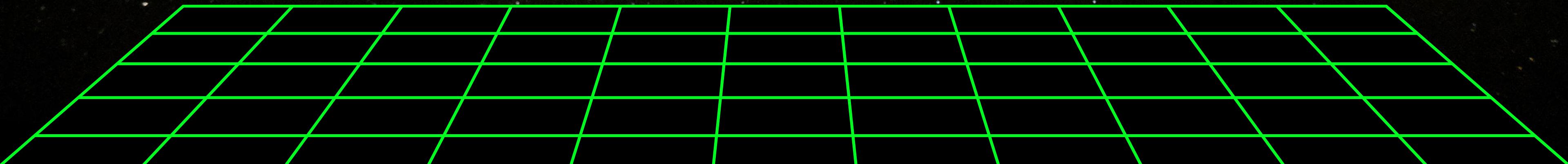




FORENSE DIGITAL

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



> objetivo

Why is a Chain of Custody Important in Cyber Security?

Importance to Examiner

- Evidence Integrity
- Accountability
- Verification and Validation
- Documentation for Analysis
- Mitigation of Human Error

Importance to the Court

- Admissibility
- Credibility
- Legal Protection
- Prevention of Legal Challenges
- Historical Accuracy

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

> **objetivo**

I

D

N

I

D

G

EVIDENCIA

C

T

I

PRUEBA

O

L

RASTROS



- Localización
- Sistema de archivos
- Tipo de tecnología

Cloud



Computer

Mobile

Network

> De forma general

**Localización de la
Fuente de información**

**Preservación de la
fuente**

**Obtención de
registros**

**Análisis y
correlación**

*Sistema de archivos
logging & events*

Replica del almacenamiento original sin contaminar

*Eventos
Recuperación de punteros
Metadatos y atributos*

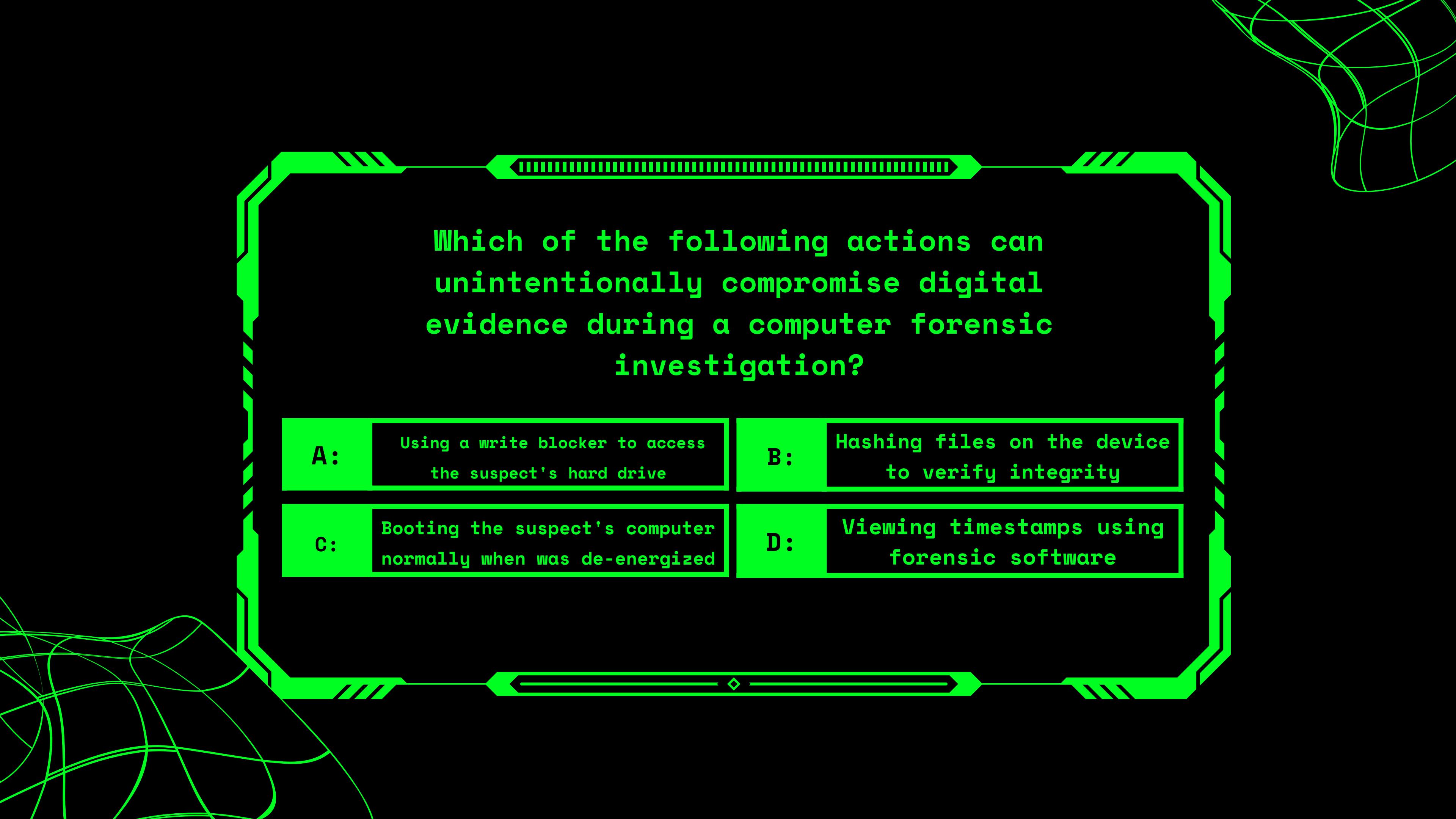
*Líneas temporales
adjudicación de eventos
Comportamiento*

Aseguramiento de la veracidad y replicabilidad

ROUND 2

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

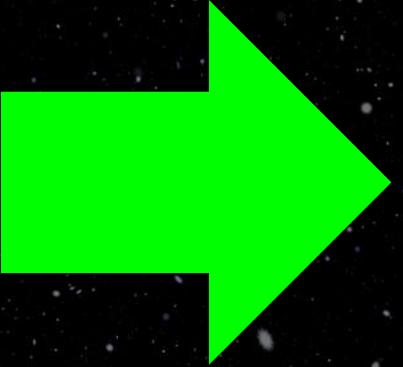
C:

