create a list of evidence items that you do not have. For the most part, this information is found in the Windows registry and in some logs, such as the `setupapi.log`. Two of the most comprehensive sources of guides for USB forensics come from Colin Cree's *Tracking USB Storage Devices*, and Rob Lee's *Guides to Profiling USB Keys/Thumbdrives* (Lee 2009). Both of these resources cover all things "USB" in regard to forensics and the information you can glean from their artifacts left behind in a computer system.

In reality, the production of every storage device ever connected to a computer system may be impossible. Flash drives, especially the micro size variety, are easily lost or misplaced. Flash drives are sometimes shared among co-workers and they eventually fail and are thrown away. Co-workers sometimes will use another person's computer, plugging in a flash drive during that time to save a file, and the assigned user may never know that a flash drive was just logged in their system's registry. Time and proximity of use should guide common sense as to if an external storage device is relevant, as a flash drive connected only once 4 years prior to an incident may not exist today.

Bomb threats by email

Scenario: An anonymous suspect emails bomb threats to a local high school. The email used is a freely available webmail. A search warrant for IP address information for the email shows origination from another Russia, yet the contents of the email appear to be created by a person local to the area. It appears that an Internet proxy was used to obscure the actual IP address. The odds of tracing the email through anonymous proxy servers are too low to even try. What to do?

Investigative Tips: In cases where there is a threat to public safety, such as a bomb or weapons of mass destruction threat, consider a wiretap on the account, or using CIPAV or similar spyware. Not every threat is credible, but every actual incident that was preceded by a threat, was. Taking chances that a threat may not be credible could end in a preventable tragedy.

CASE IN POINT

FBI “timberlinebombinfo” Investigation (Sanders & Western District of Washington. 2007)

Former Timberline High School student, Josh Glazebrook sent, multiple threats of bombs using email and enticing others to link to the suspect’s MySpace page. The IP address was obtained from the emails and comments, with the location being a compromised computer in Italy. The FBI obtained a search warrant to remotely and covertly install a spyware to the MySpace account. The spyware, Computer & Internet Protocol Address Verifier, or CIPAV, to be installed on the account would send the FBI information about the suspect once the suspect logged into the account. This would include the actual IP address of all outbound and inbound communications, MAC address of the network device used, open ports, running programs, last visited URL, and logged in user.

In conjunction with attempts to place tracking code or spyware on the suspect’s machine, online searches for any related information may be helpful. For example, given a suspect’s user name, a search across the Internet for that user name may result in finding a posting or comment with the same user name. Identifying that person to either rule out the possibility or confirm the possibility of being the suspect is worth the effort. There is always the possibility of the suspect making mistakes. A suspect may use the same account in threats as in an innocent comment on an online forum, but without using a proxy to hide his IP address. That one post with the real IP address could resolve directly to your suspect’s physical address.

Another method would be to collect any other Internet users with a connection to your suspect. Forums, social networking sites, and bulletin boards may all provide clues to the suspect’s identity through associations with others. Some associations online may be personal contacting the suspect and worth giving a second look.

ID the suspect

Scenario: An unknown suspect is wreaking havoc on network systems with denial of service attacks on several local government agencies. The suspect continually posts his exploits online in various hacker forums. All IP addresses lead to locations all over the world, obviously none being the suspect’s actual IP address. How to make it stop?

Investigative Tips: Never underestimate the power of a suspect’s mistake and arrogance, but also, keep in mind that you have to find the mistakes to be useful. In this case study, an investigator had to know that metadata might exist in the photo of Ochoa’s girlfriend, and then take the effort to

CASE IN POINT

United States of America v Higinio O. Ochoa III, 2012

Higinio Ochoa gained unauthorized access to a police department's entire user database containing usernames, passwords, and personal information of the law enforcement employees in the agency. This information was posted online and resulted in threatening phone calls to several police employees. Ochoa also posted taunting comments on Twitter about the intrusion. On one of the postings, a photo of a female taken from the neck down, in a bikini top with a sign on her skirt reading, "PwNd by w0rmer & CabinCr3w < u BiTch's!," an obvious taunt to investigators. The sign is shown in Figure 11.8.

