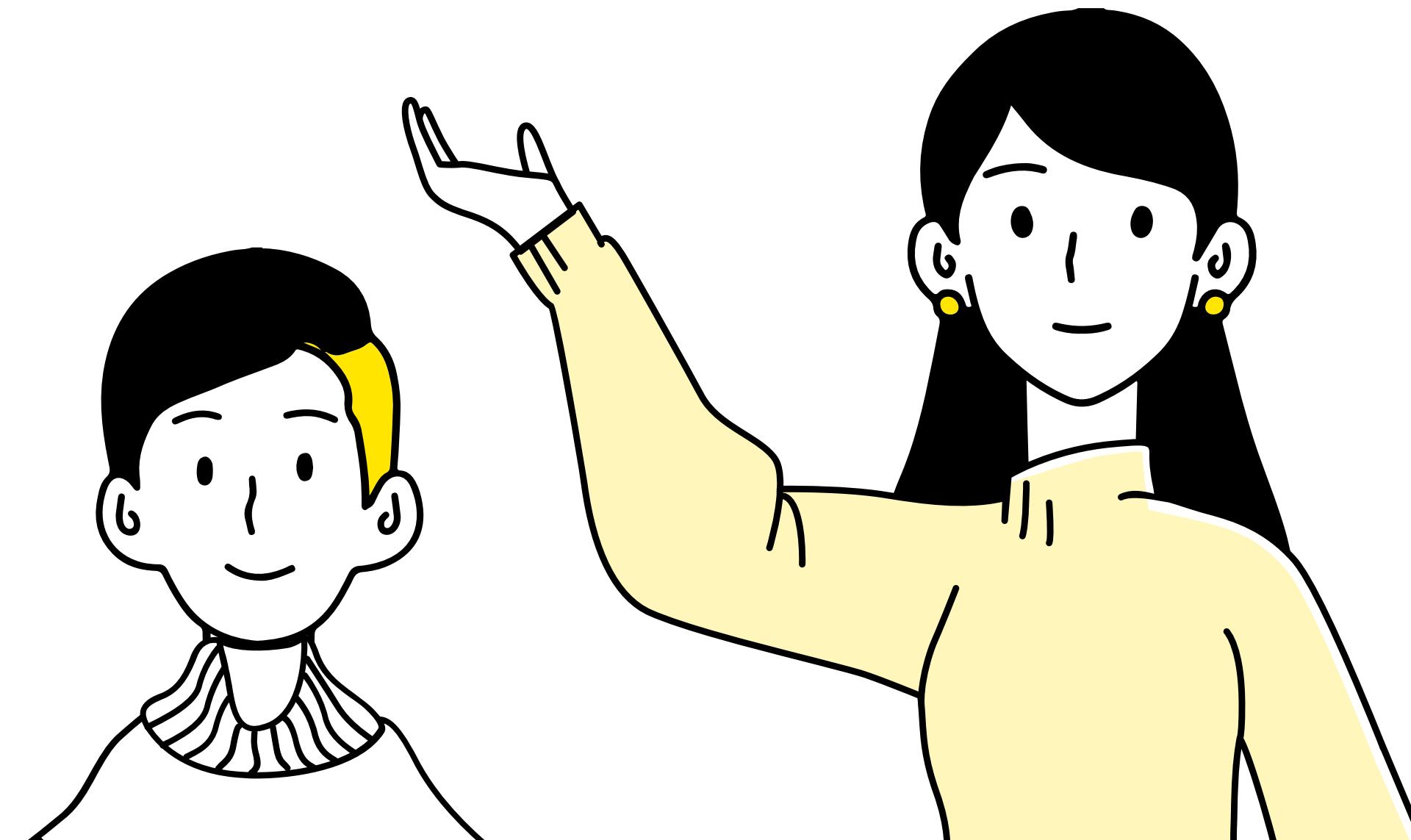


CAINE TOOLS

Strumenti per acquisire e analizzare prove digitali, molto popolare tra gli investigatori digitali.



Caine

Distribuzione per l'Investigazione Forense Digitale

- **Basata su Ubuntu:** Infrastruttura stabile e affidabile
- **Scopo:** Fornisce agli investigatori forensi digitali gli strumenti necessari per analizzare e recuperare dati da dispositivi informatici.
- **Utilizzo:** Conduce investigazioni digitali, inclusa l'analisi forense di computer, dispositivi mobili e reti.
- **Risultato:** Raccoglie prove digitali cruciali per investigazioni legali o di sicurezza informatica.



<https://www.caine-live.net/page11/page11.html>

Iniziamo!



Tool da Presentare

1

Guymager & Autopsy

3

tcpdump & Wireshark

2

StegoSuite

4

chntpw



Guymager & Autopsy

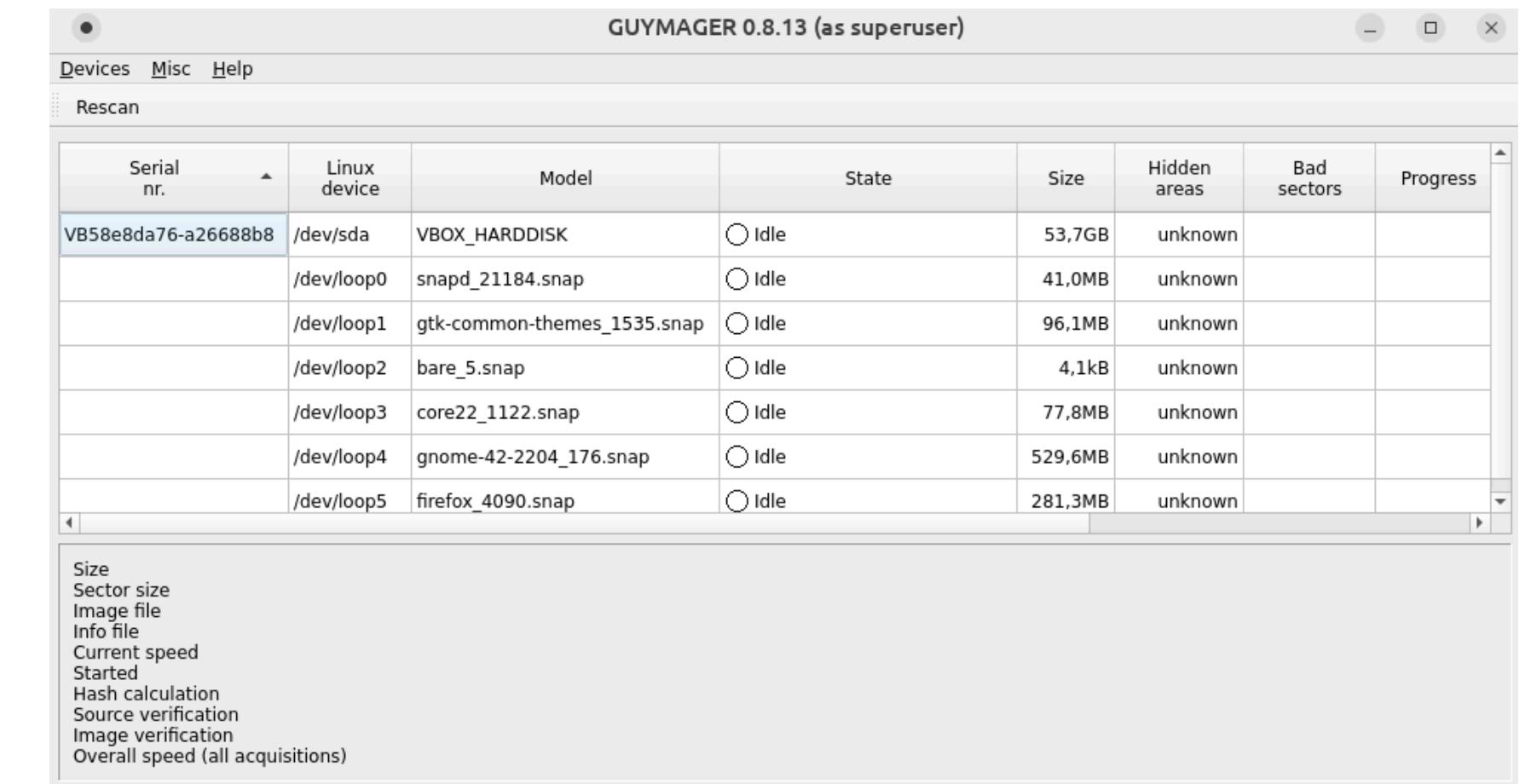
Recupero di file cancellati

Ti è mai capitato di cancellare accidentalmente un file da una chiavetta USB e di non poterlo più recuperare? Con l'aiuto di questo strumento, ora è possibile ripristinare tutti i file eliminati da una chiavetta USB in modo rapido e semplice.



