**Análisis Forense**

# Tanner

### 

### 

### 

[**Tanner 1**](#_n6arwwmay01c)

[**Instrucciones 2**](#_54baeb9ebltk)

[**Contexto 3**](#_qbc16gcve9y5)

[**Entorno de Simulación: 4**](#_o8nnrmu51s15)

[**OBJETIVOS 4**](#_v1csafyn10fx)

[1. [0,75p] A fin de que los abogados de la mafia no puedan alegar que se ha roto la cadena de custodia, comprueba que la evidencia no ha sufrido alteraciones. Haz esto tanto con PowerShell como con Autopsy. 4](#_xswqr7w3s2zr)

[2. [0,75p] Comprueba que Tanner tiene un usuario en el equipo, y cuándo hizo login por última vez. Haz esto tanto en Autopsy como en Windows Registry Recovery. 5](#_ohoam9el6br5)

[3. [0,75p] Comprueba la versión del Sistema Operativo. Haz esto tanto en Autopsy como en Windows Registry Recovery. 6](#_ju79vcmp2yqw)

[5. [0,75p] Comprueba que Tanner sólo introdujo un pendrive en el equipo, porque debería ser el pendrive en el que se creó la imagen de memoria con DumpIt. ¿Cuál es dicho pendrive y a qué hora lo introdujo? 8](#_yaowonej3qla)

[6. [1p] Tanner ha accedido a un fichero con extensión .doc recientemente ¿En qué 8](#_6emzeig1e56j)

[fecha y hora fue accedido? 9](#_bl6cu4asozqa)

[7. [1,5p] Tanner ha estado buscando información sobre un afamado terrorista. En concreto, ha estado viendo vídeos sobre él en una plataforma online. ¿Quién es dicho terrorista? 9](#_p5fjwv66dpmy)

[9. [1,5p] Tanner se aloja en el Holiday Inn Manhattan Financial District, pero Jean Paul está alojado en otro hotel diferente. Tanner tiene planeado ir a buscarlo en su coche. ¿En qué hotel se aloja Jean Paul? 10](#_k3g20ip5vv6j)

[10. [1p] Tras acabar la misión, Tanner tiene pensado ir a otro lugar. ¿Cuál es dicho lugar y cómo tiene pensado ir? 11](#_k0oxzm6m8z7o)

# Instrucciones

1. Cambiar el nombre del fichero por el de NombreApellido-Tanner.img

2. Para la parte práctica se pide hacer un informe que responda a las cuestiones que se piden más abajo. Cada una de ellas debe ser respondida aportando la mayor evidencia posible al respecto.

3. No es necesario aportar pruebas de lo que no se pide. Por ejemplo, no es necesario poner el resultado del imageinfo en Volatility, ni capturas de cómo se ha creado el caso en Autopsy, etc.

4. Sin embargo, sí se pide justificar lo más posible las respuestas a las preguntas. Es necesario sacar capturas de pantalla para apoyar dicha justificación, pero no basta con poner únicamente la captura, sino que hay que explicarla con un texto, teniendo en cuenta que el objetivo final es elaborar una pericial para ir a juicio.

5. A menos que en un apartado se especifique lo contrario, la parte de análisis de disco ha de resolverse con Autopsy.

# 

# Contexto

El ex-piloto de carreras John Tanner es ahora un policía infiltrado en la Mafia de **Nueva York**. Su capo, el señor **Castaldi**, planea un golpe de forma inminente.

Suponemos que el elegido para llevarlo a cabo es el implacable asesino a sueldo **Jean Paul**, alias “**El Francés**”, y que, como de costumbre, **Tanner** conducirá el coche de la huida. Sin embargo, aún no sabemos cuál es el objetivo. Lo que sí sabemos es que Tanner estuvo manteniendo conversaciones con el Sr. Castaldi a través de una **aplicación de chat**. Por desgracia, dicha aplicación está cifrada con un mecanismo conocido como **Double Ratchet**, similar al que usan WhatsApp y sus competidores y, por tanto, no hemos podido intervenir dichas comunicaciones.