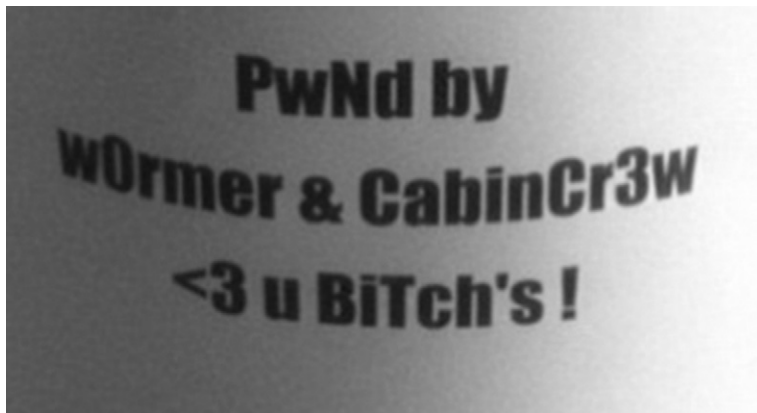


FIGURE 11.8 The taunting message pinned to skirt of Ochoa's girlfriend, ultimately leading to his capture.

Ochoa may not have realized at the time, but the photo contained embedded metadata that included geolocation information, pointing to an address in Australia. Further investigation found an Internet posting by the user name "w0rmer" on a software programming website. The posting was signed "Higino Ochoa AkA w0rmer." A further search for information on Ochoa led investigators to Ochoa's Facebook page, in which his profile listed Ochoa being in a relationship with Kylie Gardner, who lived in Australia. Other information was developed leading to the identification of Ochoa, but it was the EXIF metadata of Ochoa's girlfriend photo that 'broke the case' by giving investigative leads to Ochoa's identity.

check. Had this not been done, Ochoa may still be hacking into government databases.

Still, these mistakes may not come to light and other investigative means need to be started. Basic Internet searching can result in some useful information. Advanced searching more than likely will yield better information. Using the information at hand, such as a user name, email address, or even a tagline of a

suspect could have a hit somewhere on the Internet. An Internet forum, online club, or social networking site could each hold the one key piece of information leading to the identity of the suspect.

If not the suspect, the friends and family of the suspect could lead to the identification. A friend of the suspect could innocently brag about an incident perpetrated by his friend the suspect, in an online forum or social networking site. The identification of a known associate or family member can quickly lead to the suspect through interviews or more detailed online investigation of the friend.

Online extortion

Scenario: Suspect extorts victims by holding gaining control of their computers and encrypts the victim's data offering to decrypt it in exchange for fund wired to an overseas account. The suspect communicates via email and threatens to wipe the data or expose personal information publicly if payment is not made or the victims contact law enforcement. As this is all conducted online, you assume that there can be dozens or hundreds of victims being extorted by one suspect.

Investigative Tips: As mentioned before, consider pen registers on email addresses in hopes of discovering a lead through other email addresses of correspondence. As in many cases, online investigations through social networking sites, forums, and blogs usually will lead to your suspect. Sooner or later, suspects will create a link between that information which is legitimate to that which is their anonymous identity.

CASE IN POINT

United States of America v Luis Mijangos, 2010

Scenario: Luis Mijangos infected computers with a malware that allowed him to gain control of the computers of more than 100 computers, affecting about 230 people including dozens of juveniles. He also installed keylogging software on the victim computers, stealing their credit card numbers and personal information, which he used to make credit card purchases. Mijangos covertly recorded videos of the victims, in compromising and intimate acts. Mijangos demanded the victims to create and send sexually explicit videos to him or he would release the videos he made online.

As investigators were able to obtain his email from the victims, a search warrant of the email address identified the victims of Mijangos through the emails produced. Further investigation led to domain names associated with the email address that was registered in the name of Luis Mijangos. The break in the case was Mijangos apparently not aware his email address was associated with several of his registered domain names that used his real name.

Once a possible suspect is identified, investigative methods to place him behind the keyboard can be put into play, using any of the techniques in this book or with an ingenious method you might create.

Placing suspect at a location

Scenario: An identified suspect in a hacking case denies being at a location determined to be the origin of an intrusion based on an IP address. A forensic examination of the suspect's computer does not turn up any information as being used in the crime. How do you place the suspect at any of the locations used to access the Internet during the crimes without electronic evidence to support this belief?