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

TRAFFICO
DE RED

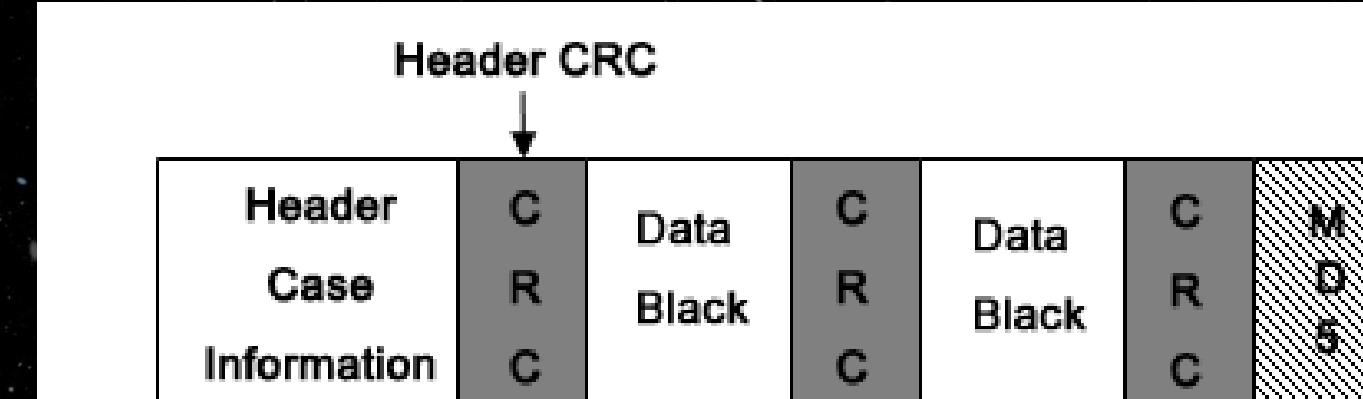
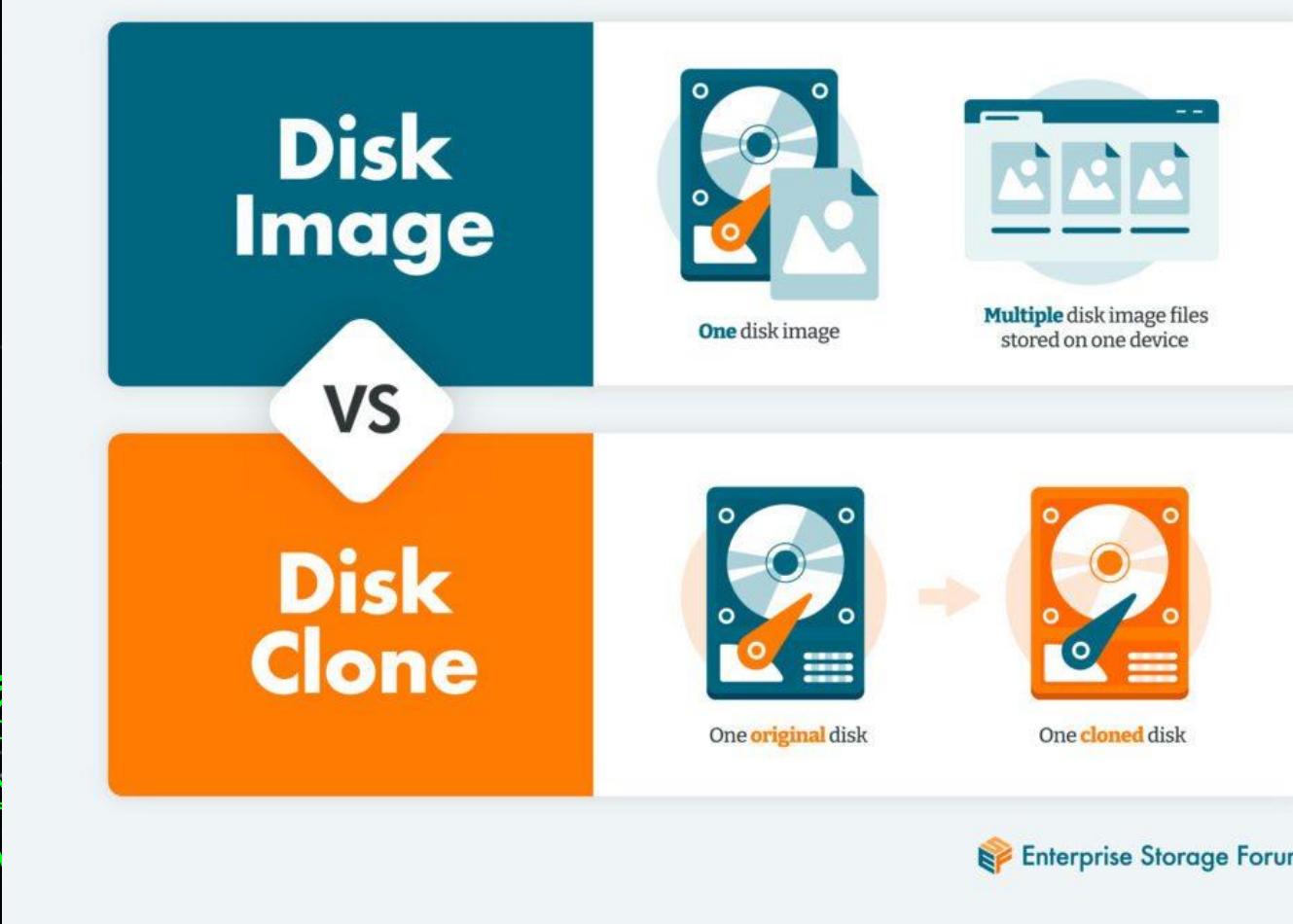
MEMORIA VOLATIL

SISTEMA DE ARCHIVOS // ARRANQUE

DISPOSITIVO DE ALMACENAMIENTO
MEMORIA NO VOLATIL

> Computer Forensics

DISPOSITIVO DE ALMACENAMIENTO
MEMORIA NO VOLATIL



E01 FILE FORMAT

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

anonna@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
anonna@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
```

```
[~] ls -l /media/mounts/errors,sync | grep -c /media/kali/kali-  
all/ICONSTROM/disco/64G.image.gzip: No such FILE or directory  
permissions: No such FILE or directory  
ownership: 'errrors'  
' for more information.  
  
[~] ls -l /media/mounts/errors,sync | grep -c /media/kali/kali-  
all/ICONSTROM/disco/64G.image.gzip: No such FILE or directory  
permissions: No such FILE or directory  
ownership: 'errrors'  
' for more information.  
  
