# FORENSE DIGITAL

101 en 90 minutos

START >

# > agenda

Game has a total of 3 rounds with multiple questions in each round.

**Teoría**
*Easy*

**Metodología**
*Medium*

**Ejemplos**
*Casos de uso*

Each team must choose a representative to answer during each round.

# > Forensia digital

Digital forensics is a branch of forensic science focused on identifying, preserving, analyzing, and presenting digital evidence in a manner that maintains its integrity and admissibility in legal proceedings. It plays a crucial role in investigating cybercrimes, data breaches, and other incidents involving digital devices.

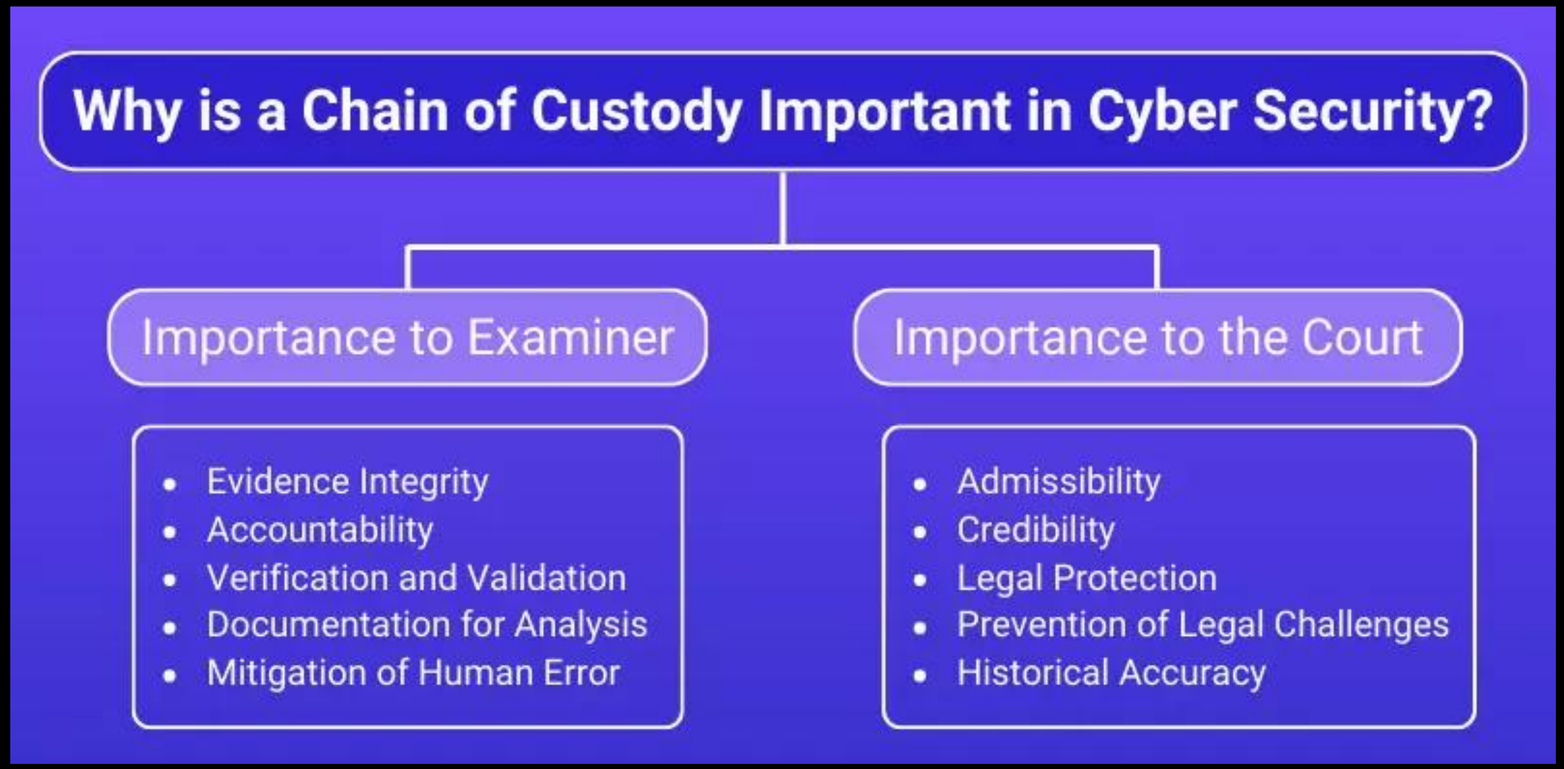
# > Ciencias forenses

Forensic science, often confused with criminalistics, is the application of science principles and methods to support legal decision-making in matters of criminal and civil law. During criminal investigation in particular, it is governed by the legal standards of admissible evidence

# > proceso


Digital Forensic Process
1
IDENTIFICATION
2
PRESERVATION
3
COLLECTION
4
EXAMINATION
5
ANALYSIS
6
INTERPRETATION
7
DOCUMENTATION
8
PRESENTATION

# > objetivo




Fuente: www.fynd.academy Chain Of Custody In Cyber Security (Digital Forensics): Importance, Process, and Best Practices in 2025