Guymager

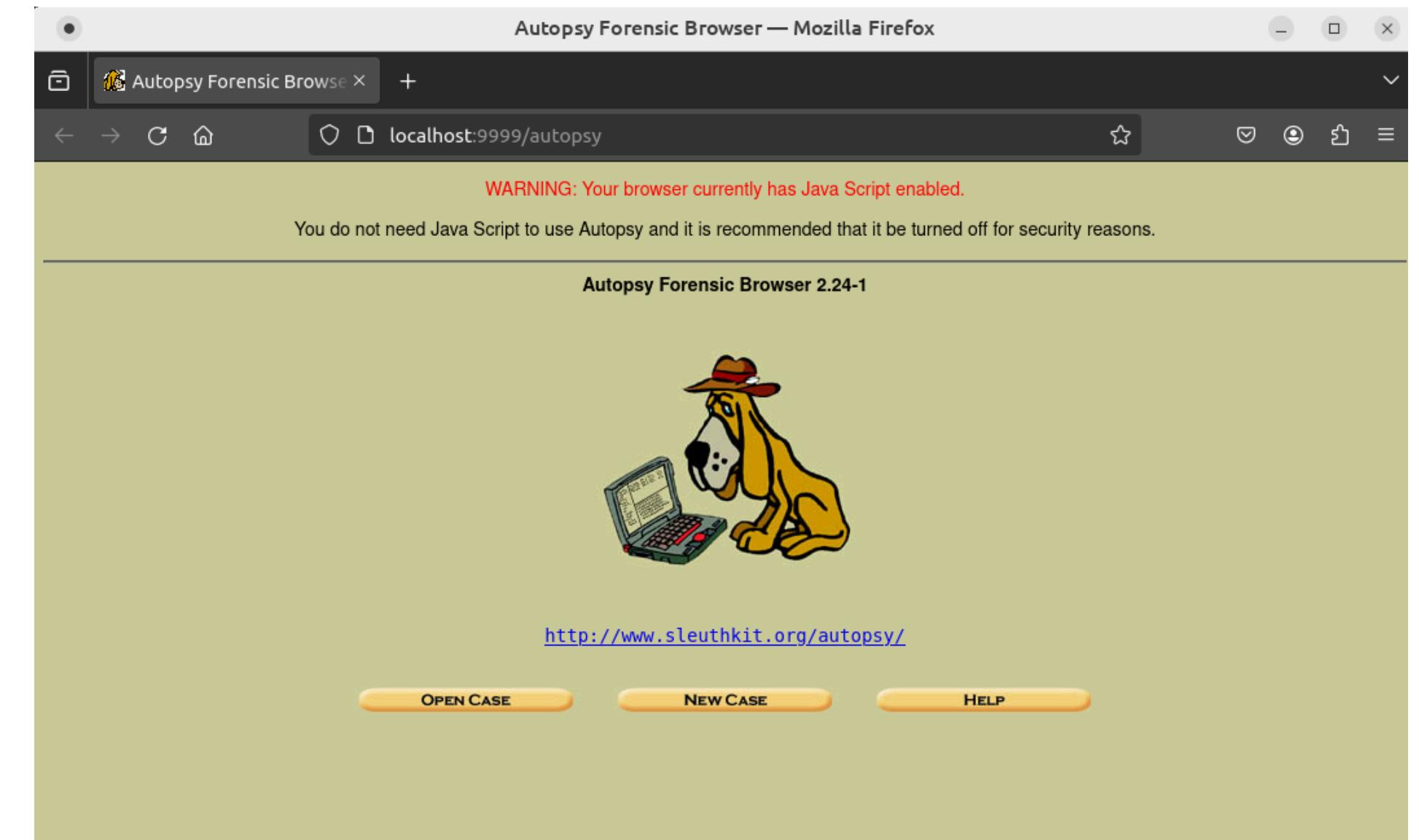
Strumento software utilizzato per acquisire immagini forensi esatte di dischi rigidi e dispositivi di archiviazione, principalmente utilizzato nell'ambito della digital forensics per preservare l'integrità dei dati.



Autopsy

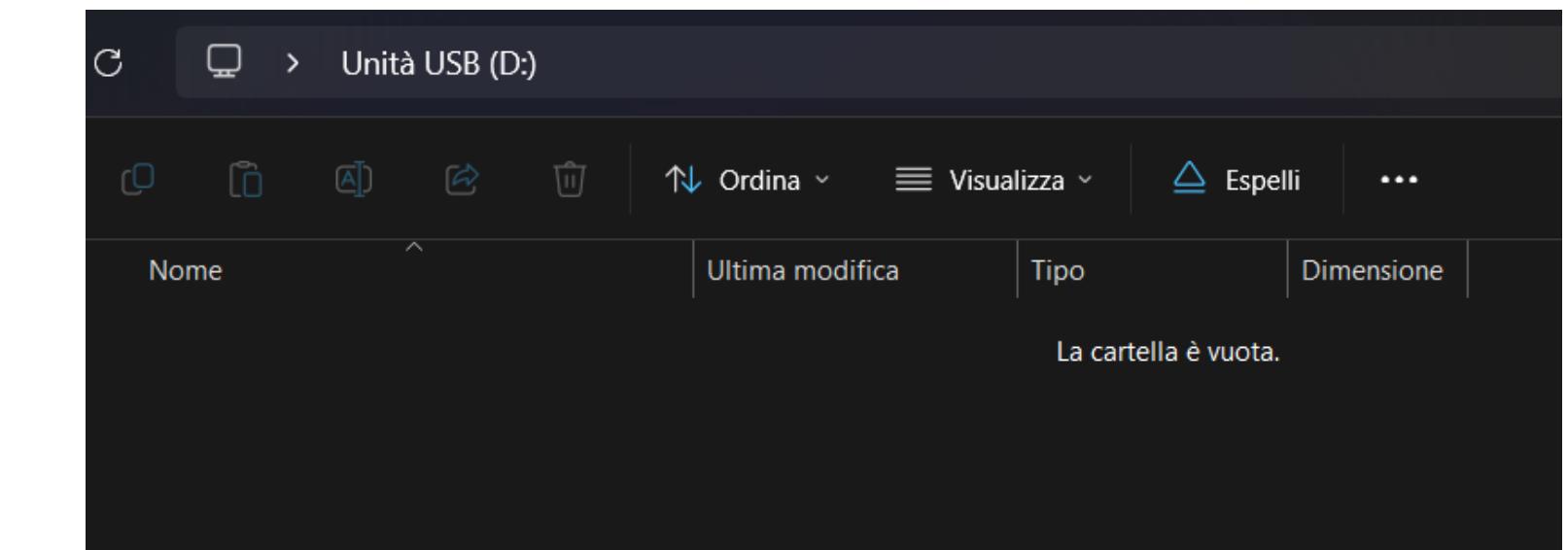
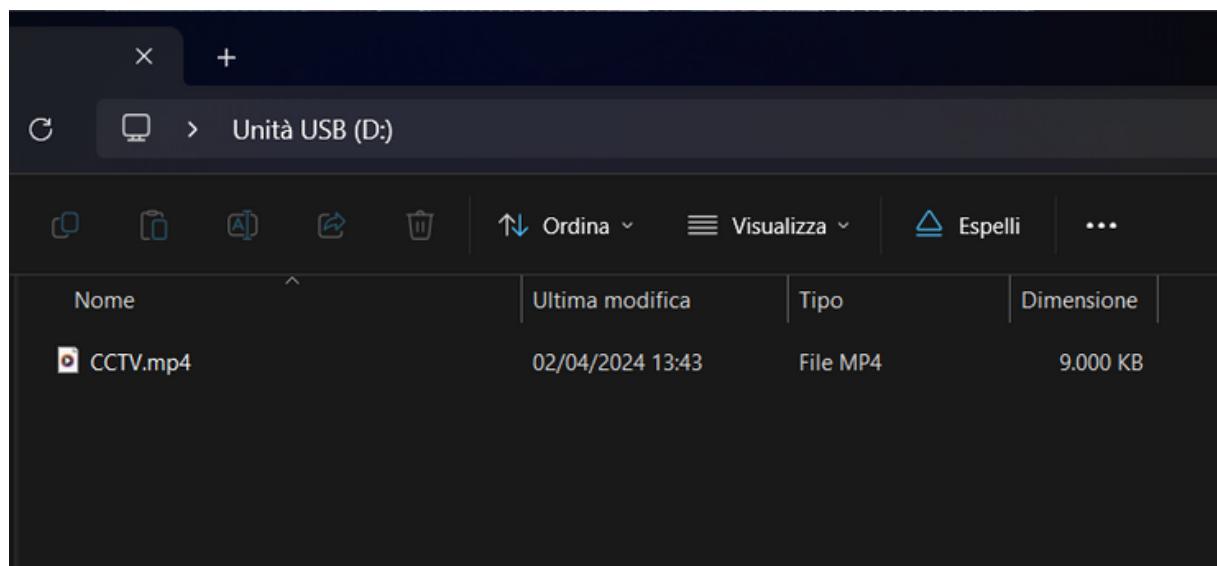
Strumento per l'analisi forense digitale che aiuta gli investigatori a esaminare dispositivi di archiviazione.

