Digital Forensics

Zack Wedding

Charleston Southern University

CSCI 405: Principles of Cybersecurity

Prof. Patrick Hill

November 15th, 2023

What is Digital Forensics?

- According to *Interpol*, "digital forensics is a branch of forensic science that focuses on identifying, acquiring, processing, analyzing, and reporting on data stored electronically"
- The main goal of digital forensics is to get data from electronic evidence, process it into "actionable intelligence", and present evidence found for prosecution

Why is Digital Forensics Important?

- *Interpol* tells us that almost all criminal activity has some sort of electronic evidence, which makes digital forensics very important for law enforcement investigations
- Computerized devices are used everywhere for just about everything, so it is not a surprise that digital evidence is becoming more and more important

Different Branches of Digital Forensics

- *Blue Voyage* tells us that there are five main branches of digital forensics: computer forensics, mobile device forensics, network forensics, forensic data analysis, and database forensics
- Computer forensics "investigate computers and digital storage evidence"
- Mobile device forensics focuses of retrieving evidence from mobile devices
- Network forensics "monitors, registers, and analyzes network activities"
- Forensic data analysis examines structured data that is found in application systems and databases
- Database forensics investigates "access to databases and reporting changes made to the data"

Digital Forensics Process

- *Blue Voyant* says that the digital forensics process may vary depending on the scenario, but typically consist of four steps: collection, examination, analysis, and reporting
- Collection "involves acquiring digital evidence, usually by seizing physical assets"
- Examination "involves identifying and extracting data"
- Analysis "involves using collected data to prove or disprove a case built by the examiners"
- Reporting "involves synthesizing the data and analysis into a format that makes sense to laypeople"

Digital Forensics Techniques

- According to *BlueVoyant*, there are several digital forensics techniques that can be used to help inspect unallocated disk space and hidden folders for copies of encrypted, deleted, or damaged files
- Reverse steganography "involves analyzing the data hashing found in a specific file" to find data inside of digital files, messages, or data streams
- Stochastic forensics "helps analyze and reconstruct digital activity that does not generate digital artifacts"
- Cross-drive analysis finds similarities to help provide some context for the investigation and uses those similarities as guidelines to catch suspicious activity
- Deleted file recovery helps recover deleted files

Becoming a Digital Forensics Investigator

- According to *EC-Council* forensic analysts typically work for police, law enforcement agencies, government, private, or other forensic companies
- Key job roles include cybersecurity forensics consultant, forensics engineer, computer forensic technician, cyber forensic investigator, and more
- Required skills include defeating anti-forensic techniques, understanding hard disks and file systems, operating system forensics, cloud forensics, mobile device forensics, investigating email crimes, and more
- The average salary of a digital forensics investigator is $72,929

Common Uses of Digital Forensics

- Can help understand how a breach happened and who the attackers were
- Can help understand the impact of a breach on organizations and the organization's customers
- Can capture digital evidence on an electronic that can be used in an investigation
- Can collect evidence that helps deal with white collar crimes such as corporate fraud, embezzlement, and extortion

History of Digital Forensics

- In the 1970's and 1980's, digital forensics teams consisted of people with a computer background who worked for law enforcement agencies
- Once most documentation happened digitally, data storage became an issue for law enforcement, which lead to the FBI launching the Magnet Media program in 1984
- Digital forensics grew once child pornography started to spread more online
- The war between Iraq and Afghanistan grew the need for digital forensics, as it "played a major role in extracting the evidential data from the digital assets gathered by U.S. troops during the war" (*EC-Council)*

Digital Forensics and the Law

- According to Jerry Wegman, the prominent federal statutes that impact digital forensics are the Electronic Communications Privacy Act (ECPA), Wiretap Statute, Pen/Trap Statute, and USA PATRIOT Act
- The ECPA is often "the controlling legal authority with regard to stored computer files that have been transmitted to a network administrator"
- The Wiretap Statute "deals with direct surveillance or real-time interception of electronic communications by government agents"
- The USA PATRIOT Act enlarges the scope of forensic investigations and "authorizes the expenditure of $50 million for the creation and support of regional computer forensic laboratories"

Famous Digital Forensics Cases

- Murder of Kari Baker: in 2010, Kari Baker had died from what looked to be a suicide by sleeping pills, however, after searching her husband's computer, he was convicted of murdering his wife after it was found that his search history revealed searches about overdosing on sleeping pills
- The BTK Killer: Dennis Rader murdered 10 people from 1974 to 1991, and in 2004 he taunted police by sending both police and media outlets items from his crimes; one of the items that Rader sent to a media outlet was a floppy disk that contained a puzzle, and police were able to extract data on the disk and trace it back to Rader
- Michelle Carter and Conrad Roy: Michelle Carter was convicted on involuntary manslaughter after text messages showed that she was able to convince her then-boyfriend Conrad Roy to commit suicide

References

4 Cases Solved With Digital Evidence | Precise Digital. (2020, January 17). https://precisedigital.com/4-cases-solved-with-digital-evidence/

Bluevoyant. (2023). Understanding Digital Forensics: Process, Techniques & Tools. BlueVoyant. https://www.bluevoyant.com/knowledge-center/understanding-digital-forensics-process-techniques-and-tools

EC-Council. (n.d.). What is Digital Forensics | Phases of Digital Forensics | EC-Council. EC-Council Logo. https://www.eccouncil.org/cybersecurity/what-is-digital-forensics/

Interpol. (2023). Digital forensics. Www.interpol.int. https://www.interpol.int/en/How-we-work/Innovation/Digital-forensics#:~:text=Digital%20forensics%20is%20a%20branch

Wegman, J. (n.d.). COMPUTER FORENSICS: ADMISSIBILITY OF EVIDENCE IN CRIMINAL CASES. https://webpages.uidaho.edu/wegman/JerryWegmanPapers/Computer%20Forensics%20AA%202004.htm