CASE IN POINT

United States of America v Timothy James McVeigh, 1995

Timothy McVeigh was convicted of bombing the Murrah Federal Building in Oklahoma City, Oklahoma in 1995. The evidence in the case was substantial, with a large focus on the historical locations of McVeigh during the planning and commission of the bombing. Of particular note is that McVeigh was captured on at least one security camera prior to the bombing. The Ryder rental truck used in the bombing can be seen in the snapshot of security footage in Figure 11.9 as it drove past a hotel. Although McVeigh cannot be seen in the truck, a combination of evidence placing McVeigh at the rental truck company and other locations shows that this security camera caught McVeigh in the truck.



FIGURE 11.9 Security footage of the Ryder rental truck occupied by Timothy McVeigh prior to the bombing of the Murrah Federal Building, <http://law2.umkc.edu/faculty/projects/ftrials/mcveightrial.html>.

Investigative Tips: Think outside the CPU. Placing your suspect at the scene of a crime and in particular, behind a keyboard, requires thought as to the many ways this can be accomplished outside of a forensic analysis of a computer. If the actual location is known through an IP address where the suspect accessed an Internet connection, it is only expected that you visit the scene to visually inspect the location. Are there security cameras inside the business? Are there security cameras in the parking lot? Does any adjacent business have security cameras? Are there red light cameras? In the businesses, do the employees seem to take notice of their customers? Perhaps they would remember your suspect and be able to pick out his photo from a montage of photos. You will only be able to answer these questions by surveying the location personally.

If the crime scene location does not have security cameras, perhaps the suspect also used an adjacent business for an unrelated purpose, such as a gas station. Any of these businesses may have caught your suspect on video. Also, if the suspect was security conscious, he certainly wouldn't use his credit card at the same coffee shop that he would be committing online crimes. That doesn't mean he wouldn't use his credit card across the street to fill up his car with gas or buy a pack of cigarettes.

Placing the suspect at an Internet café without evidence that he even had a computer with him at the time is not worthless. If he can be placed at the location, with or without a computer, this one fact placed before him could discredit an alibi and lead to an admission of guilt. You just don't know which piece of the puzzle will end up breaking the case wide open, so you try one by one until you find the piece that fits.

Placing the suspect in the office at a specific location

Scenario: An employee is suspected of accessing classified information, copying electronic files, and taking photos of confidential products under development. Unfortunately, he denies all claims of being in the area of the information. Sometimes this is an easy task, other times, a bit more difficult.

Investigative Tips: With many workplaces, there is usually some physical action needed to move about the area. Sometimes a RFID badge is needed to unlock doors or a door must be opened by a Security Officer upon display of identification and signing in. Some workplaces may have security cameras covering all areas while other workplaces may only have a security camera in the employee parking area for safety.

With a small location, an investigation may take only a few minutes to determine if there are any records of employee movement at all, besides perhaps a punch card. Other workplaces may be extensive in geography, open Wi-Fi access, and unrestricted access to all areas. Regardless of the workplace, the

CASE IN POINT**United States District Court for the Eastern District of Virginia v Robert Philip Hanssen, 2001**

Robert Hanssen pled guilty to 13 counts of espionage and was sentenced to life in prison without the possibility of parole for anthrax attacks. During the investigation, evidence of his movements and locations at his workplace were recovered through tracking logs. These logs were made possible as badge readers were used to access secure areas of the laboratories. The logs recorded both the entry and exit of persons based on the badge readers, including Hanssen.

An analysis of Hanssen's entries into the secured areas showed that his access to areas containing anthrax was unusual. The hours of entry were beyond his normal work hours and many times, he was alone. The fact that Hanssen had unobserved access to these secure rooms that contained anthrax along with other evidence obtained in emails by Hanssen gave solid evidence that he was a suspect in anthrax attacks through the mail. It would have been unbelievable if Hanssen claimed he never accessed the secure rooms since he possessed his badge reader and worked in the facility.

best method of determining how an employee moves about is to move about in that area as if you were an employee.

In a case where an alleged cybercrime occurred on a commonly accessed computer workstation, being able to understand who may have access to the workstation based on any recorded activity will help narrow the list of suspects. The recorded activity could be security cameras, entering passcodes to locked doors, or being seen by other employees that remember the suspect being at the computer on a certain date, at a specific time. Computers used in a cybercrime, in which many employees have open access, require determining their whereabouts during the incident. Obviously, this is a lot of effort, but if you want to narrow your list to one possible suspect, it is more than worth the time.