> objetivo

INDICIO

DIGITAL

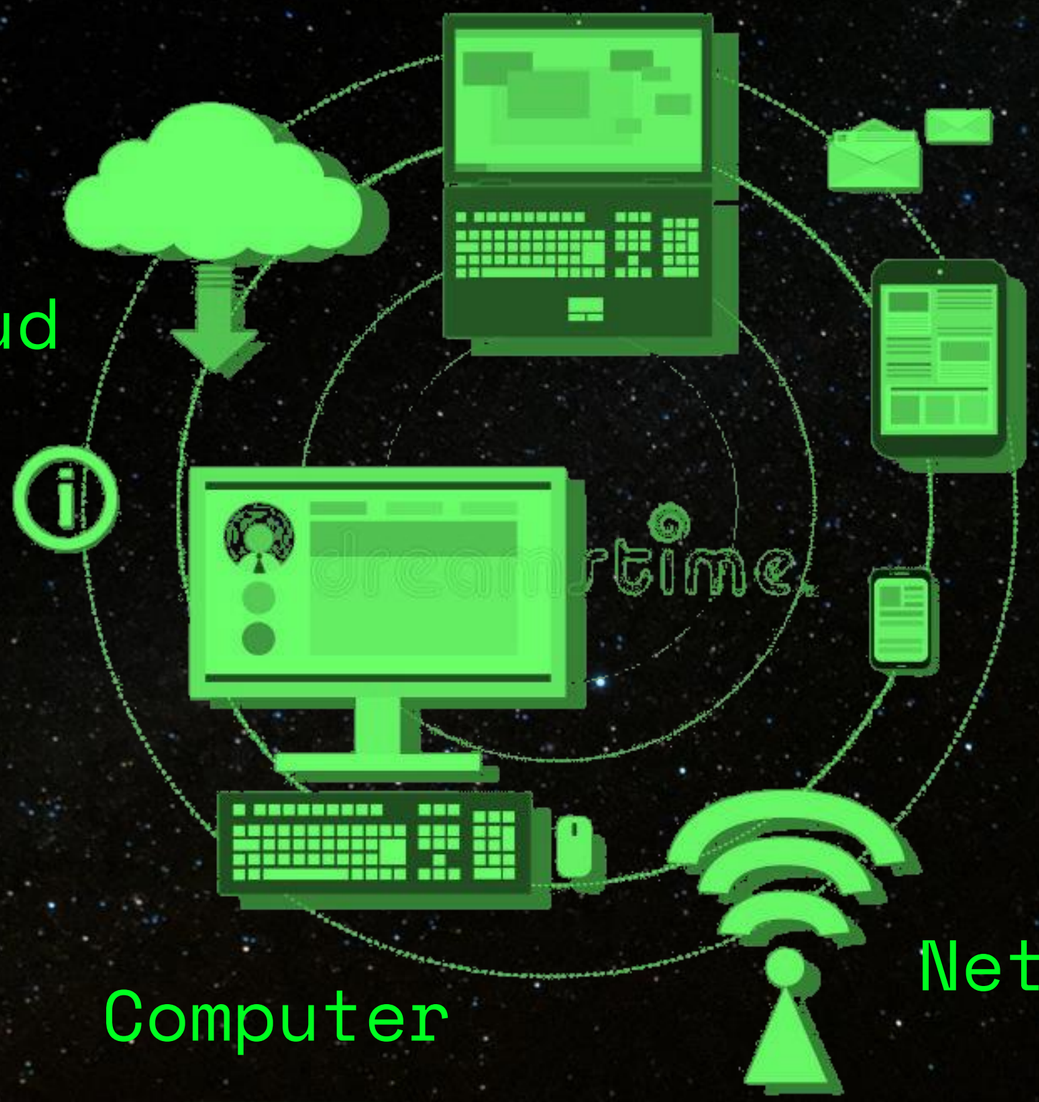
EVIDENCIA

PRUEBA

RASTROS

# > tipos

- Localización
- Sistema de archivos
- Tipo de tecnología



# > De forma general

| | |
|---|---|
| **Localizacón de la Fuente de información** | *Sistema de archivos*<br>*logging & events* |
| **Preservación de la fuente** | *Replica del almacenamiento original sin contaminar* |
| **Obtención de registros** | *Eventos*<br>*Recuperación de punteros*<br>*Metadatos y atributos* |
| **Análisis y correlación** | *Lineas temporales*<br>*adjudicación de eventos*<br>*Comportamiento*<br>*Aseguramiento de la veracidad y replicabilidad* |

# ROUND 1

EZ!

Computer Forensics

Which of the following actions can unintentionally compromise digital evidence during a computer forensic investigation?

