Civil & Legal Sciences

Gogolin and Jones, Civil Legal Sci 2013, 3:1
http://dx.doi.org/10.4172/2169-0170.1000110

Research Article Open Access

Digital Forensic Issues in Civil Proceedings

Greg Gogolin[1]* and Jim Jones[2]

[1]*Information Security and Intelligence programs, Ferris State University, United States*
[2]*Computer Forensics program, George Mason University, United States*

Abstract

Digital Forensics is an emerging field that has quickly become a key source of evidence in criminal and civil cases. While digital forensics has been challenging to incorporate into both criminal and civil cases, the environment of civil cases does not have the structure of the law enforcement processes to serve as a framework from which to conduct digital forensic examinations. Further, there is often a lack of understanding of digital forensic capabilities and evidence, which has the potential to influence legal judgments and misconstrue outcomes.

Keywords: Digital Forensic Civil Cases; Digital Forensic Legal Challenges; Digital Forensic Approaches

Introduction

Much has been written regarding how digital forensics has become a mainstream source for providing evidence in criminal investigations. Some law enforcement agencies report at least fifty percent of their cases have a digital component, and most agencies report this trend is increasing [1,2]. This is magnified by the fact that digital crime is dramatically underreported to law enforcement, and law enforcement is typically unprepared to assist businesses with computer crime [3,4]. Part of the reason for the lack of reporting includes the fact that some things perceived as cybercrimes are not necessarily defined as crimes under criminal law [5]. Further, the judicial system is generally unprepared to understand or challenge digital evidence collection and interpretation [6,7]. Gathering data on the prevalence of digital forensic investigations in civil cases is much more difficult to compile as there is no central source for information like there is for criminal cases. The purpose of this article is to illustrate how digital forensics is used in civil proceedings and point out some of the legal, ethical, and procedural challenges that can surface.

Digital Forensics in Civil Cases

Divorce and custody cases are among the most common civil proceedings that incorporate digital forensic investigations. Cases such as this often evolve over time and a divorce may be contemplated for some time before proceedings actually begin. Therefore it is not uncommon for one or both parties to begin information gathering on their spouse prior to filing for divorce. How this information is gathered is often the subject of interest to a digital forensic examiner.

A keylogger is an information gathering tool that can be utilized in a legitimate and also illegitimate fashion. Keyloggers record keystrokes and can be used for testing, creating backups, and monitoring. Using a key logger to track someone's activities without their knowledge can be the same as tapping someone's phone, and this is generally illegal – particularly when the person being tracked is an adult. Key loggers can be both hardware and software based. Software key loggers are often preferred because they can be installed with little trace and the logs of captured keystrokes can often be accessed remotely.

The remote access aspect is a key piece in that gaining physical access to a computer may not be needed. A common theme that accompanies this type of case is that things come out in court that the other party should have no knowledge of or way of gaining that information, thereby raising suspicions that some form of electronic monitoring may be occurring. A digital forensic examiner may process the suspected devices to look for artifacts that would point to a key logging or surveillance situation, but it can be difficult to locate definitive information because of the many ways that key logging and surveillance can occur. There are dozens of potential tools that someone can use to monitor another person.

Monitoring often goes beyond computer monitoring to include mobile devices such as smart phones. This type of monitoring can include capturing global positioning system (GPS) tracking information, phone call, text, and email traffic. Because of the number of devices and types of technologies utilized, it can be difficult to forensically analyze a smart phone to the level of detail that is possible to forensically analyze a computer when trying to determine if a device is being used for tracking. Linking tracking tools back to a source can be difficult as they may be passed off as some sort of malware infection or uninformed behavior on the part of the device owner. This can be further complicated in that children's devices may be the source of the tracking. The effectiveness of this is that children are often with a parent, and therefore things such as GPS tracking can be equally effective by using a child's device rather than that of a spouse. In addition to that, the legal consequences may be reduced or eliminated if the child has not reached the age to legally qualify as an adult.