Stolen property

Scenario: A burglary victim finds items for sale on the Internet that appears to be her stolen property. In one of the photos posted in the classified, the floor looks to be the same floor in her home as if the burglar took photos of the property in her home. Easy enough, but let's take it a little further.

CASE IN POINT**State of Missouri v Gary D Heggins, 2012**

A victim of theft searched online for his stolen bicycle and lawnmower. He found the items for sale on a classified ad website and contacted the seller to purchase the items. Instead of buying his own property back, he called the police, who then arrested Heggins for Burglary.

Investigative Tips: Just as you shouldn't discount a suspect's mistakes, you should also not underestimate the effort of a victim trying to find their property. In the scenario of a victim finding their property for sale through the Internet, the easiest resolution for law enforcement would be arrange a meeting place with the seller/criminal, and make an arrest upon finding the property was stolen.

Taking this a step further, consider that the items for sale may not be the only stolen items in possession, nor is this one victim the only victim. The goal is to resolve more than one case and give more than one victim closure. The common thread with investigations involving the Internet is obtaining IP addresses and this type of investigation is not different. Online classified advertising websites typically require the user to create an account before posting an advertisement. This process captures the IP address of the user, which may lead directly to the physical residence through search warrants or subpoenas to the classified ad website service and Internet Service Provider.

This newly identified location might contain evidence of many crimes and the recovery of victim property. This location most likely will also contain one or more computer systems used to post the online ads. And don't forget the actual photos used in the ads. If they were taken by a smartphone, you may have a treasure chest of historical geolocation data in a phone that may have traveled with the burglar during commission of his crimes.

With a little elbow grease, you could solve a series of burglaries, recover dozens or hundreds of stolen items, and maybe even identify a conspiracy of burglaries through an analysis of the smartphone call detail records that was used by one burglar to communicate with other burglars.

IP addresses aren't enough

Scenario: You have been given a tip that harassing emails have been originating from several IP addresses. You have the name of the resident living at the addresses and decide to make an arrest based on the content of the emails. So, do you?

CASE IN POINT

United States Court of Appeals for the Ninth Circuit, Todd M. Chism v Washington State; Washington State Patrol, 2011

Investigators for the Washington State Patrol received a tip that child pornography was contained in a website. Warrants were served to obtain any IP addresses used to create and access the website as well as the names used. The results of the search warrants showed the name to be Mr. Nicole Chism. A search warrant on the residence of Todd and Nicole Chism was served where charges were filed. The end result of this investigation concluded that the IP address alone was not enough information for probable cause, particularly when the IP addresses did not resolve to the residence or workplace of either of the Chisms.

Investigative Tips: An IP address is not a person. An IP address alone most likely will not answer all the questions needed for your case. An IP address is a lead or a clue to where you can start. Sometimes it may point directly to a physical location in which the name of the subscriber is listed. But still, the IP address by itself does not mean the subscriber is your suspect.

IP addresses are extremely easy to manipulate through anonymous proxies. Even the use of an open Wi-Fi access point can provide misleading information as to the identity of the suspect. By all means, collect all the IP addresses related to your case, but treat them like the fragile eggshells they are. There are still Internet users that use Wi-Fi in their residences, without security configured. Even those home users that enable Wi-Fi security can still be compromised by a number of means by anyone determined to break their way into the network.

The easiest cases involve the suspect using his own Internet at home, with his real name and personal information. In today's world, it is common knowledge among cybercriminals to avoid using their own Internet service at all costs, and if possible, pin the crime on someone else by using an innocent person's Internet service. Placing a suspect behind the keyboard on IP address alone does not make for a solid case.

Planted evidence

Scenario: An employee at a business is accused of downloading child pornography on his work computer. He has also accused of emailing child pornography to his coworkers. During an interview with the employee, he flatly denies ever

CASE IN POINT

United States of America v Barry Vincent Ardolf, 2012

Barry Ardolf was mad at his neighbors, Matt and Bethany Kostolniks, so much so, he exacted an anonymous reign of terror for years on the family. Shortly after moving next to Ardolf, one of the Kostolnikses' very young sons was picked up by Ardolf and Ardolf kissed him on the mouth. The police were called by the Kostolnikes and Ardolf began his campaign of terror.

