

Alumno: Dragos Cornel Iván Andrei

Fecha:14 abril 2025

# **Documentación confidencial**

## **Tipo: Cadena de custodia**

## **Índice:**

<b>1. Introducción.....</b>	<b>3</b>
<b>2. Objetivos del procedimiento.....</b>	<b>3</b>
<b>3. Identificación de la evidencia digital.....</b>	<b>4</b>
<b>4. Entorno de trabajo.....</b>	<b>8</b>
<b>5. Metodologías de adquisición.....</b>	<b>10</b>
<b>6. Medidas de integridad y custodia.....</b>	<b>15</b>
<b>7. Evaluación de autenticidad, integridad, disponibilidad y legalidad.....</b>	<b>17</b>
<b>8. Posibles limitaciones y observaciones críticas.....</b>	<b>17</b>
<b>9. Conclusiones y observaciones.....</b>	<b>19</b>

## 1. Introducción

Para el siguiente trabajo, se me ha encomendado de forma directa la realización de una cadena de custodia digital sobre una página web determinada. La página objeto de análisis es la siguiente:

<https://www.unir.net/ingenieria/curso-perito-judicial-informatico/>

Este trabajo se ha llevado a cabo **en las instalaciones de la propia UNIR**, tal como ha sido requerido por la institución. El objetivo de esta actuación pericial es asegurar, con garantías técnicas y jurídicas, la correcta **preservación de las evidencias digitales** contenidas en la página web mencionada, permitiendo su eventual análisis y verificación por terceros en un entorno judicial o académico.

Durante el proceso se han tenido en cuenta los principios fundamentales de una correcta cadena de custodia digital:

- Se ha **dejado constancia fehaciente de la fecha y hora de inicio** de la actuación.
- Se ha verificado que la **página web accedida es auténtica**, pública y accesible desde cualquier navegador estándar sin autenticación previa.
- El procedimiento seguido permite que un tercero pueda **reproducir de forma íntegra el análisis realizado**, garantizando así la trazabilidad y transparencia del proceso.
- Asimismo, se ha considerado quiénes deben estar presentes en el acto de custodia, y se ha documentado dicha información como parte esencial del informe.

Este documento refleja, por tanto, todas las acciones llevadas a cabo desde el inicio del acceso a la evidencia digital hasta su captura, almacenamiento y preservación, respetando los principios de integridad, trazabilidad, transparencia y legalidad exigidos en el ámbito del peritaje informático.

## 2. Objetivo del procedimiento

El presente procedimiento tiene como finalidad establecer una **cadena de custodia digital** sobre la página web:

<https://www.unir.net/ingenieria/curso-perito-judicial-informatico/>

Este sitio ha sido designado por UNIR como objeto de análisis en el marco del Curso de Perito Judicial Informático. El propósito es garantizar la **conservación íntegra y verificable de su contenido**, permitiendo su uso como posible evidencia digital en un contexto pericial, académico o judicial.

La actuación tiene como objetivos específicos:

- Obtener una copia exacta del contenido público visible desde dicha URL.
- Asegurar la autenticidad y la no alteración del contenido capturado.
- Documentar cada fase del proceso de adquisición y custodia.
- Permitir la replicación futura del procedimiento por otro perito o parte interesada.
- Preservar las condiciones técnicas y legales necesarias para validar dicha evidencia.

### 3. Identificación de la evidencia digital

A continuación, se detallan los datos identificativos de la evidencia digital objeto de custodia:

- **URL accedida:**  
<https://www.unir.net/ingenieria/curso-perito-judicial-informatico/>
- **Fecha y hora de acceso inicial:**  
sáb 12 abr 2025 13:09:38 AM
- **Navegador utilizado para la verificación visual previa:** Firefox Browser v137.0.1 (64-bit)
- **Sistema operativo del equipo usado:** Ubuntu 22.04.5 LTS
- **Dirección IP pública asignada al equipo:** 212.102.49.212

Se ha usado la web <https://www.whatismybrowser.com/> para consultar los detalles del navegador usado y las direcciones IP.

## Direcciones IP usadas:

### Madrid (conexión matriz):

<b>IP ADDRESS</b>	<b><u>212.102.49.212</u></b>
This is your public IP Address.	<i>Your IP Address can identify you online. <a href="#">Use a VPN to help stay private and secure.</a></i>

### Montenegro:

<b>IP ADDRESS</b>	<b><u>176.125.229.4</u></b>
This is your public IP Address.	<i>Your IP Address can identify you online. <a href="#">Use a VPN to help stay private and secure.</a></i>

### Marruecos:

<b>IP ADDRESS</b>	<b><u>95.181.232.12</u></b>
This is your public IP Address.	<i>Your IP Address can identify you online. <a href="#">Use a VPN to help stay private and secure.</a></i>

- **Nombre de dominio resuelto:**

www.unir.net

- **Verificación de autenticidad del sitio:**

Se ha accedido a la web a través de un navegador actualizado, sin utilizar VPN ni proxies, verificando que el certificado SSL es válido y que el dominio corresponde a la entidad legítima. Se han comparado los resultados con

fuentes externas para confirmar que el contenido es el mismo que ve un usuario común al acceder a dicha URL.

