Career Paper – Digital Forensics

Antonio Shields

School of Cybersecurity, Old Dominion University

CYSE 201S: Cybersecurity and the Social Sciences

Dr. Leigh Armistead

November 20, 2022

Digital forensics, according to Evans et al. (2011), is a branch of forensic science that was developed in response to a pressing need in the early 1990s. (p. 1). Although there may have been cybercrime occurring before the 1970s, there were no specific laws established against cybercrimes. (Upguard, n.d.). All cybercrimes committed at the time were considered ordinary crimes under the existing law.(Upguard, n.d.). The first computer crime was first reported in 1978, which led to the enactment of the Florida Computer Crime Act. (Upguard, n.d.). The Florida Computer Crime Act of 1978 provides legislation against unauthorized modification or deletion of data. (Upguard, n.d.). It wasn't until the 1990s that digital forensics became a well-known term. It was not until the early 21st century that national policies on digital forensics emerged. (EC-Council, 2022). According to Raghavan (2013), the Digital Forensic Research Workshop (DFRWS) Technical committee has defined digital forensic science as:

> The use of scientifically derived and proven methods toward the preservation, collection, validation, identification, analysis, interpretation, documentation and presentation of digital evidence derived from digital sources for the purpose of facilitating or furthering the reconstruction of events found to be criminal, or helping to anticipate unauthorized actions shown to be disruptive to planned operations." (p. 92).

Digital forensics can be broken up into five branches, which are Computer forensics, Mobile device forensics, Network forensics, Forensic data analysis, and Database forensics. (Upguard, n.d.). Computer forensics or computer forensic science is concerned with evidence found in computers and digital storage media. (Upguard, n.d.). The goal of computer forensics is the examination of digital data for the purpose of identifying, preserving, retrieving, analyzing and presenting facts and opinions about digital information. (Upguard, n.d.). Mobile device forensics focuses on recovering digital evidence from mobile devices using proven forensic methods. (Upguard, n.d.). Network forensics focuses on monitoring and analyzing computer network traffic for the purpose of information gathering, legal evidence, or intrusion detection. (Upguard, n.d.). Forensic data analysis examines structured data in regard to incidents of financial crime. (Upguard, n.d.). The purpose is to discover and analyze patterns of fraudulent activities. (Upguard, n.d.). Database forensics is related to databases and their related metadata. (Upguard, n.d.). The cached information may also exist in a server's RAM requiring live analysis techniques. (Upguard, n.d.). Regardless of the branch of digital forensics taken, they all utilize a multi-stage process that begins with identifying the digital media from a scene (possible criminal) that may be potential evidence to the stage where the evidence is presented to a court of law through expert testimony. (Raghavan, 2013, p. 92).

The first stage of the digital forensic process is identifying the relevant digital evidence. (Raghavan, 2013, p. 92). This involves identifying one or more sources of digital storage capable of storing digital information relevant to the current investigation. (Raghavan, 2013, p. 92). Once identified, evidence is obtained from the devices and preserved using forensic means. (Raghavan, 2013, p. 92). After the evidence is obtained, standard hash signatures are used to verify the integrity of the digital evidence. (Raghavan, 2013, p. 92). In a digital forensics investigation, investigators are tasked with collecting digital records for examination. (Raghavan, 2013, p. 92). Digital records can come in different forms and types. (Raghavan, 2013, p. 92). Once the digital evidence is collected, it is always necessary to make copies and conduct all forensic tests on such read-only copies, to prevent any activity from tampering with the data stored within the original sources. (Raghavan, 2013, p. 92). The digital evidence then is examined using multiple forensic tools. (Raghavan, 2013, p. 92). These forensic tools are used to provide

some form of file system abstraction to the digital evidence so that the contents can be examined for traces of evidence. (Raghavan, 2013, p. 92). This stage is called evidence examination where the digital evidence sources are examined for their content and can be indexed for conducting searches. (Raghavan, 2013, p. 92). In some instances, the examination of digital evidence may reveal some hidden or otherwise not explicit information which has to be extracted and subsequently analyzed, this is called evidence discovery (Raghavan, 2013, p. 93). After evidence examination and discovery, forensic analysis begins by analyzing the evidence sources and the discovered data to determine the sequence of events leading to the reported crime under investigation. (Raghavan, 2013, p. 93). The scientific method along with the 5W's (Who, What, When, Where, and Why) and How are applied at this time. (Raghavan, 2013, p. 92). The individual stages are thoroughly documented and this documentation is presented in a court of law, where usually, the presentation of digital evidence in court may be accompanied by expert witness testimony. (Raghavan, 2013, p. 92).