Rather than trying to locate evidence of installation of one of many potential tools, it may be more effective for a digital forensic examiner to look for certain types of device behavior. Since monitoring tools have many similarities with malware and in fact may be malware common malware analysis techniques such as dynamic (behavioral) and static (code analysis) investigative methods can be utilized. Malware analysis techniques are widely known [8,9]. Armed with this information it may focus the search in a more fruitful manner. It may also provide enough information to gain legal access to the devices of the person suspected of doing the monitoring.

For example, the authors were involved in a divorce case where the

***Corresponding author:** Greg Gogolin, Information Security and Intelligence programs, Ferris State University, United States, E-mail: ismgreg@yahoo.com

Received November 04, 2013; **Accepted** November 06, 2013; **Published** November 09, 2013

Citation: Gogolin G, Jones J (2013) Digital Forensic Issues in Civil Proceedings. J Civil Legal Sci 3: 110. doi:10.4172/2169-0170.1000110

wife reported that the husband appeared to "know things" that he could only have learned from her online and offline computer activities. At the time the couple was separated, but she was using a laptop which they owned prior to their separation and to which she now had sole physical access.

The wife had no solid basis to request police intervention, so her attorney retained a private investigation firm specializing in digital forensics. The firm executed antivirus and spyware searches of the system, examined the live system for indications of malware or spyware, reviewed system logs, and examined the laptop's hard drive offline. No indications of spyware, spouse ware, or malware were identified.

The authors were consulted and recommended a live sandbox dynamic analysis. The laptop disk image was loaded and booted as a virtual machine guest in a sandboxed environment with network traffic monitoring enabled (as a sniffer on the host OS). Shortly after booting, network sniffing revealed an attempted HTTPS (TCP port 443) connection to an IP address registered to a commercial company that sells and operates a remote monitoring application. Based on available documentation, the authors determined that the monitoring application runs locally as a hidden process, and sends activity reports to the company's servers, which are then accessible via a web interface to authorized remote users.

Sandboxing should be approached carefully so as to not alter evidence during the investigative process. One way to accomplish this is to always work off of a copy of the evidence rather than the original. The copy can then be booted and monitored with a tool such as Wireshark without concern about altering the original evidence. By sandboxing the evidence in a virtual environment the investigator can prevent the device being investigated from contacting an outside network such as the Internet but still be able to track potential network communication requests.

With details of the monitoring application gleaned from open sources, further analysis of the laptop system revealed the obfuscated application executable file stored on disk, disguised Windows Registry entries used to ensure persistence across reboots, and the application running as a hidden process (revealed through memory analysis). File timestamps were able to establish that the application was loaded prior to the husband relinquishing access to the laptop.

While not necessary in this case, the wife's attorney could have then requested the monitoring site's logs or user records to show use by the husband, or the husband's credit card history to show the purchase of the monitoring application, or the husband's online activity to show access to the monitoring site.

Another example of monitoring includes the use of camera technology. This may include remotely activating web cameras that are built into computers and mobile devices. Some cameras have an activation light, which indicates when a camera is being used. While a common feature on computers, this is far more uncommon in mobile devices. Additionally, mobile devices are often equipped with multiple cameras, which can provide an almost 360 degree perspective. Coupled with GPS technology, information regarding where someone is and who they are with can be determined, and understandable audio can be heard and collected.

Evidence in a digital environment is different than physical evidence in many ways. Communication and network capabilities, various types of software and configuration options, as well as techniques such as encryption are but a few of the ways that evidence can be accessed, modified, or hidden. It is not uncommon for techniques such as these to be presented as default behaviors when in fact they were employed as anti-forensic techniques. Preservation of digital evidence is frequently a central aspect of court orders, yet how evidence is preserved is often open to interpretation. Deleted files can often be recovered using digital forensic processes, yet there are utilities and common computer configuration options such as the disk defragmentation process that can reduce the potential for deleted file recovery. Time can impact how long evidence is retained, so something as basic as the length of time that elapses after evidence creation or destruction can influence evidence recoverability.

The device type and technology involved also plays a key role in the ability to preserve and recover digital evidence. Some types of smart phones are such that things like text messages are unrecoverable under normal circumstances once they are deleted. This may present a challenge to an investigator to prove that the evidence existed in the first place. Legal proceedings may be such that evidence improperly destroyed may be interpreted as damning (i.e., the legal "adverse inference rule"). The authors have investigated multiple situations where this point was central in a civil case. Proving evidence destruction can be difficult, but if proven the consequences can be dramatic.