Luego se ha accedido a la web con **PIA VPN version 3.6.1+08339**, desde 2 diferentes lugares, siendo **Madrid** (principal), luego desde **Montenegro** y desde **Marruecos** (VPN).

Así es como se vería el certificado de la web:

Certificate

*.unir.net	DigiCert TLS Hybrid ECC SHA384 2020 CA1	DigiCert Global Root CA
Subject Name		
Country	ES	
State/Province	La Rioja	
Locality	Logroño	
Organization	UNIVERSIDAD INTERNACIONAL DE LA RIOJA	
Common Name	*.unir.net	
Issuer Name		
Country	US	
Organization	DigiCert Inc	
Common Name	DigiCert TLS Hybrid ECC SHA384 2020 CA1	
Validity		
Not Before	Mon, 17 Feb 2025 00:00:00 GMT	
Not After	Wed, 18 Feb 2026 23:59:59 GMT	
Subject Alt Names		
DNS Name	*.unir.net	
DNS Name	unir.net	
Public Key Info		
Algorithm	Elliptic Curve	
Key Size	256	
Public Value	04:B2:7F:8E:C4:52:33:50:E7:63:D6:89:27:E9:5B:3D:91:29:FD:83:D9:00:AD:C0...	
Miscellaneous		
Serial Number	04:90:31:85:70:43:0C:D9:62:3C:D1:13:56:D3:7D:01	

Serial Number	04:90:31:85:70:43:0C:D9:62:3C:D1:13:56:D3:7D:01
Signature Algorithm	ECDSA with SHA-384
Version	3
Download	<a href="#">PEM (cert)</a> , <a href="#">PEM (chain)</a>

#### Fingerprints

SHA-256	07:B6:E2:61:5D:74:1E:B3:27:53:2D:92:76:00:DC:62:2B:15:1C:DA:3B:82:17:95...
SHA-1	C5:D8:9B:6E:C8:7E:CA:26:CB:7B:13:E5:3D:D1:82:A7:C5:03:69:FE

#### Basic Constraints

Certificate Authority	No
-----------------------	----

#### Key Usages

Purposes	Digital Signature, Key Agreement
----------	----------------------------------

#### Extended Key Usages

Purposes	Server Authentication, Client Authentication
----------	--

#### Subject Key ID

Key ID	AF:CB:CB:36:D4:2E:BD:90:88:39:A5:51:E9:A2:BD:95:67:DA:D6:29
--------	---

#### Authority Key ID

Key ID	0A:BC:08:29:17:8C:A5:39:6D:7A:0E:CE:33:C7:2E:B3:ED:FB:C3:7A
--------	---

#### CRL Endpoints

Distribution Point	<a href="http://crl3.digicert.com/DigiCertTLSHybridECCSHA3842020CA1-1.crl">http://crl3.digicert.com/DigiCertTLSHybridECCSHA3842020CA1-1.crl</a>
Distribution Point	<a href="http://crl4.digicert.com/DigiCertTLSHybridECCSHA3842020CA1-1.crl">http://crl4.digicert.com/DigiCertTLSHybridECCSHA3842020CA1-1.crl</a>

<b>CRL Endpoints</b>	
Distribution Point	http://crl3.digicert.com/DigiCertTLSHybridECCSHA3842020CA1-1.crl
Distribution Point	http://crl4.digicert.com/DigiCertTLSHybridECCSHA3842020CA1-1.crl
<b>Authority Info (AIA)</b>	
Location	http://ocsp.digicert.com
Method	Online Certificate Status Protocol (OCSP)
Location	http://cacerts.digicert.com/DigiCertTLSHybridECCSHA3842020CA1-1.crt
Method	CA Issuers
<b>Certificate Policies</b>	
Policy	Certificate Type ( 2.23.140.1.2.2 )
Value	Organization Validation
Qualifier	Practices Statement ( 1.3.6.1.5.5.7.2.1 )
Value	http://www.digicert.com/CPS
<b>Embedded SCTs</b>	
Log ID	96:97:64:BF:55:58:97:AD:F7:43:87:68:37:08:42:77:E9:F0:3A:D5:F6:A4:F3:36:...
Signature Algorithm	SHA-256 ECDSA
Version	1
Timestamp	Mon, 17 Feb 2025 00:09:19 GMT
Log ID	64:11:C4:6C:A4:12:EC:A7:89:1C:A2:02:2E:00:BC:AB:4F:28:07:D4:1E:35:27:AB:...
Signature Algorithm	SHA-256 ECDSA
Version	1
Timestamp	Mon, 17 Feb 2025 00:09:19 GMT
Log ID	49:9C:9B:69:DE:1D:7C:EC:FC:36:DE:CD:87:64:A6:B8:5B:AF:0A:87:80:19:D1:5...
Signature Algorithm	SHA-256 ECDSA
Version	1
Timestamp	Mon, 17 Feb 2025 00:09:19 GMT

