INTERNATIONAL JOURNAL
FOR RESEARCH

IN APPLIED SCIENCE & ENGINEERING TECHNOLOGY

www.ijraset.com

Call: ⓒ08813907089 | E-mail ID: ijraset@gmail.com

Introduction to Digital Forensics

Sajin Shivdas

Department of Cybersecurity, EC-Council University

Abstract: Crimes committed using computers are increasing rapidly, posing a challenge to law enforcement. Investigations including cybercrime, terrorism, and civil litigation all make use of digital forensics today. Because of the ever-increasing sophistication of modern technology, forensic investigations of this sort can quickly become difficult and time-consuming. In order to successfully retrieve meaningful digital evidence during such investigations, however, a standard framework for digital forensic professionals to follow must be developed. All appropriate steps that a digital forensic investigation would take should be highlighted by the framework and methodology used to conduct digital forensics. This study provides a system for conducting digital forensic investigations with an emphasis on the forensic aspects of those probes, the tools and procedures employed by examiners, and the significance of hashing in preventing the manipulation of evidence.
Digital forensics, as a whole, is still a field that is widely growing along with the continually advancing world of technology. This form of forensics is one that is also growing in importance and necessity due to crimes stemming from digital devices becoming increasingly popular as well. These steady numbers are what have and will continue to drive the field of digital forensics into meeting its full potential on a consistent basis, in both a preventative and recovering manner. However, in order to recognize this potential, it is important to first understand what digital forensics really entails

I. INTRODUCTION AND BACKGROUND

The field of study known as "Digital Forensics" focuses on the analysis of digital evidence, usually in the context of computer-related crimes. There are several uses for the findings of digital forensics investigations. Most frequently, this is done in legal settings, either to back up or disprove a theory. Due to its youth and fluidity, digital forensics is always evolving.

This is done to ensure that no corrupt data can make its way into the system. Information is retrieved, then classified and stored. The data was then reviewed to establish how the company was compromised and where the vulnerabilities were. A report documenting the events leading up to the breach is typically the final product of digital forensics. This paper will discuss the methods used in digital forensics, the significance of forensic tools in the gathering and analysis of evidence, the role of hashing in digital forensics, and the relevance of preserving the integrity of collected data.

Digital forensics, as a whole, is still a field that is widely growing along with the continually advancing world of technology. This form of forensics is one that is also growing in importance and necessity due to crimes stemming from digital devices becoming increasingly popular as well.

These steady numbers are what have and will continue to drive the field of digital forensics into meeting its full potential on a consistent basis, in both a preventative and recovering manner. However, in order to recognize this potential, it is important to first understand what digital forensics really entails.

II. DIGITAL FORENSIC METHODOLOGY

The investigator's actions should be at the center of any inquiry of the processes involved in digital forensics evidence collection. To do this, one must be familiar with the four phases that make up digital forensics methodology: collection, inspection, analysis, and reporting. With such little room for the kinds of mistakes that are all too usual, it is vital to follow the rules established at each stage when dealing with evidence.

What occurs in each phase is as follows:
1) Preparation
2) Extraction
3) Identification
4) Analysis
5) Reporting

A. Preparation

The first stage in the forensic process is to inspect all of your gear and software to ensure it is up to par. The security posture of an organization and its systems dictate how often software and hardware should be evaluated. However, before bringing new hardware or software into use, all businesses should have it validated. Additionally, retesting must be done after each update, patch, or configuration change. This establishes a benchmark that may be used by any forensics expert. Part of getting ready for an analysis is making sure the data is accurate. The forensic approach is aided by obtaining a working copy of the compromised data and a forensic image of the data on the original medium. Using forensics tools, it is possible to do searches on the compromised data and learn more about the nature and extent of the breach.

B. Extraction

The process of collecting volatile data is essential since it evolves over time. Network connections, ARP cache, logged-in sessions, running processes, open files, and RAM contents are some potential acquisition orders for volatile data. The acquisition, handling, and chain of custody of the evidence should be able to provide this. Due to the prevalence of anti-forensic detection programs, it's vital that you tread carefully. Avoiding discovery of events, disrupting information collecting, lengthening examination times, and casting doubt on forensic outcomes are all examples of anti-forensics. Anti-forensics can also be used to expose the presence of a forensic tool, to use the forensic tool to attack the examiner's organization, or to launch an attack on the examiner themselves. Although many of these tools are detectable, the fact that there is a chance of getting hacked again during this procedure raises multiple red flags and should be handled carefully.

C. Identification

Each item in the list of prep information undergoes the same identifying procedure. A processed item has been identified by its type and its significance to the forensic report. Anything that could be used as evidence during the investigation is reported up the chain of command. The Relevant Data List is where we save everything that's actually useful. Information related to the initial security breach is included on this list. There's always a chance that something you own will spark an idea for something else. An email may contain information on other hackers or the data breach itself. Results and pertinent data have now been communicated to corporate.

D. Analysis

During this stage, findings from the incident investigation's preceding steps are summarized and reported. Now is the moment to compare hashes across the system. Some hash comparison tasks can be simplified with the help of programs like hfind. Hashing is a technique for fast indexing and retrieving data by converting characters from the data into keys. When it comes to authenticating digital signatures, the approach is also utilized for encryption and decryption of data. The who, what, where, and why questions about each piece of data on the relevant list are resolved. Where the security breach occurred, what computer was hacked, and how this mess even started are all explained. By analyzing the timing of events and creating a timeline, it's simple to give a logical account of what took place and why. A forensic report detailing all the findings is then prepared after this process has been repeated several times.