Ahora, Tanner está desaparecido y su ordenador está frito, lo cual no es de extrañar, pues medio FBI y parte de la policía metropolitana están sobornados. Por suerte, poco antes del golpe, uno de nuestros técnicos pasó a Tanner un USB con un programa para ejecutar. Dicho programa, llamado **DumpIt**, sirve para recoger una imagen de memoria del equipo.

Cuando nuestros hombres llegaron, el USB estaba en el escondrijo acordado, así que quizás los agentes **corruptos del FBI** no lo habían tocado.

Como era de esperar, allí había una imagen de memoria con lo último que Tanner ejecutó en el ordenador antes de salir. Además, como habíamos quedado, en la recepción del hotel de enfrente de su apartamento nos dejó una nota en la cual estaba escrito el código **hash** de la imagen creada:

**a518111a8f288d94fb4fb0069e36a884e1483f72b51b876303b6c7cfcb945715**

Finalmente unos expertos en hardware han logrado rescatar una imagen del disco de Tanner. Con la nueva información adquirida, podemos sacar algunos datos más de su actividad en los últimos días. Los hashes que nos han pasado son los siguientes:

**MD5: 8712a3760e8fc801425309852ee1127a CapturaForense.img**

**SHA-1: eaa88659a5dd2453527ffee0ccb13447c7223184 CapturaForense.img**

**SHA-256: 4216bb636648b7a4188aacef3587c64aabfb05aade76b6070b3ce8d66d4568a CapturaForense.img**

# Entorno de Simulación:

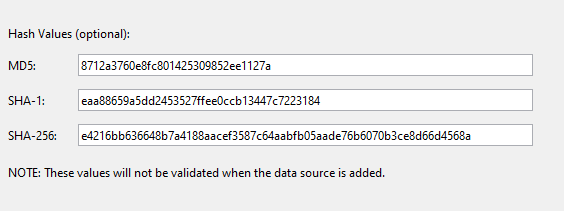
- Herramientas Forenses: Autopsy

# 

# OBJETIVOS

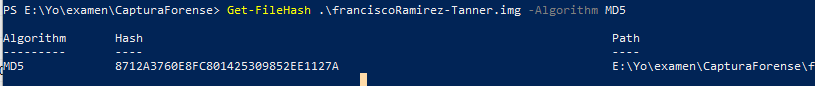
Buscar de cualquier actividad sospechosa, para ello vamos a responder a las siguientes cuestiones:

### 1. [0,75p] A fin de que los abogados de la mafia no puedan alegar que se ha roto la cadena de custodia, **comprueba** que la evidencia no ha sufrido alteraciones. Haz esto tanto con **PowerShell como con Autopsy**.

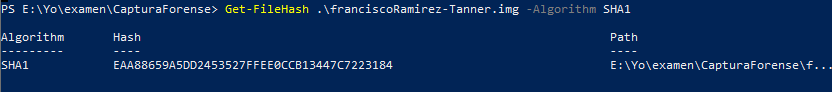


**Powershell**

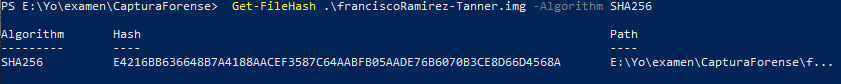
* MD5 → 8712A3760E8FC801425309852EE1127A



* SHA-1 → EAA88659A5DD2453527FFEE0CCB13447C7223184



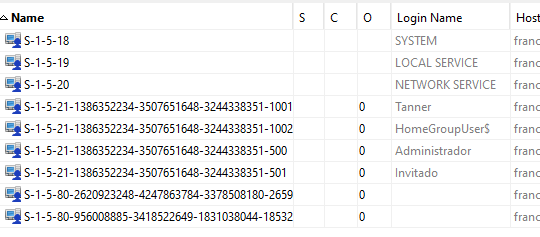
* SHA-256 → E4216BB636648B7A4188AACEF3587C64AABFB05AADE76B6070B3CE8D66D4568A