## 4. Entorno de trabajo

La adquisición de la evidencia digital se ha llevado a cabo **en las oficinas de la Universidad Internacional de La Rioja (UNIR)**, cumpliendo así con las instrucciones establecidas por el cliente.

### 3.1 Ubicación física

- **Lugar:** Sede de UNIR en Av. de la Paz, 137, 26006 Logroño, La Rioja



- **Sala / puesto de trabajo:** aula rectorado nr13, primera planta
- **Condiciones de acceso:** Espacio controlado, con acceso restringido a personas autorizadas.

### 3.2 Recursos técnicos utilizados

- **Equipo informático:**
  - Marca / Modelo: Acer-A315-R7VH-R3-8GB128-15.6-FHD-20250412
  - CPU: Intel Core i5-8220U
  - RAM: 8 GB DDR4
  - Disco duro: SSD 617GB
  - Sistema operativo: Ubuntu 22.04.5 LTS
- **Conexión a Internet:**
  - Tipo: conexión por cable Ethernet
  - Dirección IP asignada: **212.102.49.212**

- **Herramientas de captura:**

-GNU Wget 1.21.2 built on linux-gnu.

-HTTrack version 3.49-2

### 3.3 Participantes en el procedimiento

A continuación, se detallan las personas que estuvieron presentes o participaron en el proceso:

Nombre y apellidos	Rol / Cargo	Firma (si aplica)
--------------------	-------------	-------------------

Dragos Cornel Iván  
Andrei

Alumno – Perito actuante

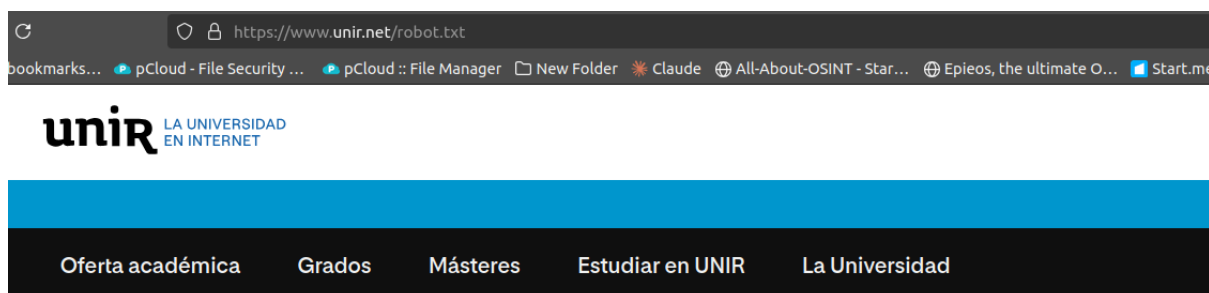
María Andrea  
Escobar Jiménez

Testigo-Observadora,  
responsable técnica del  
área de informática

## 5. Metodología de adquisición

Como vemos en la página de abajo que debemos custodiar, no parece que haya un archivo robot.txt en la web, de modo que la descarga puede llegar a ser más sencilla. ¿Por qué? Porque en el caso de estar usando **wget** y no modificar tu User-Agent, **wget** detectará esa restricción y respetará el **robots.txt** por defecto, pudiendo ser el caso que el robot.txt tenga instrucciones de bloquear a wget o a httrack.

De modo que hemos ido a la web de UNIR y en el URL hemos añadido “robot.txt”. Como hemos dicho, la respuesta fue negativa:



## Lo sentimos, la titulación que buscas no está aquí

La página solicitada puede no estar disponible, haber cambiado de dirección (URL) o no existir. Por favor, comprueba que has escrito la dirección correctamente.

Te ayudamos a encontrar los estudios que estás buscando a través de nuestra [oferta académica por Facultades](#) o entre nuestros diferentes [Grados](#) y [Postgrados](#).

- **Herramientas empleadas Wget y HTTrack.**

Para esta práctica y a modo de ejercicio, quise trabajar con ambas herramientas y documentar el proceso, ya que me eran desconocidas.

