Computer Forensics: Rapid Growth and Integral Role in Law Enforcement

Melissa Genovese

CYBR-3340.202

Dr. James E. Freedle II

November 19, 2021

Computer Forensics: Rapid Growth and Integral Role in Law Enforcement

With the development and production of cheap home computers in the early 1980's and 1990's to the introduction of the internet in people's homes becoming mainstream, it is only natural to think that crimes would migrate to people's computers then spread across the world via the internet. It even makes more sense that because of the ease of these technologies, crimes that did not exist before would event themselves because of the instinct that has always driven criminals to be criminals. To go a stretch further, it is not hard to imagine that these computers and those persons behind them could create networks and markets that make their cybercrimes possible, lucrative, and (in a business sense) function to make operations run smoothly and efficiently. Because cybercrimes are relatively new, there is a new way to collect, investigate, and potentially prosecute through computer forensics. As it is a new discipline, there are changes and challenges (compared to traditional forensics) combined with the changing technology and adopting to solve traditional crimes- making computer forensics constantly evolving and recruiting/training forensic investigators always in high demand.

As long as humans have been on earth, crimes of all kinds have existed in the lowest reaches of our societies. These crimes can include human trafficking ranging from forced human labor to sex trafficking. Other examples of crimes as old as time can include espionage, as Taylor et al. (2018) purport that one of the first reported cases was in the 1700's when China's secret production of its porcelain leaked to Europe (p. 111). Crime organizations, such as the Japanese Yakuza that have been around since the 1700's "established control over the portable booths in market fairs held at temples and shrines, and they had a reputation for shoddy goods and deceptive salesmanship" (Gragert, 1997, p. 6).

When personal computers (combined with the internet) and their ease of use, it was simple for these cohorts of criminals to go digital. Human and sex traffickers began using their computers and the internet as part of their tools to recruit their victims. Crime organizations have become professionals, mirroring huge fortune 500 companies using computers and the internet to make their operations more stealthy, widespread, profitable, and organized better. As Taylor et al. (2018) states that Russia's cybercrime organizations "are very proactive at reaching out to the global organized crime marketplace and soliciting business from other cybercrime gangs to use their malware, buy their stolen information, and use their money-making schemes" (p. 126). Russia is a good example of how traditional crime operates as usual yet has adapted to new technologies of the age and have become "better" at what they were doing than before.

It is because these criminals are now using computers to commit their crimes that "law enforcement now uses computers to fight crime" (National Institute of Justice, n.d., para. 1). Because of this need to prevent further criminal acts and catch the perpetrators, computer forensics has come into being. Computer Forensics as defined by US-CERT (2008) is "the discipline that combines 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" (p. 1). This definition clarifies its objective, to gather evidence so that it can be used in a court case and catch criminals.

One of the challenges that computer forensics faces (along with other areas that involve technology) are that technology is constantly evolving by becoming more advanced, faster, better, and efficient. These technological advances that happen daily, monthly, weekly, and yearly require all sorts of updates (software and hardware) and new training, whether in the home for personal use or for businesses, or entities that are public, private, or for government

use. Cell phones, personal computers, and laptops always come out with faster processing, better built-in cameras, more crisp screen resolutions. Convenient cloud storage with more space for a better price, faster internet speeds in the home or via the cellular network, not even to mention the Internet of Things (IoT) that are being interwoven into our everyday lives. Whether a layperson or a professional, one has to keep up or be left behind.

This is especially true for an investigator in computer forensics. As the technology evolves, so do the cybercrimes and thus the forensics that follows. According to Joshi (2021), "Due to rapid changes in the technology, operating system, and application software and hardware, reading digital evidence from an older version to support a newer version is a growing challenge" (para. 8). Joshi is just stating that along with technological advances, experts have to keep up with the pace despite the challenge, or else collecting necessary evidence will suffer as well, if not be impossible.

On this note, investigators should take the initiative to maintain their technological skills, whether by daily news, publications, or information provided by any organizations/entities/workplace initiatives as to what would be necessary, as addressed by Kent et al. (2006, p. 23). Forensic examiners should maintain themselves with the latest technologies and any tools that are required, "pertaining to computer storage media, data types and formats, and other relevant issues" (Kent et al., 2006, p. 31). Essentially to be a computer forensic expert and maintain the job responsibilities required, the expert should consider taking coursework to keep their skills updated, along with any tools and techniques that would keep them up to date. As well as on-the-job experience, on top of any certifications that might be necessarily relevant to "computer storage media, data types and formats" (Kent et al., 2006, p. 31). These are best practices to maintain any changes in policies or the law (Kent et al., 2006, p. 31).