Permette di cercare, analizzare e recuperare file, condurre ricerche forensi e trovare informazioni cruciali per le indagini.



Esempio utilizzo Autopsy

Supponiamo che un DVR abbia registrato il furto di una macchina (in questo caso un file video) e che il malvivente sia stato in grado di eliminare la prova



Utilizzare Autopsy da riga di comando

Dopo aver effettuato l'acquisizione della memoria con Guymager, possiamo avviare il terminale nella cartella contenente l'acquisizione e digitare il comando:
mmls nomeAcquisizione

```
File Edit View Search Terminal Help
salvo@salvo:~/Desktop/CopiaChiavetta$ mmls copia.E01
DOS Partition Table
Offset Sector: 0
Units are in 512-byte sectors

      Slot      Start      End      Length      Description
000: Meta      0000000000  0000000000  0000000001  Primary Table (#0)
001: -----      0000000000  0000000031  0000000032  Unallocated
002: 000:000      0000000032  0001970687  0001970656  Win95 FAT32 (0x0c)
003: -----      0001970688  0001971199  0000000512  Unallocated
```

Adesso sappiamo che la memoria è stata divisa in partizioni e che la parte allocata, in questo caso, inizia al punto 32

Utilizzare Autopsy da riga di comando

Adesso possiamo digitare il comando:

“fls -o [offset] [nomefile]”

E verrà mostrata una lista di file

```
salvo@salvo:~/Desktop/CopiaChiavetta$ fls -o 32 copia.E01
d/d 5: System Volume Information
r/r * 6: _CTV.mp4
v/v 31399427: $MBR
v/v 31399428: $FAT1
v/v 31399429: $FAT2
V/V 31399430: $OrphanFiles
```

Notiamo che il file eliminato è presente nella lista

Utilizzare Autopsy da riga di comando

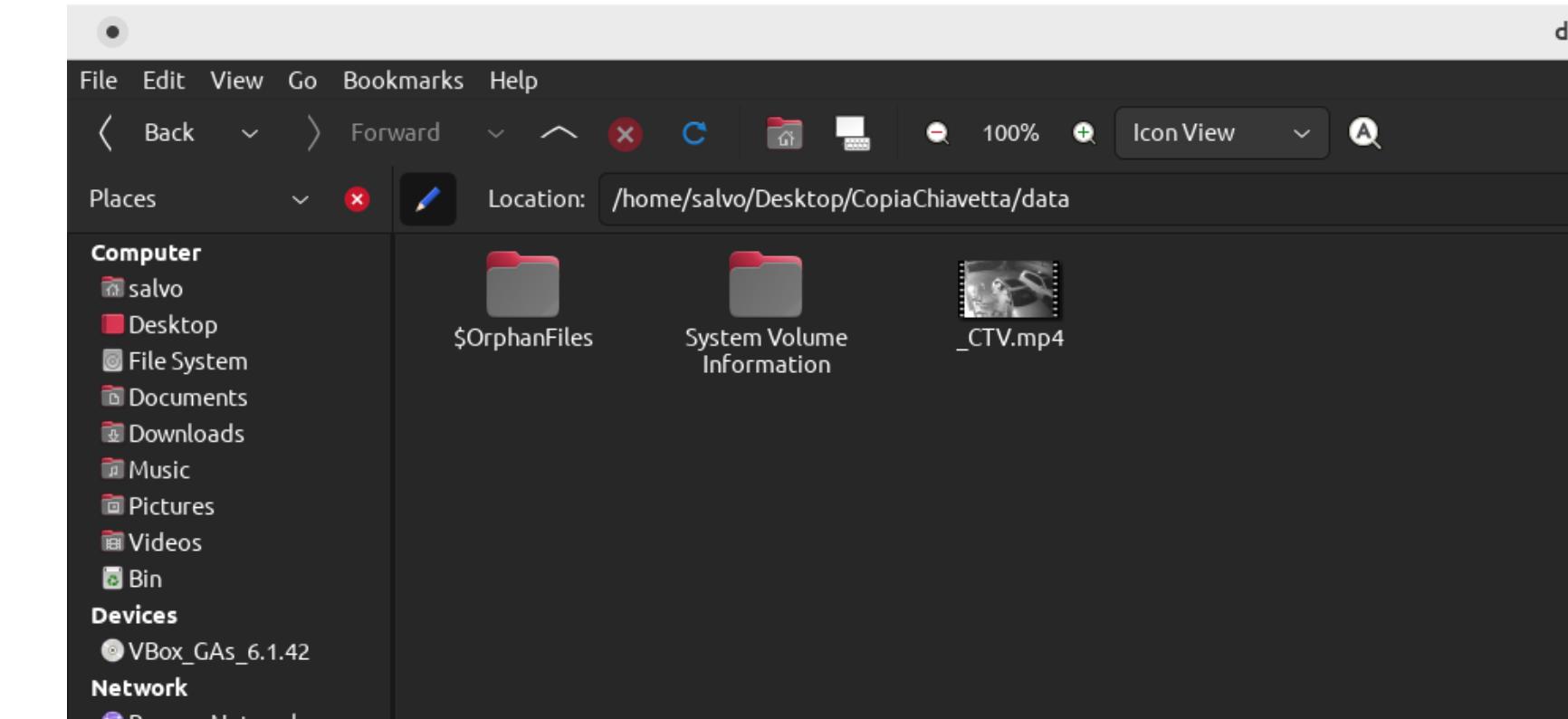
```
salvo@salvo:~/Desktop/CopiaChiavetta$ tsk_recover -i ewf -e -o 32 copia.E01 data
Files Recovered: 1480
salvo@salvo:~/Desktop/CopiaChiavetta$
```

