**Computer Forensics: An Unguided Evolution**

Raquel Gutierrez Valdes

Computer Security 180

Santa Clara University

Santa Clara, United States

rgutierrezvaldes@scu.edu

Samuel M. Vivian

Computer Security 180

Santa Clara University

Santa Clara, United States

svivian@scu.edu

**Abstract - This academic journal discusses the evolution of computer forensics, its benefits in the modern age, and its limits in the realm of legal validity as it pertains to computer-related criminal activity. It also examines preexisting court cases in which computer forensics has a pivotal role.**

***Keywords - computer forensics, digital forensics, digital evidence, computer-related crime***

1. WHAT IS COMPUTER FORENSICS

Digital forensics or computer forensics is concerned with the investigation of any suspected crime or misbehavior that may be manifested by digital evidence. Computer forensics aims to answer the following questions: Who is the attacker? How did they carry out their attack? How much and what kind of damage was done? And will these answers hold up in court? Computer forensics is unique in the forensics field because it is ever-changing and is not backed by a solid scientific foundation. DNA evidence for example is based on a standardized scientific understanding, whereas computer forensics has a much broader scope that is not always reliable. It is also impossible to alter your DNA and very difficult to falsify someone else's, but very easy to leave false trails in computer breaches. Often computer forensics tools give accurate results, but incorrect assumptions are made about these results due to the fact that most judges and lawyers have minimal understanding of computer security. Computer forensics usually deals with showing the jury how a file arrived at its current location and who put it there. There are many tools to track this kind of activity that drop informational packets, however, attackers can also forge these packets or data to be gathered from a host [4].

Due to the evolution of each computer forensic group evolving separately from one another combined with a lack of communication between experts in the field and legal authorities, there are many different models that computer forensics experts use. Generally speaking, they use a predictive formula or mapping. Some examples would be a mapping between the gathered data and admissibility in court, mapping between the physical investigative process to the digital world, and categorizing transitions between system states in order to reconstruct the actions taken between them. It seems that it should be simple to ask whether or not a file exists, but understanding the validity of the file is unreliable which leads to the creation of so many different forensic models.

1. HISTORY

According to The History of Computing Project, the beginning of the Industrial Era of Computing started in 1947. Up until the early 80s, computers were primarily owned by corporations, universities, research institutions, and the government due to their size and price. The first traces of computer security occurred around 1976 when system audits were carried out to ensure the efficiency and accuracy of the computers. At this time, inconsistencies were found that could help track down wrongdoings within the system. Due to these initial discoveries the FBI and IRS were required to have some low-level training with computers so that they could work effectively with system administrators if issues ever occurred. By 1990, people who were interested in computers and computer science who worked with them regularly began to realize that hackers could access large numbers of computers using the Unix system, however, the lack of public access to computing meant that there was very little organized computer forensics up to this point [2].

In 1985 IBM came out with the first-ever personal computer allowing computers to become available to the public as a hobby. It was around this time that the International Association of Computer Investigative Specialists (IACIS) realized that computers could be useful in criminal investigations-- especially as evidence. In 1993 the FBI held the First International Conference on Computer Evidence which was attended by 26 countries. Following this, the International Organization on Computer Evidence (IOCE) was formed at the second conference in 1995. At this time computer forensics mostly dealt with data recovery from individual computers since the internet was not yet popular. Criminals could still use dial-up access to compromise computers or hack a telephone network to get free telephone service with anonymity. The main tools that had been created to help with computer forensics were command-line prompts for imaging or recovering deleted files and some even allowed multiprogramming and early versions of piping. The IRS, FBI, and US Airforce were some of very few official groups that had organized computer forensics forces, however, these investigations were usually carried out by minimally trained officers working alone without quality control and with their own personal hardware [2].

Between 1995 and 2005 computers became increasingly popular. The internet and cell phones began to be regularly used by most people. As the internet became commonplace, more and more criminals began to take advantage of it. In 1993 there was a child pornography case that prompted an online undercover operation in 1995. The issue was a major motivation for growing the digital forensics field and by 2005 there was a child pornography task force in half of all FBI offices. The FBI has also reported that 50% of all cases in 2002 involved computers and tracking their data in some way. Additionally, 9/11 was a massive motivator for advancement in digital forensics due to the fact that the terrorists had used the internet to communicate and these communications could have hypothetically been intercepted, perhaps resulting in a successful prevention effort. This made law enforcement realize they were severely lacking in this field. Agents began to be specifically trained for digital forensics and specializations began to form within the field including audio, video, embedded devices, traditional storage media, and network forensics. The command-line tools that had been used in the past began to change into tools with full complex GUI suites. These tools included Expert Witness, EnCase, Forensic ToolKit, Automated Case Examination System (FBI), and iLook (IRS) as well as open-source tools Helix, Sleuth Kit, and Autopsy Browser. At this time the Department of Defense also formed the Defence Computer Forensic Lab [2].