Another challenge faced in computer forensics is how it is conducted, standardized, and maintains a reputation that ultimately allows any evidence collected during an investigation to be accepted in a court case. Computer forensics is based on traditional forensics (because there has always been crime and thus evidence to collect and present in a court case), there has been a standard set amongst law enforcement. Forensics means "to bring to the court" (US-CERT, 2008, p. 1). The main difference between forensics and computer forensics is that forensics deals with latent evidence, which includes different things (such as fingerprints that can be lifted, DNA analyzed from a bloodstain to files recovered on a hard drive). Computer forensics involves data collected from computers where there might be a digital fingerprint versus a literal one (US-CERT, 2008, p. 1).

Computer forensics (because it is so new) has "little standardization and consistency across the courts and industry" thus, it is not considered to be a "formal 'scientific' discipline," and it is defined as "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). The way that computer forensics can be viewed (so far long as validity is concerned) is that it just has not been around long enough for a standard to be set. Nevertheless, there is no doubt that it will happen in the future because it will no longer be a new discipline, and consistency will be developed with the gift of time. This is a challenge now because if local, state, and federal laws are not followed, or an investigator does a poor job of collecting forensic data evidence, it would not be allowed in a court case. This goes against the literal meaning of forensics (US-CERT, 2008, p. 2). The conclusion is that the burden is high (as it should be) on the computer forensics investigator.

Computers are used for digital crimes, so it is only natural to think that computers are used to collect digital evidence. However, an advantage is that it is not uncommon for Law Enforcement to use computers to help solve traditional crimes (e.g., physical theft, robberies) (National Institute of Justice, n.d., para. 2). An example would be a kidnapping taking place. The potential suspect might have their mobile account, mobile phone, or computers looked at to track a person, their movements, the money they may have spent, or the people they have contacted (National Institute of Justice, n.d., para. 2). A famous case is where the BTK killer had remained elusive from law enforcement for 31 years until a "floppy disk led investigators" to the killer that "claimed the lives of at least 10 victims" (National Institute of Justice, n.d., para. 2). It is evident that computer forensics is a necessary component for law enforcement to do their jobs regardless of the specific crime that is committed.

Due to the need for computer forensics (as it is helpful for potential criminal activities or harmful breaches in an entity), there is a high demand for trained computer forensic investigators in law enforcement. Most organizations consist of three groups of staff in order to operate computer and network forensics: Investigators, IT Professionals, and Incident Handlers (Kent et al., 2006, p. 17). The main issue is that these highly trained professionals and experts also come at a high cost for an organization. The experience and skills that such individuals have acquired for a specific digital forensic investigative need make them high in demand, thus a shortage (Kent et al., 2006, p. 18). Expected job growth is at "16% from 2020 to 2030" (U.S. Bureau of Labor Statistics, 2021, para. 4).

It is evident that computer forensics has a considerable role in law enforcement regarding all crimes involving computers or networks. Investigators are integral in ensuring the collection process is thorough from the crime scene to the courtroom and that these experts are in high

demand and need maintaining training. It is also clear that there are challenges for computer forensics, but these must be faced to make it a well-respected discipline in the ever-changing world of technology. Above all else, it is evident that computer forensics and the investigator play an integral role in law enforcement, and its continued growth will only expand as technology advances.

References

Gragert, B. A. (1997). Yakuza: The warlords of Japanese organized crime. *Annual Survey of International & Comparative Law, 4*(1), 147-204. https://digitalcommons.law.ggu.edu/annlsurvey/vol4/iss1/9

Joshi, P. S. (2021, August 20). *Challenges and applications of digital forensics*. Cisomag. https://cisomag.eccouncil.org/challenges-and-applications-of-digital-forensics/

Kent, K., Chevalier, S., Grance, T., & Dang, H. (2006, August). *Guide to integrating forensic techniques into incident response*. National Institute of Standards and Technology. https://nvlpubs.nist.gov/nistpubs/legacy/sp/nistspecialpublication800-86.pdf

National Institute of Justice. (n.d.). *Digital evidence and forensics*. Retrieved October 31, 2021, from https://nij.ojp.gov/digital-evidence-and-forensics

Taylor, R. W., Fritsch, E. J., Saylor, M. R., Liederbach, J. R., & Tafoya, W. L. (2018). Cyber Crime and Cyber Terrorism (4th ed.). Pearson.

U.S. Bureau of Labor Statistics. (2021, September 8). *Occupational Outlook Handbook: Forensic Science Technicians*. https://www.bls.gov/ooh/life-physical-and-social-science/forensic-science-technicians.htm

US-CERT. (2008). *Computer Forensics*. https://us-cert.cisa.gov/sites/default/files/publications/forensics.pdf

Good Job on the paper

James Freedle , Dec 11 at 9:11am