



Corso di Digital Forensics

CdLM in Informatica

Università degli Studi di Salerno

Docente: Ugo Fiore

5 – Fase di analisi

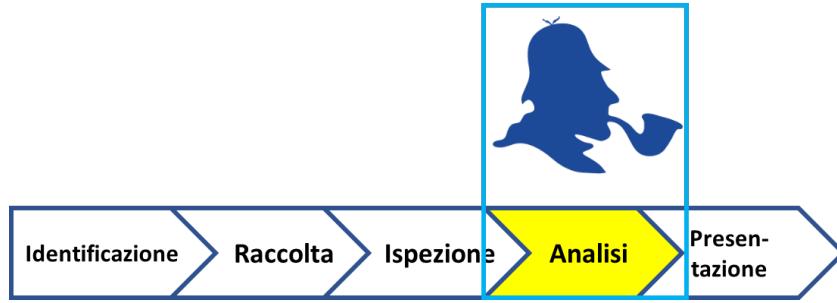
Analisi | Richiami

- Dall'Argomento 1...



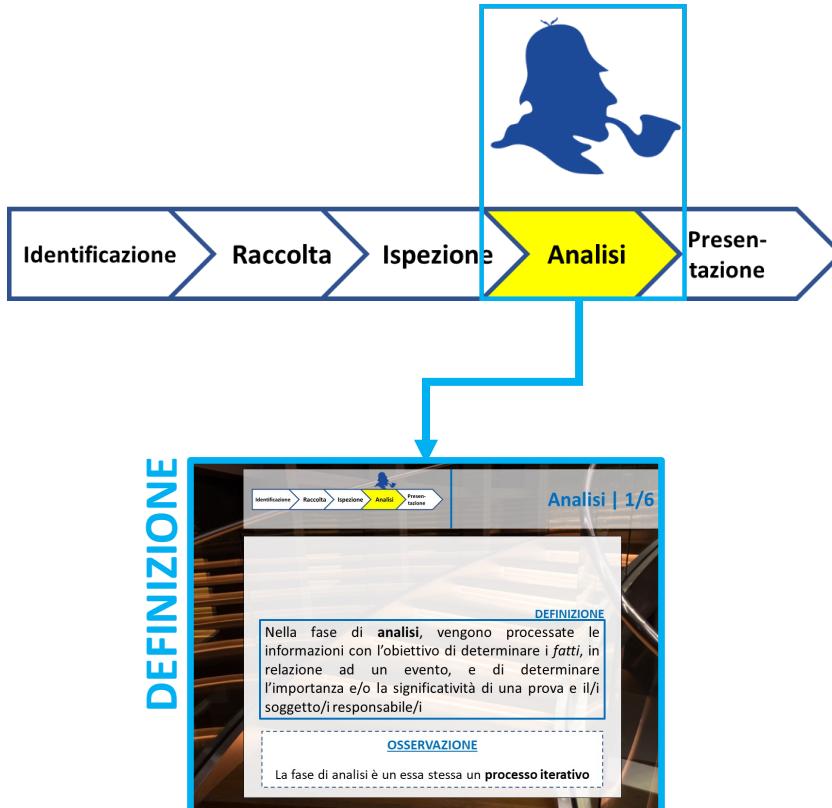
Analisi | Richiami

- Dall'Argomento 1...



Analisi | Richiami

- Dall'Argomento 1...



Analisi | Richiami

- Dall'Argomento 1...

The image shows a computer screen with a presentation slide. At the top, there is a horizontal process flow diagram with five steps: Identificazione, Raccolta, Ispezione, Analisi (which is highlighted in yellow), and Presen-tazione. Below the diagram is a small silhouette of a person. To the right of the diagram, the text "Analisi | 1/6" is displayed. The main content of the slide is contained within a large blue-bordered box. Inside this box, the word "DEFINIZIONE" is at the top, followed by the text: "Nella fase di analisi, vengono processate le informazioni con l'obiettivo di determinare i *fatti*, in relazione ad un evento, e di determinare l'importanza e/o la significatività di una prova e il/i soggetto/i responsabile/i". Below this, another blue-bordered box contains the word "OSSERVAZIONE" at the top, with the text: "La fase di analisi è un essa stessa un **processo iterativo**". The background of the slide features a blurred image of what appears to be a courtroom or a similar setting.

DEFINIZIONE

Nella fase di analisi, vengono processate le informazioni con l'obiettivo di determinare i *fatti*, in relazione ad un evento, e di determinare l'importanza e/o la significatività di una prova e il/i soggetto/i responsabile/i

OSSERVAZIONE

La fase di analisi è un essa stessa un **processo iterativo**

II tool Autopsy

Il tool Autopsy

Caratteristiche | 1/3

- Il tool **Autopsy** permette di effettuare efficientemente l'analisi di dischi fissi, immagini forensi, ecc.



Autopsy® is an easy to use, GUI-based program that allows you to efficiently analyze hard drives and smart phones. It has a plugin architecture that allows you to find add-on modules or develop custom modules in Java or Python.

Fonte: <https://www.sleuthkit.org>

Il tool Autopsy

Caratteristiche | 1/3

- Il tool **Autopsy** permette di effettuare efficientemente l'analisi di dischi fissi, immagini forensi, ecc.
 - Supporta diversi formati di immagini forensi, incluso il formato RAW, il formato EWF ed il formato AFF
 - Presenta una architettura modulare, con possibilità di realizzare plugin e/o moduli personalizzati
 - Fornisce una semplice ed efficace GUI (Graphical User Interface) [Web-based su sistemi basati su Linux]
- Autopsy è Open-Source ed è preinstallato su Kali Linux
 - Sviluppato da Brian Carrier
- Autopsy è disponibile anche per Windows, OS X e Linux
 - Ci soffermeremo sulla versione Linux, ma vedremo anche alcuni aspetti propri della versione per Windows
- Per maggiori dettagli è possibile visitare il seguente link:
 - <https://www.sleuthkit.org/autopsy/>

Il tool Autopsy

Caratteristiche | 2/3

- La maggior parte delle operazioni eseguibili con Autopsy, sono eseguibili anche mediante la suite **The Sleuth Kit (TSK)**, tramite l'interazione con il terminale
 - I tool di tale suite sono utilizzabili esclusivamente tramite terminale (Command Line Interface – CLI)



The Sleuth Kit® is a collection of command line tools and a C library that allows you to analyze disk images and recover files from them. It is used behind the scenes in Autopsy and many other open source and commercial forensics tools.

Fonte: <https://www.sleuthkit.org>

Il tool Autopsy

Caratteristiche | 2/3

- La maggior parte delle operazioni eseguibili con Autopsy, sono eseguibili anche mediante la suite **The Sleuth Kit (TSK)**, tramite l'interazione con il terminale
 - I tool di tale suite sono utilizzabili esclusivamente tramite terminale (Command Line Interface – CLI)
 - Ricordiamo, ad esempio, i tool mmls, fls, ils, blkls, jls
- La suite TSK è Open-Source ed è anch'essa preinstallata su Kali Linux
 - Sviluppata anch'essa da Brian Carrier
- Fondamentalmente, Autopsy è una sorta di GUI, per i tool forniti dalla suite TSK

Il tool Autopsy

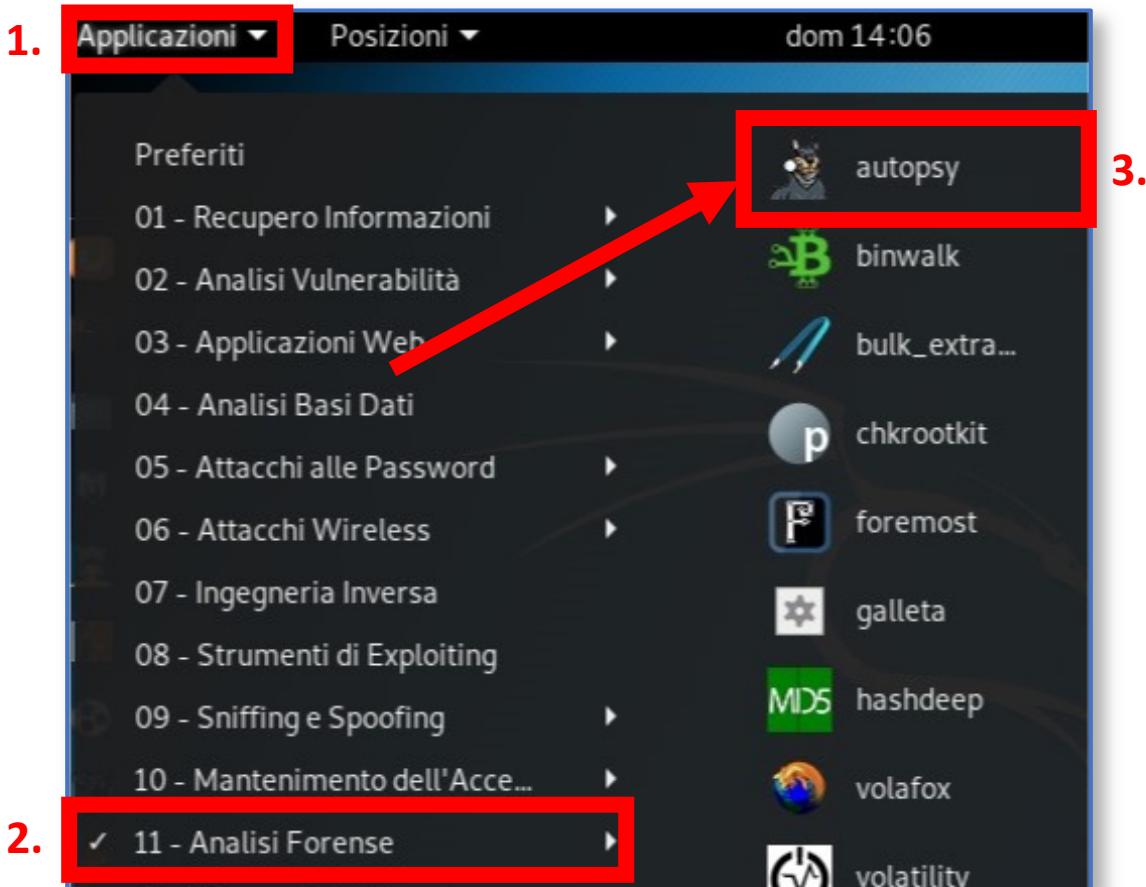
Caratteristiche | 3/3

- In Kali Linux, il tool Autopsy permette di svolgere diverse attività, fra le quali:
 - Analisi di immagini forensi
 - Permette l'analisi di una immagine forense, mostrandone informazioni su file e/o directory
 - Timeline in merito alle attività sui file
 - Permette la realizzazione di una timeline, in base ai timestamp dei file (data/ora di creazione/accesso/modifica)
 - Verifica dell'integrità di immagini forensi
 - Calcola l'hash MD5 di immagini forensi e/o di file/directory specifici
 - Ricerca mediante keyword
 - Permette di ricercare dati/informazioni mediante delle keyword e/o espressioni regolari
 - Analisi dei file e analisi di metadati
 - Permette di visualizzare i dettagli relativi ai metadati e permette l'analisi di specifici file/directory

Il tool Autopsy

Avvio del Tool | 1/4

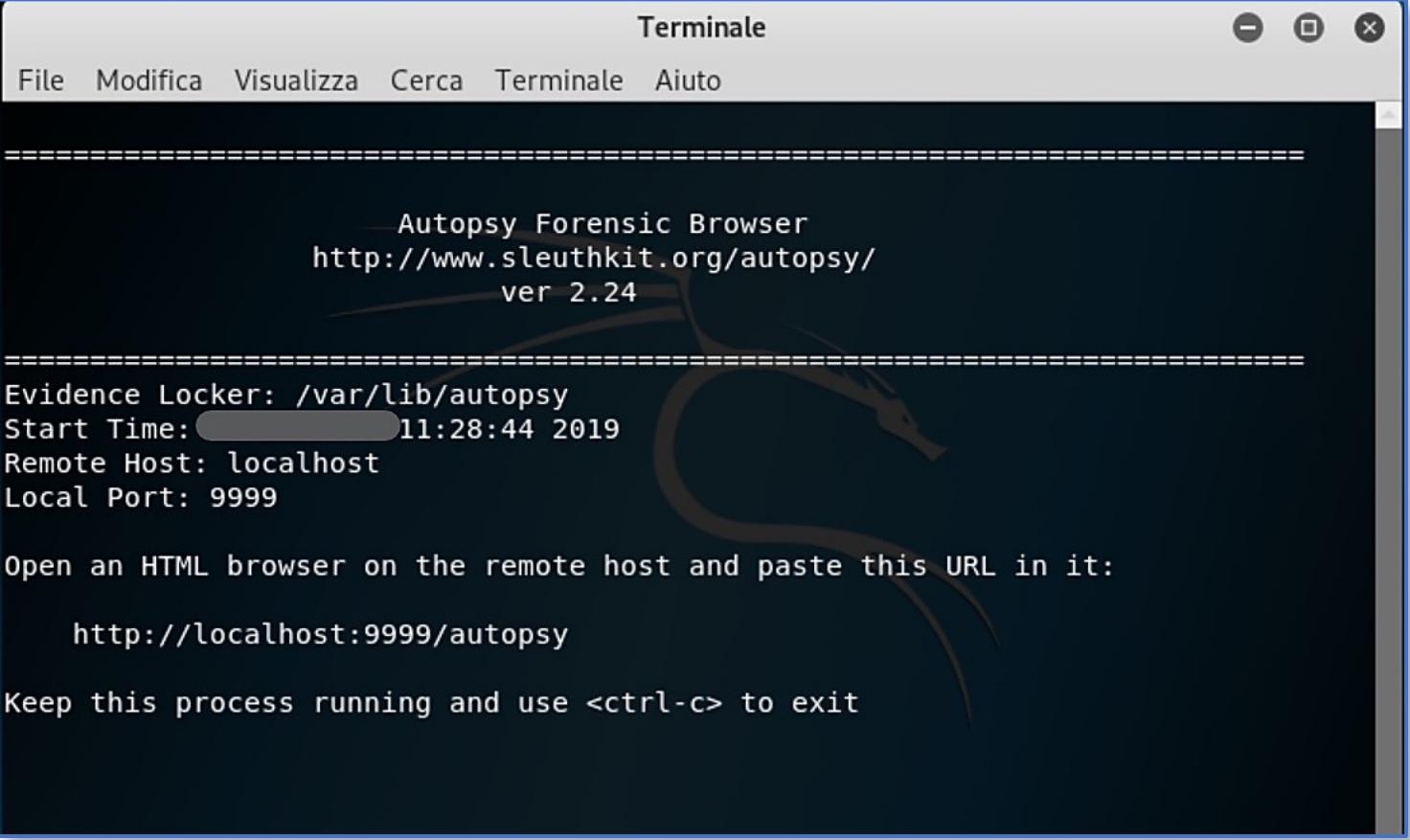
- Avvio tramite Interfaccia Grafica



Il tool Autopsy

Avvio del Tool | 2/4

- *Avvio tramite Interfaccia Grafica*



The screenshot shows a terminal window titled "Terminale". The window has a standard title bar with icons for minimize, maximize, and close. Below the title bar is a menu bar with options: File, Modifica, Visualizza, Cerca, Terminale, and Aiuto. The main area of the terminal displays the following text:

```
=====
Autopsy Forensic Browser
http://www.sleuthkit.org/autopsy/
ver 2.24
=====
Evidence Locker: /var/lib/autopsy
Start Time: [REDACTED] 11:28:44 2019
Remote Host: localhost
Local Port: 9999

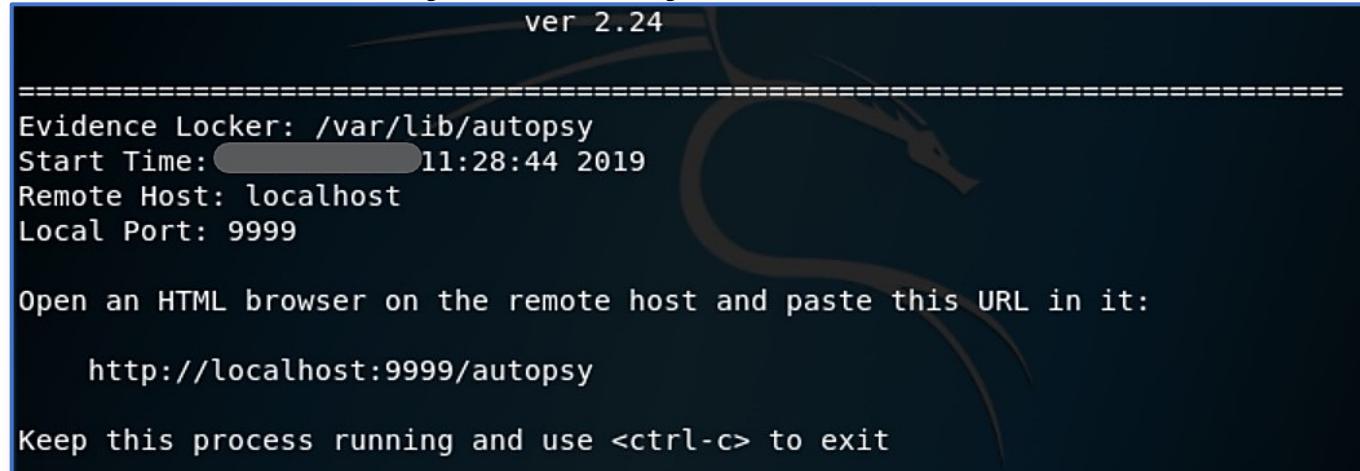
Open an HTML browser on the remote host and paste this URL in it:
http://localhost:9999/autopsy

Keep this process running and use <ctrl-c> to exit
```

Il tool Autopsy

Avvio del Tool | 3/4

- *Avvio tramite Interfaccia Grafica*



ver 2.24

=====
Evidence Locker: /var/lib/autopsy
Start Time: [REDACTED] 11:28:44 2019
Remote Host: localhost
Local Port: 9999

Open an HTML browser on the remote host and paste this URL in it:
<http://localhost:9999/autopsy>

Keep this process running and use <ctrl-c> to exit

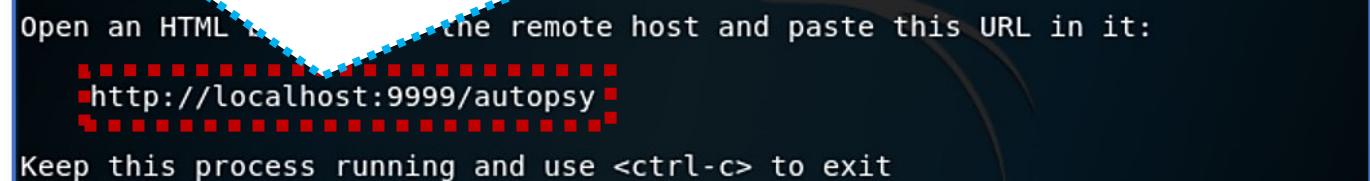
- All'avvio di Autopsy, si avvierà il terminale di Kali Linux e verranno specificate le seguenti informazioni:
 - La versione (nell'esempio, 2.24)
 - Il percorso dell'Evidence Locker (nell'esempio, /var/lib/autopsy)
 - *Maggiori dettagli in seguito*
 - L'URL e i dettagli di connessione per aprire la pagina web, denominata **Autopsy Forensic Browser**
 - **NOTA:** Il tool Autopsy rimarrà attivo, finché non verrà chiusa la finestra

Il tool Autopsy

Avvio del Tool | 3/4

Cliccando con il tasto destro sull'URL:

<http://localhost:9999/autopsy>, e cliccando su «Apri Collegamento», si aprirà la pagina **Autopsy Forensic Browser**



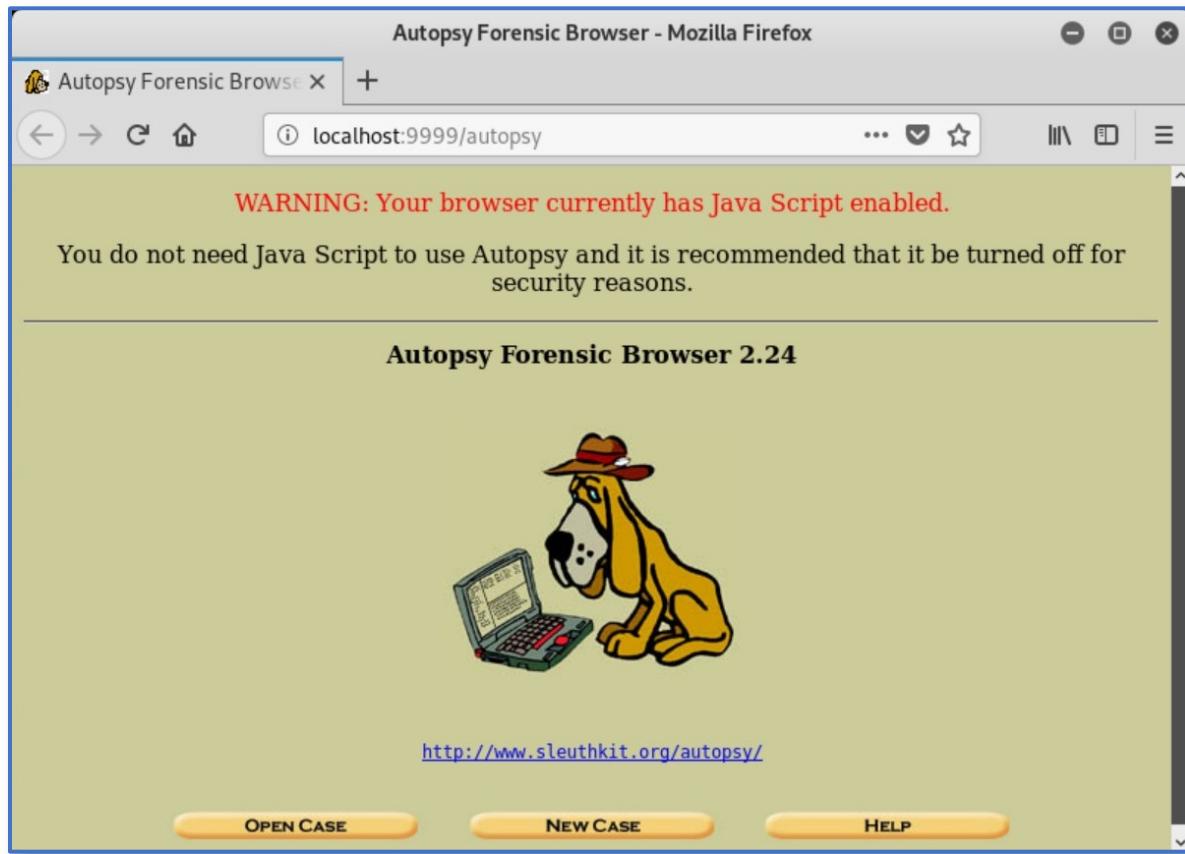
Open an HTML browser on the remote host and paste this URL in it:
http://localhost:9999/autopsy
Keep this process running and use <ctrl-c> to exit

- All'avvio di Autopsy, si avvierà il terminale di Kali Linux e verranno specificate le seguenti informazioni:
 - La versione (nell'esempio, 2.24)
 - Il percorso dell'Evidence Locker (nell'esempio, /var/lib/autopsy)
 - *Maggiori dettagli in seguito*
 - L'URL e i dettagli di connessione per aprire la pagina web, denominata **Autopsy Forensic Browser**
- **NOTA:** Il tool Autopsy rimarrà attivo, finché non verrà chiusa la finestra

Il tool Autopsy

Avvio del Tool | 4/4

- *Avvio tramite Interfaccia Grafica*
 - Pagina Web: **Autopsy Forensic Browser**



Il tool Autopsy

Approfondimenti

Creazione di un Nuovo Caso

Analisi mediante Autopsy

Riapertura di un Caso

Il tool Autopsy

Approfondimenti

Creazione di un Nuovo Caso

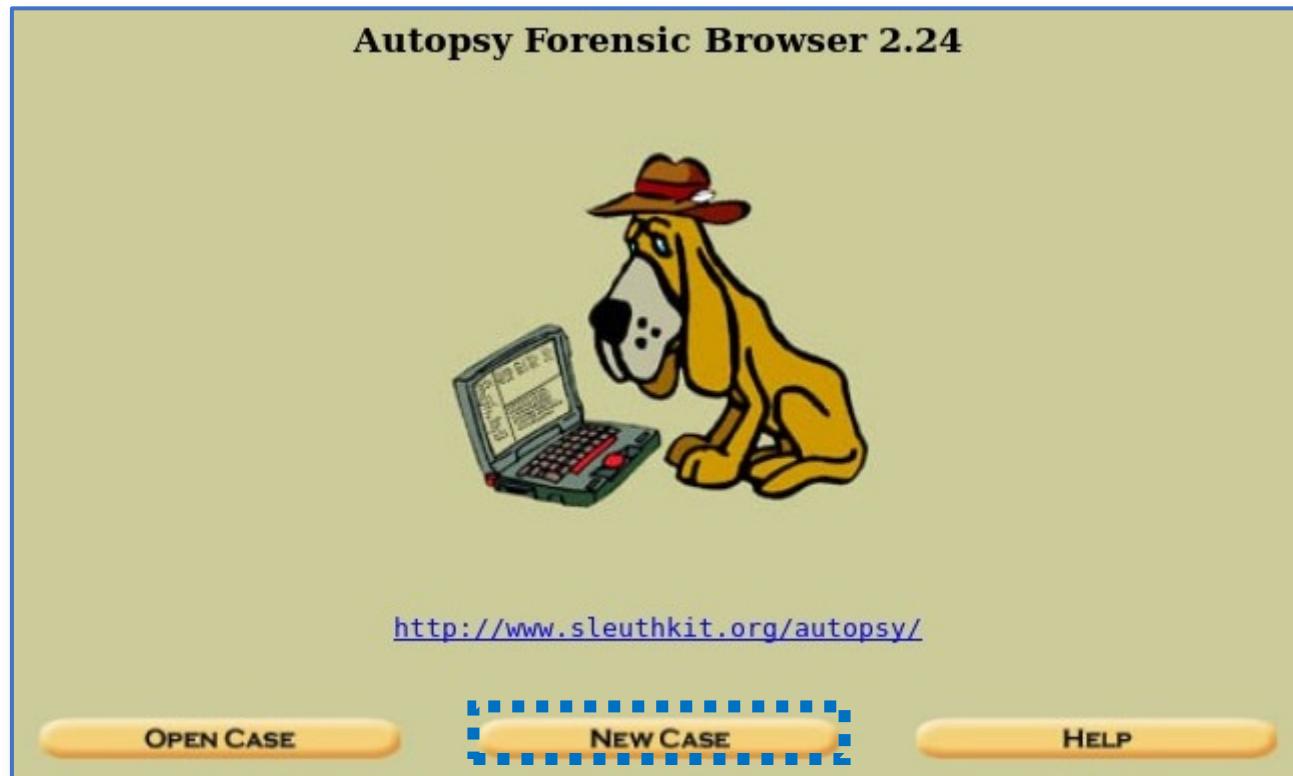
Analisi mediante Autopsy

Riapertura di un Caso

Il tool Autopsy

Creazione di un Nuovo Caso | 1/18

1. Cliccare sul bottone «New Case»



Il tool Autopsy

Creazione di un Nuovo Caso | 2/18

2. Inserire le informazioni riguardanti il **nome del caso (Case Name)**, la descrizione (**Description**), il **nome degli investigatori (Investigator Names)**, ecc.

CREATE A NEW CASE

1. **Case Name:** The name of this investigation. It can contain only letters, numbers, and symbols.

2. **Description:** An optional, one line description of this case.

3. **Investigator Names:** The optional names (with no spaces) of the investigators for this case.

a. <input type="text"/>	b. <input type="text"/>
c. <input type="text"/>	d. <input type="text"/>
e. <input type="text"/>	f. <input type="text"/>
g. <input type="text"/>	h. <input type="text"/>
i. <input type="text"/>	j. <input type="text"/>

NEW CASE **CANCEL** **HELP**

Il tool Autopsy

Creazione di un Nuovo Caso | 3/18

- Dopo aver compilato i vari campi (come nell'esempio), è necessario fare click su «New Case»

CREATE A NEW CASE

1. **Case Name:** The name of this investigation. It can contain only letters, numbers, and symbols.

Primo

2. **Description:** An optional, one line description of this case.

Primo Caso

3. **Investigator Names:** The optional names (with no spaces) of the investigators for this case.

a.	Raffaele Pizzolante	b.	
c.		d.	
e.		f.	
g.		h.	
i.		j.	

NEW CASE **CANCEL** **HELP**

Il tool Autopsy

Creazione di un Nuovo Caso | 4/18

Ci viene indicato che il caso **Primo** è stato creato e le relative informazioni sono memorizzate nella cartella /var/lib/autopsy/Primo

- **NOTA:** la cartella /var/lib/autopsy è la cartella denotata Evidence Locker, specificata all'avvio del tool, ed è la cartella in cui vengono memorizzate tutte le informazioni dei vari casi, registrati da Autopsy

Creating Case: Primo

Case directory (/var/lib/autopsy/Primo/) created
Configuration file (/var/lib/autopsy/Primo/case.aut) created

We must now create a host for this case.

ADD HOST

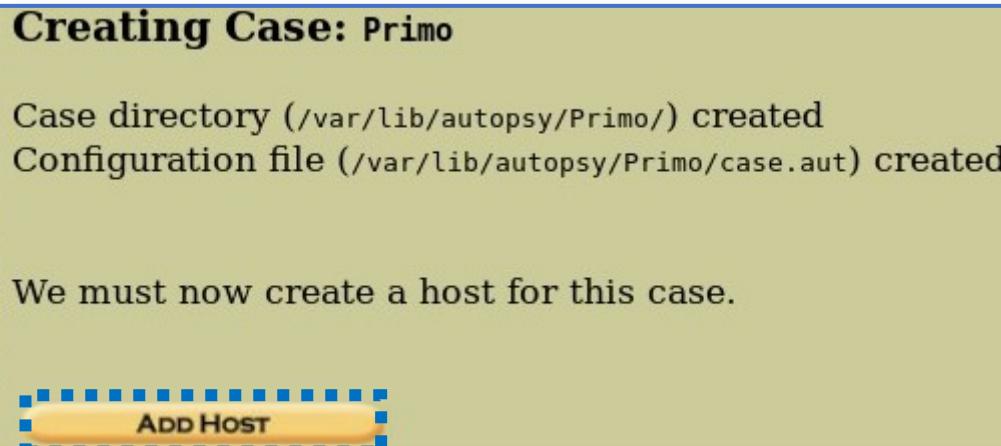
Il tool Autopsy

Creazione di un Nuovo Caso | 4/18

Ci viene indicato che il caso **Primo** è stato creato e le relative informazioni sono memorizzate nella cartella /var/lib/autopsy/Primo

- **NOTA:** la cartella /var/lib/autopsy è la cartella denotata Evidence Locker, specificata all'avvio del tool, ed è la cartella in cui vengono memorizzate tutte le informazioni dei vari casi, registrati da Autopsy

Cliccare su «Add Host» per proseguire



Il tool Autopsy

Creazione di un Nuovo Caso | 5/18

4. Inserire i dettagli relativi al **nome del computer su cui si sta investigando (Host Name)** e la relativa **descrizione (Description)**

Case: Primo

ADD A NEW HOST

1. **Host Name:** The name of the computer being investigated. It can contain only letters, numbers, and symbols.

2. **Description:** An optional one-line description or note about this computer.

Il tool Autopsy

Creazione di un Nuovo Caso | 6/18

5. È inoltre possibile aggiungere opzionalmente ulteriori dettagli dell'host, fra cui:
 - **Fuso orario (Time zone)**
 - È possibile opzionalmente specificare il fuso orario (se non viene specificato niente, si utilizza il fuso orario del Sistema Operativo)

3. **Time zone:** An optional timezone value (i.e. EST5EDT). If not given, it defaults to the local setting. A list of time zones can be found in the help files.

4. **Timeskew Adjustment:** An optional value to describe how many seconds this computer's clock was out of sync. For example, if the computer was 10 seconds fast, then enter -10 to compensate.

Il tool Autopsy

Creazione di un Nuovo Caso | 7/18

6. Cliccare sul tasto «Add Host» per proseguire
7. Verrà mostrata la conferma che l'host (nell'esempio, host1) è stato **aggiunto correttamente** e verranno indicate le informazioni relative alle directory, in cui è avvenuta la memorizzazione delle informazioni



Il tool Autopsy

Creazione di un Nuovo Caso | 7/18

6. Cliccare sul tasto «**Add Host**» per proseguire
7. Verrà mostrata la conferma che l'host (nell'esempio, host1) è stato **aggiunto correttamente** e verranno indicate le informazioni relative alle directory, in cui è avvenuta la memorizzazione delle informazioni



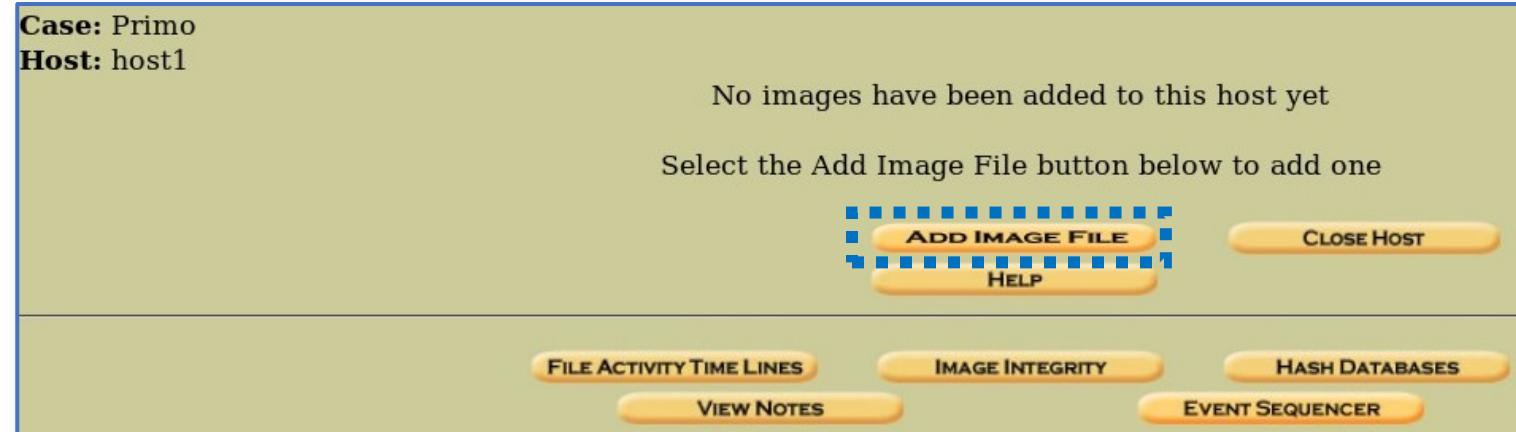
Cliccare quindi su «**Add Image**» per proseguire



Il tool Autopsy

Creazione di un Nuovo Caso | 8/18

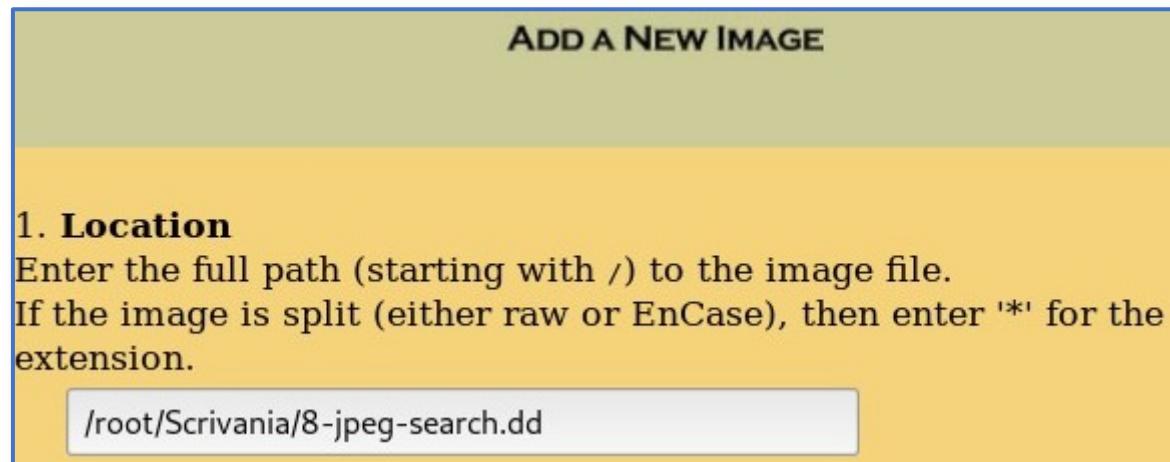
8. Cliccare sul tasto «Add Image File» per aggiungere una immagine forense



Il tool Autopsy

Creazione di un Nuovo Caso | 9/18

9. Specificare, in primo luogo, la **posizione (location)** dove è memorizzata l'immagine forense (nell'esempio, /host/Scrivania/8-jpeg-search.dd)



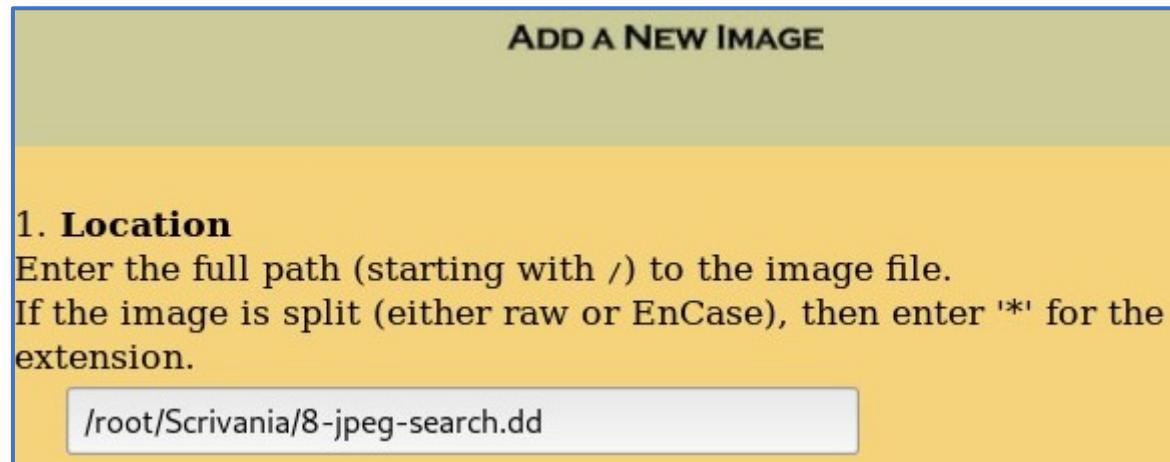
NOTA: L'immagine 8-jpeg-search.dd è gratuitamente scaricabile (in formato ZIP, peso circa 2MB) al seguente link:
<http://dftt.sourceforge.net/test8/index.html>

Tale immagine contiene diversi file JPG, ai quali è stata modificata l'estensione e/o sono stati nascosti in altri file

Il tool Autopsy

Creazione di un Nuovo Caso | 10/18

9. Specificare, in primo luogo, la **posizione (location)** dove è memorizzata l'immagine forense (nell'esempio, /host/Scrivania/8-jpeg-search.dd)



Viene poi richiesto se l'immagine è relativa ad un **intero disco fisico (Disk)**, oppure, è relativa ad una **singola partizione (Partition)**, come nell'esempio



Il tool Autopsy

Creazione di un Nuovo Caso | 11/18

Infine, viene richiesto di specificare il **metodo di importazione** (**Import Method**), in virtù del fatto che l'immagine necessariamente acceduta dalla cartella Evidence Locker

3. Import Method

To analyze the image file, it must be located in the evidence locker. It can be imported from its current location using a symbolic link, by copying it, or by moving it. Note that if a system failure occurs during the move, then the image could become corrupt.

Symlink

Copy

Move

Le possibilità sono le seguenti:

- La creazione di un collegamento (*link*) simbolico (opzione **Simlink**) all'immagine specificata, all'interno della cartella Evidence Locker
- La creazione di una copia (opzione **Copy**), dell'immagine specificata, all'interno cartella Evidence Locker
- Lo spostamento dell'immagine all'interno della cartella Evidence Locker (opzione **Move**)

Il tool Autopsy

Creazione di un Nuovo Caso | 12/18

3. Import Method

To analyze the image file, it must be located in the evidence locker. It can be imported from its current location using a symbolic link, by copying it, or by moving it. Note that if a system failure occurs during the move, then the image could become corrupt.



Symlink

Copy

Move

Nell'esempio, è stata selezionata l'opzione **Symlink**, come è possibile vedere dall'immagine

Il tool Autopsy

Creazione di un Nuovo Caso | 12/18

3. Import Method

To analyze the image file, it must be located in the evidence locker. It can be imported from its current location using a symbolic link, by copying it, or by moving it. Note that if a system failure occurs during the move, then the image could become corrupt.



Symlink

Copy

Move

Nell'esempio, è stata selezionata l'opzione **Symlink**, come è possibile vedere dall'immagine

MOTIVAZIONE: È stata selezionata l'opzione **Symlink (Symbolic Link)**, poiché con un collegamento simbolico si evitano i rischi legati alla copia e spostamento (ad esempio, copia corrotta, ecc.)

Il tool Autopsy

Creazione di un Nuovo Caso | 12/18

3. Import Method

To analyze the image file, it must be located in the evidence locker. It can be imported from its current location using a symbolic link, by copying it, or by moving it. Note that if a system failure occurs during the move, then the image could become corrupt.



Symlink

Copy

Move

Nell'esempio, è stata selezionata l'opzione **Symlink**, come è possibile vedere dall'immagine

MOTIVAZIONE: È stata selezionata l'opzione **Symlink (Symbolic Link)**, poiché con un collegamento simbolico si evitano i rischi legati alla copia e spostamento (ad esempio, copia corrotta, ecc.)

10. Cliccare sul tasto «**Next**» per proseguire



Il tool Autopsy

Creazione di un Nuovo Caso | 13/18

11. Verranno mostrati diversi dettagli dell'immagine importata

Image File Details

Local Name: images/8-jpeg-search.dd

Data Integrity: An MD5 hash can be used to verify the integrity of the image. (With split images, this hash is for the full image file)

Ignore the hash value for this image.

Calculate the hash value for this image.

Add the following MD5 hash value for this image:

Verify hash after importing?

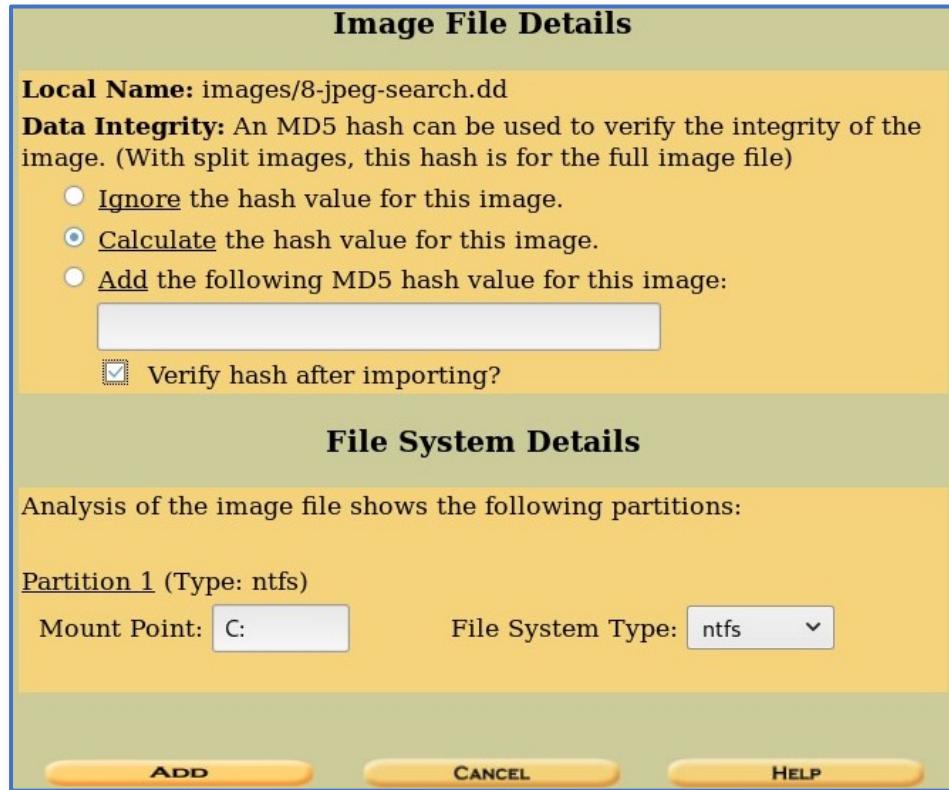
File System Details

Analysis of the image file shows the following partitions:

Partition 1 (Type: ntfs)

Mount Point: File System Type:

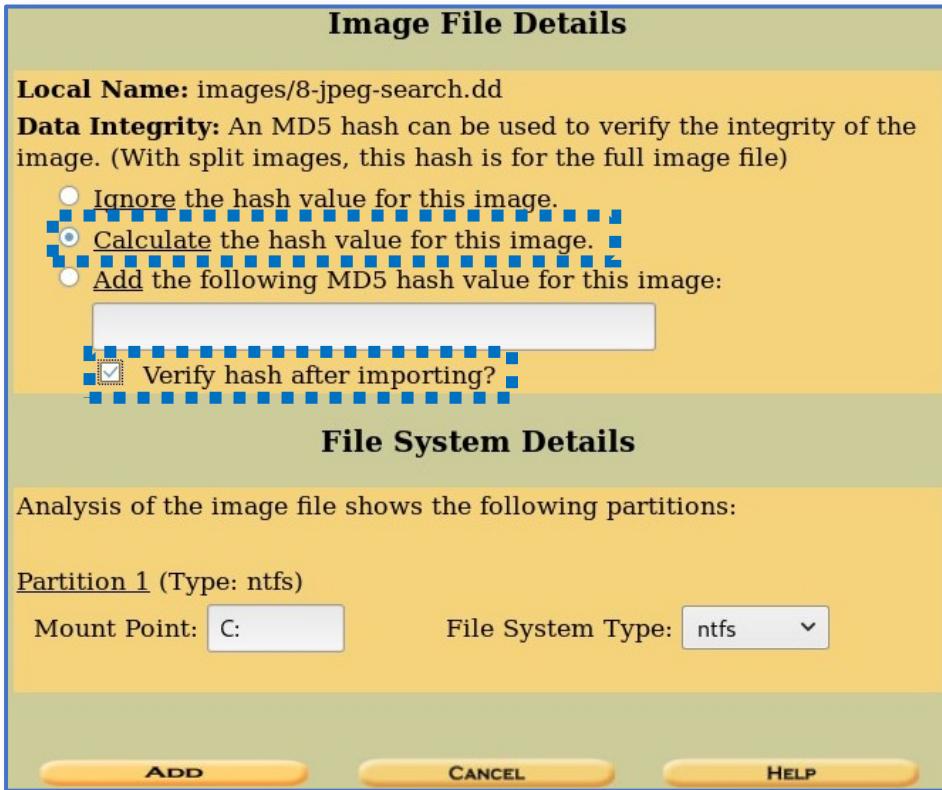
ADD **CANCEL** **HELP**



Il tool Autopsy

Creazione di un Nuovo Caso | 13/18

11. Verranno mostrati diversi dettagli dell'immagine importata

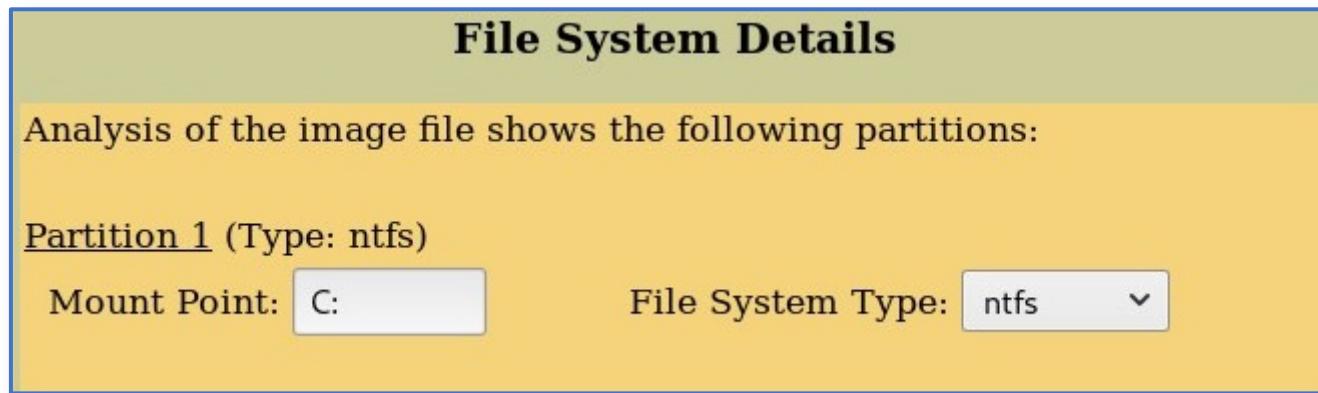


Selezioniamo la checkbox «**Calculate**» e spuntiamo la checkbox «**Verify hash after importing?**», per verificare l'integrità dell'immagine importata

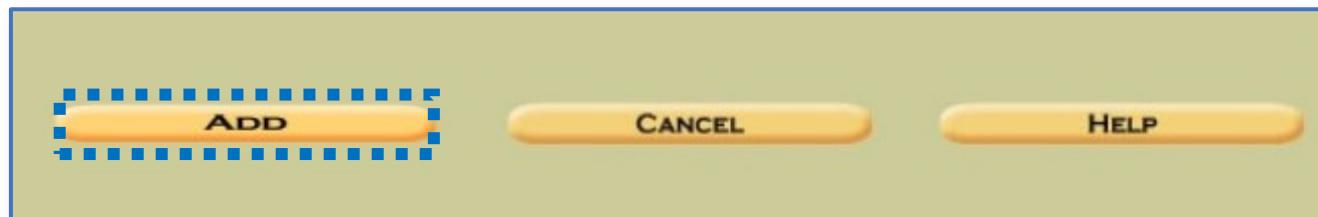
Il tool Autopsy

Creazione di un Nuovo Caso | 14/18

12. Come ulteriori informazioni, è possibile osservare come venga indicato che il **file system** dell'immagine è di tipo **NTFS**



13. Cliccare su «Add» per proseguire



Il tool Autopsy

Creazione di un Nuovo Caso | 15/18

14. Dopo aver cliccato «Add», al passo precedente, viene riportato il valore dell'hash MD5 ed il link simbolico creato, nella cartella Evidence Locker

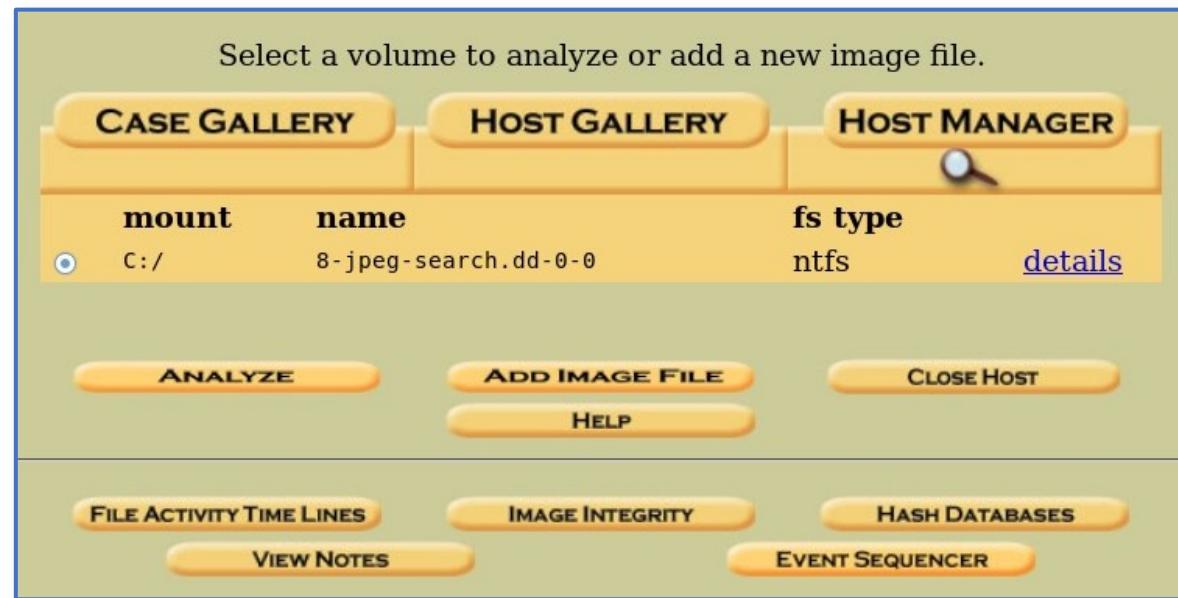


Possiamo quindi cliccare il tasto «OK», per proseguire; eventualmente, è anche possibile inserire una ulteriore immagine (cliccando il tasto «Add Image»)

Il tool Autopsy

Creazione di un Nuovo Caso | 16/18

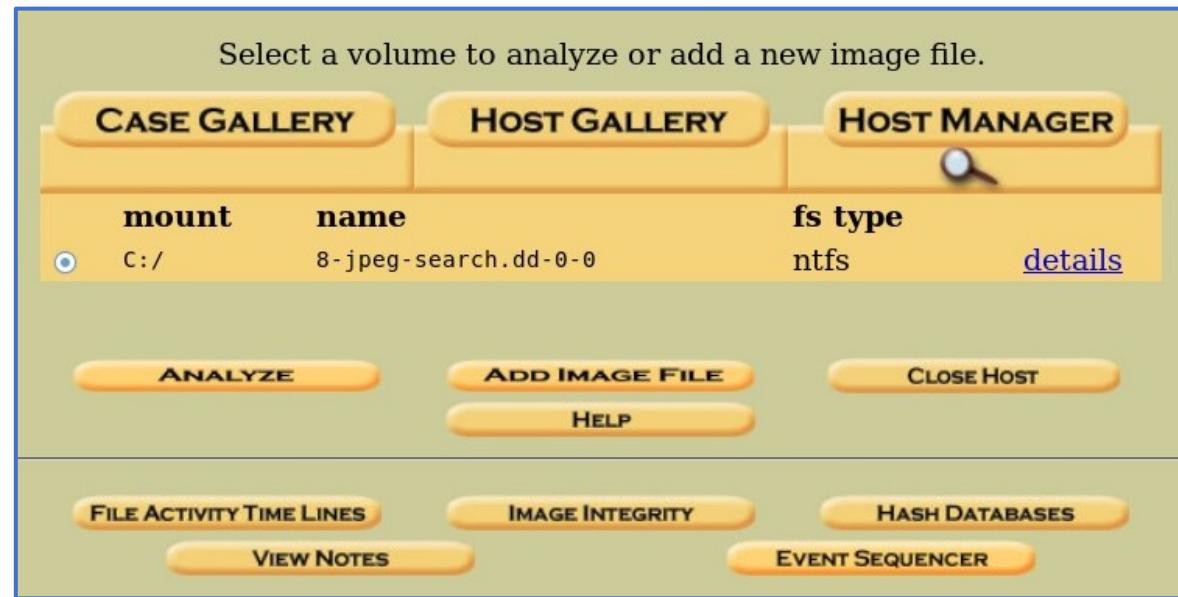
15. A questo punto, è possibile avviare il **processo di analisi** dell'immagine importata



Il tool Autopsy

Creazione di un Nuovo Caso | 16/18

15. A questo punto, è possibile avviare il **processo di analisi** dell'immagine importata



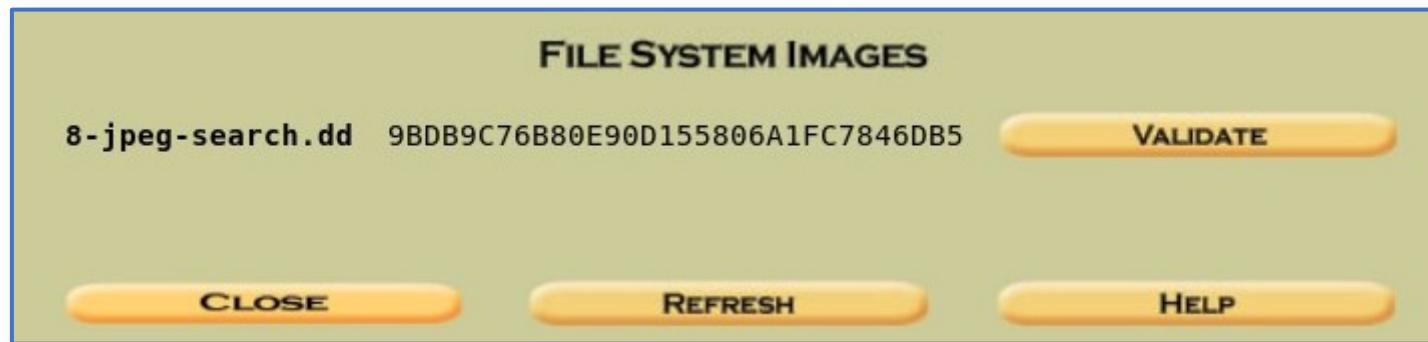
16. È preferibile però effettuare prima una verifica dell'integrità dell'immagine importata, cliccando sul tasto «**Image Integrity**»