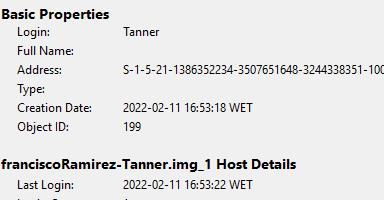
Tras comparar los hashes, podemos comprobar que la prueba **NO ha sido modificada.**

**Autopsy**

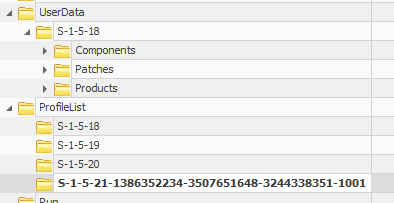
### 2. [0,75p] Comprueba que **Tanner tiene un usuario** en el equipo, y **cuándo hizo login por última vez**.Haz esto tanto en Autopsy como en Windows Registry Recovery.

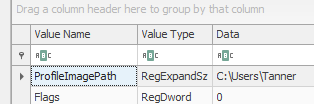
**Autopsy** Usuario Tanner

Última vez accedido el usuario **Tanner: 2022-02-11 16:53:18 WET**

****

Windows Explorer→ Usuario Tanner



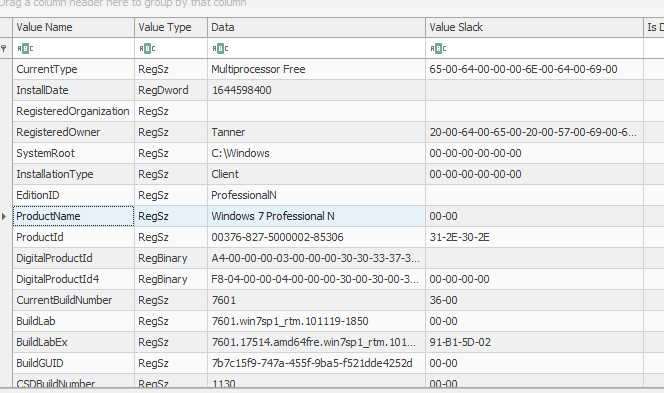


### 3. [0,75p] Comprueba la **versión del Sistema Operativ**o. Haz esto tanto en Autopsy como en Windows Registry Recovery.

**Autopsy versión →** Windows 7 Professional N

* ****

**Windows Explorer →** Data Windows 7 Professional N

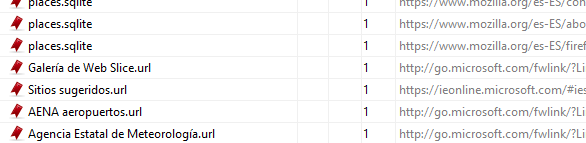


4. [1p] Por seguridad, Tanner ha instalado en el sistema un **navegador web** que no es de Microsoft. Consigue pruebas de **cuál es y de que ha sido instalado**. Haz esto tanto en Autopsy como en Windows Registry Recovery.

**Autopsy Navegador**

**-**Indirectamente podemos saber los navegadores con el módulo de webs.

Rápidamente sabemos que cuenta tambien con mozilla firefox



Su navegador por defecto es Mozilla



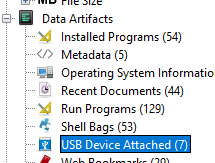
**Instalación**

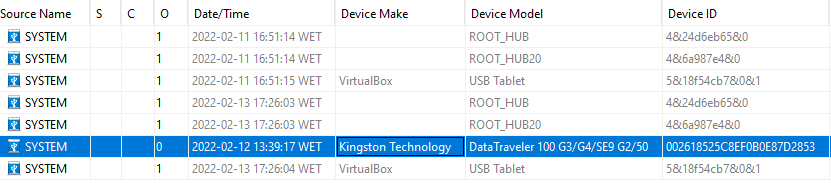
****

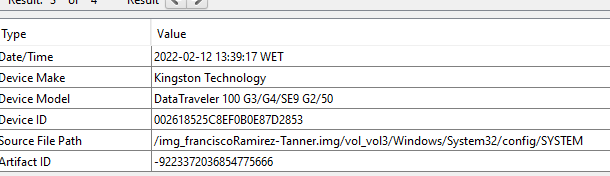
**Windows Registry Recovery**

### 5. [0,75p] Comprueba que Tanner sólo introdujo un pendrive en el equipo, porque debería ser el pendrive en el que se creó la imagen de memoria con DumpIt. ¿Cuál es dicho pendrive y a qué hora lo introdujo?