Con **wget** en terminal escribimos:

```
wget --user-agent="Mozilla/5.0 (X11; Ubuntu; Linux x86_64; rv:137.0) Gecko/20100101 Firefox/137.0.1" https://www.unir.net/ingenieria/curso-perito-judicial-informatico/
```

Donde `--user-agent`: le indica a wget que use ese **User-Agent** en lugar del predeterminado.

La salida sería esta:

```
_Avanzado/Trabajos/Trabajo1_cadenaCustodia_UNIR$ wget --user-agent="Mozilla/5.0 (X11; Ubuntu; Linux x86_64; rv:137.0) Gecko/20100101 Firefox/137.0.1" https://www.unir.net/ingenieria/curso-perito-judicial-informatico/
--2025-04-12 13:09:38-- https://www.unir.net/ingenieria/curso-perito-judicial-informatico/
Resolving www.unir.net (www.unir.net)... 2a02:26f0:2380:c::212:bc16, 2a02:26f0:2380:c::212:bc17, 96.16.88.191, ...
Connecting to www.unir.net (www.unir.net)|2a02:26f0:2380:c::212:bc16|:443... connected.
HTTP request sent, awaiting response... 200 OK
Length: unspecified [text/html]
Saving to: 'index.html'

index.html           [ <=>          ] 386,12K  2,32MB/s   in 0,2s

2025-04-12 13:09:38 (2,32 MB/s) - 'index.html' saved [395385]

chocolate@intel:~/windows2024/escritorio_final/1 UNIR ciber/Peritaje_Informatico
_Avanzado/Trabajos/Trabajo1_cadenaCustodia_UNIR$
```

Si hubiera sido una página con fuertes restricciones, hubiéramos tenido que reforzar también nuestro script. Ejemplo hipotético:

```
wget --mirror --convert-links --adjust-extension --page-requisites --no-parent \ --user-agent="Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/123.0.0.0 Safari/537.36" \ --wait=2 --random-wait --limit-rate=100k
```

```
--execute robots=off \  
https://www.unir.net/ingenieria/curso-perito-judicial-informatico/
```

Donde:

- mirror: Modo espejo (equivale a -r -N -l inf --no-remove-listing)
- convert-links: Convierte los enlaces para navegación local
- adjust-extension: Añade extensiones adecuadas a los archivos
- page-requisites: Descarga imágenes, CSS, etc.
- limit-rate=100k: Evita sobrecargar el servidor
- user-agent: Muy importante para parecer un navegador

Por otro lado, con **HTTrack** me he encontrado lo siguiente:

He probado el script:

```
httrack  
"https://www.unir.net/ingenieria/curso-perito-judicial-informatico  
/" \ --user-agent "Mozilla/5.0 (Windows NT 10.0; Win64; x64)  
AppleWebKit/537.36 (KHTML, like Gecko) Chrome/123.0.0.0  
Safari/537.36" \ -r3 -c1 --robots=0 --disable-security-limits  
--max-rate=100000
```

Donde:

- r3: Nivel de profundidad (3 es moderado)
- c1: Solo 1 conexión a la vez
- robots=0: Ignora robots.txt
- disable-security-limits: Desactiva límites automáticos de HTTrack
- max-rate=100000: Limita la velocidad a ~100 KB/s

Sin embargo me he encontrado el error 403, es decir, “forbidden”, es decir la web me ha bloqueado el acceso (el servidor ha comprendido la solicitud, pero se niega a autorizarla).

```
chocolate@intel:~/windows2024/escritorio_final/1 UNIR ciber/Peritaje_Informatico_Avanzado/Trabajos/httrack-3.49.2$ httrack "https://www.unir.net/ingenieria/curso-perito-judicial-informatico/" \
--user-agent "Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/123.0.0.0 Safari/537.36" \
-r3 -cl --robots=0 --disable-security-limits --max-rate=100000
Mirror launched on Mon, 14 Apr 2025 16:27:25 by HTTrack Website Copier/3.49-2+libhtsjava.so.2 [XR&C0'2014]
mirroring https://www.unir.net/ingenieria/curso-perito-judicial-informatico/ with the wizard help..
* https://www.unir.net/ingenieria/curso-perito-judicial-informatico/ (431 bytes)
1/2: https://www.unir.net/ingenieria/curso-perito-judicial-informatico/ (431 byte)
Done.403
Thanks for using HTTrack!
chocolate@intel:~/windows2024/escritorio_final/1 UNIR ciber/Peritaje_Informatico_Avanzado/Trabajos/httrack-3.49.2$
```

Si la app no funciona a pesar de haber usado un User-Agent legítimo (Chrome), haber desactivado robots.txt, y haber eliminado los límites de seguridad de HTTrack, esto puede significar que la web puede tener otros mecanismos de defensa (por ejemplo: protección contra scrapers, firewall web, detección por IP, etc.)

