Computer Forensics in Law Enforcement

Robert Crager

CYBR 3340 - Cyber Crime

Collin College

October 31, 2021

Abstract

Computer forensics has been a crucial aspect of almost every law enforcement investigation since its inception and widespread adoption in the late 1980s. With the adoption came more useful and reasonably priced tools investigators and hobbyists could use to extract information from devices. Law enforcement saw the need for computer forensics once technology began to rise and communication between users (or criminals) saw a shift into technology as their medium of plotting criminal activity. In addition to tracking criminals through their digital fingerprints, law enforcement uses computer forensics to study the behavior of criminals to ultimately understand their motives, means of operation, and other crucial factors leading to their arrest or incarceration.

Computer Forensics Explained

Forensic science has been a crucial element to solving any investigation since criminal justice, the Department of Justice and other law enforcement agencies have been developed. Law enforcement utilizes forensic science practices to gather evidence such as DNA, and chemical evidence to prove beyond a reasonable doubt that a criminal committed a crime. As the Department of Justice’s website states “forensic scientists examine and analyze evidence from crime scenes and elsewhere to develop objective findings” (DOJ 2021), to ultimately prosecute the involved criminals. Computer forensics, however, takes traditional forensics to another level while keeping the fundamental ideology. Computer forensics is the collection, analysis, or presentation of digital evidence within a court or court system to prove a criminal committed a crime. The US-CERT defines computer forensics as “the disciplines that combine elements of law and computer science to collect and analyze data from computer systems, networks, wireless communications, and storage devices in a way that is admissible as evidence in a court of law” (US-CERT 2008, p. 1). Digital and computer forensics usually consist of recovering and analyzing computer evidence which would typically be stored through some digital medium. Or in other words, computer forensics is traditional forensics purely within the scope of computers, digital means, or technology (which is slowly becoming the only option in our modern world).

History of Computer Forensics

Computer and digital forensics, while they are fairly new developments and concepts, are crucial to any law enforcement agency's subject matter expert (SME) collection. Although digital forensics only began to see a rise in the 80s and 90s, it was being utilized much before that. In the 1960s, computers alone were just beginning to gain popularity as they were extremely new developments that were extremely costly and buggy machines. Therefore, around that time

(1960-70s), computers were only being leveraged effectively for commercial and industrial means through agencies like the Department of Defense (DoD), Internal Revenue Service (IRS), Federal Bureau of Investigation (FBI), which all developed specialized teams of individuals knowledgeable of computing systems (Chow, Shenoi, et al. 2010). These specialized teams would utilize their skills, typically provided through Agency-led training, to retrieve information from the mainframe computers often investigated by these agencies. This was the first instance of computer forensics being used in the wild.

Then, with the overall boom of computers in the mid-80s and 90s, consumers were getting their hands on personal computers, the internet began to rise in popularity, and naturally, computer forensics saw a massive increase in popularity too. Law enforcement personnel began writing their own programs to obtain information from and automate various processes for the computing systems they were interfacing with. Furthermore, multiple hobbyists interested in computer forensics would go on to become the founding members of the International Association of Computer Investigative Specialists (IACIS). The IACIS was built to provide helpful tips, tools, and standardizations for forensic data retrieval from various computing systems any forensic investigator might be interacting with during an investigation. After the development of this organization, the FBI, in 1993, held the first international conference surrounding computer evidence at the FBI academy in Quantico, Virginia. Many individuals from around the world came to this conference to show their support for digital forensics, especially within the scope of law enforcement, ultimately indicating the large-scale support for digital forensics as a whole. During this era, people would rely on their own hand-built tools to perform data retrieval functions and would begin sharing their tools with other enthusiasts. However, the commercial support for digital forensics at this time was nonexistent, there were no commercially provided tools, and most, if not all, hobbyists were practicing these investigations in their own homes on their own time. Although, some major agencies support forensics on a commercial scale at this time:

- IRS – Seized Computer evidence Recovery Specialist (SCERS) program
- U.S. Secret Service – Electronic Crimes Special Agent Program (ECSAP)
- FBI - Computer Analysis Response Team (CART)
- U.S. Air Force – Computer Crime Investigator (CCI) Program

In addition to the above programs, the following associations were created as well:

- U.S. Air Force - Defense Computer Forensic Laboratory (DCFL)
- Forensic Association of Computer Technologists (FACT)
- Geeks with Guns (Informal group of FBI, Secret Service, etc. Digital forensic practitioners)