As of 2006 new rules had been added allowing the acceptance of digital information as evidence and the FBI examined over 2.5 petabytes of evidence in 2007 alone. Computer forensics became a full-fledged career path taught in universities across the globe. The number of effective conferences on the issue increased and over time more and more devices have some kind of digital storage (smart refrigerators). As such the usage of computer forensics has become an integral part of our law enforcement systems as computer crime also increases along with continued advancements in computer technology [2].

1. COMPUTER FORENSICS IN LAW

The legal aspect of Computer Forensics is to this day, very unclear and complex. At its core, both digital and traditional forensics in court serve the purpose of providing a correlation between characteristics in evidence. In particular, digital forensics uncover digital traces in order to prove or disprove that an event occurred. Because of the rapid evolution of digital forensics and its lack of tangibility, digital evidence cannot follow the same rules as traditional evidence. For example, the “seize everything” strategy cannot be applied to digital evidence since information is stored throughout a series of networks and easily transmitted from one computer to another. This makes it economically infeasible to get a hold of all relevant hardware and it would take an enormous amount of time to process all of the stored data to find a condemning piece of evidence that would apply to one particular case. Also, search warrants are much more complicated for digital forensics since there are no physical boundaries in the digital world, compared to physical evidence which would be bound by walls or buildings [3].

In general, digital evidence must satisfy two conditions to be admissible in court: it must be relevant to the case and it must be derived by the scientific method with supported appropriate validation [5], the problem with this is that these two conditions are too vague and weak to provide uniformity for all digital evidence. Some steps have been taken in order to resolve this issue starting in 1999 when the International High-Tech Crime Conference adopted a set of guidelines for digital evidence recovery which state that:

1. All digital evidence must be recovered by a forensically competent individual.
2. All activity of access, storage and transfer of evidence must be documented, preserved and available to review at any given time, and
3. An individual is responsible for all actions towards the evidence while it is in his/her possession [5].

Since digital information is easily modified and duplicated without any trace, these guidelines offer a way to limit or detect these possible changes to the evidence that might make it inadmissible.

1. FAMOUS CASES

The previous section talked about the complexity of digital evidence and the steps lawmakers have taken in order to lay out a clear set of rules. In the past decade, digital evidence has been successfully used to condemn the accused.

In 2009, authorities were able to track down Krenar Lusha, an illegal immigrant living in the UK, based on his internet search patterns. After seizing his computer, forensics were able to find internet searches on how to make bombs and correspondences with people posing as a terrorist. He was sentenced to 7 years in prison. Another similar case where search history was used to disprove an alibi was in 2016 when college student Mikayla Munn claimed that she passed out while taking a bath in an attempt to relieve menstrual pains. She woke up to find she had given labor and the baby had drowned in the bathtub. Further investigating her personal computer, her search history showed she had googled how to cut an umbilical cord and how to abort at home. She was sentenced to 12 years in prison.

On the other hand, the lack of guidelines in digital forensics has made it possible to lengthen court trials and dismiss potential incriminatory evidence. In 2017, Ross Compton was charged for committing insurance fraud and arson. He claimed he woke up in the middle of the night and his house was on fire, so he packed up a few things, broke the second-floor window, and climbed out with few belongings. What makes his claim suspicious is the fact that Compton has a heart condition and a pacemaker that after an expert cardiologist analyzed his heart rate and medical information, concluded that it is highly unlikely that Compton could’ve kept his heart rate as steady as it was during the stressful events and couldn’t have climbed out the window safely. To this day, there has been a delay in court since the judge has to rule whether heart rate as evidence is considered admissible and substantial, or if it is considered (as Compton’s lawyers are claiming), stealing personal information [6].

Another case that displays the difficulties of using computer forensics as evidence is the case of Gates vs. Bando. In this case the Gates Rubber Company accused Robert Newman, a former employee of violating Gate’s intellectual property by stealing a program called “Life in Hours” when he left Gates to work at Bando Chemical Industries. Gates provided a hard drive that they said had previously contained the software and alleged that the information and program that were not currently on it had not been deleted until after Newman left the company. Newman had stated that he had used a cleanup software on the drive which should have deleted the file, before he left the company. Some files were recovered, but there was not enough admissible evidence to come to any conclusions about the software being used before or after Newman left Gates. A lack of technological understanding and access to standardized computer forensics by the prosecution lead Gates to spend millions of dollars on an unsuccessful case [4].