Infine col comando
mostrato in figura
recupereremo tutti i file e
verranno inseriti in una
cartella chiamata “data”

Ulteriori spiegazioni: -i ewf serve per il tipo di file che abbiamo acquisito, in questo caso .EXX;
-e serve per recuperare i file eliminati e quelli presenti in memoria;
-o 32 serve per sapere da quale offset partire;
copia.E01 è il nome della copia;
data è la cartella di destinazione dei file recuperati;

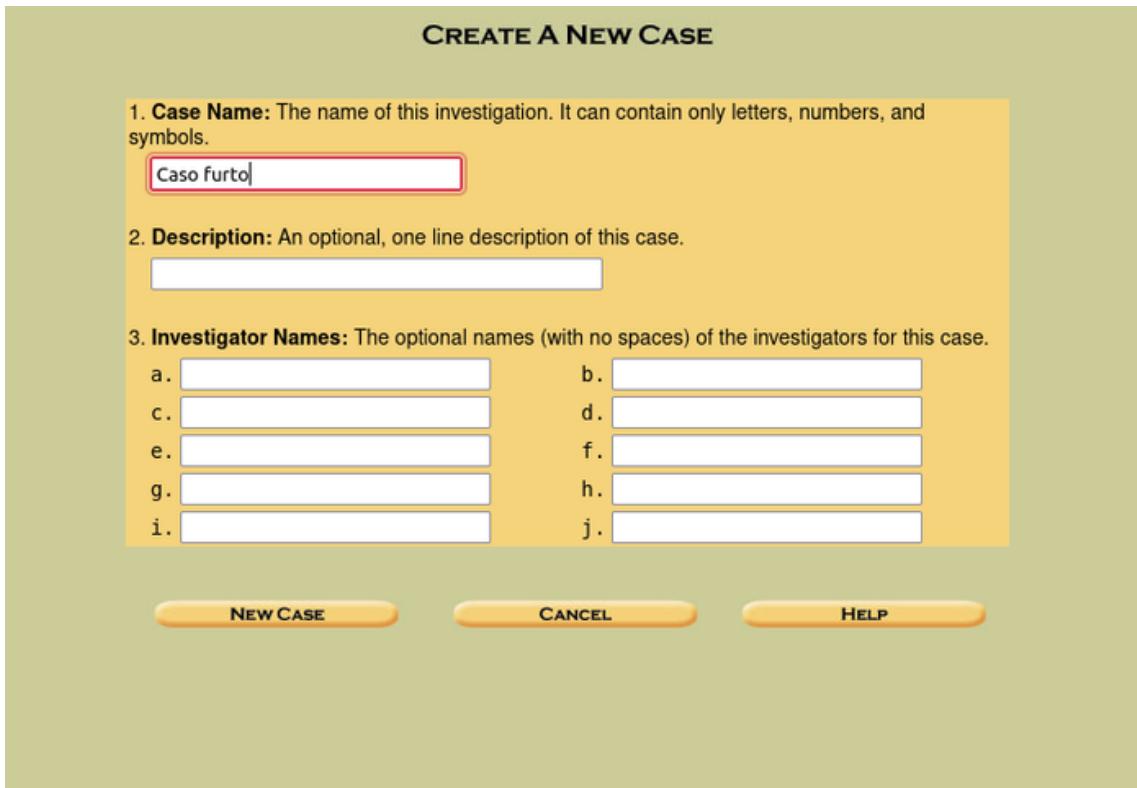
Utilizzare Autopsy da riga di comando

Abbiamo recuperato correttamente il file che era stato eliminato

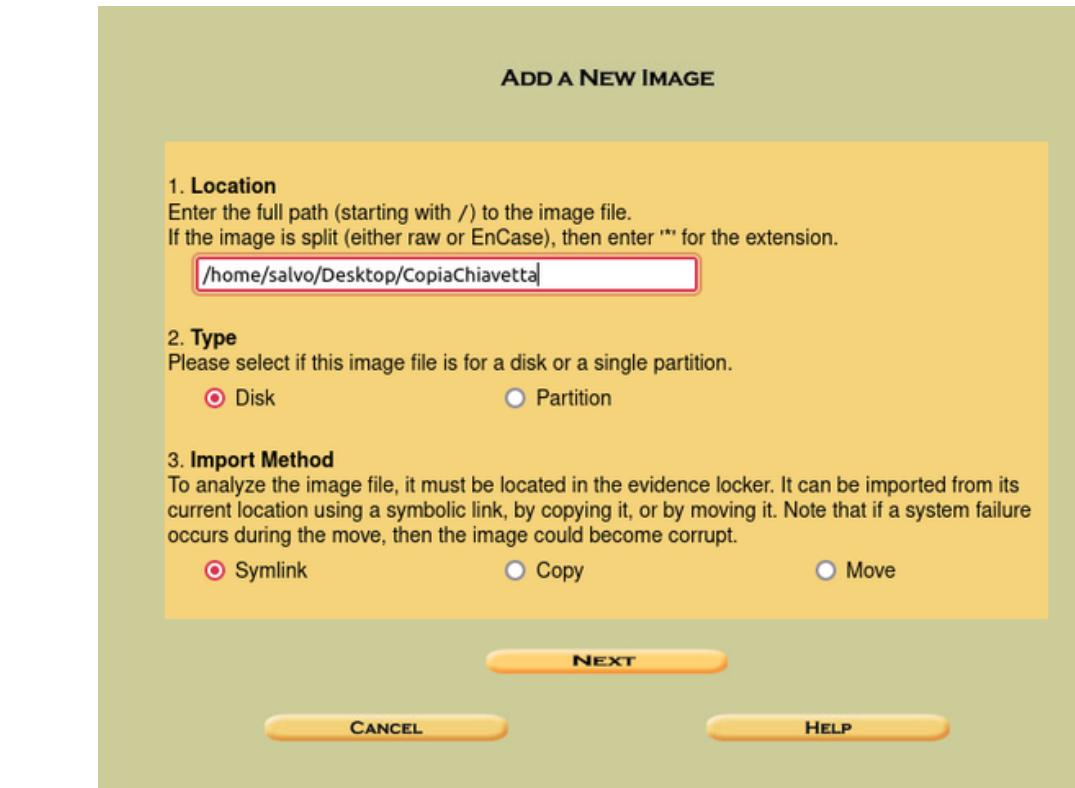


Autopsy

È possibile effettuare il recupero di un file utilizzando una GUI: Autopsy.
Dopo aver acquisito l'immagine, creiamo un nuovo caso e aggiungiamo
l'immagine precedentemente acquisita



Creazione caso



Aggiunta immagine

Autopsy

Aprendo il caso vedremo una lista di file, nella quale, evidenziati in rosso quelli eliminati.