Moving into the late 1990s and early 2000s, digital forensics began to grow in popularity even more, as law enforcement began to see the very realistic and practical use of the practice. As a result, computer forensics began to become more specialized, establishing more specializations like digital, video, audio, cell phone, etc. In addition to the specializations, during this era it started to become more formalized too such as the "IOCE, G-8 High Tech Crime Subcommittee and Scientific Working Group on Digital Evidence (SWGDE)” which “all published digital forensic principles between 1999 and 2000.” (Chow, Shenoi, et. Al 2010). Another key addition to the computer forensics field during this period was the publishing of several tools that would later be widely used and become almost industry standards. Some tools that were developed during this period include:

- Expert Witness (now Encase) – For Macintosh forensics
- Forensics ToolKit (FTK)
- FBI’s Automated Case Examination System (ACES)

- IRS's iLook tool

The aforementioned tools are commercially available solutions, but there were also several community-built tools that became available too:

- Helix
- Sleuth Kit (Open source)
- Autospy Browser

Although computer forensics essentially blew up in the late 90s and early 2000s, it only kept growing bigger as a community, profession, and practice in the years that followed (2005 and beyond). In 2006, the U.S. court developed new Rules for Civil Procedures stating that digital evidence could be utilized and examined in a court as evidence of a crime scene or crime. This was one of the largest steps towards standardizing computer forensics and ultimately allowed it to be realistically utilized today. Additionally, the FBI claimed that their Computer Analysis and Response Team (CART) analyzed more than 2.5 Petabytes (2,500,000 Gigabytes) of digital data as criminal evidence in 2007 alone (Chow, Shenoi, et al. 2010). Furthermore, the tools previously mentioned were getting even better as they evolved to accommodate emerging technologies such as virtual machines used within software like VMware, Storage Area Network (SANs), and implementing more automation features to streamline various forms of data extraction from multiple device types. Along with the law enforcement community, court system, and other communities, educational institutions around the world began offering more classes and programs for specialized digital forensics studies, further increasing the number of digital and computer forensics practitioners in the workforce.

Forensics in Law Enforcement

Judging by the history of computer forensics thus far, it doesn’t stray far from the truth to say that computer forensics is tightly engrained within law enforcement. While there are many other practical uses for computer forensics, law enforcement, to catch criminals, is the most practical and widely used in any real-world scenario. Through digital forensics, law enforcement can discover digital fingerprints of criminals to give investigators an idea of the criminal's location, motives, passions, weaknesses, etc. However, the ultimate question in any scenario akin to this is: **In what ways has law enforcement utilized digital forensics to find criminals?** And how might evidence found hold up in court given the various means it could be collected?

The depth of computer forensics is extremely far-reaching, not as far-reaching as forensic science as a whole but can still get very granular in the various fields and topics it offers. However, one main subject law enforcement utilizes computer forensics for often is to trace a criminal's steps from a crime scene, leading to their ultimate capture and arrest. In one very famous case, the BTK Killer from Wichita, Kansas, law enforcement, who thought he was dead, was able to obtain a drive from the serial killer in the early 2000s as he left an intentional trail for police to follow, proving he was still alive. However, in the intentional trail was a floppy disk drive that was improperly cleared or formatted so that investigators could retrieve the metadata from the drive. Metadata within the drive showcased a username involving the names 'Christ Lutheran Church’ and ‘Dennis’ which, after some open-source intelligence searching, investigators were able to make the connection back to Dennis Rader, who was the president of the church council at the time and who ultimately confessed to over 200 killings. (Rivera 2018). Without the widespread implementation, support, and use of digital and computer forensics nowadays and in the early 2000s, the BTK Killer could very well have escaped without any repercussions for his careless and heartless actions.

In addition to allowing investigators to make more in-depth and accurate connections to criminals, computer forensics allows investigators to study criminals' habits overall, allowing for them to predict criminal activity, whereabouts, and other key information that could lead to an arrest. By gathering intelligence on criminals and their behavior, investigators can further predict where other criminals may go, what they might do, how they might act in a certain scenario, etc. Through this, investigators can remain one step ahead of the criminals and ideally be at the location of the criminal's next step to capture them. Studying criminal behavior doesn't correlate to the specific criminal or type of criminal in particular though, it could involve the entire criminal group or organization. Ultimately, law enforcement is after the criminal organizer at the top of the pyramid within a criminal organization or crime group. Therefore, when they study the actions of a specific criminal, that is likely towards the bottom of the pyramid, it is probable that they will find the criminals medium for communicating with the higher-ups within that organization if there are any, ultimately leading to the criminal either converting to an informant for law enforcement to attempt to bring the entire operation down, or the criminal being prosecuted for the crimes they committed as an individual.