In civil cases a digital forensic examiner often operates under a court order, which may define the parameters that dictate the examination procedures and techniques employed. A common digital forensic practice is to make a bit for bit copy (image) of a device that can be verified as an exact duplicate by means of arithmetic hashes such as the MD-5 and SHA-1 algorithms, which are far more precise than DNA evidence. In ideal circumstances, multiple hashes are utilized to ensure accuracy and provide confirmation that evidence has not been altered. Hashes should be taken of the source and copy of the source as part of the imaging process. All forensic work should occur on the copy of the source to eliminate the chance of impacting the original source. Once work is completed, the hashing process should be performed again on the copy of the source. All hash values should match those of the original source. This basic step verifies that no evidence has been altered, yet it is often overlooked and/or not documented in forensic reports. If hash values are reported, they are generally the verification hash values of when the copy was taken, not verification hash values after the examination was completed. Neglecting this step opens the door for an alteration of evidence argument.

Computing hash values after completing a digital forensic examination, while an often overlooked step, points to a larger challenge in digital forensics. Education, training, and other qualifications of digital forensic examiners vary considerably [10]. Some states require that digital forensic examiners be licensed, but many states have no standard. In civil proceedings where digital forensic capabilities are required, forensic investigators for both parties often examine the same evidence as a means of verifying or discrediting findings. This emphasizes the importance of accuracy and verification of findings on the part of the investigator because inaccurate results can lead to lack of credibility of the examiner and their findings.

Digital forensic examiners should provide a report of findings that is signed and each page initialed if possible. Sometimes preliminary findings are requested and they should be designated as such. The wording of the report, whether a preliminary or final report, is critical to its interpretation and accuracy. For example, in a hacking case an investigator may find that no evidence exists that data was copied. This may be true, but it may also be true that no evidence exists that data was not copied, and to represent findings only as the former can call

into question the findings of the whole report and the ethics of the entire procedure. Given the lack of technical understanding by judges and juries, unscrupulous digital forensic investigators may abuse the system, going so far as to destroy, alter, or misrepresent evidence [11-13].

Digital forensic examinations in civil cases have many similarities to those of criminal cases, but there are also many key differences. First of all, law enforcement may have limited or no involvement in civil proceedings. Second, the burden of proof may be to a different standard. Third, the forensic exam may be governed by a court order. Additionally, the procedures and techniques may be different from case to case and jurisdiction to jurisdiction. Lawyers may spend considerable time arguing the wording and constraints of each court order, and this may also spill over into legal issues for the digital forensic examiner if the court order is not interpreted consistently between both parties.

Civil cases often have a financial aspect as a central focus. As such, there is considerable pressure to maximize or minimize the financial implications. Court orders that govern digital forensic examinations often have date constraints. In other words, only artifacts from a particular date range or meeting other criteria are admissible [14]. Items that don't meet these constraints are supposed to be eliminated from consideration in the case. That doesn't mean eliminated information is not beneficial to a party, but it is to be eliminated under the language of the court order.

Court orders often provide for a forensic examiner to take a complete image of evidence and then expect the examiner to filter findings based on the court order constraints [15]. Sometimes this means providing the initial draft report of findings to the opposing counsel for verification of meeting the court order before providing findings to the counsel that has engaged the examiner's services. In theory this eliminates providing incorrect or undiscoverable information. In practice, there may be leakage of findings to those that should not have the information. One way to reduce the potential for this is to have someone observe the forensic investigation process. This can be cumbersome and time consuming, and it likely won't eliminate the chance of information leakage, but it is one of the best ways to help ensure that the intent of a court order is followed. It also provides the opportunity to recognize what information may be uncovered that is outside the scope of the court order, so that if a question of where such information came from it may be possible to tie back to a source.

