PERSPECTIVES

Cyber Forensic Analysis: Strengthening Digital Evidence for Legal Proceedings

July 2023

Introduction

Cybercrime poses an escalating threat in the digital age, with cybercriminals developing increasingly sophisticated techniques to stay one step ahead. Consequently, detecting and preventing cyber-criminal activities have become more challenging. In response to this growing threat, law enforcement agencies and legal professionals have turned to cyber forensic analysis as a reliable method of gathering evidence for legal proceedings. This article explores the process of cyber forensic analysis, emphasising the importance of adhering to established guidelines and procedures and the need to invest in this technology to combat cybercrime effectively.

Cyber Forensic Analysis: Collecting, Preserving, and Analysing Digital Evidence

Cyber forensic analysis involves a comprehensive approach to collecting, preserving, handling, and analysing digital evidence, the information stored or transmitted in binary form that may be relied upon in court. Such evidence can be found on a computer hard drive or mobile phone, among other places, and the forensic analysis process ensures its integrity and admissibility in formal proceedings. The process requires strict adherence to established guidelines and procedures that guarantee the reliability of the evidence [1], such as those created by Interpol [2] or the International Organization on Computer Evidence [3], for instance.

Identification Phase: Obtaining Preliminary Information

The identification phase marks the first step in the cyber forensic analysis process. During this phase, forensic investigators gather preliminary information regarding the cybercrime case, such as details on the parties involved, the nature of the crime, when and where it occurred, and the methods employed. This helps the forensic investigator collect the data in a forensically sound way, all while following recognised standards and best practices (e.g. National Institute of Standards and Technology guidelines in the United States [4]).

One of the significant dangers of a late identification phase in an investigation is the potential loss or degradation of critical evidence. As time passes, digital evidence can be modified, deleted, or overwritten, intentionally or as a part of regular system operations. In some cases, cybercriminals might actively work to erase their traces after committing a crime, making it even more challenging to gather helpful evidence. If the identification phase is delayed, investigators might miss the chance to capture volatile data such as active network connections, running processes, or in-memory data.

Another risk is the continuation of malicious activities. Any delay to the identification phase could risk perpetrators extending their illegal activities, causing more damage to victims. They could steal more data, disrupt systems, or spread their activities to other parts of the victim's network.

During the identification phase, investigators will likely encounter sensitive data. This could include personal information, proprietary data, or confidential business details. There are various regulations concerning the protection of this data, like the General Data Protection Regulation (GDPR) [5,6], in the European Union or the California Consumer Privacy Act (CCPA) [7] in California, USA. They provide guidelines on how personal data should be treated during investigations, including requirements for consent, data minimisation, and transparency.

It is essential to follow these regulations and any related local laws during the identification phase of a cyber forensic analysis and throughout the investigation. Violations of such data protection rules can result in legal challenges, financial penalties, and damage to the reputation of the investigators or their organisations.

Notes

[1] US National Institute of Justice, "Digital Evidence and Forensics", https://nij.ojp.gov/digital-evidence-and-forensics

[2] Interpol, "Guidelines for Digital Forensics First Responders", March 2021, https://www.interpol.int/content/download/16243/file/Guidelines%20to%20Digital%20Forensics%20First%20Responders_V7.pdf

[3] ISO/IEC 27037:2012, "Guidelines for identification, collection, acquisition, and preservation of digital evidence", The standard was first published in 2012 and confirmed unchanged in 2018, https://www.iso.org/standard/44381.html

[4] Casey, E. (2011). Digital evidence and computer crime: Forensic science, computers, and the internet (3rd ed.). Academic Press

[5] European Council (September 2022), "The general data protection regulation", https://www.consilium.europa.eu/en/policies/data-protection/data-protection-regulation

[6] European Union (2016). Regulation (EU) 2016/679 (General Data Protection Regulation). Retrieved from https://eur-lex.europa.eu/eli/reg/2016/679/oj

[7] State of California Department of Justice (May 2023), "California Consumer Privacy Act (CCPA), https://oag.ca.gov/privacy/ccpa

Preservation of Evidence: Ensuring Integrity

Once the identification phase is complete, evidence preservation becomes crucial to maintaining the integrity of digital evidence. This involves establishing a strict chain of custody and employing proper storage and handling procedures. A chain of custody is a process that creates a trail or record of all actions applied to the digital evidence, ensuring that its integrity remains intact throughout the analysis. The evidence becomes admissible in formal legal proceedings by meticulously documenting each step. [8]