1. CHALLENGES AND SOLUTIONS

Computer forensics can be very powerful, but there are many challenges for the future of digital data and law. Firstly the tools that have been built to support computer forensics have to be ever-changing to keep up with new and more advanced technology as well as more different variations of digital attacks. As such, these tools are created at a great expense which could be a potential issue moving forward. If it costs a lot to make these tools, and the types of attacks are changing continuously it may be hard to keep up with computer crimes as time goes on. A possible solution to this would be to look to open source tools, however, these tools tend to carry less weight in court due to a lack of ability to carry out exhaustive testing. Some of these tools come close, but it is still an immense challenge to maintain high-quality results with assured outcomes across many different tools. An extension of this challenge that is appearing as a result of advancements in technology is the increased usage of embedded systems in general. More and more devices are being built with embedded systems and network connectivity. Many household appliances including microwaves, dishwashers and refrigerators often contain embedded systems. The issue here is that any of these embedded systems can be attacked and often each device requires a different tool to collect data about breaches into all of these new devices [1].

Another major issue is that due to the ability to easily fake data, it is extremely difficult to maintain authenticity, especially when certainty is required in high-profile corporate court cases. Additionally, the sheer volume of data that exists as computers have become the normal place to store and do everything and anything is immense. In order to combat the growth in both personal and corporate data storage, there needs to be an increase in the abilities of data mining techniques and an acceptable resolution to the trade-off between personal privacy and data mining large data sets. There will also be a need for monitoring the internet. A major issue that stands in the way of network security is worms. Worms are standalone computer malware that self replicate to spread to other computers. They often use computer networks to spread relying on computer security failures to gain access. They then use the compromised machine as a host to scan and infect other computers. The challenge with worms is to develop tools that can enable hosts and networks to recognize and contain worms quickly before they can spread. It appears, however, that the biggest issue is deciding where the accepted middle ground is in the discussion between privacy and security. Most of the other issues can be solved simply by increasing the funding and overall effort put into developing the tools to combat and track computer security breaches. This tradeoff is a bigger issue as collecting data as evidence could be seen as a massive breach of privacy and until the collective computer security community can lay out exact rules and guidelines, this issue needs to be considered [1].

1. CONCLUSION

Our daily lives are deeply intertwined in the digital world. Everyday more devices become reliant on networks and embedded systems. The number of breaches reported increased 52% from 2018 to 2019, and it is only estimated to rise [7]. Computer forensics provides the top-notch tools to uncover these breaches and process them according to the law to keep everyone safe. Not only that, when cyberattacks occur, it is important to constantly adapt and update the guidelines and rules of use for computer forensics to maintain its numerous benefits in the legal field, valid and normalized.

As time passses it becomes increasingly important and difficult to stop digital crime, and find a good balance between privacy and security. As such, this area should be constantly in development with many people working to combat potential risks and issues that occur. Most of all, it seems that the area that is lacking is the laws that support digital evidence as it is admissible in court. Moving forward digital evidence and the laws supporting it need to be standardized so that we can accurately and consistently uphold the law and the truth.

REFERENCES

1. G. Mohay, "Technical challenges and directions for digital forensics," *First International Workshop on Systematic Approaches to Digital Forensic Engineering (SADFE'05)*, Taipei, Taiwan, 2005, pp. 155-161, DOI: 10.1109/SADFE.2005.24.
2. “A History of Digital Forensics.” *Advances in Digital Forensics: IFIP International Conference on Digital Forensics, National Center for Forensic Science, Orlando, Florida, February 13-16, 2005*, by Mark Pollitt and Sujeet Shenoi, Springer/International Federation for Information Processing, 2010, pp. 3–15.
3. Kenneally, E. (2002). Computer forensics. login: The Magazine of USENIX and SAGE, vol. 27. https://www.usenix.org/system/files/login/articles/1275-kenneally.pdf
4. Peisert, Sean, et al. “Computer Forensics in Forensis.” *2008 Third International Workshop on Systematic Approaches to Digital Forensic Engineering*, 20 June 2008, doi:10.1109/SADFE.2008.18.
5. Ryan, Daniel J., and Gal Shpantzer. "Legal aspects of digital forensics." Proceedings: Forensics Workshop. 2002
6. 5 Cases Cracked With Digital Forensics: IIGPI: Blog. (2020, October 01). https://www.iigpi.com/5-cases-cracked-with-digital-forensics/
7. 29 Must-know Cybersecurity Statistics for 2020. (2020, March 08). https://www.cyber-observer.com/cyber-news-29-statistics-for-2020-cyber-observer/