Current Directory: C:/

ADD NOTE GENERATE MD5 LIST OF FILES

DEL	Type	NAME	WRITTEN	ACCESSED	CREATED	SIZE	UID	GID	META	
	dir / in									
	v / v	\$FAT1	0000-00-00 00:00:00 (UTC)	0000-00-00 00:00:00 (UTC)	0000-00-00 00:00:00 (UTC)	0 0 0	981504	0	0	31399428
	v / v	\$FAT2	0000-00-00 00:00:00 (UTC)	0000-00-00 00:00:00 (UTC)	0000-00-00 00:00:00 (UTC)	0 0 0	981504	0	0	31399429
	v / v	\$MBR	0000-00-00 00:00:00 (UTC)	0000-00-00 00:00:00 (UTC)	0000-00-00 00:00:00 (UTC)	0 0 0	512	0	0	31399427
✓	r / r	CTV.mp4	2024-04-02 13:43:58 (CEST)	2024-04-02 00:00:00 (CEST)	2024-04-02 13:45:20 (CEST)	9215042 0 0 6				
	d / d	System Volume Information/	2024-04-02 13:45:06 (CEST)	2024-04-02 00:00:00 (CEST)	2024-04-02 13:45:05 (CEST)	4096 0 0 5				

Error Parsing File (Invalid Characters?):
V/V 31399430: \$OrphanFiles 0000-00-00 00:00:00 (UTC) 0000-00-00 00:00:00 (UTC) 0000-00-00 00:00:00 (UTC) 0000-00-00 00:00:00 (UTC) 0 0 0

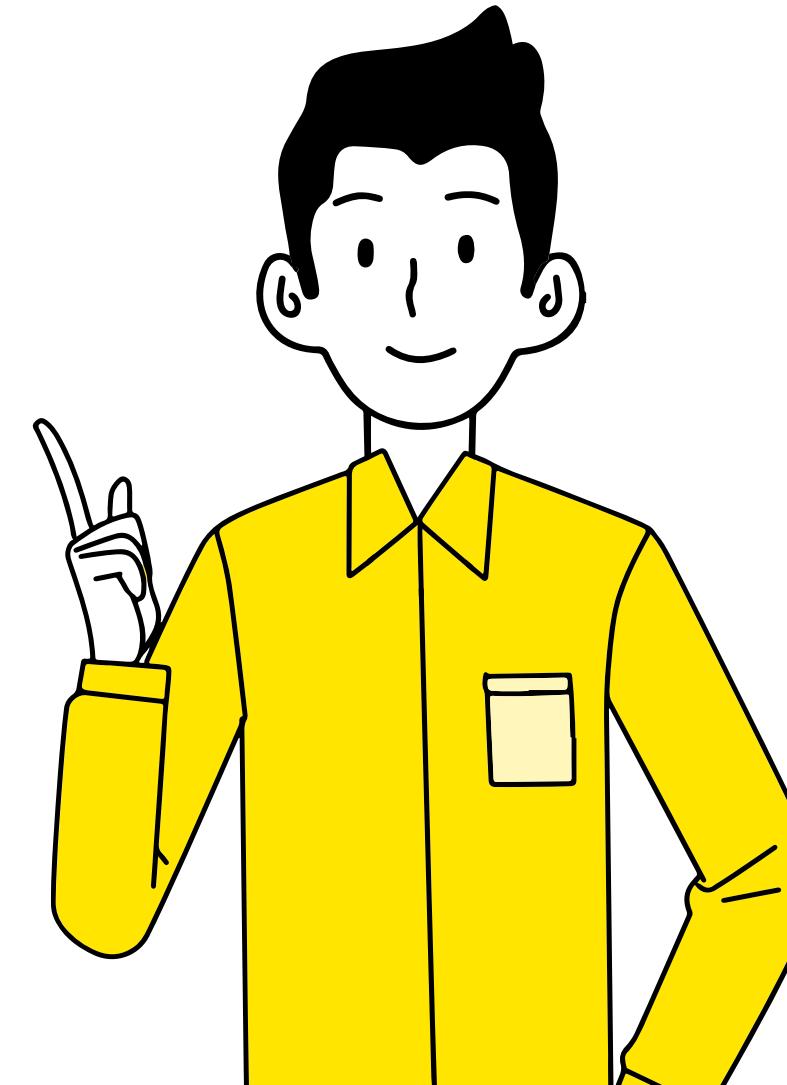
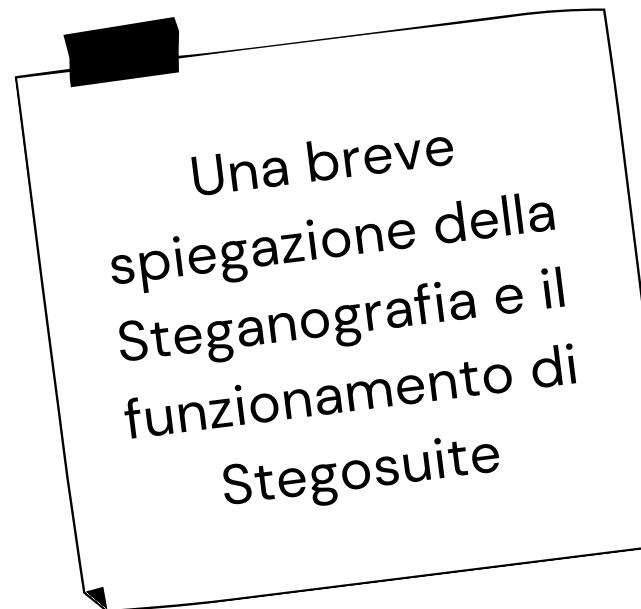




StegoSuite

Vincenzo Villanova

Steganografia tramite l'utilizzo di Stegosuite



Steganografia

Arte di nascondere messaggi o informazioni all'interno di altri dati, in modo tale che l'esistenza del messaggio nascosto non sia apparente per un osservatore casuale.

Questo può essere fatto inserendo il messaggio in file multimediali come immagini (ciò che faremo noi), audio o video, senza compromettere l'aspetto o il suono del file originale.



Stegosuite

Stegosuite offre un'interfaccia utente intuitiva per incorporare messaggi segreti all'interno di immagini utilizzando diversi metodi di steganografia, come la modifica dei bit meno significativi (Least Significant Bit - LSB), algoritmi di trasformazione o algoritmi basati su frequenza.



Vincenzo Villanova

Diamoci da fare!