E. Reporting

Steps must be taken at this stage for the acquired data to be presented, typically in a courtroom. First and foremost, there must be numerous reports and documents present, such as notes (with dates, times, and descriptions of actions), chain of command log, list of authorized users, passwords, and networks used on the device, additional notes of step-by-step process that was taken; detailed enough for someone else to copy the actions exactly, what operating system and patches were installed on the device, and lastly, documentation of the device's configuration (Department Justice, 2014).

III. DIGITAL FORENSICS TOOLS

Users of digital forensics tools come from a wide variety of disciplines and specializations, reflecting the growing importance of forensics in modern investigations (Hibshi, 2011). Toolkits built for Windows, Linux, and Mac are used to do forensic analysis. Developer-created aids for gathering digital evidence as it will be accomplished with the help of the tool kits, each of which has its own set of technical parameters. With each new incident, criminals become more cunning, therefore businesses must respond by creating cutting-edge technologies that shorten the investigative time. National Institute of Standards and Technology (NIST) is developing new as per the work carried on by Computer Forensics Tool Testing" (NIST, 2022), see *References* for details, to its comprehensive catalog of forensic tools.

A. Importance of Forensic tools

If you need trustworthy computer analysis or Digital Evidence collection for any number of judicial or business purposes, you can count on tools developed specifically for digital forensics. It is common practice to employ such instruments during computer-related judicial proceedings in order to gather evidence of criminal activity. In addition to their employment in law enforcement, the same technologies are also put to use in non-official capacities, such as system upkeep, debugging, data recovery, and reverse engineering (Hibshi, 2011). Inappropriate and illegal activities like cybercrime, e-mail and Internet abuse, fraud, financial mismanagement, unauthorized disclosure of corporate information, and intellectual property theft can all be traced back to information stored on computer hard drives, and this software is designed to help security personnel, law enforcement, and legal investigators do just that. E-discovery activities in the context of civil litigation and regulatory compliance are also making increasing use of these instruments (Brandel, 2008). Forensic Toolkit (FTK) Imager and EnCase are two widely used programs around the world.

1) FTK

As far as digital forensics goes, FTK is the gold standard. This suite's features include, but are not limited to, the ability to decipher encrypted files and emails, visualize data to examine it visually, filter and classify it, and so on

2) EnCase

Forensic investigations involving computers and servers frequently make use of EnCase, a commercial digital forensics application. EnCase's features can be expanded upon because to the software's modifiability, powerful scripting capabilities, and abundance of available third-party modules. Expertise with EnCase and its processing and analytical skills is essential for today's digital forensic investigators (UMUC)

IV. HASHING AND EVIDENCE TAMPERING

Hashing is the process of using hash functions to ensure a copy of a file is identical to its original. In digital forensics, hash functions like MD5 (Message Digest) and SHA (Secured Hash Algorithm) are used to compute and verify that a data set has not been modified as a result of the use of different evidence gathering and processing tools and methods. Since the hash validates the integrity of the disk image, it plays a crucial role in the scope of forensics investigations. At any moment during or after the investigation, any interested party should be able to rehash the disk image and obtain the same hash value as the original.

Some methods used to protect tangible evidence from tampering include password protection, encryption, tamper-evident seals, and airtight plastic bags. On the other hand, hashing is the most reliable method for protecting digital evidence. The hash of a duplicate will no longer be the same as the original if even a single bit of data is altered from the original. No one will be able to miss the meddling. Legal proceedings can be significantly impacted by digital evidence. Further, just as with any other physical evidence, it is crucial that law enforcement keep a clear, documented line of custody for the evidence they collect. A trail must record who handled the evidence, when, and why from the minute it was obtained. In order for digital evidence to be acceptable in court, its integrity must be preserved along the chain of custody.

V. CONCLUSION

A. The Outcome of Analysis and Studies

1) Summary of Findings

In conclusion, digital evidence is everywhere. Digital forensics is an important aspect of not only law enforcement investigations, but also; counter-terrorism investigations, civil litigations, and investigating cyber-incidents. Digital forensics tools play a critical role in providing reliable computer analysis and digital evidence collection to serve a variety of legal and industry purposes. In addition to evidence collection and analysis tools and procedures, hashing is pivotal in the scope of forensics investigations. As the world continues to immerse deeper and deeper into digital technologies and devices, it will be critical agencies develop a well thought out strategy for digital forensics and evidence handling.

REFERENCES

[1] Department Justice, U. S. (2014). Forensic Examination of Digital Evidence: A Guide for Law Enforcement.

[2] Hibshi, H., Vidas, T., & Cranor, L. (2011, May). Usability of forensics tools: a user study. Usability of Forensics Tools: A User Study. https://scholar.google.com/citations?view_op=view_citation&hl=en&user=6p23pUgAAAAJ&citation_for_view=6p23pUgAAAAJ:hefNtdE4IMkC

[3] Brandel, M. (2008, June). Rules of Evidence - Digital Forensics Tools | CSO Online. CSO Online. https://www.csoonline.com/article/2117658/rules-of-evidence---digital-forensics-tools.html

[4] NIST, N. (2022, August). Computer Forensics Tools & Techniques Catalog - Home. Computer Forensics Tools & Techniques Catalog - Home. https://toolcatalog.nist.gov/index.php

[5] Jadhav, H. (2022, May). Computer forensics: chain of custody. Nasscom Community | The Official Community of Indian IT Industry. https://community.nasscom.in/communities/cyber-forensics/computer-forensics-chain-custody

[6] Forensics Digest. (2020, July 12). Hashing and Data Imaging - Forensics Digest. Forensics Digest. https://forensicsdigest.com/hashing-and-data-imaging/

INTERNATIONAL JOURNAL FOR RESEARCH

IN APPLIED SCIENCE & ENGINEERING TECHNOLOGY

Call : 08813907089 (24*7 Support on Whatsapp)