[~] ls -l /media/mounts/errors,sync | grep -c /media/kali/kali-  
all/ICONSTROM/disco/64G.image.gzip: No such FILE or directory  
permissions: No such FILE or directory  
  
[~] ls -l /media/mounts/errors,sync status=progress | grep -c /media/kali/kali-  
all/ICONSTROM/disco/try.image.gzip: No such FILE or directory  
  
[~] ls -l /media/mounts/errors,sync status=progress | grep -c /media/kali/kali-  
all/ICONSTROM/disco/try.image.gzip: No such FILE or directory  
  
[~] ls -l /media/mounts/errors,sync status=progress | grep -c /media/kali/kali-  
all/ICONSTROM/disco/try.image.gzip: No such FILE or directory  
100% (0x0, 0x0 min) copied, 20 s, 31.5 MB/s
```

Computer Forensics

DISPOSITIVO DE ALMACENAMIENTO
MEMORIA NO VOLATIL

```
$ sudo apt update && sudo apt install -y ewf-tools
Hit:1 http://kali.download/kali kali-rolling InRelease
168 packages can be upgraded. Run 'apt list --upgradable' to see them.
ewf-tools is already the newest version (20140816-1+b1).
Summary:
Upgrading: 0, Installing: 0, Removing: 0, Not Upgrading: 168

(kali㉿kali)-[~]
$ ewfexport -t jean-pc.raw -f raw -S 0 -u -v nps-2008-jean.E01
ewfexport 20140816

Export started at: Apr 21, 2025 20:04:32
This could take a while.

Status: at 3%.
exported 374 MiB (392724480 bytes) of total 10 GiB (10737418240 bytes).
completion in 2 minute(s) and 9 second(s) with 76 MiB/s (80732467 bytes/second).

Status: at 6%.
exported 697 MiB (731676672 bytes) of total 10 GiB (10737418240 bytes).
completion in 2 minute(s) and 5 second(s) with 76 MiB/s (80732467 bytes/second).

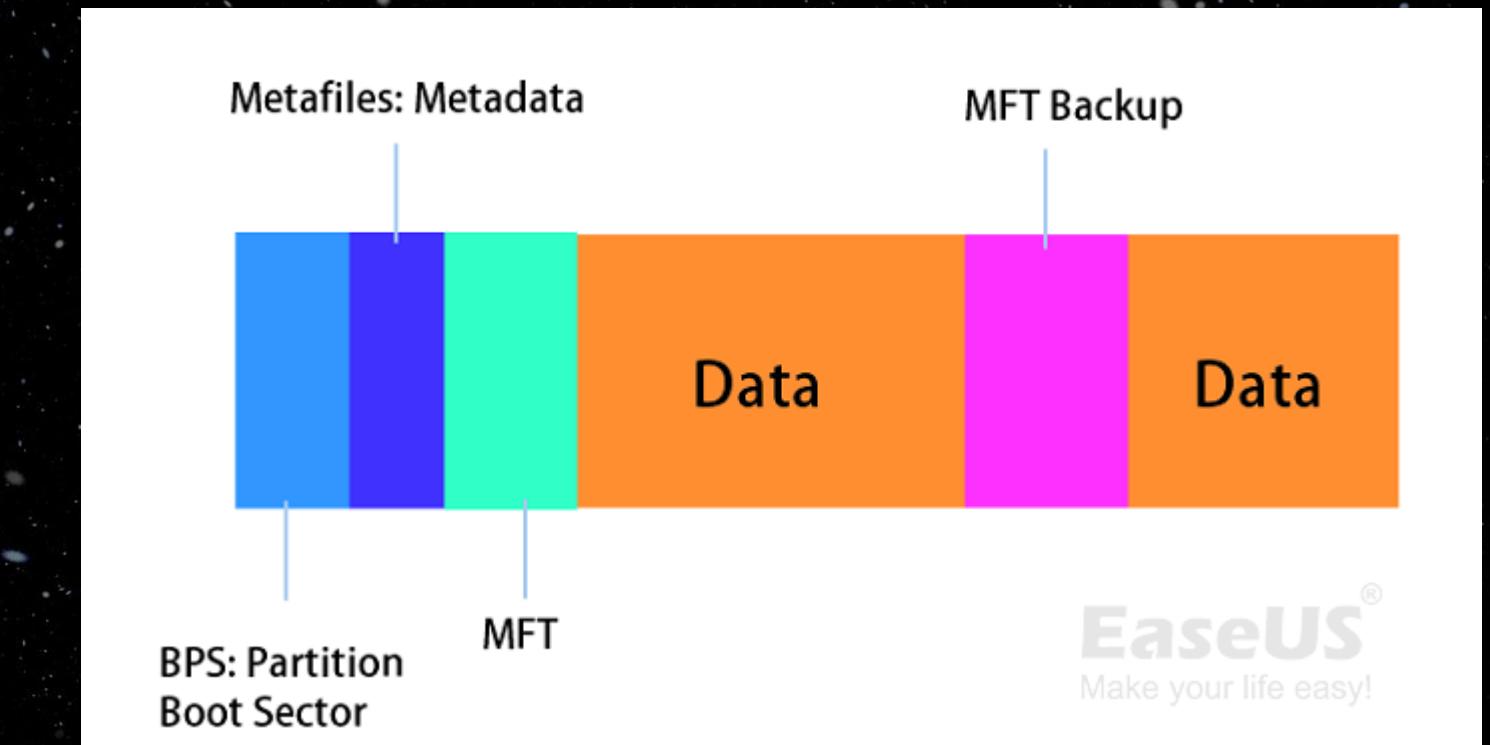
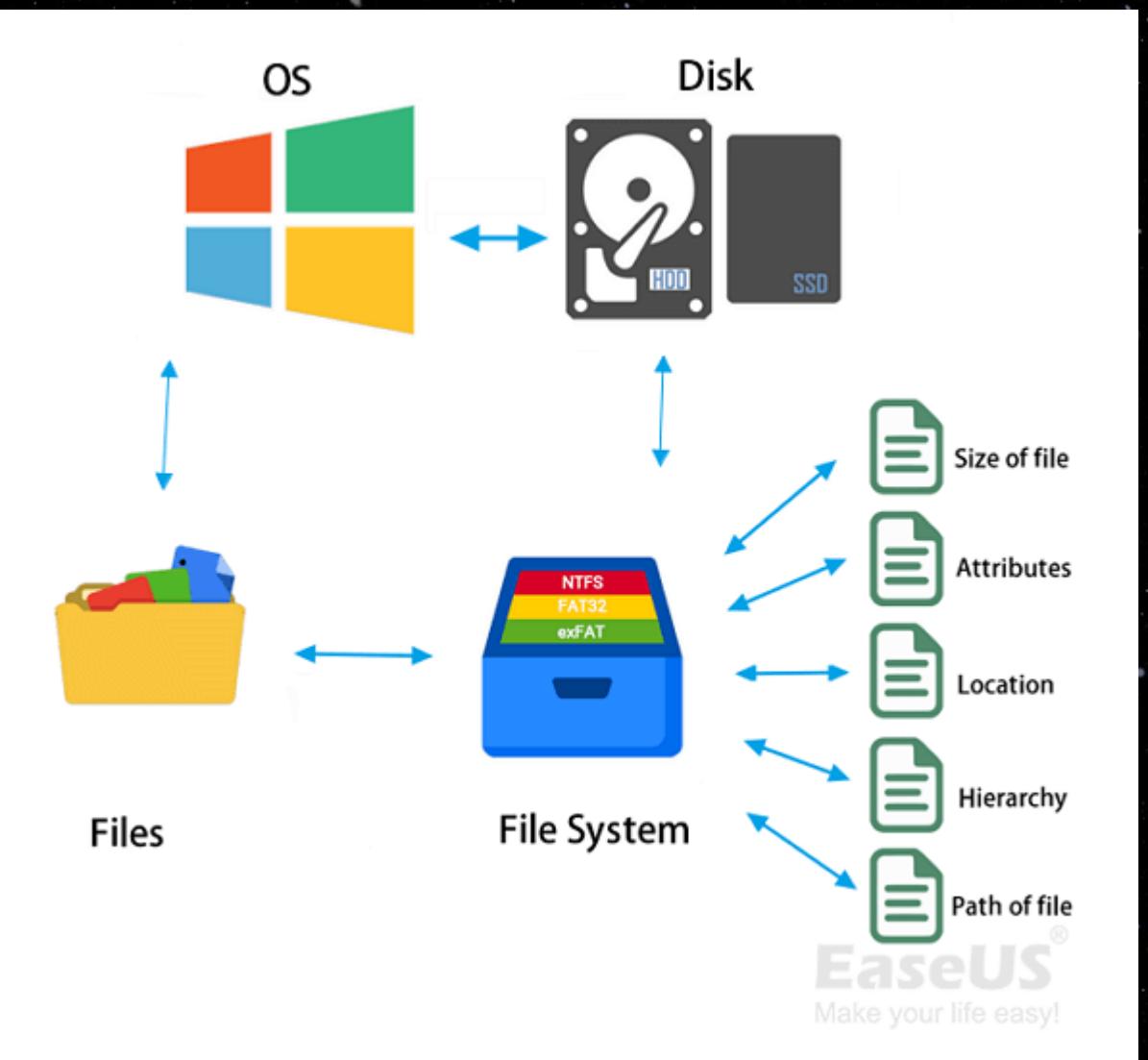
Status: at 7%.
exported 755 MiB (791871488 bytes) of total 10 GiB (10737418240 bytes).
completion in 2 minute(s) and 39 second(s) with 59 MiB/s (62791919 bytes/second).