Digital forensics is multidisciplinary in the sense of depending not only on technical aspects of investigation, but on a combination of skills and knowledge of application areas including mathematics, statistics, law and courtroom procedure, government policies, psychology, library science, and finance. (Palmer et al., 2015, p.3). The psychology approach, for example, with digital forensics is looking closely into the motivations of cybercriminals. (Paraben Corporation, 2021). With psychology and digital forensics, businesses can gain knowledge of how, why, and where cybercriminals hack their systems. (Paraben Corporation, 2021). Also, using psychology to anticipate the behaviors of a business's employees, can help protect its assets by learning where the internal vulnerabilities lie. (Paraben Corporation, 2021). As more data comes from social media, smartphones, and cloud-related data to obtain digital forensics, the data will reflect more of an accurate timeline of the digital life of a potential suspect. (Paraben Corporation, 2021). Looking at the psychology behind that data adds a deeper view that can be valuable to an investigation. (Paraben Corporation, 2021).

Having people of different races, ethnicities, genders, socioeconomic statuses, and backgrounds in the workplace can foster innovation, problem-solving, and competitiveness. (Wagstaff & LaPorte, 2018, p. 1). Research has shown that diverse teams perform better, are more creative, and perform better than homogeneous groups. (Wagstaff & LaPorte, 2018, p. 1). The growing diversity of thoughts, perspectives and backgrounds enables new and more complex research problems and questions to be addressed. (Wagstaff & LaPorte, 2018, p. 1). With the entire forensic science profession continuing to evolve and modernize, it is imperative that all segments of the population are valued and leveraged to tackle complex criminal justice issues. (Wagstaff & LaPorte, 2018, p. 9). It is well documented that diversity in STEM fosters innovation and discovery, broadens the questions that can be probed, and taps into unique perspectives and skill sets. (Wagstaff & LaPorte, 2018, p. 9). While gender, racial, and ethnic diversity is essential to expanding the pool of forensic and criminal justice researchers, the diversity in scientific disciplines is equally important in order to take advantage of more interdisciplinary approaches to problem-solving. (Wagstaff & LaPorte, 2018, p. 9).

Digital forensics is not strictly limited to just digital and computing environments, it has a societal impact. (BlueVoyant, n.d.). As computers and technological devices are now used in every aspect of life, digital evidence has become essential in solving many types of crimes and legal problems, in both the digital and physical world. (BlueVoyant, n.d.). Digital evidence obtained from these devices can be used for investigations and legal proceedings like Data theft and network breaches, Online fraud and identity

theft, Violent crimes like burglary, assault, and murder, and White collar crimes as examples. (BlueVoyant, n.d.).

Some of the concepts from class that the Digital Forensics field must have are Parsimony, where when providing testimony or explaining their finds, they must keep the level of explanation as simple as possible. They will have to explain their findings so that members of the court will be able to understand it plain and simple. They will also have to utilize Empiricism and only use facts and data to conduct methods and procedures and to understand their findings. Digital Forensics requires ethical neutrality where they must adhere to ethical standards when they conduct their research and procedures. Any deviation in standards can compromise the evidence and make it admissible in court. Also, relativism is utilized to problem-solve the digital evidence obtained and analyzed to discover the relationship between the evidence and potential suspects.

Works Cited:

Digital Forensics. EC-Council. (2022, November 9). Retrieved November 30, 2022, from https://www.eccouncil.org/what-is-digital-forensics/#phase-iii---collect-the-evidence

Evans, A., Williams, A., & Graham, J. (2011). *Future of Digital Forensics: A Survey of Available Training*. The Steering Committee of The World Congress in Computer Science, Computer Engineering and Applied Computing (WorldComp).

Palmer, I., Wood, E., Nagy, S., Garcia, G., Bashir, M., & Campbell, R. (2015). Digital Forensics Education: A multidisciplinary curriculum model. *Lecture Notes of the Institute for Computer Sciences, Social Informatics and Telecommunications Engineering*, 3–15. https://doi.org/10.1007/978-3-319-25512-5_1

Raghavan, S. (2012). Digital Forensic Research: Current State of the art. *CSI Transactions on ICT*, *1*(1), 91–114. https://doi.org/10.1007/s40012-012-0008-7

The role of psychology in Digital Forensics. Paraben Corporation. (2021, August 24). Retrieved November 30, 2022, from https://paraben.com/the-role-of-psychology-in-digital-forensics/#:~:text=Online%20forensic%20psychology%20programs%20teach,operate%20in%20today's%20digital%20landscape.

Understanding Digital Forensics: Process, techniques, and Tools. BlueVoyant. (n.d.). Retrieved November 30, 2022, from https://www.bluevoyant.com/knowledge-center/understanding-digital-forensics-process-techniques-and-tools

Wagstaff, I. R., & LaPorte, G. (2018, March 8). *The importance of diversity and inclusion in the forensic sciences*. National Institute of Justice. Retrieved November 30, 2022, from https://nij.ojp.gov/topics/articles/importance-diversity-and-inclusion-forensic-sciences

What is digital forensics? Upguard. (n.d.). Retrieved November 30, 2022, from https://www.upguard.com/blog/digital-forensics