Encontramos que solamente se ha introducido un pendrive **DataTraveler 100 G3/G4/SE9 G2/50,** de **Kingston Technology .** A las **2022-02-12 13:39:17 WET.**





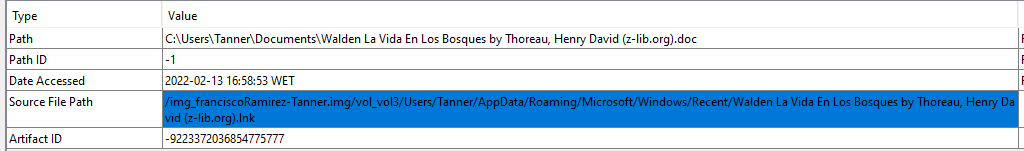


### 6. [1p] Tanner ha accedido a un fichero con extensión .doc recientemente ¿En qué

### fecha y hora fue accedido?

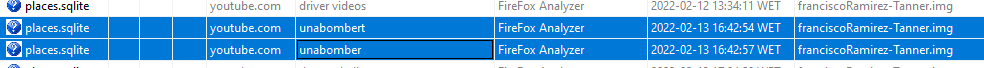
El último archivo de tipo **.doc** se trata de **Walden La Vida En Los Bosques by Thoreau, Henry David (z-lib.org).doc,**  accedido el **2022-02-13 16:58:53 WET**

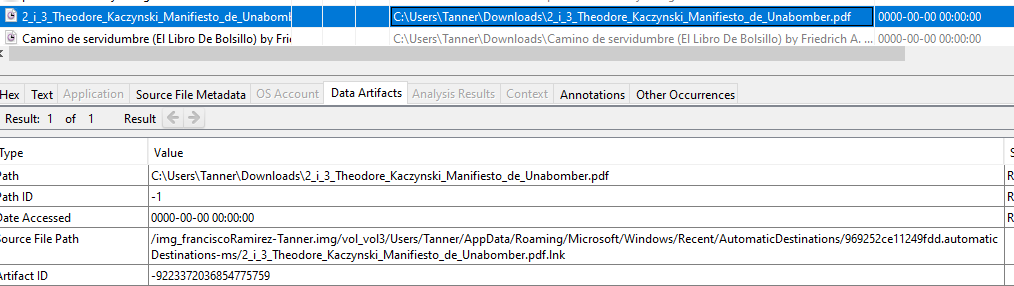
### 



### 7. [1,5p] Tanner ha estado buscando información sobre un afamado terrorista. En concreto, ha estado viendo vídeos sobre él en una plataforma online. ¿Quién es dicho terrorista?

* [**Unabomber**](https://www.google.com/url?sa=t&rct=j&q=&esrc=s&source=web&cd=&cad=rja&uact=8&ved=2ahUKEwjng-mMwpaEAxXfhv0HHdAhDAkQFnoECDkQAQ&url=https%3A%2F%2Fen.wikipedia.org%2Fwiki%2FTed_Kaczynski&usg=AOvVaw0lfA6X1JL-CmBQ7WvSlYV2&opi=89978449)
* La plataforma es  **Youtube.**



También descargo y accedió recientemente a su manifiesto:

8. [1p] Para acabar con Jean Paul, Tanner ha adquirido un arma. ¿Sobre qué arma en concreto ha buscado información?

