The Role of Forensics in IT

Reading

1h

Status | Incomplete

Introduction

Ever heard of Edmond Locard (1877–1966)? He is a must-know in the field of forensic investigation. Operating out of Lyon, France in the first half of the twentieth century, Edmond came up with a concept that still resonates today in the field of IT. His idea was simple yet powerful: every interaction leaves a trace. Think of it like the footprints you leave on the sand as you walk along a beach.

Just like in physical crime scenes where detectives uncover fingerprints or fabric fibers, the digital world has its version of these traces. Every action on a network, server, or device leaves behind digital footprints. As you delve into the world of IT forensics, you'll discover how these traces are often the keys to uncovering cyber crimes and data breaches.

This reading introduces you to the role forensics play in IT. It refers to the process of investigating and analyzing digital evidence to determine the cause of security incidents, data breaches, or other forms of cybercrime.

As you start a new role in IT and Cyber Security, you'll often find yourself playing detective, peering into the depths of digital devices to recover lost or deleted data, or connecting information from different sources to identify security breaches or cybercrime. The reports you produce can guide high-level decision-making or even serve as evidence in a court case. As a part of an incident response team, your analysis can help enhance the organization's security systems and prevent future incidents.

Forensic investigations may be required for databases, email, server logs, user activity logs via centralized logging systems, and breakdown of malware flow. Some key skills you would want to develop are a keen analytical mind, technical expertise, and attention to detail. It will push you to spot anomalies in datasets, understand complex digital evidence, and maintain composure under pressure.

By the end of your journey into IT forensics, you will have not just learned, but experienced, the intersection of technology and investigative work. You will be part of a community of professionals dedicated to combating digital misconduct and upholding cyber integrity.

Reading

Defining Forensics in IT

Just as a physical forensic investigator may have expertise in a particular type of evidence, digital forensic investigators may specialize in a particular area. Here it is broken down:

- **Database forensics** is the investigation and analysis of databases to find and save evidence of when an attacker tries to access the database without permission, up to and including when information is stolen from it. This is done by looking at

how the database is set up, how people use it, and what the computer keeps track of in its logs, to find the digital traces left behind that someone was doing something they shouldn't have.

Can you think of an example where database forensics might come in handy? *Click Toggle Answer to share your thoughts.*

Your Answer

Type in your answer here and Compass will let you reveal our answer below. Compass will auto-save your answer as you type. Once you click Toggle Answer below, your answer cannot be changed.

Toggle Answer

- **Email forensics**: here, you're the digital Sherlock Holmes of emails, scanning messages and email systems to uncover traces of fraud or cybercrime. You'll delve into email servers, attachments, and other data to find the origins of threats.

What kind of evidence might you look for in email forensics? *Click Toggle Answer to share your thoughts.*

Your Answer

Type in your answer here and Compass will let you reveal our answer below. Compass will auto-save your answer as you type. Once you click Toggle Answer below, your answer cannot be changed.

Toggle Answer

- **Malware forensics** investigates dangerous software called malware. Your goal? To figure out where it came from, what it does, and what damage it has caused. Experts examine the code of the malware, how it communicates with other computers on the network, and any records the system has kept of what happened.

Consider a malware attack scenario; what information would be useful to uncover? *Click Toggle Answer to share your thoughts.*

Your Answer

Type in your answer here and Compass will let you reveal our answer below. Compass will auto-save your answer as you type. Once you click Toggle Answer below, your answer cannot be changed.

Toggle Answer

- **Network forensics** is the process of examining and analyzing network traffic to collect and preserve evidence of unauthorized access, data breaches, or other security incidents. This process involves looking at information such as network logs, network packets, and network devices to detect and track any harmful or unauthorized activity.

Think of an example of a network security incident; what steps would you take after it happens? *Click Toggle Answer to share your thoughts.*

Your Answer

Type in your answer here and Compass will let you reveal our answer below. Compass will auto-save your answer as you type. Once you click Toggle Answer below, your answer cannot be changed.

Toggle Answer

Cyber Security and Forensics - Similarities and Differences

The allocation of Cyber Security roles and separation of duties within an organization's security program may vary based on its size, available staff resources, and the maturity level of its security program.

Think of **Cyber Security Experts** as digital architects. They ***create*** secure services using the latest software and security tools, like firewalls and access controls, to prevent cyber threats.

Example: designing a secure network for a startup

Cyber Security experts may serve as advisors, reviewers, or implementers of such controls to minimize risk and safeguard the confidentiality, integrity, and availability of services.

Forensic Analysts, on the other hand, are like detectives. They step in ***post-incident*** to investigate breaches, help repair any damages, and suggest solutions and measures.

In short, Cyber Security is about prevention, while forensics is about investigation and response. Both are important for robust security.