A: Using a write blocker to access the suspect's hard drive

B: Hashing files on the device to verify integrity

C: Booting the suspect's computer normally when was de-energized

D: Viewing timestamps using forensic software

# > POV Digital Forensics

APLICACIONES (visor de eventos)
FICHEROS
DATOS

SISTEMA OPERATIVO

TRAFICO DE RED

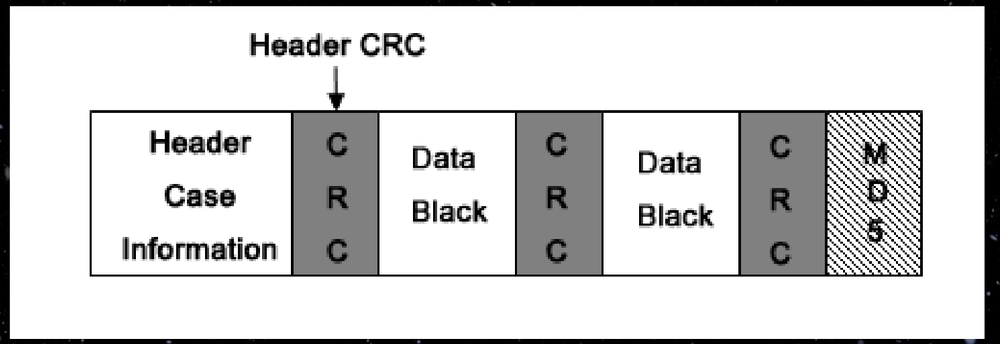
MEMORIA VOLATIL

SISTEMA DE ARCHIVOS// ARRANQUE

DISPOSITIVO DE ALMACENAMIENTO
MEMORIA NO VOLATIL

# > Computer Forensics

DISPOSITIVO DE ALMACENAMIENTO
MEMORIA NO VOLATIL


## E01 FILE FORMAT

```
anonnya@ubuntu:~$ cat file_lower
a b c d
e f g h
i j k l
m n o p
```

Input file contents

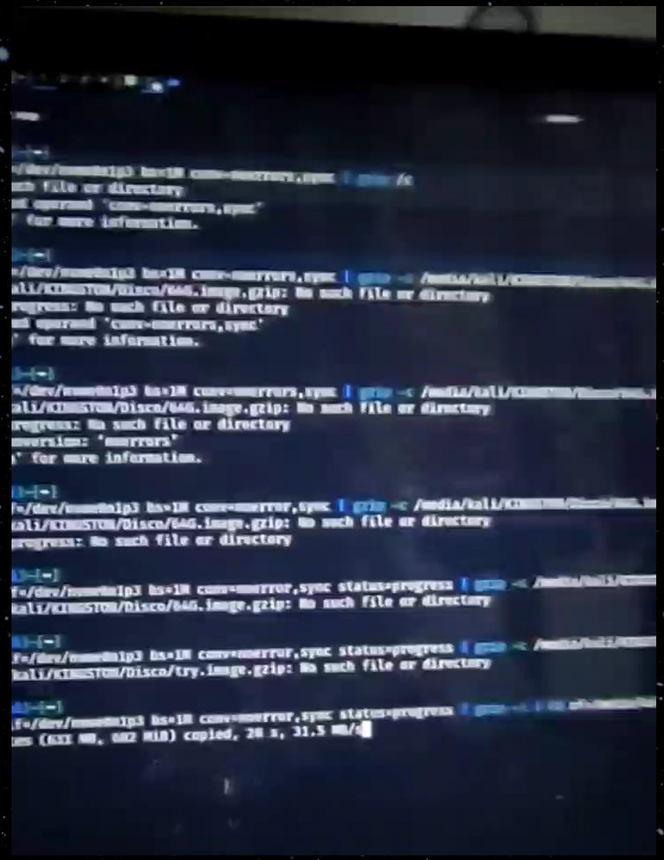
```
anonnya@ubuntu:~$ dd if=~/file_lower of=~/file_upper conv=ucase
0+1 records in
0+1 records out
33 bytes copied, 0.00230218 s, 14.3 kB/s
anonnya@ubuntu:~$ cat file_upper
A B C D
E F G H
I J K L
M N O P
```

Output file contents

# > Computer Forensics

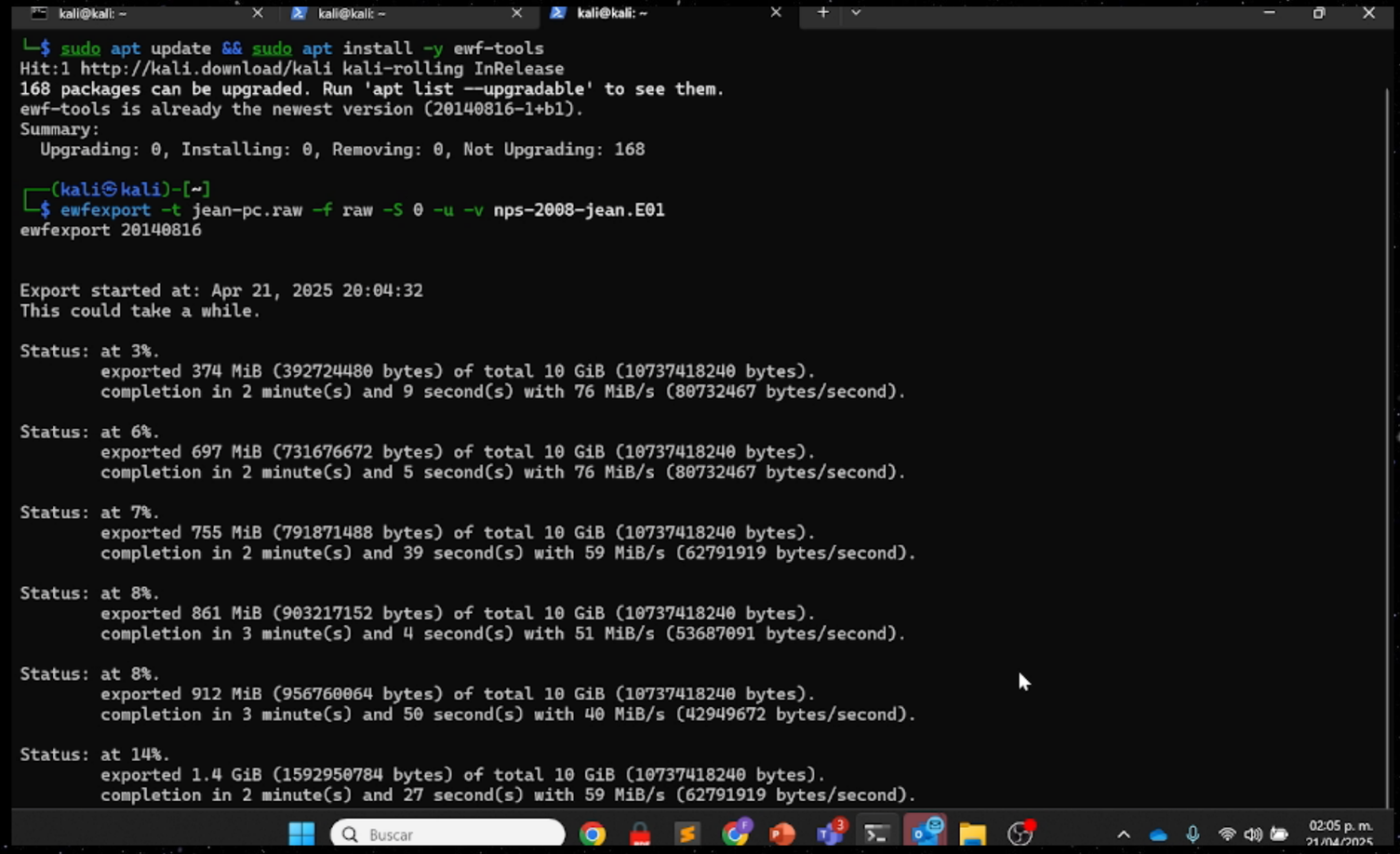
DISPOSITIVO DE ALMACENAMIENTO
MEMORIA NO VOLATIL

```
dd if=/dev/sda of=/dev/sdb bs=4096
conv=sync
```