Status: at 8%.
exported 861 MiB (903217152 bytes) of total 10 GiB (10737418240 bytes).
completion in 3 minute(s) and 4 second(s) with 51 MiB/s (53687091 bytes/second).

Status: at 8%.
exported 912 MiB (956760064 bytes) of total 10 GiB (10737418240 bytes).
completion in 3 minute(s) and 50 second(s) with 40 MiB/s (42949672 bytes/second).

Status: at 14%.
exported 1.4 GiB (1592950784 bytes) of total 10 GiB (10737418240 bytes).
completion in 2 minute(s) and 27 second(s) with 59 MiB/s (62791919 bytes/second).
```

Computer Forensics



SISTEMA DE ARCHIVOS// ARRANQUE

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

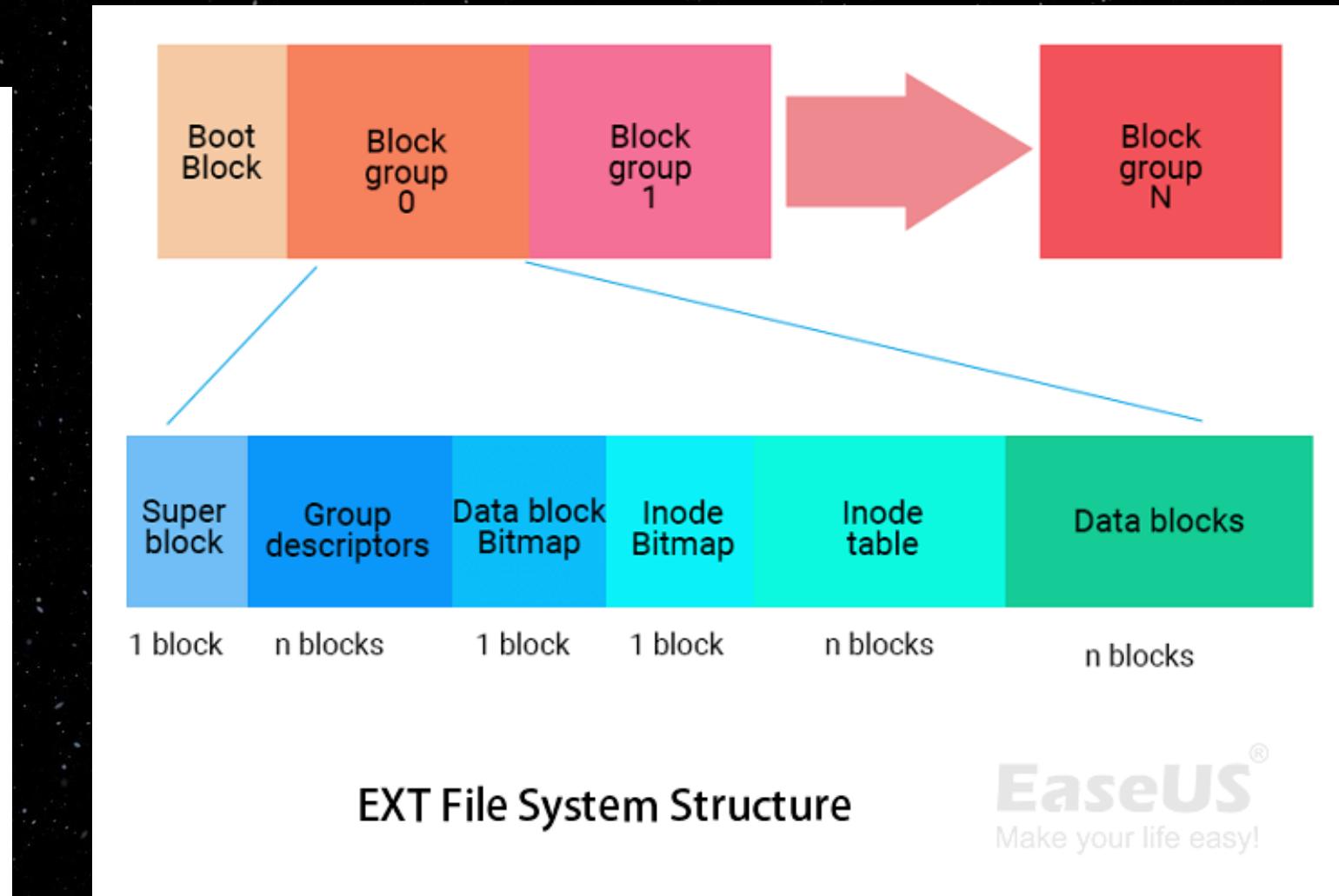
> Computer Forensics



FAT File System Structure