Il tool Autopsy

Creazione di un Nuovo Caso | 17/18

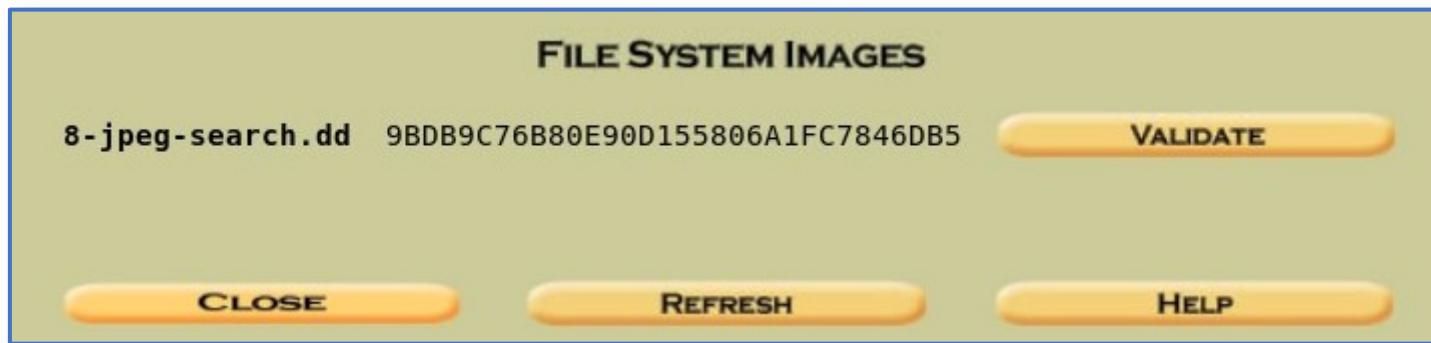
16. Viene poi mostrato il **nome dell'immagine** (8-jpeg-search.dd) e l'hash MD5



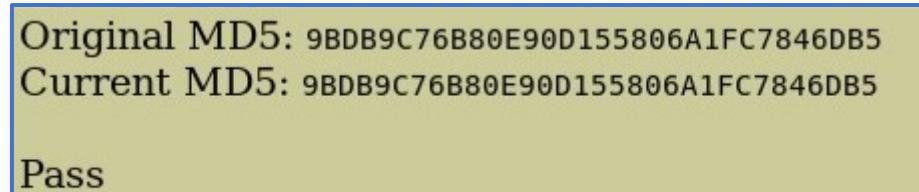
Il tool Autopsy

Creazione di un Nuovo Caso | 17/18

16. Viene poi mostrato il **nome dell'immagine** (8-jpeg-search.dd) e l'hash MD5



17. Cliccando su «Validate», è possibile visualizzare il risultato della validazione

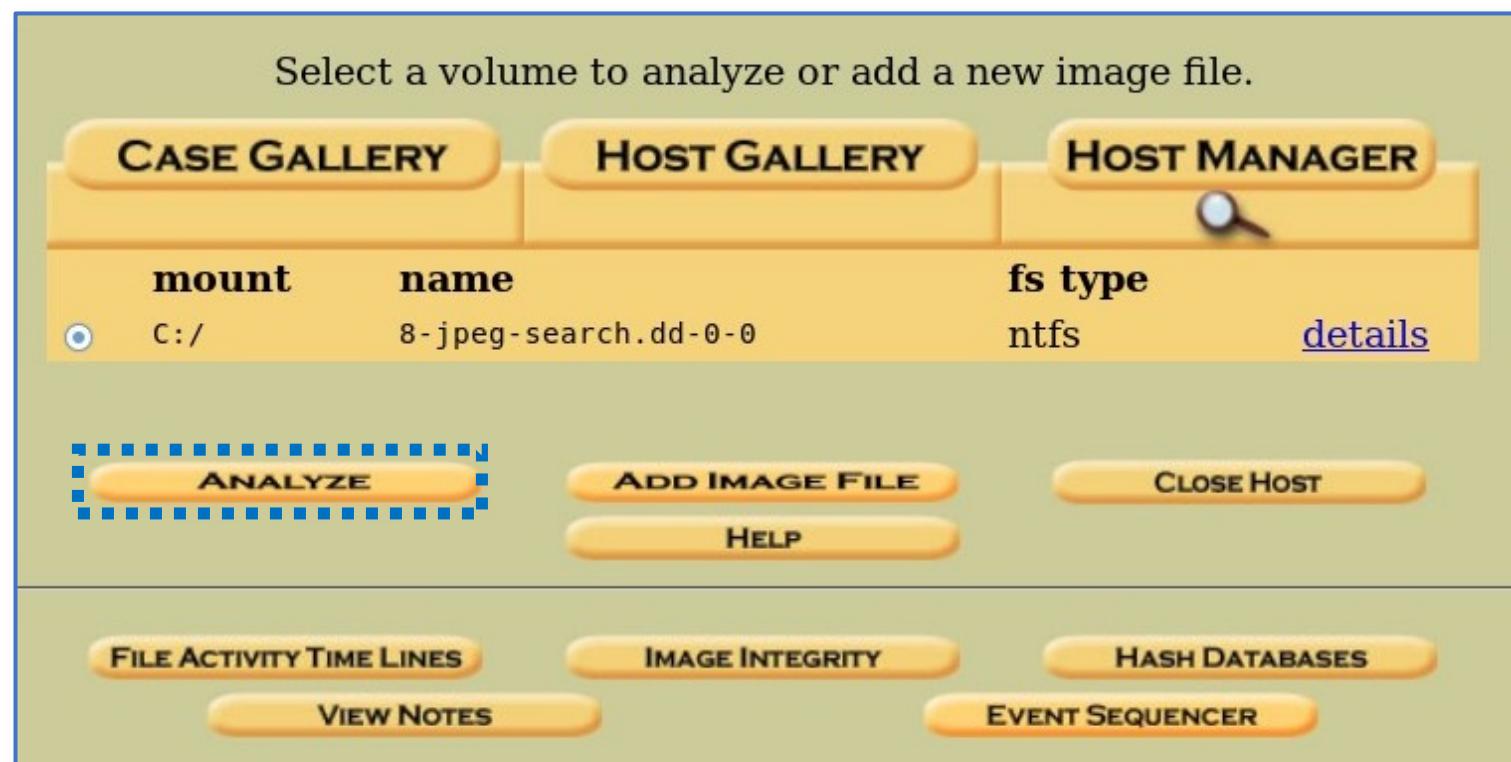


Clicchiamo su «Close», per ritornare al **menu precedente**

Il tool Autopsy

Creazione di un Nuovo Caso | 18/18

18. È ora possibile cliccare sul tasto «Analyze» per iniziare il processo di analisi



Il tool Autopsy

Approfondimenti

Creazione di un Nuovo Caso

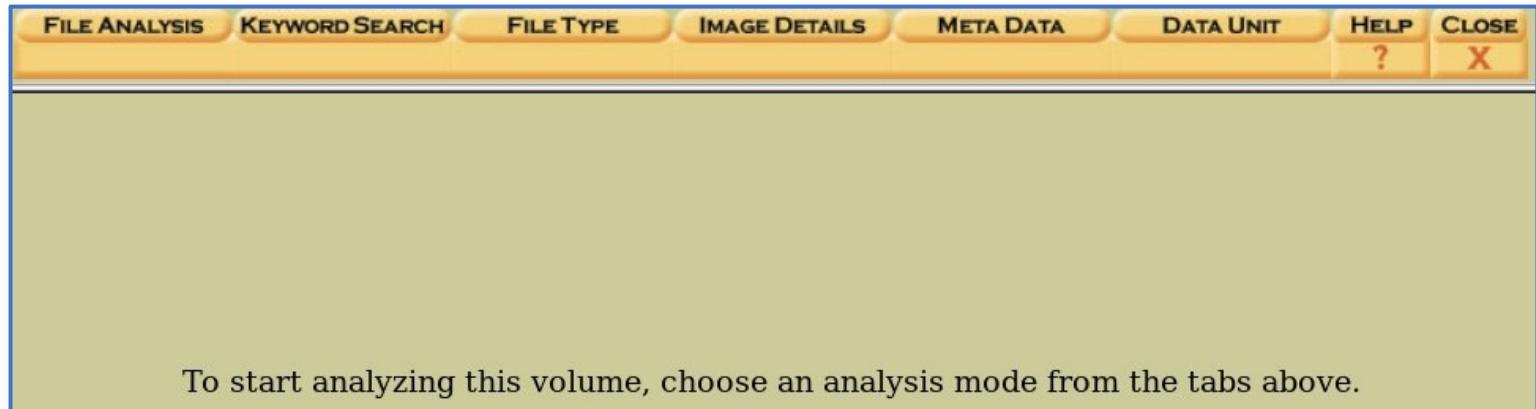
Analisi mediante Autopsy

Riapertura di un Caso

Il tool Autopsy

Analisi mediante Autopsy | 1/27

- Dopo aver creato il caso, aggiunto l'host (o gli host) e l'immagine (o le immagini), nella fase di analisi, il tool Autopsy, presenterà una schermata simile alla seguente:



Il tool Autopsy

Analisi mediante Autopsy | 1/27

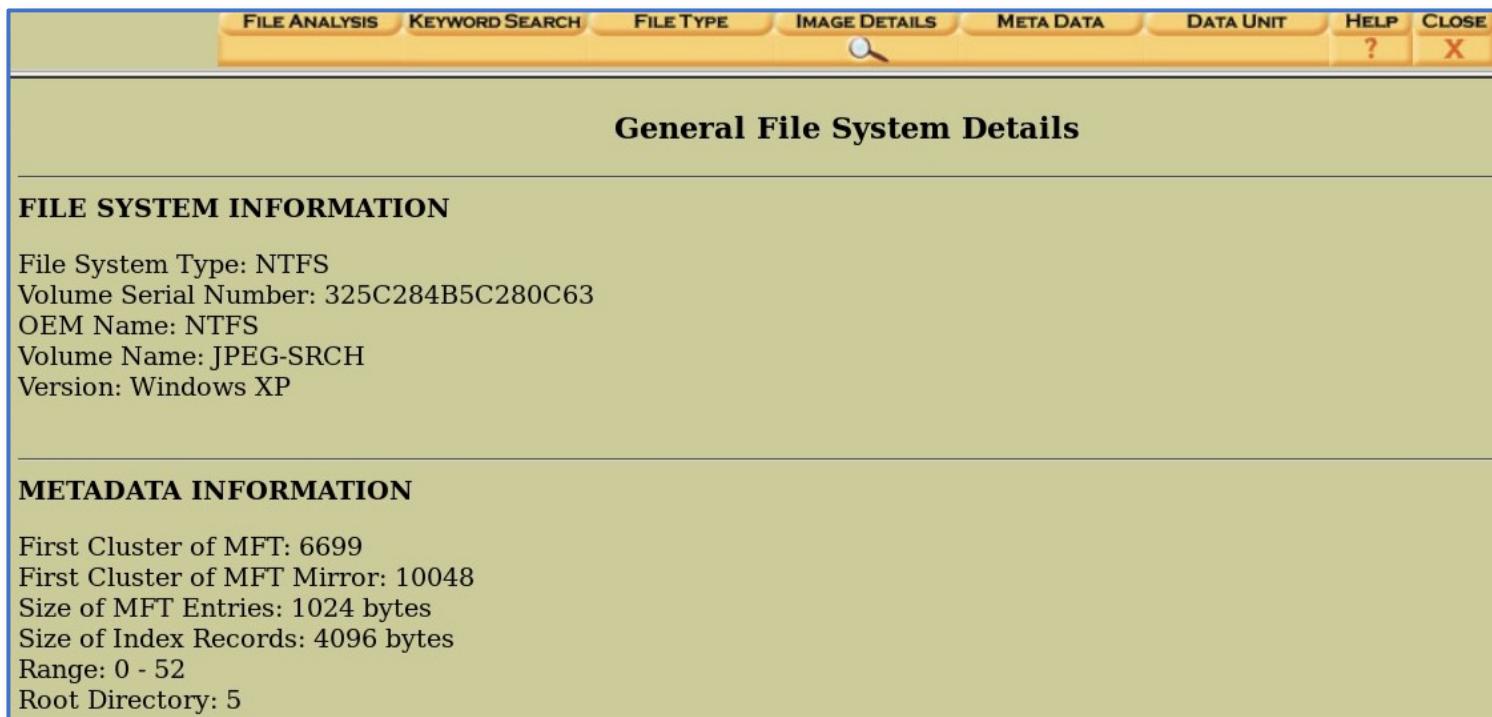
- Per avere informazioni dettagliate in relazione all'immagine importata, è possibile cliccare su «**Image Details**»



Il tool Autopsy

Analisi mediante Autopsy | 2/27

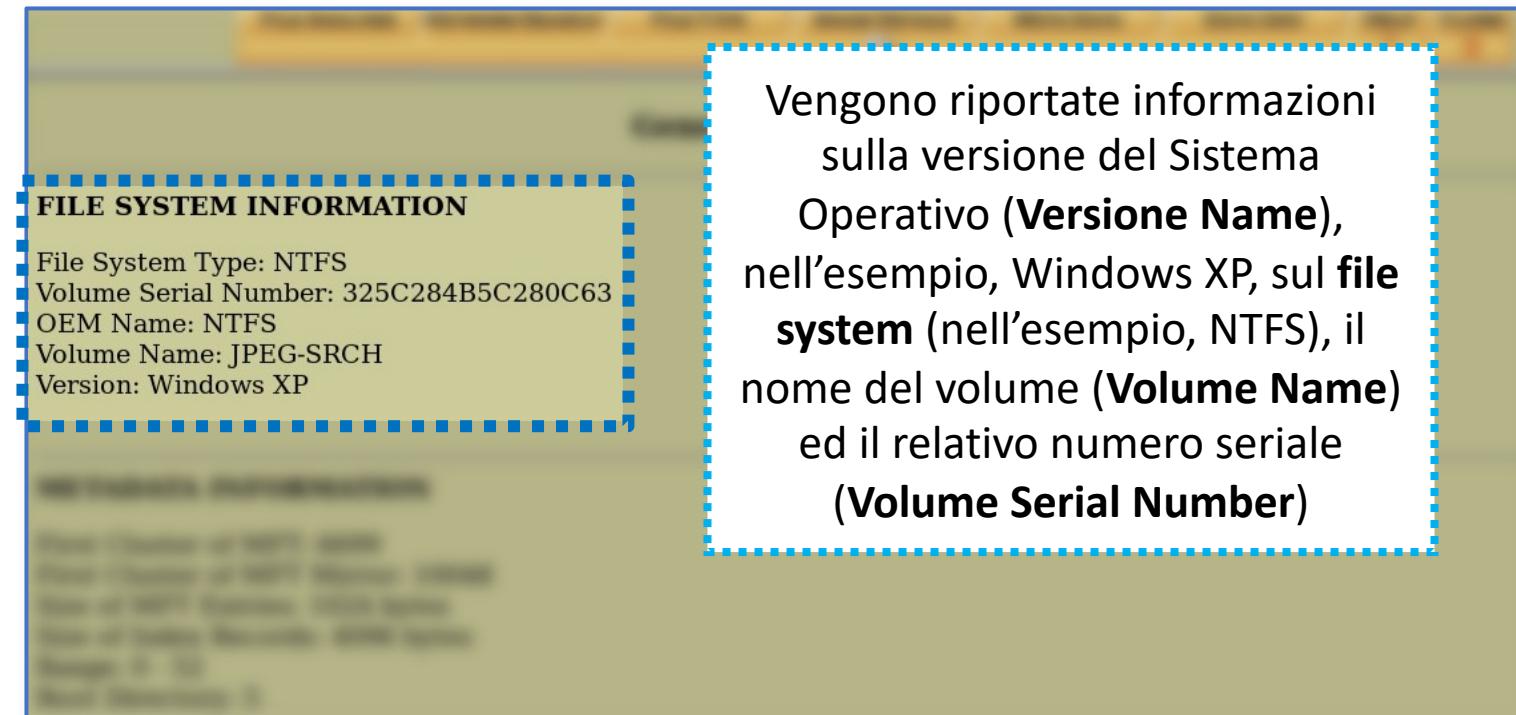
- *Informazioni dettagliate sull'immagine importata | 1/2*



Il tool Autopsy

Analisi mediante Autopsy | 2/27

- *Informazioni dettagliate sull'immagine importata | 1/2*



Il tool Autopsy

Analisi mediante Autopsy | 3/27

- *Informazioni dettagliate sull'immagine importata | 2/2*

The screenshot shows the Autopsy software interface with the following details:

METADATA INFORMATION

- First Cluster of MFT: 6699
- First Cluster of MFT Mirror: 10048
- Size of MFT Entries: 1024 bytes
- Size of Index Records: 4096 bytes
- Range: 0 - 52
- Root Directory: 5

CONTENT INFORMATION

- Sector Size: 512
- Cluster Size: 512
- Total Cluster Range: 0 - 20095
- Total Sector Range: 0 - 20095

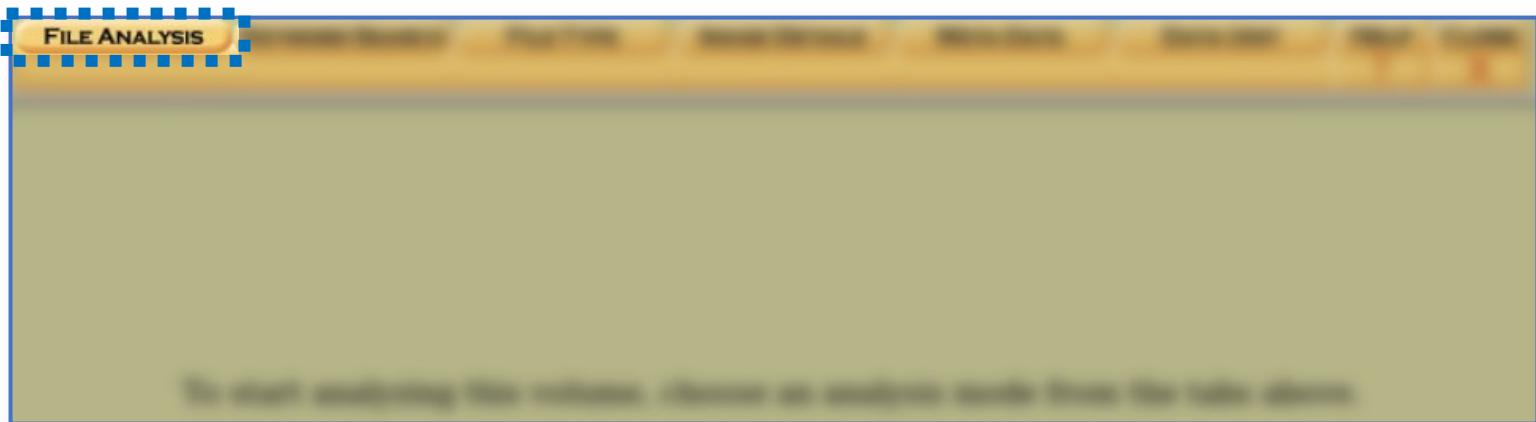
\$AttrDef Attribute Values:

- \$STANDARD_INFORMATION (16) Size: 48-72 Flags: Resident
- \$ATTRIBUTE_LIST (32) Size: No Limit Flags: Non-resident
- \$FILE_NAME (48) Size: 68-578 Flags: Resident,Index
- \$OBJECT_ID (64) Size: 0-256 Flags: Resident
- \$SECURITY_DESCRIPTOR (80) Size: No Limit Flags: Non-resident
- \$VOLUME_NAME (96) Size: 2-256 Flags: Resident
- \$VOLUME_INFORMATION (112) Size: 12-12 Flags: Resident
- \$DATA (128) Size: No Limit Flags:
- \$INDEX_ROOT (144) Size: No Limit Flags: Resident
- \$INDEX_ALLOCATION (160) Size: No Limit Flags: Non-resident
- \$BITMAP (176) Size: No Limit Flags: Non-resident
- \$REPARSE_POINT (192) Size: 0-16384 Flags: Non-resident
- \$EA_INFORMATION (208) Size: 8-8 Flags: Resident
- \$EA (224) Size: 0-65536 Flags:
- \$LOGGED.Utility STREAM (256) Size: 0-65536 Flags: Non-resident

Il tool Autopsy

Analisi mediante Autopsy | 4/27

- Cliccando su «**File Analysis**», si accederà ad una nuova schermata che permetterà di effettuare diverse opzioni in merito ai file



Il tool Autopsy

Analisi mediante Autopsy | 5/27

- Vengono mostrati tutti i file e le directory, contenuti nella **Current Directory** (nell'esempio, è C:\)

The screenshot shows the Autopsy interface in 'File Analysis' mode. The left sidebar has sections for 'Directory Seek' (with input field 'C:\') and 'File Name Search' (with input field). The main area displays a table of files from the current directory:

DEL	Type	NAME	WRITTEN	ACCESSED	CHANGED	CREATED	SIZE	UID	GID	META
	r / r	\$AttrDef	2004-06-10 05:22:22 (CEST)	2004-06-10 05:22:22 (CEST)	2004-06-10 05:22:22 (CEST)	2004-06-10 05:22:22 (CEST)	2560	48	0	4-128-4
	r / r	\$BadClus	2004-06-10 05:22:22 (CEST)	2004-06-10 05:22:22 (CEST)	2004-06-10 05:22:22 (CEST)	2004-06-10 05:22:22 (CEST)	0	0	0	8-128-2
	r / r	\$BadClus:\$Bad	2004-06-10 05:22:22 (CEST)	2004-06-10 05:22:22 (CEST)	2004-06-10 05:22:22 (CEST)	2004-06-10 05:22:22 (CEST)	10289152	0	0	8-128-1
	r / r	\$Bitmap	2004-06-10 05:22:22 (CEST)	2004-06-10 05:22:22 (CEST)	2004-06-10 05:22:22 (CEST)	2004-06-10 05:22:22 (CEST)	2512	0	0	6-128-1
	r / r	\$Boot	2004-06-10 05:22:22 (CEST)	2004-06-10 05:22:22 (CEST)	2004-06-10 05:22:22 (CEST)	2004-06-10 05:22:22 (CEST)	8192	48	0	7-128-1
	d / d	\$Extend/	2004-06-10	2004-06-10	2004-06-10	2004-06-10	344	0	0	11-144-4

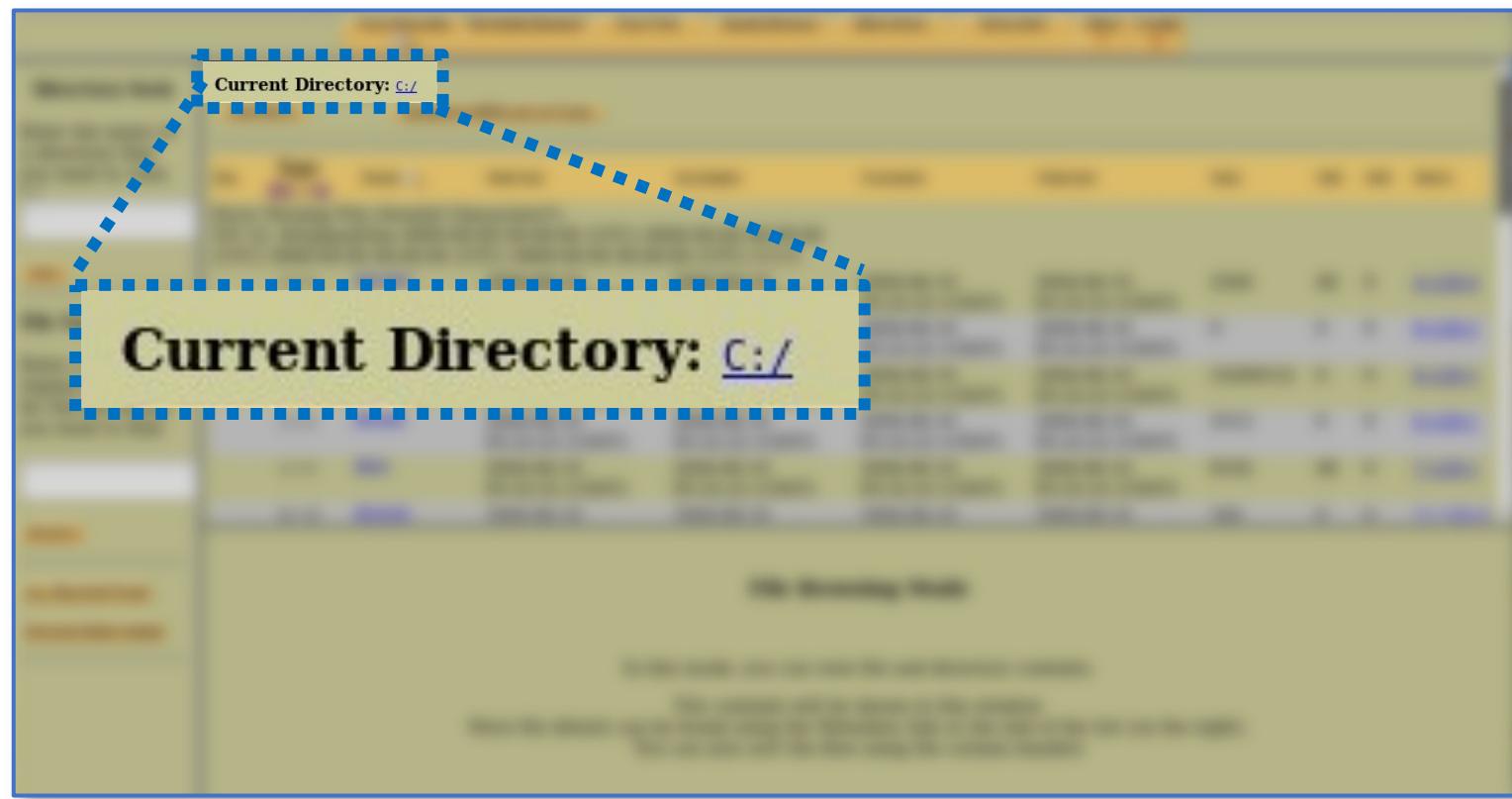
The right side of the interface displays a 'File Browsing Mode' window with instructions:

In this mode, you can view file and directory contents.
File contents will be shown in this window.
More file details can be found using the Metadata link at the end of the list (on the right).
You can also sort the files using the column headers.

Il tool Autopsy

Analisi mediante Autopsy | 5/27

- Vengono mostrati tutti i file e le directory, contenuti nella **Current Directory** (nell'esempio, è C:\)



Il tool Autopsy

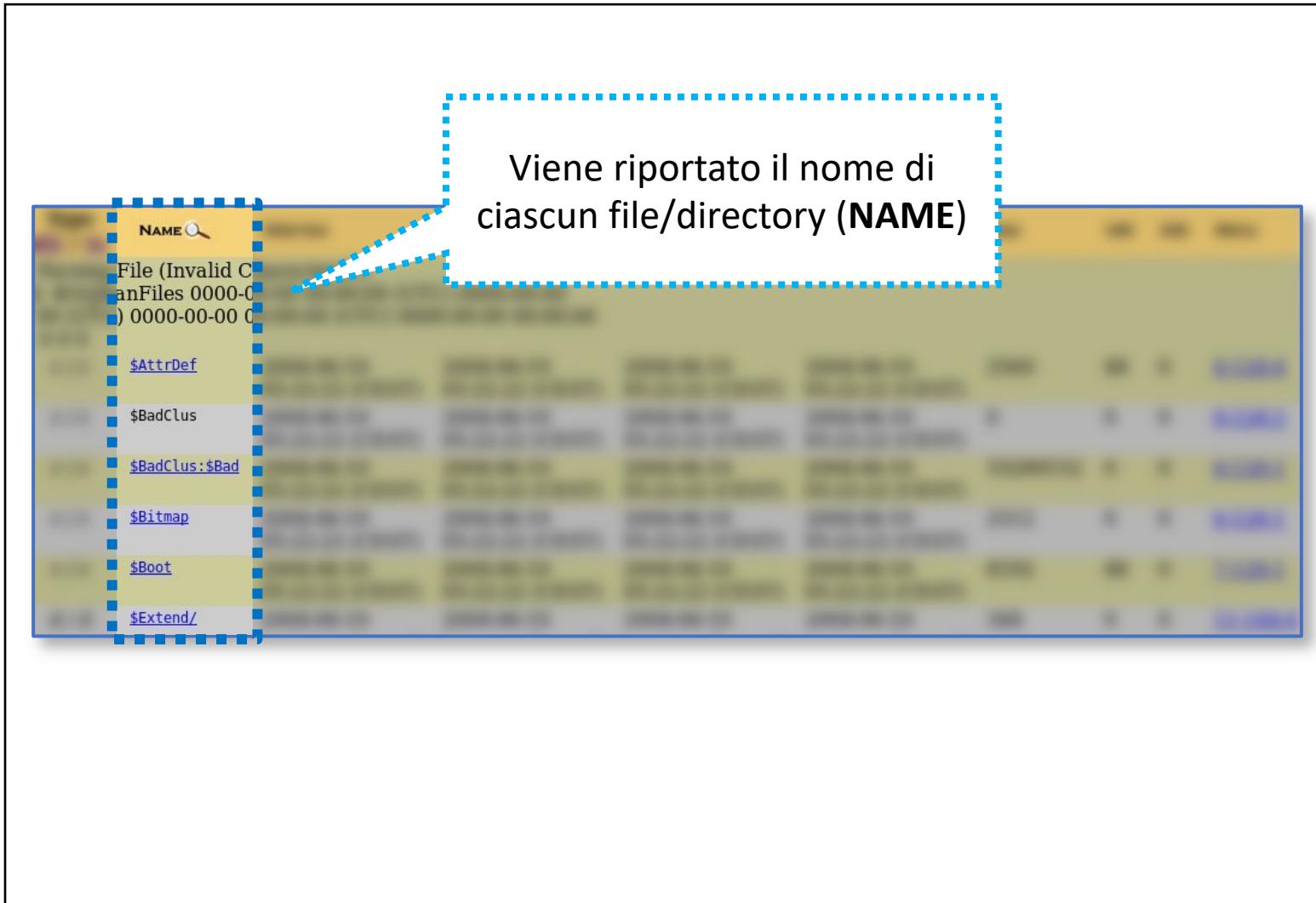
Analisi mediante Autopsy | 6/27

- Per ciascuno dei file/directory nella lista, vengono mostrate diverse caratteristiche

Type	Name	Written	Accessed	Changed	Created	Size	UID	GID	META
dir / in									
Parsing File (Invalid Characters?):									
?: \$OrphanFiles 0000-00-00 00:00:00 (UTC) 0000-00-00 00 (UTC) 0000-00-00 00:00:00 (UTC) 0000-00-00 00:00:00 0 0 0									
r / r	\$AttrDef	2004-06-10 05:22:22 (CEST)	2004-06-10 05:22:22 (CEST)	2004-06-10 05:22:22 (CEST)	2004-06-10 05:22:22 (CEST)	2560	48	0	4-128-4
r / r	\$BadClus	2004-06-10 05:22:22 (CEST)	2004-06-10 05:22:22 (CEST)	2004-06-10 05:22:22 (CEST)	2004-06-10 05:22:22 (CEST)	0	0	0	8-128-2
r / r	\$BadClus:\$Bad	2004-06-10 05:22:22 (CEST)	2004-06-10 05:22:22 (CEST)	2004-06-10 05:22:22 (CEST)	2004-06-10 05:22:22 (CEST)	10289152	0	0	8-128-1
r / r	\$Bitmap	2004-06-10 05:22:22 (CEST)	2004-06-10 05:22:22 (CEST)	2004-06-10 05:22:22 (CEST)	2004-06-10 05:22:22 (CEST)	2512	0	0	6-128-1
r / r	\$Boot	2004-06-10 05:22:22 (CEST)	2004-06-10 05:22:22 (CEST)	2004-06-10 05:22:22 (CEST)	2004-06-10 05:22:22 (CEST)	8192	48	0	7-128-1
d / d	\$Extend/	2004-06-10	2004-06-10	2004-06-10	2004-06-10	344	0	0	11-144-4

Il tool Autopsy

Analisi mediante Autopsy | 6/27



Il tool Autopsy

Analisi mediante Autopsy | 6/27

Per ciascuno dei file/directory (riportati/e sulle righe), viene riportata la **data** e l'**ora dell'ultima scrittura (WRITTEN)**

Il tool Autopsy

Analisi mediante Autopsy | 6/27

Per ciascuno dei file/directory (riportati/e sulle righe), viene riportata la **data e l'ora dell'ultimo accesso (ACCESED)**

Il tool Autopsy

Analisi mediante Autopsy | 6/27

CHANGED
2004-06-10 05:22:22 (CEST)
2004-06-10

Per ciascuno dei file/directory (riportati/e sulle righe), viene riportata la **data e l'ora dell'ultima modifica (CHANGED)**

Il tool Autopsy

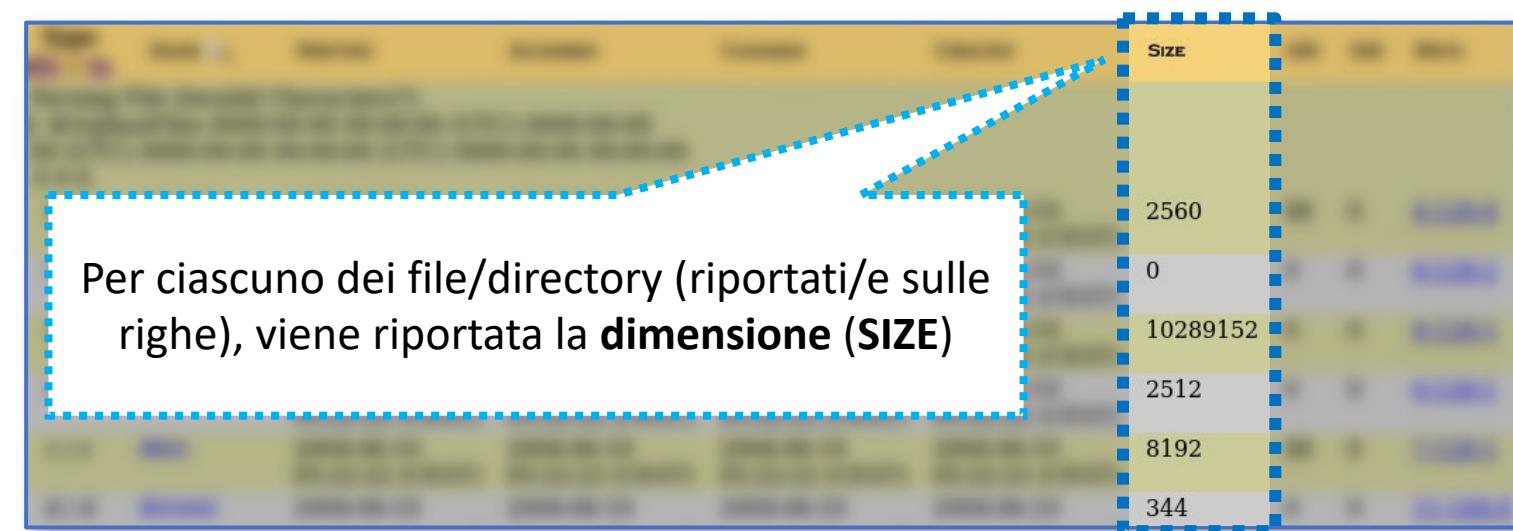
Analisi mediante Autopsy | 6/27

CREATED
2004-06-10 05:22:22 (CEST)

Per ciascuno dei file/directory (riportati/e sulle righe), viene riportata la **data e l'ora relativa alla creazione (CREATED)**

Il tool Autopsy

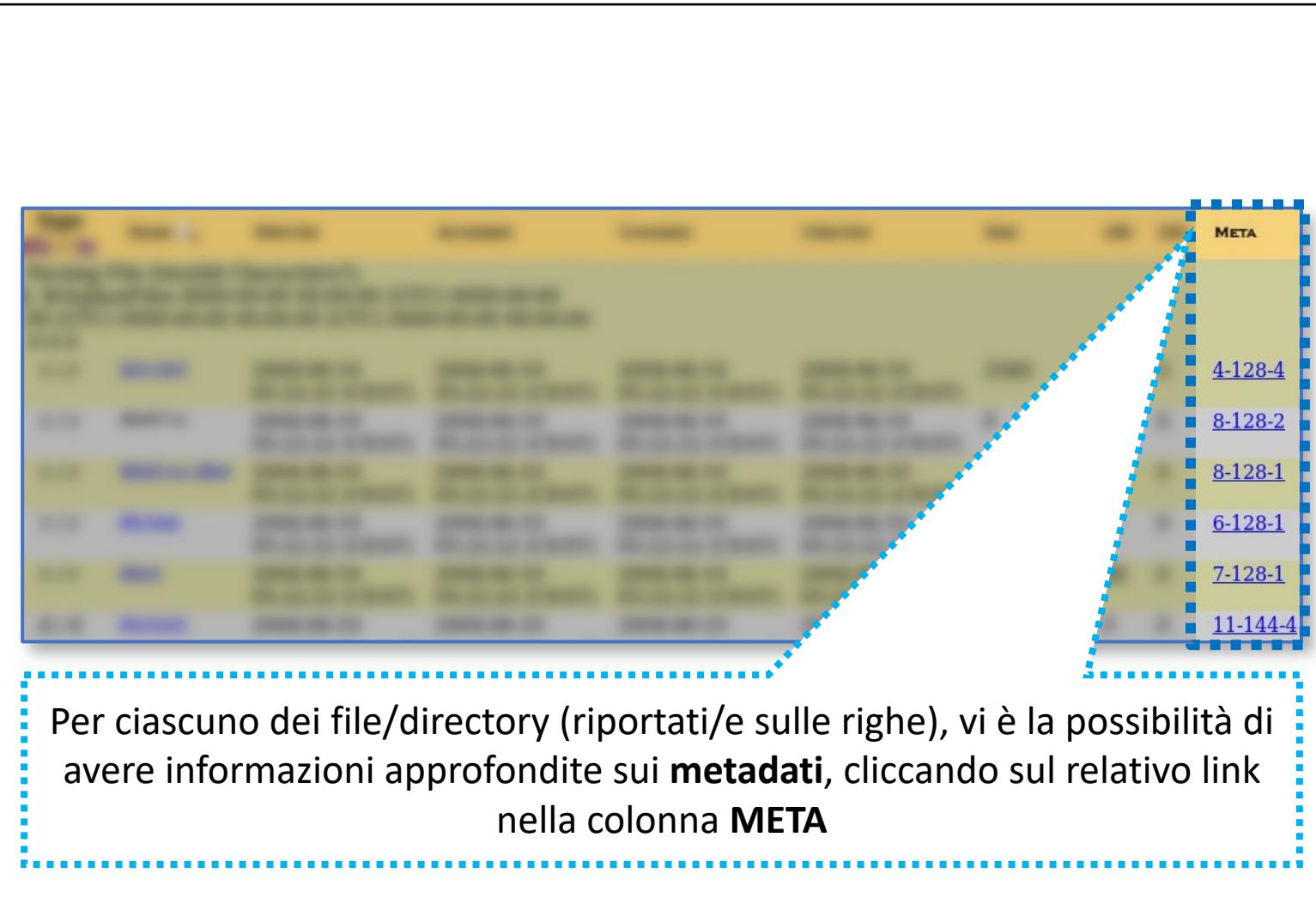
Analisi mediante Autopsy | 6/27



Per ciascuno dei file/directory (riportati/e sulle righe), viene riportata la **dimensione (SIZE)**

Il tool Autopsy

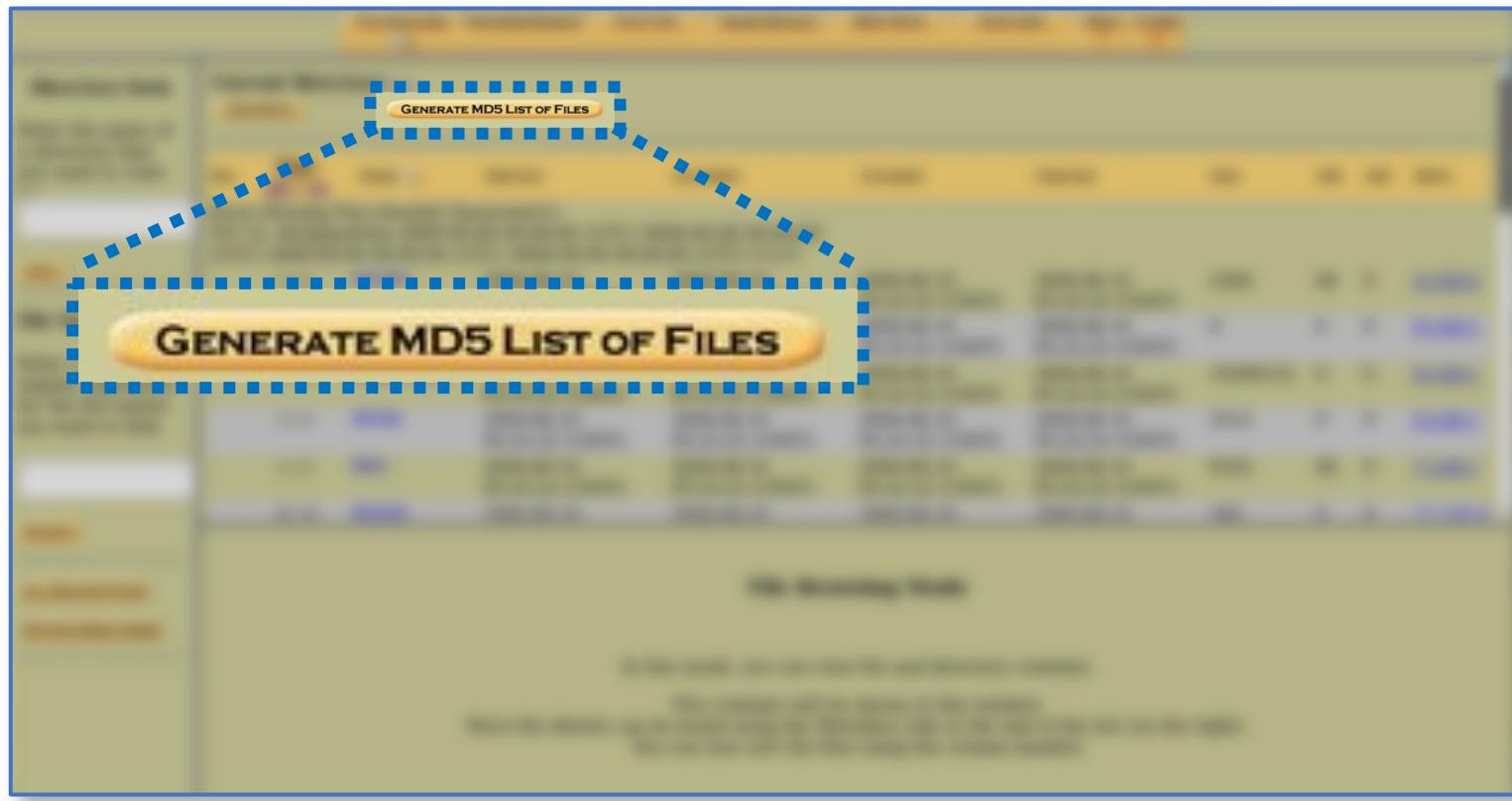
Analisi mediante Autopsy | 6/27



Il tool Autopsy

Analisi mediante Autopsy | 7/27

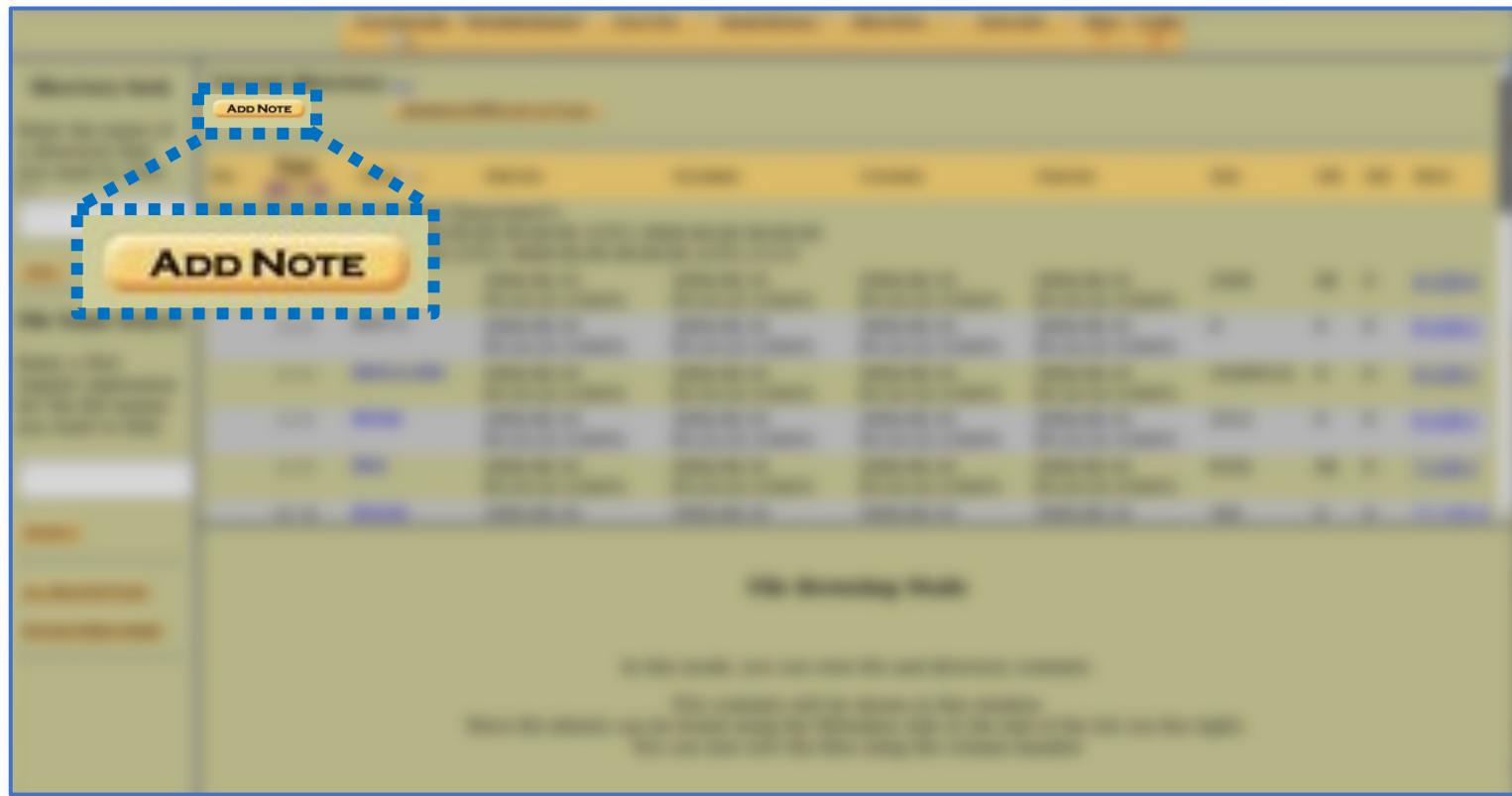
- Con il tasto «**Generate MD5 List of Files**» è possibile generare i valori di hash MD5, per ciascun file/directory (utile per controlli sull'integrità)



Il tool Autopsy

Analisi mediante Autopsy | 8/27

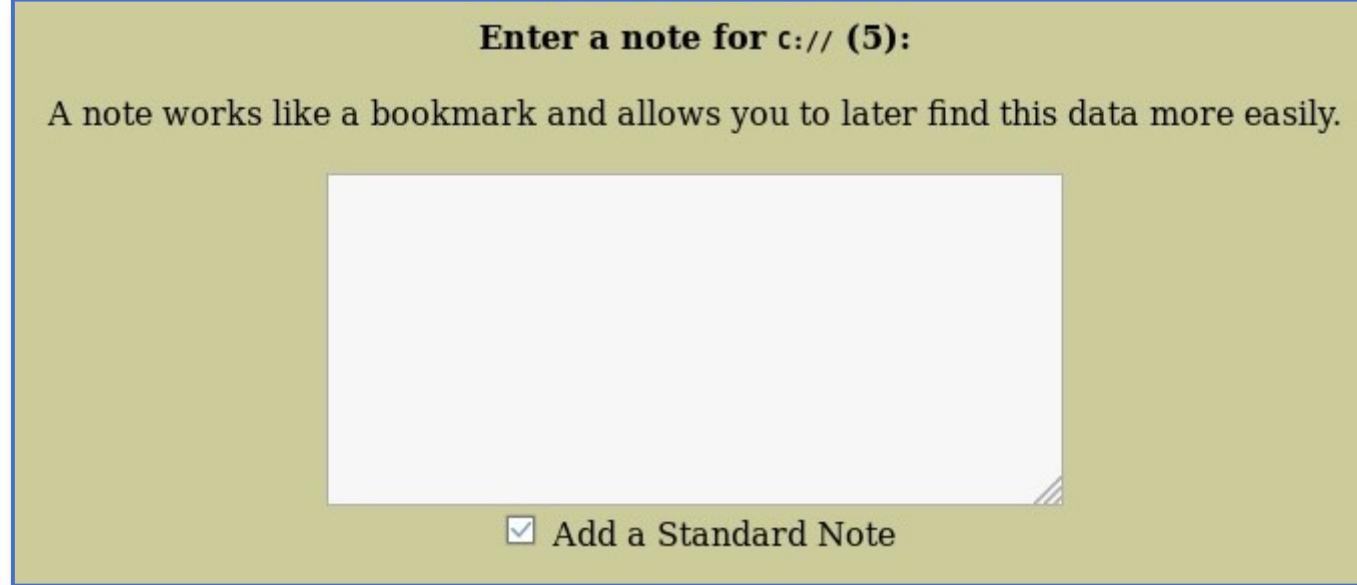
- L'investigatore potrà aggiungere anche delle annotazioni sui file (ad esempio, anomalie, ecc.), con il tasto «**Add Note**»



Il tool Autopsy

Analisi mediante Autopsy | 9/27

- *Interfaccia per l'aggiunta di una annotazione*



Il tool Autopsy

Analisi mediante Autopsy | 10/27

- Il pannello a sinistra permette di svolgere quattro utili operazioni



Il tool Autopsy

Analisi mediante Autopsy | 11/27

The screenshot shows the search interface of the Autopsy tool. It consists of two main sections: 'Directory Seek' on the left and 'File Name Search' on the right.

Directory Seek

Enter the name of a directory that you want to view.
C:/

VIEW

File Name Search

Enter a Perl regular expression for the file names you want to find.

SEARCH

ALL DELETED FILES

EXPAND DIRECTORIES

Il tool Autopsy

Analisi mediante Autopsy | 11/27

Directory Seek

Enter the name of a directory that you want to view.

C:/

VIEW

Directory Seek

Permette la ricerca di directory

Il tool Autopsy

Analisi mediante Autopsy | 11/27



The image shows a screenshot of the Autopsy digital forensics tool's interface. On the left, there is a search panel titled "File Name Search" with the sub-instruction "Enter a Perl regular expression for the file names you want to find." Below this is a text input field and a yellow "SEARCH" button. A blue dashed rectangular box highlights this entire search section.

File Name Search

Permette di effettuare ricerche di file
(è anche possibile utilizzare
espressioni regolari)

Il tool Autopsy

Analisi mediante Autopsy | 11/27

Expand Directories

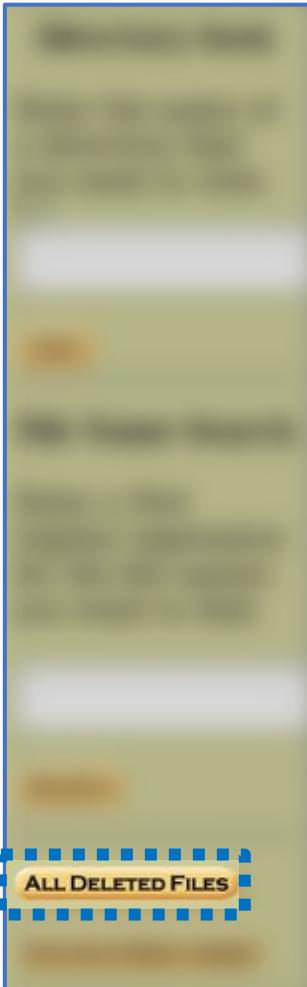
Espande la visualizzazione di tutte le directory, per avere una vista più completa
(come mostrato nell'immagine)

The screenshot shows a list of directory entries under drive C:/, each preceded by a plus sign indicating they can be expanded. The entries are:

- C:/
- +/\$Extend
- +/alloc
- +/archive
- +/dell
- +/del2
- +/invalid
- +/misc
- +/RECYCLER
- ++/S-1-5-21-17579812
- +/System Volume Information

Il tool Autopsy

Analisi mediante Autopsy | 11/27



The image shows a screenshot of the Autopsy digital forensics tool. On the left, there is a large preview window displaying a blurred image of a document or file. On the right, a search results panel titled "All Deleted Files" is visible. The results list contains several entries, with the top one being "Cerca, all'interno dell'immagine, eventuali file eliminati (maggiori dettagli nelle prossime slide)". A blue dotted line highlights this specific search result.

All Deleted Files

Cerca, all'interno dell'immagine,
eventuali file eliminati
(maggiori dettagli nelle prossime slide)

Il tool Autopsy

Analisi mediante Autopsy | 11/27

- Autopsy recupera eventuali file eliminati, basandosi su eventuali metadati, ancora disponibili, relativi a tali file
 - Ad esempio, in NTFS, considera eventuali entry, della MFT, contrassegnate come *unallocated*, non ancora sovrascritte

OSSERVAZIONE: Non si tratta quindi di un processo di file recovery/data carving; Inoltre, è necessario considerare che verosimilmente le entry, contrassegnate come *unallocated*, vengono sovrascritte da nuove entry (che si riferiscono a nuovi file), durante il normale utilizzo del sistema

Il tool Autopsy

Analisi mediante Autopsy | 12/27

- Cliccando quindi su «**All Deleted Files**», verranno mostrati tutti i file eliminati (riportati **in rosso**), che Autopsy ha recuperato

All Deleted Files									
Type dir / in	NAME	WRITTEN	ACCESSED	CHANGED	CREATED	SIZE	UID	GID	META
- / r	C:/del1/file6.jpg	2004-06-10 08:48:08 (CEST)	2004-06-10 05:28:00 (CEST)	2004-06-10 05:28:00 (CEST)	2004-06-10 05:28:00 (CEST)	175630	0	0	32-128-3
- / r	C:/del2/file7.hmm	2004-06-10 08:49:18 (CEST)	2004-06-10 05:43:38 (CEST)	2004-06-10 05:43:44 (CEST)	2004-06-10 05:28:00 (CEST)	326859	0	0	31-128-3

- Inoltre, per ciascuno di tali file, sono riportate le informazioni relative alla **data e ora dell'ultima scrittura/modifica/accesso** e della **creazione** del file, la **dimensione** ed i relativi **metadati**
- Nell'esempio, vengono recuperati due file eliminati:
 - C:/del1/file6.jpg
 - C:/del2/file7.hmm

Il tool Autopsy

Analisi mediante Autopsy | 13/27

All Deleted Files									
Type dir / in	NAME	WRITTEN	ACCESSED	CHANGED	CREATED	SIZE	UID	GID	META
- / r	C:/del1 /file6.jpg	2004-06-10 08:48:08 (CEST)	2004-06-10 05:28:00 (CEST)	2004-06-10 05:28:00 (CEST)	2004-06-10 05:28:00 (CEST)	175630	0	0	32-128-3
- / r	C:/del2 /file7.hmm	2004-06-10 08:49:18 (CEST)	2004-06-10 05:43:38 (CEST)	2004-06-10 05:43:44 (CEST)	2004-06-10 05:28:00 (CEST)	326859	0	0	31-128-3

- Cliccando sul nome di un file (riportato nella colonna **Name**), nel pannello **File Browsing Mode** (*figura in basso*), verrà mostrata un'anteprima del file selezionato

File Browsing Mode

In this mode, you can view file and directory contents.

File contents will be shown in this window.

More file details can be found using the Metadata link at the end of the list (on the right).
You can also sort the files using the column headers

Il tool Autopsy

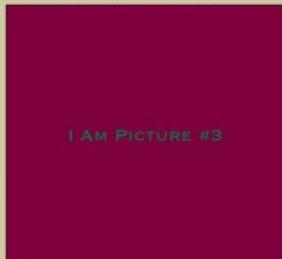
Analisi mediante Autopsy | 14/27

- /r C:/dell/file6.jpg 2004-06-10 08:48:08 (CEST) 2004-06-10 05:28:00 (CEST) 2004-06-10 05:28:00 (CEST) 2004-06-10 05:28:00 (CEST) 175630 0 0 32-128-3

Anteprima del file C:/dell/file6.jpg
(trattasi di una immagine JPEG)

ASCII ([display](#) - [report](#)) * Hex ([display](#) - [report](#)) * ASCII Strings ([display](#) - [report](#)) * [Export](#) * [View](#) * [Add Note](#)
File Type: JPEG image data, JFIF standard 1.01, aspect ratio, density 1x1, segment length 16, baseline, precision 8, 563x527, frames 3
C:/dell/file6.jpg

Thumbnail: [View Full Size Image](#)



Il tool Autopsy

Analisi mediante Autopsy | 15/27

The screenshot shows the Autopsy digital forensics tool interface. At the top, there is a timeline or file list with several entries. One entry is highlighted with a blue dashed border and contains the following information:

- / r	C:/del2	2004-06-10	2004-06-10	2004-06-10	2004-06-10	326859	0	0	31-128-3
	/file7.hmm	08:49:18 (CEST)	05:43:38 (CEST)	05:43:44 (CEST)	05:28:00 (CEST)				

Below this, a preview window displays the file C:/del2/file7.hmm, which is identified as a JPEG image. The preview image is very blurry and yellowish.