Examination and Interpretation: Communicating Findings

After evidence preservation, cyber forensic experts examine and interpret digital evidence, communicating their findings in a forensic report. This report should be clear, precise, and inclusive, providing the scope of the investigation, supporting documents, and a detailed explanation of the methods and steps taken to examine, identify and extract digital evidence. Forensic investigators must possess a solid technical skillset, covering all types of digital media and practical communication skills, to effectively explain complex technical concepts in plain language, allowing non-technical individuals, including judges and juries, to comprehend the findings readily. [9]

Admissibility and Judicial Scrutiny

Different jurisdictions have different legal standards for the admissibility of digital evidence. Generally, evidence must be relevant, reliable, and authenticated to be admissible. The cyber forensic analysis process may also be subjected to judicial scrutiny, and the investigator may be required to testify in formal proceedings regarding their analysis. To ensure the trustworthiness of the digital evidence, it is essential to have a robust analysis process and comprehensive documentation.

Factors Affecting Reliability

The reliability of the cyber forensic analysis process depends on several critical factors. Firstly, the qualifications and experience of the forensic investigator play a crucial role in conducting a thorough and accurate analysis. Secondly, adherence to established procedures and guidelines, such as those mentioned earlier, ensures consistency and reliability in the analysis process. Finally, maintaining a strict chain of custody, meticulously documenting each step, is imperative to preserve the integrity of the digital evidence. [10]

Importance and Future Significance

The evolution of technology and the rising prevalence of cybercrime make cyber forensic analysis increasingly important. With digital devices becoming ubiquitous in everyday life and business operations, the potential for cybercrime has grown. Consequently, investing in cyber forensic analysis is essential for law enforcement agencies and legal professionals to combat cybercrime effectively. It provides a sound, objective method of gathering evidence that can be used in legal proceedings to hold cybercriminals accountable. [11]

Cyber forensic analysis is a critical weapon in the ever-changing cybercrime landscape. The integrity of the forensic analysis process must be fortified by leveraging cutting-edge tools and techniques that keep pace with rapid technological advancements. As cyber criminals devise more sophisticated attack methods, forensic investigators must capitalise on technological progress, including machine learning and artificial intelligence, to identify, trace, and interpret digital evidence more effectively. [12]

Prevention and Resolution

It is worth noting that cyber forensic analysis is not just about crime resolution; it also plays a critical role in crime prevention. By uncovering the modi operandi of cybercriminals, forensic findings can feed into broader cyber defence strategies, assisting in creating more resilient systems and awareness programs.

However, the scope of cyber forensics extends beyond the purely technical. The importance of education and communication with legal professionals cannot be overstated as the field becomes increasingly intertwined with the judicial system. This involves translating complex technical evidence into understandable information that can be used in court, fostering greater understanding and cooperation between the technical and legal fields.

Notes

[8] Quick, D., & Choo, K. R. (2013). Forensic collection of cloud storage data: Does the act of collection result in changes to the data or its metadata? Digital Investigation, 10(3), 266-277

[9] Choo, K. R., & Dehghantanha, A. (2016). Cloud storage forensics. Syngress

[10] Palmer, G. (2001). A road map for digital forensic research. Report From the First Digital Forensic Research Workshop, DFRWS

[11] European Union (2016). Regulation (EU) 2016/679 (General Data Protection Regulation). Retrieved from https://eur-lex.europa.eu/eli/reg/2016/679/oj

[12] Garfinkel, S. L. (2010). Digital forensics research: The next 10 years. Digital Investigation, 7, S64-S73

Conclusion

Cyber forensic analysis is a critical tool in combating cybercrime. Reliability depends on the forensic investigator's qualifications and experience, adherence to established procedures and guidelines, and maintaining a strict chain of custody. Given the evolution of technology and the prevalence of cybercrime, it is crucial to develop objective cyber forensic findings that can assist in investigating and prosecuting perpetrators of crime or absolve an innocent person from suspicion. By implementing robust cyber forensic analysis practices, law enforcement agencies and legal professionals can strengthen their ability to combat cybercrime effectively and uphold the rule of law.

Contacts

Darren Mullins
Partner
darren.mullins@accuracy.com
+971 56 682 5681

Morgan Heavener
Partner
morgan.heavener@accuracy.com
+33 7 84 46 13 26

Paul Wright
Senior Adviser
paul.wright@accuracy.com
+971 522 449429

Accuracy partners and professionals are available to discuss your needs and design an appropriate solution with the relevant experts.