De modo que para este ejercicio nos quedaremos con lo que hemos encontrado con wget. Al ser **wget** más ligero y menos detectado que httrack sí hemos conseguido al primer intento nuestra carpeta “index.html”.

- **Compresión del archivo y verificación de integridad de cálculo de hash: SHA1 y SHA256:**

Antes de calcular el hash, hemos comprimido el archivo ‘**index.html**’ con la aplicación de compresión **RAR**, **versión 6.23** Copyright (c) 1993-2023 Alexander Roshal 1 Aug 2023 Trial version.

Para ello se ha usado el siguiente comando:

```
rar a -m5 -hp -tl -k -rr3 nombre_archivo_destino.rar archivo.html
```

Donde:

- **a:** añadir archivos al archivo RAR

- **-m5**: nivel máximo de compresión
- **-hp**: solicita contraseña para cifrar el contenido
- **-tl**: guarda la hora de modificación del archivo
- **-k**: bloquea el archivo RAR contra escritura posterior
- **-rr3**: añade 3% de información de recuperación ante errores

Comprobamos que el archivo sigue ahí y solo se abre con la contraseña “contraseña”:

```
chocolate@intel: ~/windows2024/escritorio_final/1 UNIR ciber/Peritaje_Informatico_Avanzado/Trabajos/Trabajo1_cadenaCustodia_UNIR$ unrar l evidencia_destino.rar

UNRAR 6.11 beta 1 freeware      Copyright (c) 1993-2022 Alexander Roshal

Enter password (will not be echoed) for evidencia_destino.rar:

Archive: evidencia_destino.rar
Details: RAR 5, recovery record, lock, encrypted headers

  Attributes      Size      Date      Time      Name
  -----
*-rw-rw-r--      395385    2025-04-12 03:21  index.html
  -----
                        395385                        1

chocolate@intel:~/windows2024/escritorio_final/1 UNIR ciber/Peritaje_Informatico_Avanzado/Trabajos/Trabajo1_cadenaCustodia_UNIR$
```

Aquí el hash del archivo comprimido a custodiar:

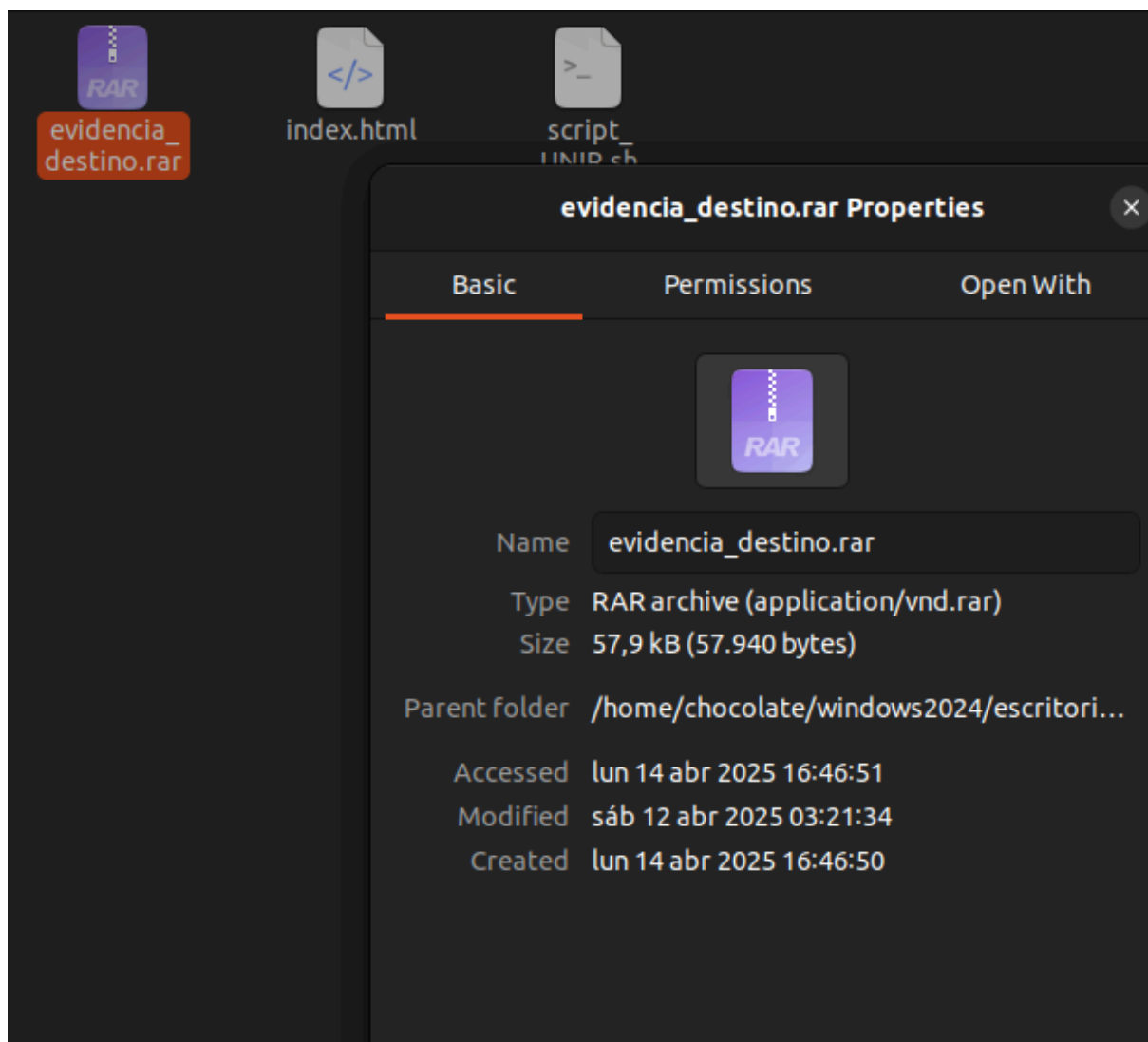
```
chocolate@intel:~/windows2024/escritorio_final/1 UNIR ciber/Peritaje_Informatico_Avanzado/Trabajos/Trabajo1_cadenaCustodia_UNIR$ shasum evidencia_destino.rar
3188097b8952d79c3eb465e4e80438cf44ee14b6  evidencia_destino.rar
chocolate@intel:~/windows2024/escritorio_final/1 UNIR ciber/Peritaje_Informatico_Avanzado/Trabajos/Trabajo1_cadenaCustodia_UNIR$
```