**Anteprima del file C:/del2/file7.hmm
(trattasi di una immagine JPEG)**

ASCII ([display](#) - [report](#)) * Hex ([display](#) - [report](#)) * ASCII Strings ([display](#) - [report](#)) * [Export](#) * [View](#) * [Add Note](#)
File Type: JPEG image data, JFIF standard 1.01, aspect ratio, density 1x1, segment length 16, baseline, precision 8, 698x752, frames 3
C:/del2/file7.hmm

Thumbnail: [View Full Size Image](#)

I AM PICTURE #4

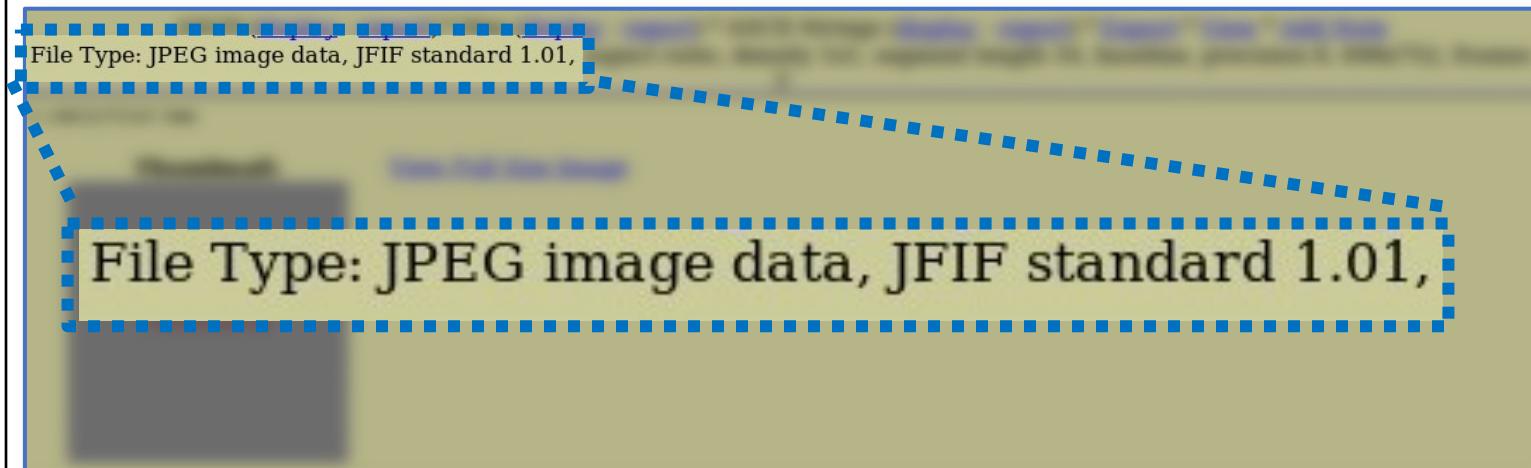
Il tool Autopsy

Analisi mediante Autopsy | 16/27

OSSERVAZIONE IMPORTANTE

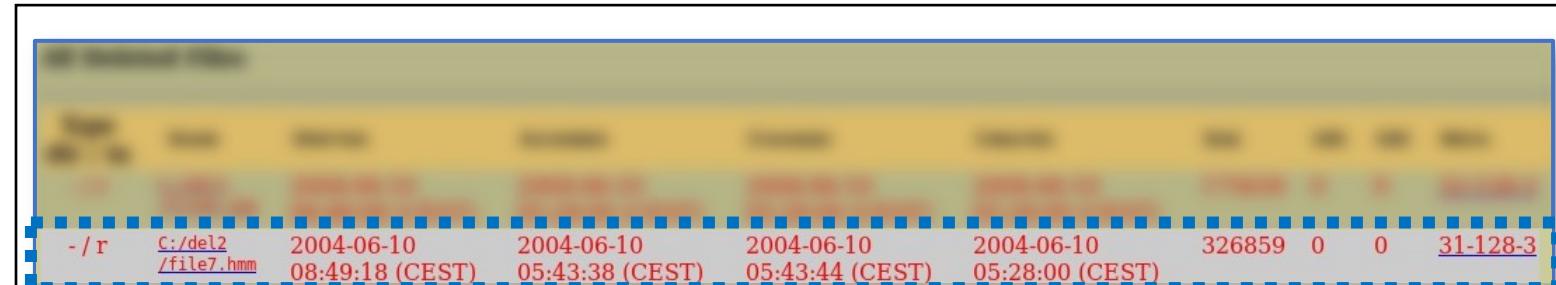
Il file C:/de12/file7.hmm viene riportato come immagine JPEG (standard *JPEG File Interchange Format – JFIF*, in versione 1.01) e ne viene mostrata la relativa anteprima, nonostante il file non abbia estensione .jpg (o .jpeg, o .jfif)

Anteprima del file C:/de12/file7.hmm
(trattasi di una immagine JPEG)



Il tool Autopsy

Analisi mediante Autopsy | 16/27



The screenshot shows a table of file metadata from the Autopsy tool. The columns include:

- / r	C:/del2 /file7.hmm	2004-06-10 08:49:18 (CEST)	2004-06-10 05:43:38 (CEST)	2004-06-10 05:43:44 (CEST)	2004-06-10 05:28:00 (CEST)	326859	0	0	31-128-3
-------	-----------------------	-------------------------------	-------------------------------	-------------------------------	-------------------------------	--------	---	---	----------

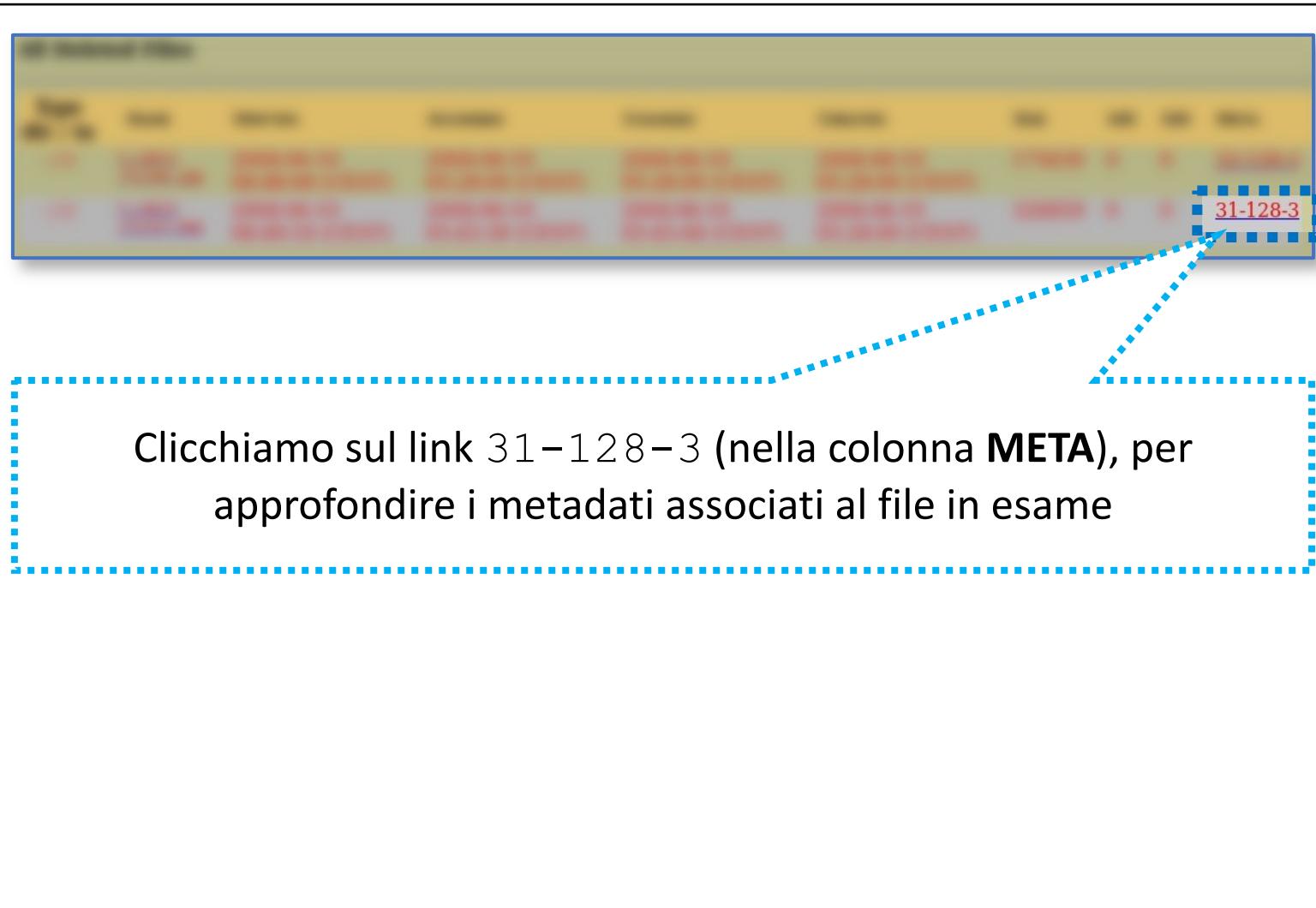
A blue dashed box highlights the first row of the table.



Approfondiamo ulteriormente l'analisi del file C:/del2/file7.hmm, poiché potrebbe essere un file potenzialmente importante per l'indagine: in primo luogo, poiché è stato eliminato ed, in secondo luogo, è stato verosimilmente rinominato (alterandone l'estensione)

Il tool Autopsy

Analisi mediante Autopsy | 16/27



Il tool Autopsy

Analisi mediante Autopsy | 17/27

- *Metadati per il file C:/de12/file7.hmm (Parziale)*

Pointed to by file:

C:/de12/file7.hmm (deleted)

File Type (Recovered):

JPEG image data, JFIF standard 1.01, aspect ratio, density 1x1, segment length 16, baseline, precision 8, 698x752, frames 3

MD5 of recovered content:

0c452c5800fcfa7c66027ae89c4f068a -

SHA-1 of recovered content:

7fe0602ea83956867553fa3ca98d03d90e675866 -

Details:

MFT Entry Header Values:

Entry: 31 Sequence: 2

\$LogFile Sequence Number: 1117937

Not Allocated File

Links: 1

\$STANDARD_INFORMATION Attribute Values:

Flags: Archive

Owner ID: 0

Security ID: 262 ()

Created: 2004-06-10 05:28:00.742657600 (CEST)

File Modified: 2004-06-10 08:49:18.000000000 (CEST)

MFT Modified: 2004-06-10 05:43:44.157187200 (CEST)

Accessed: 2004-06-10 05:43:38.899627200 (CEST)

Il tool Autopsy

Analisi mediante Autopsy | 18/27

- *Metadati per il file C:/de12/file7.hmm*
 - Sezione *Attributi (Attributes) – Parziale*

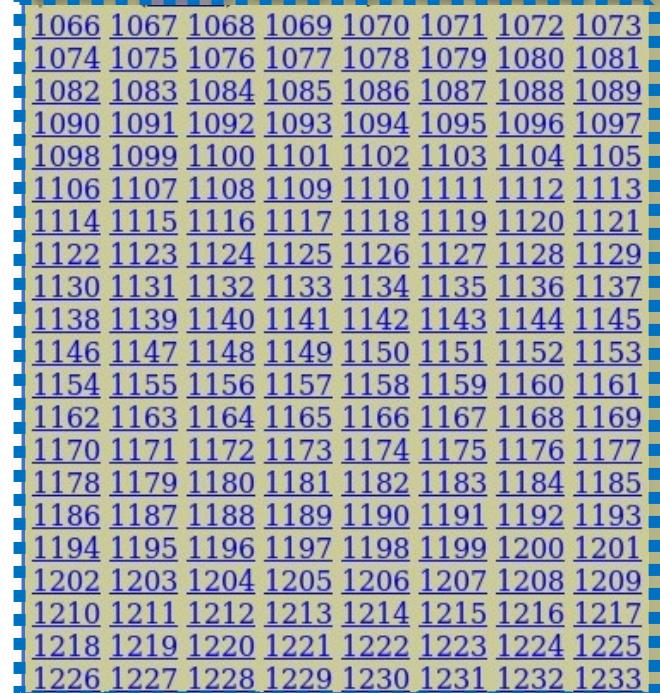
Attributes:

```
$STANDARD_INFORMATION (16-0) Name: N/A Resident size: 72
$FILE_NAME (48-4) Name: N/A Resident size: 84
$DATA (128-3) Name: N/A Non-Resident size: 326859 init_size: 326859
1066 1067 1068 1069 1070 1071 1072 1073
1074 1075 1076 1077 1078 1079 1080 1081
1082 1083 1084 1085 1086 1087 1088 1089
1090 1091 1092 1093 1094 1095 1096 1097
1098 1099 1100 1101 1102 1103 1104 1105
1106 1107 1108 1109 1110 1111 1112 1113
1114 1115 1116 1117 1118 1119 1120 1121
1122 1123 1124 1125 1126 1127 1128 1129
1130 1131 1132 1133 1134 1135 1136 1137
1138 1139 1140 1141 1142 1143 1144 1145
1146 1147 1148 1149 1150 1151 1152 1153
1154 1155 1156 1157 1158 1159 1160 1161
1162 1163 1164 1165 1166 1167 1168 1169
1170 1171 1172 1173 1174 1175 1176 1177
1178 1179 1180 1181 1182 1183 1184 1185
1186 1187 1188 1189 1190 1191 1192 1193
1194 1195 1196 1197 1198 1199 1200 1201
1202 1203 1204 1205 1206 1207 1208 1209
1210 1211 1212 1213 1214 1215 1216 1217
1218 1219 1220 1221 1222 1223 1224 1225
1226 1227 1228 1229 1230 1231 1232 1233
```

Il tool Autopsy

Analisi mediante Autopsy | 18/27

In questa sezione, sono riportate tutte le parti (ciascuna memorizzata all'interno di un cluster), che compongono il file C:/de12/file7.hmm



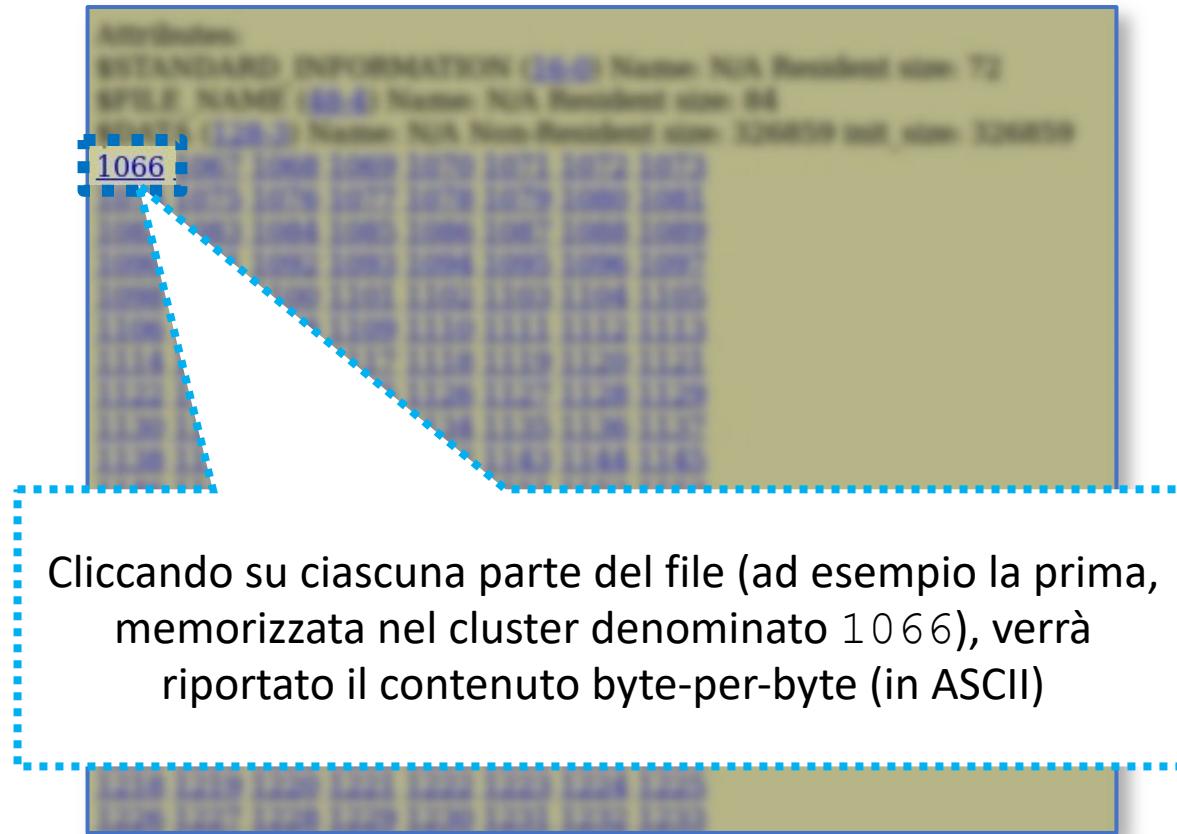
The screenshot shows a list of sequence identifiers, likely HMM states, arranged in a grid. The first column contains identifiers from 1066 to 1226, and the second column contains identifiers from 1067 to 1227. The background of the list area is light green, and the entire list is enclosed in a blue dashed border.

1066	1067	1068	1069	1070	1071	1072	1073
1074	1075	1076	1077	1078	1079	1080	1081
1082	1083	1084	1085	1086	1087	1088	1089
1090	1091	1092	1093	1094	1095	1096	1097
1098	1099	1100	1101	1102	1103	1104	1105
1106	1107	1108	1109	1110	1111	1112	1113
1114	1115	1116	1117	1118	1119	1120	1121
1122	1123	1124	1125	1126	1127	1128	1129
1130	1131	1132	1133	1134	1135	1136	1137
1138	1139	1140	1141	1142	1143	1144	1145
1146	1147	1148	1149	1150	1151	1152	1153
1154	1155	1156	1157	1158	1159	1160	1161
1162	1163	1164	1165	1166	1167	1168	1169
1170	1171	1172	1173	1174	1175	1176	1177
1178	1179	1180	1181	1182	1183	1184	1185
1186	1187	1188	1189	1190	1191	1192	1193
1194	1195	1196	1197	1198	1199	1200	1201
1202	1203	1204	1205	1206	1207	1208	1209
1210	1211	1212	1213	1214	1215	1216	1217
1218	1219	1220	1221	1222	1223	1224	1225
1226	1227	1228	1229	1230	1231	1232	1233

Il tool Autopsy

Analisi mediante Autopsy | 18/27

- *Metadati per il file C:/de12/file7.hmm*
 - Sezione *Attributi (Attributes) – Parziale*



Il tool Autopsy

Analisi mediante Autopsy | 19/27

- *Metadati per il file C:/de12/file7.hmm*
 - Sezione *Attributi (Attributes)*
 - Contenuto (*Parziale*) del Cluster [**non allocato**], denominato 1066

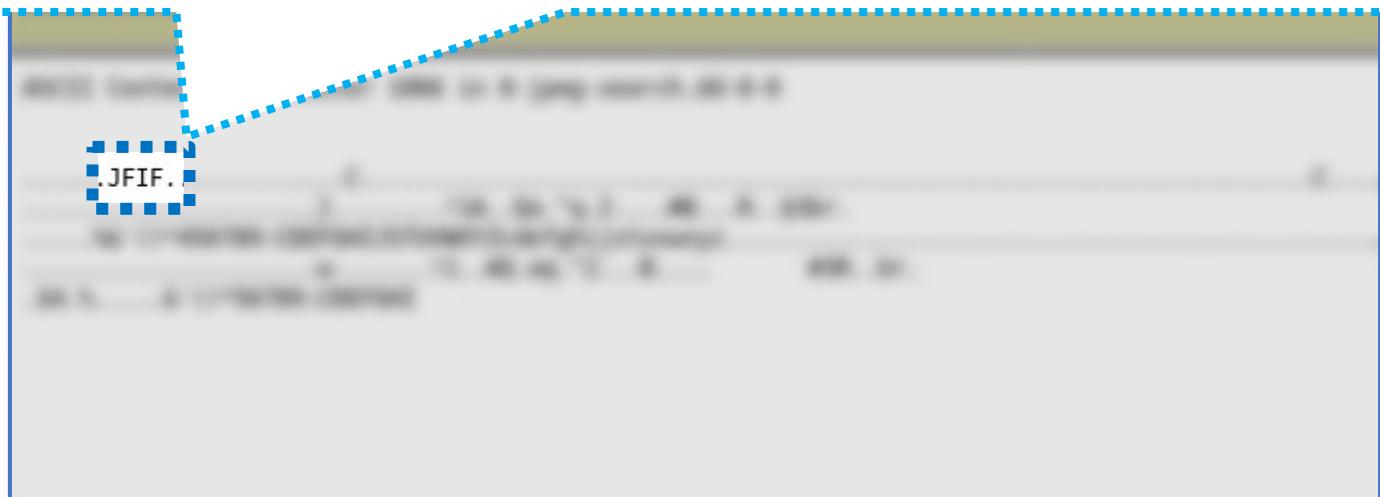
Cluster: 1066
Status: Not Allocated
[Find Meta Data Address](#)

ASCII Contents of Cluster 1066 in 8-jpeg-search.dd-0-0

```
.....JFIF.....C.....C.....  
.....}.....!1A..Qa."q.2....#B...R..$3br.  
....%&'()*456789:CDEFGHIJSTUVWXYZcdefghijstuvwxyz.....  
.....w.....!1..AQ.aq."2...B..... #3R..br.  
.4.%....&'()*56789:CDEFGHI
```

OSSERVAZIONE IMPORTANTE

- Il cluster, denominato 1066, è il cluster contenente la prima parte del file (eliminato), in cui è memorizzato anche l'header del file stesso
- Proprio tramite l'header, come è possibile osservare, si può risalire alla tipologia del file in esame (in questo caso, file memorizzato in accordo allo standard *JFIF*)



Il tool Autopsy

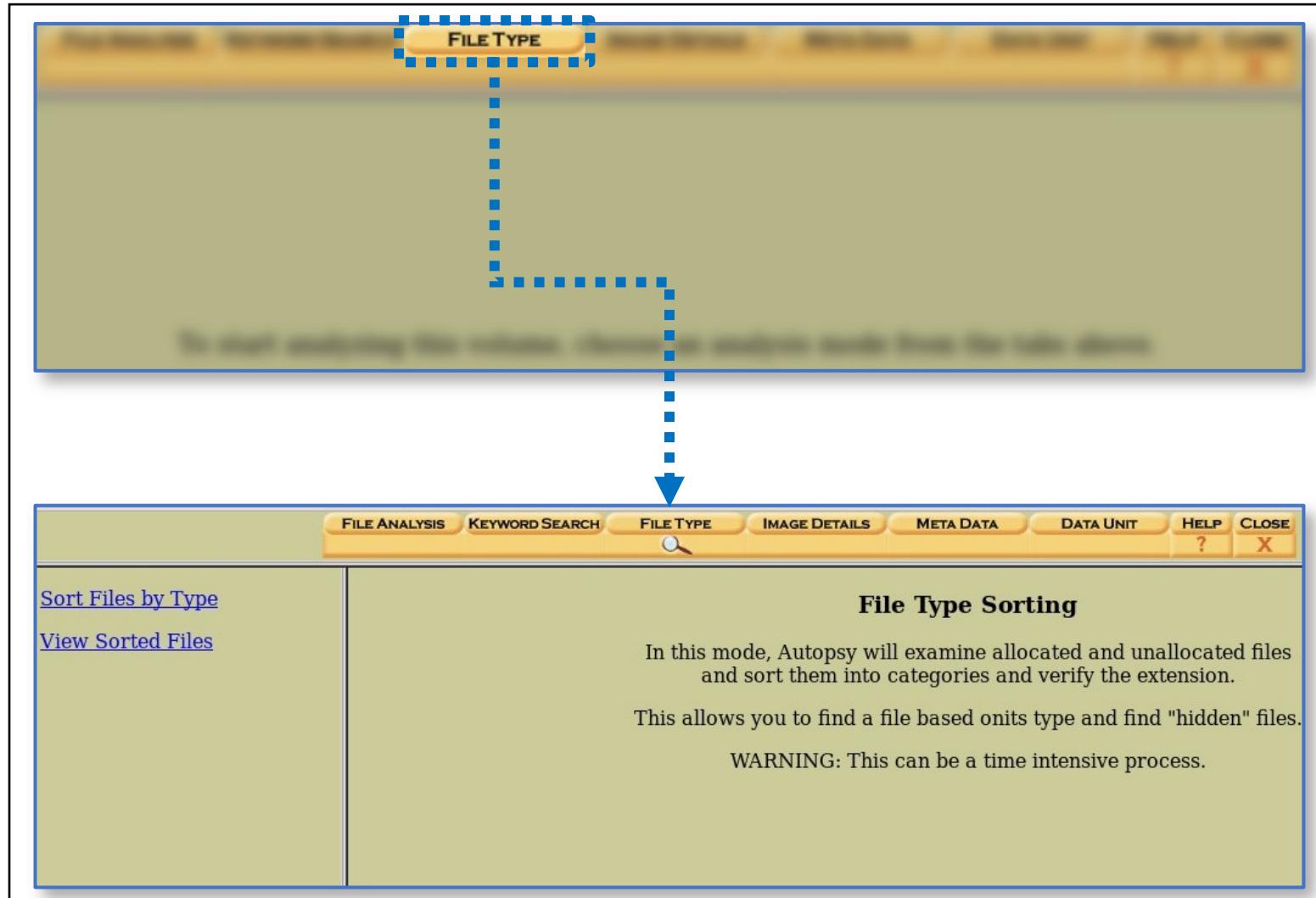
Analisi mediante Autopsy | 20/27

- L'utilizzo dei metadati è poco pratico quando, nell'immagine forense, sono presenti diverse tipologie di file da analizzare
- È possibile utilizzare l'opzione «**File Type**» per ordinare, in base alla tipologia, le seguenti categorie di file:
 - File presenti nell'immagine (*allocated*)
 - File cancellati (*unallocated*)
 - File nascosti
- Cliccare su «**File Type**» per proseguire



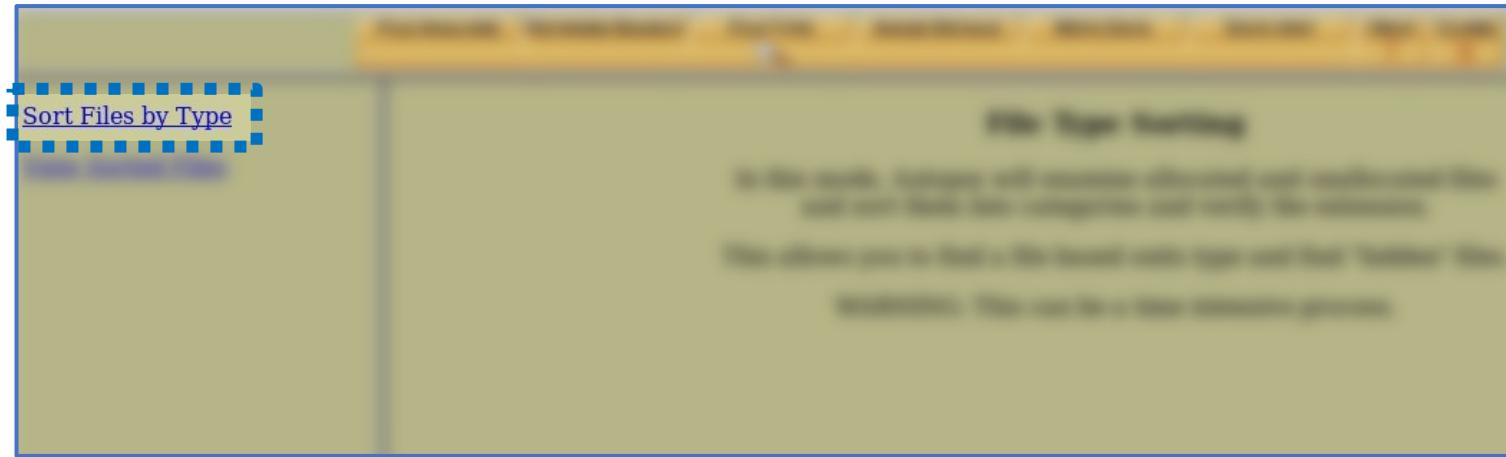
Il tool Autopsy

Analisi mediante Autopsy | 21/27



Il tool Autopsy

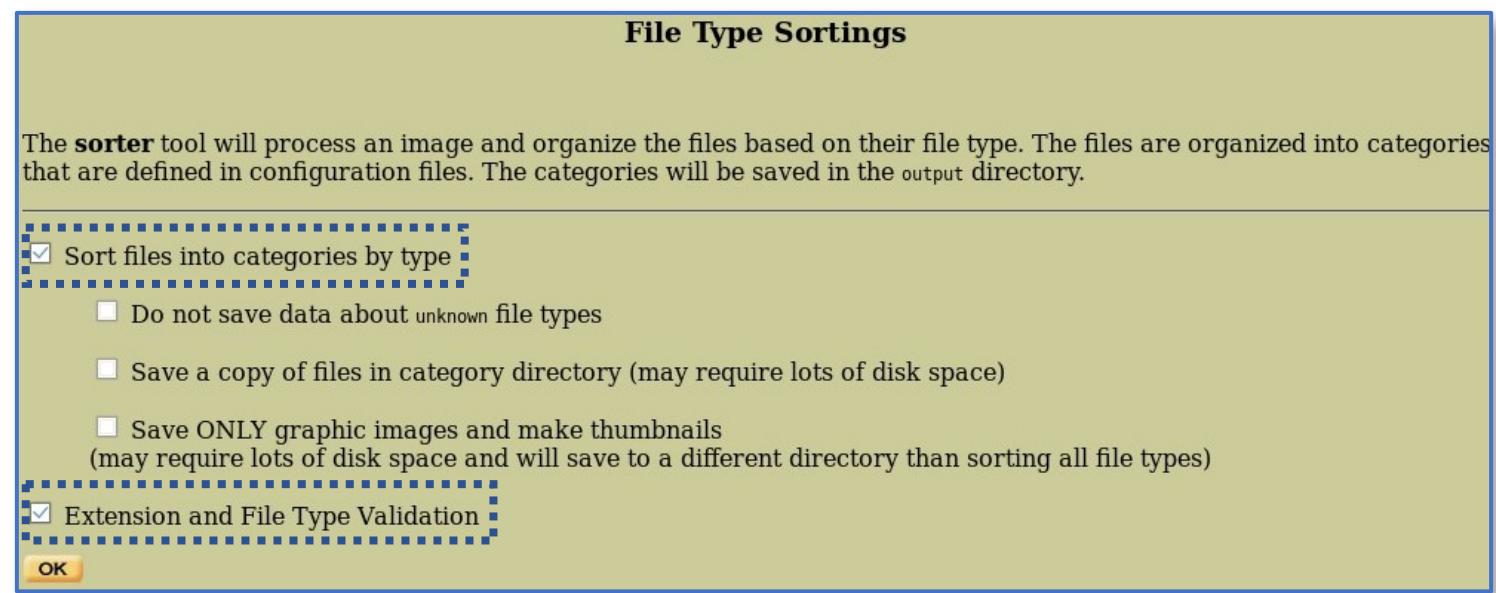
Analisi mediante Autopsy | 22/27



- Cliccando su «**Sort Files by Type**», si aprirà una nuova schermata che chiederà come deve essere effettuato l'ordinamento dei file

Il tool Autopsy

Analisi mediante Autopsy | 23/27



- Successivamente, cliccando «Ok», verrà creata una lista dei file, ordinata per tipologia dei file stessi e ci verrà mostrata una **sintesi del risultato**

Il tool Autopsy

Analisi mediante Autopsy | 24/27

Results Summary

Images

- /var/lib/autopsy/Primo/host1/images/8-jpeg-search.dd

Files (45)

Files Skipped (14)

- Non-Files (14)
- Reallocated Name Files (0)
- 'ignore' category (0)

Extensions

- Extension Mismatches (5)

Categories (31)

- archive (2)
- audio (0)
- compress (1)
- crypto (0)
- data (13)
- disk (1)
- documents (1)
- exec (0)
- images (7)
- system (0)
- text (1)
- unknown (5)
- video (0)

Sintesi del Risultato

Viene riportato il numero di file, appartenenti a ciascuna tipologia

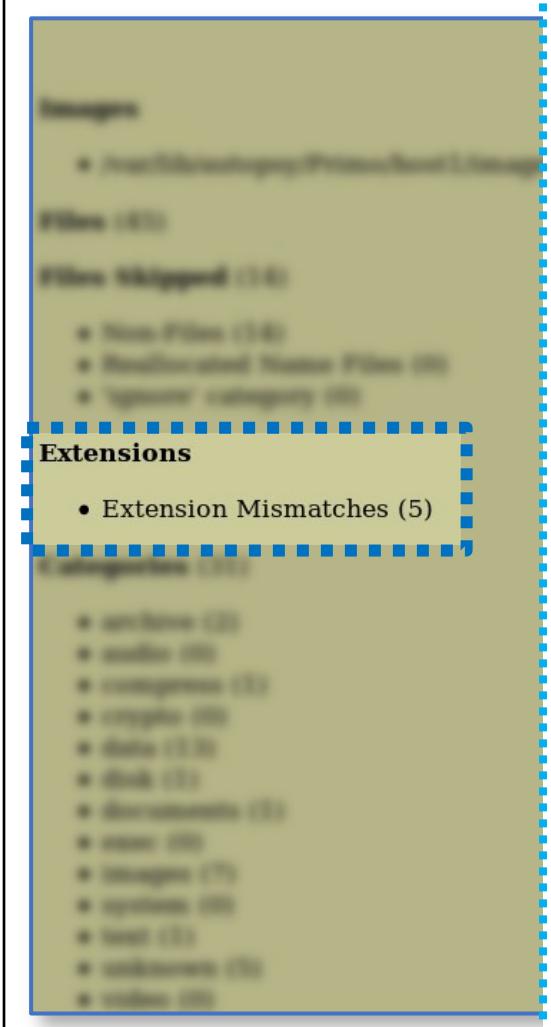
L'ordinamento per tipologia è stato eseguito, poiché, nella schermata precedente, è stata selezionata la voce, riportata nella figura in basso

Sort files into categories by type

OSSERVAZIONE

- Poiché, nella schermata precedente, è stata selezionata la voce, riportata nella figura in basso, Autopsy ha verificato se vi fossero eventuali file con incoerenze tra l'estensione e la tipologia effettiva

Extension and File Type Validation

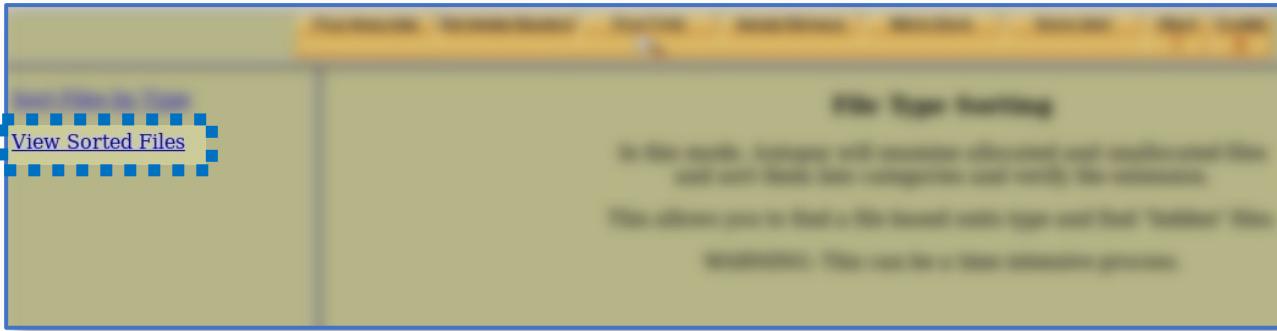


- Esempio:* Si consideri un file, avente estensione .doc (in base all'estensione, questo file dovrebbe essere un documento), ma la tipologia effettiva è però una immagine JPEG (in accordo all'header di tale file): vi è una incoerenza
- Tali file sono rilevanti, per l'indagine forense, poiché l'estensione potrebbe essere stata alterata maliziosamente
- In questo caso, Autopsy ha identificato **5 file** con incoerenze tra l'estensione e la tipologia effettiva

Il tool Autopsy

Analisi mediante Autopsy | 25/27

- Autopsy (nella versione corrente, la 2.4) non supporta la visualizzazione (diretta) dei file ordinati per tipologia



- Cliccando infatti su «**View Sorted Files**», appare il seguente messaggio informativo, in cui ci viene indicato il percorso per visionare la lista ordinata



Il tool Autopsy

Analisi mediante Autopsy | 26/27

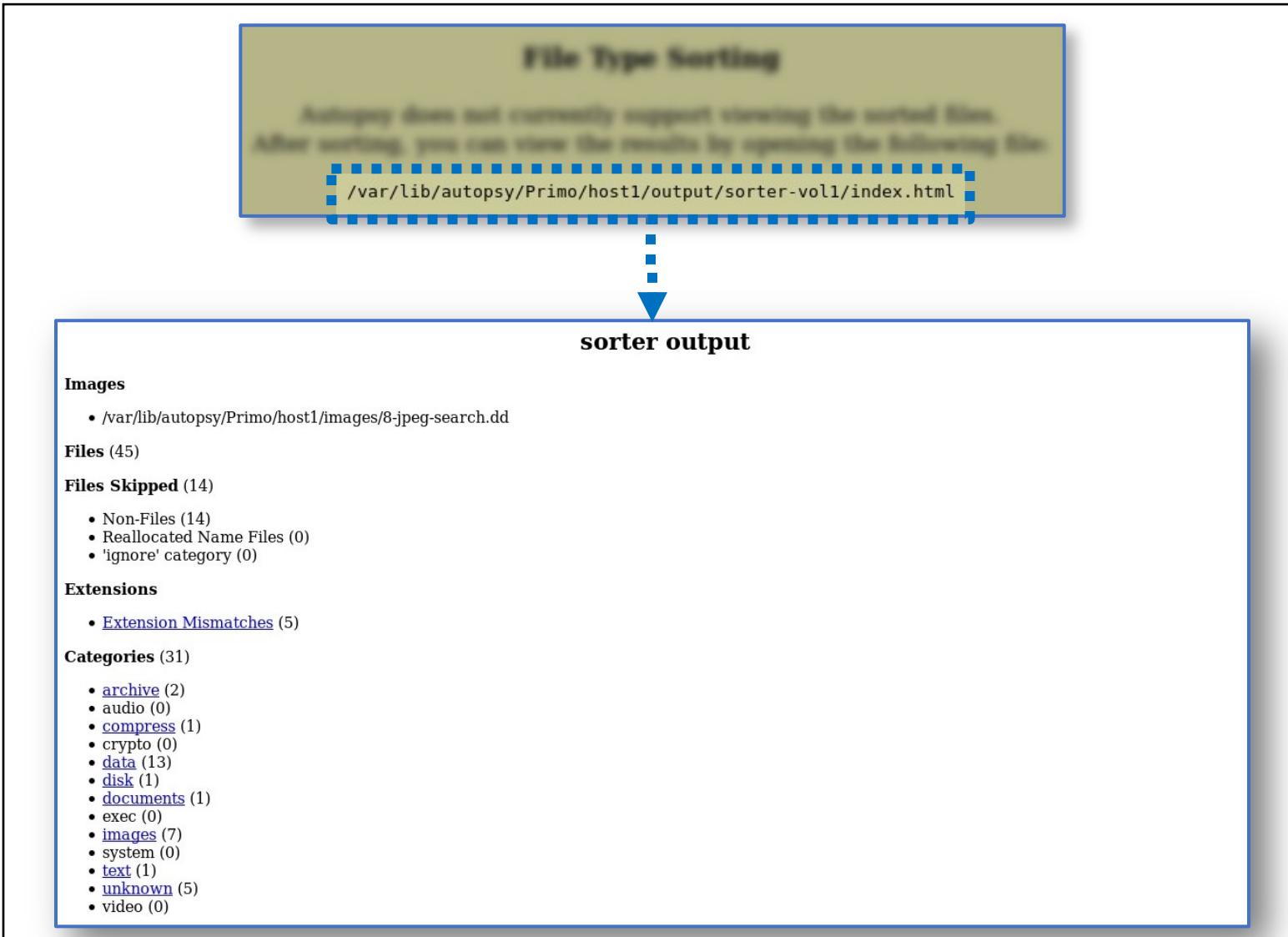
File Type Sorting

Autopsy does not currently support viewing the sorted files.
After sorting, you can view the results by opening the following file:

`/var/lib/autopsy/Primo/host1/output/sorter-vol1/index.html`

Il tool Autopsy

Analisi mediante Autopsy | 26/27



Il tool Autopsy

Analisi mediante Autopsy | 27/27

sorter output

Images

- /var/lib/autopsy/Primo/host1/images/8-jpeg-search.dd

Files (45)

Files Skipped (14)

- Non-Files (14)
- Reallocated Name Files (0)
- 'ignore' category (0)

Extensions

- Extension Mismatches (5)

Categories (31)

- [archive](#) (2)
- [audio](#) (0)

Cliccando sul link evidenziato, verrà visualizzata la lista relativa ad i **5 file**, che presentano una incoerenza tra l'estensione e la tipologia effettiva (deducibile dall'header)

Il tool Autopsy

Analisi mediante Autopsy | 27/27

sorter output

Images

- /var/lib/autopsy/Primo/host1/images/8-jpeg-search.dd

Files (45)

Files Skipped (14)

- Non-Files (14)
- Reallocated Name Files (0)
- 'ignore' category (0)

Extensions

- Extension Mismatches (5)

Categories (31)

- archive (2)
- audio (0)

↓

Extension Mismatch

C:/alloc/file2.dat
JPEG image data, JFIF standard 1.01, aspect ratio, density 1x1, segment length 16, baseline, precision 8, 437x365, frames 3 (Ext: dat)
Image: /var/lib/autopsy/Primo/host1/images/8-jpeg-search.dd Inode: 28-128-3

C:/archive/file9.boo
ERROR:[gzip: Exec ` gzip' failed, No such file or directory] (Zip archive data, at least v2.0 to extract) (Ext: boo)
Image: /var/lib/autopsy/Primo/host1/images/8-jpeg-search.dd Inode: 40-128-3

C:/del2/file7.hmm
JPEG image data, JFIF standard 1.01, aspect ratio, density 1x1, segment length 16, baseline, precision 8, 698x752, frames 3 (Ext: hmm)
Image: /var/lib/autopsy/Primo/host1/images/8-jpeg-search.dd Inode: 31-128-3

C:/invalid/file3.jpg
ASCII text (Ext: jpg)
Image: /var/lib/autopsy/Primo/host1/images/8-jpeg-search.dd Inode: 35-128-3

C:/misc/file13.dll:here
JPEG image data, JFIF standard 1.01, aspect ratio, density 1x1, segment length 16, baseline, precision 8, 518x563, frames 3 (Ext: dll:here)
Image: /var/lib/autopsy/Primo/host1/images/8-jpeg-search.dd Inode: 44-128-5

Il tool Autopsy

Analisi mediante Autopsy | 27/27

OSSERVAZIONE

I file, appartenenti alla lista sottostante, dovrebbero essere tutti oggetto di ulteriori approfondimenti da parte dell'investigatore, analizzandone i relativi metadati, prendendo eventuali annotazioni, ecc.

Extension Mismatch

```
C:/alloc/file2.dat
JPEG image data, JFIF standard 1.01, aspect ratio, density 1x1, segment length 16, baseline, precision 8, 437x365, frames 3 (Ext: dat)
Image: /var/lib/autopsy/Primo/host1/images/8-jpeg-search.dd Inode: 28-128-3

C:/archive/file9.boo
ERROR:[gzip: Exec ` gzip' failed, No such file or directory] (Zip archive data, at least v2.0 to extract) (Ext: boo)
Image: /var/lib/autopsy/Primo/host1/images/8-jpeg-search.dd Inode: 40-128-3

C:/del2/file7.hmm
JPEG image data, JFIF standard 1.01, aspect ratio, density 1x1, segment length 16, baseline, precision 8, 698x752, frames 3 (Ext: hmm)
Image: /var/lib/autopsy/Primo/host1/images/8-jpeg-search.dd Inode: 31-128-3

C:/invalid/file3.jpg
ASCII text (Ext: jpg)
Image: /var/lib/autopsy/Primo/host1/images/8-jpeg-search.dd Inode: 35-128-3

C:/misc/file13.dll:here
JPEG image data, JFIF standard 1.01, aspect ratio, density 1x1, segment length 16, baseline, precision 8, 518x563, frames 3 (Ext: dll:here)
Image: /var/lib/autopsy/Primo/host1/images/8-jpeg-search.dd Inode: 44-128-5
```

Il tool Autopsy

Approfondimenti

Creazione di un Nuovo Caso

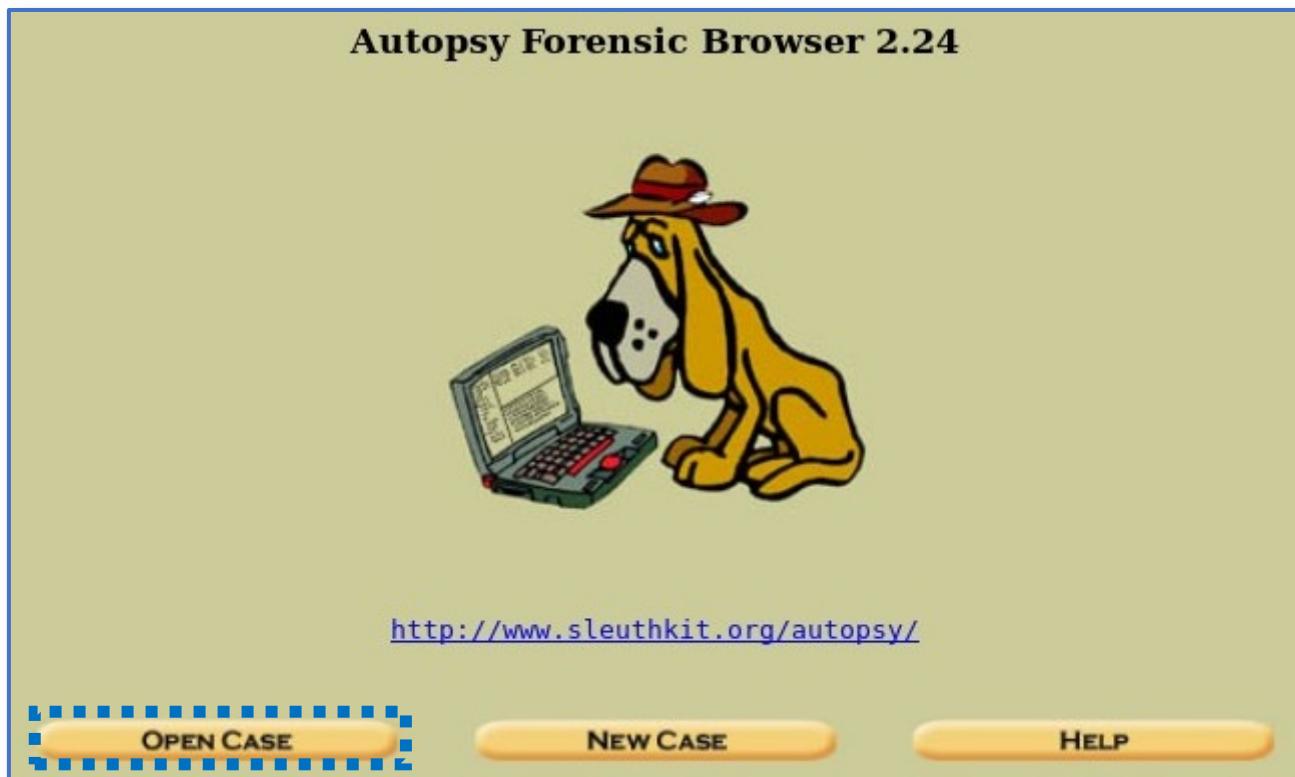
Analisi mediante Autopsy

Riapertura di un Caso

Il tool Autopsy

Riaprire un Caso | 1/3

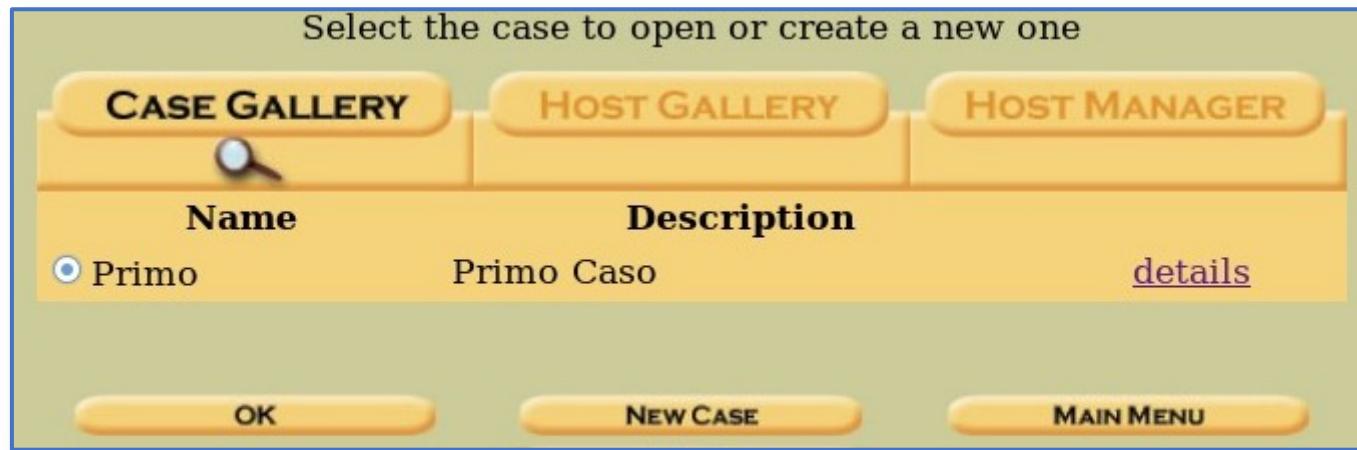
1. Per riaprire un caso, precedentemente creato, cliccare sul tasto «Open Case»



Il tool Autopsy

Riaprire un Caso | 2/3

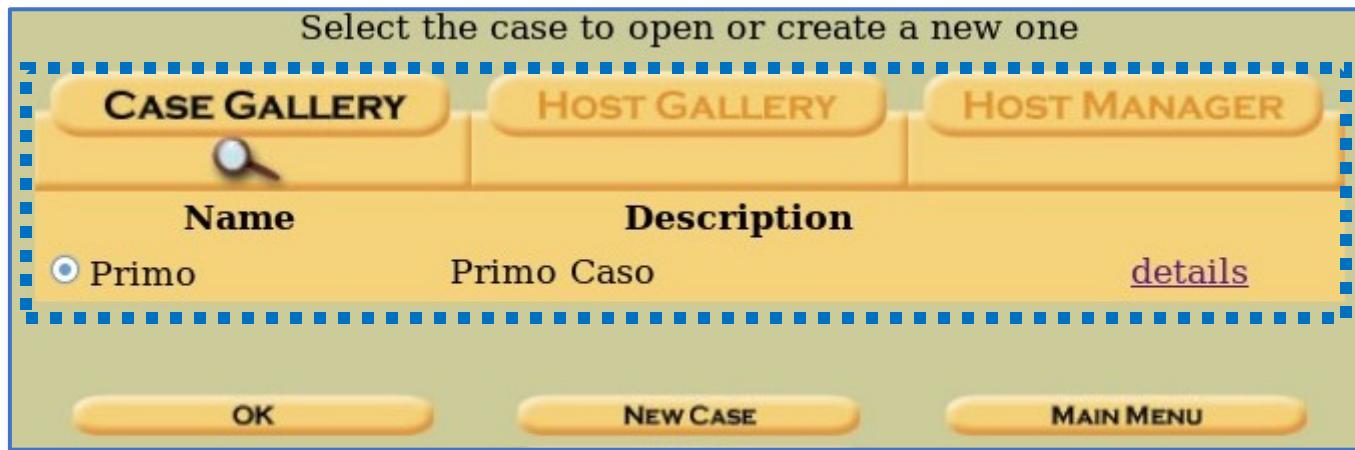
2. Selezionare il caso desiderato, fra quelli elencati nella colonna «**Case Gallery**»



Il tool Autopsy

Riaprire un Caso | 2/3

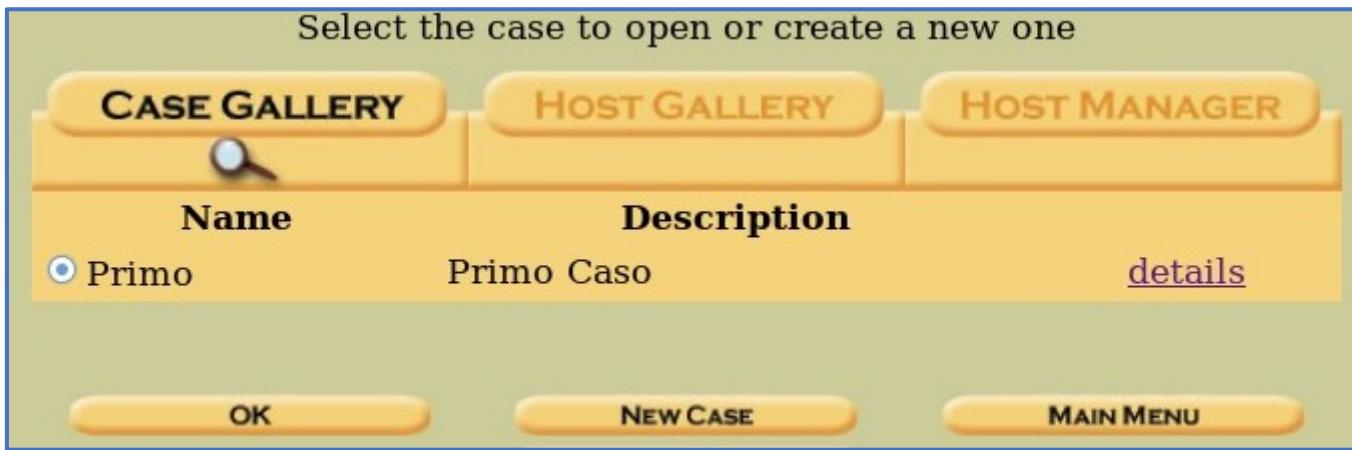
2. Selezionare il caso desiderato, fra quelli elencati nella colonna «**Case Gallery**»



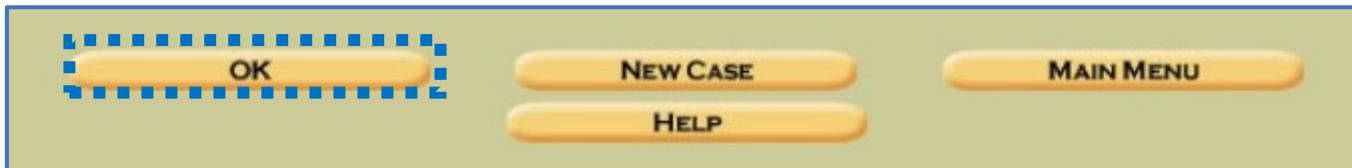
Il tool Autopsy

Riaprire un Caso | 3/3

2. Selezionare il caso desiderato, fra quelli elencati nella colonna «**Case Gallery**»



3. Cliccare su «Ok» per riaprire il caso selezionato



Le Super Timeline

Le Super Timeline

Concetti, Motivazioni e Caratteristiche | 1/15

- Un *timestamp* (letteralmente, *marca temporale*) registra il momento temporale, in cui un evento avviene
- Le evidenze dispongono di un timestamp
- *Alcuni Esempi*
 - Timestamp di un File
 - È possibile reperire, dal file system, la data e l'ora di creazione, la data e l'ora dell'ultima modifica, ecc.
 - Timestamp di un Processo
 - Nei live system, dal memory dump è possibile ottenere la data e l'ora di avvio/terminazione
 - Ecc.