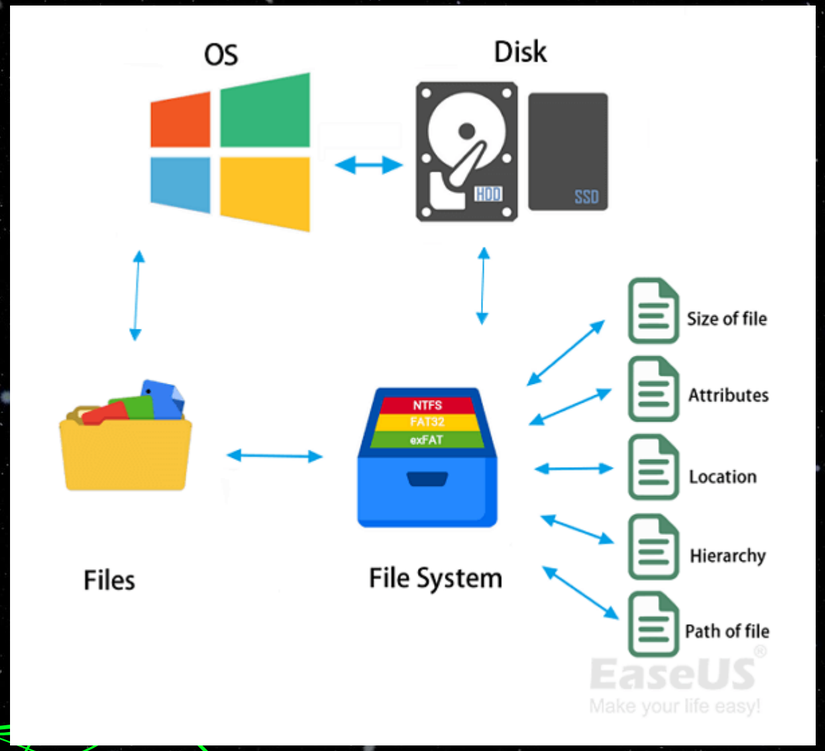


# > Computer Forensics

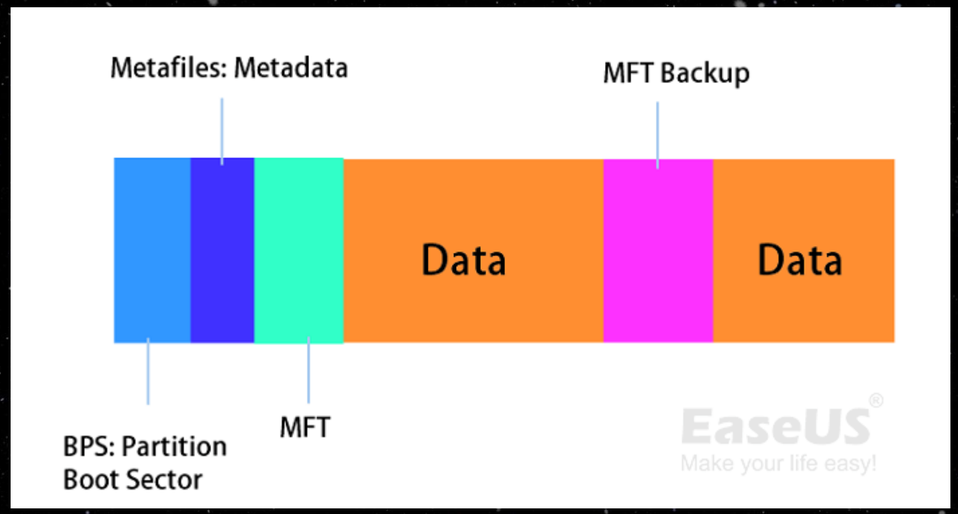
DISPOSITIVO DE ALMACENAMIENTO
MEMORIA NO VOLATIL



# > Computer Forensics

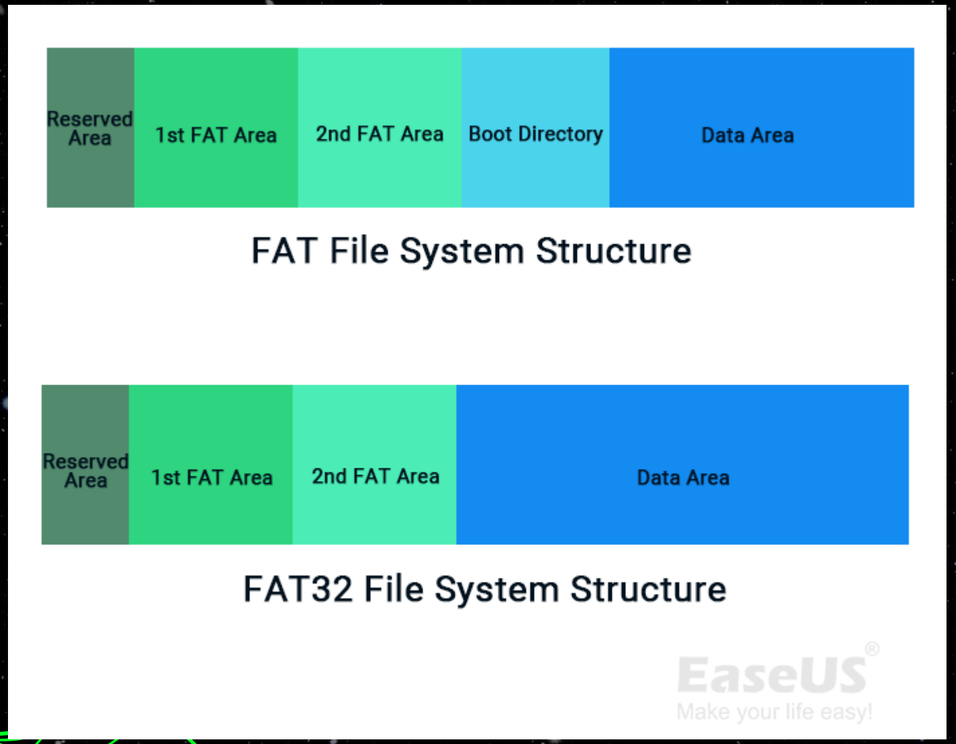


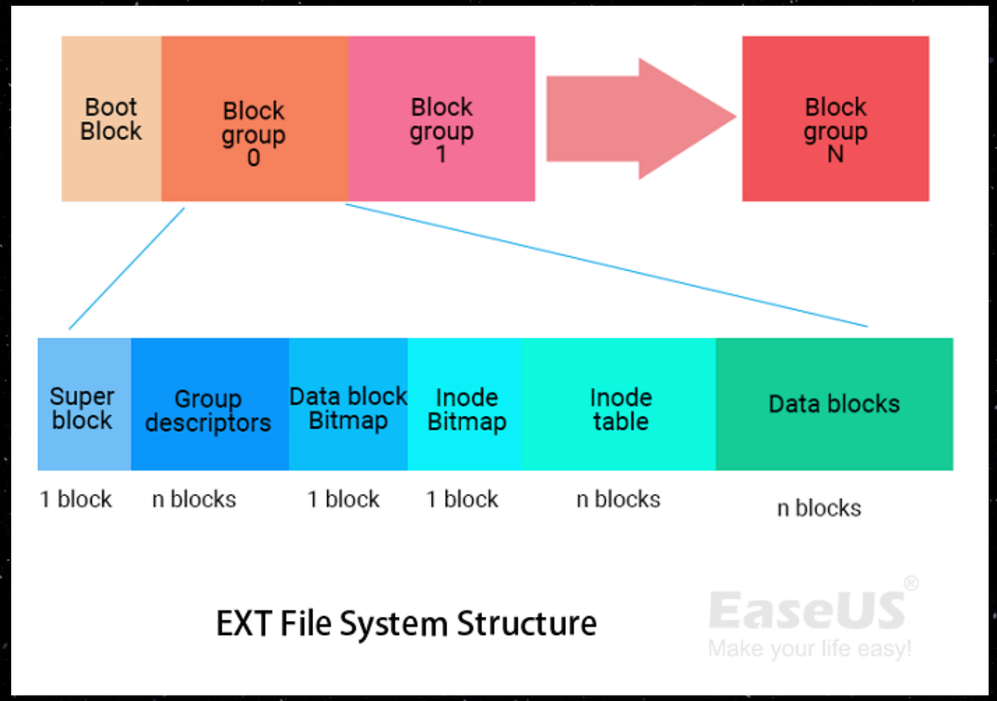

Fuente: https://www.easeus.com/diskmanager/file-system.html




SISTEMA DE ARCHIVOS// ARRANQUE

# > Computer Forensics



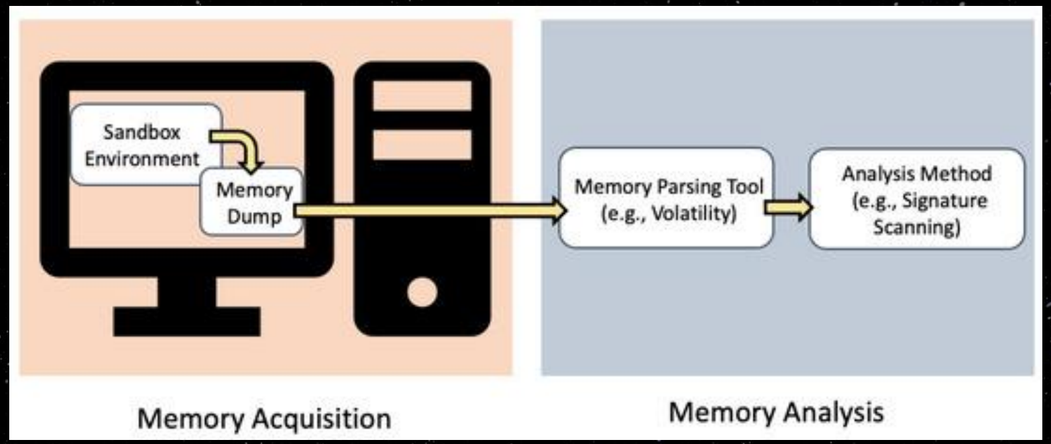



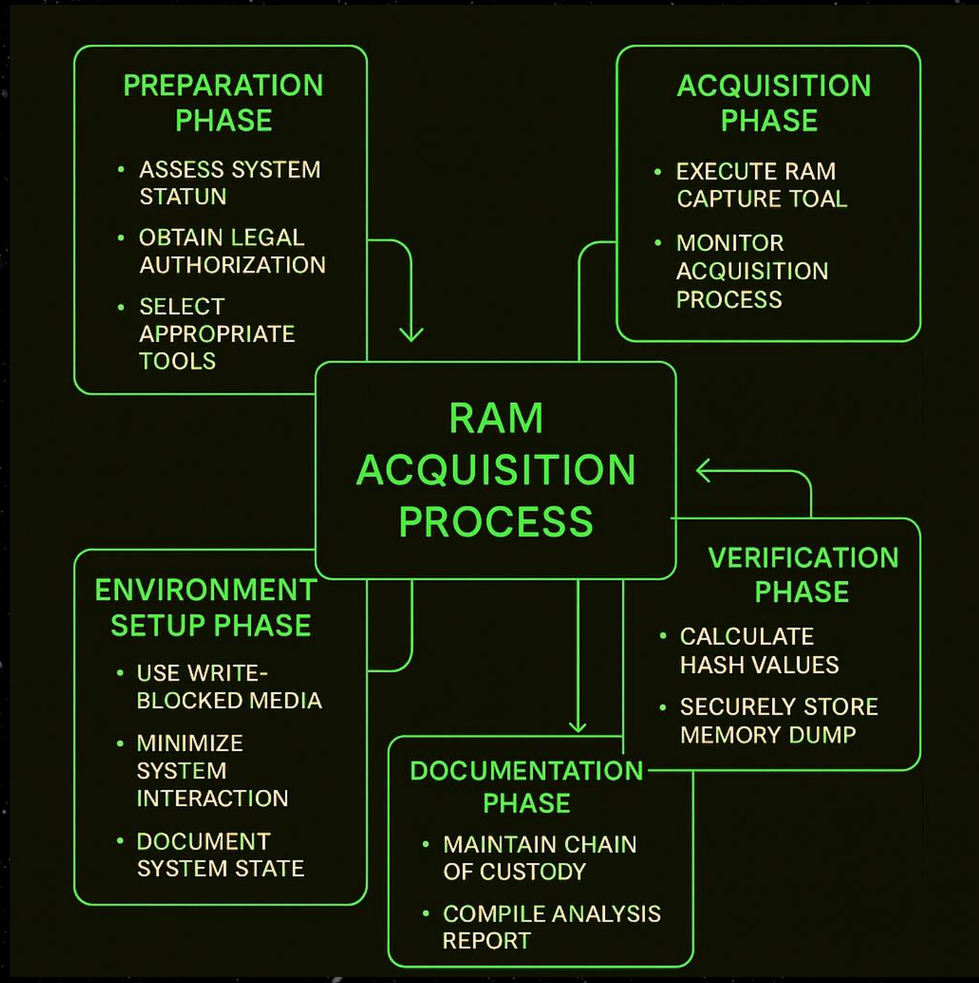

**SISTEMA DE ARCHIVOS// ARRANQUE**

Fuente: https://www.easeus.com/diskmanager/file-system.html

# > Computer Forensics

## MEMORIA VOLATIL



# > caso de la vida real

SISTEMA OPERATIVO

TRAFICO DE RED

APLICACIONES FICHEROS DATOS

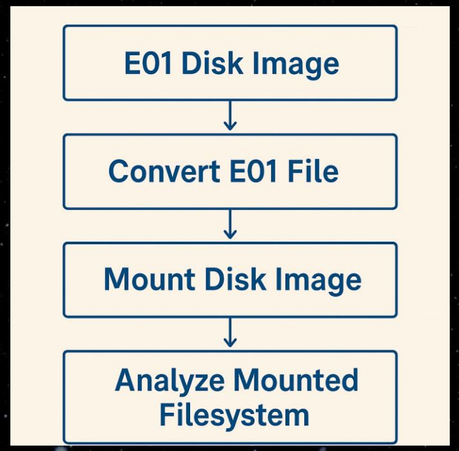