Come aggiornare le librerie

1

sudo su

3

sudo update-alternatives --config java

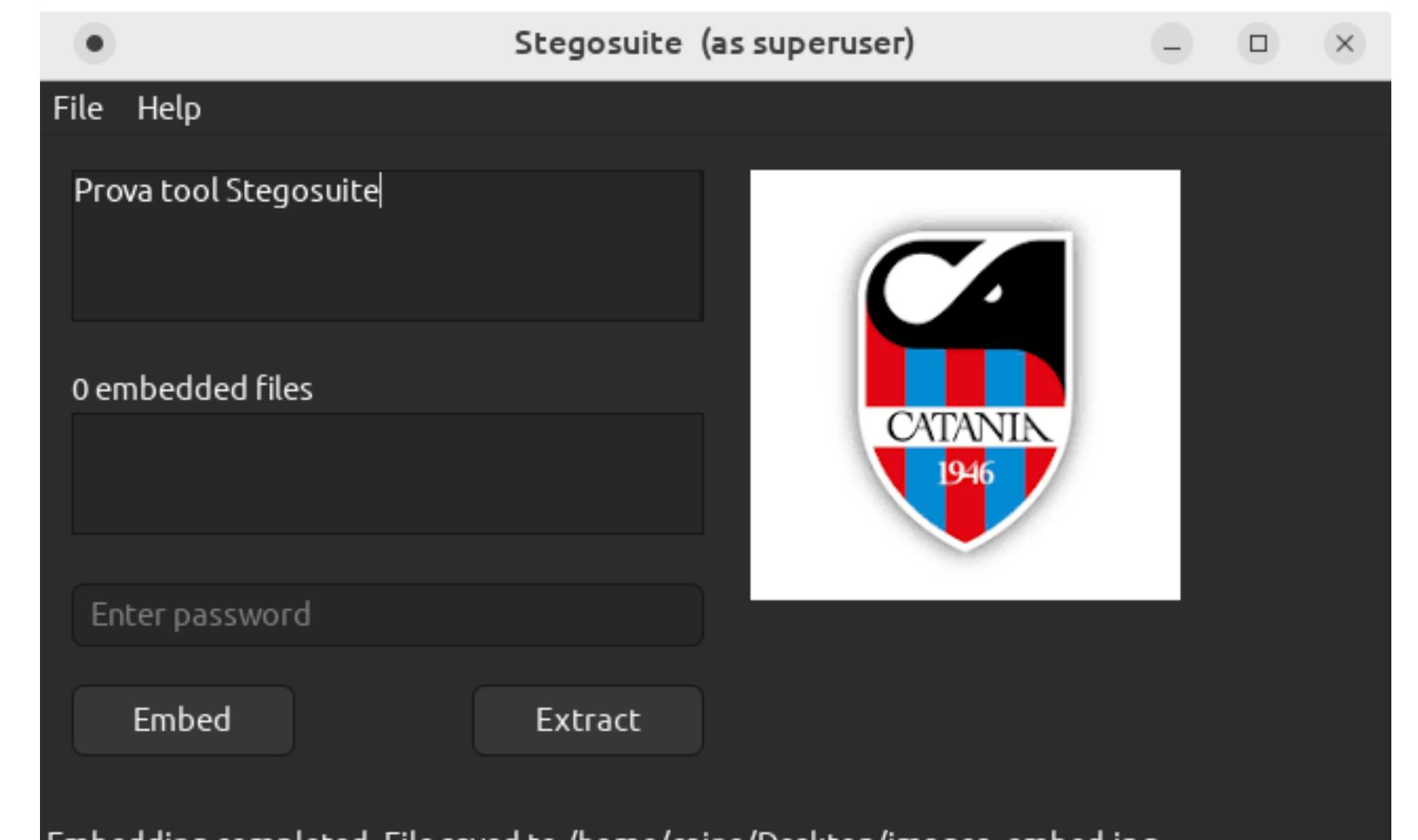
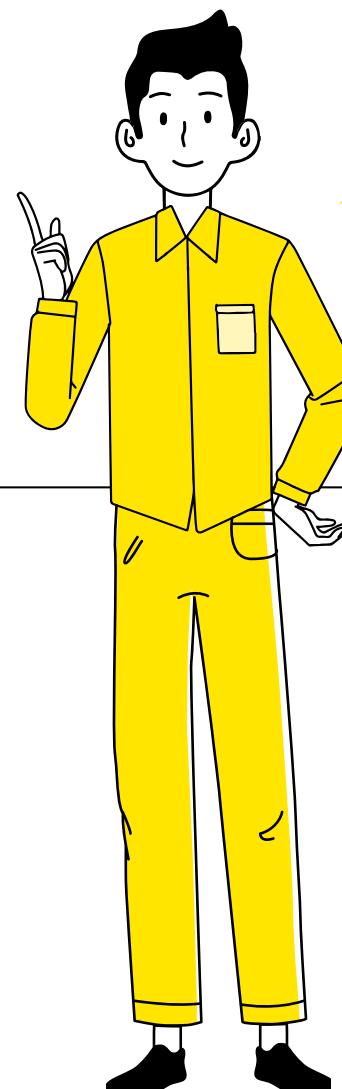
2

ln -s /usr/lib/jni/libswt-*
~/.swt/lib/linux/x86_64/

4

stegosuite

Come nascondere dati all'interno di un'immagine?



1

Avvia stegosuite

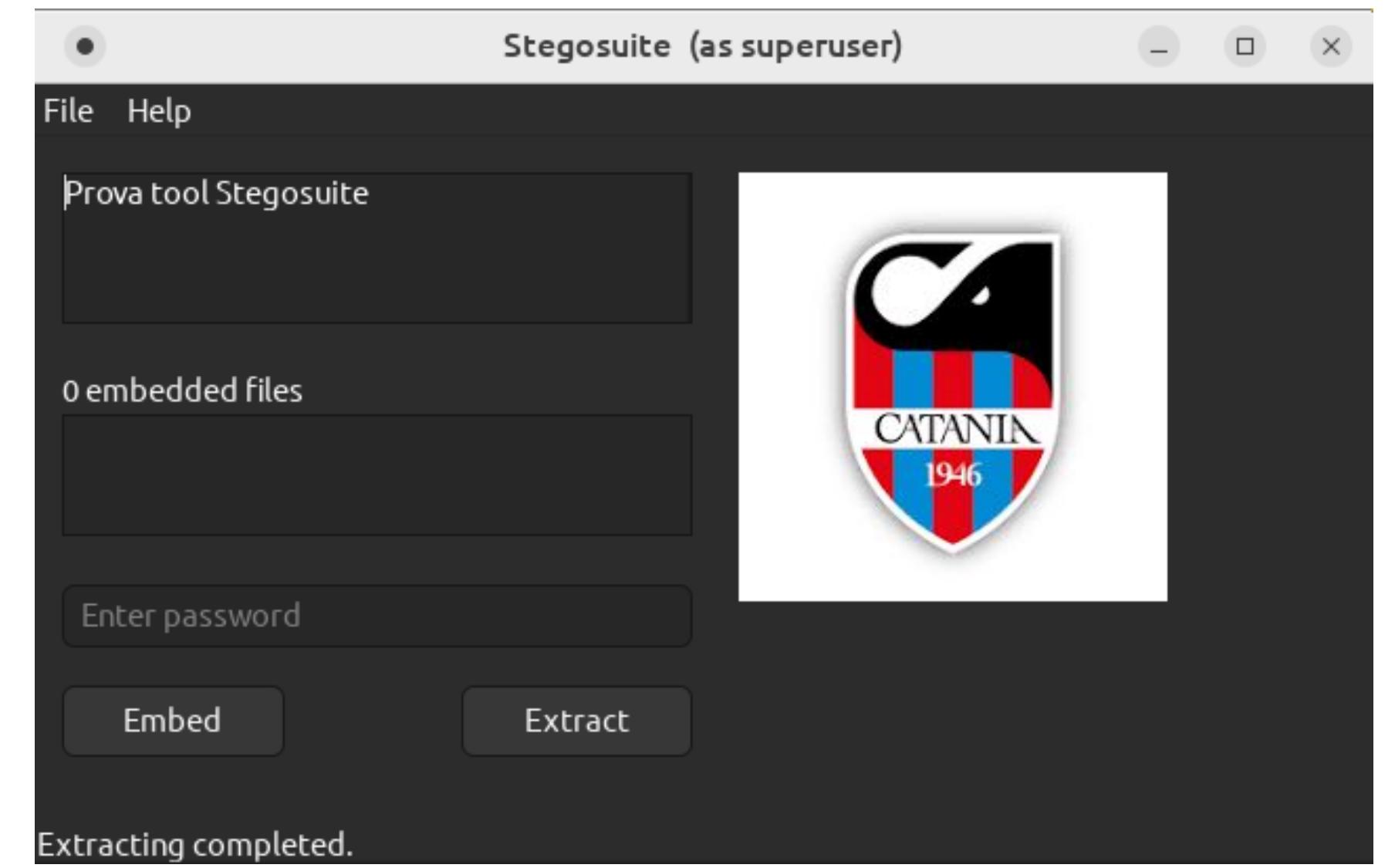
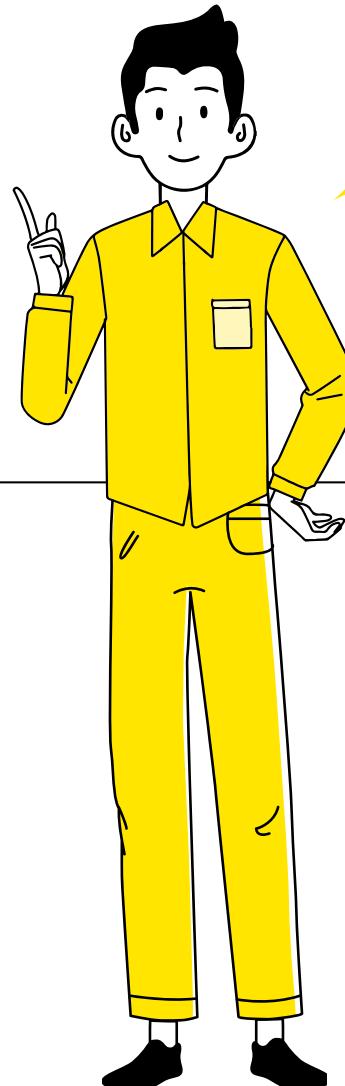
2