Le Super Timeline

Concetti, Motivazioni e Caratteristiche | 2/15

- Esistono diversi formati di timestamp, provenienti dal file system, relativi ai file
- Nei sistemi Windows-based, un timestamp è rappresentato con 64 bit, nel formato *FILETIME*
 - Le informazioni sul fuso orario (timezone) sono specificate nel registro di Windows, al percorso:
 - HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Control\TimeZoneInformation
- Nei sistemi Linux-based, un timestamp è memorizzato in formato *Posix* o *Epoch* (32 bit)
 - Le informazioni sul fuso orario sono specificate in /etc/localtime

Le Super Timeline

Concetti, Motivazioni e Caratteristiche | 3/15

- Nei sistemi Windows-based, per ciascun file, vengono memorizzati diversi timestamp, che riportano le cosiddette informazioni MACB

Lettera	Descrizione
M	Data e ora dell'ultima modifica
A	Data e ora dell'ultimo accesso al file
C	Data e ora dell'ultima modifica ai metadati
B	Data e ora di creazione del file

Le Super Timeline

Concetti, Motivazioni e Caratteristiche | 3/15

- Nei sistemi Windows-based, per ciascun file, vengono memorizzati diversi timestamp, che riportano le cosiddette informazioni MACB

Lettera	Descrizione
M	Data e ora dell'ultima modifica
A	Data e ora dell'ultimo accesso al file
C	Data e ora dell'ultima modifica ai metadati
B	Data e ora di creazione del file

- Alcuni timestamp, relativi a un file, sono visibili, in formato user-friendly, sul tab *Dettagli*, della finestra *Proprietà*, di tale file

Le Super Timeline

Motivazioni e Caratteristiche | 3/15

ased, per ciascun file, diversi timestamp, che formazioni MACB

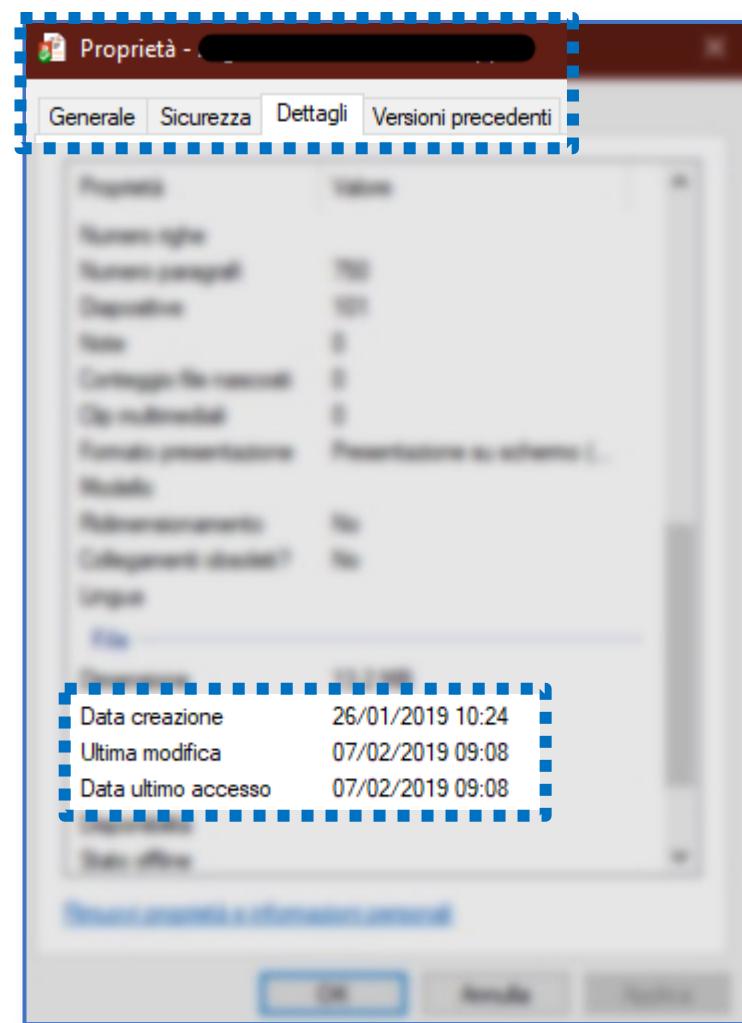
modifica

accesso al file

modifica ai metadati

e del file

- Alcuni timestamp, relativi a un file, sono visibili, in formato user-friendly, sul tab Dettagli, della finestra *Proprietà*, di tale file



Le Super Timeline

Concetti, Motivazioni e Caratteristiche | 4/15

- In alcuni casi, vengono riportate esclusivamente le cosiddette informazioni MAC
 - Nello specifico, non viene riportata la data e l'ora di creazione di un file

Lettera	Descrizione
M	Data e ora dell'ultima modifica
A	Data e ora dell'ultimo accesso al file
C	Data e ora dell'ultima modifica ai metadati

Le Super Timeline

Concetti, Motivazioni e Caratteristiche | 5/15

- I timestamp sono generalmente memorizzati nei metadati di ciascun file
- Nel file system NTFS, ad esempio, i timestamp sono memorizzati, per ciascun file, all'interno della Master File Table (MFT)
 - Tutti i file e gli oggetti memorizzati dal file system sono descritti all'interno della MFT
 - Ciascuna *entry* (detta anche *record*) della MFT contiene la descrizione di un file ed il puntatore ai dati (ovvero, il contenuto del file)
 - In caso di un file di piccole dimensioni, la entry conterrà direttamente il contenuto del file

Le Super Timeline

Concetti, Motivazioni e Caratteristiche | 6/15

Un record della MFT (*Rappresentazione Parziale*)

Standard Information	Nome del File	Security Descriptor	Data
----------------------	---------------	---------------------	------

Le Super Timeline

Concetti, Motivazioni e Caratteristiche | 7/15

Un record della MFT (*Rappresentazione Parziale*)

Standard Information	Nome del File	Security Descriptor	Data
----------------------	---------------	---------------------	------

OSSERVAZIONE

I timestamp vengono memorizzati all'interno del campo

Standard Information

Le Super Timeline

Concetti, Motivazioni e Caratteristiche | 8/15

- Utilizzando i timestamp è possibile realizzare una **timeline**
- Grazie alla timeline, gli investigatori forensi possono analizzare **l'andamento temporale degli eventi**
- Inoltre, è anche possibile **individuare eventi temporali vicini** ed effettuare, di conseguenza, delle ipotesi sulla loro eventuale correlazione
 - *Esempio*
 - Creazione di un file → Modifica di una presentazione
 - Apertura di un programma → Creazione di un documento
 - Modifica di una immagine → Modifica di un file di testo

Le Super Timeline

Concetti, Motivazioni e Caratteristiche | 9/15

- Le timeline tradizionali sono essenzialmente basate sui timestamp, specificati dal file system

Le Super Timeline

Concetti, Motivazioni e Caratteristiche | 10/15

- Le timeline tradizionali sono essenzialmente basate sui timestamp, specificati dal file system

Esempio di una semplice timeline, basata su timestamp del file system



Timestamp	Operazione	Nome del File	Note
03/03/2019 10:00	Ultimo Accesso	C:\DigFor.txt	Apertura di un file di testo
03/03/2019 10:30	Creazione	C:\DF_TEST.doc	Creazione di un documento
03/03/2019 10:45	Modifica del Contenuto	C:\DF_TEST.doc	Salvataggio del documento

Le Super Timeline

Concetti, Motivazioni e Caratteristiche | 11/15

Problemi delle Timeline Tradizionali | 1/3

- Uno dei principali problemi della timeline, basata su timestamp del file system, è che i timestamp **possono essere modificati moltissime volte da:**
 - **Utenti**
 - Anche in maniera legittima e/o involontaria (ad esempio, apertura/modifica erronea di un file)
 - **Comportamento (legittimo) del Sistema Operativo e/o di software autorizzati**
 - *Esempio 1 di 2*
 - La scansione di un certo file, da parte di un antivirus/anti-malware, farà sì che il timestamp di tale file venga alterato (data e ora dell'ultimo accesso corrispondente alla data e ora di scansione del software antivirus/anti-malware)
 - *Esempio 2 di 2*
 - Possibile accesso, da parte del sistema operativo a file (talvolta poco interessanti dal punto di vista forense), per via di una ricerca effettuata dall'utente

Le Super Timeline

Concetti, Motivazioni e Caratteristiche | 11/15

Problemi delle Timeline Tradizionali | 2/3

- Alcuni sistemi operativi, per ragioni legate principalmente alle performance, potrebbero NON effettuare sempre l'aggiornamento della data e dell'ora relativa all'ultimo accesso di un file
- In Windows, mediante una modifica al registro di sistema, è possibile disabilitare completamente l'aggiornamento della data ed ora dell'ultimo accesso di un file
 - Anche in Linux è possibile specificare l'opzione noatime, del comando mount, che disabilita l'aggiornamento delle suddette informazioni (tale opzione può anche essere resa permanente)

Le Super Timeline

Concetti, Motivazioni e Caratteristiche | 11/15

Problemi delle Timeline Tradizionali | 3/3

- Inoltre, il fatto di basarsi esclusivamente sui timestamp del file system, non indica il contesto (o lo indica parzialmente)
 - *Esempio*
 - Un file potrebbe essere ripetutamente acceduto dal sistema operativo (ad esempio, file di *log* di sistema/servizi/programmi), per svariate ragioni

Le Super Timeline

Concetti, Motivazioni e Caratteristiche | 11/15

Problemi delle Timeline Tradizionali | 3/3

- Inoltre, il fatto di basarsi esclusivamente sui timestamp del file system, non indica il contesto (o lo indica parzialmente)
 - *Esempio*
 - Un file potrebbe essere ripetutamente acceduto dal sistema operativo (ad esempio, file di *log* di sistema/servizi/programmi), per svariate ragioni

OSSERVAZIONE IMPORTANTE

- È possibile notare come i timestamp del file system abbiano una natura potenzialmente poco attendibile
- Ciò potrebbe portare gli investigatori a realizzare una timeline non corretta o parzialmente alterata

Le Super Timeline

Concetti, Motivazioni e Caratteristiche | 12/15

Tecniche Anti-Forensi per l'alterazione dei Timestamp

- Come qualsiasi dato digitale, il valore del timestamp (del file system) può essere alterato maliziosamente, tramite appositi tool
 - Ad esempio, tramite dei tool specifici, è possibile modificare il campo **Standard Information** di un record della MFT (File System NTFS)
- Esistono poi altre tecniche anti-forensi in grado di alterare i timestamp

Le Super Timeline

Concetti, Motivazioni e Caratteristiche | 13/15

Tecniche Anti-Forensi per l'alterazione dei Timestamp

- Come qualsiasi dato digitale, il valore del timestamp (del file system) può essere alterato maliziosamente, tramite appositi tool
 - Ad esempio, tramite dei tool specifici, è possibile modificare il campo **Standard Information** di un record della MFT (File System NTFS)
- Esistono poi altre tecniche anti-forensi in grado di alterare i timestamp

OSSERVAZIONE IMPORTANTE

A causa delle tecniche anti-forensi, è estremamente importante che gli investigatori abbiano accesso a informazioni da più punti, per validare/confutare il risultato ottenuto

Le Super Timeline

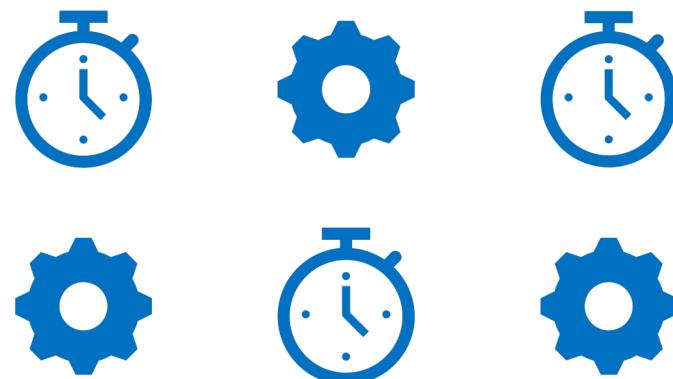
Concetti, Motivazioni e Caratteristiche | 14/15

- Una possibile soluzione ai problemi identificati precedentemente è quella di estendere la timeline, arricchendola con informazioni provenienti da più fonti
- In tal modo, è possibile avere un quadro più chiaro e minimizzare anche l'eventuale impatto ottenuto dall'utilizzo di tecniche anti-forensi
 - Infatti, è estremamente più difficile, tramite tecniche anti-forensi, alterare tutte le informazioni ottenute da diverse fonti

Le Super Timeline

Concetti, Motivazioni e Caratteristiche | 15/15

- La **super timeline** è una estensione della timeline, che prevede l'inclusione di diverse informazioni, provenienti da diverse fonti, fra cui:
 - File di log (del sistema operativo, ecc.)
 - Metadati del file system
 - Registro di sistema (sistemi Windows-based)
 - Ecc.



Le Super Timeline

Il framework Plaso | 1/2

- Il framework **plaso** (*Plaso Langar Að Safna Öllu*, dall'islandese, letteralmente, *Plaso vuole raccogliere tutto*) è un tool per la realizzazione di super timeline
- È scritto in Python ed è Open-Source, disponibile per diverse piattaforme
 - Linux
 - Windows
 - macOS/OS X
- Essenzialmente, **Plaso** è una nuova «implementazione» (*riscrittura*) del back-end di un altro framework, ovvero, il framework **log2timeline**
- Scaricabile dal seguente link:
 - <https://github.com/log2timeline/plaso/releases>

Le Super Timeline

Il framework Plaso | 1/2

- Il framework **plaso** (*Plaso Langar Að Safna Öllu*, dall'islandese, letteralmente, *Plaso vuole raccogliere tutto*) è un tool per la realizzazione di super timeline
- È scritto in Python ed è Open-Source, disponibile per

OSSERVAZIONE

Plaso necessita dell'installazione di Python, in versione 2.7 oppure 3.6 (in base alla versione scaricata), inoltre, sono necessari ulteriori moduli [Suggerito l'utilizzo su sistemi Windows-based]

- Scaricabile dal seguente link:
 - <https://github.com/log2timeline/plaso/releases>

Le Super Timeline

Il framework Plaso | 2/2

- Plaso supporta tantissimi formati di input

Supported Formats

The information below is based of version 1.4.0

Storage Media Image File Formats

Storage Media Image File Format support is provided by [dfvfs](#).

Volume System Formats

Volume System Format support is provided by [dfvfs](#).

File System Formats

File System Format support is provided by [dfvfs](#).

File formats

- [Apple System Log \(ASL\)](#)
- Android usage-history (app usage)
- [Basic Security Module \(BSM\)](#)
- Bencode files
- [Chrome cache files](#)
- Chrome preferences file
- CUPS IPP

Elenco parziale dei formati supportati da Plaso

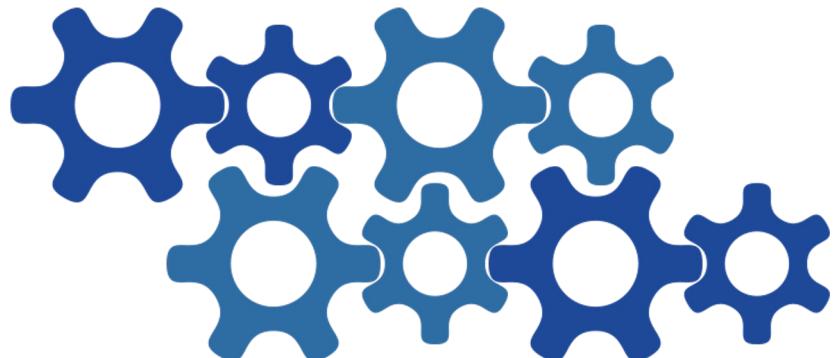
La lista completa è accessibile dal link in Fonte

Fonte: <http://www.forensicswiki.org/wiki/Plaso>

Le Super Timeline

Architettura di Plaso | Componenti

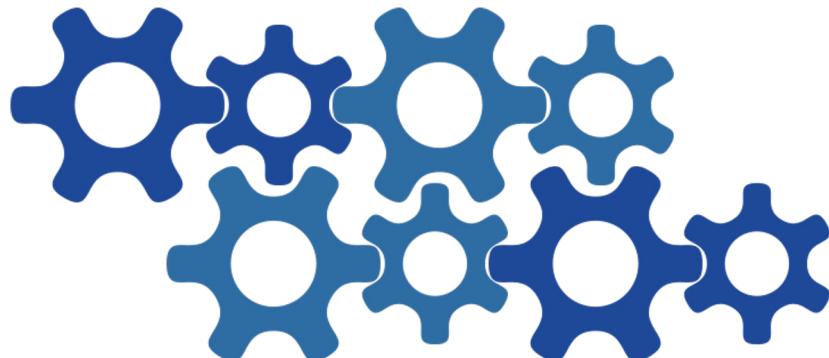
- Plaso presenta un'architettura, suddivisa in **quattro componenti principali**, indipendenti:
 - Preprocessing
 - Collection
 - Worker
 - Storage



Le Super Timeline

Architettura di Plaso | Componenti

- Plaso presenta un'architettura, suddivisa in **quattro componenti principali**, indipendenti:
 - Preprocessing
 - Collection
 - Worker
 - Storage



Le Super Timeline

Architettura di Plaso | Preprocessing

- L'attività di **preprocessing** è svolta preliminarmente da Plaso e si occupa di reperire alcune informazioni, in relazione a quelle che saranno le fasi successive
- Alcune delle informazioni reperite:
 - Versione del Sistema Operativo
 - Informazioni sul fuso orario (*timezone*)
 - Eventuale nome della macchina (*hostname*)
 - Determinare le applicazioni di default (ad esempio, browser di default, ecc.)
 - Determinare gli utenti e l'eventuale path associato ad essi

Le Super Timeline

Architettura di Plaso | Componenti

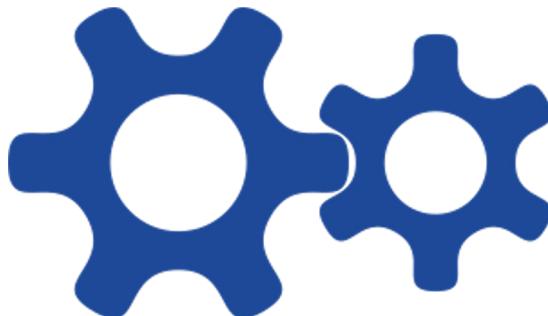
- Plaso presenta un'architettura, suddivisa in **quattro componenti principali**, indipendenti:
 - Preprocessing
 - **Collection**
 - Worker
 - Storage



Le Super Timeline

Architettura di Plaso | Collection

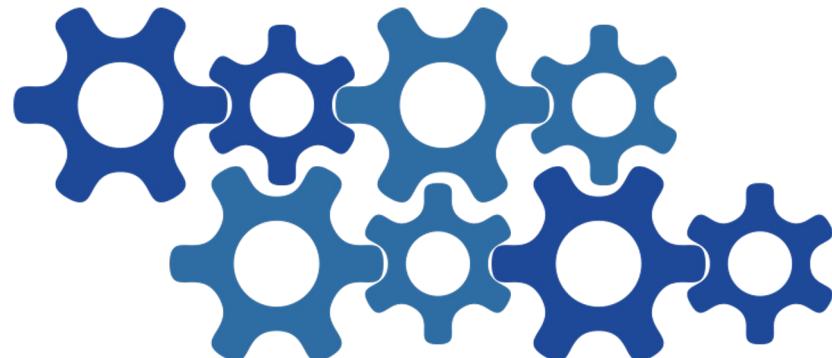
- Nell'attività di **collection**, invece, vengono individuati tutti i file, che dovranno essere elaborati, nelle fasi successive



Le Super Timeline

Architettura di Plaso | Componenti

- Plaso presenta un'architettura, suddivisa in **quattro componenti principali**, indipendenti:
 - Preprocessing
 - Collection
 - **Worker**
 - **Storage**



Le Super Timeline

Architettura di Plaso | Worker & Storage



- I **worker** costituiscono l'elemento chiave di Plaso, infatti, elaborano ciascun file della lista degli input, individuata precedentemente (attività di collection)
- Nello specifico, un worker si occuperà di determinare, in primo luogo, la tipologia del file e, successivamente, svolgerà diverse attività



Le Super Timeline

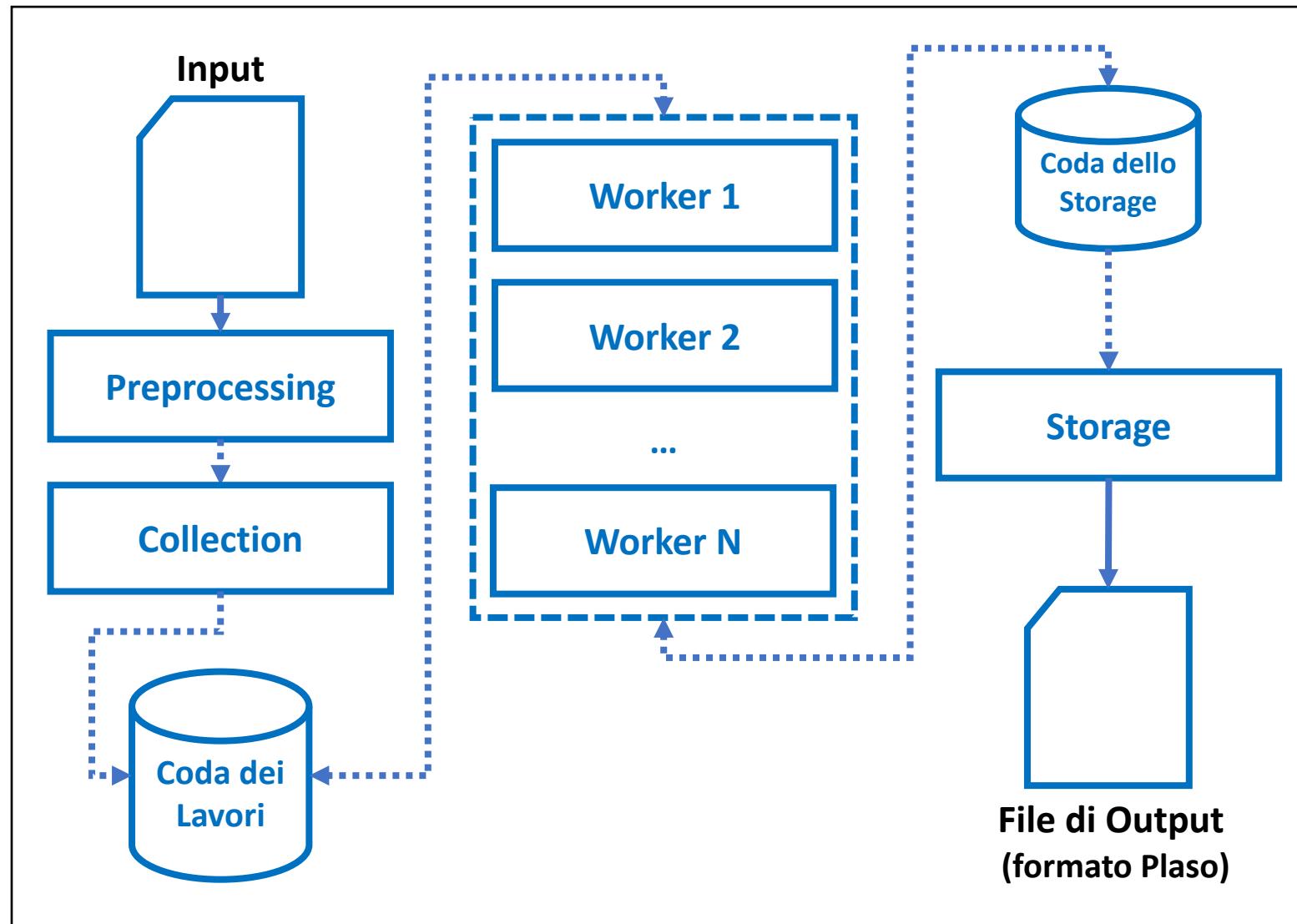
Architettura di Plaso | Worker & Storage

Alcune attività svolte da un Worker

- Determinare quale *parser* dovrà essere applicato al file
 - Il *parser* è in grado di elaborare un determinato file, in base alla sua struttura
- Elaborare il file, con il parser adeguato
- Applicare alcuni filtri predefiniti al file
- Inviare le informazioni estratte alla componente di **storage**
 - La componente di **storage**, si occupa della costruzione/memorizzazione del file di output, in accordo alle specifiche fornite
- Determinare eventualmente se si sta elaborando un archivio, il quale potrebbe contenere, al suo interno, dei file che devono essere elaborati

Le Super Timeline

Architettura di Plaso | Rappresentazione Grafica



Le Super Timeline

Tool di Plaso | 1/15

- Plaso mette a disposizione diversi tool, utilizzabili da linea di comando

`log2timeline`

`pinfo`

`pprof`

`preg`

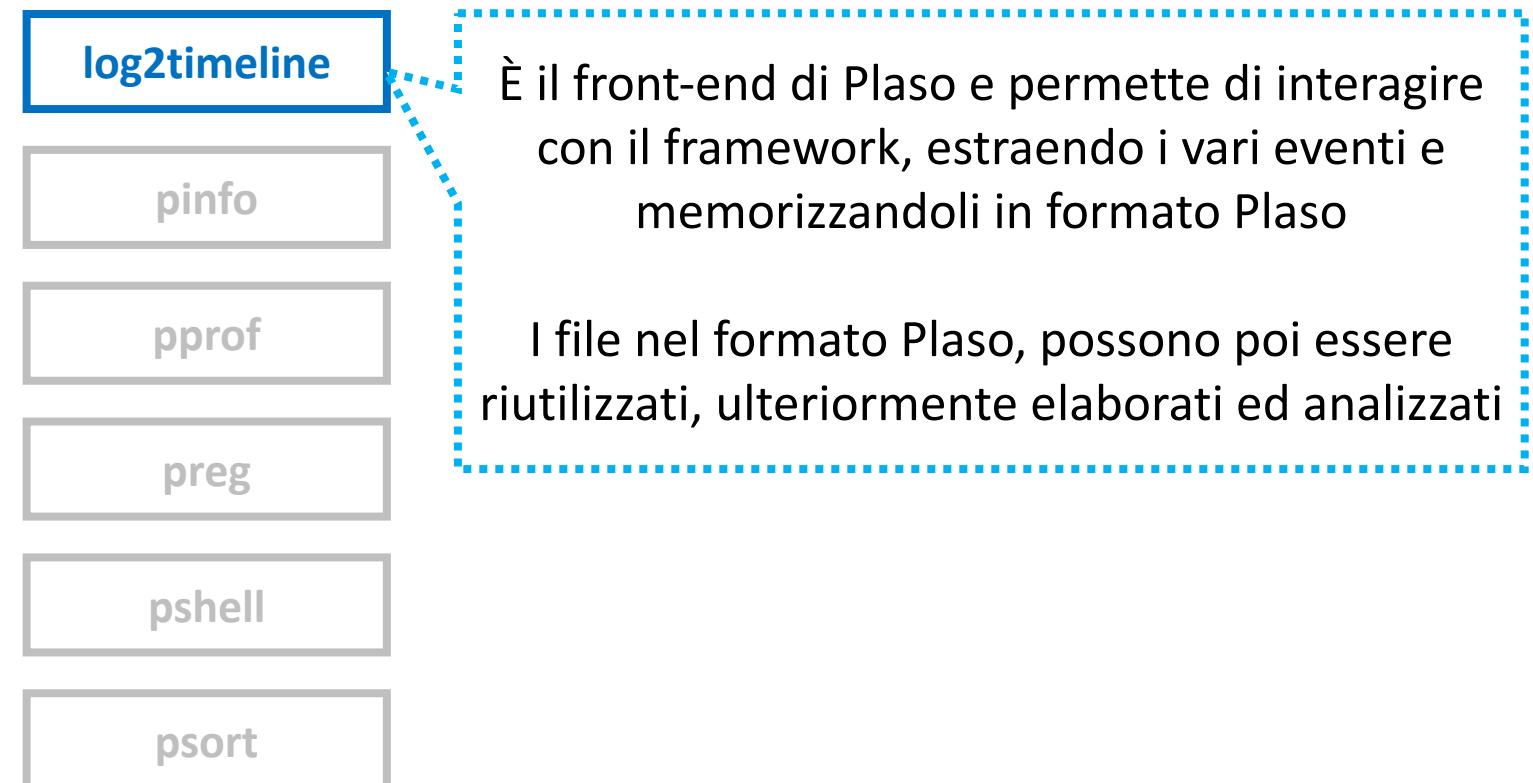
`pshell`

`psort`

Le Super Timeline

Tool di Plaso | 2/15

- Plaso mette a disposizione diversi tool, utilizzabili da linea di comando



Le Super Timeline

Tool di Plaso | 3/15

- Plaso mette a disposizione diversi tool, utilizzabili da linea di comando

log2timeline

pinfo

pprof

preg

pshell

psort

Semplice tool che permette di estrarre e visualizzare informazioni contenute all'interno di un file, in formato Plaso

Le Super Timeline

Tool di Plaso | 4/15

- Plaso mette a disposizione diversi tool, utilizzabili da linea di comando

log2timeline

pinfo

pprof

preg

pshell

psort

Serve soprattutto per gli sviluppatori, al fine di ottimizzare determinati parser

Le Super Timeline

Tool di Plaso | 5/15

- Plaso mette a disposizione diversi tool, utilizzabili da linea di comando

log2timeline

pinfo

pprof

preg

pshell

psort

Fornisce un front-end diverso dedicato alla gestione dei parser del registro di sistema dei sistemi Windows-based

Permette anche di ottenere informazioni sul registro, partendo da una sua sotto-chiave

Le Super Timeline

Tool di Plaso | 6/15

- Plaso mette a disposizione diversi tool, utilizzabili da linea di comando

log2timeline

pinfo

pprof

preg

pshell

psort

Terminale (basato su Python) per l'interazione
con il back-end di Plaso, permette l'analisi
avanzata tramite l'accesso a tutte le librerie di
Plaso

Le Super Timeline

Tool di Plaso | 7/15

- Plaso mette a disposizione diversi tool, utilizzabili da linea di comando

log2timeline

pinfo

pprof

preg

pshell

psort

Importante tool che effettua la conversione dal formato Plaso (non human-readable) a diversi formati, che possono essere visualizzati e post elaborati (eventualmente con tool esterni, come, ad esempio, Microsoft Excel, ecc.)

Le Super Timeline

Tool di Plaso | 8/15

- Plaso mette a disposizione diversi tool, utilizzabili da linea di comando



Ci focalizzeremo principalmente sui
tool **log2timeline** e **psort**

Le Super Timeline

Tool di Plaso | 9/15

- Sintassi Semplificata (*Descrizione*) di **log2timeline**

```
log2time [STORAGE_FILE] [SOURCE]
```

Le Super Timeline

Tool di Plaso | 9/15

- Sintassi Semplificata (*Descrizione*) di **log2timeline**

```
log2time [STORAGE_FILE] [SOURCE]
```

- **[STORAGE_FILE]**: Permette di specificare il percorso del **file di output**
 - **OSSERVAZIONE**: il file di output, verrà memorizzato in formato Plaso

Le Super Timeline

Tool di Plaso | 9/15

- Sintassi Semplificata (*Descrizione*) di **log2timeline**

```
log2time [STORAGE_FILE] [SOURCE]
```

- **[STORAGE_FILE]**: Permette di specificare il percorso del **file di output**
 - **OSSERVAZIONE**: il file di output, verrà memorizzato in formato Plaso
- **[SOURCE]** : Permette di specificare l'**input da elaborare** (l'input deve essere in uno dei formati supportati)

Le Super Timeline

Tool di Plaso | 10/15

- Sintassi Completa di **log2timeline**

```
usage: log2timeline [-h] [-V] [--artifact_definitions PATH]
                    [--custom_artifact_definitions PATH] [--data PATH]
                    [--artifact_filters ARTIFACT_FILTERS]
                    [--artifact_filters_file PATH] [--preferred_year YEAR]
                    [--process_archives] [--skip_compressed_streams]
                    [-f FILE_FILTER] [--hasher_file_size_limit SIZE]
                    [--hashers HASHER_LIST] [--parsers PARSER_LIST]
                    [--yara_rules PATH] [--partitions PARTITIONS]
                    [--volumes VOLUMES] [-z TIMEZONE] [--no_vss] [--vss_only]
                    [--vss_stores VSS_STORES] [--credential TYPE:DATA] [-d]
                    [-q] [--info] [--use_markdown] [--no_dependencies_check]
                    [--logfile FILENAME] [--status_view TYPE] [-t TEXT]
                    [--buffer_size BUFFER_SIZE] [--queue_size QUEUE_SIZE]
                    [--single_process] [--temporary_directory DIRECTORY]
                    [--worker_memory_limit SIZE] [--workers WORKERS]
                    [--disable_zeromq] [--sigsegv_handler]
                    [--profilers PROFILERS_LIST]
                    [--profiling_directory DIRECTORY]
                    [--profiling_sample_rate SAMPLE_RATE]
                    [--storage_format FORMAT]
                    [STORAGE_FILE] [SOURCE]
```

- Viene mostrata quando viene avviato il comando **log2timeline**, senza alcun argomento

Le Super Timeline

Tool di Plaso | 11/15

```
log2timeline -h
```

- Schermata (*parziale*) di help (opzione `-h`), del comando di **log2timeline**
 - Parte 1 di 3

```
More information can be gathered from here:  
https://plaso.readthedocs.io/en/latest/sources/user/Using-log2timeline.html

positional arguments:  
  STORAGE_FILE      Path to a storage file.  
  SOURCE            Path to a source device, file or directory. If the  
                    source is a supported storage media device or image  
                    file, archive file or a directory, the files within  
                    are processed recursively.

optional arguments:  
  -h, --help          Show this help message and exit.  
  -V, --version       Show the version information.
```

Le Super Timeline

Tool di Plaso | 12/15

```
log2timeline -h
```

- Schermata (*parziale*) di help (opzione `-h`), del comando di **log2timeline**
 - Parte 2 di 3

```
optional arguments:
  -h, --help            Show this help message and exit.
  -V, --version         Show the version information.

data location arguments:
  --artifact_definitions PATH, --artifact-definitions PATH
                        Path to a directory containing artifact definitions,
                        which are .yaml files. Artifact definitions can be
                        used to describe and quickly collect data of interest,
                        such as specific files or Windows Registry keys.
  --custom_artifact_definitions PATH, --custom-artifact-definitions PATH
                        Path to a file containing custom artifact definitions,
                        which are .yaml files. Artifact definitions can be
                        used to describe and quickly collect data of interest,
                        such as specific files or Windows Registry keys.
  --data PATH           Path to a directory containing the data files.
```

Le Super Timeline

Tool di Plaso | 13/15

```
log2timeline -h
```

- Schermata (*parziale*) di help (opzione `-h`), del comando di **log2timeline**
 - Parte 3 di 3

```
extraction arguments:  
  --artifact_filters ARTIFACT_FILTERS, --artifact-filters ARTIFACT_FILTERS  
      Names of forensic artifact definitions, provided on  
      the command command line (comma separated). Forensic  
      artifacts are stored in .yaml files that are directly  
      pulled from the artifact definitions project. You can  
      also specify a custom artifacts yaml file (see  
      --custom_artifact_definitions). Artifact definitions  
      can be used to describe and quickly collect data of  
      interest, such as specific files or Windows Registry  
      keys.  
  --artifact_filters_file PATH, --artifact-filters_file PATH  
      Names of forensic artifact definitions, provided in a  
      file with one artifact name per line. Forensic  
      artifacts are stored in .yaml files that are directly  
      pulled from the artifact definitions project. You can  
      also specify a custom artifacts yaml file (see  
      --custom_artifact_definitions). Artifact definitions  
      can be used to describe and quickly collect data of  
      interest, such as specific files or Windows Registry  
      keys.
```

Le Super Timeline

Tool di Plaso | 14/15

- Sintassi Semplificata (*Descrizione*) di **psort**

```
psort [STORAGE_FILE] -o FORMATO -w OUTPUT
```

Le Super Timeline

Tool di Plaso | 14/15

- Sintassi Semplificata (*Descrizione*) di **psort**

```
psort [STORAGE_FILE] -o FORMATO -w OUTPUT
```

- **[STORAGE_FILE]**: Permette di specificare il percorso del **file di input**
 - **OSSERVAZIONE**: il file di input (**N.B.** Non di output, come per il comando `log2timeline`), deve necessariamente essere memorizzato in formato Plaso

Le Super Timeline

Tool di Plaso | 14/15

- Sintassi Semplificata (*Descrizione*) di **psort**

```
psort [STORAGE_FILE] -o FORMATO -w OUTPUT
```

- **[STORAGE_FILE]**: Permette di specificare il percorso del file di input
 - **OSSERVAZIONE**: il file di input (**N.B.** Non di output, come per il comando `log2timeline`), deve necessariamente essere memorizzato in formato Plaso
- **-o**: Con l'opzione **-o**, è possibile specificare il formato (FORMATO) di output
 - **OSSERVAZIONE**: `psort` supporta tantissimi formati di output, i quali sono visibili con il seguente comando:

```
psort -o list
```

Le Super Timeline

Tool di Plaso | 15/15

```
***** Output Modules *****
Name : Description
-----
l2tcsv : CSV format used by legacy log2timeline, with 17 fixed fields.
    xlsx : Excel Spreadsheet (XLSX) output
l2tln : Extended TLN 7 field | delimited output.
elastic : Saves the events into an Elasticsearch database.
4n6time_sqlite : Saves the data in a SQLite database, used by the tool 4n6time.
    kml : Saves events with geography data into a KML format.
dynamic : Dynamic selection of fields for a separated value output
format.
rawpy : "raw" (or native) Python output.
json : Saves the events into a JSON format.
json_line : Saves the events into a JSON line format.
null : Output module that does not output anything.
tln : TLN 5 field | delimited output.
elastic5 : Saves the events into an Elasticsearch5 database.
```

visibili con il comando:

```
psort -o list
```

Le Super Timeline

Tool di Plaso | 15/15

- Sintassi Semplificata (*Descrizione*) di **psort**

```
psort [STORAGE_FILE] -o FORMATO -w OUTPUT
```

- **[STORAGE_FILE]**: Permette di specificare il percorso del **file di input**
 - **OSSERVAZIONE**: il file di input (**N.B.** Non di output, come per il comando `log2timeline`), deve necessariamente essere memorizzato in formato Plaso
 - **-o**: Con l'opzione **-o**, è possibile specificare il **formato (FORMATO)** di output
 - **OSSERVAZIONE**: `psort` supporta tantissimi formati di output, i quali sono visibili con il seguente comando:
- **-w**: Con l'opzione **-w**, è possibile specificare il percorso del **file di output (OUTPUT)**

Le Super Timeline

Esempi di Utilizzo

1

Esempio di Utilizzo 1
Cronologia Browser Chrome

2

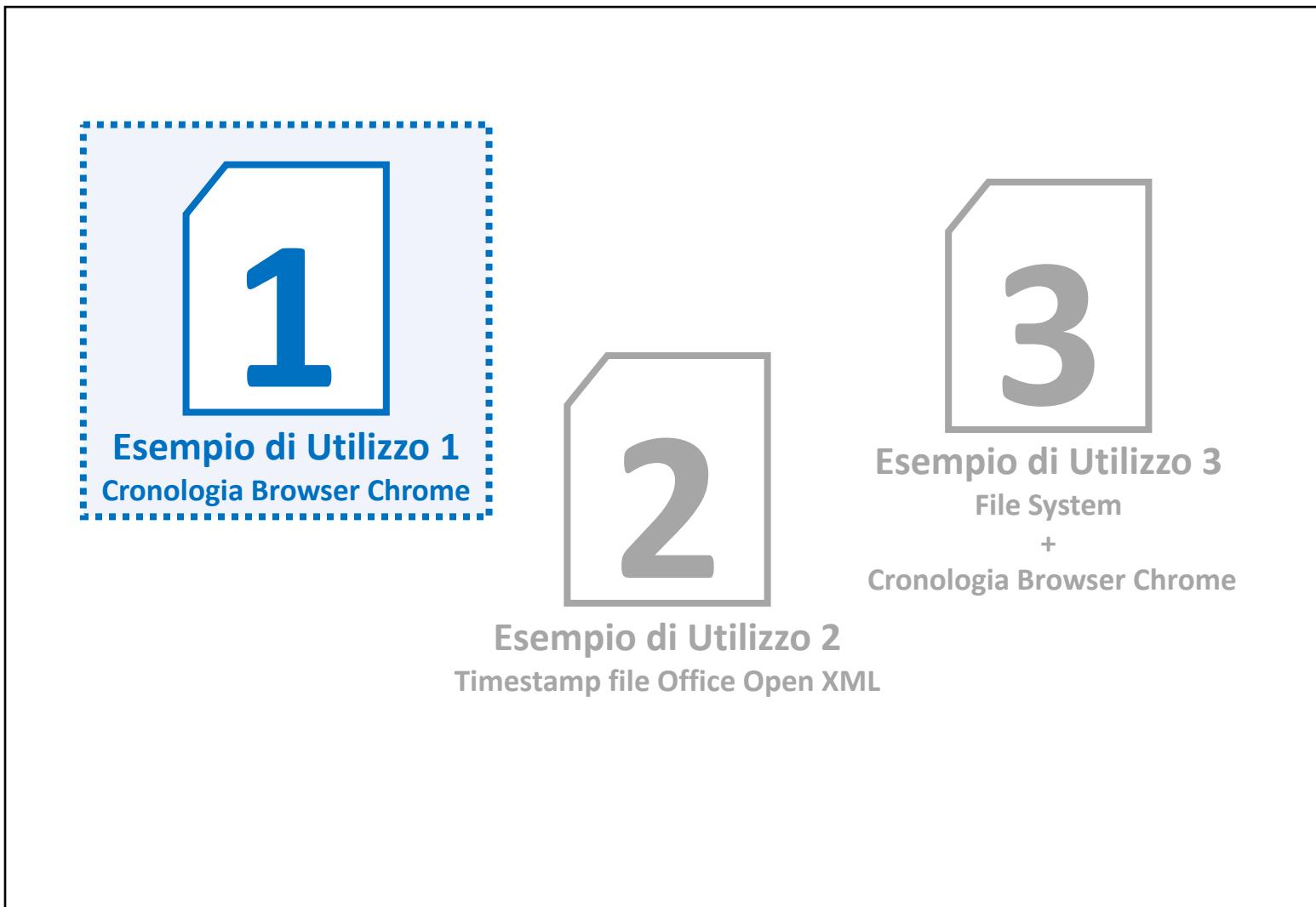
Esempio di Utilizzo 2
Timestamp file Office Open XML

3

Esempio di Utilizzo 3
File System
+
Cronologia Browser Chrome

Le Super Timeline

Esempi di Utilizzo



Le Super Timeline

Esempi di Utilizzo

1

Esempio di Utilizzo 1
Cronologia Browser Chrome

2

Esempio di Utilizzo 3
File System
+
Cronologia Browser Chrome

L'analisi della timeline della cronologia del browser, è molto importante dal punto di vista forense, per avere un quadro più chiaro sulle attività effettuate tramite il Web

Esempio di Utilizzo 2
File Open XML

Le Super Timeline

Esempio di Utilizzo 1 | Cronologia Chrome | 1/30

1. Il primo passo consiste nel fornire in input il file, relativo alla cronologia di Google Chrome, di cui si intende analizzare la timeline al fine di ottenere, in output, un file in formato Plaso

Le Super Timeline

Esempio di Utilizzo 1 | Cronologia Chrome | 2/30

- Il primo passo consiste nel fornire in input, il file, relativo alla cronologia di Google Chrome, di cui si intende analizzare la timeline al fine di ottenere, in output, un file, in formato Plaso

Nei sistemi Windows-based, il file relativo alla cronologia di Google Chrome, è denominato `History` ed il percorso tipico, ove esso risiede, è il seguente:

C:\Users\<NomeUtente>\AppData\Local\Google\Chrome\User
Data\Default

Dove `<NomeUtente>` deve essere sostituito con il nome dell'utente di cui si intende reperire la cronologia (**NOTA:** In tale percorso, la cartella `AppData` è generalmente una cartella nascosta)

Ulteriori dettagli ed informazioni sul file della cronologia di Chrome sono reperibili al seguente link: http://www.forensicswiki.org/wiki/Google_Chrome

Le Super Timeline

Esempio di Utilizzo 1 | Cronologia Chrome | 3/30

1. Il primo passo consiste nel fornire in input, il file, relativo alla cronologia di Google Chrome, di cui si intende analizzare la timeline, al fine di ottenere, in output, un file, in formato Plaso

OSSERVAZIONE IMPORTANTE | 1/3

È possibile effettuare il mounting di una immagine forense precedentemente acquisita, su un drive «virtuale» ed accedere al contenuto dell'immagine forense stessa. Il mounting viene tipicamente effettuato in modalità di sola lettura (read only), per evitare qualsiasi rischio di alterazione

Ad esempio, sui sistemi Windows-based è possibile effettuare il mounting di una immagine forense su un drive «*virtuale*», a cui viene associato un riferimento logico, costituito da una lettera (a patto che tale lettera non sia già utilizzata dal S.O.)

Esempio: Supponendo di aver effettuato il mounting, in un sistema Windows-based, di una immagine forense su un drive «*virtuale*» identificato dalla lettera **E**, sarà quindi possibile accedere ad un file (contenuto nell'immagine forense) tramite un percorso di questo tipo: **E:\Cartella5\Pippo.txt**

Le Super Timeline

Esempio di Utilizzo 1 | Cronologia Chrome | 3/30

1. Il primo passo consiste nel fornire in input, il file, relativo alla cronologia di Google Chrome, di cui si intende analizzare la timeline al fine di ottenere, in output, un file, in formato Plaso

OSSERVAZIONE IMPORTANTE | 2/3

Anche Plaso potrà quindi accedere (specificando adeguatamente il percorso) al file History (o ad eventuali altri file di interesse), memorizzati nella immagine forense di cui si è effettuato il mounting su un drive «virtuale»

In questo *Esempio di Utilizzo*, accederemo al file, relativo alla cronologia del browser Google Chrome, da un drive «virtuale» (identificato dalla lettera E:) su cui si è effettuato il mounting, in sola lettura, dell'immagine forense contenente la cronologia da analizzare

```
log2timeline CronologiaChrome.plaso "E:\Users\[\...]\History"
```

Le Super Timeline

Esempio di Utilizzo 1 | Cronologia Chrome | 3/30

1. Il primo passo consiste nel fornire in input, il file, relativo alla cronologia di Google Chrome, di cui si intende analizzare la timeline, al fine di ottenere, in output, un file, in formato Plaso

OSSERVAZIONE IMPORTANTE | 3/3

È sempre fortemente consigliato l'accesso ai file, dal drive «virtuale», su cui si è effettuato il mounting dell'immagine forense, in modalità di sola lettura, per evitare qualsiasi alterazione

NOTA: Il mounting di immagini forensi può essere utile per diversi tool forensi

Le Super Timeline

Esempio di Utilizzo 1 | Cronologia Chrome | 4/30

1. Il primo passo consiste nel fornire in input, il file, relativo alla cronologia di Google Chrome, di cui si intende analizzare la timeline al fine di ottenere, in output, un file, in formato Plaso

```
log2timeline CronologiaChrome.plaso "E:\[...]\\History"
```

Le Super Timeline

Esempio di Utilizzo 1 | Cronologia Chrome | 4/30

- Il primo passo consiste nel fornire in input, il file, relativo alla cronologia di Google Chrome, di cui si intende analizzare la timeline al fine di ottenere, in output, un file, in formato Plaso

```
log2timeline CronologiaChrome.plaso "E:\[...]\History"
```

Per brevità, il percorso completo, è stato omesso ed è il seguente:

E:\Users\Raffaele\AppData\Local\Google\Chrome\User Data\Default\History

Le Super Timeline

Esempio di Utilizzo 1 | Cronologia Chrome | 4/30

1. Il primo passo consiste nel fornire in input, il file, relativo alla cronologia di Google Chrome, di cui si intende analizzare la timeline al fine di ottenere, in output, un file, in formato Plaso

```
log2timeline CronologiaChrome.plaso "E:\[...]\\History"
```

Plaso è in grado, automaticamente, mediante il preprocessing, di riconoscere il formato del file ed analizzarlo correttamente

Le Super Timeline

Esempio di Utilizzo 1 | Cronologia Chrome | 5/30

- Il primo passo consiste nel fornire in input, il file, relativo alla cronologia di Google Chrome, di cui si intende analizzare la timeline al fine di ottenere, in output, un file, in formato Plaso

```
log2timeline CronologiaChrome.plaso "E:\[...]\\History"
```

Output (Parziale) del comando log2timeline

```
2019-04-09 17:09:52,914 [INFO] DETERMINED_ARTIFACTS_INVESTIGATED [Determined artifacts]
users\Raffaele\Plaso\artifacts
Checking availability and versions of dependencies.
[OPTIONAL]      missing: lz4.
[OPTIONAL]      missing: lzma.
[OK]

Source path      : E:\Users\Raffaele\AppData\Local\Google\Chrome\User Data\Default\History
Source type     : single file
Processing time : 00:00:00

Processing started.
Processing completed.
```

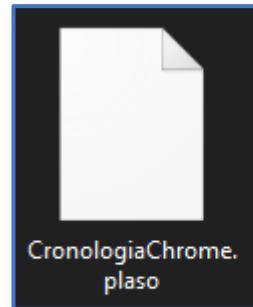
Le Super Timeline

Esempio di Utilizzo 1 | Cronologia Chrome | 5/30

- Il primo passo consiste nel fornire in input, il file, relativo alla cronologia di Google Chrome, di cui si intende analizzare la timeline al fine di ottenere, in output, un file, in formato Plaso

```
log2timeline CronologiaChrome.plaso "E:\[...]\\History"
```

File Prodotto (~64 KB)



Le Super Timeline

Per completezza, utilizzeremo anche il comando **pinfo**, il quale mostra informazioni in merito ad un file, in formato Plaso (nel nostro esempio, CronologiaChrome.plaso)

pinfo CronologiaChrome.paso

*Output (parziale) del comando **pinfo** sul file in formato Plaso | 1/3*

Le Super Timeline

Esempio di Utilizzo 1 | Cronologia Chrome | 6/30

Per completezza, utilizzeremo anche il comando **pinfo**, il quale mostra informazioni in merito ad un file, in formato Plaso (nel nostro esempio, CronologiaChrome.plaso)

```
pinfo CronologiaChrome.plaso
```

*Output (parziale) del comando **pinfo** sul file in formato Plaso | 2/3*

```
plist/macOSX_install_history, plist/macuser,
plist/maxos_software_update, plist/plist_default,
plist/safari_history, plist/spotlight,
plist/spotlight_volume, plist/time_machine,
pls_recall, popularity_contest, prefetch,
recycle_bin, recycle_bin_info2, rplog, santa,
sccm, selinux, skydrive_log, skydrive_log_old,
sophos_av, sqlite, sqlite/android_calls,
sqlite/android_sms, sqlite/android_webview,
sqlite/android_webviewcache, sqlite/appusage,
sqlite/chrome_27_history, sqlite/chrome_8_history,
sqlite/chrome_autofill, sqlite/chrome_cookies,
sqlite/chrome_extension_activity,
sqlite/firefox_cookies, sqlite/firefox_downloads,
sqlite/firefox_history, sqlite/google_drive,
sqlite/hangouts_messages, sqlite/imessage,
sqlite/kik_messenger, sqlite/kodi,
sqlite/ls_quarantine,
sqlite/mac_document_versions,
sqlite/mac_notificationcenter,
sqlite/mackeeper_cache, sqlite/safari_history,
sqlite/skvne, sqlite/tango_android_profile.
```

Le Super Timeline

Esempio di Utilizzo 1 | Cronologia Chrome | 6/30

Per completezza, utilizzeremo anche il comando **pinfo**, il quale mostra informazioni in merito ad un file, in formato Plaso (nel nostro esempio, CronologiaChrome.plaso)

```
pinfo CronologiaChrome.plaso
```

*Output (parziale) del comando **pinfo** sul file in formato Plaso | 3/3*

```
***** Events generated per parser *****
Parser (plugin) name : Number of events
-----
    chrome_27_history : 20
        filestat : 3
            Total : 23
-----
No errors stored.
No analysis reports stored.
```

Le Super Timeline

Esempio di Utilizzo 1 | Cronologia Chrome | 7/30

2. Tramite **psort** è possibile convertire il file in formato Plaso (non *human-readable*), in un formato human-readable, ad esempio, il formato XLSX, leggibile da Microsoft Excel (o altri software, come OpenOffice, ecc.)

```
psort CronologiaChrome.plaso -o XLSX -w CronologiaChrome.xlsx
```

Le Super Timeline

Esempio di Utilizzo 1 | Cronologia Chrome | 8/30

- Tramite **psort** è possibile convertire il file in formato Plaso (non *human-readable*), in un formato human-readable, ad esempio, il formato XLSX, leggibile da Microsoft Excel (o altri software, come OpenOffice, ecc.)

```
psort CronologiaChrome.plaso -o XLSX -w CronologiaChrome.xlsx
```

Output del comando psort

```
C:\Users\Raffaele\Plaso>psort CronologiaChrome.plaso -o XLSX -w CronologiaChrome.xlsx
2019-02-08 23:13:33,904 [INFO] (MainProcess) PID:2684 <data_location> Determined data location: C:\Users\Raffaele\Plaso\data
2019-02-08 23:13:33,904 [WARNING] (MainProcess) PID:2684 <psort_tool> Appending to an already existing storage file.
Processing completed.

***** Export results *****
Events processed : 23
Events MACB grouped : 3
Events filtered : 0
Events from time slice : 0
-----
C:\Users\Raffaele\Plaso>
```

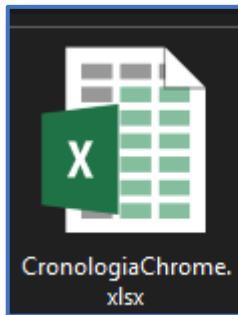
Le Super Timeline

Esempio di Utilizzo 1 | Cronologia Chrome | 9/30

- Tramite **psort** è possibile convertire il file in formato Plaso (non *human-readable*), in un formato human-readable, ad esempio, il formato XLSX, leggibile da Microsoft Excel (o altri software, come OpenOffice, ecc.)

```
psort CronologiaChrome.plaso -o XLSX -w CronologiaChrome.xlsx
```

File Prodotto (~7 KB)



Le Super Timeline

Esempio di Utilizzo 1 | Cronologia Chrome | 10/30

3. Analisi del File Prodotto (CronologiaChrome.xlsx)

Le Super Timeline

Esempio di Utilizzo 1 | Cronologia Chrome | 11/30

3. Analisi del File Prodotto (CronologiaChrome.xlsx)

datetime	timestamp_desc	source	source_long	message	parser	display_name
2019-02-08 09:20:11,298	Last Visited Time	WEBHIST	Chrome History	http://www.google.it/ (Google) [count: 0] Visit from: http://sqlite/chrome_27_history	OS:E:\Users\Raffaele\AppData\Local\G	
2019-02-08 09:20:11,298	Last Visited Time	WEBHIST	Chrome History	https://www.google.it/?gws_rd=ssl (Google) [count: 0] Visit sqlite/chrome_27_history	OS:E:\Users\Raffaele\AppData\Local\G	
2019-02-08 09:20:11,298	Last Visited Time	WEBHIST	Chrome History	http://google.it/ (Google) [count: 1] Type: [TYPED - User typed] sqlite/chrome_27_history	OS:E:\Users\Raffaele\AppData\Local\G	
2019-02-08 09:20:15,570	Last Visited Time	WEBHIST	Chrome History	https://www.google.it/search?source=hp&ei=yOldXJbgHYyFsqlite/chrome_27_history	OS:E:\Users\Raffaele\AppData\Local\G	
2019-02-08 09:20:18,890	Last Visited Time	WEBHIST	Chrome History	https://www.unisa.it/ (UNISA Home) [count: 0] Type: [LINK] sqlite/chrome_27_history	OS:E:\Users\Raffaele\AppData\Local\G	
2019-02-08 09:20:29,302	Last Visited Time	WEBHIST	Chrome History	https://www.unisa.it/unisa-rescue-page/search/id/529/url/sqlite/chrome_27_history	OS:E:\Users\Raffaele\AppData\Local\G	
2019-02-08 09:20:33,879	Last Visited Time	WEBHIST	Chrome History	https://www.di.unisa.it/ (DI Home) [count: 1] Visit From: https://sqlite/chrome_27_history	OS:E:\Users\Raffaele\AppData\Local\G	
2019-02-08 09:20:33,879	Last Visited Time	WEBHIST	Chrome History	https://www.google.com/url?q=https://www.di.unisa.it&s=sqlite/chrome_27_history	OS:E:\Users\Raffaele\AppData\Local\G	
2019-02-08 09:20:41,926	Last Visited Time	WEBHIST	Chrome History	https://www.di.unisa.it/home/news (Home News) [count: sqlite/chrome_27_history]	OS:E:\Users\Raffaele\AppData\Local\G	
2019-02-08 09:20:41,926	Last Visited Time	WEBHIST	Chrome History	http://www.di.unisa.it/home/news (Home News) [count: sqlite/chrome_27_history]	OS:E:\Users\Raffaele\AppData\Local\G	
2019-02-08 10:26:24,134	Last Visited Time	WEBHIST	Chrome History	https://www.di.unisa.it/ (DI Home) [count: 1] Type: [TYPE] sqlite/chrome_27_history	OS:E:\Users\Raffaele\AppData\Local\G	
2019-02-08 10:26:35,475	Last Visited Time	WEBHIST	Chrome History	https://www.di.unisa.it/home/contatti (Home Contatti) [csqlite/chrome_27_history]	OS:E:\Users\Raffaele\AppData\Local\G	
2019-02-08 10:26:35,475	Last Visited Time	WEBHIST	Chrome History	http://www.di.unisa.it/home/contatti (Home Contatti) [ccsqlite/chrome_27_history]	OS:E:\Users\Raffaele\AppData\Local\G	
2019-02-08 10:26:43,728	Last Visited Time	WEBHIST	Chrome History	https://www.di.unisa.it/ (DI Home) [count: 1] Visit From: https://chrome_27_history	OS:E:\Users\Raffaele\AppData\Local\G	
2019-02-08 10:26:43,728	Last Visited Time	WEBHIST	Chrome History	http://www.di.unisa.it/ (DI Home) [count: 0] Type: [LINK - sqlite/chrome_27_history]	OS:E:\Users\Raffaele\AppData\Local\G	
2019-02-08 10:26:44,000	Last Access Time	FILE	OS Last Access Time	OS:E:\Users\Raffaele\AppData\Local\Google\Chrome\User filestat	OS:E:\Users\Raffaele\AppData\Local\G	
2019-02-08 10:26:55,890	Last Visited Time	WEBHIST	Chrome History	https://www.di.unisa.it/unisa-rescue-page/search/id/1356.sqlite/chrome_27_history	OS:E:\Users\Raffaele\AppData\Local\G	
2019-02-08 10:27:06,839	Last Visited Time	WEBHIST	Chrome History	https://docenti.unisa.it/000769/ricerca/pubblicazioni?anno=sqlite/chrome_27_history	OS:E:\Users\Raffaele\AppData\Local\G	
2019-02-08 10:27:06,839	Last Visited Time	WEBHIST	Chrome History	https://www.google.com/url?q=https://docenti.unisa.it/00 sqlite/chrome_27_history	OS:E:\Users\Raffaele\AppData\Local\G	
2019-02-08 10:27:16,288	Last Visited Time	WEBHIST	Chrome History	https://docenti.unisa.it/000769/didattica (Alfredo DE SANTI sqlite/chrome_27_history)	OS:E:\Users\Raffaele\AppData\Local\G	
2019-02-08 10:27:16,288	Last Visited Time	WEBHIST	Chrome History	http://docenti.unisa.it/000769/didattica (Alfredo DE SANTI sqlite/chrome_27_history)	OS:E:\Users\Raffaele\AppData\Local\G	
2019-02-08 10:27:54,000	Content Modification Time	FILE	OS Content Modification Time	OS:E:\Users\Raffaele\AppData\Local\Google\Chrome\User filestat	OS:E:\Users\Raffaele\AppData\Local\G	
2019-02-08 10:27:54,000	Metadata Modification Time	FILE	OS Metadata Modification Time	OS:E:\Users\Raffaele\AppData\Local\Google\Chrome\User filestat	OS:E:\Users\Raffaele\AppData\Local\G	

Le Super Timeline

Esempio di Utilizzo 1 | Cronologia Chrome | 12/30

3. Analisi del File

(CronologiaChrome.xlsx)

datetime
2019-02-08 09:20:11,298
2019-02-08 09:20:11,298
2019-02-08 09:20:11,298
2019-02-08 09:20:15,570
2019-02-08 09:20:18,890
2019-02-08 09:20:29,302
2019-02-08 09:20:33,879
2019-02-08 09:20:33,879
2019-02-08 09:20:41,926
2019-02-08 09:20:41,926
2019-02-08 10:26:24,134
2019-02-08 10:26:35,475
2019-02-08 10:26:35,475
2019-02-08 10:26:43,728
2019-02-08 10:26:43,728
2019-02-08 10:26:44,000
2019-02-08 10:26:55,890
2019-02-08 10:27:06,839
2019-02-08 10:27:06,839
2019-02-08 10:27:16,288
2019-02-08 10:27:16,288
2019-02-08 10:27:54,000
2019-02-08 10:27:54,000

datetime
2019-02-08 09:20:11,298
2019-02-08 09:20:11,298
2019-02-08 09:20:11,298
2019-02-08 09:20:15,570
2019-02-08 09:20:18,890
2019-02-08 09:20:29,302
2019-02-08 09:20:33,879
2019-02-08 09:20:33,879
2019-02-08 09:20:41,926
2019-02-08 09:20:41,926
2019-02-08 10:26:24,134
2019-02-08 10:26:35,475
2019-02-08 10:26:35,475
2019-02-08 10:26:43,728
2019-02-08 10:26:43,728
2019-02-08 10:26:44,000
2019-02-08 10:26:55,890
2019-02-08 10:27:06,839
2019-02-08 10:27:06,839
2019-02-08 10:27:16,288
2019-02-08 10:27:16,288
2019-02-08 10:27:54,000
2019-02-08 10:27:54,000