# > caso de la vida real

The scenario involves a small start-up company, M57.Biz. A few weeks into inception a confidential spreadsheet that contains the names and salaries of the company's key employees was found posted to the "comments" section of one of the firm's competitors. The spreadsheet only existed on one of M57's officers, Jean.

Jean says that she has no idea how the data left her laptop and that she must have been hacked.

You have been given a disk image of Jean's laptop. Your job is to figure out how the data was stolen, or if Jean isn't as innocent as she claims.

# > Computer Forensics




mount
(ewfmount)

SISTEMA OPERATIVO

TRAFICO DE RED

APLICACIONES
FICHEROS
DATOS

Authopsy

Authopsy

Authopsy

MEMORIA VOLATIL

SISTEMA DE ARCHIVOS// ARRANQUE

FTK Imager
/Autopsy

DISPOSITIVO DE ALMACENAMIENTO
MEMORIA NO VOLATIL

E0/Encase

# > Casos de uso

- Insider threat vs external compromise
- Phishing attack leading ransomware
- Intellectual property leakage
- Sabotage
- Business Email Compromise

Which of the following actions can unintentionally compromise digital evidence during a computer forensic investigation?

| | | | |
|---|---|---|---|
| | | | |
| C: | Booting the suspect's computer normally when was de-energized | | |

# ROUND 2

## NETWORK FORENSICS

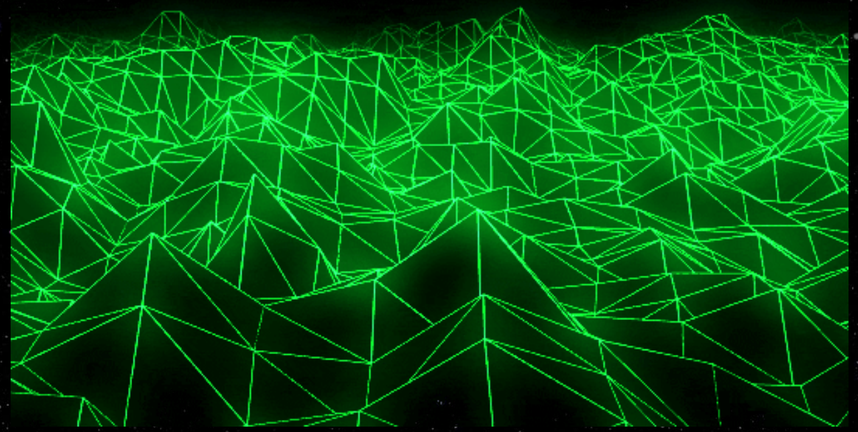
Which of the following statements about data remnants and forensic recovery is MOST accurate?

A: Encrypted partitions cannot be identified during forensic imaging unless the encryption key is already known.

B: Unallocated space can contain fragments of previously deleted files, which can sometimes be reconstructed during forensic analysis.

C: Metadata such as timestamps and file paths are stored in the file's content, making them immune to changes in the file system.

