TALENTO TECH

TIC

REGIÓN 3

CAUCA - NARIÑO

LESSON 3 -UNIT 1

Universidad Tecnológica de Pereira

faceIT

Lesson 3: Reading

What is Digital Forensics?

Digital forensics is a branch of forensic science that involves the identification, preservation, analysis, and presentation of digital evidence. It is used in legal investigations to uncover and interpret electronic data. Digital forensics plays a crucial role in solving cybercrimes, such as hacking, identity theft, and online fraud, but it also aids in non-cybercrime cases where electronic devices might hold critical evidence.

The Process of Digital Forensics

Digital forensics follows a structured process, similar to a traditional police investigation:

1. Identification: Determining which devices or data might contain relevant evidence. For example, in a cyberbullying case, investigators might analyze the victim's and suspect's smartphones and social media accounts.
2. Preservation: Ensuring that the data remains unchanged and is securely stored. This is comparable to sealing a crime scene in a physical investigation.
3. Analysis: Examining the data for clues. For instance, forensic experts might look for deleted emails, chat logs, or hidden files on a computer.
4. Documentation: Recording findings systematically. Just like police officers write reports, forensic experts document every step of their investigation.
5. Presentation: Sharing the evidence in a clear and admissible manner, often in court.

Aspect	Digital Forensics	Police Investigation
Crime Scene	A computer, smartphone, or network system.	A physical location such as a house or street.
Evidence	Emails, logs, deleted files, metadata.	Fingerprints, DNA, and physical objects.
Investigation Tools	Specialized software like EnCase or FTK.	Tools like fingerprint kits, cameras, or sketch pads.
Challenges	Encryption, data deletion, jurisdictional issues.	Witness reliability, environmental contamination.
Expertise Required	Knowledge of cybersecurity and data recovery techniques.	Knowledge of criminology and physical evidence.

TIC

TALENTO TECH

Universidad Tecnológica de Pereira

faceIT

Both types of investigations require meticulous attention to detail, adherence to legal procedures, and a clear chain of custody for evidence to ensure admissibility in court.

Examples of Digital Forensics in Action

1. Case: Recovering Deleted Files

- A company suspects that an ex-employee stole confidential documents before leaving. Digital forensic experts use recovery tools to retrieve deleted files from the employee's laptop and uncover evidence of theft.

2. Case: Tracking a Cybercriminal

- Law enforcement agencies track down a hacker who uses phishing emails to steal financial information. By analyzing IP addresses and server logs, digital forensic investigators trace the hacker's location.

3. Case: Solving a Murder

- A smartphone found at a crime scene reveals the suspect's location history and messages leading up to the crime. This evidence provides critical leads in the case.

Conclusion

Digital forensics is a modern extension of traditional investigative techniques. While it involves unique challenges, such as dealing with encrypted data or rapidly evolving technology, its principles mirror those of police work. Both fields rely on careful analysis and methodical documentation to build a strong case and deliver justice.

TIC

TALENTO TECH

Universidad Tecnológica de Pereira

faceIT