Per ciascun evento, specificato sulle righe, la colonna **datetime** ne riporta il timestamp, esplicitando la data e l'ora, nel seguente formato:

YYYY-MM-DD HH:mm:ss, lll

(lll indicano i millisecondi)

Le Super Timeline

Esempio di Utilizzo 1 | Cronologia Chrome | 13/30

Per ciascun evento, specificato sulle righe, la colonna **message** ne riporta una descrizione, esplicitando alcune informazioni utili

CronologiaChrome.xlsx)

message
http://www.google.it/ (Google) [count: 0] Visit from: http://
https://www.google.it/?gws_rd=ssl (Google) [count: 0] Visit
http://google.it/ (Google) [count: 1] Type: [TYPED - User typed]
https://www.google.it/search?source=hp&ei=yOldXJbgHYF
https://www.unisa.it/ (UNISA Home) [count: 0] Type: [LINK]
https://www.unisa.it/unisa-rescue-page/search/id/529/url/
https://www.di.unisa.it/ (DI Home) [count: 1] Visit From: h
https://www.google.com/url?q=https://www.di.unisa.it/&s
https://www.di.unisa.it/home/news (Home News) [count: 1]
http://www.di.unisa.it/home/news (Home News) [count: 1]
https://www.di.unisa.it/ (DI Home) [count: 1] Type: [TYPE]
https://www.di.unisa.it/home/contatti (Home Contatti) [c
http://www.di.unisa.it/home/contatti (Home Contatti) [co
https://www.di.unisa.it/ (DI Home) [count: 1] Visit from: h
http://www.di.unisa.it/ (DI Home) [count: 0] Type: [LINK -
OS:E:\Users\Raffaele\AppData\Local\Google\Chrome\User
https://www.unisa.it/unisa-rescue-page/search/id/1356/
https://docenti.unisa.it/000769/ricerca/pubblicazioni?ann:
https://www.google.com/url?q=https://docenti.unisa.it/00
https://docenti.unisa.it/000769/didattica (Alfredo DE SANTI)
http://docenti.unisa.it/000769/didattica (Alfredo DE SANTI)
OS:E:\Users\Raffaele\AppData\Local\Google\Chrome\User
OS:E:\Users\Raffaele\AppData\Local\Google\Chrome\User

Le Super Timeline

ome | 14/30

Colonne **datetime** e **message**

datetime	message
2019-02-08 09:20:11,298	http://www.google.it/ (Google) [count: 0] Visit from: http://www.di.unisa.it/
2019-02-08 09:20:11,298	https://www.google.it/?gws_rd=ssl (Google) [count: 0] Visit from: http://www.di.unisa.it/
2019-02-08 09:20:11,298	http://google.it/ (Google) [count: 1] Type: [TYPED - User typed]
2019-02-08 09:20:15,570	https://www.google.it/search?source=hp&ei=y0ldXJbgHYyF
2019-02-08 09:20:18,890	https://www.unisa.it/ (UNISA Home) [count: 0] Type: [LINK - Clicked]
2019-02-08 09:20:29,302	https://www.unisa.it/unisa-rescue-page/search/id/529/url/
2019-02-08 09:20:33,879	https://www.di.unisa.it/ (DI Home) [count: 1] Visit from: https://www.google.com/url?q=https://www.di.unisa.it/&t=1
2019-02-08 09:20:33,879	https://www.google.com/url?q=https://www.di.unisa.it/&t=1
2019-02-08 09:20:41,926	https://www.di.unisa.it/home/news (Home News) [count: 0] Type: [LINK - Clicked]
2019-02-08 09:20:41,926	http://www.di.unisa.it/home/news (Home News) [count: 0] Type: [LINK - Clicked]
2019-02-08 10:26:24,134	https://www.di.unisa.it/ (DI Home) [count: 1] Type: [TYPE]
2019-02-08 10:26:35,475	https://www.di.unisa.it/home/contatti (Home Contatti) [count: 0] Type: [LINK - Clicked]
2019-02-08 10:26:35,475	http://www.di.unisa.it/home/contatti (Home Contatti) [count: 0] Type: [LINK - Clicked]
2019-02-08 10:26:43,728	https://www.di.unisa.it/ (DI Home) [count: 1] Visit from: https://www.google.com/url?q=https://www.di.unisa.it/000769/ricerca/pubblicazioni?anno=2018&t=1
2019-02-08 10:26:43,728	http://www.di.unisa.it/ (DI Home) [count: 0] Type: [LINK - Clicked]
2019-02-08 10:26:44,000	OS:E:\Users\Raffaele\AppData\Local\Google\Chrome\User Data\Default\Crash Reports\crash_2019-02-08_10-26-44.000
2019-02-08 10:26:55,890	https://www.di.unisa.it/unisa-rescue-page/search/id/1356,1
2019-02-08 10:27:06,839	https://docenti.unisa.it/000769/ricerca/pubblicazioni?anno=2018
2019-02-08 10:27:06,839	https://www.google.com/url?q=https://docenti.unisa.it/000769/ricerca/pubblicazioni?anno=2018&t=1
2019-02-08 10:27:16,288	https://docenti.unisa.it/000769/didattica (Alfredo DE SANTI)
2019-02-08 10:27:16,288	http://docenti.unisa.it/000769/didattica (Alfredo DE SANTI)
2019-02-08 10:27:54,000	OS:E:\Users\Raffaele\AppData\Local\Google\Chrome\User Data\Default\Crash Reports\crash_2019-02-08_10-27-54.000
2019-02-08 10:27:54,000	OS:E:\Users\Raffaele\AppData\Local\Google\Chrome\User Data\Default\Crash Reports\crash_2019-02-08_10-27-54.000

3. Analisi

Per ciascun evento, specificato sulle righe, le colonne `timestamp_desc`, `source` e `source_long` ne indicano rispettivamente la tipologia del timestamp (`timestamp_desc`), l'identificativo della fonte (`source`), da cui è stato estrappolato il timestamp, e la descrizione, in formato *human-readable*, della fonte (`source_long`)

3. Analisi del File P

Le Super Timeline

Esempio di Utilizzo 1 | Cronologia Chrome | 16/30

3. Analisi del File P

ologiaChrome.xlsx)

Per ciascun evento, specificato sulle righe, la colonna **parser** ne riporta il parser, utilizzato da Plaso

parser
sqlite/chrome_27_history
filestat
sqlite/chrome_27_history
filestat
filestat

Le Super Timeline

Nella colonna **display_name** è specificato, in questo caso, il percorso completo del file della cronologia: E:\ [...] \History

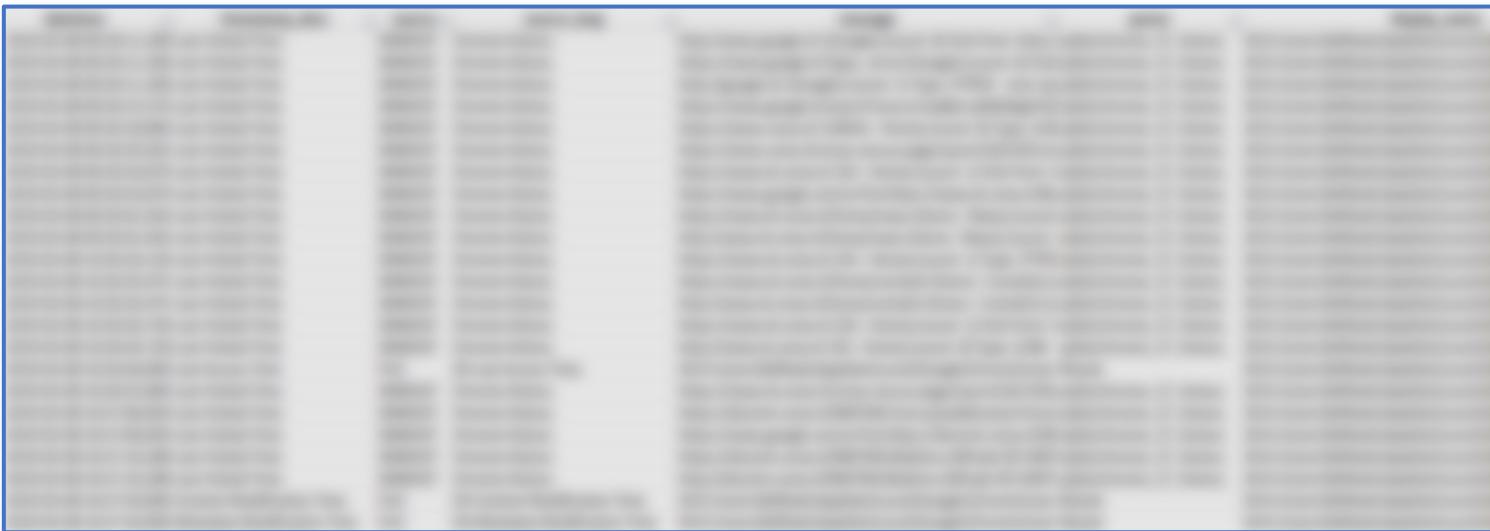
Izzo 1 | Cronologia Chrome | 17/30

3. Analisi del File Progetto (CronologiaChrome.xlsx)

Le Super Timeline

Esempio di Utilizzo 1 | Cronologia Chrome | 18/30

3. Analisi del File Prodotto (CronologiaChrome.xlsx)



In primo luogo, consideriamo ed analizziamo il campo **message**, di alcuni eventi, per avere reperire eventuali informazioni utili

Le Super Timeline

Esempio di Utilizzo 1 | Cronologia Chrome | 19/30



Analisi campo message (9° riga, 8° evento)

```
https://www.google.com/url?q=https://www.di.unisa.it/&sa=U&ved=0ah  
UKEwiQya3D56vgAhUNaFAKHT0RAHsQFggEMAA&client=internal-uds-  
cse&cx=001028597582454049833:hnoxg-  
aydtw&usg=AOvVaw0qVNWAgVwiQAKI6o9KsK_Q (DI | Home) [count: 0]  
Type: [LINK - User clicked a link] (URL not typed directly - no  
typed count)
```

Le Super Timeline

Esempio di Utilizzo 1 | Cronologia Chrome | 19/30



Analisi campo message (9° riga, 8° evento)

```
https://www.google.com/url?q=https://www.di.unisa.it/&sa=U&ved=0ah  
UKEwiQya3D56vgAhUNaFAKHT0RAHsQFggEMAA&client=internal-uds-  
cse&cx=001028597582454049833:hnoxg-  
aydtw&usg=AOvVaw0qVNWAgVwiQAKI6o9KsK_Q (DI | Home) [count: 0]  
Type: [LINK - User clicked a link] (URL not typed directly - no  
typed count)
```

Informazioni ripotate in altri campi:

Data e Ora (campo **datetime**) dell'ultima visita (valore «*Last Visited Time*» del campo **timestamp_desc**): 08/02/2019, 09:20:34

Le Super Timeline

Esempio di Utilizzo 1 | Cronologia Chrome | 19/30



Analisi campo message (9° riga, 8° evento)

```
https://www.google.com/url?q=https://www.di.unisa.it/&sa=U&ved=0ah  
UKEwiQya3D56vgAhUNaFAKHT0RAHsQFggEMAA&client=internal-uds-  
cse&cx=001028597582454049833:hnoxg-  
aydtw&usg=AOvVaw0qVNWAgVwiQAKI6o9KsK_Q (DI | Home) [count: 0]  
Type: [LINK - User clicked a link] (URL not typed directly - no  
typed count)
```

I parametri in grassetto, sono detti ***referral parameters*** (parametri di riferimento), dettagli al seguente link:

<https://developers.google.com/custom-search/v1/cse/list>

Le Super Timeline

Esempio di Utilizzo 1 | Cronologia Chrome | 19/30



Analisi campo message (9° riga, 8° evento)

```
https://www.google.com/url?q=https://www.di.unisa.it/&sa=U&ved=0ah  
UKEwiQya3D56vgAhUNaFAKHT0RAHsQFggEMAA&client=internal-uds-  
cse&cx=001028597582454049833:hnoxg-  
aydtw&usg=AOvVaw0qVNWAgVwiQAKI6o9KsK_Q (DI | Home) [count: 0]  
Type: [LINK - User clicked a link] (URL not typed directly - no  
typed count)
```

Accesso **indiretto** al sito (URL: <https://www.di.unisa.it>), tramite
Google (<https://www.google.com/url?q=>)

Accesso tramite **barra di ricerca (sa=U)**, da parte dell'utente

Le Super Timeline

Esempio di Utilizzo 1 | Cronologia Chrome | 19/30

Analisi campo message (9° riga, 8° evento)



```
https://www.google.com/url?q=https://www.di.unisa.it/&sa=U&ved=0ahUKEwiQya3D56vgAhUNaFAKHT0RAHsQFggEMAA&client=internal-uds-cse&cx=001028597582454049833:hnoxg-aydtw&usg=AOvVaw0qVNWAgVwiQAKI6o9KsK_Q (DI | Home) [count: 0]
Type: [LINK - User clicked a link] (URL not typed directly - no typed count)
```

Link visitato per la prima volta ([count: 0])

Le Super Timeline

Esempio di Utilizzo 1 | Cronologia Chrome | 20/30



Analisi campo message (7° riga, 6° evento)

```
https://www.unisa.it/unisa-rescue-
page/search/id/529/url/Lw%3D%3D?q=dipartimento+di+informatica
(UNISA | Home) [count: 0] Visit from: https://www.unisa.it/ (UNISA
| Home) Type: [FORM_SUBMIT - A form the user has submitted values
to] (URL not typed directly - no typed count)
```

Le Super Timeline

Esempio di Utilizzo 1 | Cronologia Chrome | 20/30

Analisi campo message (7° riga, 6° evento)

<https://www.unisa.it/unisa-rescue-page/search/id/529/url/Lw%3D%3D?q=dipartimento+di+informatica>
(UNISA | Home) [count: 0] Visit from: <https://www.unisa.it/> (UNISA | Home) Type: [FORM_SUBMIT - A form the user has submitted values to] (URL not typed directly - no typed count)

Tramite un **form** (nello specifico, una casella di testo), è stata effettuata una **ricerca** della stringa **dipartimento di informatica** dal sito dell'Università degli Studi di Salerno (<https://www.unisa.it>)

La pagina è stata acceduta per la prima volta ([count: 0])

Informazioni ripotate in altri campi:
Data e Ora (campo **datetime**) dell'ultima visita (valore «*Last Visited Time*» del campo **timestamp_desc**): 08/02/2019, 09:20:29

Le Super Timeline

Esempio di Utilizzo 1 | Cronologia Chrome | 21/30



Analisi campo message (15° riga, 14° evento)

```
https://www.di.unisa.it/ (DI | Home) [count: 1] Visit from:  
http://www.di.unisa.it/ (DI | Home) Type: [LINK - User clicked a  
link] (type count 1 time)
```

Le Super Timeline

Esempio di Utilizzo 1 | Cronologia Chrome | 21/30

Analisi campo message (15° riga, 14° evento)



```
https://www.di.unisa.it/ (DI | Home) [count: 1] Visit from:  
http://www.di.unisa.it/ (DI | Home) Type: [LINK - User clicked a  
link] (type count 1 time)
```

Tramite un **link** è stato effettuato l'accesso alla pagina del Dipartimento di Informatica, dell'Università degli Studi di Salerno
(<https://www.di.unisa.it>)

Informazioni ripotate in altri campi:
Data e Ora (campo **datetime**) dell'ultima visita (valore «*Last Visited Time*» del campo **timestamp_desc**): 08/02/2019, 10:26:44

Le Super Timeline

Esempio di Utilizzo 1 | Cronologia Chrome | 22/30

ALCUNE CONSIDERAZIONI

- Avendo a disposizione gli URL dei vari siti visitati, estratti dalla cronologia, sarebbe possibile accedere direttamente a tali siti, per visionarne l'eventuale contenuto, senza effettuarne una analisi preventiva (o effettuandone una superficiale), ***come verrà mostrato nelle seguenti slide...***

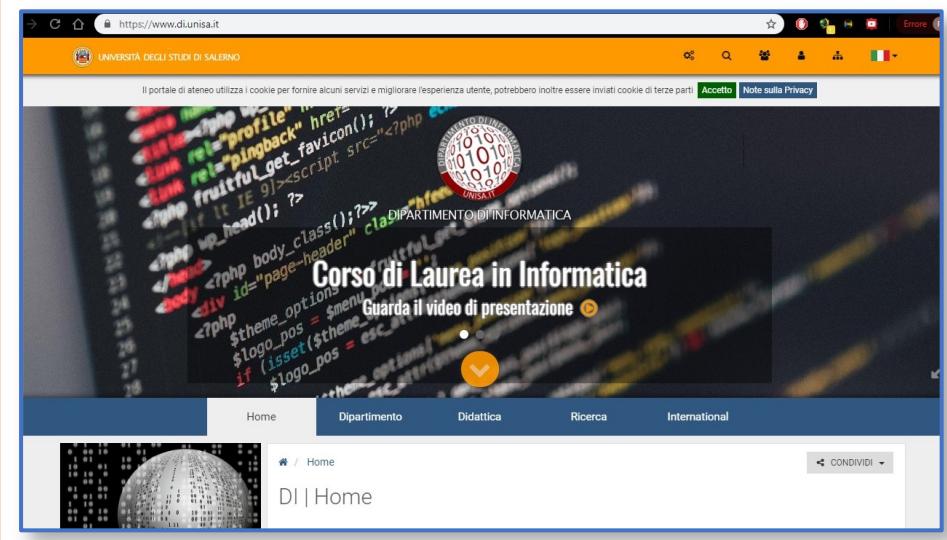
Le Super Timeline

Esempio di Utilizzo 1 | Cronologia Chrome | 23/30

Analisi campo message (9° riga, 8° evento)

https://www.google.com/url?q=https://www.di.unisa.it/&sa=U&ved=0ahUKEwiQya3D56vgAhUNaFAKHT0RAHsQFggEMAA&client=internal-uds-cse&cx=001028597582454049833:hnoxg-aydtw&lr=A0vVaw0qVNWAgVwIQAKI6o9KsK_Q
(DI | Home) [count: 0] Type: [LINK - User clicked a link] (URL not typed directly - no typed count)

<https://www.di.unisa.it>



Le Super Timeline

Esempio di Utilizzo 1 | Cronologia Chrome | 24/30

Analisi campo message (7° riga, 6° evento)

<https://www.unisa.it/unisa-rescue-page/search/id/529/url/Lw%3D%3D?q=dipartimento+di+informatica> (UNISA | Home)
[count: 0] Visit from: https://www.unisa.it (UNISA | Home) Type:
[FORM_SUBMIT - A form the user has submitted to] (URL not typed directly - no typed count)

<https://www.unisa.it/unisa-rescue-page/search/id/529/url/Lw%3D%3D?q=dipartimento+di+informatica>

The screenshot shows the homepage of the University of Salerno. At the top, there's a banner with the university's name and logo. Below it, a search bar contains the query "dipartimento di informatica". The main content area displays search results, with the first result being a link to the "dipartimento di informatica" page. The URL of this result is highlighted in red, matching the one shown in the analysis above.

Le Super Timeline

Esempio di Utilizzo 1 | Cronologia Chrome | 25/30

Analisi campo message (15° riga, 14° evento)

<https://www.di.unisa.it/> (DI | Home) [count: 1] Visit from:
http://www.di.unisa.it/ (DI | Home) Type: [LINK - User clicked a link] (type count 1 time)

<https://www.di.unisa.it>

The screenshot shows the University of Salerno's website. The URL https://www.di.unisa.it is displayed in the browser's address bar. The main content area features a banner for the Faculty of Informatics (DIPARTIMENTO DI INFORMATICA) with the text "Corso di Laurea in Informatica" and "Guarda il video di presentazione". Below the banner, there are navigation links for Home, Dipartimento, Didattica, Ricerca, and International. The overall layout is clean with a blue and white color scheme.

Le Super Timeline

Esempio di Utilizzo 1 | Cronologia Chrome | 26/30

ALCUNE CONSIDERAZIONI

- Avendo a disposizione gli URL dei vari siti visitati, estratti dalla cronologia, sarebbe possibile accedere direttamente a tali siti, per visionarne l'eventuale contenuto, senza effettuarne una analisi preventiva (o effettuandone una superficiale), *come verrà mostrato nelle seguenti slide...*
- È bene però considerare che gli URL potrebbero essere diretti a siti malevoli/illegali/ecc.
 - Una richiesta, proveniente da una fonte sconosciuta (ovvero, la richiesta effettuata con il link diretto, effettuata dall'investigatore), potrebbe mettere «in allerta» gli «amministratori» dei suddetti siti (ed eventualmente alterare il corso di eventuali altre indagini, in atto, o ulteriori indagini su questi siti)
 - Pertanto, un'accurata analisi è sicuramente preferibile ed è consigliabile accedere all'URL solo in caso vi sia sufficiente sicurezza e/o per valide motivazioni, ai fini dell'indagine che si sta svolgendo
 - Oppure, gli URL potrebbero innescare azioni (ad esempio, cancellazione di dati, attivare/disattivare oggetti, ecc.)

Le Super Timeline

Esempio di Utilizzo 1 | Cronologia Chrome | 27/30

3. Analisi del File Prodotto (CronologiaChrome.xlsx)



Soffermiamoci ancora sull'analisi del file prodotto da Plaso, ovvero, CronologiaChrome.xlsx

Le Super Timeline

Esempio di Utilizzo 1 | Cronologia Chrome | 27/30

3. Analisi del File Prodotto (CronologiaChrome.xlsx)

Focalizziamo l'attenzione sulla colonna **source**, la quale riporta la fonte da cui è stato estratto il timestamp, di ciascun evento

source
WEBHIST
FILE
WEBHIST
FILE
WEBHIST
FILE
WEBHIST
FILE
FILE

Le Super Timeline

Esempio di Utilizzo 1 | Cronologia Chrome | 28/30

3. Analisi del File Prodotto (CronologiaChrome.xlsx)

source
WEBHIST
FILE
WEBHIST
WEBHIST
WEBHIST
WEBHIST
FILE
FILE

Le Super Timeline

Esempio di Utilizzo 1 | Cronologia Chrome | 28/30

3. Analisi del File Prodotto (CronologiaChrome.xlsx)

source
WEBHIST
FILE
WEBHIST
FILE
FILE

source
WEBHIST
FILE
WEBHIST
FILE
FILE

Le Super Timeline

Esempio di Utilizzo 1 | Cronologia Chrome | 28/30

3. Analisi del File Prodotto (CronologiaChrome.xlsx)

source
WEBHIST
FILE
WEBHIST
FILE
FILE

source
WEBHIST
FILE
WEBHIST
FILE
FILE

OSSERVAZIONE

È possibile osservare che sono presenti due fonti:

- WEBHIST
- FILE

Le Super Timeline

Esempio di Utilizzo 1 | Cronologia Chrome | 29/30

3. Analisi del File Prodotto (CronologiaChrome.xlsx)

timestamp_desc	source	message
Last Visited Time	WEBHIST	http://www.google.it/ (Google) [count: 0] Visit from: http://google.it/ (Google) Type: [TYPED - User typed the URL in the URL bar]
Last Visited Time	WEBHIST	https://www.google.it/?gws_rd=ssl (Google) [count: 0] Visit from: http://www.google.it/ (Google)
Last Visited Time	WEBHIST	http://google.it/ (Google) [count: 1] Type: [TYPED - User typed the URL in the URL bar] (type count)
Last Visited Time	WEBHIST	https://www.google.it/search?source=hp&ei=y0ldXJbgHYyPlwTtuJKYAw&q=unisa&btnK=Cerca+cerca
Last Visited Time	WEBHIST	https://www.unisa.it/ (UNISA Home) [count: 0] Type: [LINK - User clicked a link] (URL not typed directly)
Last Visited Time	WEBHIST	https://www.unisa.it/unisa-rescue-page/search/id/529/url/Lw%3D%3D?q=dipartimento+di+infor
Last Visited Time	WEBHIST	https://www.di.unisa.it/ (DI Home) [count: 1] Visit from: https://www.google.com/url?q=https://www.di.unisa.it/
Last Visited Time	WEBHIST	https://www.google.com/url?q=https://www.di.unisa.it/&sa=U&ved=0ahUKEwiQya3D56vgAhUN
Last Visited Time	WEBHIST	https://www.di.unisa.it/home/news (Home News) [count: 0] Visit from: http://www.di.unisa.it/
Last Visited Time	WEBHIST	http://www.di.unisa.it/home/news (Home News) [count: 0] Type: [LINK - User clicked a link] (URL not typed directly)
Last Visited Time	WEBHIST	https://www.di.unisa.it/ (DI Home) [count: 1] Type: [TYPED - User typed the URL in the URL bar]
Last Visited Time	WEBHIST	https://www.di.unisa.it/home/contatti (Home Contatti) [count: 0] Visit from: http://www.di.unisa.it/
Last Visited Time	WEBHIST	http://www.di.unisa.it/home/contatti (Home Contatti) [count: 0] Type: [LINK - User clicked a link]
Last Visited Time	WEBHIST	https://www.di.unisa.it/ (DI Home) [count: 1] Visit from: http://www.di.unisa.it/ (DI Home) Type: [TYPED - User typed the URL in the URL bar]
Last Visited Time	WEBHIST	http://www.di.unisa.it/ (DI Home) [count: 0] Type: [LINK - User clicked a link] (URL not typed directly)
Last Access Time	FILE	OS:E:\Users\Raffaele\AppData\Local\Google\Chrome\User Data\Default\History Type: file
Last Visited Time	WEBHIST	https://www.di.unisa.it/unisa-rescue-page/search/id/1356/url/Lw%3D%3D?q=de+santis () [count: 0] Type: [TYPED - User typed the URL in the URL bar]
Last Visited Time	WEBHIST	https://docenti.unisa.it/000769/ricerca/pubblicazioni?anno=2018 (Alfredo DE SANTIS Pubblicazioni)
Last Visited Time	WEBHIST	https://www.google.com/url?q=https://docenti.unisa.it/000769/ricerca/pubblicazioni%3Fanno%3D2018
Last Visited Time	WEBHIST	https://docenti.unisa.it/000769/didattica (Alfredo DE SANTIS Didattica) [count: 0] Visit from: https://www.di.unisa.it/
Last Visited Time	WEBHIST	http://docenti.unisa.it/000769/didattica (Alfredo DE SANTIS Didattica) [count: 0] Type: [LINK - User clicked a link]
Content Modification Time	FILE	OS:E:\Users\Raffaele\AppData\Local\Google\Chrome\User Data\Default\History Type: file
Metadata Modification Time	FILE	OS:E:\Users\Raffaele\AppData\Local\Google\Chrome\User Data\Default\History Type: file

Analizzando meglio il file, in virtù dell'osservazione precedente, è possibile individuare **quali siano le due fonti**, da cui sono stati reperiti i timestamp:

- **Contenuto del file History (relativo alla cronologia del browser Google Chrome)**
 - I timestamp sono relativi al momento dell'ultima visita (*Last Visited Time*) di un URL
- **Metadati del file system, relativi al file History**
 - Tali metadati sono reperiti dalla file table (del file system), considerando l'entry, associata al file History
 - Ad esempio, in NTFS, i suddetti metadati sono contenuti nelle entry della MFT

timestamp_desc	source	message
Last Visited Time	WEBHIST	http://www.google.it/ (Google) [count: 0] Visit from: http://google.it/ (Google) Type: [TYPED - User typed the URL in the URL bar]
Last Visited Time	WEBHIST	https://www.google.it/?gws_rd=ssl (Google) [count: 0] Visit from: http://www.google.it/ (Google)
Last Visited Time	WEBHIST	http://google.it/ (Google) [count: 1] Type: [LINK - User clicked a link] (URL not typed directly)
Last Visited Time	WEBHIST	https://www.google.it/search?source=hp&ei=yOldXJbgHYyPlwTtuJKYAw&q=unisa&btnK=Cerca+cerca
Last Visited Time	WEBHIST	https://www.unisa.it/ (UNISA Home) [count: 0] Type: [LINK - User clicked a link] (URL not typed directly)
Last Visited Time	WEBHIST	https://www.unisa.it/unisa-rescue-page/search/id/529/url/Lw%3D%3D?q=dipartimento+di+infor
Last Visited Time	WEBHIST	https://www.di.unisa.it/ (DI Home) [count: 1] Visit from: https://www.google.com/url?q=https:/
Last Visited Time	WEBHIST	https://www.google.com/url?q=https://www.di.unisa.it/&sa=U&ved=0ahUKEwiQya3D56vgAhUN
Last Visited Time	WEBHIST	https://www.di.unisa.it/home/news (Home News) [count: 0] Visit from: http://www.di.unisa.it/
Last Visited Time	WEBHIST	http://www.di.unisa.it/home/news (Home News) [count: 0] Type: [LINK - User clicked a link] (URL not typed directly)
Last Visited Time	WEBHIST	https://www.di.unisa.it/ (DI Home) [count: 1] Type: [TYPED - User typed the URL in the URL bar]
Last Visited Time	WEBHIST	https://www.di.unisa.it/home/contatti (Home Contatti) [count: 0] Visit from: http://www.di.unis
Last Visited Time	WEBHIST	http://www.di.unisa.it/home/contatti (Home Contatti) [count: 0] Type: [LINK - User clicked a link]
Last Visited Time	WEBHIST	https://www.di.unisa.it/ (DI Home) [count: 1] Visit from: http://www.di.unisa.it/ (DI Home) Type: [LINK - User clicked a link]
Last Visited Time	WEBHIST	http://www.di.unisa.it/ (DI Home) [count: 0] Type: [LINK - User clicked a link] (URL not typed directly)
Last Access Time	FILE	OS:E:\Users\Raffaele\AppData\Local\Google\Chrome\User Data\Default\History Type: file
Last Visited Time	WEBHIST	https://www.di.unisa.it/unisa-rescue-page/search/id/1356/url/Lw%3D%3D?q=de+santis () [count: 0] Visit from: http://www.di.unisa.it/
Last Visited Time	WEBHIST	https://docenti.unisa.it/000769/ricerca/pubblicazioni?anno=2018 (Alfredo DE SANTIS Pubblicaz
Last Visited Time	WEBHIST	https://www.google.com/url?q=https://docenti.unisa.it/000769/ricerca/pubblicazioni%3Fanno%
Last Visited Time	WEBHIST	https://docenti.unisa.it/000769/didattica (Alfredo DE SANTIS Didattica) [count: 0] Visit from: ht
Last Visited Time	WEBHIST	http://docenti.unisa.it/000769/didattica (Alfredo DE SANTIS Didattica) [count: 0] Type: [LINK - User clicked a link]
Content Modification Time	FILE	OS:E:\Users\Raffaele\AppData\Local\Google\Chrome\User Data\Default\History Type: file
Metadata Modification Time	FILE	OS:E:\Users\Raffaele\AppData\Local\Google\Chrome\User Data\Default\History Type: file

Le Super Timeline

Esempio di Utilizzo 1 | Cronologia Chrome | 30/30

3. Analisi del File Prodotto (CronologiaChrome.xlsx)

2019-02-08 10:26:44,000	Last Access Time	FILE	OS Last Access Time
2019-02-08 10:27:54,000	Content Modification Time	FILE	OS Content Modification Time
2019-02-08 10:27:54,000	Metadata Modification Time	FILE	OS Metadata Modification Time

Le Super Timeline

Esempio di Utilizzo 1 | Cronologia Chrome | 30/30

3. Analisi del File Prodotto (CronologiaChrome.xlsx)

2019-02-08 10:26:44,000	Last Access Time	FILE	OS Last Access Time
2019-02-08 10:27:54,000	Content Modification Time	FILE	OS Content Modification Time
2019-02-08 10:27:54,000	Metadata Modification Time	FILE	OS Metadata Modification Time

In questo esempio, Plaso riporta esclusivamente le informazioni MAC, in merito ai timestamp, provenienti dai metadati del file system

Lettera	Descrizione	Nome specificato da Plaso
M	Data e ora dell'ultima modifica	OS Content Modification Time
A	Data e ora dell'ultimo accesso al file	OS Last Access Time
C	Data e ora dell'ultima modifica ai metadati	OS Metadata Modification Time

Le Super Timeline

Esempio di Utilizzo 1 | Cronologia Chrome | 30/30

3. Analisi del File Prodotto (CronologiaChrome.xlsx)

2019-02-08 10:26:44,000	Last Access Time	FILE	OS Last Access Time
2019-02-08 10:27:54,000	Content Modification Time	FILE	OS Content Modification Time
2019-02-08 10:27:54,000	Metadata Modification Time	FILE	OS Metadata Modification Time

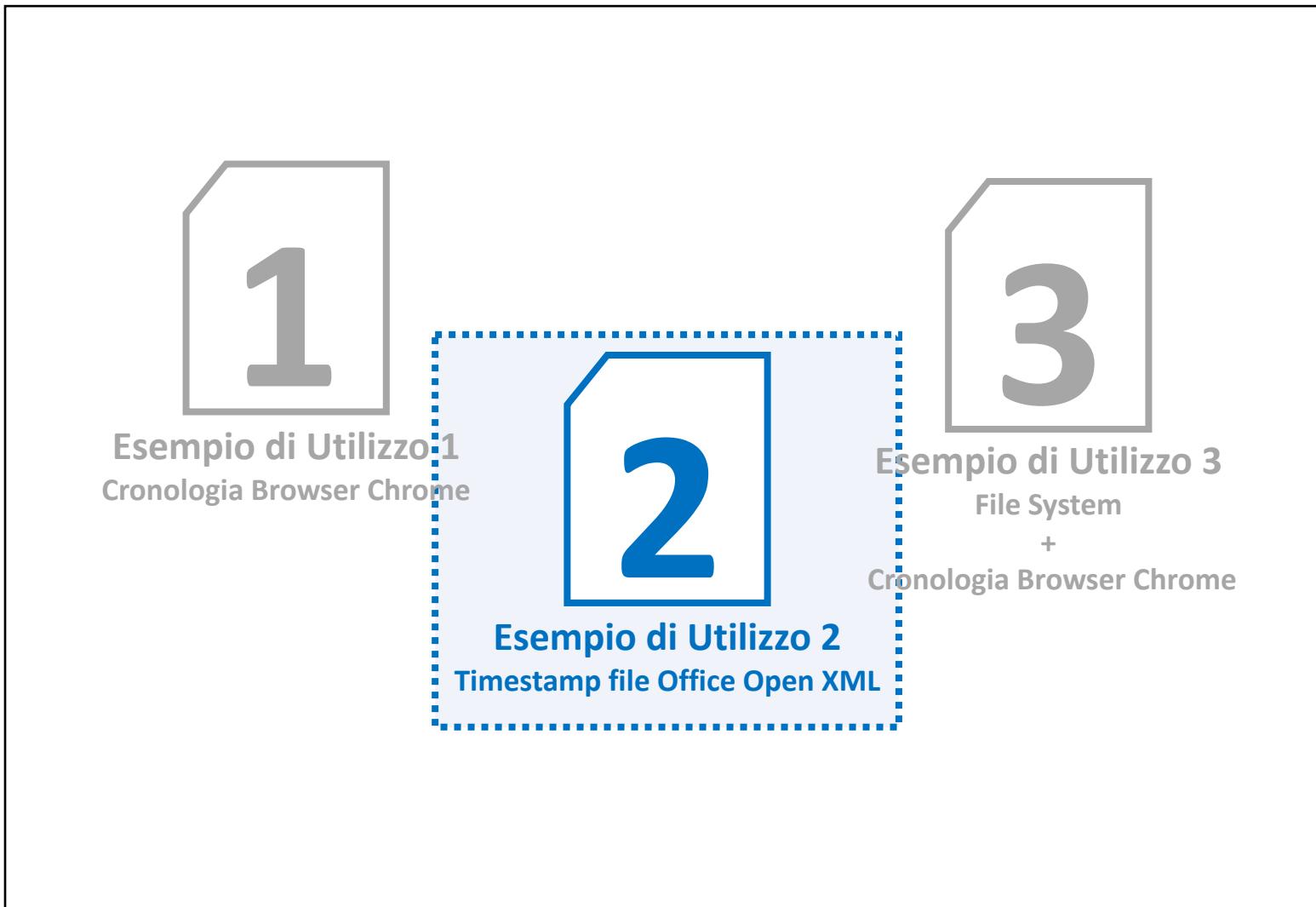
OSSERVAZIONE IMPORTANTE

Le tracce, provenienti dalle due fonti: **metadati del file system** e **cronologia del browser Google Chrome**, risultano essere coerenti

Infatti, tutti e tre i timestamp (**metadati del file system**) riportano orari coerenti ed in linea con gli orari, relativi all'attività di navigazione Web, individuata dalla **cronologia del browser**

Le Super Timeline

Esempi di Utilizzo



Le Super Timeline

Esempi di Utilizzo

1

Esempio di Utilizzo 1
Cronologia Browser Chrome

2

Esempio di Utilizzo 2
Timestamp file Office Open XML

3

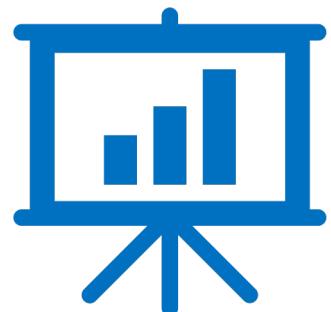
Esempio di Utilizzo 3
File System
+
Cronologia Browser Chrome

L'analisi dei timestamp dei file Office (memorizzati generalmente nel formato *Office Open XML*) è particolarmente importante (a volte, tali file sono utilizzati come alibi, ecc.)

Le Super Timeline

Esempio di Utilizzo 2 | File OOXML | 1/18

- In questo esempio, verrà realizzata una super timeline, utilizzando un file, in formato **Office Open XML** (*maggiori dettagli nelle prossime slide*)
 - Il nome del file, utilizzato per l'esempio, è il seguente: presentazione.pptx
- Nello specifico, si tratta di una presentazione, redatta con il software Microsoft PowerPoint
 - Il file ha dimensione pari a ~23,1MB



Le Super Timeline

Esempio di Utilizzo 2 | File OOXML | 2/18

- Il formato Office Open XML (OOXML) è un formato di memorizzazione per **presentazioni** (file `.pptx`), **file di testo formattati** (file `.docx`) e **fogli di calcolo** (file `.xlsx`)
 - Sviluppato da Microsoft ed utilizzato per la memorizzazione di file, in Microsoft Office
 - Il formato è successivamente divenuto uno standard ISO (ISO/IEC DIS 29500)
 - Due differenti set di specifiche:
 - *Transitional*
 - Specifiche volte al supporto della retrocompatibilità
 - *Strict*
 - Set di specifiche che definiscono effettivamente lo standard

Le Super Timeline

Esempio di Utilizzo 2 | File OOXML | 3/18

- Un file OOXML è essenzialmente un **contenitore compresso**, in formato ZIP
 - Contiene diversi elementi e file XML: questi ultimi, sono essenzialmente **metadati**, che specificano la struttura del documento ed altre caratteristiche/informazioni

Le Super Timeline

Esempio di Utilizzo 2 | File OOXML | 3/18

- Un file OOXML è essenzialmente un **contenitore compresso**, in formato ZIP
 - Contiene diversi elementi e file XML: questi ultimi, sono essenzialmente **metadati**, che specificano la struttura del documento ed altre caratteristiche/informazioni

Per estrarre e visionare la **struttura interna** di un file, in formato Office Open XML, è sufficiente **decomprimerlo**, in una qualsiasi cartella (per la decompressione, è anche possibile utilizzare tool gratuiti come 7-zip, ecc.)

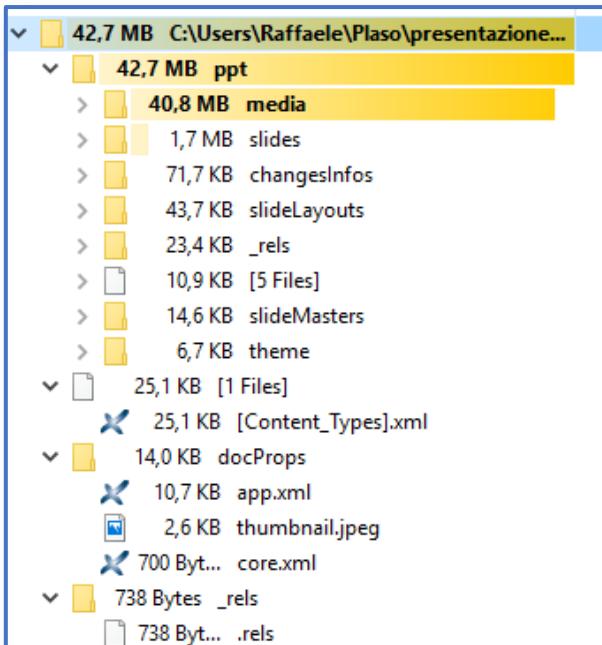
Le Super Timeline

Esempio di Utilizzo 2 | File OOXML | 3/18

- Un file OOXML è essenzialmente un **contenitore compresso**, in formato ZIP
 - Contiene diversi elementi e file XML: questi ultimi, sono essenzialmente **metadati**, che specificano la struttura del documento ed altre caratteristiche/informazioni

Esempio

Struttura Interna del File presentazione.pptx



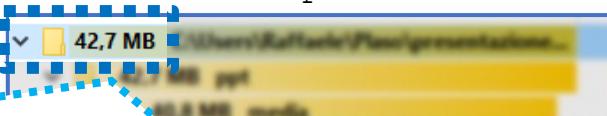
Le Super Timeline

Esempio di Utilizzo 2 | File OOXML | 3/18

- Un file OOXML è essenzialmente un **contenitore compresso**, in formato ZIP
 - Contiene diversi elementi e file XML: questi ultimi, sono essenzialmente **metadati**, che specificano la struttura del documento ed altre caratteristiche/informazioni

Esempio

Struttura Interna del File presentazione.pptx



In questo esempio, la cartella, in cui è stata effettuata la decompressione di presentazione.pptx, ha dimensione pari a **~42,7 MB** (invece, il file presentazione.pptx ha dimensione pari a **~23,1 MB**)

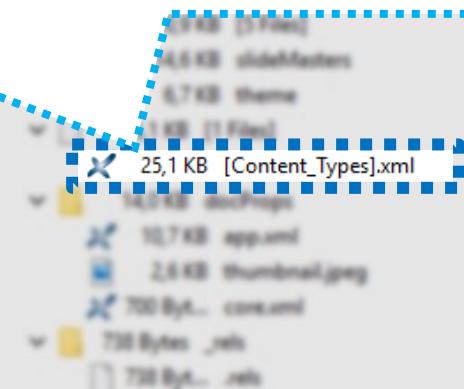


Le Super Timeline

Esempio di Utilizzo 2 | File OOXML | 3/18

Il file [Content_Types].xml, contiene informazioni sul contenuto del documento

```
<Types>
  <Default ContentType="image/x-emf" Extension="emf"/>
  <Default ContentType="image/jpeg" Extension="jfif"/>
  <Default ContentType="image/jpeg" Extension="jpeg"/>
  <Default ContentType="image/jpeg" Extension="jpg"/>
  <Default ContentType="image/png" Extension="png"/>
  <Default ContentType="application/vnd.openxmlformats-package.relationships+xml" Extension="rels"/>
  <Default ContentType="image/svg+xml" Extension="svg"/>
  <Default ContentType="image/tiff" Extension="tiff"/>
  <Default ContentType="image/vnd.ms-photo" Extension="wdp"/>
  <Default ContentType="application/xml" Extension="xml"/>
  <Override
    ContentType="application/vnd.openxmlformats-officedocument.presentationml.presentation.main+xml"
    PartName="/ppt/presentation.xml"/>
<Override
  ContentType="application/vnd.openxmlformats-officedocument.presentationml.slideMaster+xml"
  PartName="/ppt/slideMasters/slideMaster1.xml"/>
```

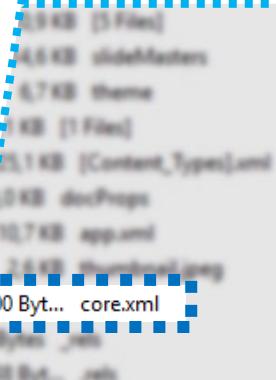


Le Super Timeline

Esempio di Utilizzo 2 | File OOXML | 3/18

Il file `core.xml` (nella directory `docProps`), contiene alcuni metadati, i quali indicano informazioni di carattere generale, in merito al documento (titolo, creatore, **data e ora di creazione, data e ora dell'ultima modifica**, ecc.)

```
<cp:coreProperties>
    <dc:title>Presentazione standard di PowerPoint</dc:title>
    <dc:creator>Raffaele P</dc:creator>
    <cp:lastModifiedBy>Raffaele P</cp:lastModifiedBy>
    <cp:revision>195</cp:revision>
    <dcterms:created xsi:type="dcterms:W3CDTF">
        2019-01-09T07:04:45Z
    </dcterms:created>
    <dcterms:modified xsi:type="dcterms:W3CDTF">
        2019-02-06T12:15:46Z
    </dcterms:modified>
</cp:coreProperties>
```



Le Super Timeline

Esempio di Utilizzo 2 | File OOXML | 3/18

Il file .rels (file XML), nella directory _rels, contiene eventuali informazioni sulle relazioni di alcuni elementi strutturali del documento

```
<Relationships>
  <Relationship Id="rId3" Target="docProps/core.xml"
    Type="http://schemas.openxmlformats.org/package/2006/relationships/metadata/core-properties"/>
  <Relationship Id="rId2" Target="docProps/thumbnail.jpeg"
    Type="http://schemas.openxmlformats.org/package/2006/relationships/metadata/thumbnail"/>
  <Relationship Id="rId1" Target="ppt/presentation.xml"
    Type="http://schemas.openxmlformats.org/officeDocument/2006/relationships/officeDocument"/>
  <Relationship Id="rId4" Target="docProps/app.xml"
    Type="http://schemas.openxmlformats.org/officeDocument/2006/relationships/extended-properties"/>
</Relationships>
```

1.4KB slideMaster
3.7KB theme
2B [1 File]
1KB [Content_Types].xml
6KB docProps
7KB app.xml
2.6KB thumbnail.jpeg
84B core.xml
738 Byt... .rels

Le Super Timeline

Esempio di Utilizzo 2 | File OOXML | 4/18

1. Analogamente all'esempio precedente, effettuiamo la memorizzazione del file di output, in formato Plaso, fornendo in input il percorso relativo al file presentazione.pptx

```
log2timeline EsempioOOXML.plaso presentazione.pptx
```

Le Super Timeline

Esempio di Utilizzo 2 | File OOXML | 4/18

1. Analogamente all'esempio precedente, effettuiamo la memorizzazione del file di output, in formato Plaso, fornendo in input il percorso relativo al file presentazione.pptx

```
log2timeline EsempioOOXML.plaso presentazione.pptx
```

Anche in questo caso, sarebbe stato possibile effettuare la super timeline, basandosi su un file OOXML, contenuto all'interno di una immagine forense (effettuando il mounting, in sola lettura, dell'immagine su un drive «virtuale»)

Tuttavia, in questo esempio, il file utilizzato (ovvero, presentazione.pptx) è memorizzato nella stessa cartella del framework Plaso (ovvero, la cartella C:\Users\Raffaele\Plaso, in cui sono presenti gli eseguibili dei vari tool di Plaso)

Le Super Timeline

Esempio di Utilizzo 2 | File OOXML | 4/18

1. Analogamente all'esempio precedente, effettuiamo la memorizzazione del file di output, in formato Plaso, fornendo in input il percorso relativo al file presentazione.pptx

```
log2timeline EsempioOOXML.plaso presentazione.pptx
```

Output del comando log2timeline

```
Source path      : C:\Users\Raffaele\Plaso\presentazione.pptx
Source type     : single file
Processing time : 00:00:00

Processing started.
Processing completed.
```

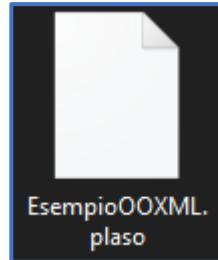
Le Super Timeline

Esempio di Utilizzo 2 | File OOXML | 4/18

- Analogamente all'esempio precedente, effettuiamo la memorizzazione del file di output, in formato Plaso, fornendo in input il percorso relativo al file presentazione.pptx

```
log2timeline EsempioOOXML.plaso presentazione.pptx
```

File Prodotto (~56 KB)



Le Super Timeline

Esempio di Utilizzo 2 | File OOXML | 5/18

- Mediante il tool **psort**, il file in formato Plaso (output del tool **log2timeline**) verrà convertito in formato XLSX

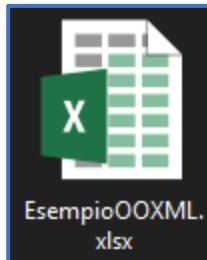
```
psort EsempioOOXML.plaso -o xlsx -w EsempioOOXML.xlsx
```

Output del comando psort

```
C:\Users\Raffaele\Plaso>psort EsempioOOXML.plaso -o xlsx -w EsempioOOXML.xlsx
2019-02-09 13:14:58,108 [INFO] (MainProcess) PID:10012 <data_location> Determined data location: C:\Users\Raffaele\Plaso
\data
2019-02-09 13:14:58,109 [WARNING] (MainProcess) PID:10012 <psort_tool> Appending to an already existing storage file.
Processing completed.

***** Export results *****
Events MACB grouped : 5
Events processed : 5
Events filtered : 0
Events from time slice : 0
```

File Prodotto (~6 KB)



Le Super Timeline

Esempio di Utilizzo 2 | File OOXML | 6/18

3. Analisi del File Prodotto (EsempioOOXML.xlsx)

datetime	timestamp_desc	source	source_long	message	parser
2019-01-09 07:04:45,000	Creation Time	META	Open XML Metadata	Creating App: Microsoft Office PowerPoint App version: 1 (zip/oxml	
2019-02-06 12:15:46,000	Content Modification Time	FILE	OS Content Modification Time	OS:C:\Users\Raffaele\Plaso\presentazione.pptx Type: file	filestat
2019-02-06 12:15:46,000	Content Modification Time	META	Open XML Metadata	Creating App: Microsoft Office PowerPoint App version: 1 (zip/oxml	
2019-02-09 09:31:33,000	Metadata Modification Time	FILE	OS Metadata Modification Time	OS:C:\Users\Raffaele\Plaso\presentazione.pptx Type: file	filestat
2019-02-09 09:31:34,000	Last Access Time	FILE	OS Last Access Time	OS:C:\Users\Raffaele\Plaso\presentazione.pptx Type: file	filestat

È stata omessa la colonna **display_name**, la quale riportava, per ogni entry della tabella, il seguente valore: OS:C:\Users\Raffaele\Plaso\presentazione.pptx (ovvero il percorso del file analizzato)

Le Super Timeline

Esempio di Utilizzo 2 | File OOXML | 7/18

3. Analisi del File Prodotto (EsempioOOXML.xlsx)

2019-01-09 07:04:45,000 Creation Time	META	Open XML Metadata	Creating App: Microsoft Office PowerPoint App version: 1\czip/oxml
[Redacted]			

Le Super Timeline

Esempio di Utilizzo 2 | File OOXML | 7/18

3. Analisi del File Prodotto (EsempioOOXML.xlsx)

2019-01-09 07:04:45,000	Creation Time	META	Open XML Metadata	Creating App: Microsoft Office PowerPoint App version: 16.0000 czip/oxml
-------------------------	---------------	------	-------------------	---

Campo	Valore
<code>datetime</code>	09/01/2019 07:04:45
<code>timestamp_desc</code>	Creation Time
<code>source</code>	META
<code>source_long</code>	Open XML Metadata
<code>message</code>	Creating App: Microsoft Office PowerPoint App version: 16.0000 Last saved by: Raffaele P Author: Raffaele P Revision number: 195 [...]
<code>parser</code>	czip/oxml

Il file presentazione.pptx è stato **creato** (valore **Creation Time**, nel campo **timestamp_desc**) il **09/01/2019** alle ore **07:04:45** (valore del campo **datetime**)

3

Le informazioni sono state reperite dai **metadati del formato OXML** (come indicato dai campi **source**, **source_long** e **parser**), i quali sono memorizzati all'interno del file presentazione.pptx

Nel campo **message**, vengono riportate altre ulteriori informazioni sul file (autore, applicazione che ha creato il file e relativa versione dell'applicazione, autore dell'ultima modifica, ecc.)