Selezione l'immagine da
usare

3

Immettere il messaggio da
nascondere

**Qual è il metodo
per estrarre
dati da
un'immagine?**



1

Avvia stegosuite

2

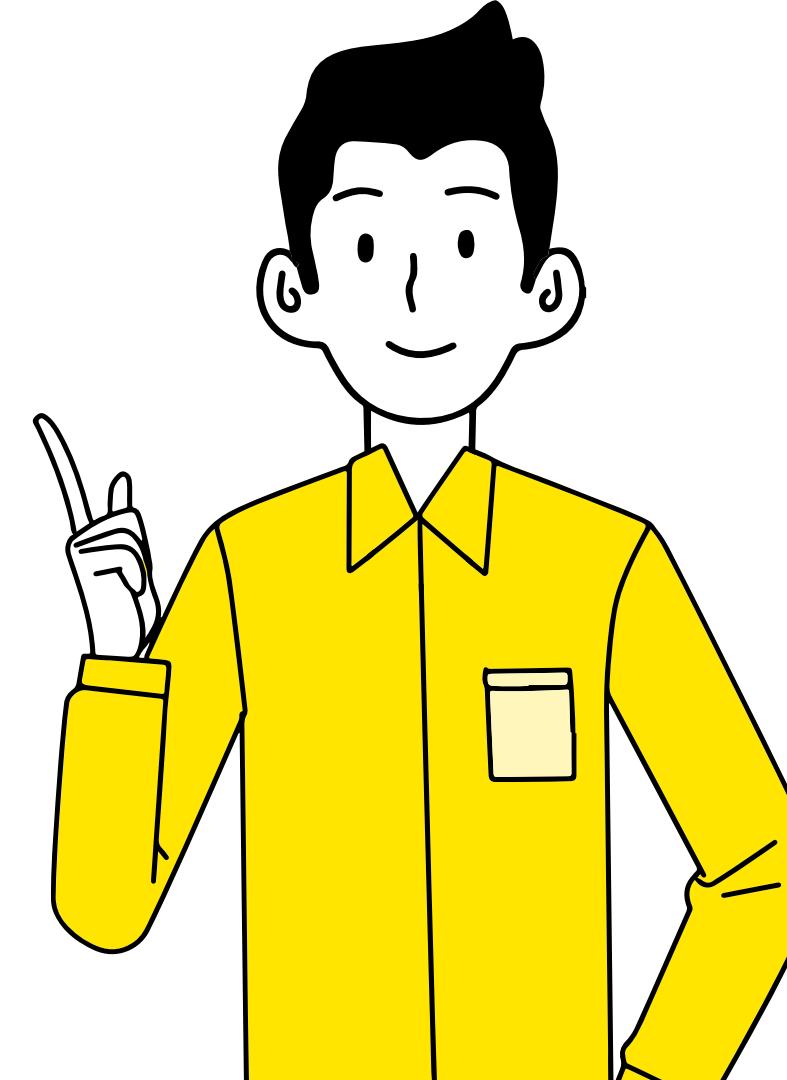
Seleziona l'immagine da
verificare

3

Cliccare il tasto Extract

Vincenzo Villanova

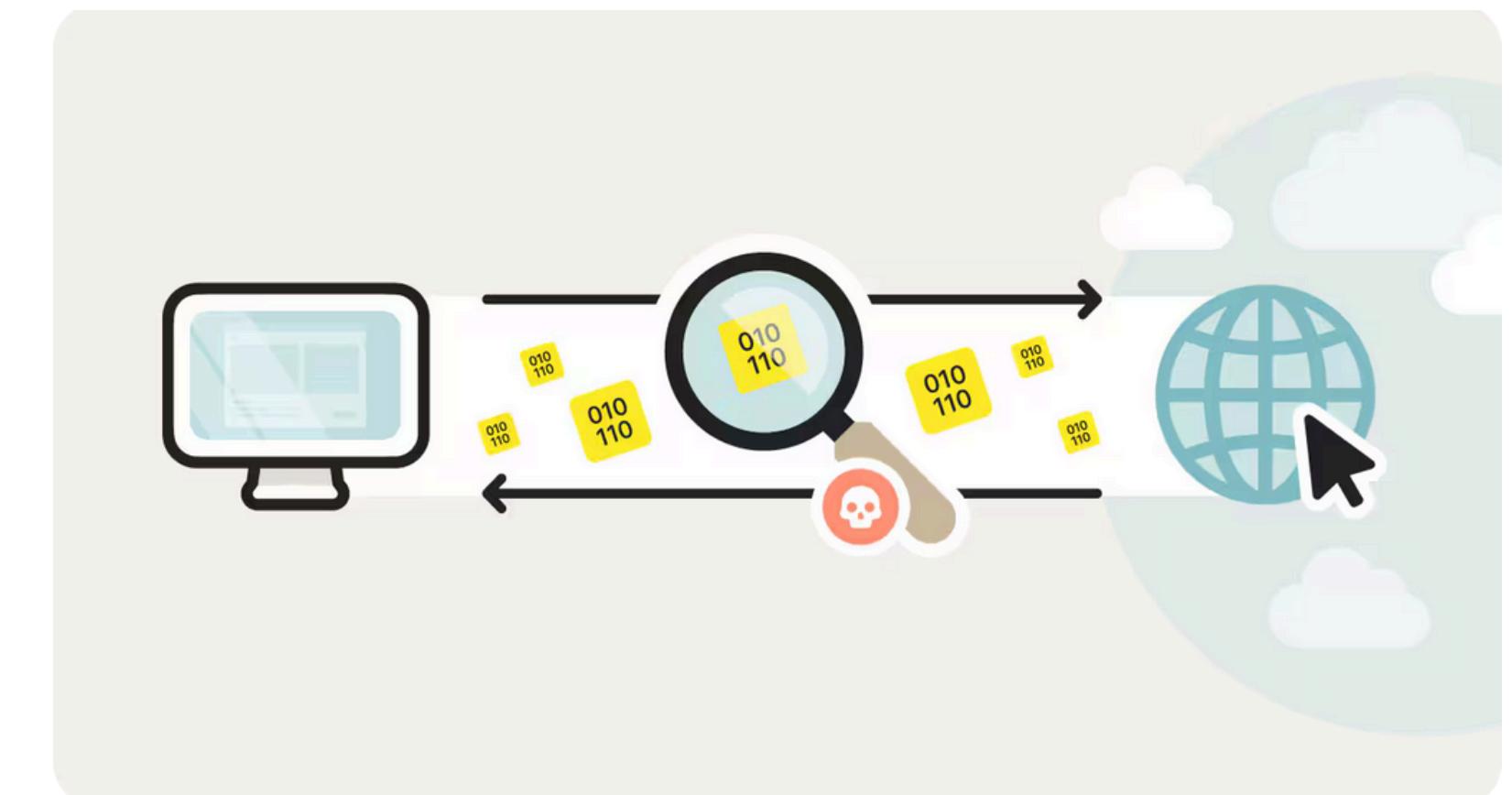
Grazie!



**tcpdump
&
Wireshark**

Packet Sniffing

Il packet sniffing è l'atto di **intercettare** e **analizzare** i pacchetti di dati in una rete, spesso con software chiamato "sniffer", per ottenere informazioni sul traffico di rete.