[Smith and wesson 9mm](https://www.google.com/url?sa=t&rct=j&q=&esrc=s&source=web&cd=&cad=rja&uact=8&ved=2ahUKEwi-kIXXwpaEAxX9UaQEHUTPA4kQFnoECBYQAQ&url=https%3A%2F%2Fwww.tiendashoke.es%2Fpistolas-de-fuego%2Fpistola-smith-wesson-mp9-shield-m2-0&usg=AOvVaw0vn5clJbQJtIrQwma5kywK&opi=89978449)

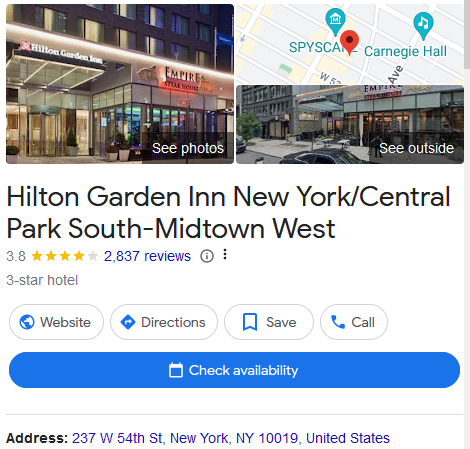


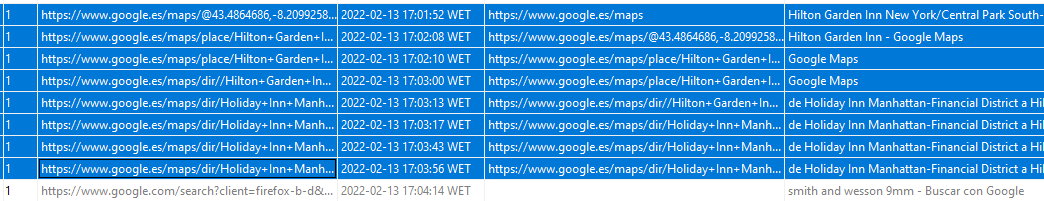


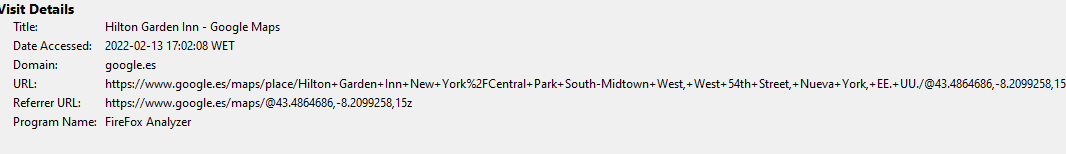
### 9. [1,5p] Tanner se aloja en el Holiday Inn Manhattan Financial District, pero Jean Paul está alojado en otro hotel diferente. Tanner tiene planeado ir a buscarlo en su coche. ¿En qué hotel se aloja Jean Paul?

En el historial de búsqueda Tanner busca la dirección en google maps del

**Hilton Garden Inn New York/Central Park South-Midtown West,** justo antes de comenzar a hacer búsquedas sobre pistolas Smith Wesson. Puede relacionarse el destino de la víctima.

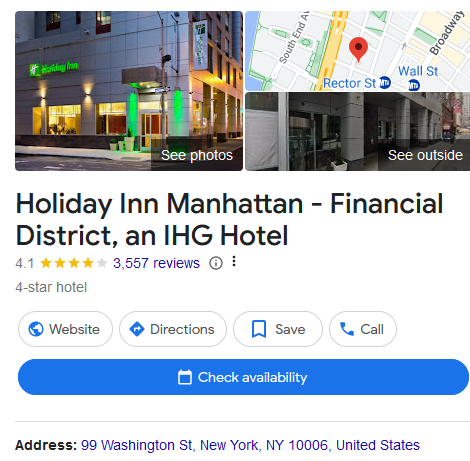






### 10. [1p] Tras acabar la misión, Tanner tiene pensado ir a otro lugar. ¿Cuál es dicho lugar y cómo tiene pensado ir?

Tanner se aloja en el Holiday Inn Manhattan Financial Distric, **Nueva York**.



Teniendo el origen, las siguientes búsquedas indican que tiene pensado viajar a **Cancún.**

****

****