# > POV Digital Forensics



METADATOS

LOGS

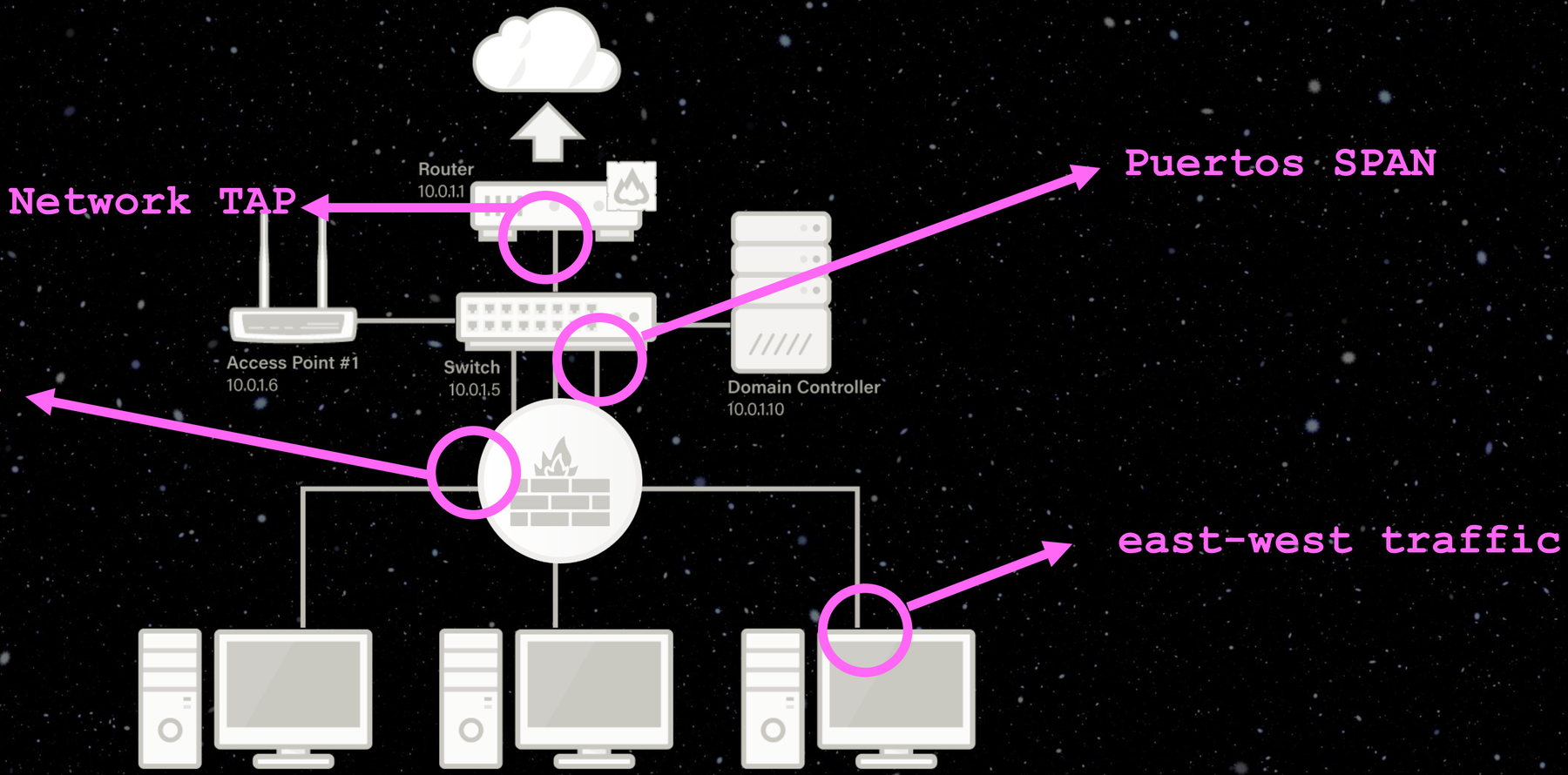
TRANSFERENCIAS DE ARCHIVOS

RECONSTRUCCION DE SESIONES

FLUJOS DE RED

PUNTOS DE COLECTA

# > POV Digital Forensics



# > Network Forensics

## PUNTOS DE COLECTA

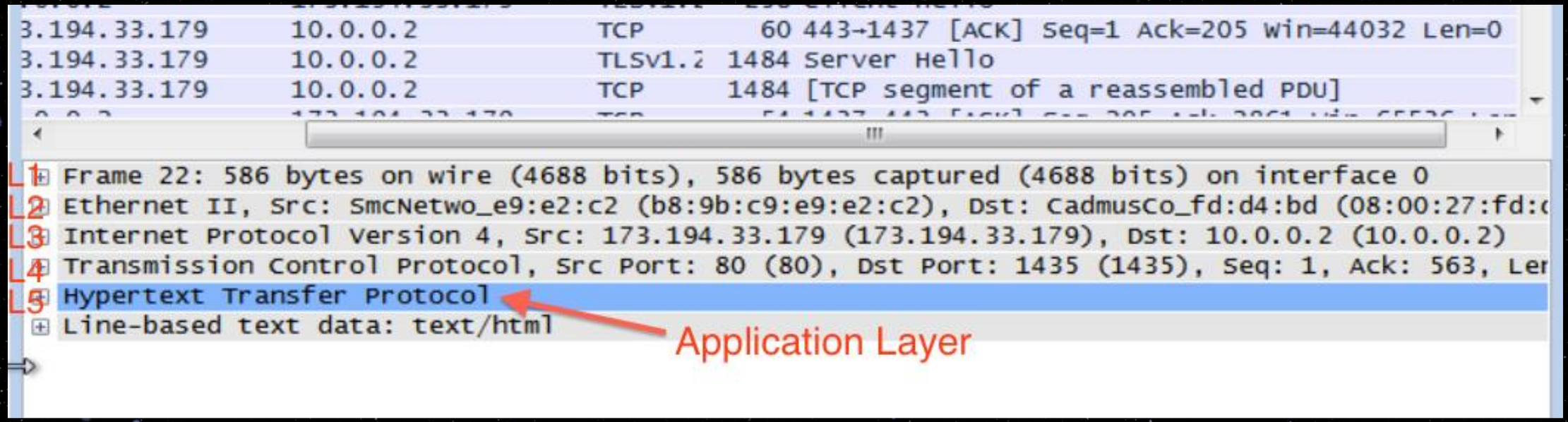
- Customer records are leaked after a vulnerability in the internal CRM web server.
- APT suspected of slow persistent data exfiltration over months.
- C2 instance in AWS hosting a production app suddenly shows port scans and weird POST requests.
- Multiple employees report phishing emails over several weeks.

# > Network Forensics

## PUNTOS DE COLECTA

| File Format | Extension | Description | Pros | Cons | Common Use Case |
|---|---|---|---|---|---|
| **PCAP** | .pcap | A standard packet capture format used by many network analysis tools, like Wireshark and tcpdump. | Widely supported, human-readable, contains full packet data. | Large file sizes for long captures, lacks file compression. | General network analysis, troubleshooting. |
| **PCAPNG** | .pcapng | A more advanced version of PCAP with additional features like metadata, multiple interfaces, and more. | Supports multiple interfaces, better metadata, extensible. | Not as universally supported as PCAP. | Advanced network analysis, modern tools like Wireshark. |
| **Snoop** | .snoop | A capture format primarily used by Solaris-based systems for packet analysis. | Simple and lightweight, native to Solaris. | Limited support, less feature-rich compared to PCAP. | Network analysis on Solaris-based systems. |
| **TCPDUMP** | .dmp | A format used by tcpdump, similar to PCAP, but can have slightly different structure. | Supports detailed capture, widely used for diagnostics. | Limited to tcpdump tools, potential incompatibility with other tools. | Diagnostics and packet capture with tcpdump. |
| **Wireshark** | .cap | The default capture format for Wireshark, essentially the same as PCAP but with Wireshark-specific optimizations. | High compatibility with Wireshark and many analysis features. | Large files, not always portable. | Detailed packet analysis in Wireshark. |
| **NetFlow** | .netflow | A format used for flow data (aggregated traffic data) rather than individual packet captures. | Efficient for network traffic analysis, summarization. | Doesn’t capture full packet data, only flows. | Network traffic analysis, monitoring performance. |
| **NFDUMP** | .nfdump | Used with the NFDUMP tool to analyze NetFlow exports, focuses on flow-based network traffic data. | Efficient for flow-based analysis. | Not suitable for detailed packet-level analysis. | Network flow analysis. |
| **ERF** | .erf | A proprietary format used by Endace network appliances, optimized for high-speed capture. | Optimized for high-speed captures, supports metadata. | Proprietary format, requires specialized software. | High-speed network capture, large-scale analysis. |
| **PFR** | .pfr | A proprietary format used by PacketForensics for capturing and analyzing network traffic. | Detailed analysis features, optimized for PacketForensics tools. | Limited to PacketForensics tools, less common. | Specialized forensic analysis with PacketForensics. |