One of the reasons it is difficult to completely eliminate information recovered from a digital forensic investigation is that court orders are often date driven. A court order may allow for examination of communication between two dates. While file timestamps can be used to determine when files are accessed, electronic communication doesn't necessarily have the same feature. Communication that is accessed via a browser, such as a web-based email account, may not create a typical file. Since the message may only be viewed with a browser, a copy of the message may only reside in unallocated space on a disk. This information is typically carved out of unallocated by means of keyword searches and similar means. It is possible that only part of a message can be recovered rather than the entire message. Since it is a fragment, time and date information may not be part of the record, thereby making interpretation as to whether the message falls within the date parameters of the court order unclear. This is the kind of information that often becomes part of a review process with the opposing counsel to determine if the message should be supplied to the commissioning counsel. This is an example of a situation where data leakage may occur because the commissioning counsel knows that there is information that could potentially help their case that they want access to, and through the argument process or backdoor channels may gain insight into what the message contains.

Summary

Digital evidence will continue to play an important role in the justice system, but the system has yet to catch up with the technology. Digital evidence continues to be treated as if it was physical evidence, which in many respects it is not, and many members of the judicial system simply don't have the technical background to understand digital evidence collection and interpretation. However, the judicial system has adapted to new technology in the past, and it will do so again. DNA evidence was widely misunderstood (and abused) when first introduced, but we now consider it to be a key evidentiary component of many proceedings. While few judges could sequence a gene or perform DNA matching analysis, the judicial system adopted processes, procedures, and access to external expertise so that such evidence can be collected, trusted, and interpreted in a consistent manner. While the same will eventually be true for digital evidence, we are currently floundering in an uncertain state of questionable collection, processing, and interpretation. Our challenge is to find our way out of this maze as quickly as possible, and to minimize the damage until we do.

Reference

1. Ami-Narh JT, Williams PA (2008) Digital forensics and the legal system: A dilemma of our times. In Australian Digital Forensics Conference.
2. Gogolin G (2010) The Digital Crime Tsunami. Digital Investigations 7: 3-8.
3. Bryant R (2008) Investigating digital crime. Wiley Hoboken NJ.
4. Gogolin G, Jones J (2010) Law Enforcement's Ability to Deal with Digital Crime and the Implications for Business. Information Security Journal: A Global Perspective 19: 109-117.
5. Hunton P (2009) The growing phenomenon of crime and the Internet: A cybercrime execution and analysis model. Computer Law & Security Review 25: 528-535.
6. Rothstein BJ, Hedges RJ, Wiggins EC (2007) Managing discovery of electronic information: A pocket guide for judges. Federal Judicial Center.
7. Kessler GC (2010) Judges' awareness, understanding, and application of digital evidence (Doctoral dissertation, Nova Southeastern University).
8. Sikorski M, Honing A (2012) Practical Malware Analysis: The Hands-On Guide to Dissecting Malicious Software. San Fransico CA: No Starch Press .
9. Zelstser L (2013) 5 Steps to Building a Malware Analysis Toolkit Using Free Tools.
10. Harrington SL (2011) Collaborating with a digital forensics expert: ultimate tag-team or disastrous duo. Wm. Mitchell L. Rev. 38: 353.
11. Losey RC (2008) Lawyers Behaving Badly: Understanding Unprofessional Conduct in E-Discovery. Mercer L. Rev. 60: 983.
12. Lambert WG (2013) Keeping the Inference in the Adverse Inference Instruction: Ensuring the Instruction Is an Effective Sanction in Electronic Discovery Cases. SCL Rev. 64: 681-765.
13. Parry ZB (2009) Digital manipulation and photographic evidence: defrauding the courts one thousand words at a time. JL Tech. & Pol'y.
14. Alexander RK (2011) E-Discovery Practice, Theory, an Precedent: Finding the Right Pond, Lure, and Lines without Going on a Fishing Expedition. SDL Rev.
15. Hardaway R, Berger DD, Defield A (2010) E-Discovery's Threat to Civil Litigation: Reevaluating Rule 26 for the Digital Age. Rutgers L. Rev.

Citation: Gogolin G, Jones J (2013) Digital Forensic Issues in Civil Proceedings. J Civil Legal Sci 3: 110. doi:10.4172/2169-0170.1000110