During the next 5 years Ardolf focused on revenge. He hacked into their wireless network by breaking the encryption password. Ardolf also created email accounts and social networking sites in the name of Matt Kostolnikes without his knowledge or permission.

Ardolf, using the Kostolnikeses' IP address, sent sexually explicit emails to Matt's coworkers. He uploaded child pornography to the MySpace page created with Matt's name. Ardolf also emailed threats to the Vice President of the United States, the Governor of Minnesota, and a US Senator. Ardolf also emailed child pornography using the email account he created with Matt's name.

A forensic examination by the Secret Service, which included examining the Internet traffic on the Kostolnikes' network, showed that their neighbor, Ardolf, was the suspect. A search warrant for Ardolf recovered more than enough information needed to prove.

even seeing child pornography or having anything to do with the allegations. Is there something that sticks out in this case?

Investigative Tips: If something in your investigation doesn't seem right, it probably isn't. In the scenario above, where an employee denies sending emails containing child pornography using his work provided computer, does it make sense? Is this something a person would do, at work, where the network oversees computer activity?

This type of allegation where the acts do not fit the alleged suspect should scream out that something is wrong. As with the Kostolnikes case, the all too obvious criminal contraband posted publicly on the Internet along with emailing contraband to others using a real name doesn't seem plausible. Of course, it can happen, but given the background of the alleged suspect and the audacity of the crimes that are obvious attempts to bring law enforcement attention, what is the motivation? Consider that the planting of electronic evidence is a simple process. A flash drive containing contraband can be connected to a computer perhaps that of a supervisor at a company, and the files copied onto the supervisor's computer by a disgruntled employee. Later, an anonymous 911 call results in the supervisor having his computer seized and his reputation slandered, not to mention having potential criminal charges. Hacking or accessing a home owner's Wi-Fi can lead to the same type of allegations or worse.

When working to place the suspect behind the keyboard, be aware that the suspect you have identified may be an innocent victim, chosen by the actual suspect. Verify. Validate. Corroborate. Double-check. You have nothing to lose by doing a thorough job and a lot to lose if you don't.

THE LIFE AND CASEWORK OF A CYBER INVESTIGATOR

This investigative field is not just digital forensics. This field encompasses all things digital, not just computers, from the flash drive to a global network. Our personal electronic devices become interconnected and our personal devices connect to the devices of others around the world instantly, sharing information. Each person has their own personal virtual network consisting of social networking websites, home networks, work networks, and mobile devices connected wirelessly to their personal networks.

Of course this doesn't help explain to a client or case agent that even if digital forensics on a hard drive may be easy, but proving a particular person was at that keyboard is not. There are many factors to consider beyond the electronic data to build enough circumstantial evidence identifying the suspect.

So from now, take a different look at your suspects. Look at each suspect as having their own personal network of connectivity between devices and people. There are connections to be found. A connection that links your suspect to a crime could be an IP address or a username or a posting on a blog. There certainly will be a connection between the victim and suspect, at least an electronic connection. Just make sure the connections are real and not planted as red herrings to mislead your investigation.

Technical knowledge and skills

The vast amount of technical knowledge needed to place a suspect behind a keyboard makes this task difficult. No longer are cybercrime investigations just the forensic analysis of a computer hard drive. Cybercrimes require the identification of any and all devices connected to the crime which can be any number of devices and many different types of devices. Smartphones, tablets, flash drives, and digital cameras add to the complexity of cyber cases if not just for the sheer number of devices involved but also the technical skills needed for analysis.

Today's cybercrime fighter must have an overall grasp of how any electronic device may be used to facilitate a crime as well as having specific and specialized knowledge to examine these devices. Just as one device may contain evidence that supports allegations, another device may give evidence that is exculpatory to those allegations. Keeping up with technology is challenging when you are constantly trying to keep up with your cases. So what can you do to keep up with your skills?

One of the ways to keep up with your analysis skills is to modify your reading habits. Instead of reading a fictional love story, read a non-fiction book on file systems. Find and evaluate the casework of others, either found online or in your own office. Review cases you have completed in the past and see if there is anything you would do different today. Maybe you have since learned new methods or now use better software that could have resulted in better results. To keep up on your skills means evaluating and improving yourself constantly.