FAT32 File System Structure



EXT File System Structure

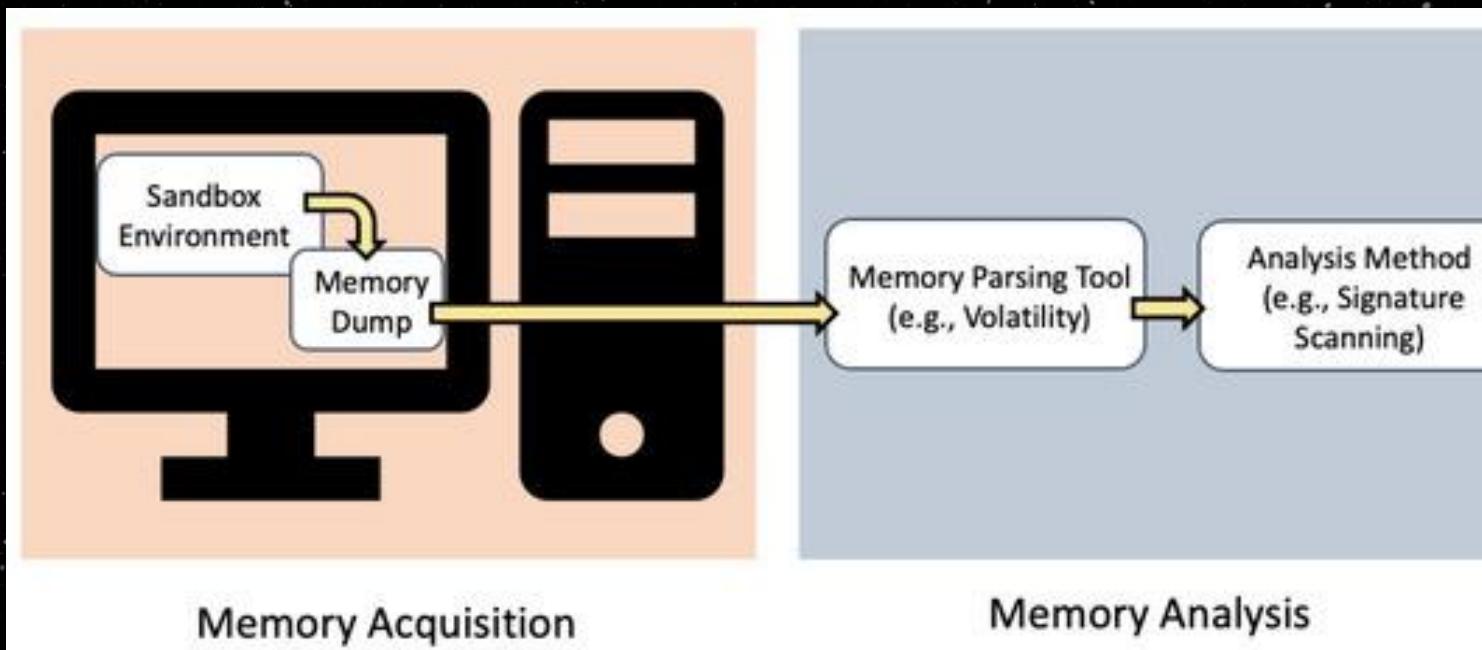
EaseUS®
Make your life easy!

SISTEMA DE ARCHIVOS// ARRANQUE

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

Computer Forensics

MEMORIA VOLATIL



PREPARATION PHASE

- ASSESS SYSTEM STATUS
- OBTAIN LEGAL AUTHORIZATION
- SELECT APPROPRIATE TOOLS

ACQUISITION PHASE

- EXECUTE RAM CAPTURE TOAL
- MONITOR ACQUISITION PROCESS

RAM ACQUISITION PROCESS

ENVIRONMENT SETUP PHASE

- USE WRITE-BLOCKED MEDIA
- MINIMIZE SYSTEM INTERACTION
- DOCUMENT SYSTEM STATE

VERIFICATION PHASE

- CALCULATE HASH VALUES
- SECURELY STORE MEMORY DUMP

DOCUMENTATION PHASE

- MAINTAIN CHAIN OF CUSTODY