Para mayor seguridad hemos calculado también el sha256:

```
chocolate@intel:~/windows2024/escritorio_final/1 UNIR ciber/Peritaje_Informatico_Avanzado/Trabajos/Trabajo1_cadenaCustodia_UNIR$ sha256sum evidencia_destino.rar
86150de5ad01d1a908350c4f75ba21b6e003a81505dad083e860b5ad8c967a7e  evidencia_destino.rar
chocolate@intel:~/windows2024/escritorio_final/1 UNIR ciber/Peritaje_Informatico_Avanzado/Trabajos/Trabajo1_cadenaCustodia_UNIR$
```

## 6. Medidas de integridad y custodia

- Cómo se asegura que la evidencia no ha sido manipulada: tanto el haber **comprimido con contraseña** de acceso el archivo .html a custodiar, como el haberle **calculado el hash con sha1 y sha256**, todo ello asegura la no manipulación de la evidencia. De modo que si nos vamos a las propiedades de nuestro archivo, podremos ver **fecha y hora de acceso, modificación y creación**.



- Dónde se almacena:

La evidencia se almacenará en dos pendrives marca Kingston v3, siendo uno de ellos de respaldo, encriptado con contraseña, y código de barras 1234567890 (original) y 0987654321 (backup). El alumno en prácticas Dragos Cornel Iván Andrei se hará responsable del pendrive y de la evidencia hasta nueva orden, desde la fecha 12 de abril de 2025 a las 15:00h UTC.



### Cadena de custodia

- Tabla cronológica:
  - **Fecha/hora:** 12/abril/2025, 15:00h UTC.
  - **Persona responsable:** Dragos Cornel Iván Andrei
  - **Acción realizada:** descarga de archivo .html vía wget, compresión del archivo via .rar con contraseña añadida, comprobación de la correcta descompresión del archivo, creación de hash sha1 y sha256 del archivo comprimido, comprobación de la hora y fecha de la creación del archivo comprimido.



- **Observaciones:** Se han usado 2 pendrives para custodiar la prueba. Desde uno se trabajará y el otro se guardará como copia de respaldo, estando ambos pendrives encriptados.

## **7. Evaluación de autenticidad, integridad, disponibilidad y legalidad**

### **Autenticidad**

La autenticidad de la evidencia digital ha sido garantizada mediante la verificación directa del sitio web objeto de análisis desde múltiples ubicaciones geográficas (Madrid, Montenegro y Marruecos) usando VPN, además de una inspección del certificado SSL válido y la coincidencia del contenido con lo que un usuario común vería. Esta validación asegura que el contenido capturado pertenece legítimamente al dominio [www.unir.net](http://www.unir.net).