Forensic Data in Cyber Security

Types of forensic data collection: in the world of forensics, the "evidence" can be *digital or physical*. Digital evidence can be found in the form of emails, files, system logs, or metadata. Physical evidence, on the other hand, can be found stored on hard drives, smartphones, and other storage media.

Locations for forensic data: this evidence can lurk in many places. Digital data is often found on devices, like computers, servers, smartphones, and tablets, and even network devices like routers, switches, and firewalls. Physical evidence could be at crime scenes or with a suspect.

Forensic data collection process: the process of collecting data varies depending on the type of evidence and the circumstances of the investigation. Collecting this evidence is a precise task. For digital data, analysts use specialized tools to create an exact copy, or 'forensic image', of a device's data.

Physical evidence collection follows strict protocols to maintain its integrity for court use—this includes protective gear, detailed documentation, and secure packaging.

Whether collecting digital or physical evidence, maintaining the integrity of the data is critical.

Consider how you can maintain the integrity of digital and physical evidence as you further explore the roles within Cyber Security and IT forensics.

Importance of Forensic Data

Forensic investigations help stop criminals from future cyber crimes by collecting and analyzing digital evidence they leave behind. This evidence can reveal their identity, location, motives, and methods. While this process is vital in cybercrime cases, it's also used in other criminal investigations like homicides or financial fraud, where physical and digital evidence, from DNA samples to social media posts, is analyzed.

These investigations offer a powerful way to uncover hidden evidence, paving the way to uncover hidden evidence, which can be used to build a strong case against the perpetrators of criminal activities.

A 2014 Example

One case that highlights the power of forensic investigation is the 2014 cyber attack on Sony Pictures. Cyber Security firm Mandiant led the investigation, analyzing the malware, tactics, tactics and techniques (TTP), and other indicators of compromise (IoCs). This analysis, identifying links to North Korea, was essential for the US government to impose sanctions on the country.

A recent 2021 Example

Another significant example happened in 2021 with the SolarWinds hack attributed to the Russian Foreign Intelligence Service (SVR). Forensic investigations by Cyber Security firms and the FBI revealed a backdoor (Sunburst) planted in SolarWinds' software, allowing attackers to access and steal sensitive data.

The forensic analysis revealed that the attackers had been in the victim's networks for several months before being discovered. The attackers also used various tactics to evade detection, including modifying registry keys, deleting log files, and using IP addresses and domain names that appeared legitimate. The investigators' ability to uncover the attackers' evasion tactics led to the attribution of the attack to the SVR.

Key Takeaways

- Forensic roles in IT and Cyber Security involve investigating and analyzing digital evidence to identify and track unauthorized or malicious activity.
- Computer forensics focuses on individual devices or systems, while Cyber Security forensics analyzes data from multiple sources to detect and respond to broader security threats.
- Forensic data is crucial in today's digital age to catch criminals, protect against cyberattacks, and maintain the security of our digital infrastructure.

Conclusion

In this reading, you learned that forensic roles in IT and Cyber Security involve investigating and analyzing digital evidence to identify and track unauthorized or malicious activity. This can include recovering lost or deleted data, collecting digital evidence from various sources, and analyzing it to identify patterns or anomalies that may indicate a security breach or cybercrime.

While similar, computer and Cyber Security forensics differ in scope. Computer forensics focus on individual devices or systems, while Cyber Security forensics analyze data from various sources to tackle wider security threats.

In our increasingly digital world, forensic data's importance is undeniable. It's a powerful tool to catch criminals, prevent cyberattacks, and secure our digital landscape.

In the next reading, you'll delve deeper into specific responsibilities of a security analyst in forensics.

Further Readings

> Don’t miss out on these important resources. Diving into them will provide you with a deeper understanding and enrich your knowledge in this field.

1. Computer Forensics Roles and Responsibilities (Infosec Institute):
2. A Complete Career Guide for Computer Forensics: Steps to Success (EC-Council Cyber Security Exchange)
3. Digital Forensics, Incident Response & Attribution (Cyber Security Intelligence)
4. Digital Forensics Analyst Career Paths (Infosec Institute)

References

- Casey, E. (2011). Handbook of Digital Forensics and Investigation. Academic Press.
- Quick, D., & Choo, K. K. R. (2014). Handbook of research on digital crime, cyberspace security, and information assurance. IGI Global.
- Mandiant. (2014). APT28: A Window into Russia's Cyber Espionage Operations?
- APT28: At the Center of the Storm (Download PDF):
- Reuters. (2021, April 15). U.S. Blames Russia's SVR for SolarWinds Hack

---

✓ Mark Completed

Previous
Overview - Forensics

Next
Forensic Duties of a Security Analyst

How well did this activity help you to understand the content?

Let us know how we're doing

☆ ☆ ☆ ☆ ☆

W08D5

Fri Aug 16

Forensic Duties of a Security Analyst

Other (1)

W08D5 Schedule »