Campo	Valore
datetime	09/01/2019 07:04:45
timestamp_desc	Creation Time
source	META
source_long	Open XML Metadata
message	Creating App: Microsoft Office PowerPoint App version: 16.0000 Last saved by: Raffaele P Author: Raffaele P Revision number: 195 [...]
parser	czip/oxml

Le Super Timeline

Esempio di Utilizzo 2 | File OOXML | 8/18

3. Analisi del File Prodotto (EsempioOOXML.xlsx)

Campo	Valore
datetime	06/02/2019 12:15:46
timestamp_desc	Content Modification Time
source	FILE
source_long	OS Content Modification Time
message	OS:C:\Users\Raffaele\Plaso\presentazione.pptx Type: file
parser	filestat

Campo	Valore
datetime	06/02/2019 12:15:46
timestamp_desc	Content Modification Time
source	META
source_long	Open XML Metadata
message	Creating App: Microsoft Office PowerPoint App version: 16.0000 Last saved by: Raffaele P Author: Raffaele P Revision number: 195 [...]
parser	czip/oxml

L'ultima modifica (valore **Content Modification Time**, nel campo **timestamp_desc**) del file presentazione.pptx, è avvenuta in data **06/02/2019** alle ore **12:15:46** (valore del campo **datetime**)

I timestamp sono reperiti da due fonti:

- **Metadati del file system**
 - Tali metadati sono reperiti dalla file table (del file system), considerando l'entry, associata al file presentazione.pptx
 - Ad esempio, in NTFS, i suddetti metadati sono contenuti nelle entry della MFT
- **Metadati del formato OOXML**
 - Sono memorizzati all'interno del file presentazione.pptx (ovvero, sono memorizzati direttamente nel contenuto del file)

Campo	Valore
datetime	06/02/2019 12:15:46
timestamp_desc	Content Modification Time
source	FILE
source_long	OS Content Modification Time
message	OS:C:\Users\Raffaele\Plaso\presentazione.pptx Type: file
parser	filestat

Campo	Valore
datetime	06/02/2019 12:15:46
timestamp_desc	Content Modification Time
source	META
source_long	Open XML Metadata
message	Creating App: Microsoft Office PowerPoint App version: 16.0000 Last saved by: Raffaele P Author: Raffaele P Revision number: 195 [...]
parser	czip/oxml

L'ultima modifica (valore **Content Modification Time**, nel campo **timestamp_desc**) del file presentazione.pptx, è avvenuta in data **06/02/2019** alle ore **12:15:46** (valore del campo **datetime**)

I timestamp sono reperiti da due fonti:

- **Metadati del file system**
 - Tali metadati sono reperiti dalla file table (del file system), considerando l'entry, associata al file presentazione.pptx
 - Ad esempio, in NTFS, i suddetti metadati sono contenuti nelle entry della MFT
- **Metadati del formato OOXML**
 - Sono memorizzati all'interno del file presentazione.pptx (ovvero, sono memorizzati direttamente nel contenuto del file)

Campo	Valore
datetime	06/02/2019 12:15:46
timestamp_desc	Content Modification Time
source	FILE
source_long	OS Content Modification Time

Campo	Valore
datetime	06/02/2019 12:15:46
timestamp_desc	Content Modification Time
source	META
source_long	Open XML Metadata

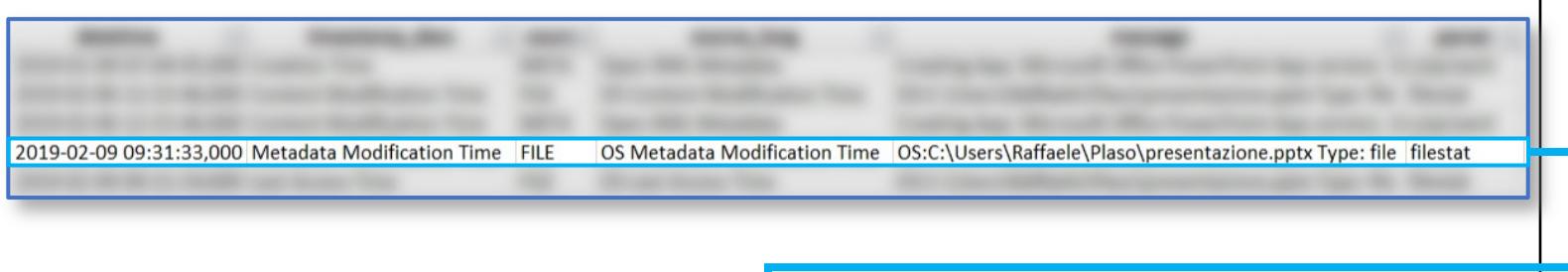
I timestamp, provenienti dalle due fonti, sono coerenti, infatti, la data e l'ora dell'ultima modifica coincidono, sia considerando i **metadati del file system** sia considerando i **metadati del formato OOXM**

Le Super Timeline

Esempio di Utilizzo 2 | File OOXML | 9/18

3. Analisi del File Prodotto (EsempioOOXML.xlsx)

2019-02-09 09:31:33,000 Metadata Modification Time FILE OS Metadata Modification Time OS:C:\Users\Raffaele\Plaso\presentazione.pptx Type: file filestat



Campo	Valore
<code>datetime</code>	09/02/2019 09:31:33
<code>timestamp_desc</code>	Metadata Modification Time
<code>source</code>	FILE
<code>source_long</code>	OS Metadata Modification Time
<code>message</code>	OS:C:\Users\Raffaele\Plaso\presentazione .pptx Type: file
<code>parser</code>	filestat

L'ultima modifica dei metadati, relativi al **file system** (valore **Metadata Modification Time**, nel campo **timestamp_desc**), del file presentazione.pptx, è avvenuta in data **09/02/2019** alle ore **09:31:33** (valore del campo **datetime**)

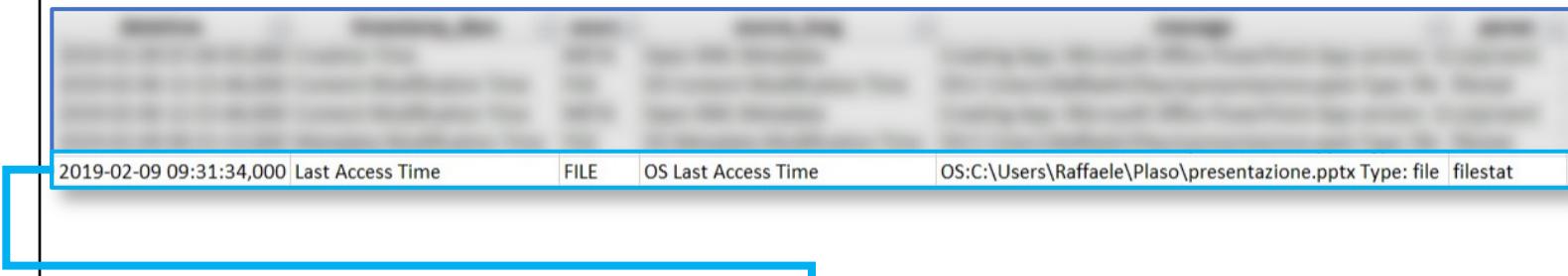
Il timestamp è reperito dai **metadati del file system** (come indicato dai campi **source**, **source_long** e **parser**)

Campo	Valore
datetime	09/02/2019 09:31:33
timestamp_desc	Metadata Modification Time
source	FILE
source_long	OS Metadata Modification Time
message	OS:C:\Users\Raffaele\Plaso\presentazione .pptx Type: file
parser	filestat

Le Super Timeline

Esempio di Utilizzo 2 | File OOXML | 10/18

3. Analisi del File Prodotto (EsempioOOXML.xlsx)

2019-02-09 09:31:34,000	Last Access Time	FILE	OS Last Access Time	OS:C:\Users\Raffaele\Plaso\presentazione.pptx	Type: file	filestat														
																				
<table border="1"><thead><tr><th>Campo</th><th>Valore</th></tr></thead><tbody><tr><td>datetime</td><td>09/02/2019 09:31:34</td></tr><tr><td>timestamp_desc</td><td>Last Access Time</td></tr><tr><td>source</td><td>FILE</td></tr><tr><td>source_long</td><td>OS Last Access Time</td></tr><tr><td>message</td><td>OS:C:\Users\Raffaele\Plaso\presentazione.pptx Type: file</td></tr><tr><td>parser</td><td>filestat</td></tr></tbody></table>							Campo	Valore	datetime	09/02/2019 09:31:34	timestamp_desc	Last Access Time	source	FILE	source_long	OS Last Access Time	message	OS:C:\Users\Raffaele\Plaso\presentazione.pptx Type: file	parser	filestat
Campo	Valore																			
datetime	09/02/2019 09:31:34																			
timestamp_desc	Last Access Time																			
source	FILE																			
source_long	OS Last Access Time																			
message	OS:C:\Users\Raffaele\Plaso\presentazione.pptx Type: file																			
parser	filestat																			

L'ultimo accesso al file (valore **Last Access Time**, nel campo **timestamp_desc**), del file presentazione.pptx, è stato registrato in data **09/02/2019** alle ore **09:31:34** (valore del campo **datetime**)

Il timestamp è reperito dai **metadati del file system** (come indicato dai campi **source**, **source_long** e **parser**)

Campo	Valore
datetime	09/02/2019 09:31:34
timestamp_desc	Last Access Time
source	FILE
source_long	OS Last Access Time
message	OS:C:\Users\Raffaele\Plaso\presentazione .pptx Type: file
parser	filestat

Le Super Timeline

Esempio di Utilizzo 2 | File OOXML | 11/18

OSSERVAZIONE

In questo esempio, Plaso riporta le informazioni MAC in merito ai timestamp, provenienti dai **metadati del file system**

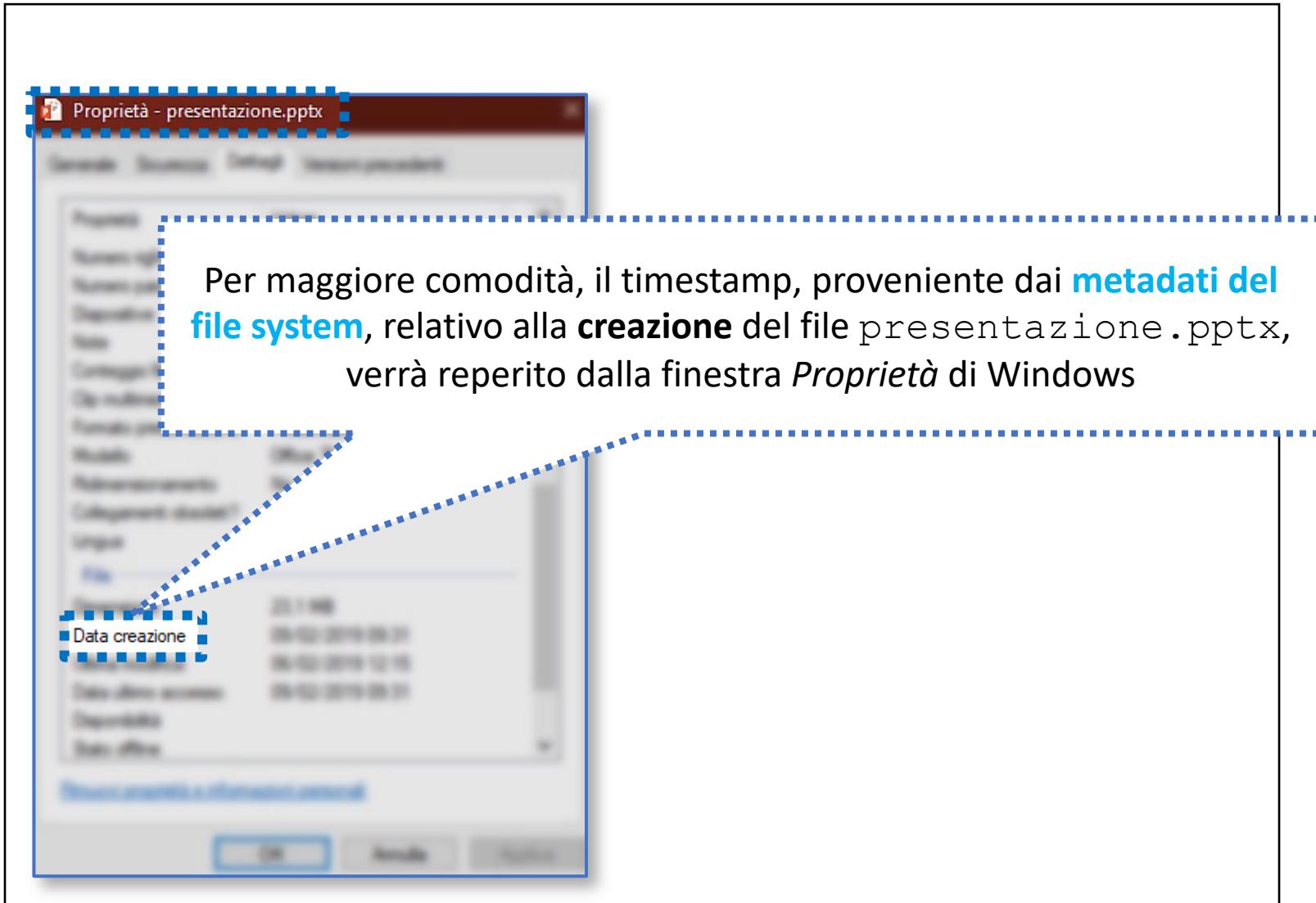
Lettera	Descrizione
M	Data e ora dell'ultima modifica
A	Data e ora dell'ultimo accesso al file
C	Data e ora dell'ultima modifica ai metadati

Nella super timeline, non è quindi presente il timestamp relativo alla **creazione** del file presentazione.pptx, proveniente dai **metadati del file system** (è invece presente solo il timestamp relativo alla creazione, proveniente dai **metadati del formato OOXML**)

Nelle prossime slide, verrà verificata la coerenza, considerando anche il timestamp di creazione, proveniente dai **metadati del file system**

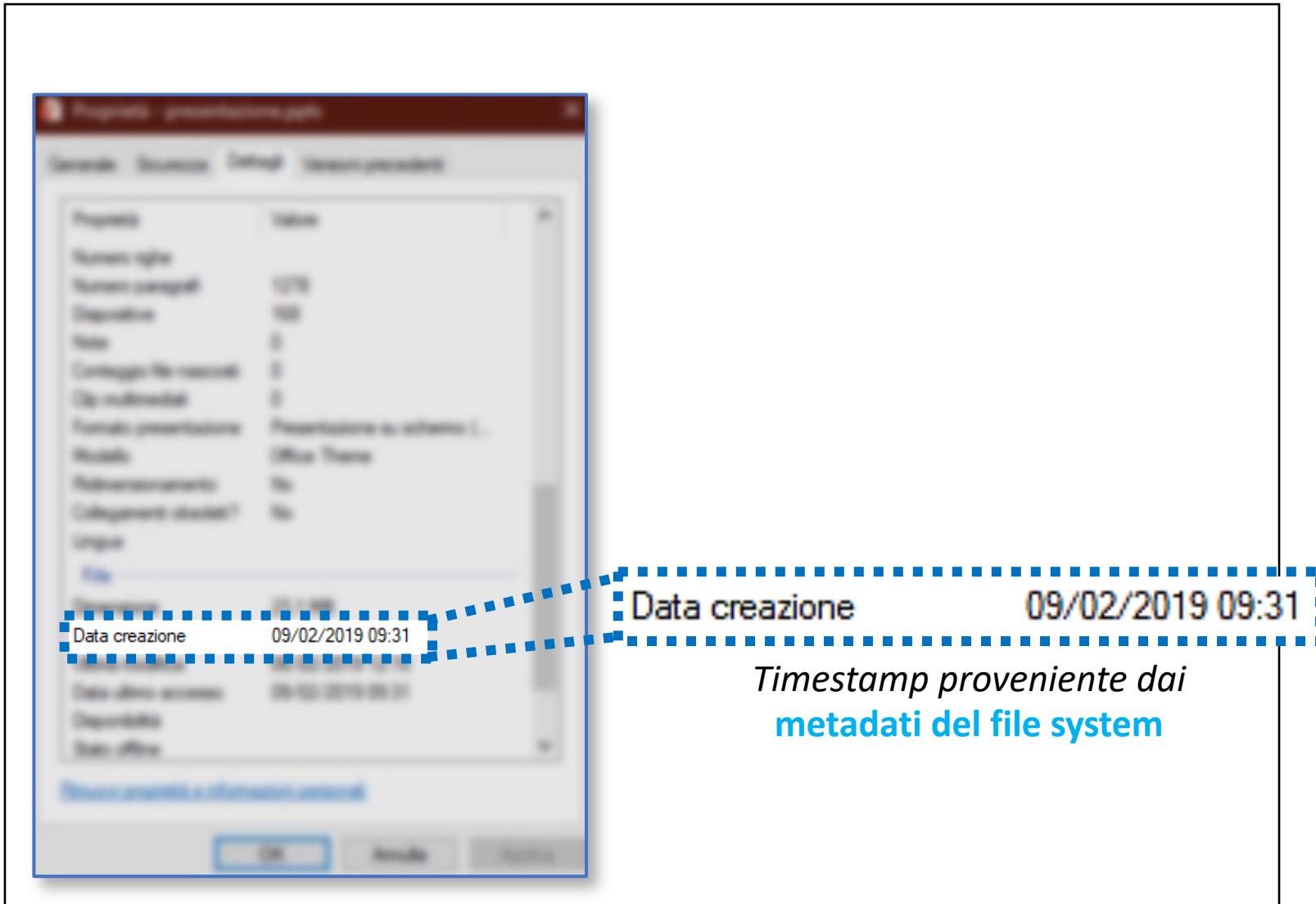
Le Super Timeline

Esempio di Utilizzo 2 | File OOXML | 12/18



Le Super Timeline

Esempio di Utilizzo 2 | File OOXML | 14/18



Le Super Timeline

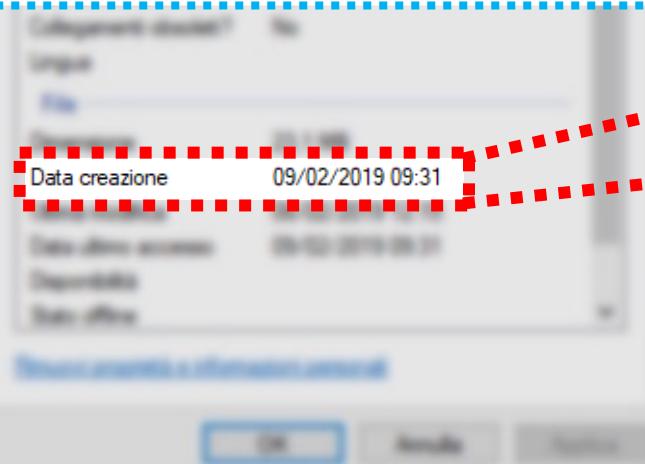
Esempio di Utilizzo 2 | File OOXML | 15/18

Informazioni riguardo la data di creazione incoerenti

Data e ora di creazione fornita da Plaso (ottenuta dai metadati del formato OOXML)	09/01/2019, 07:04:45
Data e ora di creazione, proveniente dai metadati del file system	09/02/2019, 09:31:33

Timestamp ottenuto da Plaso (metadati del formato OOXML)

2019-01-09 07:04:45,000 Creation Time META



Data creazione 09/02/2019 09:31

*Timestamp proveniente dai
metadati del file system*

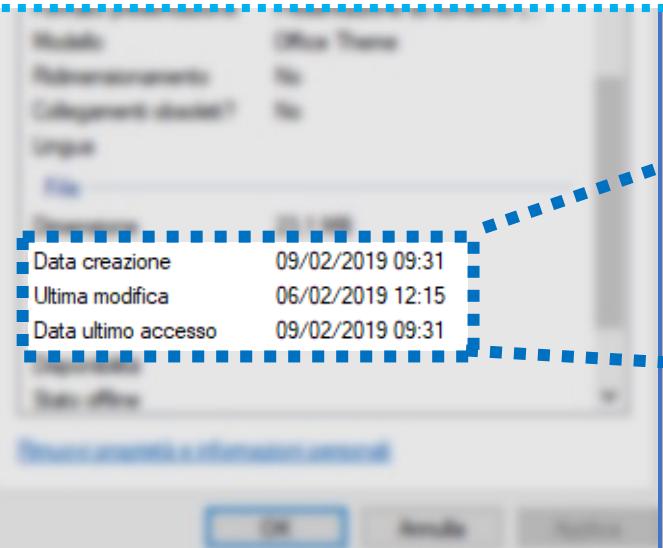
Le Super Timeline

Esempio di timeline di un file nuovo L.16/10

OSSERVAZIONE

In questo caso, è possibile osservare delle **incoerenze**, direttamente dai timestamp, provenienti dai **metadati del file system** (infatti, è possibile notare che la data di creazione sia successiva alla data dell'ultima modifica)

Questo esempio è stato strutturato, volutamente, con l'obiettivo di enfatizzare e semplificare l'individuazione delle incoerenze (le quali sono state evidenziate precedentemente), tuttavia, l'individuazione di tali incoerenze **non è sempre semplice**, ed è pertanto necessario porre particolare attenzione



Data creazione	09/02/2019 09:31
Ultima modifica	06/02/2019 12:15
Data ultimo accesso	09/02/2019 09:31

Timestamp provenienti dai
metadati del file system

Le Super Timeline

Esempio di Utilizzo 2 | File OOXML | 17/18

ALCUNE CONSIDERAZIONI | 1/2

- In generale, una eventuale **incoerenza** tra il timestamp, relativo alla **creazione**, proveniente dai **metadati del file system**, e quello, proveniente dai **metadati del formato del file** (sia esso, un file OOXML, come nell'esempio, oppure, un altro formato che includa metadati nel contenuto del file stesso), dovrebbe far sorgere **diversi interrogativi all'investigatore**, ad esempio:
 - Il file è la copia di un altro file?
 - In caso **affermativo**:
 - L'originale è più aggiornato?
 - L'originale è stato eliminato? Eventualmente, per quale motivo? Potrebbe essersi trattato di un errore?
 - L'originale potrebbe contenere dati che volevano essere tenuti nascosti?
 - È possibile che esistano altre copie, con contenuti (rilevanti) leggermente diversi?
 - In caso **negativo**:
 - L'autore del file è il soggetto su cui si indaga? Può averlo creato su un altro dispositivo e poi copiato su quello in analisi?

Le Super Timeline

Esempio di Utilizzo 2 | File OOXML | 18/18

ALCUNE CONSIDERAZIONI | 2/2

- Altri possibili interrogativi...
 - Potrebbe trattarsi di una sorta di copia di **backup**?
 - In tal caso, ci sono stati aggiornamenti sul file originale?
 - È possibile che si tratti di un tentativo di nascondere qualcosa agli investigatori (strategia anti-forense)?
 - Il soggetto era in possesso di adeguate competenze?
 - È stato aiutato da un'altra persona?
 - Potrebbe contenere dati nascosti, ad esempio, mediante tecniche di steganografia/watermarking (*maggiori dettagli nelle prossime lezioni*)
 - ...

Le Super Timeline

Esempio di Utilizzo 2 | File OOXML | 18/18

ALCUNE CONSIDERAZIONI | 2/2

- Altri possibili interrogativi...
 - Potrebbe trattarsi di una sorta di copia di backup?
 - In tal caso, ci sono stati aggiornamenti sul file originale?

OSSERVAZIONE

Quando viene recuperato un file eliminato, in formato OOXML, durante le attività di file recovery, potrebbe risultare utile analizzare i **metadati del formato OOXML** (poiché non è detto che i **metadati del file system** risultino disponibili)

(dettagli nelle prossime lezioni)

- ...

Le Super Timeline

Esempi di Utilizzo



Esempio di Utilizzo 1
Cronologia Browser Chrome



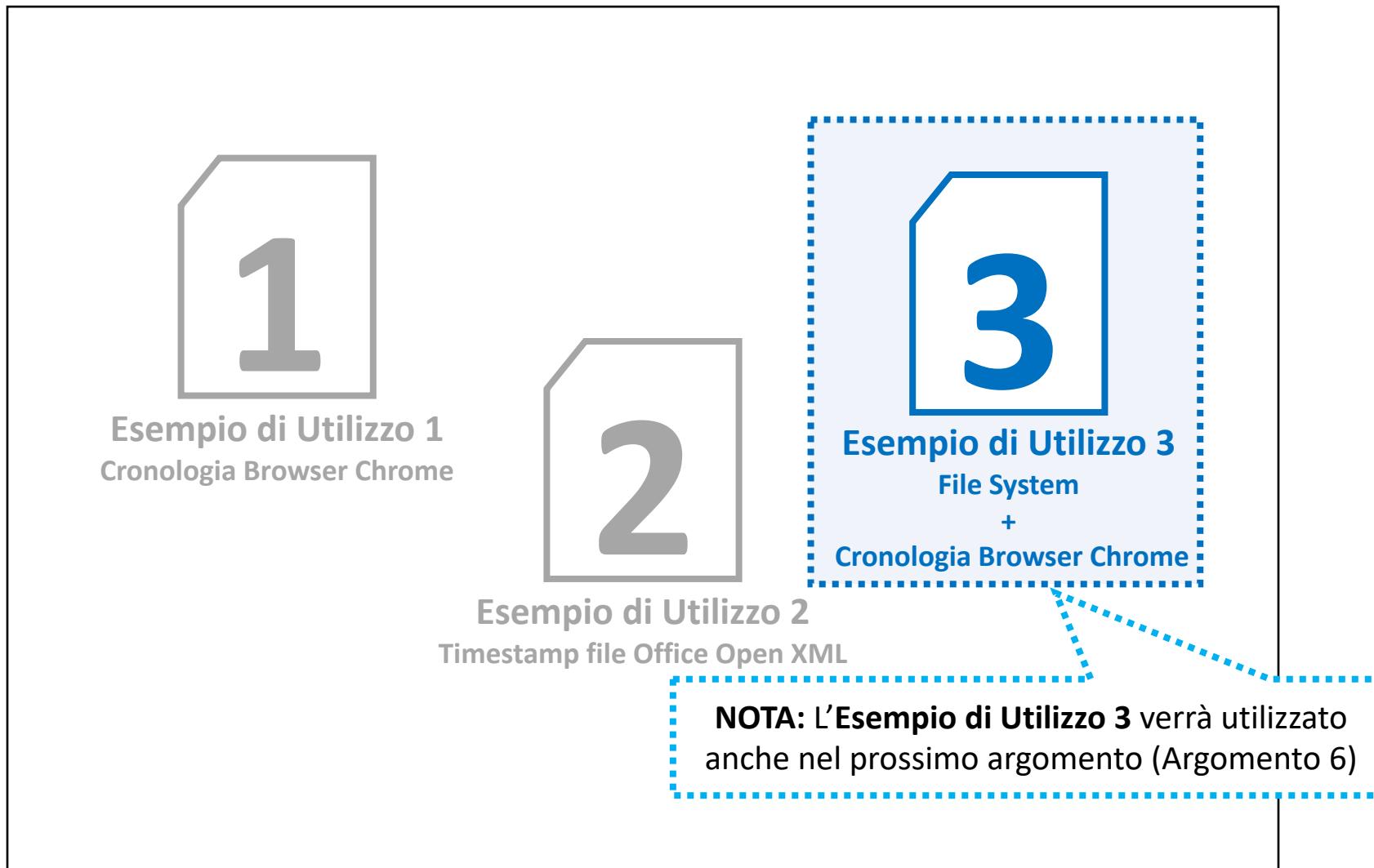
Esempio di Utilizzo 2
Timestamp file Office Open XML



Esempio di Utilizzo 3
File System
+
Cronologia Browser Chrome

Le Super Timeline

Esempi di Utilizzo



Le Super Timeline

Esempio di Utilizzo 3 | File System & Cronologia Chrome | 1/24

- In questo esempio, verrà realizzata una super timeline, in cui saranno considerate due fonti:
 1. **Metadati dell'intero file system NTFS, di un dead system**
 - Tali metadati sono reperiti da una immagine forense (denominata `Win10.dd`), acquisita dal disco fisso (circa ~20GB), di un dead system *simulato* (ospitato su una macchina virtuale), equipaggiato con il sistema operativo Microsoft Windows 10
 2. **Cronologia del browser Google Chorme, estrapolata dal relativo file (memorizzato nel sudetto dead system)**
 - Il file relativo alla cronologia è stato acceduto dal drive «*virtuale*» (contrassegnato dalla lettera `E:`), sul quale è stato effettuato il mounting, in modalità «sola lettura», della suddetta immagine forense
- Per la realizzazione di questa super timeline, utilizzeremo anche il tool **`f1s`** (*dettagli nelle prossime slide*) della suite The Sleuth Kit (TSK)

Le Super Timeline

Esempio di Utilizzo 3 | File System & Cronologia Chrome | 2/24

1. e 2. Creazione della super timeline (1.) e output della stessa in formato human-readable (2.), mediante i tool **f1s**, **log2timeline** e **psort**

Liste delle Istruzioni

- a) **f1s -z Europe/Rome -f ntfs -r -m C: Win10.dd > InfoFileSystem.body**
- b) **log2timeline esempio3.plaso "E:\[...]\History"**
- c) **log2timeline esempio3.plaso InfoFileSystem.body**
- d) **psort -z Europe/Rome -o XLSX -w FileCronologia.xlsx esempio3.plaso**

Le Super Timeline

Esempio di Utilizzo 3 | File System & Cronologia Chrome | 2/24

1. e 2. Creazione della super timeline (1.) e output della stessa in formato human-readable (2.), mediante i tool **f1s**, **log2timeline** e **psort**

Liste delle Istruzioni

- a) `f1s -z Europe/Rome -f ntfs -r -m C: Win10.dd > InfoFileSystem.body`
- b) `log2timeline esempio3.plaso "E:\[...]\History"`
- c) `log2timeline esempio3.plaso InfoFileSystem.body`
- d) `psort -z Europe/Rome -o XLSX -w FileCronologia.xlsx esempio3.plaso`

Le Super Timeline

Esempio di Utilizzo 3 | File System & Cronologia Chrome | 2/24

a)

```
f1s -z Europe/Rome -f ntfs -r -m C: Win10.dd > InfoFileSystem.body
```

- Il tool **f1s** elenca tutti i file e le directory, presenti all'interno di un file system, esplicitando, per ciascuno di essi, diverse informazioni
- Nell'esempio, **f1s** è stato utilizzato per i timestamp (in formato MACB) di tutti i file/directory
- I parametri forniti sono i seguenti:

-z Europe/Rome Specifica il fuso orario (*timezone*): Europa/Roma

-f Specifica il tipo di file system: NTFS

-r Specifica che il contenuto delle directory deve essere considerato ricorsivamente (es., contenuto di directory all'interno di altre directory, e così via)

C: Specifica che i file devono essere considerati a partire dalla cartella **C:**

Win10.dd L'immagine da cui ottenere le informazioni sui file

InfoFileSystem.body Il file in cui verrà memorizzato l'output (nel formato denominato *body* (specificato dall'opzione **-m**))

Le Super Timeline

Esempio di Utilizzo 3 | File System & Cronologia Chrome | 2/24

1. e 2. Creazione della super timeline (1.) e output della stessa in formato human-readable (2.), mediante i tool **f1s**, **log2timeline** e **psort**

Liste delle Istruzioni

- a) `f1s -z Europe/Rome -f ntfs -r -m C: Win10.dd > InfoFileSystem.body`
- b) `log2timeline esempio3.plaso "E:\[...]\History"`
- c) `log2timeline esempio3.plaso InfoFile body`
- d) `psort -z Europe/Rome -o XLSX -w FileC esempio3.plaso`

Per brevità, il percorso completo, è stato omesso (si ricorda che il file è acceduto dal drive «*virtuale*», associato alla lettera **E:**, in cui si è effettuato il mounting, in sola lettura, dell'immagine forense)

Il percorso completo del file è il seguente:

`E:\Users\Raffaele\AppData\Local\Google\Chrome\User Data\Default\History`

Le Super Timeline

Esempio di Utilizzo 3 | File System & Cronologia Chrome | 2/24

1. e 2. Creazione della super timeline (1.) e output della stessa in formato human-readable (2.), mediante i tool **f1s**, **log2timeline** e **psort**

Liste delle Istruzioni

- a) `f1s -z Europe/Rome -f ntfs -r -m C: Win10.dd > InfoFileSystem.body`
- b) `log2timeline esempio3.plaso "E:\[...]\History"`
- c) `log2timeline esempio3.plaso InfoFileSystem.body`
- d) `psort -z Europe/Rome -o XLSX -w FileCronologia.xlsx esempio3.plaso`

Le due esecuzioni del tool **log2timeline**, del framework Plaso, fanno riferimento al medesimo file di output (**esempio3.plaso**), al quale vengono aggiunte:

- Informazioni provenienti dal file, relativo alla cronologia di Chrome (**istruzione b)**)
- Informazioni provenienti dal file system (**istruzione c)**
 - Si ricorda che tali informazioni sono state ottenute, tramite il tool **f1s**, dall'**istruzione a)**

Le Super Timeline

Esempio di Utilizzo 3 | File System & Cronologia Chrome | 2/24

1. e 2. Creazione della super timeline (1.) e output della stessa in formato human-readable (2.), mediante i tool **f1s**, **log2timeline** e **psort**

Liste delle Istruzioni

a) `f1s -z Europe/Rome -f ntfs -r -m C: Win10.dd > InfoFileSystem.body`

b) `log2timeline esempio3.plaso "E:\[...]\History"`

c) `log2timeline esempio3.plaso InfoFileSystem.body`

d) `psort -z Europe/Rome -o XLSX -w FileCronologia.xlsx esempio3.plaso`

- Viene infine eseguito il tool **psort**, al fine di convertire il file `esempio3.plaso` (in formato Plaso), in formato XLSX (opzione `-o XLSX`)
- Anche in questo caso è utilizzato il fuso orario Europa/Roma (opzione `-z Europe/Rome`)
- Il nome prodotto è **FileCronologia.xlsx**
 - NOTA: Tale file è disponibile al download sulla piattaforma e-Learning (in formato ZIP, ~30 MB)

Le Super Timeline

Esempio di Utilizzo 3 | File System & Cronologia Chrome | 3/24

3. Analisi (*parziale*) Versione *Preprocessata* del File Prodotto

- Il file prodotto è costituito da oltre **un milione di entry**
 - Sono stati infatti estrapolati **1.039.826** di eventi
- Il suddetto file è stato **preliminarmente preprocessato ed esemplificato**, in modo da renderlo più fruibile, ed è strutturato come segue:
 - In **nero e grassetto** sono riportati, esclusivamente, i **file** (ed i relativi timestamp), **potenzialmente rilevanti**, per la definizione di un **possibile scenario investigativo** [informazioni estrapolate dalla *Fonte 1.*]
 - In **ciano e grassetto** sono riportate alcune informazioni, in maniera sintetica, in merito ad alcuni eventi [*Fonte 1.*]
 - In **rosso scuro e grassetto** sono riportati gli **URL visitati** (ed i relativi timestamp), estrapolati dalla *Fonte 2.*

Le Super Timeline

Esempio di Utilizzo 3 | File System & Cronologia Chrome | 3/24

3. Analisi (parziale) Versione Preprocessata del File Prodotto

- Il file prodotto è costituito da oltre un milione di entry
 - Sono stati infatti estrapolati 1.039.826 di eventi
- Il suddetto file è stato preliminarmente preprocessato ed esemplificato, in modo da renderlo più fruibile, ed è strutturato come segue:
 - In **nero e grassetto** sono riportati, esclusivamente, i **file** (ed i relativi timestamp), potenzialmente rilevanti, per la definizione di un possibile scenario investigativo [informazioni estrapolate dalla *Fonte 1.*]
 - In **ciano e grassetto** sono riportate alcune informazioni, in maniera sintetica, in merito ad alcuni eventi [*Fonte 1.*]
 - In **rosso scuro e grassetto** sono riportati gli **URL visitati** (ed i relativi timestamp), estrapolati dalla *Fonte 2.*

La versione preprocessata del file è scaricabile dalla piattaforma e-Learning, in formato ZIP (Nome del file: `FileCronologia_Preprocessato.zip`)

Le Super Timeline

Esempio di Utilizzo 3 | File System & Cronologia Chrome | 4/24

3. Analisi (parziale) Versione Preprocessata del File Prodotto

Ora	Descrizione	Path oppure URL
00:00:00	Accesso al sito web	/index.html

Il file preprocessato è organizzato in una tabella, costituita dalle seguenti tre colonne:

- **Ora**
 - Riporta l'ora in cui si è verificato l'evento (gli eventi di interesse, si sono verificati tutti nella stessa data)
- **Descrizione**
 - Riporta una breve descrizione testuale dell'evento (ad esempio, visita di un URL)
- **Path oppure URL**
 - Specifica il path nel file system o l'URL, coinvolto nell'evento

Le Super Timeline

Esempio di Utilizzo 3 | File System & Cronologia Chrome | 5/24

3. Analisi (parziale) Versione Preprocessata del File Prodotto

18:37:34	Visita URL	http://www.di.unisa.it/home/eventi	[Aggiornamenti Cache di Google Chrome]
18:37:39	Visita URL	https://www.di.unisa.it/home/eventi?archive=1	[Aggiornamenti Cache di Google Chrome]
18:37:34	Visita URL	http://www.di.unisa.it/home/eventi	[Aggiornamenti Cache di Google Chrome]
18:37:39	Visita URL	https://www.di.unisa.it/home/eventi?archive=1	[Aggiornamenti Cache di Google Chrome]

Iniziamo l'analisi dalle prime due entry significative,
ovvero, i due URL, riportati in **rosso scuro e grassetto**

Le Super Timeline

Esempio di Utilizzo 3 | File System & Cronologia Chrome | 6/24

3. Analisi (parziale) Versione Preprocessata del File Prodotto

18:37:34	Visita URL	http://www.di.unisa.it/home/eventi	[Aggiornamenti Cache di Google Chrome]
18:37:39	Visita URL	https://www.di.unisa.it/home/eventi?archive=1	[Aggiornamenti Cache di Google Chrome]

È possibile osservare che sono stati visitati i seguenti URL:

- <http://www.di.unisa.it/home/eventi>
 - Lista degli Eventi del Dipartimento di Informatica (DI) dell'Università di Salerno
 - Visita avvenuta alle 18:37:34
- <https://www.di.unisa.it/home/eventi?archive=1>
 - Lista degli Eventi Archiviati
 - Visita avvenuta alle 18:37:39

Le Super Timeline

Esempio di Utilizzo 3 | File System & Cronologia Chrome | 6/24

3. Analisi (parziale) Versione Preprocessata del File Prodotto

18:37:34	Visita URL	http://www.di.unisa.it/home/eventi
----------	------------	---

[Aggiornamenti Cache di Google Chrome]

18:37:39	Visita URL	https://www.di.unisa.it/home/eventi?archive=1
----------	------------	---

[Aggiornamenti Cache di Google Chrome]

Esempio Aggiornamenti Cache di Google Chrome [Dal File NON Preprocessato]

18:37:34,237	Last Visited Time	WEBHIST	Chrome History	https://www.di.unisa.it/home/eventi (Home Eventi) [count: 0] Visit from: http://www.di.unisa.it/home/eventi
18:37:34,237	Last Visited Time	WEBHIST	Chrome History	http://www.di.unisa.it/home/eventi (Home Eventi) [count: 0] Type: [LINK - User clicked a link] (URL not type)
18:37:35,000	Content Modification Time	FILE	Mactime Bodyfile	C:/Windows/Logs/dosvc/dosvc.20190209_183234_547.etl
18:37:35,000	Metadata Modification Time	FILE	Mactime Bodyfile	C:/Windows/Logs/dosvc/dosvc.20190209_183234_547.etl
18:37:36,000	Content Modification Time	FILE	Mactime Bodyfile	C:/Users/Raffaele/AppData/Local/Google/Chrome/User Data/Default/Cache/f_000015 (\$FILE_NAME)
18:37:36,000	Creation Time	FILE	Mactime Bodyfile	C:/Users/Raffaele/AppData/Local/Google/Chrome/User Data/Default/Cache/f_000015 (\$FILE_NAME)
18:37:36,000	Last Access Time	FILE	Mactime Bodyfile	C:/Users/Raffaele/AppData/Local/Google/Chrome/User Data/Default/Cache/f_000015 (\$FILE_NAME)
18:37:36,000	Metadata Modification Time	FILE	Mactime Bodyfile	C:/Users/Raffaele/AppData/Local/Google/Chrome/User Data/Default/Cache/f_000015 (\$FILE_NAME)
18:37:36,000	Content Modification Time	FILE	Mactime Bodyfile	C:/Users/Raffaele/AppData/Local/Google/Chrome/User Data/Default/Cache/f_000015
18:37:36,000	Creation Time	FILE	Mactime Bodyfile	C:/Users/Raffaele/AppData/Local/Google/Chrome/User Data/Default/Cache/f_000015
18:37:36,000	Last Access Time	FILE	Mactime Bodyfile	C:/Users/Raffaele/AppData/Local/Google/Chrome/User Data/Default/Cache/f_000015
18:37:36,000	Metadata Modification Time	FILE	Mactime Bodyfile	C:/Users/Raffaele/AppData/Local/Google/Chrome/User Data/Default/Cache/f_000015
18:37:39,000	Last Visited Time	WEBHIST	Chrome History	https://www.di.unisa.it/home/eventi?archive=1 (Home Eventi) [count: 0] Visit from: https://www.di.unisa.it/home/eventi
18:37:39,000	Content Modification Time	FILE	Mactime Bodyfile	C:/Users/Raffaele/AppData/Local/Google/Chrome/User Data/Default/Cache/f_000016 (\$FILE_NAME)
18:37:39,000	Creation Time	FILE	Mactime Bodyfile	C:/Users/Raffaele/AppData/Local/Google/Chrome/User Data/Default/Cache/f_000016 (\$FILE_NAME)
18:37:39,000	Last Access Time	FILE	Mactime Bodyfile	C:/Users/Raffaele/AppData/Local/Google/Chrome/User Data/Default/Cache/f_000016 (\$FILE_NAME)
18:37:39,000	Metadata Modification Time	FILE	Mactime Bodyfile	C:/Users/Raffaele/AppData/Local/Google/Chrome/User Data/Default/Cache/f_000016 (\$FILE_NAME)
18:37:39,000	Content Modification Time	FILE	Mactime Bodyfile	C:/Users/Raffaele/AppData/Local/Google/Chrome/User Data/Default/Cache/f_000016
18:37:39,000	Creation Time	FILE	Mactime Bodyfile	C:/Users/Raffaele/AppData/Local/Google/Chrome/User Data/Default/Cache/f_000016
18:37:39,000	Last Access Time	FILE	Mactime Bodyfile	C:/Users/Raffaele/AppData/Local/Google/Chrome/User Data/Default/Cache/f_000016
18:37:39,000	Metadata Modification Time	FILE	Mactime Bodyfile	C:/Users/Raffaele/AppData/Local/Google/Chrome/User Data/Default/Cache/f_000016
18:37:40,000	Content Modification Time	FILE	Mactime Bodyfile	C:/Users/Raffaele/AppData/Local/Google/Chrome/User Data/Default/Local Storage/leveldb/000003.log
18:37:40,000	Metadata Modification Time	FILE	Mactime Bodyfile	C:/Users/Raffaele/AppData/Local/Google/Chrome/User Data/Default/Local Storage/leveldb/000003.log

Le Super Timeline

Esempio di Utilizzo 3 | File System & Cronologia Chrome | 6/24

3. Analisi (parziale) Versione Preprocessata del File Prodotto

18:37:34	Visita URL	http://www.di.unisa.it/home/eventi
[Aggiornamenti Cache di Google Chrome]		

18:37:39	Visita URL	https://www.di.unisa.it/home/eventi?archive=1
[Aggiornamenti Cache di Google Chrome]		

Esempio Aggiornamenti Cache di Google Chrome [Dal File NON Preprocessato]

18:37:34,237	Last Visited Time	WEBHIST	Chrome History	https://www.di.unisa.it/home/eventi (Home Eventi) [count: 0] Visit from: http://www.di.unisa.it/home/ev
18:37:34,237	Last Visited Time	WEBHIST	Chrome History	http://www.di.unisa.it/home/eventi (Home Eventi) [count: 0] Type: [LINK - User clicked a link] (URL not type
18:37:35,000	Content Modification Time	FILE	Mactime Bodyfile	C:/Windows/Logs/dosvc/dosvc.20190209_183234_547.etl
18:37:35,000	Metadata Modification Time	FILE	Mactime Bodyfile	C:/Windows/Logs/dosvc/dosvc.20190209_183234_547.etl
18:37:36,000	Content Modification Time	FILE	Mactime Bodyfile	C:/Users/Raffaele/AppData/Local/Google/Chrome/User Data/Default/Cache/f_000015 (\$FILE_NAME)
18:37:36,000	Creation Time	FILE	Mactime Bodyfile	C:/Users/Raffaele/AppData/Local/Google/Chrome/User Data/Default/Cache/f_000015 (\$FILE_NAME)
18:37:36,000	Last Access Time	FILE	Mactime Bodyfile	C:/Users/Raffaele/AppData/Local/Google/Chrome/User Data/Default/Cache/f_000015 (\$FILE_NAME)
18:37:36,000	Metadata Modification Time	FILE	Mactime Bodyfile	C:/Users/Raffaele/AppData/Local/Google/Chrome/User Data/Default/Cache/f_000015 (\$FILE_NAME)
18:37:36,000	Content Modification Time	FILE	Mactime Bodyfile	C:/Users/Raffaele/AppData/Local/Google/Chrome/User Data/Default/Cache/f_000015

OSSERVAZIONE IMPORTANTE

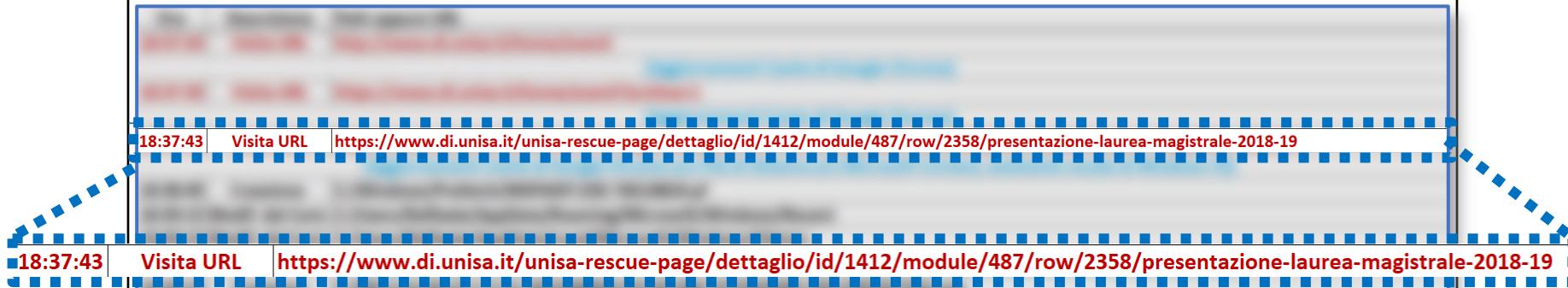
In questo e nei successivi casi, l'attività di navigazione Web, mediante Google Chrome, presenta tracce, osservabili dalla super timeline, fra loro coerenti, reperite dalle seguenti due fonti:

- Visita di un URL [Informazione ottenuta dalla **Fonte 2.** – Cronologia di Google Chrome]
- Conseguenti aggiornamenti dei file di cache di Google Chrome [Informazioni ottenute dalla **Fonte 1.** – Metadati del file system]

Le Super Timeline

Esempio di Utilizzo 3 | File System & Cronologia Chrome | 7/24

3. Analisi (parziale) Versione Preprocessata del File Prodotto

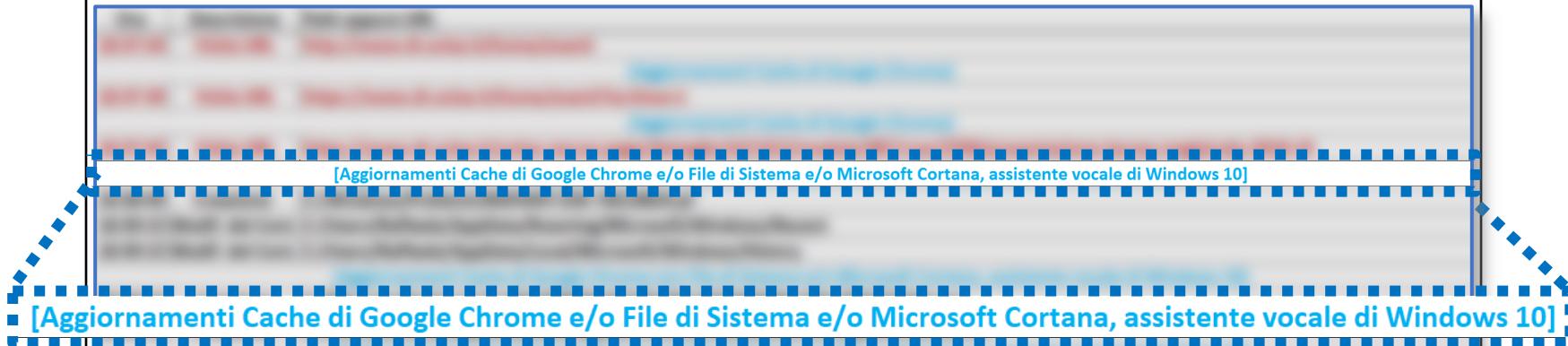


Alle 18:37:43, è stata effettuata una visita al seguente URL:
<https://www.di.unisa.it/unisa-rescue-page/dettaglio/id/1412/module/487/row/2358/presentazione-laurea-magistrale-2018-19>
(Dettaglio di un evento archiviato del DI dell'Università di Salerno)

Le Super Timeline

Esempio di Utilizzo 3 | File System & Cronologia Chrome | 8/24

3. Analisi (parziale) Versione Preprocessata del File Prodotto



Successivamente, sono state effettuate delle operazioni di aggiornamento delle cache di Google Chrome, seguite da operazioni di aggiornamento di file di sistema e Microsoft Cortana (*maggiori dettagli nella prossima slide*)

NOTA: Microsoft Cortana è l'assistente vocale di Microsoft Windows 10

Le Super Timeline

Esempio di Utilizzo 3 | File System & Cronologia Chrome | 9/24

3. Analisi (parziale) Versione Preprocessata del File Prodotto

[Aggiornamenti Cache di Google Chrome e/o File di Sistema e/o Microsoft Cortana, assistente vocale di Windows 10]

Esempio Aggiornamenti Cache di Microsoft Cortana e File di Sistema [Dal File NON Preprocessato]

18:38:20,000	Metadata Modification Time	FILE	Mactime Bodyfile	C:/Users/Raffaele/AppData/Local/Google/Chrome/User Data/BrowserMetrics-spare.pma
18:38:23,000	Content Modification Time	FILE	Mactime Bodyfile	C:/Users/Raffaele/AppData/Local/Packages/Microsoft.MicrosoftEdge_8wekyb3d8bbwe/AC/#!001/MicrosoftEdge/Cache/H4FZA4H3
18:38:23,000	Last Access Time	FILE	Mactime Bodyfile	C:/Users/Raffaele/AppData/Local/Packages/Microsoft.MicrosoftEdge_8wekyb3d8bbwe/AC/#!001/MicrosoftEdge/Cache/H4FZA4H3
18:38:23,000	Metadata Modification Time	FILE	Mactime Bodyfile	C:/Users/Raffaele/AppData/Local/Packages/Microsoft.MicrosoftEdge_8wekyb3d8bbwe/AC/#!001/MicrosoftEdge/Cache/H4FZA4H3
18:38:34,000	Content Modification Time	FILE	Mactime Bodyfile	C:/Users/Raffaele/AppData/Local/Packages/Microsoft.Windows.Cortana_cw5n1h2txyewy/AC/INetCache/DDLDAYY8/3a8048a4[1].js (\$FILE_NAME)
18:38:34,000	Creation Time	FILE	Mactime Bodyfile	C:/Users/Raffaele/AppData/Local/Packages/Microsoft.Windows.Cortana_cw5n1h2txyewy/AC/INetCache/DDLDAYY8/3a8048a4[1].js (\$FILE_NAME)
18:38:34,000	Last Access Time	FILE	Mactime Bodyfile	C:/Users/Raffaele/AppData/Local/Packages/Microsoft.Windows.Cortana_cw5n1h2txyewy/AC/INetCache/DDLDAYY8/3a8048a4[1].js (\$FILE_NAME)
18:38:34,000	Metadata Modification Time	FILE	Mactime Bodyfile	C:/Users/Raffaele/AppData/Local/Packages/Microsoft.Windows.Cortana_cw5n1h2txyewy/AC/INetCache/DDLDAYY8/3a8048a4[1].js (\$FILE_NAME)
18:38:34,000	Content Modification Time	FILE	Mactime Bodyfile	C:/Users/Raffaele/AppData/Local/Packages/Microsoft.Windows.Cortana_cw5n1h2txyewy/AC/INetCache/DDLDAYY8/3a8048a4[1].js
18:38:34,000	Creation Time	FILE	Mactime Bodyfile	C:/Users/Raffaele/AppData/Local/Packages/Microsoft.Windows.Cortana_cw5n1h2txyewy/AC/INetCache/DDLDAYY8/3a8048a4[1].js
18:38:34,000	Last Access Time	FILE	Mactime Bodyfile	C:/Users/Raffaele/AppData/Local/Packages/Microsoft.Windows.Cortana_cw5n1h2txyewy/AC/INetCache/DDLDAYY8/3a8048a4[1].js
18:38:34,000	Metadata Modification Time	FILE	Mactime Bodyfile	C:/Users/Raffaele/AppData/Local/Packages/Microsoft.Windows.Cortana_cw5n1h2txyewy/AC/INetCache/DDLDAYY8/3a8048a4[1].js
18:38:34,000	Content Modification Time	FILE	Mactime Bodyfile	C:/Users/Raffaele/AppData/Local/Packages/Microsoft.Windows.Cortana_cw5n1h2txyewy/AC/INetCache/IQNPS7EX/2743db28[1].css (\$FILE_NAME)
18:38:34,000	Creation Time	FILE	Mactime Bodyfile	C:/Users/Raffaele/AppData/Local/Packages/Microsoft.Windows.Cortana_cw5n1h2txyewy/AC/INetCache/IQNPS7EX/2743db28[1].css (\$FILE_NAME)
18:38:34,000	Last Access Time	FILE	Mactime Bodyfile	C:/Users/Raffaele/AppData/Local/Packages/Microsoft.Windows.Cortana_cw5n1h2txyewy/AC/INetCache/IQNPS7EX/2743db28[1].css (\$FILE_NAME)
18:38:34,000	Metadata Modification Time	FILE	Mactime Bodyfile	C:/Users/Raffaele/AppData/Local/Packages/Microsoft.Windows.Cortana_cw5n1h2txyewy/AC/INetCache/IQNPS7EX/2743db28[1].css (\$FILE_NAME)
18:38:34,000	Content Modification Time	FILE	Mactime Bodyfile	C:/Users/Raffaele/AppData/Local/Packages/Microsoft.Windows.Cortana_cw5n1h2txyewy/AC/INetCache/IQNPS7EX/2743db28[1].css
18:38:34,000	Creation Time	FILE	Mactime Bodyfile	C:/Users/Raffaele/AppData/Local/Packages/Microsoft.Windows.Cortana_cw5n1h2txyewy/AC/INetCache/IQNPS7EX/2743db28[1].css
18:38:34,000	Last Access Time	FILE	Mactime Bodyfile	C:/Users/Raffaele/AppData/Local/Packages/Microsoft.Windows.Cortana_cw5n1h2txyewy/AC/INetCache/IQNPS7EX/2743db28[1].css
18:38:34,000	Metadata Modification Time	FILE	Mactime Bodyfile	C:/Users/Raffaele/AppData/Local/Packages/Microsoft.Windows.Cortana_cw5n1h2txyewy/AC/INetCache/IQNPS7EX/2743db28[1].css
18:38:34,000	Content Modification Time	FILE	Mactime Bodyfile	C:/Users/Raffaele/AppData/Local/Packages/Microsoft.Windows.Cortana_cw5n1h2txyewy/AC/INetCache/Q10U0JDH/home[1].htm (\$FILE_NAME)
18:38:34,000	Creation Time	FILE	Mactime Bodyfile	C:/Users/Raffaele/AppData/Local/Packages/Microsoft.Windows.Cortana_cw5n1h2txyewy/AC/INetCache/Q10U0JDH/home[1].htm (\$FILE_NAME)
18:38:34,000	Last Access Time	FILE	Mactime Bodyfile	C:/Users/Raffaele/AppData/Local/Packages/Microsoft.Windows.Cortana_cw5n1h2txyewy/AC/INetCache/Q10U0JDH/home[1].htm (\$FILE_NAME)

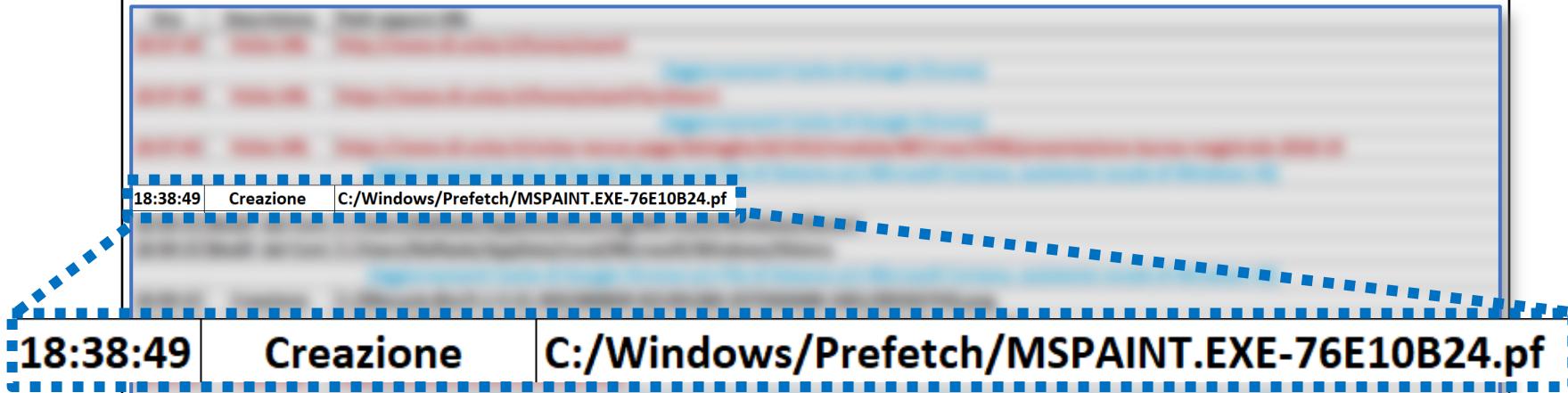
NOTA: Gli aggiornamenti sono stati effettuati da Windows e/o dal software Cortana stesso

Si noti che verosimilmente non esiste alcuna correlazione tra l'aggiornamento della cache di Google Chrome e l'aggiornamento di Microsoft Cortana/file di sistema (i due eventi sono verosimilmente non correlati)

Le Super Timeline

Esempio di Utilizzo 3 | File System & Cronologia Chrome | 10/24

3. Analisi (parziale) Versione Preprocessata del File Prodotto



A questo punto, vengono effettuate alcune operazioni, svolte in automatico da Windows (comportamento legittimo), potenzialmente rilevanti per l'investigazione, poiché probabilmente effettuate a seguito di azioni dell'utente

Le Super Timeline

Esempio di Utilizzo 3 | File System & Cronologia Chrome | 11/24

3. Analisi (parziale) Versione Preprocessata del File Prodotto

18:38:49

Creazione

C:/Windows/Prefetch/MSPAIN.TEX-76E10B24.pf

Viene creato un file dal nome MSPAIN.TEX-76E10B24.pf, all'interno della cartella C:\Windows\Prefetch

NOTA: Nei percorsi del file system, Windows non fa differenza tra i caratteri / e \ (quindi, ad esempio, C:/Pippo.txt è equivalente a C:\Pippo.txt)

Le Super Timeline

Esempio di Utilizzo 3 | File System & Cronologia Chrome | 11/24

3. Analisi (parziale) Versione Preprocessata del File Prodotto

18:38:49

Creazione

C:/Windows/Prefetch/MSPAIN.TEXE-76E10B24.pf

Viene creato un file dal nome MSPAIN.TEXE-76E10B24.pf, all'interno della cartella C:\Windows\Prefetch

La cartella Prefetch (Cenni) | 1/3

La cartella C:\Windows\Prefetch fa riferimento ad una cartella speciale di Windows, denominata appunto Prefetch

Questa cartella viene utilizzata da Windows per incrementare le performance di sistema, effettuando un pre-caricamento di alcune «parti» di codice delle applicazioni usate più comunemente

Dal punto di vista forense, la cartella Prefetch è molto utile, al fine di individuare quali applicativi sono stati utilizzati nel sistema

Le Super Timeline

Esempio di Utilizzo 3 | File System & Cronologia Chrome | 11/24

3. Analisi (parziale) Versione Preprocessata del File Prodotto

18:38:49

Creazione

C:/Windows/Prefetch/MSPAIN.TEXE-76E10B24.pf

Viene creato un file dal nome MSPAIN.TEXE-76E10B24.pf, all'interno della cartella C:\Windows\Prefetch

La cartella Prefetch (Cenni) | 2/3

Ogni «parte» di applicazione/processo viene mappata in un file, il cui nome ha il seguente formato:

<NOMEFILE_ESEGUIBILE>-<VALORE_HASH>.pf

Il file MSPAIN.TEXE-76E10B24.pf, ha un formato conforme:

MSPAIN.TEXE-76E10B24.pf

Le Super Timeline

Esempio di Utilizzo 3 | File System & Cronologia Chrome | 11/24

3. Analisi (parziale) Versione Preprocessata del File Prodotto

18:38:49

Creazione

C:/Windows/Prefetch/MSPAIN.TEXE-76E10B24.pf

Viene creato un file dal nome MSPAIN.TEXE-76E10B24.pf, all'interno della cartella C:\Windows\Prefetch

La cartella Prefetch (Cenni) | 3/3

La cartella Prefetch ed altri artefatti di Windows (alcuni dei quali, introdotti brevemente nelle prossime slide, ed evidenziati in **grassetto e viola**) verranno trattati con maggior dettaglio nelle prossime lezioni

Le informazioni derivanti dai suddetti artefatti, possono essere molto utili, al fine di ricostruire in maniera più accurata possibile lo scenario

Le Super Timeline

Esempio di Utilizzo 3 | File System & Cronologia Chrome | 12/24

3. Analisi (parziale) Versione Preprocessata del File Prodotto

18:38:49

Creazione

C:/Windows/Prefetch/MSPAIN.TEXE-76E10B24.pf

Viene creato un file dal nome MSPAIN.TEXE-76E10B24.pf, all'interno della cartella C:\Windows\Prefetch

In questo caso, Windows ha memorizzato, nella cartella Prefetch, una «parte» di codice dell'applicazione, avente come eseguibile il file MSPAIN.TEXE, poiché probabilmente il software è stato avviato dall'utente