### **Integridad**

Se ha preservado la integridad de la evidencia mediante la compresión del archivo en formato [.rar](#) con contraseña y con bloqueo contra escritura (-k). Posteriormente, se han calculado los hashes SHA1 y SHA256, lo cual permite detectar cualquier alteración posterior. La coincidencia futura de estos valores hash garantizará que el archivo no ha sido modificado desde su custodia original.

### **Disponibilidad**

La evidencia se ha almacenado en dos dispositivos físicos USB (pendrives Kingston), uno principal y otro de respaldo, ambos cifrados y etiquetados. Esta doble custodia física garantiza la disponibilidad continua del material frente a fallos técnicos o pérdida del soporte original.

### **Legalidad**

El procedimiento se ha realizado en cumplimiento con los principios técnicos y jurídicos aceptados en peritaje informático. Se ha documentado la totalidad del proceso, incluyendo la fecha y hora de actuación, herramientas utilizadas, entorno de trabajo, participantes y medidas de protección de la evidencia. La participación de un testigo-cliente y la trazabilidad completa del proceso aseguran la validez legal y probatoria de la cadena de custodia.

## **8. Posibles limitaciones y observaciones críticas**

Puntos débiles o áreas de mejora:

### **1. Ausencia de un sellado temporal externo (timestamping)**

Aunque se ha dejado constancia fehaciente de la fecha y hora de actuación, no se ha realizado un sellado temporal certificado por una autoridad externa (como un TSA – Time Stamping Authority). Esto podría ser utilizado para cuestionar si los hashes fueron realmente generados en la fecha que se indica, dado que no hay prueba externa e inmutable de ello.

### **2. Protección basada en .rar, no en contenedor forense estandarizado**

El uso de compresión .rar con contraseña y bloqueo es eficaz, pero no corresponde con formatos de contenedor forense estandarizados como E01 (EnCase), AFF o incluso formatos abiertos como .dd con metadatos. Aunque es una elección válida en un contexto académico, podría ser objeto de crítica si se exigiera una cadena forense profesional más rigurosa.

### **3. Contraseña no depositada ante tercero**

La contraseña utilizada para cifrar el archivo no ha sido registrada o depositada ante una tercera parte independiente. En un procedimiento judicial formal, se recomendaría que la clave estuviera disponible bajo custodia notarial o encriptada mediante clave pública para permitir la apertura sin dependencia del perito actuante.

### **4. Entorno de captura no monitorizado digitalmente**

Aunque el procedimiento se realizó en una sala controlada, no se ha incluido evidencia de monitoreo del entorno (registro en vídeo, logs del sistema, auditoría de accesos, etc.) durante la captura. Esto deja un pequeño margen a la especulación sobre la posibilidad de manipulación del entorno digital o físico durante la actuación.

### **5. Limitaciones propias de la metodología empleada (wget)**

La elección de wget frente a herramientas especializadas en adquisición forense de sitios web limita el tipo de contenido capturable. Por ejemplo, wget no accede a contenido generado dinámicamente mediante JavaScript ni a sesiones autenticadas, lo cual restringe la cobertura del análisis a contenido puramente estático.

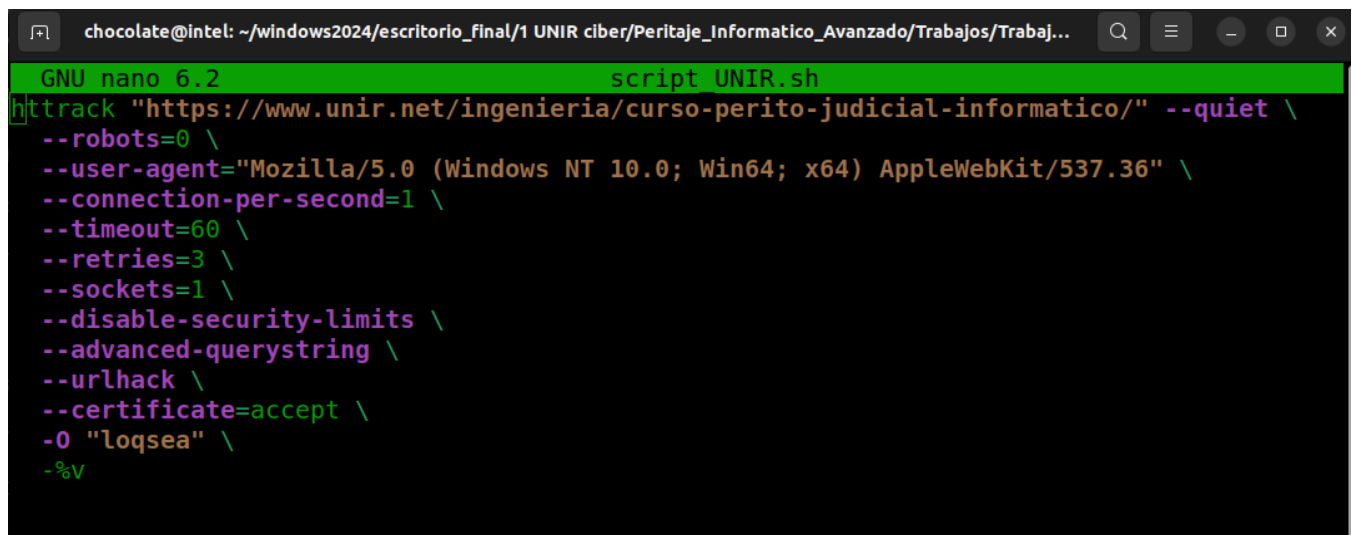
### **6. Fallo de HTTrack no documentado exhaustivamente**