- COMPILE ANALYSIS REPORT

> caso de la vida real

SISTEMA
OPERATIVO

TRAFICO
DE RED

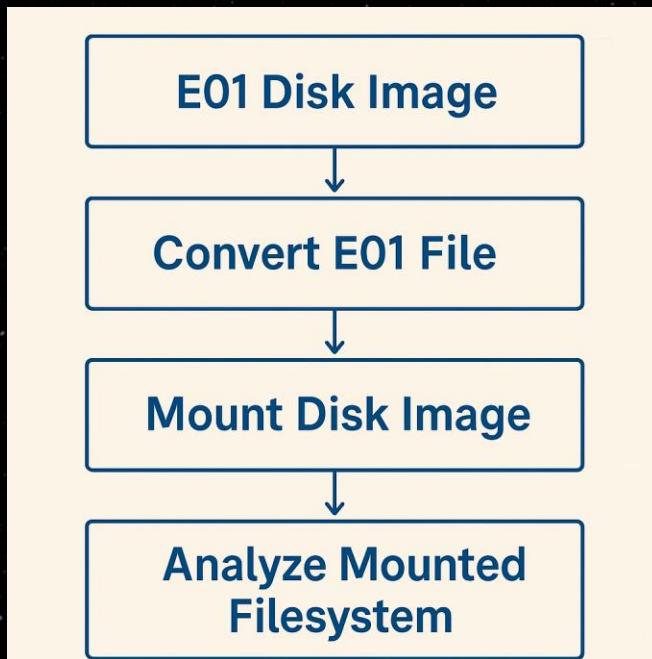
APLICACIO
NES
FICHEROS
DATOS

> 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

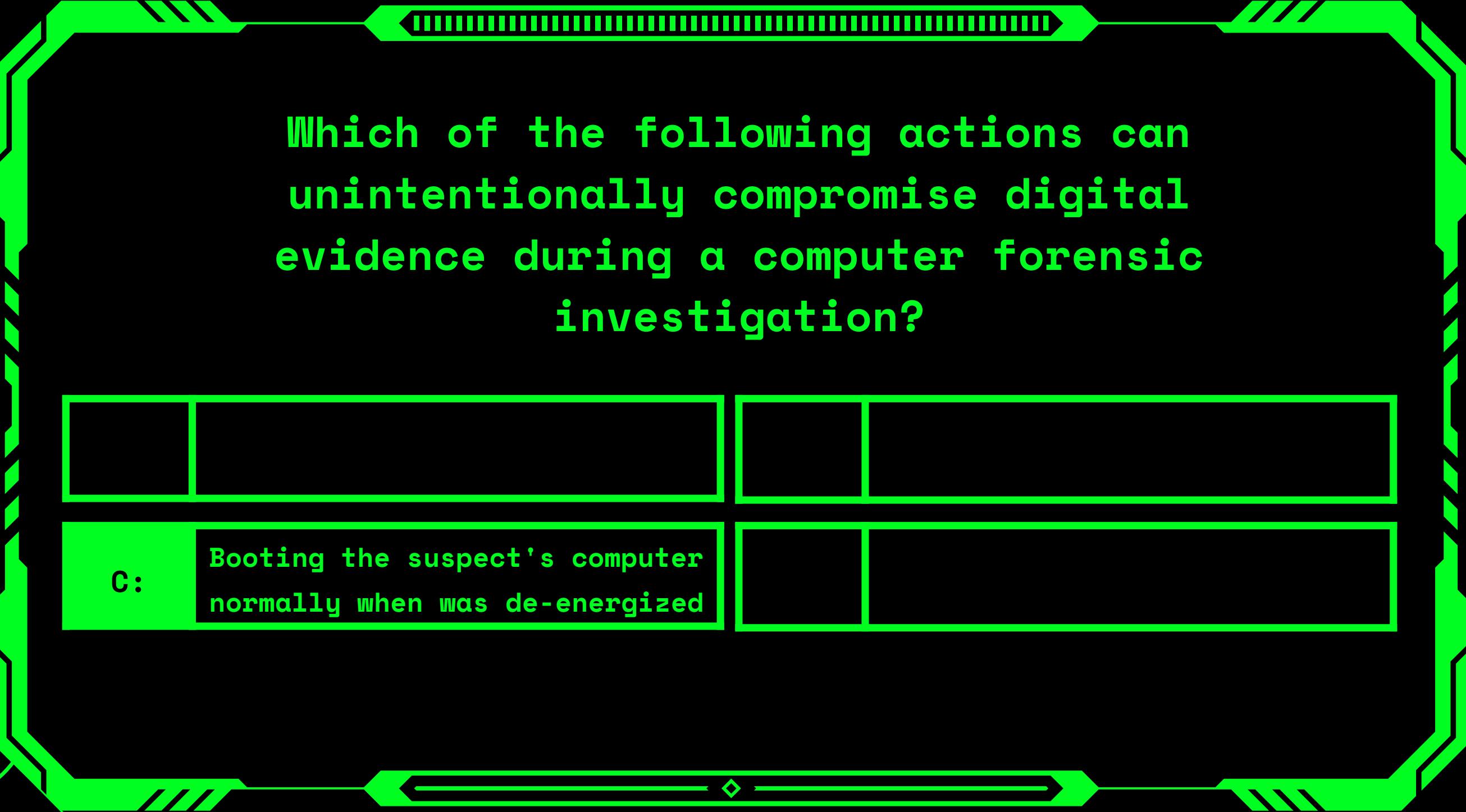


**mount
(ewfmount)**



> 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?

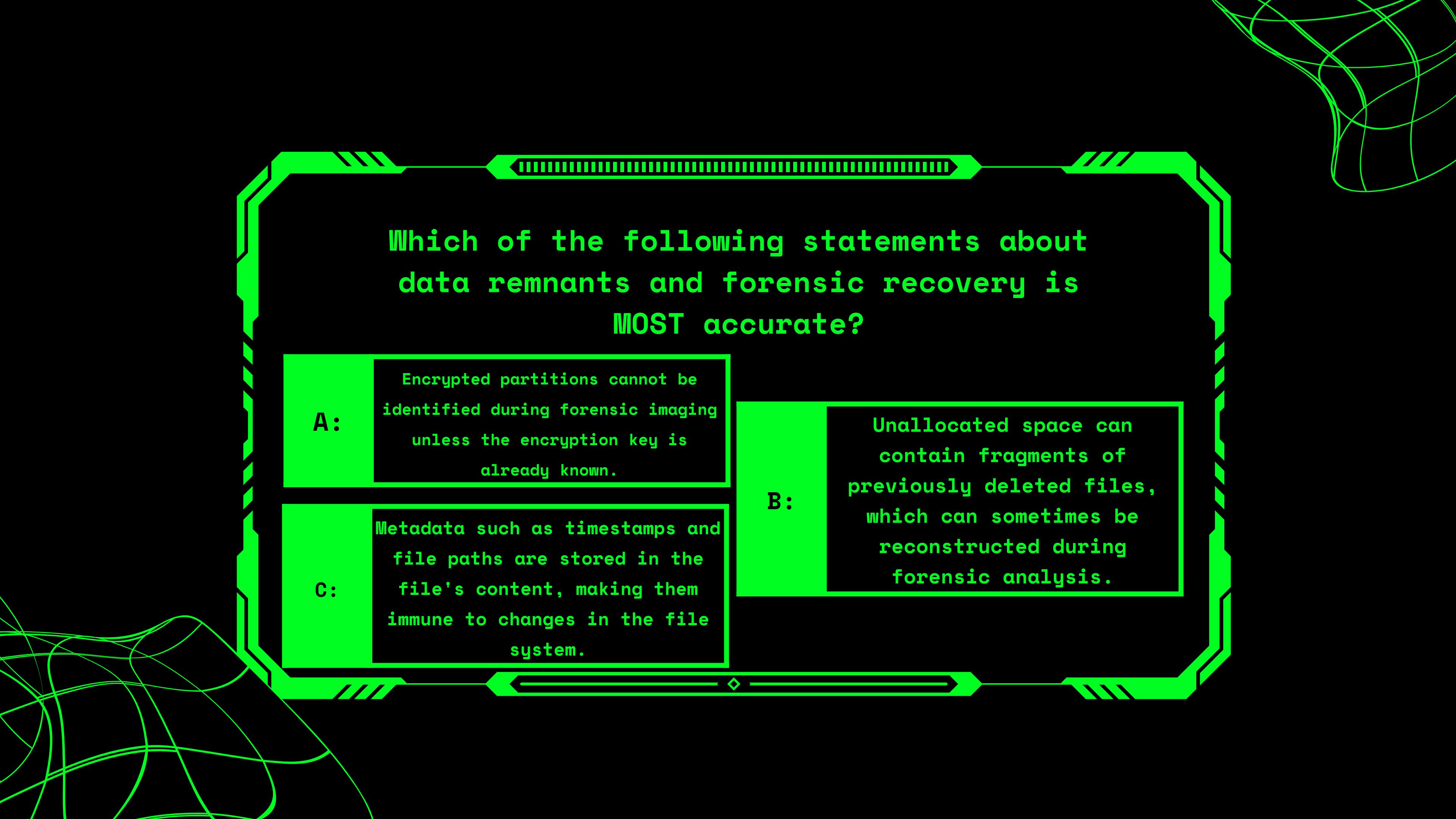
C:

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.

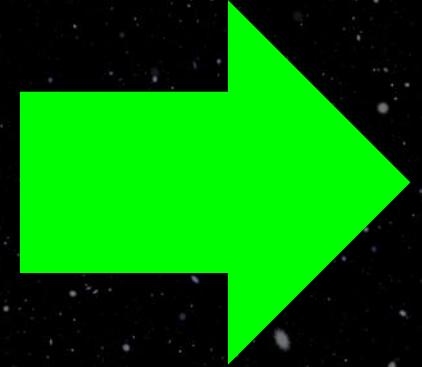
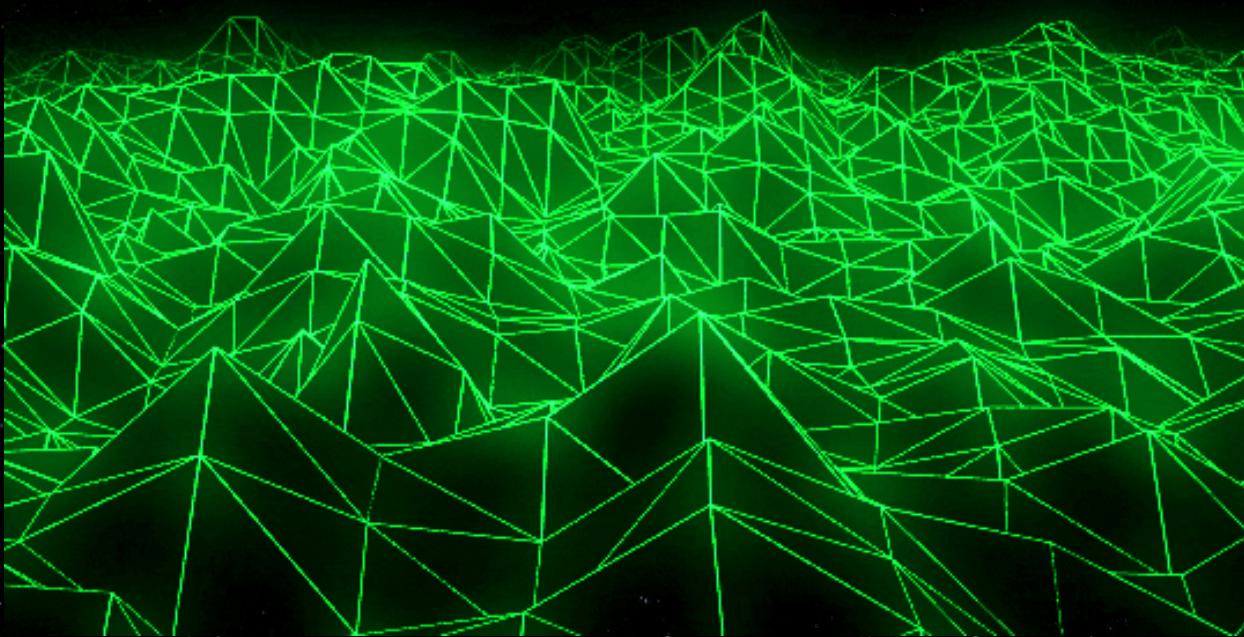
C:

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

B:

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

> POV Digital Forensics



METADATOS

LOGS

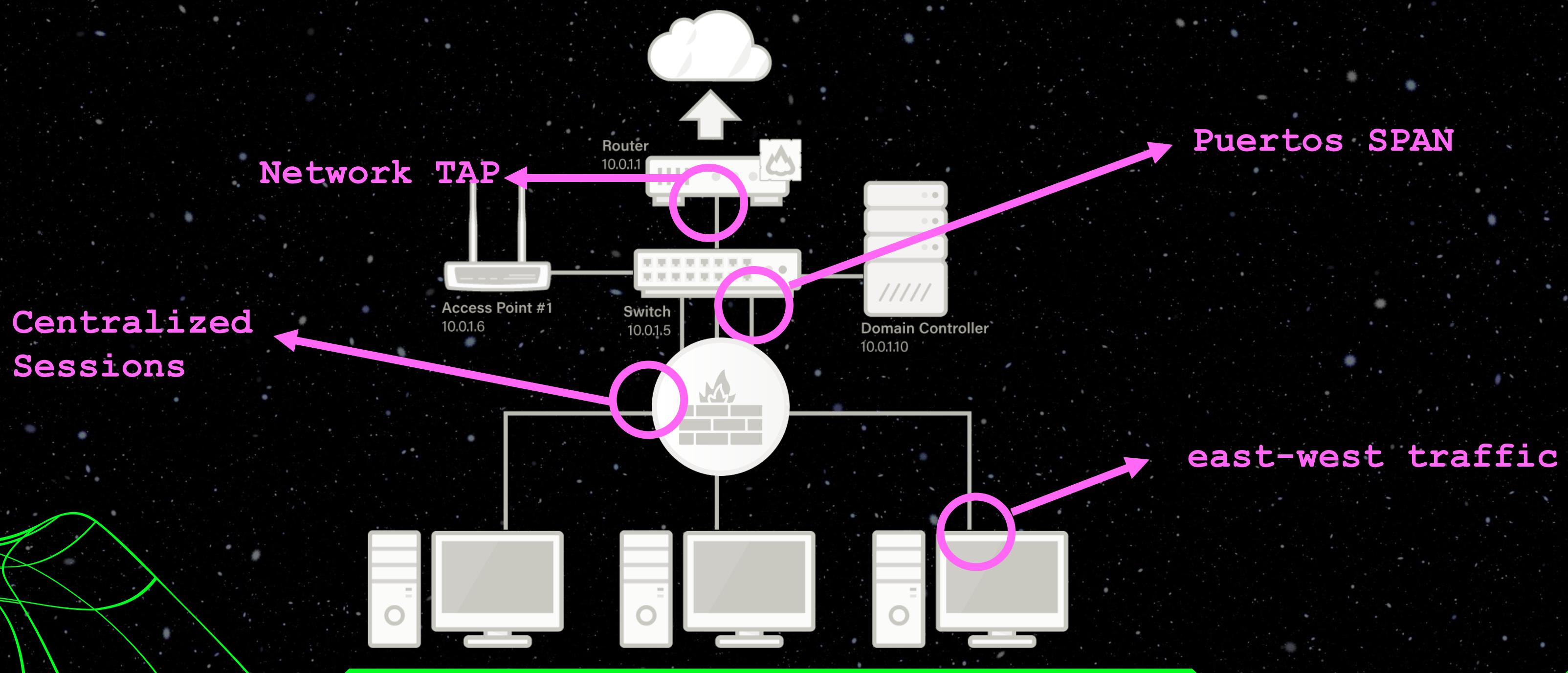