Le Super Timeline

Esempio di Utilizzo 3 | File System & Cronologia Chrome | 12/24

3. Analisi (parziale) Versione Preprocessata del File Prodotto

18:38:49

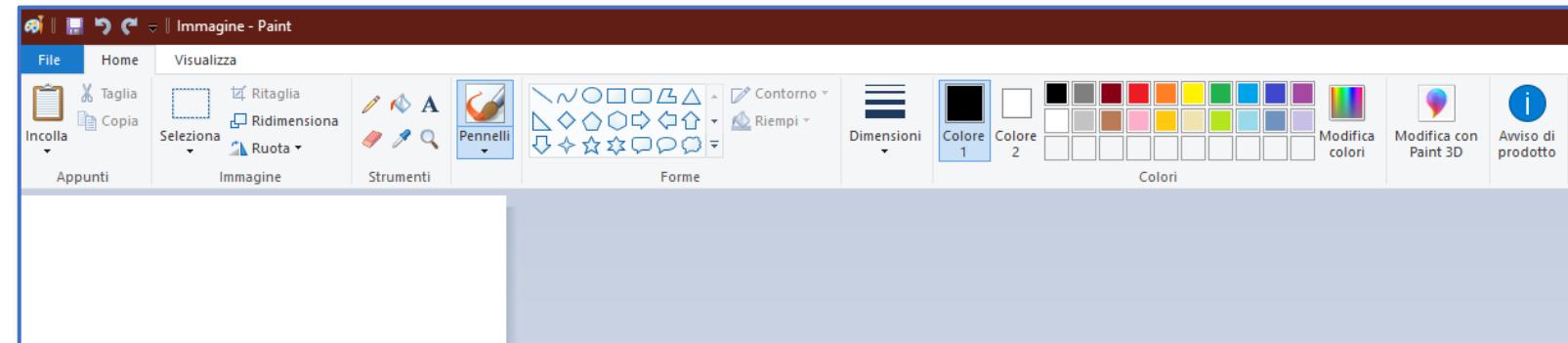
Creazione

C:/Windows/Prefetch/MSPAIN.TEX-76E10B24.pf

Viene creato un file dal nome MSPAIN.TEX-76E10B24.pf, all'interno della cartella C:\Windows\Prefetch

In questo caso, Windows ha memorizzato, nella cartella Prefetch, una «parte» di codice dell'applicazione, avente come eseguibile il file **MSPAIN . EXE**, poiché probabilmente il software è stato avviato dall'

L'eseguibile MSPAIN . EXE, fa riferimento al noto e semplice software di grafica, Microsoft Paint



Le Super Timeline

Esempio di Utilizzo 3 | File System & Cronologia Chrome | 13/24

3. Analisi (parziale) Versione Preprocessata del File Prodotto

18:38:49 Creazione C:/Windows/Prefetch/MSPAIN.T.EXE-76E10B24.pf

OSSERVAZIONE IMPORTANTE

È stata individuata una informazione importante, ovvero, il **probabile avvio del software Microsoft Paint** (avvenuto alle ore 18 : 38 : 49), dopo la visita dei link, individuati precedentemente

Le Super Timeline

Esempio di Utilizzo 3 | File System & Cronologia Chrome | 14/24

3. Analisi (parziale) Versione Preprocessata del File Prodotto

18:39:15 Modif. del Cont. C:/Users/Raffaele/AppData/Roaming/Microsoft/Windows/Recent

18:39:15 Modif. del Cont. C:/Users/Raffaele/AppData/Local/Microsoft/Windows/History

18:39:15 Modif. del Cont. C:/Users/Raffaele/AppData/Roaming/Microsoft/Windows/Recent

18:39:15 Modif. del Cont. C:/Users/Raffaele/AppData/Local/Microsoft/Windows/History

Proseguiamo l'analisi della super timeline, analizzando le successive due entry

Le Super Timeline

Esempio di Utilizzo 3 | File System & Cronologia Chrome | 15/24

3. Analisi (parziale) Versione Preprocessata del File Prodotto

18:39:15	Modif. del Cont.	C:/Users/Raffaele/AppData/Roaming/Microsoft/Windows/Recent
18:39:15	Modif. del Cont.	C:/Users/Raffaele/AppData/Local/Microsoft/Windows/History

Anche queste due entry sono **potenzialmente rilevanti**, in quanto si riferiscono a due cartelle speciali di Windows, all'interno delle quali sono memorizzate informazioni sui **documenti recenti** (ovvero, i documenti che sono stati utilizzati di recente dall'utente)

Le Super Timeline

Esempio di Utilizzo 3 | File System & Cronologia Chrome | 15/24

3. Analisi (parziale) Versione Preprocessata del File Prodotto

18:39:15	Modif. del Cont.	C:/Users/Raffaele/AppData/Roaming/Microsoft/Windows/Recent
18:39:15	Modif. del Cont.	C:/Users/Raffaele/AppData/Local/Microsoft/Windows/History

Anche queste due entry sono potenzialmente rilevanti, in quanto si riferiscono a due cartelle speciali di Windows, all'interno delle quali sono memorizzate informazioni sui documenti recenti (ovvero, i documenti che sono stati utilizzati di recente dall'utente)

OSSERVAZIONE IMPORTANTE

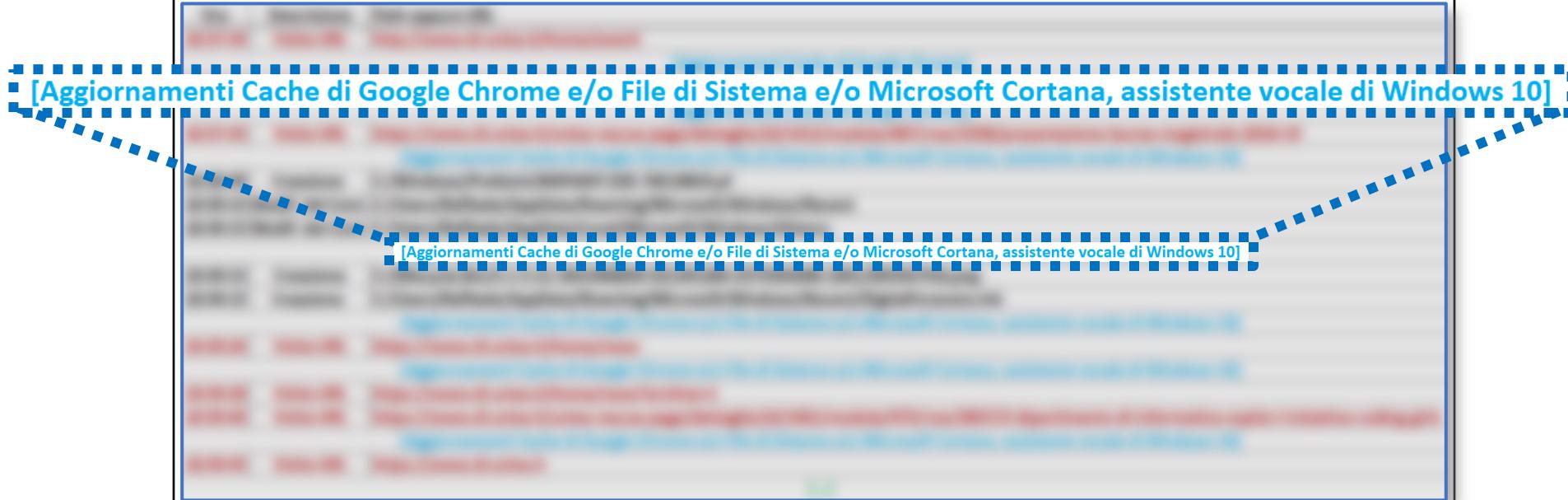
Il fatto che vi siano state delle modifiche nel contenuto di queste directory, fa supporre che vi sia stata l'apertura o il salvataggio di un documento (o un qualche file)

Considerando che è stato aperto il software Paint, si potrebbe supporre che vi sia stata l'apertura o il salvataggio di una immagine

Le Super Timeline

Esempio di Utilizzo 3 | File System & Cronologia Chrome | 16/24

3. Analisi (parziale) Versione Preprocessata del File Prodotto

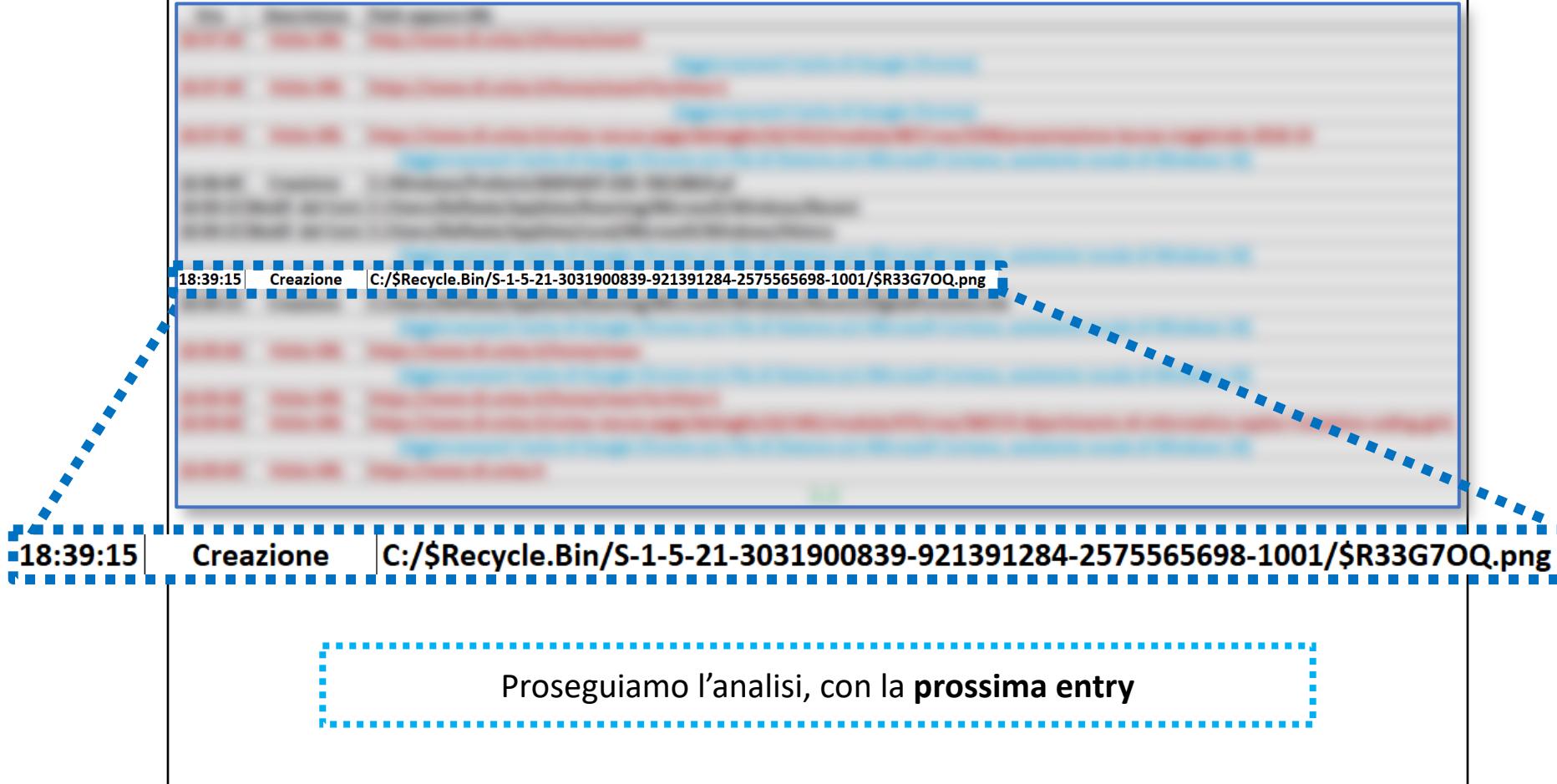


Seguono diversi aggiornamenti di Cache di Chrome ed aggiornamenti di Cortana e/o aggiornamenti di file di sistema (anche in questo caso non vi è alcuna correlazione tra gli aggiornamenti della cache di Chrome e gli altri aggiornamenti)

Le Super Timeline

Esempio di Utilizzo 3 | File System & Cronologia Chrome | 17/24

3. Analisi (parziale) Versione Preprocessata del File Prodotto



Le Super Timeline

Esempio di Utilizzo 3 | File System & Cronologia Chrome | 18/24

3. Analisi (parziale) Versione Preprocessata del File Prodotto

18:39:15

Creazione

C:/Recycle.Bin/S-1-5-21-3031900839-921391284-2575565698-1001/\$R33G7OQ.png

Viene creato il file \$R33G7OQ.png, all'interno della cartella
C:/Recycle.Bin/S-1-5-21-3031900839-921391284-
2575565698-1001\

Le Super Timeline

Esempio di Utilizzo 3 | File System & Cronologia Chrome | 18/24

3. Analisi (parziale) Versione Preprocessata del File Prodotto

18:39:15

Creazione

C:/Recycle.Bin/S-1-5-21-3031900839-921391284-2575565698-1001/\$R33G7OQ.png

Viene creato il file \$R33G7OQ.png, all'interno della cartella
C : \\$Recycle.Bin\S-1-5-21-3031900839-921391284-
2575565698-1001\

OSSERVAZIONI IMPORTANTI

La cartella C : /\$Recycle.Bin è la cartella che Windows utilizza per il Cestino

Il fatto che sia stato creato un nuovo file all'interno della cartella del Cestino, fa supporre che l'utente abbia spostato nel Cestino un file (per «eliminarlo»), pertanto, potrebbe essere utile approfondire di cosa si tratti e soprattutto delineare delle possibili ipotesi/motivazioni



Le Super Timeline

Esempio di Utilizzo 3 | File System & Cronologia Chrome | 18/24

3. Analisi (parziale) Versione Preprocessata del File Prodotto

18:39:15

Creazione

C:/\\$Recycle.Bin/S-1-5-21-3031900839-921391284-2575565698-1001/\$R33G7OQ.png

Viene creato il file **\$R33G7OQ.png**, all'interno della cartella
C : \\$Recycle.Bin\S-1-5-21-3031900839-921391284-
2575565698-1001\

OSSERVAZIONI IMPORTANTI

La cartella C : /\$Recycle.Bin è la cartella che Windows utilizza per il Cestino



Il fatto che sia stato creato un nuovo file all'interno della cartella del Cestino, fa supporre che l'utente abbia spostato nel Cestino un file (per «eliminarlo»), pertanto, potrebbe essere utile approfondire di cosa si tratti e soprattutto delineare delle possibili ipotesi/motivazioni

Quando un file viene «eliminato» (spostato nel Cestino), il S.O., lo rinomina, senza alterarne l'estensione, e lo sposta nella cartella \$Recycle.Bin, quindi, anche dal «nuovo nome del file», è possibile individuare l'estensione del file «eliminato» [nell'esempio, l'estensione è: **.png**, si tratta verosimilmente di una immagine, in formato PNG]

Le Super Timeline

Esempio di Utilizzo 3 | File System & Cronologia Chrome | 18/24

3. Analisi (parziale) Versione Preprocessata del File Prodotto

18:39:15

Creazione

C:/Recycle.Bin/S-1-5-21-3031900839-921391284-2575565698-1001/\$R33G7OQ.png

Viene creato il \$R33G7OQ.png, all'interno della cartella
C:/Recycle.Bin/S-1-5-21-3031900839-921391284-
2575565698-1001\

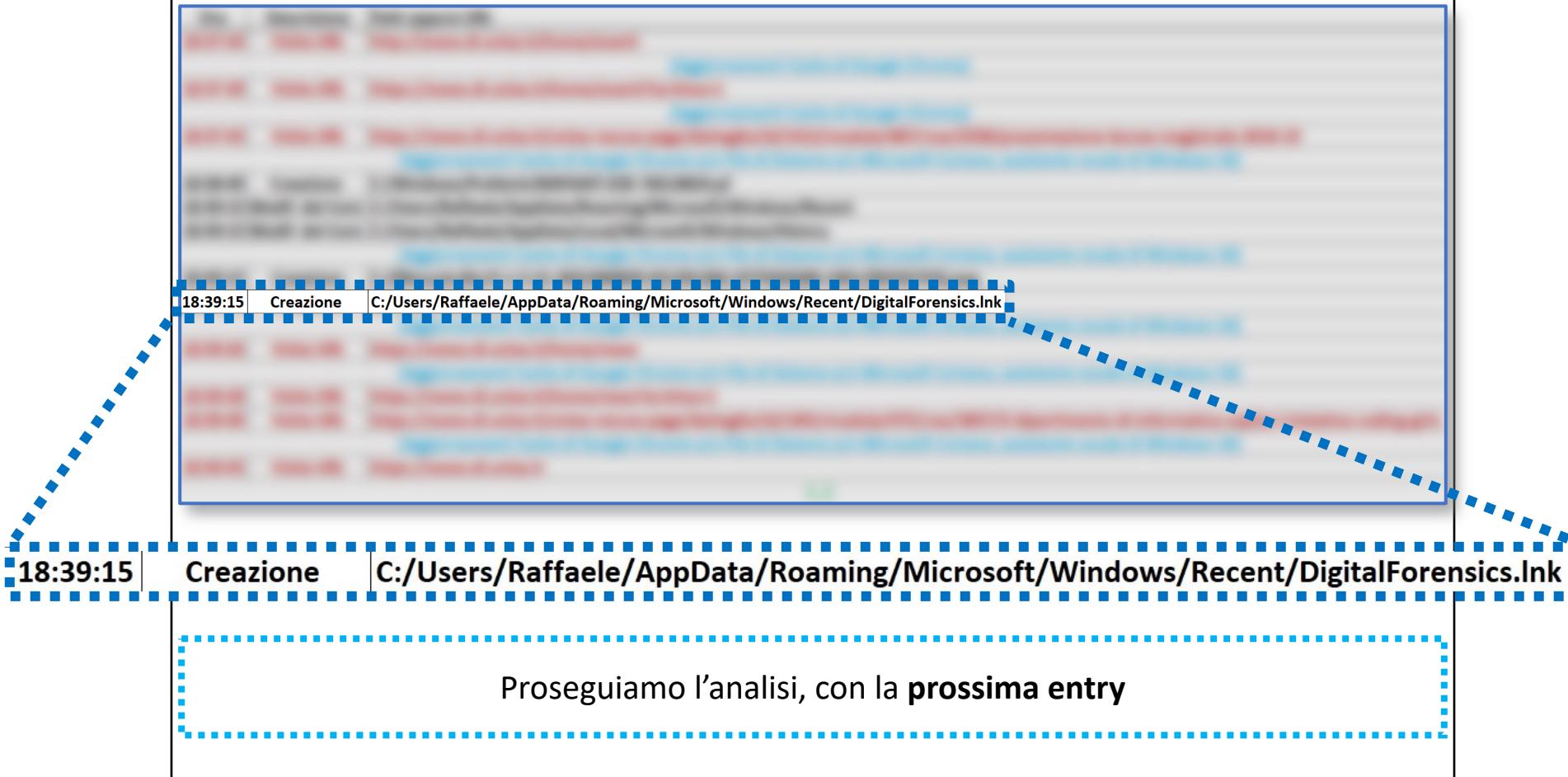
Secure IDentifier (SID) dell'utente

Il SID è un identificativo univoco associato a
ciascun utente all'interno del sistema

Le Super Timeline

Esempio di Utilizzo 3 | File System & Cronologia Chrome | 19/24

3. Analisi (parziale) Versione Preprocessata del File Prodotto



Le Super Timeline

Esempio di Utilizzo 3 | File System & Cronologia Chrome | 19/24

3. Analisi (parziale) Versione Preprocessata del File Prodotto

■ 18:39:15 Creazione C:/Users/Raffaele/AppData/Roaming/Microsoft/Windows/Recent/DigitalForensics.lnk

Viene creato il file **DigitalForensics.lnk**, all'interno della cartella
C:\Users\Raffaele\AppData\Roaming\Microsoft\Windows\Recent\

Con l'estensione **.lnk**, in Windows, si fa riferimento ad un collegamento rapido (scorciatoia o link), tramite il quale si accede al programma e/o al file a cui il collegamento stesso punta

Generalmente, i collegamenti sono creati automaticamente dal sistema e vengono riportati in apposite liste di file/documenti recenti (aperti/modificati di recente), per essere rapidamente richiamati dall'utente

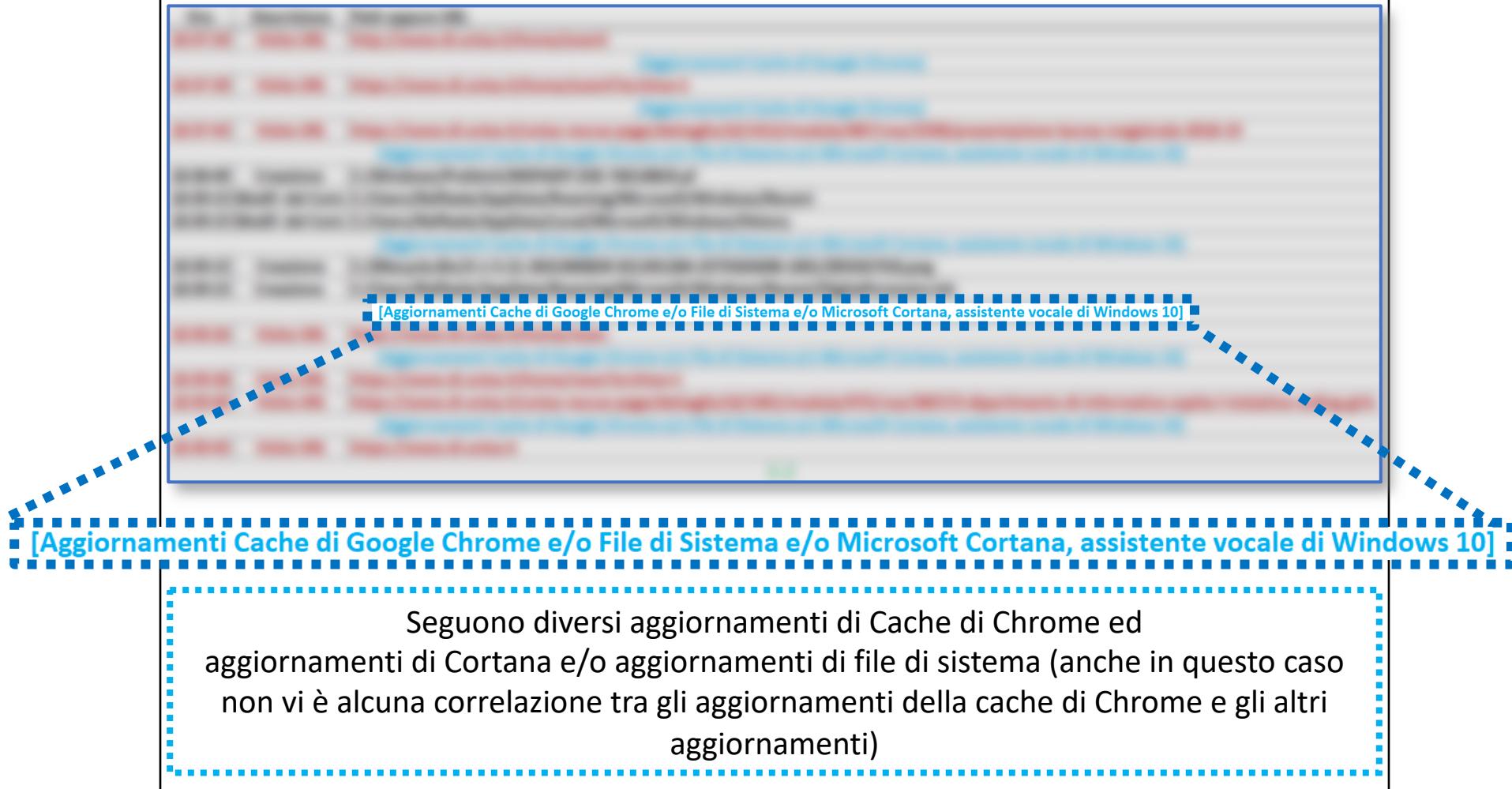
C:\Users\Raffaele\AppData\Roaming\Microsoft\Windows\Recent\ è una delle due cartelle speciali di Windows, osservate precedentemente, che memorizza proprio i collegamenti rapidi che vengono mostrati in specifiche liste di file/documenti recenti (presenti in alcuni punti della GUI di Windows)

Quando il collegamento viene creato in automatico (come avvenuto probabilmente in questo caso), il nome del collegamento (in questo caso **DigitalForensics.lnk**) fa riferimento ad un file denominato **DigitalForensics** (non è possibile individuare l'estensione originale)

Le Super Timeline

Esempio di Utilizzo 3 | File System & Cronologia Chrome | 20/24

3. Analisi (parziale) Versione Preprocessata del File Prodotto



Le Super Timeline

Esempio di Utilizzo 3 | File System & Cronologia Chrome | 21/24

3. Analisi (parziale) Versione Preprocessata del File Prodotto

18:39:26	Visita URL	https://www.di.unisa.it/home/news
[Aggiornamenti Cache di Google Chrome e/o File di Sistema e/o Microsoft Cortana, assistente vocale di Windows 10]		
18:39:28	Visita URL	https://www.di.unisa.it/home/news?archive=1
18:39:40	Visita URL	https://www.di.unisa.it/unisa-rescue-page/dettaglio/id/1401/module/475/row/3837/il-dipartimento-di-informatica-ospita-l-iniziativa-coding-girls
[Aggiornamenti Cache di Google Chrome e/o File di Sistema e/o Microsoft Cortana, assistente vocale di Windows 10]		
18:39:45	Visita URL	https://www.di.unisa.it

[...]

18:39:26	Visita URL	https://www.di.unisa.it/home/news
[Aggiornamenti Cache di Google Chrome e/o File di Sistema e/o Microsoft Cortana, assistente vocale di Windows 10]		
18:39:28	Visita URL	https://www.di.unisa.it/home/news?archive=1
18:39:40	Visita URL	https://www.di.unisa.it/unisa-rescue-page/dettaglio/id/1401/module/475/row/3837/il-dipartimento-di-informatica-ospita-l-iniziativa-coding-girls
[Aggiornamenti Cache di Google Chrome e/o File di Sistema e/o Microsoft Cortana, assistente vocale di Windows 10]		
18:39:45	Visita URL	https://www.di.unisa.it

[...]

La navigazione prosegue con la visita ad altri quattro link ed il conseguente aggiornamento della cache e/o di altri file di sistema e/o di Microsoft Cortana

Le Super Timeline

Esempio di Utilizzo 3 | File System & Cronologia Chrome | 21/24

3. Analisi (parziale) Versione Preprocessata del File Prodotto



OSSERVAZIONE IMPORTANTE | 1/3

Dopo la visita all'URL: <https://www.di.unisa.it>, avvenuta alle ore 18:39:45 (09/02/2019), dalla super timeline (versione completa), è osservabile che non siano stati visitati ulteriori URL, mediante Google Chrome

Infatti, dal file History, relativo alla cronologia di Google Chrome ([Fonte 2.](#)), non risultano tracce di ulteriori URL visitati

Le Super Timeline

Esempio di Utilizzo 3 | File System & Cronologia Chrome | 21/24

3. Analisi (parziale) Versione Preprocessata del File Prodotto



OSSERVAZIONE IMPORTANTE | 2/3

Inoltre, dalla super timeline (versione completa) è osservabile che l'ultima modifica, al file History, risulti essere avvenuta alle 18:39:49 (09/02/2019)
[NOTA: informazione reperita dalla [Fonte 1](#).]



Le suddette tracce, provenienti dalla [Fonte 1](#). e dalla [Fonte 2](#)., sono dunque coerenti: dopo alcuni secondi dalla visita dell'URL, di cui sopra, è stato verosimilmente aggiornato il file della cronologia (e, conseguentemente, la data e l'ora relative alla modifica del file)

Le Super Timeline

Esempio di Utilizzo 3 | File System & Cronologia Chrome | 21/24

3. Analisi (parziale) Versione Preprocessata del File Prodotto

18:39:45	Visita URL	https://www.di.unisa.it
18:39:45	Visita URL	https://www.di.unisa.it
OSSERVAZIONE IMPORTANTE 3/3		
18:36:51,000	Last Access Time	OS:E:\Users\Raffaele\AppData\Local\Google\Chrome\User Data\Default\History Type: file
18:36:51,000	Metadata Modification Time	OS:E:\Users\Raffaele\AppData\Local\Google\Chrome\User Data\Default\History Type: file

Anche l'ora dell'ultimo accesso (*Last Access Time*) e l'ora dell'ultima modifica dei metadati del file (*Metadata Modification Time*), le quali risultano essere uguali a 18 : 36 : 51 (in entrambi i casi la data è 09/02/2019), risultano essere coerenti con l'attività di navigazione Web, individuata dalla cronologia di Google Chrome ([Fonte 2.](#))

È possibile supporre che il file sia stato acceduto, da Google Chrome, per fornire suggerimenti all'utente, su un sito già visitato o altre attività, comunque correlate alla navigazione Web

Le Super Timeline

Esempio di Utilizzo 3 | File System & Cronologia Chrome | 22/24

POSSIBILE SCENARIO | 1/2

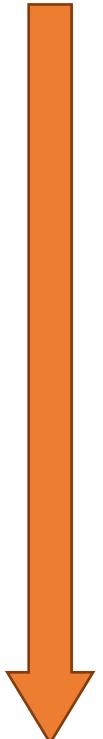
- Dalle osservazioni e le informazioni precedenti, potrebbe essere possibile delineare uno scenario verosimile degli eventi, sufficientemente accurato, in riferimento alla (piccola) porzione della super timeline analizzata

Le Super Timeline

Esempio di Utilizzo 3 | File System & Cronologia Chrome | 22/24

POSSIBILE SCENARIO | 1/2

- Dalle osservazioni e le informazioni precedenti, potrebbe essere possibile delineare uno scenario verosimile degli eventi, sufficientemente accurato, in riferimento alla (piccola) porzione della super timeline analizzata
 1. Navigazione Web sulla pagina Eventi del Dipartimento di Informatica (DI) dell'Università di Salerno
 2. Visita alla pagina dedicata di un evento archiviato (già svoltosi)
 3. Avvio del programma Microsoft Paint
 4. Visualizzazione/Creazione di una immagine (probabilmente tramite Paint)
 5. Cancellazione di una immagine PNG (probabilmente l'immagine di cui sopra)
 6. Creazione (verosimilmente automatica) di un collegamento rapido (.lnk) ad un file il cui nome è **DigitalForensics** (non è nota l'estensione del file al quale il collegamento fa riferimento)
 7. La navigazione Web prosegue con la visita ad altri URL, relativi ad altre pagine del suddetto Dipartimento

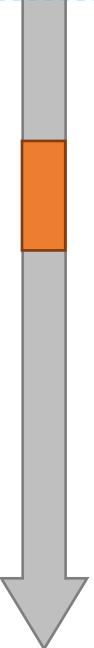


Motivazione di questa Possibile Ipotesi

Sono state rinvenute delle tracce di modifica del contenuto di due cartelle speciali di Windows, all'interno delle quali sono memorizzate informazioni sui documenti/file recenti

18:39:15	Modif. del Cont.	C:/Users/Raffaele/AppData/Roaming/Microsoft/Windows/Recent
18:39:15	Modif. del Cont.	C:/Users/Raffaele/AppData/Local/Microsoft/Windows/History

Dal momento che Microsoft Paint è stato avviato al passo 3., è verosimile supporre che sia stata creata/visualizzata una immagine e le suddette tracce siano riferite ad essa

- 
- 2. Visita alla pagina dedicata di un evento
 - 3. Avvio del programma Microsoft Paint
 - 4. Visualizzazione/Creazione di una immagine (probabilmente tramite Paint)**
 - 5. Cancellazione di una immagine PNG (probabilmente l'immagine di cui sopra)
 - 6. Creazione (verosimilmente automatica) di un collegamento rapido (.lnk) ad un file il cui nome è **DigitalForensics** (non è nota l'estensione del file al quale il collegamento fa riferimento)
 - 7. La navigazione Web prosegue con la visita ad altri URL, relativi ad altre pagine del suddetto Dipartimento

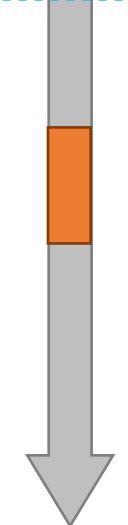
Motivazione di questa Possibile Ipotesi

Supponiamo che non si tratti della cancellazione dell'immagine, creata/visualizzata al passo **4.**, ma si tratti della cancellazione di un'altra immagine

Se così fosse, dovrebbe essere possibile individuare delle tracce, in riferimento all'immagine creata/visualizzata al passo **4.** (ad esempio, la data e l'ora dell'ultimo accesso, ecc.)

Invece, dall'analisi della super timeline completa (file non pre-processato), non è stata rinvenuta alcuna traccia, riconducibile alla suddetta immagine, quindi, è possibile dedurre che sia proprio questa l'immagine che è stata cancellata, al passo **5.**

Inoltre, siamo in grado di determinare che si possa trattare di una immagine PNG, dal nome del file contenuto nel Cestino (che mantiene l'estensione del file originale): \$R33G70Q.**.png**

- 
4. Visualizzazione/Creazione di una immagine (probabilmente tramite Paint)
 - 5. Cancellazione di una immagine PNG (probabilmente l'immagine di cui sopra)**
 6. Creazione (verosimilmente automatica) di un collegamento rapido (.lnk) ad un file il cui nome è **DigitalForensics** (non è nota l'estensione del file al quale il collegamento fa riferimento)
 7. La navigazione Web prosegue con la visita ad altri URL, relativi ad altre pagine del suddetto Dipartimento

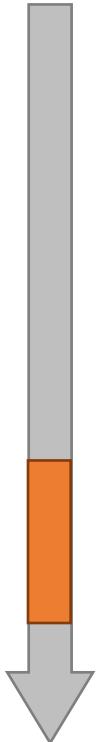
Le Super Timeline

Esempio di Utilizzo 3 | File System & Cronologia Chrome | 22/24

POSSIBILE SCENARIO | 1/2

- Dalle osservazioni e le informazioni precedenti, potrebbe essere possibile delineare uno scenario verosimile degli eventi, sufficientemente accurato, in riferimento alla (piccola) porzione della super timeline analizzata

1. Navigazione Web sulla pagina Eventi del Dipartimento di Informatica dell'Università di Salerno
2. Visita alla pagina dedicata di **DigitalForensics**
3. Avvio del programma
4. Visualizzazione/Creazione di un'immagine (probabilmente tramite Paint)
5. Cancellazione di una immagine PNG (probabilmente l'immagine di cui sopra)
6. Creazione (verosimilmente automatica) di un collegamento rapido (.lnk) ad un file il cui nome è **DigitalForensics** (non è nota l'estensione del file al quale il collegamento fa riferimento)
7. La navigazione Web prosegue con la visita ad altri URL, relativi ad altre pagine del suddetto Dipartimento



Soffermiamoci ora sul passo 6.

(già svoltosi)

Le Super Timeline

Esempio di Utilizzo 3 | File System & Cronologia Chrome | 23/24

POSSIBILE SCENARIO | 2/2

6. Creazione (verosimilmente automatica) di un collegamento rapido (.lnk) ad un file il cui nome è **DigitalForensics** (non è nota l'estensione del file al quale il collegamento fa riferimento)

Possibile Ipotesi | 1/2

- Collegamento all'immagine PNG che è stata appena visualizzata o creata, denominata probabilmente **DigitalForensics.png**
- Inoltre, è verosimile supporre che si possa trattare della creazione dell'immagine e **NON** della sua visualizzazione
 - **MOTIVAZIONE:**
 - Supponiamo che si possa trattare della visualizzazione dell'immagine
 - È verosimile che l'utente l'abbia già aperta/visualizzata recentemente
 - In tal caso, il collegamento rapido dovrebbe già essere esistente (e potrebbe essere stato anche già utilizzato dall'utente)
 - Invece, il collegamento è stato creato (come si evince dalla super timeline), ciò nega la supposizione iniziale

Le Super Timeline

Esempio di Utilizzo 3 | File System & Cronologia Chrome | 24/24

POSSIBILE SCENARIO | 2/2

6. Creazione (verosimilmente automatica) di un collegamento rapido (.lnk) ad un file il cui nome è **DigitalForensics** (non è nota l'estensione del file al quale il collegamento fa riferimento)

Possibile Ipotesi | 2/2

- L'immagine è stata cancellata subito dopo la sua apertura/visualizzazione
- Non risultano tracce però della cancellazione del collegamento rapido, il quale fa riferimento ad un file non più esistente (ovvero, l'immagine cancellata)
 - Conseguentemente, il collegamento non è più valido
- Tuttavia, non è detto che Windows elimini immediatamente il collegamento rapido
 - Il collegamento potrebbe non venire eliminato affatto, oppure, potrebbe venire eliminato solo al verificarsi di alcune azioni dell'utente
 - Ad esempio, l'eliminazione di un collegamento, non valido, potrebbe avvenire (con la conferma dell'utente/segnalazione all'utente), in seguito ad un click sul collegamento stesso, oppure, tramite l'eliminazione esplicita da parte dell'utente
 - Ciò implica che il collegamento potrebbe essere ancora presente nel sistema

Le Super Timeline

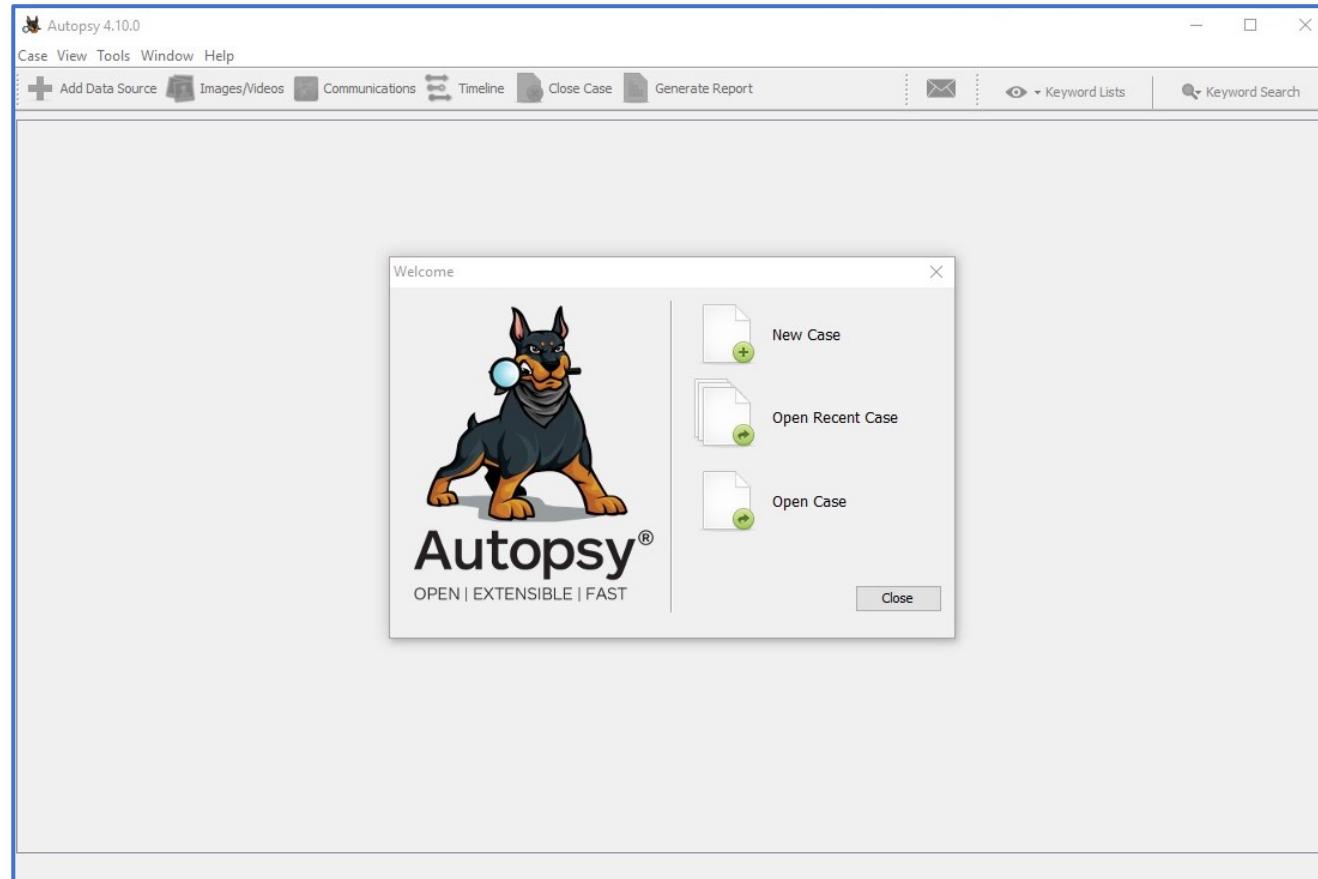
Timeline con Autopsy [Versione Windows] | 1/15

- La **versione per Microsoft Windows**, del tool **Autopsy**, prevede diverse opzioni per la gestione della super timeline, tutte gestibili mediante una **GUI molto curata ed user-friendly**
- Nelle prossime slide, verranno mostrati alcuni **screenshot** di Autopsy per Windows, **in relazione alla GUI ed alla gestione delle timeline e super timeline**
 - La versione utilizzata è la **4.10.0**

Le Super Timeline

Timeline con Autopsy [Versione Windows] | 2/15

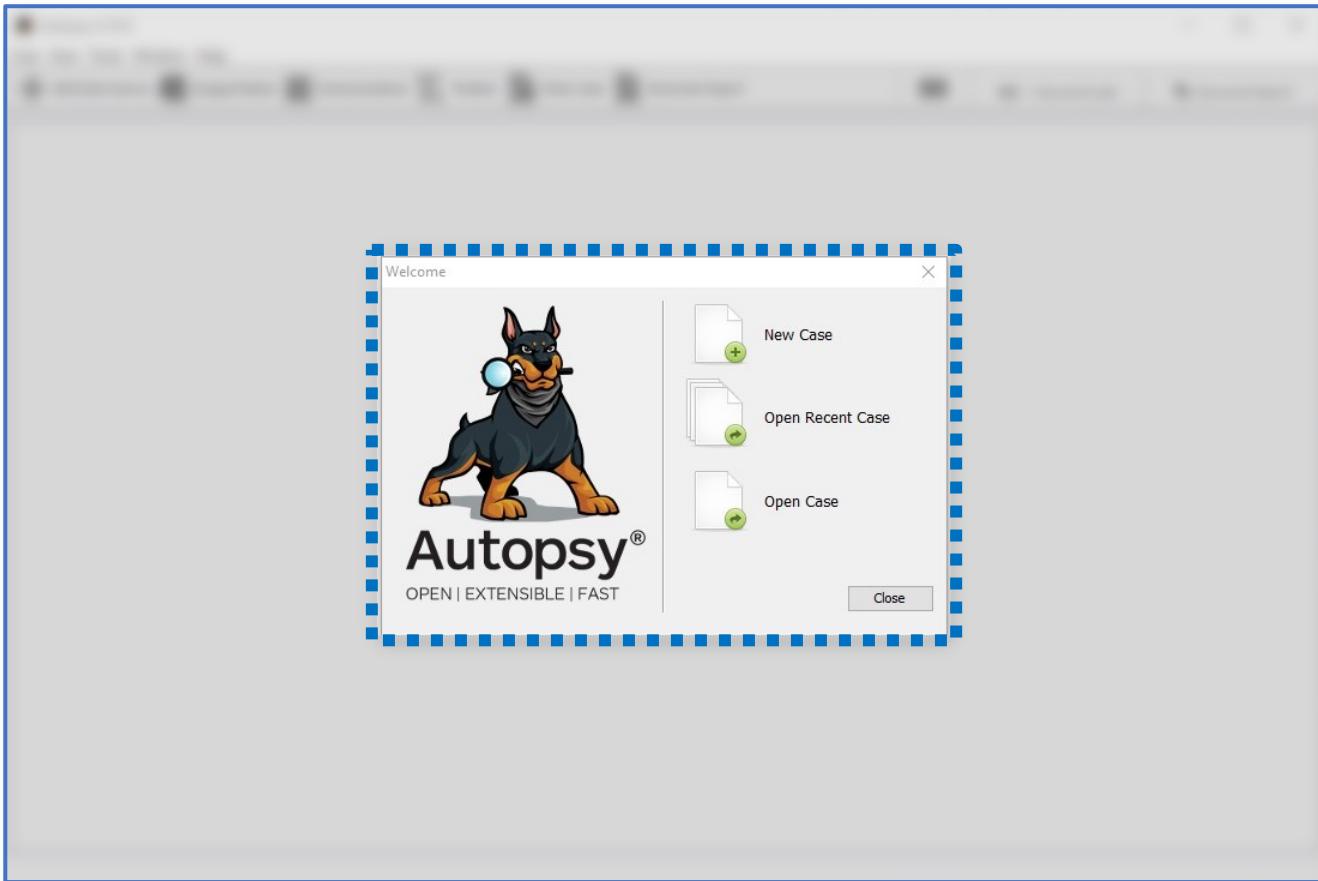
- *Interfaccia Utente di Autopsy (Versione Windows) | 1/2*



Le Super Timeline

Timeline con Autopsy [Versione Windows] | 2/15

- *Interfaccia Utente di Autopsy (Versione Windows) | 2/2*



Le Super Timeline

Timeline con Autopsy [Versione Windows] | 3/15

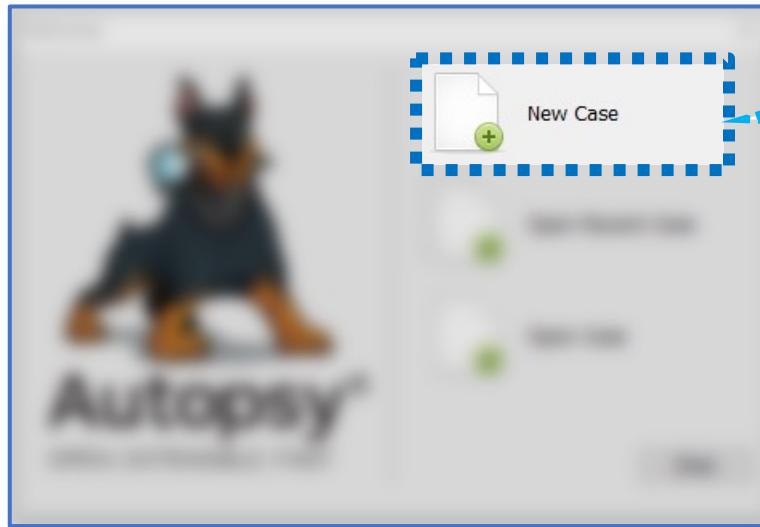
- *Operazioni sui Casi*



Le Super Timeline

Timeline con Autopsy [Versione Windows] | 3/15

- *Operazioni sui Casi*

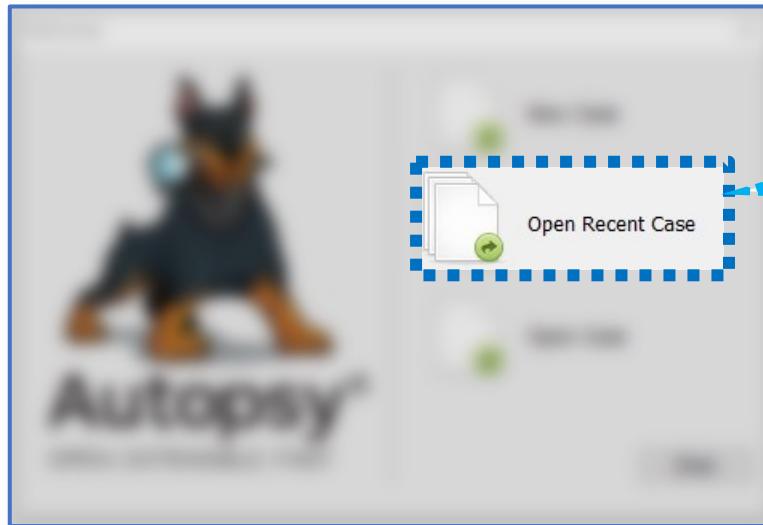


Creazione di un Nuovo Caso

Le Super Timeline

Timeline con Autopsy [Versione Windows] | 3/15

- *Operazioni sui Casi*

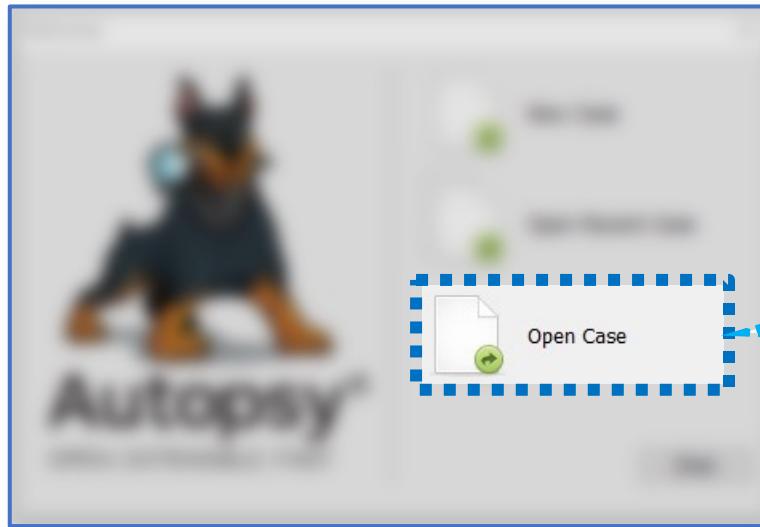


Apertura di un Caso,
recentemente memorizzato

Le Super Timeline

Timeline con Autopsy [Versione Windows] | 3/15

- *Operazioni sui Casi*

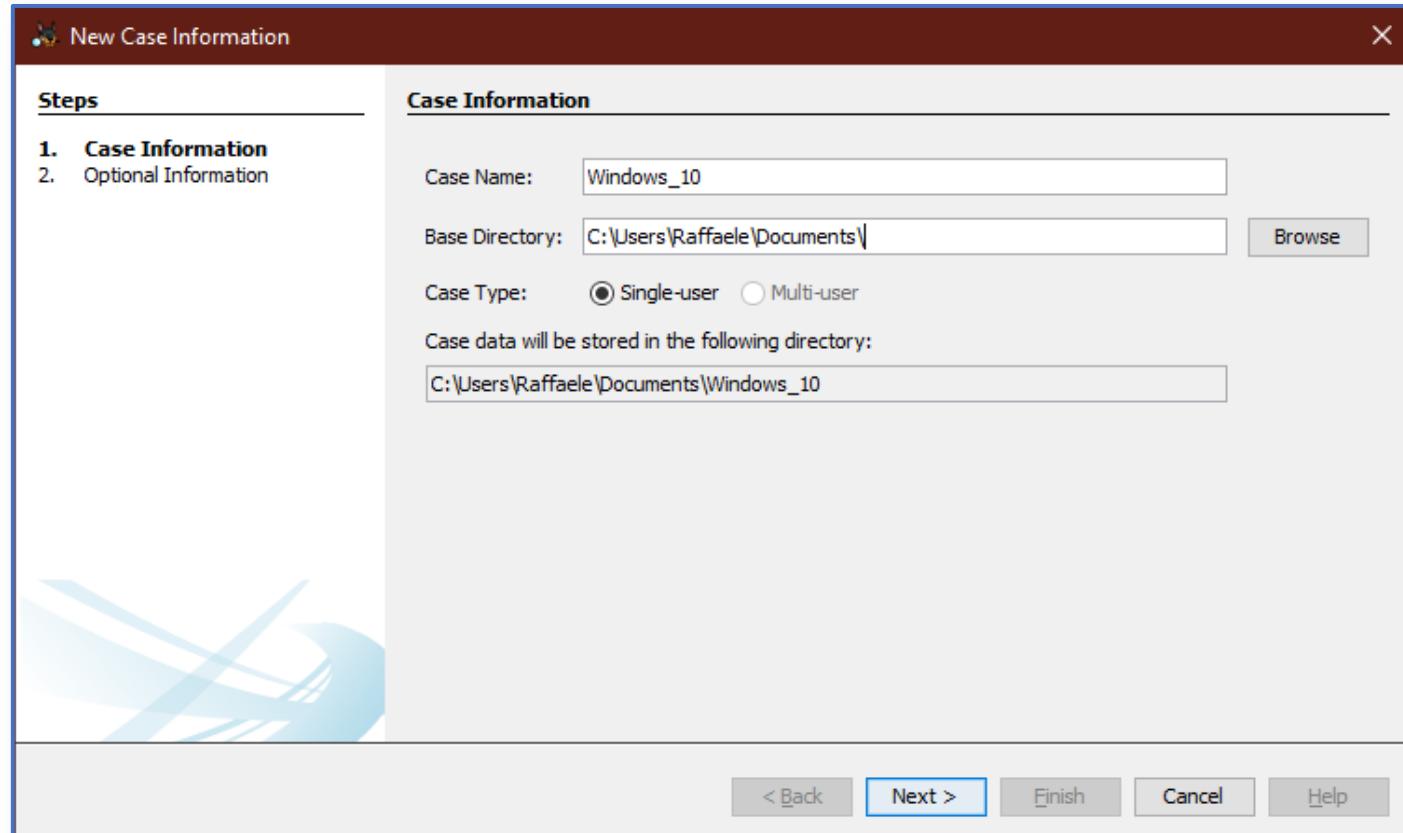


Apertura di un Caso

Le Super Timeline

Timeline con Autopsy [Versione Windows] | 4/15

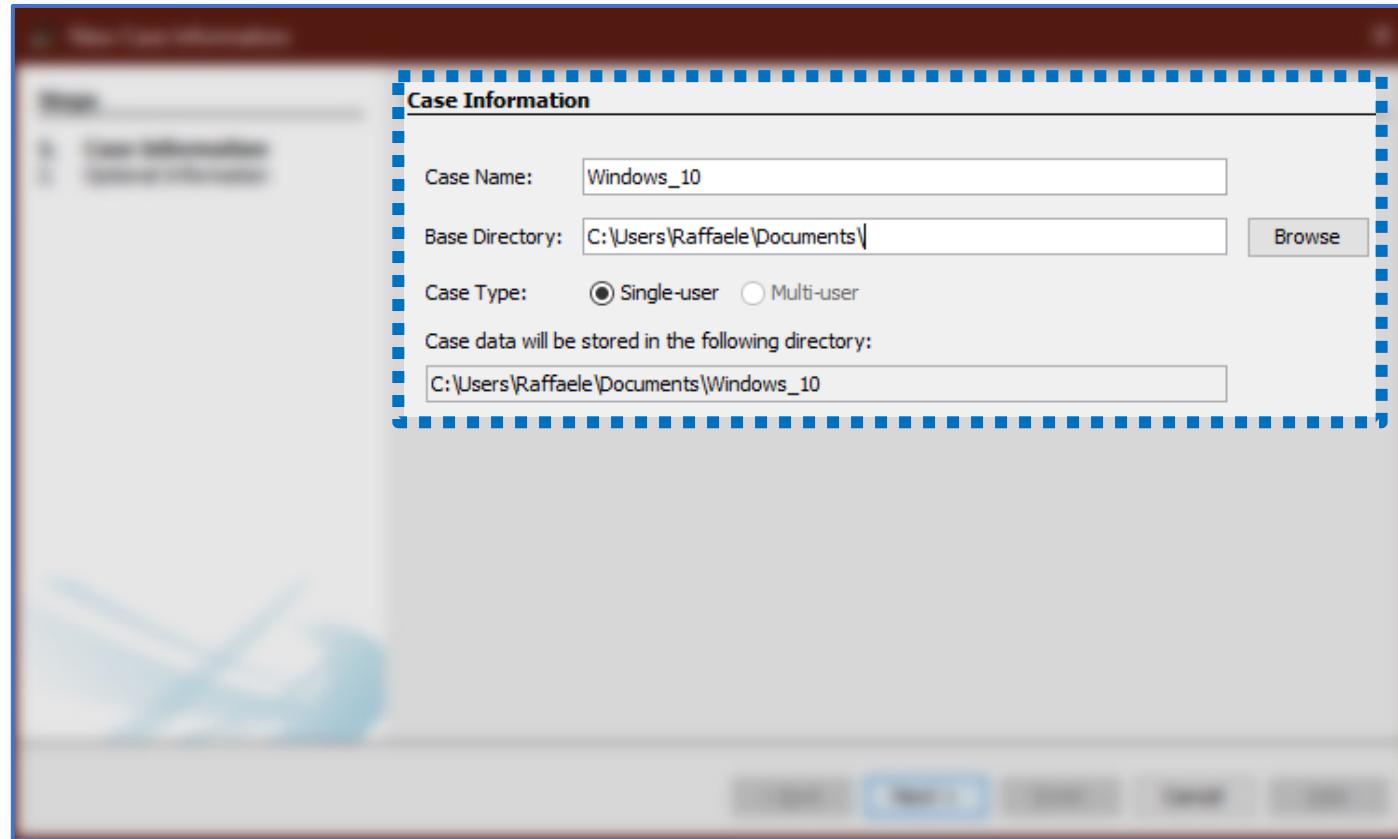
- *Creazione di un Nuovo Caso*



Le Super Timeline

Timeline con Autopsy [Versione Windows] | 4/15

- *Creazione di un Nuovo Caso*
 - *Informazioni di un Caso*



Le Super Timeline

Timeline con Autopsy [Versione Windows] | 5/15

- *Creazione di un Nuovo Caso*

New Case Information

Steps

1. Case Information
2. **Optional Information**

Optional Information

Case

Number: 123456789

Examiner

Name: Raffaele

Phone:

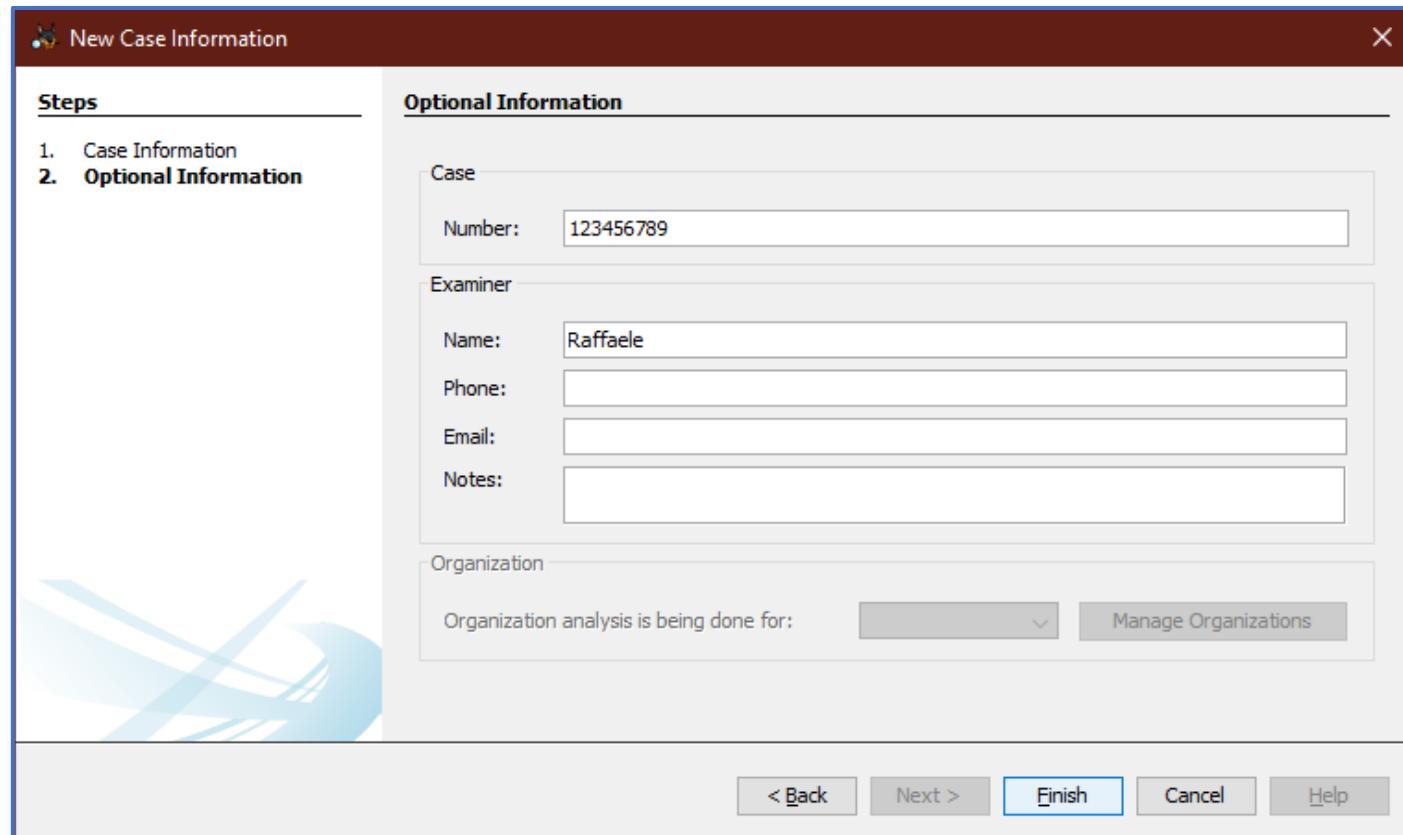
Email:

Notes:

Organization

Organization analysis is being done for: Manage Organizations

< Back Next > **Finish** Cancel Help



Le Super Timeline

Timeline con Autopsy [Versione Windows] | 5/15

- *Creazione di un Nuovo Caso*
 - *Informazioni Opzionali di un Caso*

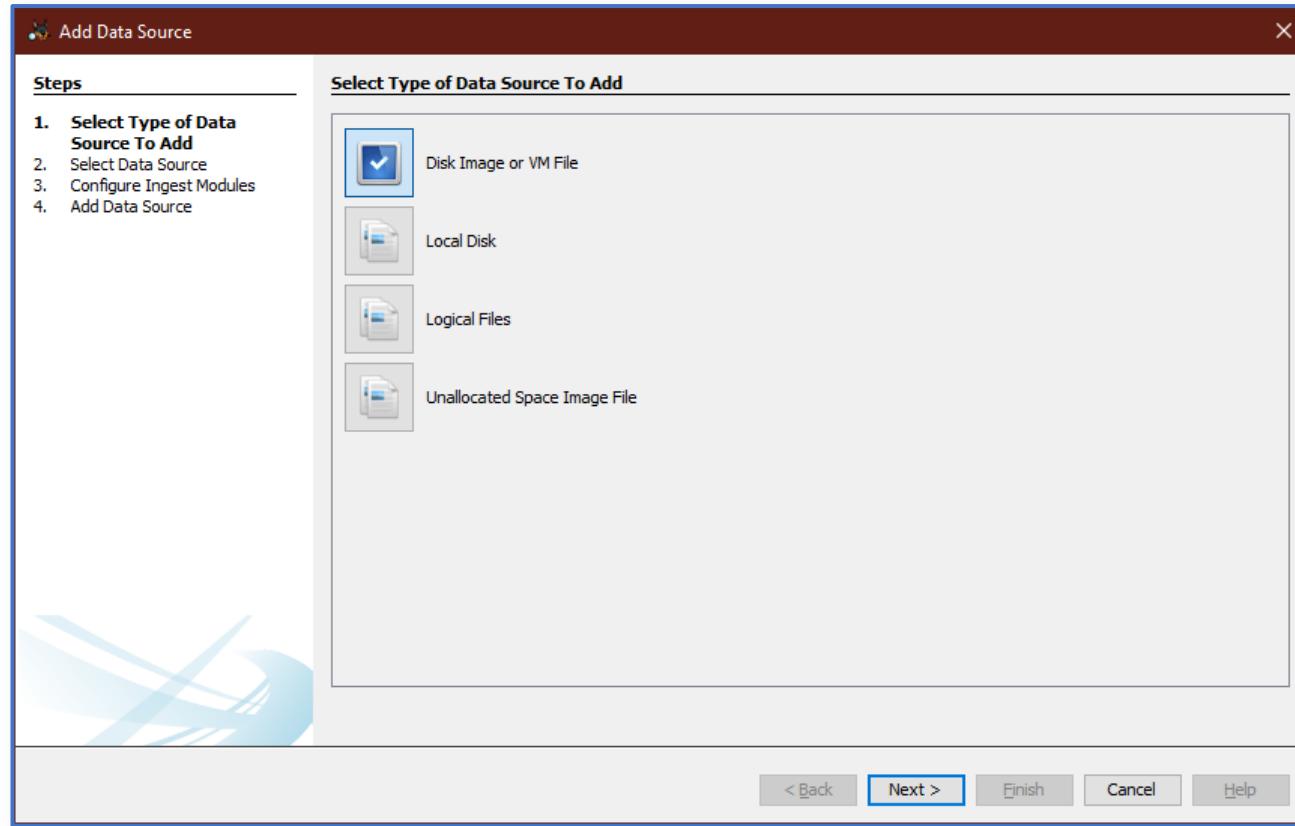
The screenshot shows a software interface for creating a new case. A blue dashed rectangular box highlights the 'Optional Information' section. This section contains fields for Case Number (123456789), Examiner Name (Raffaele), and other optional contact information like Phone and Email, all of which are currently empty.