Aunque se indica que HTTrack fue bloqueado con error 403 y se incluye parte del log, podría considerarse una omisión no haber adjuntado el archivo hts-log.txt completo para su evaluación técnica por terceros. Este archivo podría haber aportado más contexto sobre los mecanismos de defensa del servidor y sobre el comportamiento de la herramienta.

## 9. Conclusiones y observaciones

- **Observaciones finales:** todo se desarrolló sin contratiempos importantes.
- **Reflexión sobre presencia en la realización de la cadena de custodia:** El perito informático en este caso aporta el conocimiento técnico necesario para realizar una captura forense precisa, siguiendo métodos reproducibles y verificables. La presencia de la testigo-cliente garantiza la legitimidad del encargo y actúa como respaldo humano del procedimiento. No es necesario un notario, ya que su función se limita al testimonio visual, sin capacidad técnica para validar la integridad digital. En este contexto, la validez probatoria reside en la metodología forense y la trazabilidad de la evidencia, no en la figura notarial.
- **Limitaciones,** si las hubo:

Como no me he rendido con **httrack**, se ha intentado crear un script algo más complejo en bash, con la esperanza de forzar una descarga mucho más discreta.



```
chocolate@intel: ~/windows2024/escritorio_final/1 UNIR ciber/Peritaje_Informatico_Avanzado/Trabajos/Trabaj...
GNU nano 6.2 script UNIR.sh
httrack "https://www.unir.net/ingenieria/curso-perito-judicial-informatico/" --quiet \
--robots=0 \
--user-agent="Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36" \
--connection-per-second=1 \
--timeout=60 \
--retries=3 \
--sockets=1 \
--disable-security-limits \
--advanced-querystring \
--urlhack \
--certificate=accept \
-o "loqsea" \
-%V
```

A modo de curiosidad, destacar que **no hubo éxito** y acabamos siendo bloqueados igualmente, siendo este el error recibido:

Information, Warnings and Errors reported for this mirror:

note: the hts-log.txt file, and hts-cache folder, may contain

sensitive information, such as username/password authentication for websites mirrored in this project do not share these files/folders if you want these information to remain private

```
21:21:18 Warning: * security warning: !!! BYPASSING SECURITY
LIMITS - MONITOR THIS SESSION WITH EXTREME CARE !!!
21:21:19 Warning: Retry after error -5
(error:00000005:lib(0)::reason(5)) at link
https://www.unir.net/ingenieria/curso-perito-judicial-informatico/
(from primary/primary)
21:21:20 Warning: Retry after error -5
(error:00000005:lib(0)::reason(5)) at link
https://www.unir.net/ingenieria/curso-perito-judicial-informatico/
(from primary/primary)
21:21:22 Warning: Retry after error -5
(error:00000005:lib(0)::reason(5)) at link
https://www.unir.net/ingenieria/curso-perito-judicial-informatico/
(from primary/primary)
21:21:23 Error: "error:00000005:lib(0)::reason(5)" (-5)
after 3 retries at link
https://www.unir.net/ingenieria/curso-perito-judicial-informatico/
(from primary/primary)
21:21:23 Warning: No data seems to have been transferred
during this session! : restoring previous one!
```

Podemos traducir estos errores de la siguiente manera:

### **security warning: !!! BYPASSING SECURITY LIMITS**

-Has desactivado límites de seguridad del programa, lo que puede hacer que el comportamiento parezca sospechoso para el servidor.

### **Retry after error -5 (error:00000005:lib(0)::reason(5))**

-El servidor ha **rechazado la conexión** o ha **bloqueado el acceso** tras detectar actividad no deseada (como scraping).

### **Error: error:00000005 después de 3 intentos**

-HTTrack ha **fallado en los 3 intentos de conexión** con la URL objetivo, por protección del servidor.

**No data seems to have been transferred during this session**

**-No se ha descargado nada útil**, probablemente porque el acceso fue completamente denegado.

Final de trabajo.