One of the quickest methods of learning about a newly discovered forensic artifact or method is through the sharing of others. Many of us painfully learn from our own mistakes while some of us choose to learn from the mistakes of others. Those that have suffered through a forensic analysis and solved difficult problems usually tried many different methods and tools to overcome obstacles. When these examiners share their efforts of what worked and what didn't, everyone can benefit. Ideally, these successful efforts with sharing will result in further advancements of forensic analysis and sharing with the community.

Not sharing the discovery of a new forensic artifact can be considered selfish, but no one will know about it anyway. The concept of not sharing advanced

skills and knowledge with the community at large stymies the development of the digital forensics field as well as not allowing the newly discovered process to be vetted by the community.

In order for common practices and procedures to become accepted, they must be commonly used and practiced by a community of practitioners. Courts generally approve of commonly used practices without little, if any, questioning. Those that have kept the “secret sauce” to themselves run the risk of having to have their efforts and work vetted, and potentially destroyed, in court.

There are many examples of how sharing information among the community results in more effective forensic analysts. One example is that of collecting physical memory. Not so many years ago, physical memory was not considered a primary evidence source, so much so, that computers were forcefully and abruptly shut down by pulling the power cord from the back of computers while they were running. Today, that same action will destroy gigabytes of electronic data. Had not those that researched, tested, and shared their findings about physical memory, we’d still be yanking power cords on every machine we find, including the machines that absolutely need physical memory preserved.

This case is different from that case

Every investigation is unique because people are unique. Forensic artifacts in one case may not exist in another. Even within the same case, the storage media being analyzed will be different, requiring different skill sets and tools. Motives are different from each other suspect, as is each suspect’s technology skill level.

Knowing that every suspect is different from the next, that there are many ways to commit the same crime, and that the technology used is dependent upon the choices of the suspect, take a breath and think before going fishing in an ocean of electronic data. If your job is solely digital forensics, where you have no interaction with victims or suspects, you need to have constant communication with the case agent. The forensic examiner needs to know the objectives and goals of the investigation. Already, analyzing terabytes of data is akin to searching for a needle in a haystack of needles. Being made aware of the case details and needs of the investigator will prevent frustration for everyone involved in the case.

Investigations, whether criminal or civil in nature, where the forensic examiner is purposely not made aware of intimate case details will only result in a massive amount of time spent needlessly hoping to find evidence that miraculously jumps out during an exam. In most cases, knowing the details of an investigation will enable the forensic analyst to target specific data, in specific

areas, that may resolve the case or lead to investigative leads that will satisfy case goals. It is up to the forensic examiner to ask just as much as it is the responsibility of the case agent (or client) to inform the forensic examiner of important information.

TESTIFYING TO YOUR WORK

Your work does influence the odds of being deposed, going to trial, or even having to personally present your findings to your internal company in a corporate matter. If you do a comprehensive analysis, detailing your findings succinctly and accurately, where the facts are clearly established, there may be no need to go further in the investigation regarding testimony. The facts may speak loud enough to cause a suspect to plea guilty and your testimony is avoided.

However, I do not believe that doing great work will always mean you never go to trial. Your great work may only reduce the amount of personal testimony you have over a period of time. Some suspects may face such great lengths of incarceration that they have to go to trial as a last ditch hope, no matter how high the evidence is stacked. Others may have nothing to lose and want to go to trial.

So prepare every examination as if you will be testifying to it. A seemingly simple internal corporate matter can quickly be made into a federal criminal case with a single piece of evidence. Companies with government contracts that involve national security are always at risk of any internal investigation becoming a federal investigation. The discovery of child pornography during an employee Internet abuse internal investigation automatically reaches a criminal investigation.

Any forensic examiner risks being called to testify to their work. That includes the interns. That includes the person who may not be a trained forensic examiner that was fishing around a hard drive for evidence. Any person who wishes to touch evidence must also know that touching evidence means risking testifying to everything you saw and did in regard to that evidence. Many organizations, corporate and government alike, take great steps to minimize the number of hands and eyes that interact with evidence. The more eyes and hands involved increases that many more persons risking giving testimony that could negatively affect the case.

Testimony that negatively affects the case doesn't only affect that one case. It can affect every case like it in the future, for everyone. To give testimony which a court accepts as factual means that other cases may use those findings to support future cases, even if the facts weren't accurately stated originally. This means that testimony in other cases, even in a different state, will require

arguments between opposing counsels to accept your version of the facts compared to another court's acceptance of different facts in a different case.