Optional Information	
Case	
Number:	123456789
Examiner	
Name:	Raffaele
Phone:	
Email:	
Notes:	

Le Super Timeline

Timeline con Autopsy [Versione Windows] | 6/15

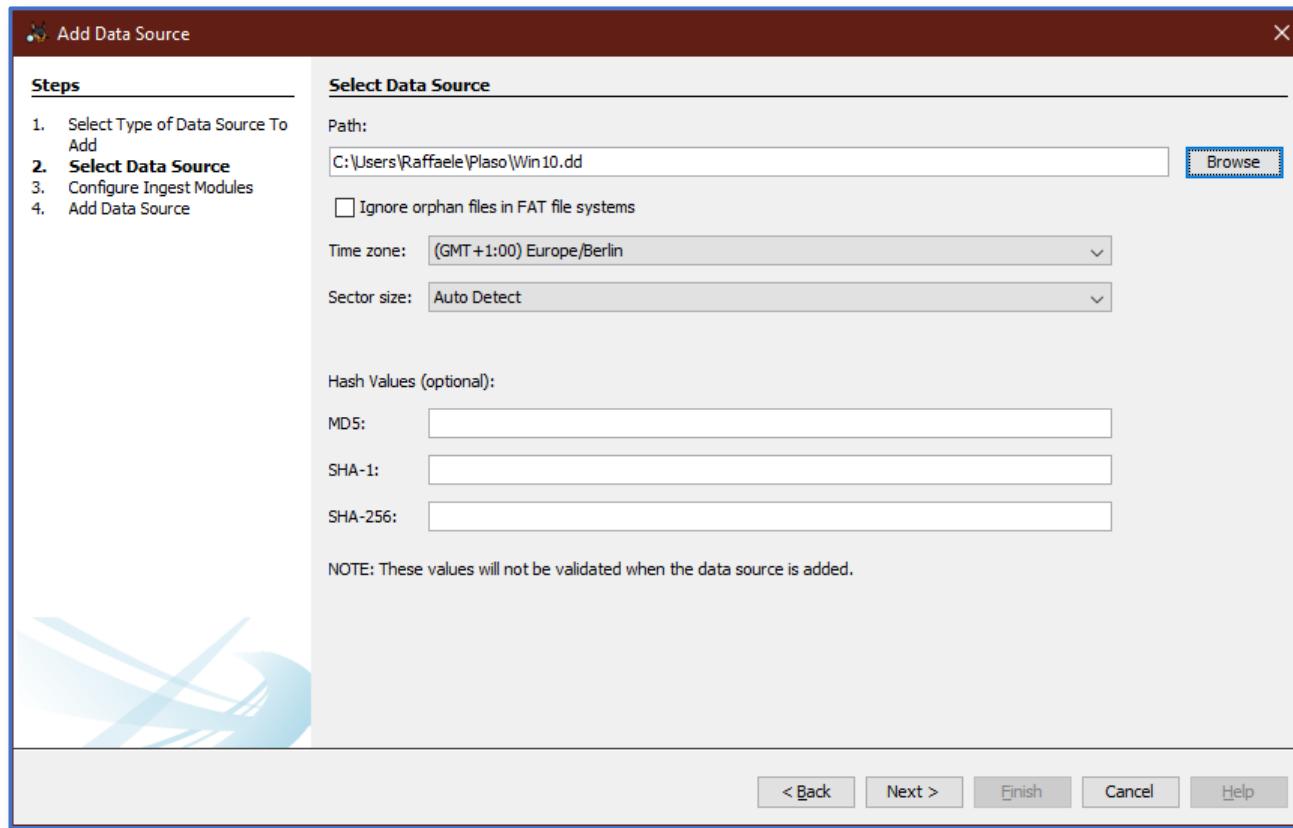
- *Creazione di un Nuovo Caso*
 - *Aggiunta delle Sorgenti (ad esempio, immagini forensi, ecc.)*



Le Super Timeline

Timeline con Autopsy [Versione Windows] | 7/15

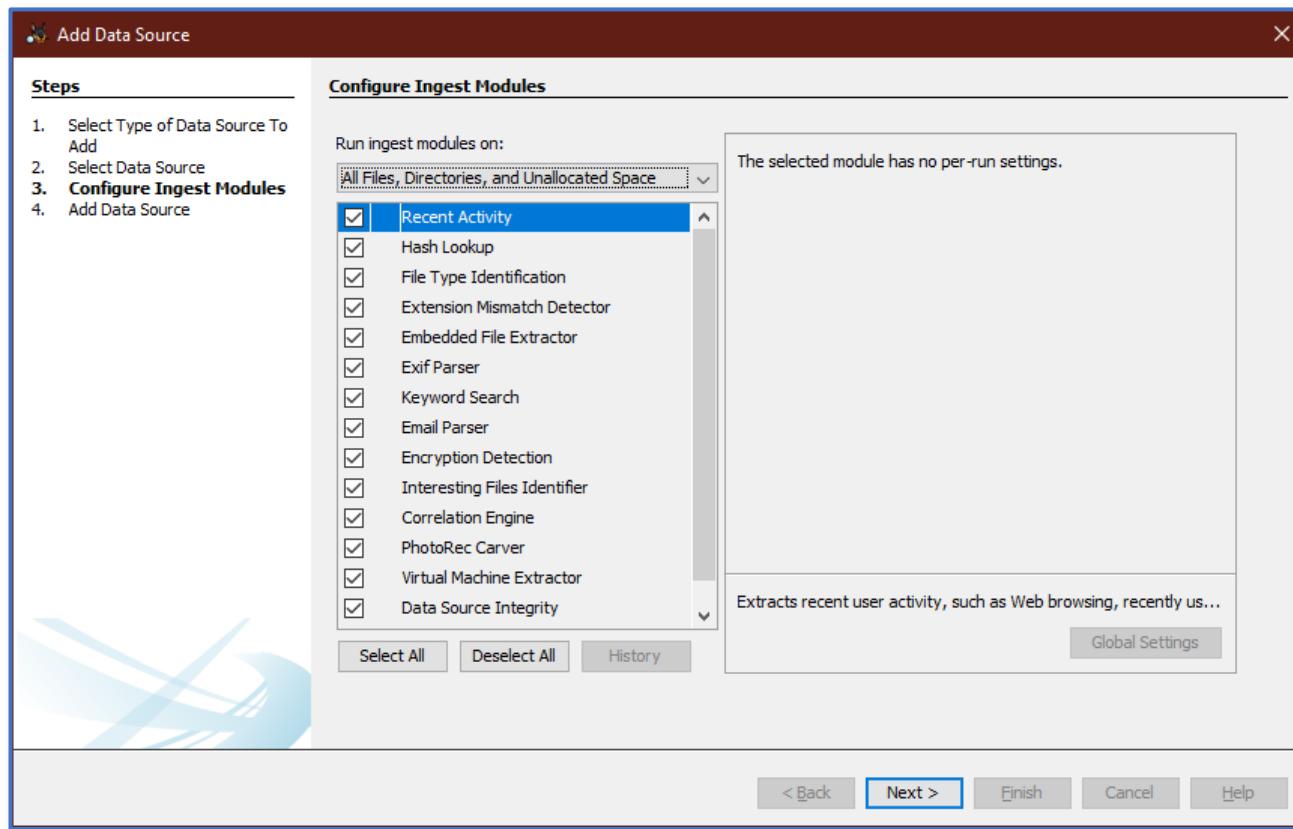
- *Creazione di un Nuovo Caso*
 - *Aggiunta delle Sorgenti (ad esempio, immagini forensi, ecc.)*



Le Super Timeline

Timeline con Autopsy [Versione Windows] | 8/15

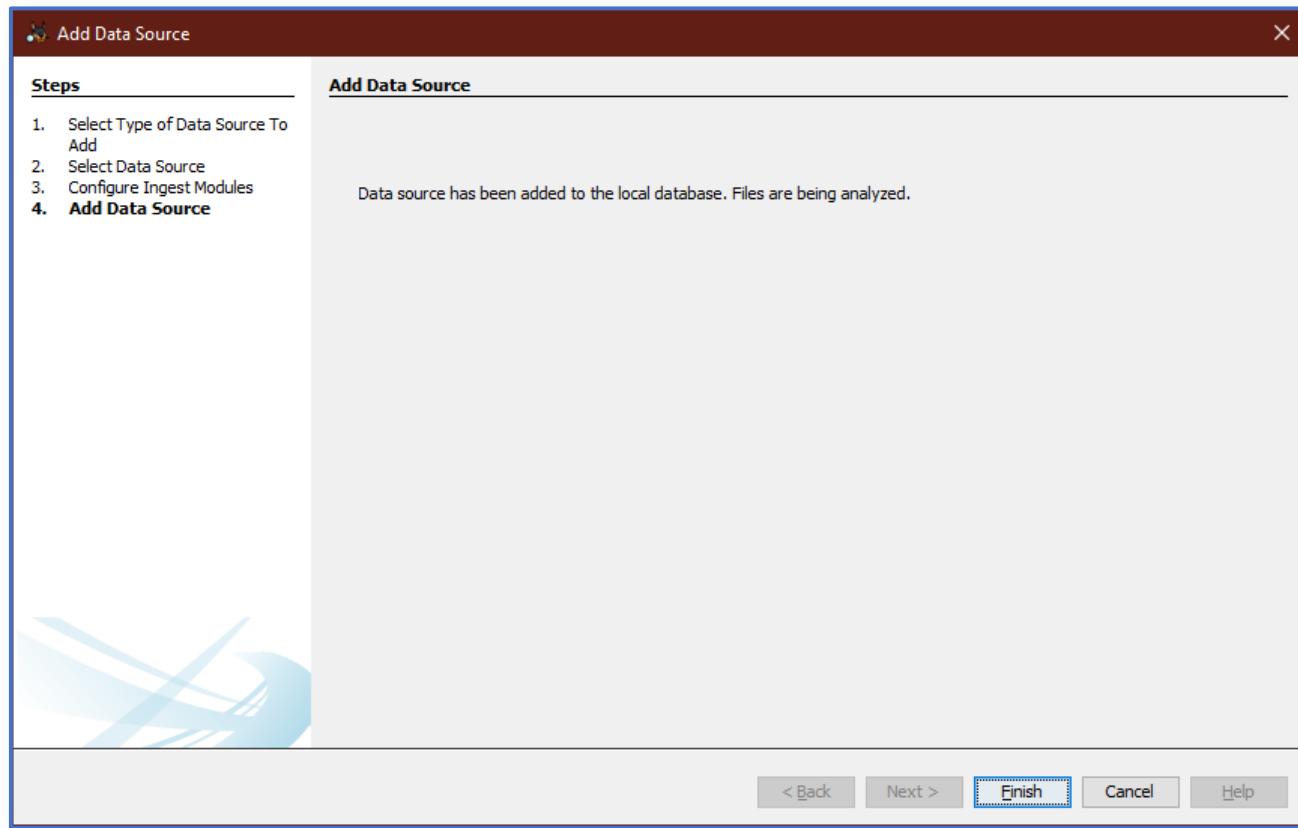
- *Creazione di un Nuovo Caso*
 - *Aggiunta delle Sorgenti (ad esempio, immagini forensi, ecc.)*



Le Super Timeline

Timeline con Autopsy [Versione Windows] | 9/15

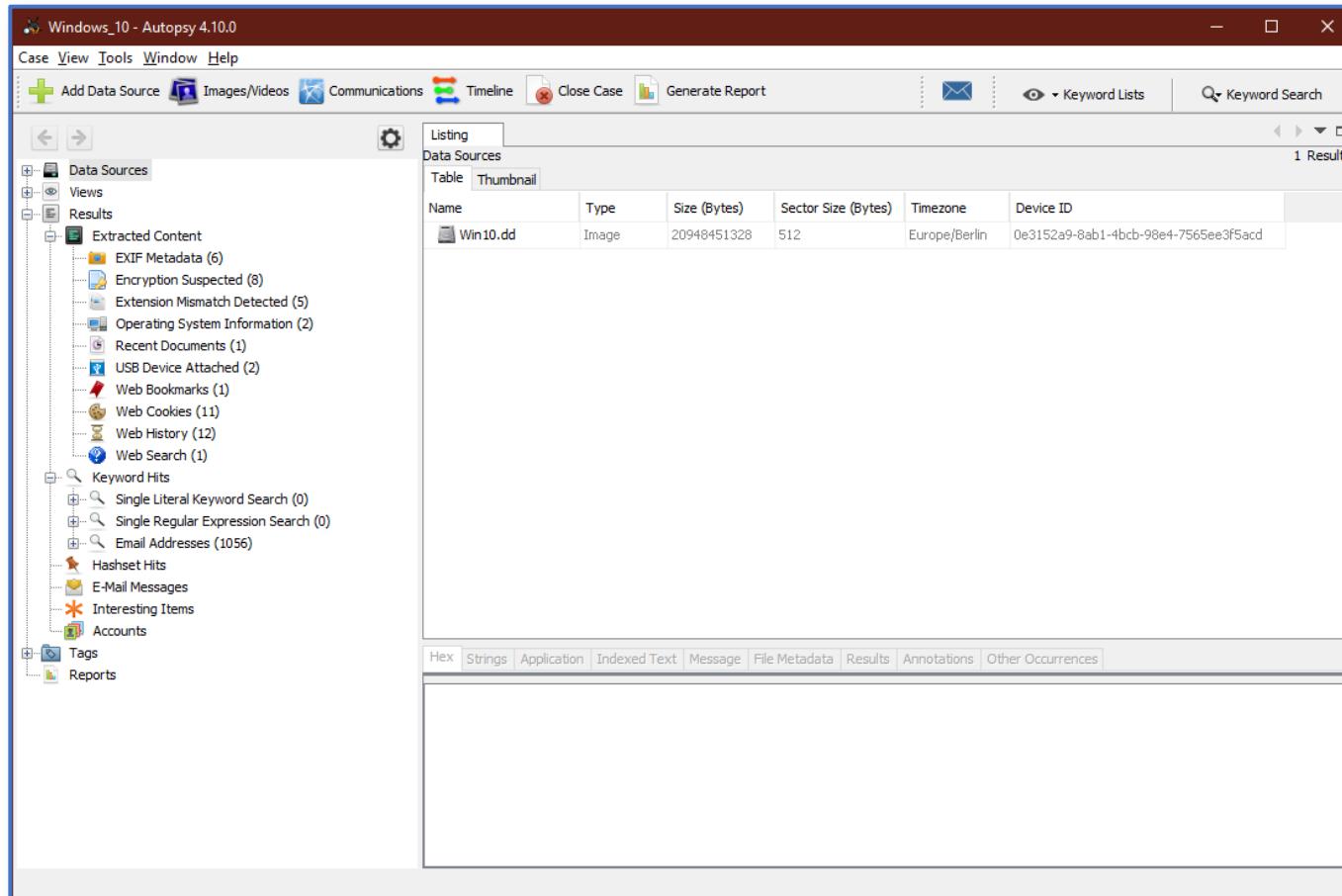
- *Creazione di un Nuovo Caso*
 - *Aggiunta delle Sorgenti (ad esempio, immagini forensi, ecc.)*



Le Super Timeline

Timeline con Autopsy [Versione Windows] | 10/15

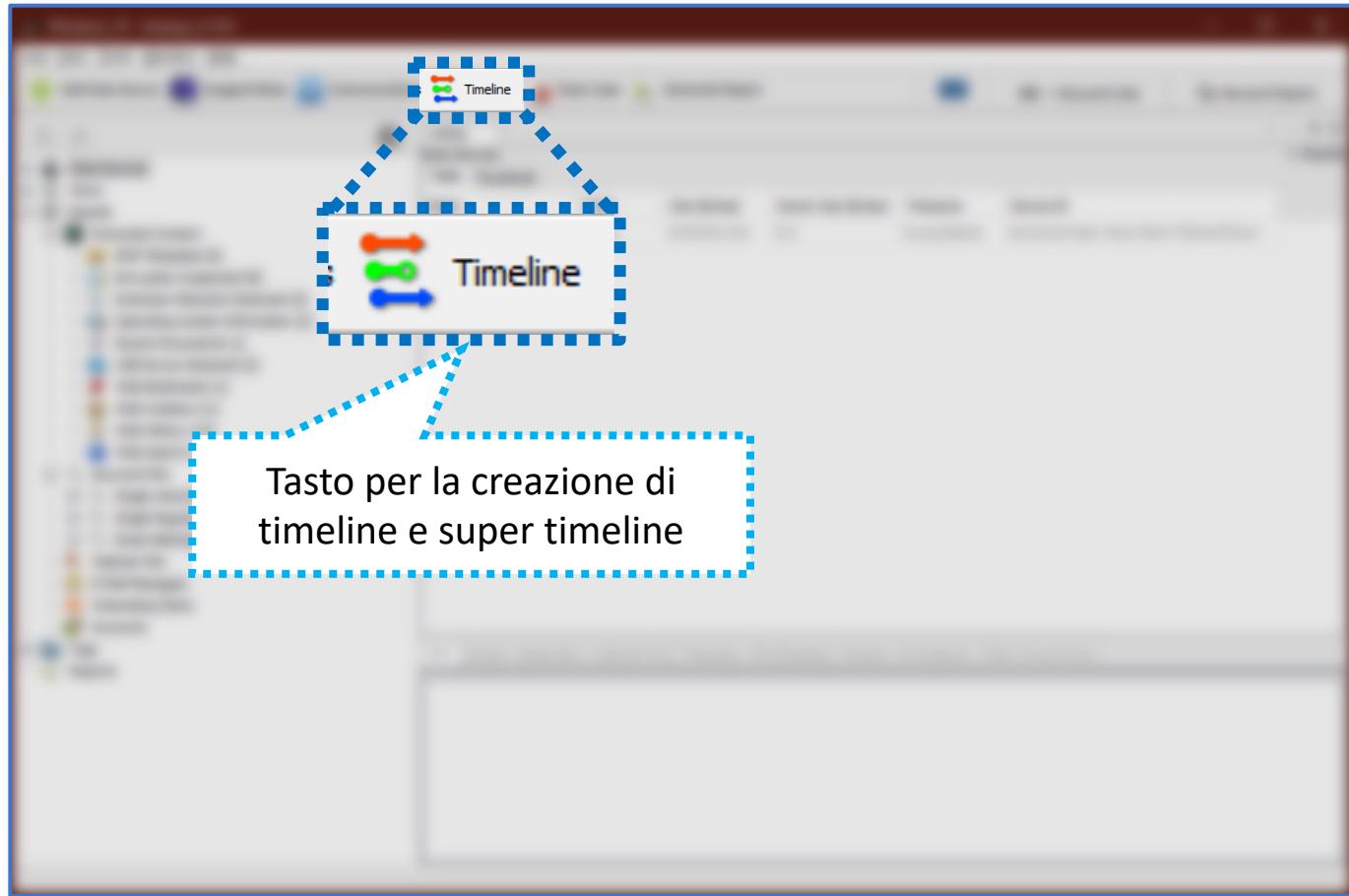
- *Interfaccia Utente per la Gestione di un Caso*



Le Super Timeline

Timeline con Autopsy [Versione Windows] | 10/15

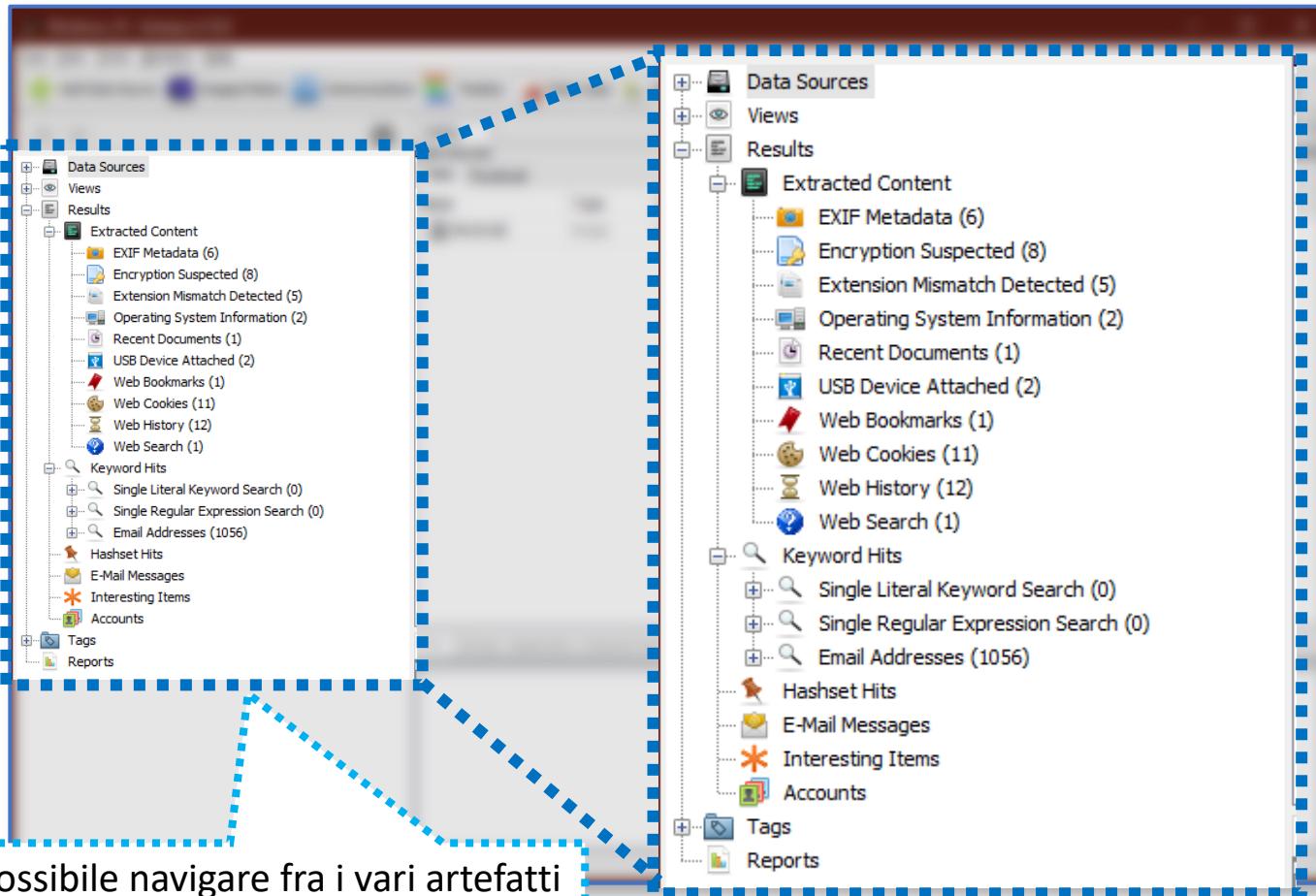
- *Interfaccia Utente per la Gestione di un Caso*



Le Super Timeline

Timeline con Autopsy [Versione Windows] | 10/15

- *Interfaccia Utente per la Gestione di un Caso*

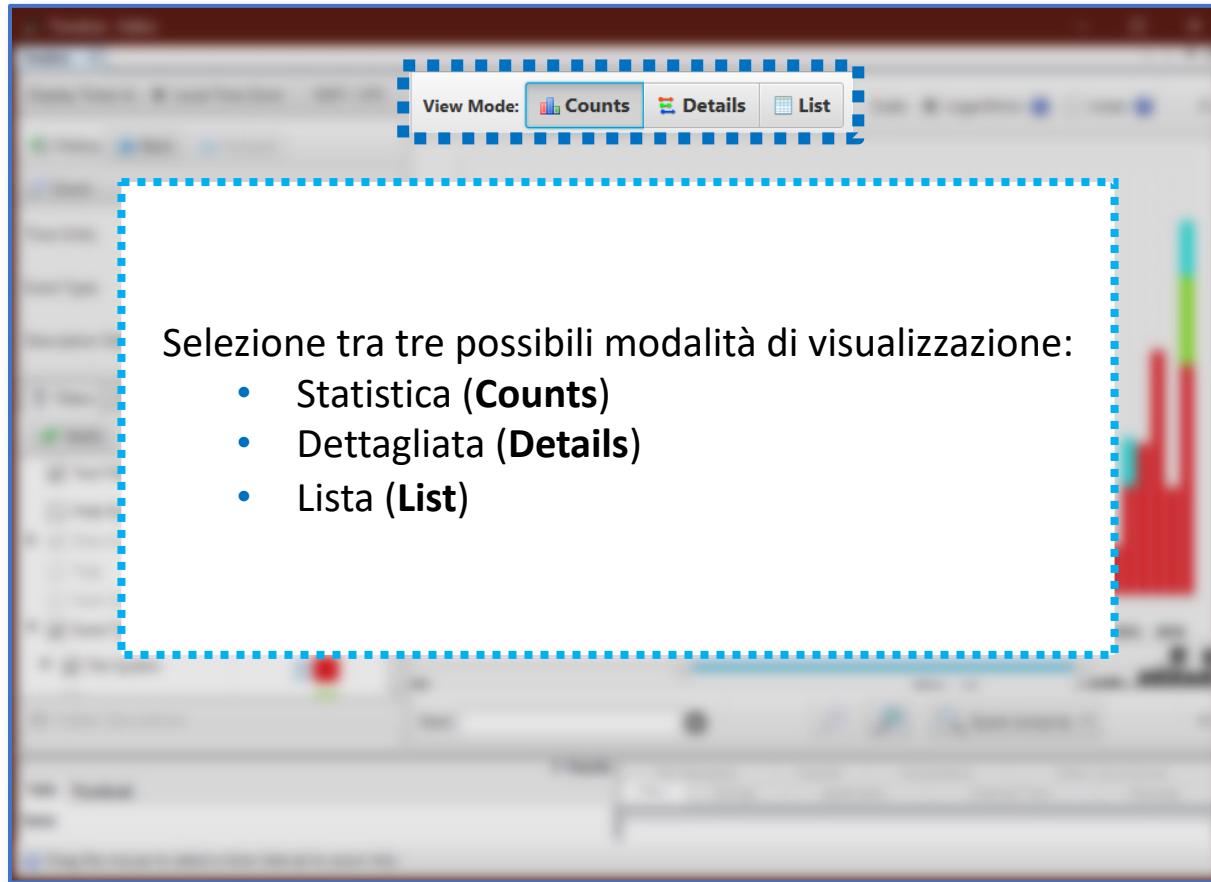


Area in cui è possibile navigare fra i vari artefatti individuati da Autopsy, suddivisi per categoria

Le Super Timeline

Timeline con Autopsy [Versione Windows] | 11/15

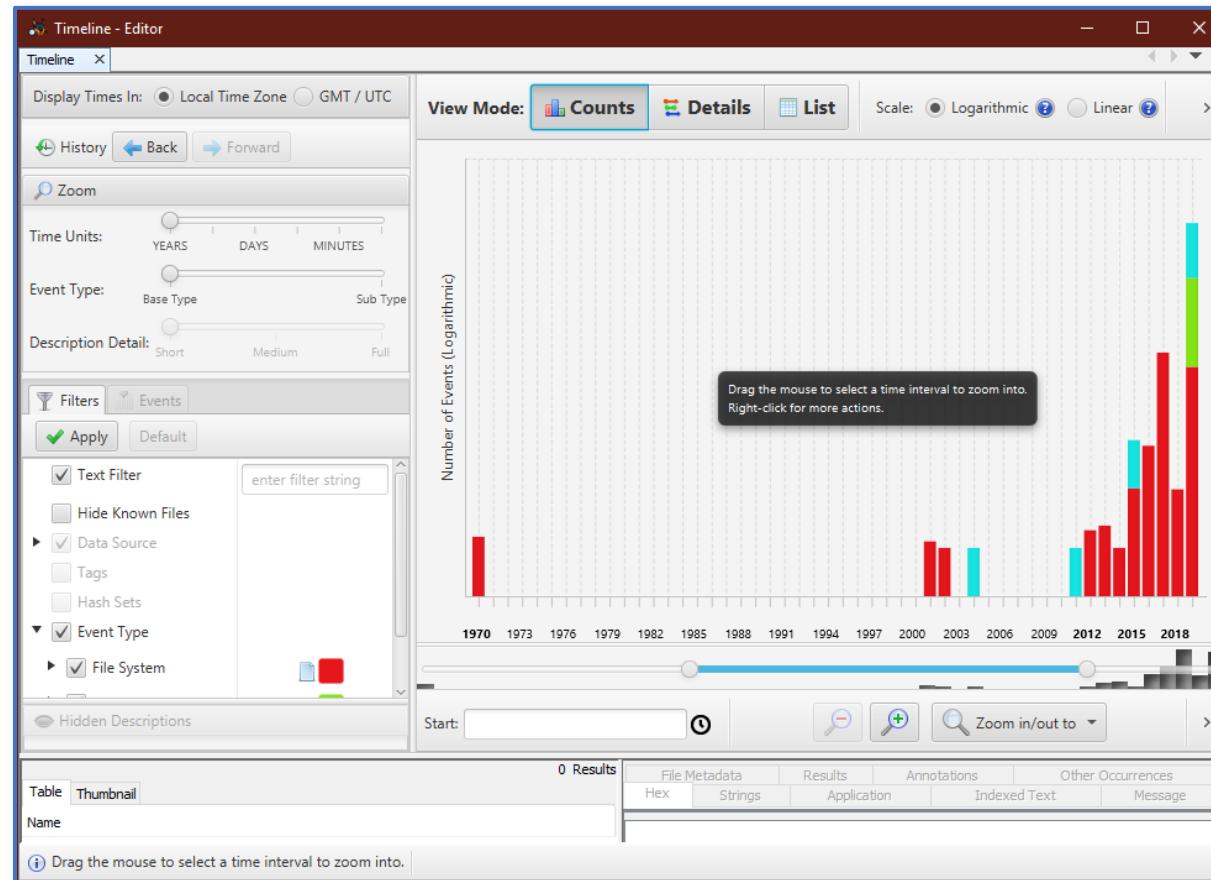
- *Interfaccia Utente per la Gestione della Timeline*



Le Super Timeline

Timeline con Autopsy [Versione Windows] | 12/15

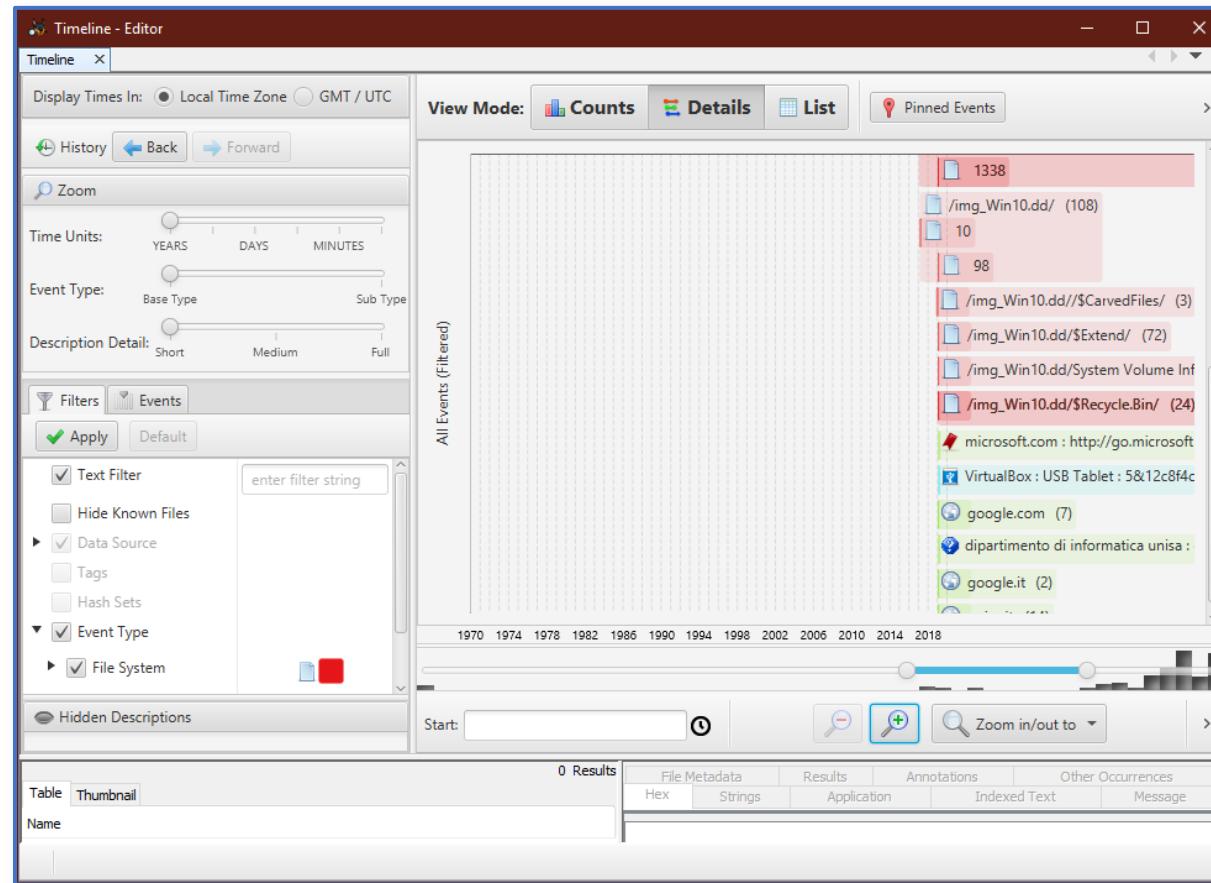
- *Interfaccia Utente per la Gestione della Timeline*
 - *Modalità di Visualizzazione: Statistica (Counts)*



Le Super Timeline

Timeline con Autopsy [Versione Windows] | 13/15

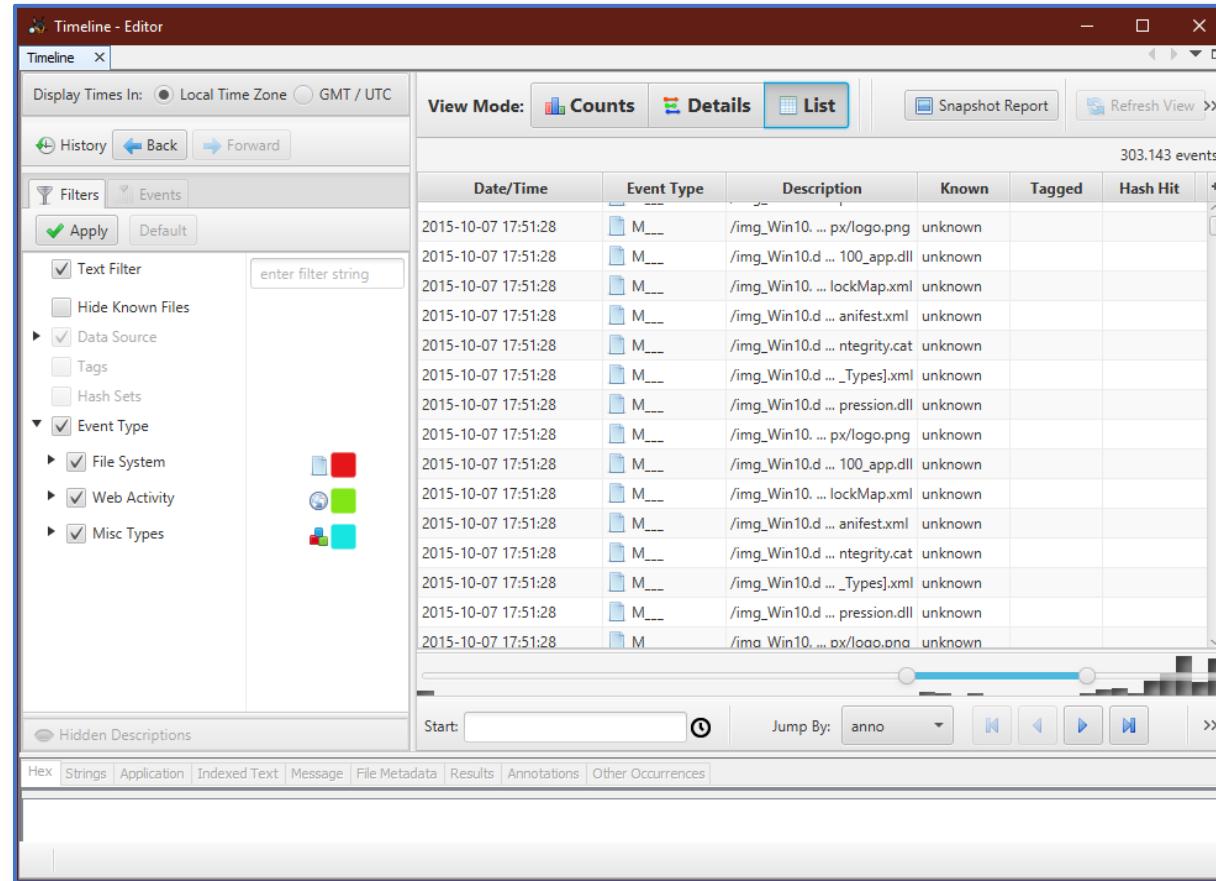
- *Interfaccia Utente per la Gestione della Timeline*
 - Modalità di Visualizzazione: Dettagliata (**Details**)



Le Super Timeline

Timeline con Autopsy [Versione Windows] | 14/15

- *Interfaccia Utente per la Gestione della Timeline*
 - Modalità di Visualizzazione: Lista (**List**)



Le Super Timeline

Timeline con Autopsy [Versione Windows] | 15/15

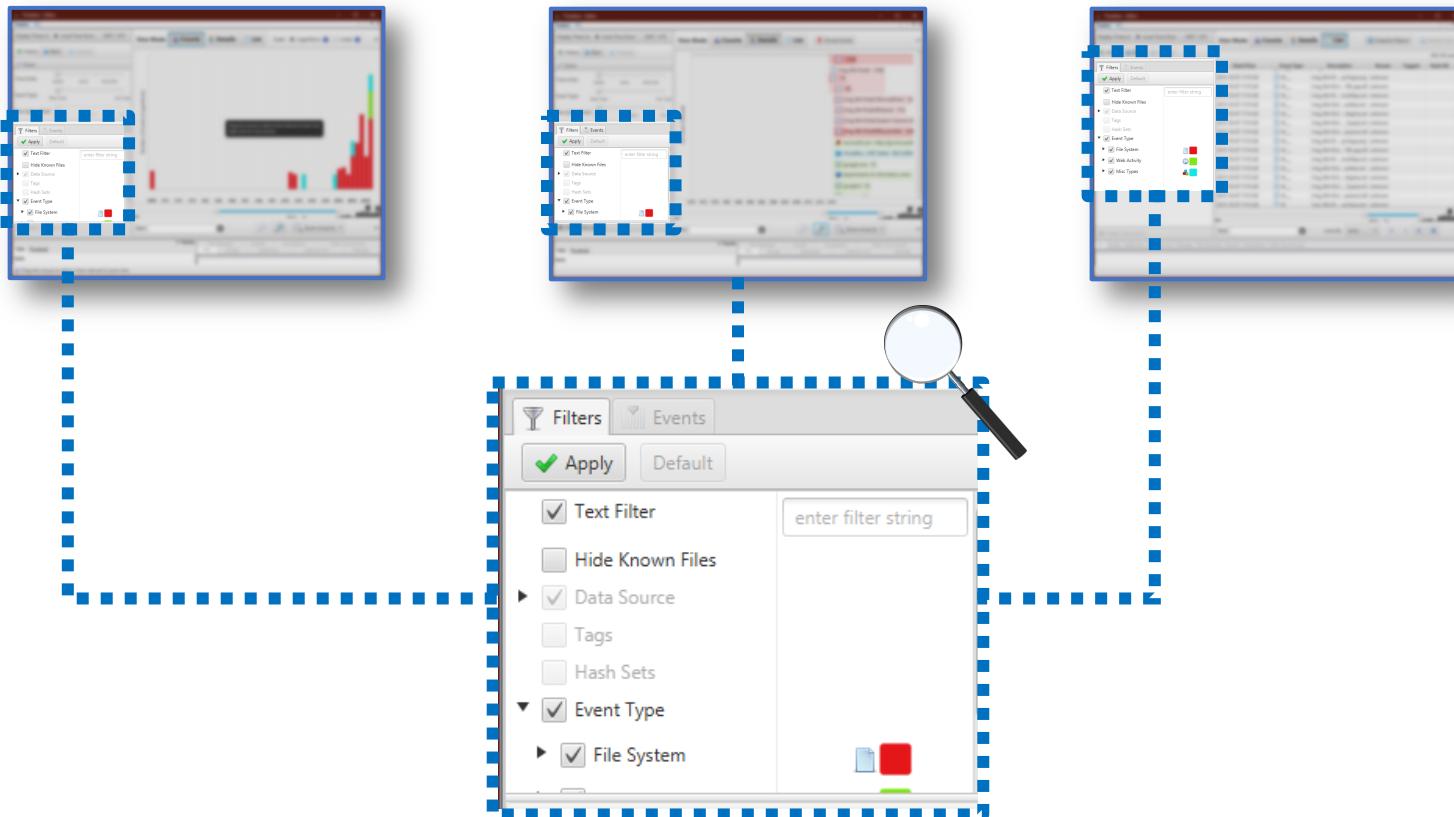
- *Interfaccia Utente per la Gestione della Timeline*
 - Per ogni modalità di visualizzazione è possibile specificare dei filtri, al fine di analizzare una porzione di interesse della timeline



Le Super Timeline

Timeline con Autopsy [Versione Windows] | 15/15

- *Interfaccia Utente per la Gestione della Timeline*
 - Per ogni modalità di visualizzazione è possibile specificare dei filtri, al fine di analizzare una porzione di interesse della timeline



Le Super Timeline

Visualizzazione mediante Timeline Explorer | 1/3

- **Timeline Explorer** è un software, sviluppato da Eric Zimmerman, che permette la **visualizzazione di timeline/super timeline**
 - Le timeline di input devono essere in formato XLS o in formato CSV (*Comma-Separated Values*)
 - Possono essere ottenute come output da vari tool (The Sleuth Kit, Volatility, Plaso, ecc.)
 - Visualizza le righe con **colori diversi**, in base alla tipologia di evento
 - Il software è disponibile per Windows ed è gratuitamente scaricabile al seguente link:
 - <https://ericzimmerman.github.io/#!index.md>

Le Super Timeline

Visualizzazione mediante Timeline Explorer | 2/3

- *Interfaccia Utente di Timeline Explorer | 1/2*

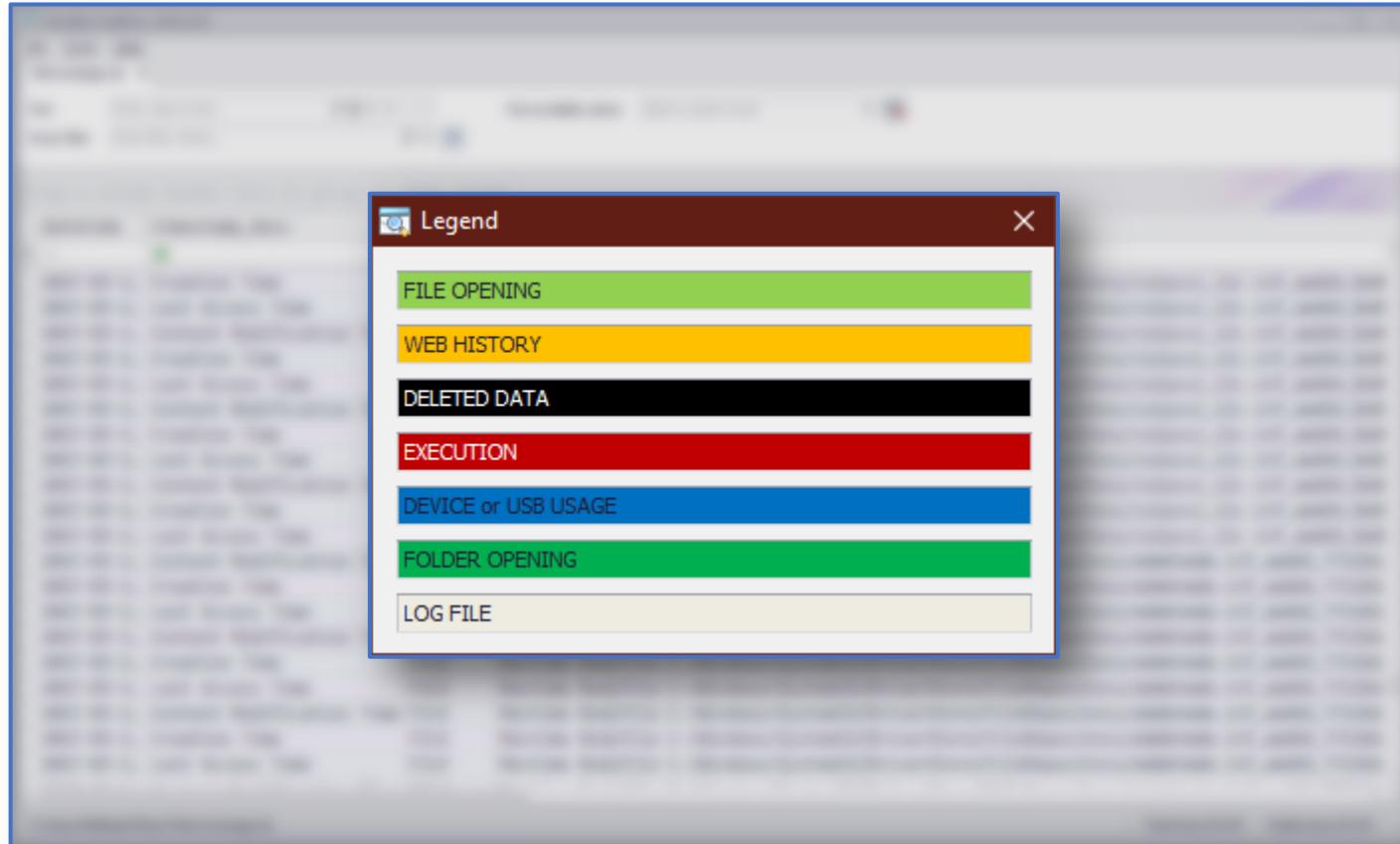
The screenshot shows the Timeline Explorer application window. The title bar reads "Timeline Explorer v0.8.12.0". The menu bar includes "File", "Tools", and "Help". A tab bar shows "FileCronologia.xls". Below the tabs are search and filter fields: "Find" (Enter value to find...) and "Power filter" (Enter filter criteria...). The main area is a table with the following columns: "datetime", "timestamp_desc", "source", "source_long", and "Long Description". The table contains numerous rows of data, mostly consisting of "Creation Time", "Last Access Time", and "Content Modification Time" entries for various files in the "Mactime Bodyfile" source, located at paths like "C:/Windows/System32/DriverStore/FileRepository/ialpssi_i2c.inf_amd64_8e0". The bottom status bar indicates "Total lines 65.535 | Visible lines 65.535".

datetime	timestamp_desc	source	source_long	Long Description
2017-03-1...	Creation Time	FILE	Mactime Bodyfile	C:/Windows/System32/DriverStore/FileRepository/ialpssi_i2c.inf_amd64_8e0
2017-03-1...	Last Access Time	FILE	Mactime Bodyfile	C:/Windows/System32/DriverStore/FileRepository/ialpssi_i2c.inf_amd64_8e0
2017-03-1...	Content Modification Time	FILE	Mactime Bodyfile	C:/Windows/System32/DriverStore/FileRepository/ialpssi_i2c.inf_amd64_8e0
2017-03-1...	Creation Time	FILE	Mactime Bodyfile	C:/Windows/System32/DriverStore/FileRepository/ialpssi_i2c.inf_amd64_8e0
2017-03-1...	Last Access Time	FILE	Mactime Bodyfile	C:/Windows/System32/DriverStore/FileRepository/ialpssi_i2c.inf_amd64_8e0
2017-03-1...	Content Modification Time	FILE	Mactime Bodyfile	C:/Windows/System32/DriverStore/FileRepository/ialpssi_i2c.inf_amd64_8e0
2017-03-1...	Creation Time	FILE	Mactime Bodyfile	C:/Windows/System32/DriverStore/FileRepository/ialpssi_i2c.inf_amd64_8e0
2017-03-1...	Last Access Time	FILE	Mactime Bodyfile	C:/Windows/System32/DriverStore/FileRepository/ialpssi_i2c.inf_amd64_8e0
2017-03-1...	Content Modification Time	FILE	Mactime Bodyfile	C:/Windows/System32/DriverStore/FileRepository/ialpssi_i2c.inf_amd64_8e0
2017-03-1...	Creation Time	FILE	Mactime Bodyfile	C:/Windows/System32/DriverStore/FileRepository/ialpssi_i2c.inf_amd64_8e0
2017-03-1...	Last Access Time	FILE	Mactime Bodyfile	C:/Windows/System32/DriverStore/FileRepository/ialpssi_i2c.inf_amd64_8e0
2017-03-1...	Content Modification Time	FILE	Mactime Bodyfile	C:/Windows/System32/DriverStore/FileRepository/ialpssi_i2c.inf_amd64_8e0
2017-03-1...	Creation Time	FILE	Mactime Bodyfile	C:/Windows/System32/DriverStore/FileRepository/ialpssi_i2c.inf_amd64_8e0
2017-03-1...	Last Access Time	FILE	Mactime Bodyfile	C:/Windows/System32/DriverStore/FileRepository/ialpssi_i2c.inf_amd64_8e0
2017-03-1...	Content Modification Time	FILE	Mactime Bodyfile	C:/Windows/System32/DriverStore/FileRepository/mdmbtmdm.inf_amd64_7712bb.
2017-03-1...	Creation Time	FILE	Mactime Bodyfile	C:/Windows/System32/DriverStore/FileRepository/mdmbtmdm.inf_amd64_7712bb.
2017-03-1...	Last Access Time	FILE	Mactime Bodyfile	C:/Windows/System32/DriverStore/FileRepository/mdmbtmdm.inf_amd64_7712bb.
2017-03-1...	Content Modification Time	FILE	Mactime Bodyfile	C:/Windows/System32/DriverStore/FileRepository/mdmbtmdm.inf_amd64_7712bb.
2017-03-1...	Creation Time	FILE	Mactime Bodyfile	C:/Windows/System32/DriverStore/FileRepository/mdmbtmdm.inf_amd64_7712bb.
2017-03-1...	Last Access Time	FILE	Mactime Bodyfile	C:/Windows/System32/DriverStore/FileRepository/mdmbtmdm.inf_amd64_7712bb.
2017-03-1...	Content Modification Time	FILE	Mactime Bodyfile	C:/Windows/System32/DriverStore/FileRepository/mdmbtmdm.inf_amd64_7712bb.
2017-03-1...	Creation Time	FILE	Mactime Bodyfile	C:/Windows/System32/DriverStore/FileRepository/mdmbtmdm.inf_amd64_7712bb.
2017-03-1...	Last Access Time	FILE	Mactime Bodyfile	C:/Windows/System32/DriverStore/FileRepository/mdmbtmdm.inf_amd64_7712bb.

Le Super Timeline

Visualizzazione mediante Timeline Explorer | 3/3

- *Interfaccia Utente di Timeline Explorer | 2/2 | Legenda*



Riferimenti Bibliografici

- **Digital Forensics with Kali Linux, Shiva V.N. Parasram, Packt Publishing, 2017**
 - Capitolo 8
- **Practical Windows Forensics, Ayman Shaaban, Konstantin Sapronov, Packt Publishing, 2016**
 - Capitolo 5
- **Documentazione Utente del Framework Plaso**
 - <https://plaso.readthedocs.io/en/latest/sources/user/Users-Guide.html>
- **Timeline Explorer**
 - <https://ericzimmerman.github.io/#!index.md>