Lastly, as technology continues to expand and allow for a more interconnected society, criminals are making use of such technology to coordinate their criminal attacks, actions, and activities, along with recruiting impressionable individuals to their crimes. Because of this, there were a number of laws and regulations put in place for law enforcement to be able to monitor suspected criminals within our modern digital age. The regulations being referenced are mainly applicable to suspected terrorists, hate criminals, or otherwise threats to national security by law enforcement. One of the regulations is the US Patriot Act put in place because of the terrorist attacks from September 11, 2001. The US Patriot Act allows U.S. law enforcement authorities to build an online profile (or digital fingerprint) of any citizen without requiring a warrant to do so

(Dept. Of Justice 2001). The profile would include online search history, general interests, etc., on the given individual, and law enforcement would regularly monitor this digital fingerprint for any suspicious activity that would indicate criminal activity (specifically harmful to national security). This is only possible through the use of digital and computer forensics within law enforcement.

Final Thoughts

Computer and digital forensics were initially developed out of sheer hobby and interest by a community that was unsuspecting of its ultimate outcome. They were mainly developed by law enforcement practitioners who had an interest in gathering information from various computers and information systems, but soon became a necessity within the law enforcement community to solve crimes, gather intelligence, and prosecute criminals. As a result of the massive uproar and need for computer forensics specialists throughout the late 90s and early 2000s, law enforcement, government agencies, and other organizations began offering classes, developed specialized tools, and ultimately created an entire profession for computer forensics. Computer forensics allows law enforcement to not only catch criminals, but also study individual criminals to develop profiles based on their actions and predict their behavior. In the modern age of technology, law enforcement utilizes computer forensics to find evidence to prosecute a criminal, trace the criminals steps (through digital fingerprinting), and ultimately present evidence in a court of law that provides, beyond a reasonable doubt, that a criminal committed the crime in question.

References

Chow, K.-P., & Shenoi, S. (2010, January). Advances in Digital Forensics VI. Retrieved from https://link.springer.com/content/pdf/10.1007%2F978-3-642-15506-2.pdf.

Flory, T. A. C. (2016). *Digital Forensics in law enforcement: A needs based analysis of Indiana agencies*. Scholarly Commons. Retrieved October 30, 2021, from https://commons.erau.edu/jdfsl/vol11/iss1/4/.

Forensic science. The United States Department of Justice. (2021, January 15). Retrieved October 30, 2021, from https://www.justice.gov/olp/forensic-science.

Hart, S. V. (2004, April). *Forensic Examination of Digital Evidence: A Guide for Law ...* Forensic Examination of Digital Evidence. Retrieved October 30, 2021, from https://www.ojp.gov/pdffiles1/nij/199408.pdf.

IACIS. (2021, February 23). *History*. IACIS. Retrieved October 30, 2021, from https://www.iacis.com/about/history/.

Lytle, A., Stephens, N., Conner, J., Bashiri, S., & Jones, S. (2018, March). *Digital Forensics and enforcement of the law*. IEEE Internet Initiative. Retrieved October 30, 2021, from https://internetinitiative.ieee.org/newsletter/march-2018/digital-forensics-and-enforcement-of-the-law.

Online, N. U. (2015, December 7). *Role of computer forensics in crime*. Norwich University Online. Retrieved October 30, 2021, from https://online.norwich.edu/academic-programs/resources/role-of-computer-forensics-in-crime.

Rivera, A. (2018, February 12). *BTK Serial Killer: Power of Computer Forensics*. The Bakersfield Californian. Retrieved October 30, 2021, from https://www.bakersfield.com/kern-business-journal/btk-serial-killer-power-of-computer-forensics/article_dd8f0ad3-f833-50b6-8e25-dcf6d406d5c4.html.

U.S. Department of Justice. (2001). *USA PATRIOT Act*. What is the USA Patriot Web. Retrieved October 30, 2021, from https://www.justice.gov/archive/ll/highlights.htm.

US-CERT. (2008). *Computer forensics10 updated - CISA*. Computer Forensics. Retrieved October 30, 2021, from https://us-cert.cisa.gov/sites/default/files/publications/forensics.pdf.