The best advice for preparing your testimony is to start before you leave your office to collect the first piece of evidence. Make a plan, be sure everyone involved is using the same plan, and stick to the plan unless an unexpected event comes up during the execution. If you are not the plan maker and have suggestions, give them. Don't let someone else make mistakes because everyone involved will potentially pay for it later.

The best advice for giving testimony is simply following the court's instructions to tell the truth and nothing but the truth. When you don't know an answer, just state you don't know the answer. There is no need to fill in the blanks or guess. Let someone else fill in the blanks to an investigation with facts, not conjecture. And as difficult as it may seem, if you are called on an error you made, admit the error because we all make one sooner or later.

A personal rule I have for evidence is to have a single point of entry for all evidence. You may have as many evidence collectors as necessary, each collector copying files, imaging hard drives, or bagging physical items, but have each collector report to a single evidence handler. One person with the one master list as a sole duty will be one of the best ideas you will ever have in evidence collection as it directly affects testimony regarding evidence admission in your case.

SUMMARY

The point of the above exercises in case studies was to show how different cases have placed the suspect behind the keyboard using a variety of investigative and forensic analysis means. Not one method always worked, was needed, or could be used every time. The software and hardware used did not make the cases, as nothing has been developed yet that automatically finds the evidence for you. These cases used a combination of technical know-how and pure gumshoe detective work to put the cases together.

As a forensic examiner or general investigator that has electronic evidence in a case, your duty and responsibility requires awareness beyond your primary duty. The investigator must be aware of technology and the potential of evidence available through forensic analysis of storage media. The forensic analyst also needs to be aware of the case outside the hard drive. The goal of both jobs is not just to collect mounds of evidence, but it is to place the suspect behind the keyboard, in the name of justice for the victim. Otherwise, all this work is for nothing.

Bibliography

- Arredondo M., Federal Bureau of Investigation, Search warrant (2008). Retrieved from US District Court website: <http://www.fbi.gov/about-us/history/famous-cases/anthrax-amerithrax/08-489-m-01.pdf/at_download/file>.
- Cree C., Tracking USB devices (2009). Retrieved from <https://encaseondemand.adobeconnect.com/_a799910323/p80426859>.
- Justin Lee Firestone v Hawker Beechcraft International Service Company (2012).
- Lee R., (2009, September 09). Computer forensic guide to profiling USB device thumbdrives. Retrieved from <<http://computer-forensics.sans.org/blog/2009/09/09/computer-forensic-guide-to-profiling-usb-thumbdrives-on-win7-vista-and-xp/>>.
- Mandyllion Research Labs. <<http://www.mandyllionlabs.com/>>.
- Odom v. Microsoft and Best Buy (United States Court of Appeals 2006).
- Paul D. Ceglia v Mark Elliot Zuckerberg, and Facebook Inc. (US District Court 2012).
- Sanders N., US District Court, Western District of Washington (2007). Search warrant. Retrieved from website: <<http://politechbot.com/docs/fbi.cipav.sanders.search.warrant.071607.pdf>>.
- State of Kansas v Dennis Rader (District Court of Kansas 2005).
- State of Missouri v Gary D Heggins (Missouri Circuit Court 2012).
- State of Wisconsin v Brian Pierick (Waukesha County Circuit Court 2010).
- Stexbar. <<http://code.google.com/p/stexbar/>>.
- The People of the State of Illinois v Steven Zirko (Circuit Court of Cook County 2009).
- United States Court of Appeals for the Ninth Circuit. Todd M Chism v Washington State; Washington State Patrol (US Court of Appeals 2011).
- United States District Court for the Eastern District of Virginia v Robert Philip Hanssen (US District Court 2001).
- United States District Court. Western District of Washington at Tacoma v Daniel Christopher Leonard (US District Court 2010).
- United States of America v Barry Vincent Ardolf (US District Court 2012).
- United States of America v Biswamohan Pani (US District Court 2008).
- United States of America v Higinio O. Ochoa III (US District Court 2012).
- United States of America v Luis Mijangos (US District Court 2010).
- United States of America v Timothy James McVeigh (US District Court 1995).
- US District Court v Clifton Dwayne Brooks (US District Court 2012).
- US District Court. Eastern District of Wisconsin v Harry J Janikowski (US District Court 2009).
- USBDeview. <<http://www.nirsoft.net>>.