TRANSFERENCIAS DE ARCHIVOS

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

The screenshot shows a NetworkMiner interface with a list of captured network packets at the top and a detailed packet analysis window below. The analysis window for the fifth packet (Frame 22) is expanded, showing the following layers:

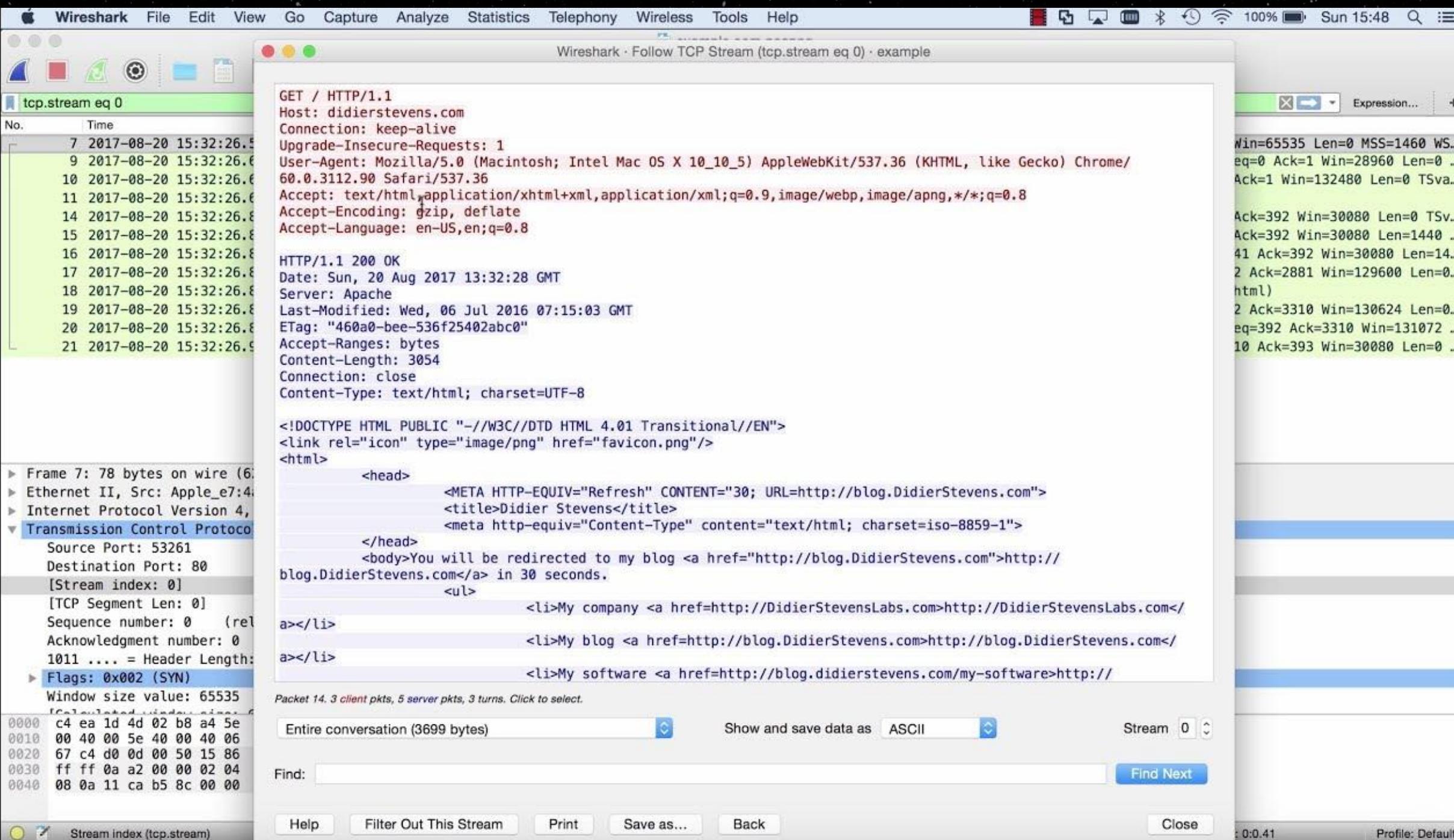
- L1 Frame 22: 586 bytes on wire (4688 bits), 586 bytes captured (4688 bits) on interface 0
- L2 Ethernet II, Src: SMCNetwo_e9:e2:c2 (b8:9b:c9:e9:e2:c2), Dst: CadmusCo_fd:d4:bd (08:00:27:fd:c0:00)
- L3 Internet Protocol version 4, Src: 173.194.33.179 (173.194.33.179), Dst: 10.0.0.2 (10.0.0.2)
- L4 Transmission Control Protocol, Src Port: 80 (80), Dst Port: 1435 (1435), Seq: 1, Ack: 563, Len: 563
- L5 Hypertext Transfer Protocol
- + Line-based text data: text/html

A red arrow points from the text "Application Layer" to the L5 entry in the analysis window.

FLUJOS DE RED

> Network Forensics

RECONSTRUCCIÓN 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 Mitigation**
- **Sabotage**
- **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



☰ Retro Talleres - Fati...

Q&A

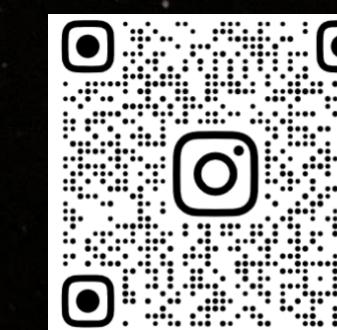
Polls

De forma general ¿cómo
calificas el taller? (Speaker +
teoría + ejercicios) 10

COMUNIDADES DE MUJERES EN CIBERSEGURIDAD



PRÓXIMAS ACTIVIDADES





THE END

Thank you for playing! Talino nga yorn! CHAR!