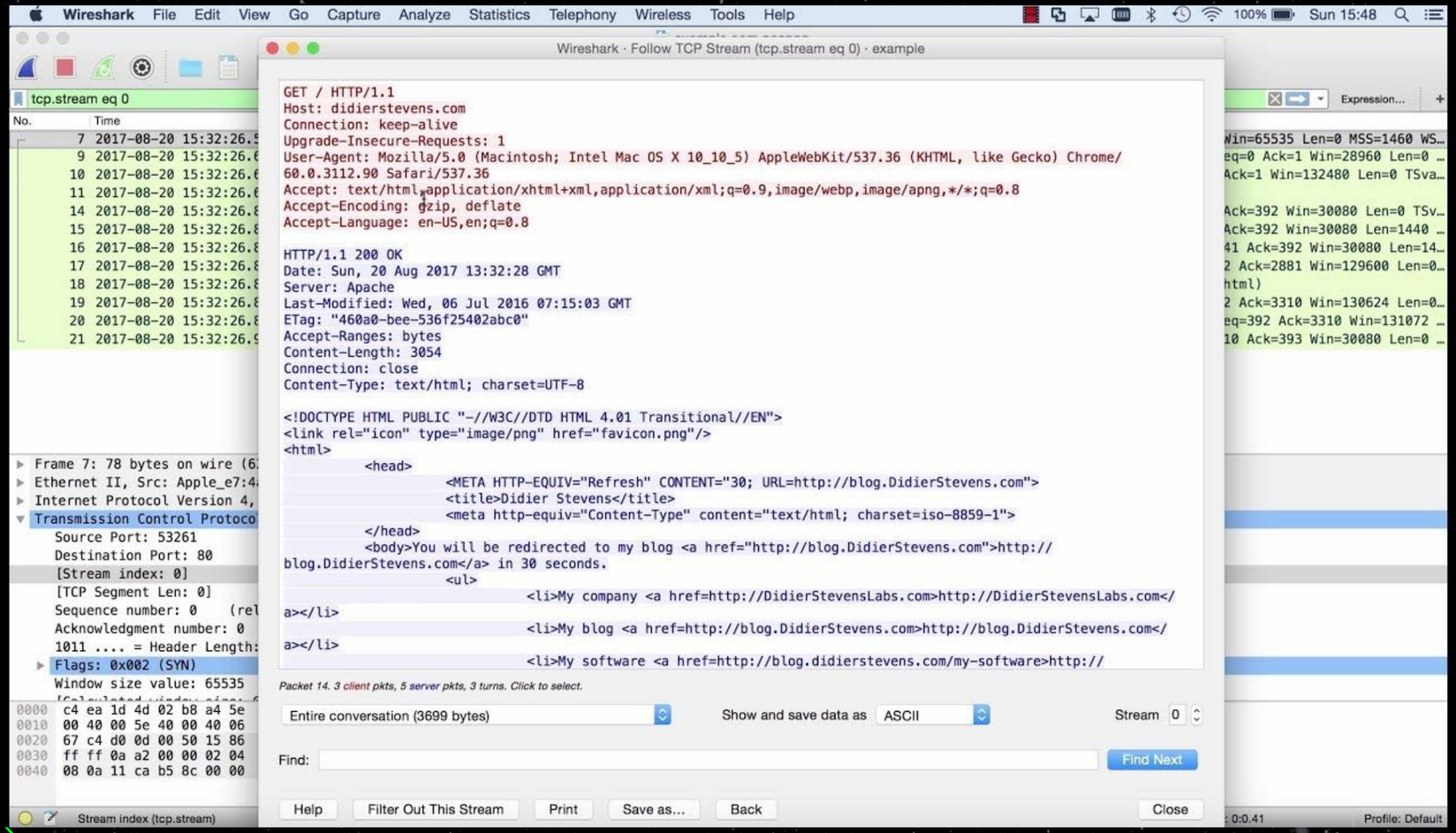
# > Network Forensics




FLUJOS DE RED

# > Network Forensics

RECONSTRUCCION DE SESIONES



# > caso de la vida real

METADATOS

LOGS

TRANSFERENCIAS DE ARCHIVOS

# > caso de la vida real

A SOC Analyst at Umbrella Corporation is going through SIEM alerts and sees the alert for connections to a known malicious domain. The traffic is coming from Sara's computer, an Accountant who receives a large volume of emails from customers daily. Looking at the email gateway logs for Sara's mailbox there is nothing immediately suspicious, with emails coming from customers. Sara is contacted via her phone and she states a customer sent her an invoice that had a document with a macro, she opened the email and the program crashed. The SOC Team retrieved a PCAP for further analysis.

# > Network Forensics

# > Casos de uso

- Insider threat vs external compromise
- Malware outbreak
- DDoS Attack MitigationSabotage
- Policy Violation Enforcement

Which of the following statements about data remnants and forensic recovery is MOST accurate?

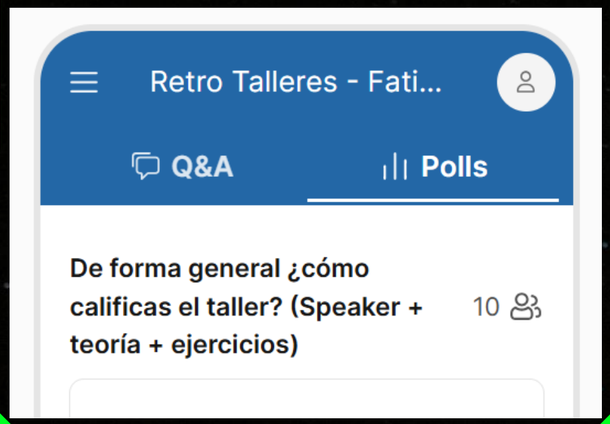
B: Unallocated space can contain fragments of previously deleted files, which can sometimes be reconstructed during forensic analysis.

# ROUND 3

## TO BE CONTINUED...

Hard

# AGRADEZCO MUCHO SUS COMENTARIOS




## COMUNIDADES DE MUJERES EN CIBERSEGURIDAD

## PRÓXIMAS ACTIVIDADES

# THE END

Thank you for playing! Talino nga yorn! CHAR!

2 PTS.

5 PTS.

3 PTS.