Packet Sniffer

1 tcpcdump

2 Wireshark



Tcpdump	Wireshark
Interfaccia a riga di comando	Interfaccia grafica
Fornisce solo un'analisi semplice di tipi di traffico come le query DNS	Analizza e decodifica i payload dati se identificate le chiavi di crittografia, riconosce payload dati da trasferimenti di file come smtp, http, ecc.
Interfacce convenzionali basate sul sistema	Interfacce di rete avanzate
Utilizzato per filtri semplici	Adatto per filtri complessi
Meno efficiente nella decodifica rispetto a Wireshark	Decodifica dei pacchetti basata su protocollo

tcpdump

```
root@giulio-CAINE:/home/giulio (as superuser)
File Edit View Search Terminal Help
root@giulio-CAINE:/home/giulio# tcpdump -i enp0s3
tcpdump: verbose output suppressed, use -v[v]... for full protocol decode
listening on enp0s3, link-type EN10MB (Ethernet), snapshot length 262144 bytes
08:21:59.958624 IP giulio-CAINE.35017 > 151.97.242.91.domain: 18072+ [1au] A? detectportal.firefox.com. (53)
08:21:59.958719 IP giulio-CAINE.60745 > 151.97.242.91.domain: 30600+ [1au] AAAA? detectportal.firefox.com. (53)
08:21:59.963505 IP 151.97.242.91.domain > giulio-CAINE.60745: 30600 3/0/1 CNAME detectportal.prod.mozaws.net., CNAME prod.detectportal.prod.cloudops.mozgcp.net., AAAA 2600:1901:0:38d7:: (176)
08:21:59.963505 IP 151.97.242.91.domain > giulio-CAINE.35017: 18072 3/0/1 CNAME detectportal.prod.mozaws.net., CNAME prod.detectportal.prod.cloudops.mozgcp.net., A 34.107.221.82 (164)
08:21:59.985279 IP giulio-CAINE.55452 > 151.97.242.91.domain: 43682+ [1au] PTR? 91.242.97.151.in-addr.arpa. (55)
08:21:59.988232 IP 151.97.242.91.domain > giulio-CAINE.55452: 43682 NXDomain 0/1/1 (113)
08:21:59.988304 IP giulio-CAINE.55452 > 151.97.242.91.domain: 43682+ PTR? 91.242.97.151.in-addr.arpa. (44)
08:21:59.990747 IP 151.97.242.91.domain > giulio-CAINE.55452: 43682 NXDomain 0/1/0 (102)
08:21:59.992061 IP giulio-CAINE.56779 > 151.97.242.91.domain: 27715+ [1au] PTR? 15.2.0.10.in-addr.arpa. (51)
08:21:59.995402 IP 151.97.242.91.domain > giulio-CAINE.56779: 27715 NXDomain 0/1
```

1

Scansione dei pacchetti dall'interfaccia **enp0s3**
tcpdump -i enp0s3

```
root@giulio-CAINE:/home/giulio (as superuser)
File Edit View Search Terminal Help
0 packets dropped by kernel
root@giulio-CAINE:/home/giulio# tcpdump -i enp0s3 port 80 or port 443
tcpdump: verbose output suppressed, use -v[v]... for full protocol decode
listening on enp0s3, link-type EN10MB (Ethernet), snapshot length 262144 bytes
08:30:49.356583 IP giulio-CAINE.47552 > mil04s24-in-f36.1e100.net.https: Flags [S], seq 2171002054, win 64240, options [mss 1460,sackOK,TS val 3367260142 ecr 0, nop,wscale 7], length 0
08:30:49.379155 IP mil04s24-in-f36.1e100.net.https > giulio-CAINE.47552: Flags [S.], seq 76800001, ack 2171002055, win 65535, options [mss 1460], length 0
08:30:49.379248 IP giulio-CAINE.47552 > mil04s24-in-f36.1e100.net.https: Flags [.], ack 1, win 64240, length 0
08:30:49.380563 IP giulio-CAINE.47552 > mil04s24-in-f36.1e100.net.https: Flags [P.], seq 1:1233, ack 1, win 64240, length 1232
08:30:49.380769 IP giulio-CAINE.47552 > mil04s24-in-f36.1e100.net.https: Flags [P.], seq 1233:1239, ack 1, win 64240, length 6
08:30:49.380789 IP giulio-CAINE.47552 > mil04s24-in-f36.1e100.net.https: Flags [P.], seq 1239:1409, ack 1, win 64240, length 170
08:30:49.381097 IP mil04s24-in-f36.1e100.net.https > giulio-CAINE.47552: Flags [.], ack 1233, win 65535, length 0
08:30:49.381097 IP mil04s24-in-f36.1e100.net.https > giulio-CAINE.47552: Flags [.], ack 1239, win 65535, length 0
08:30:49.381097 IP mil04s24-in-f36.1e100.net.https > giulio-CAINE.47552: Flags [.], ack 1409, win 65535, length 0
08:30:49.419638 IP mil04s24-in-f36.1e100.net.https > giulio-CAINE.47552: Flags [
```

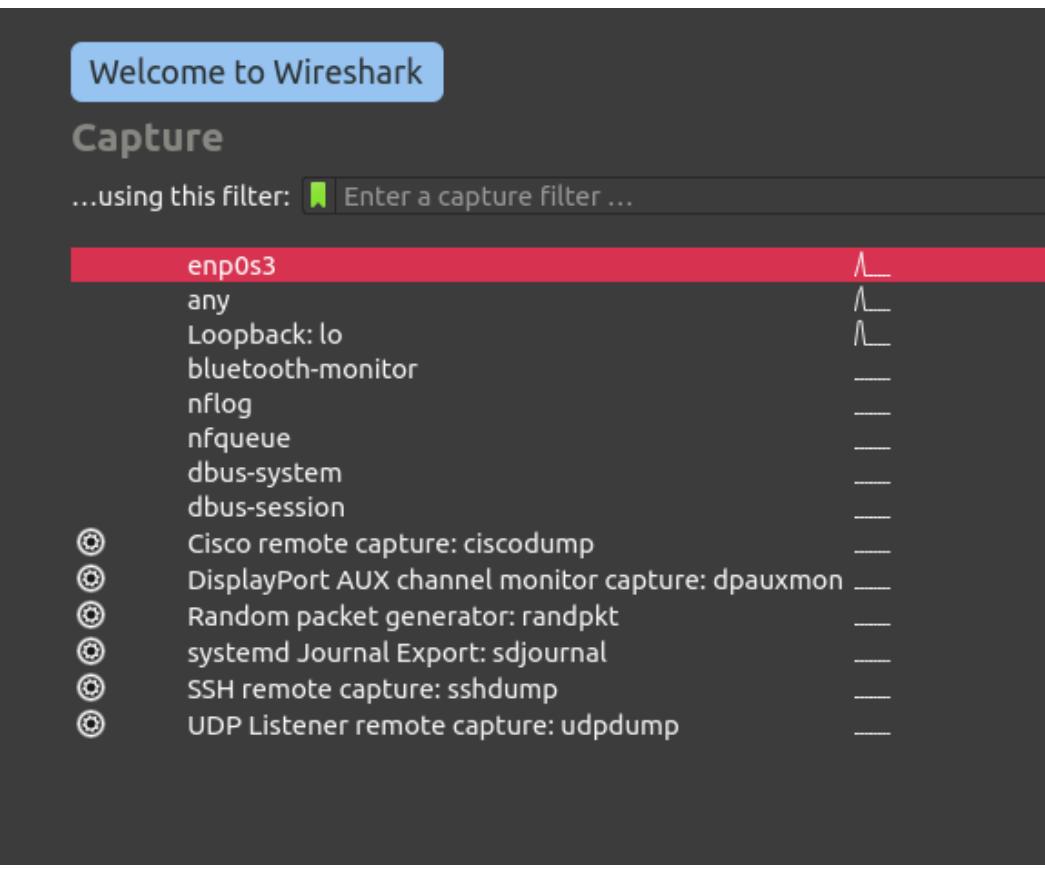
2

Scansione dei pacchetti **HTTP o HTTPS**
tcpdump -i enp0s3 port 80 or port 443

tcpdump: Filtri aggiuntivi

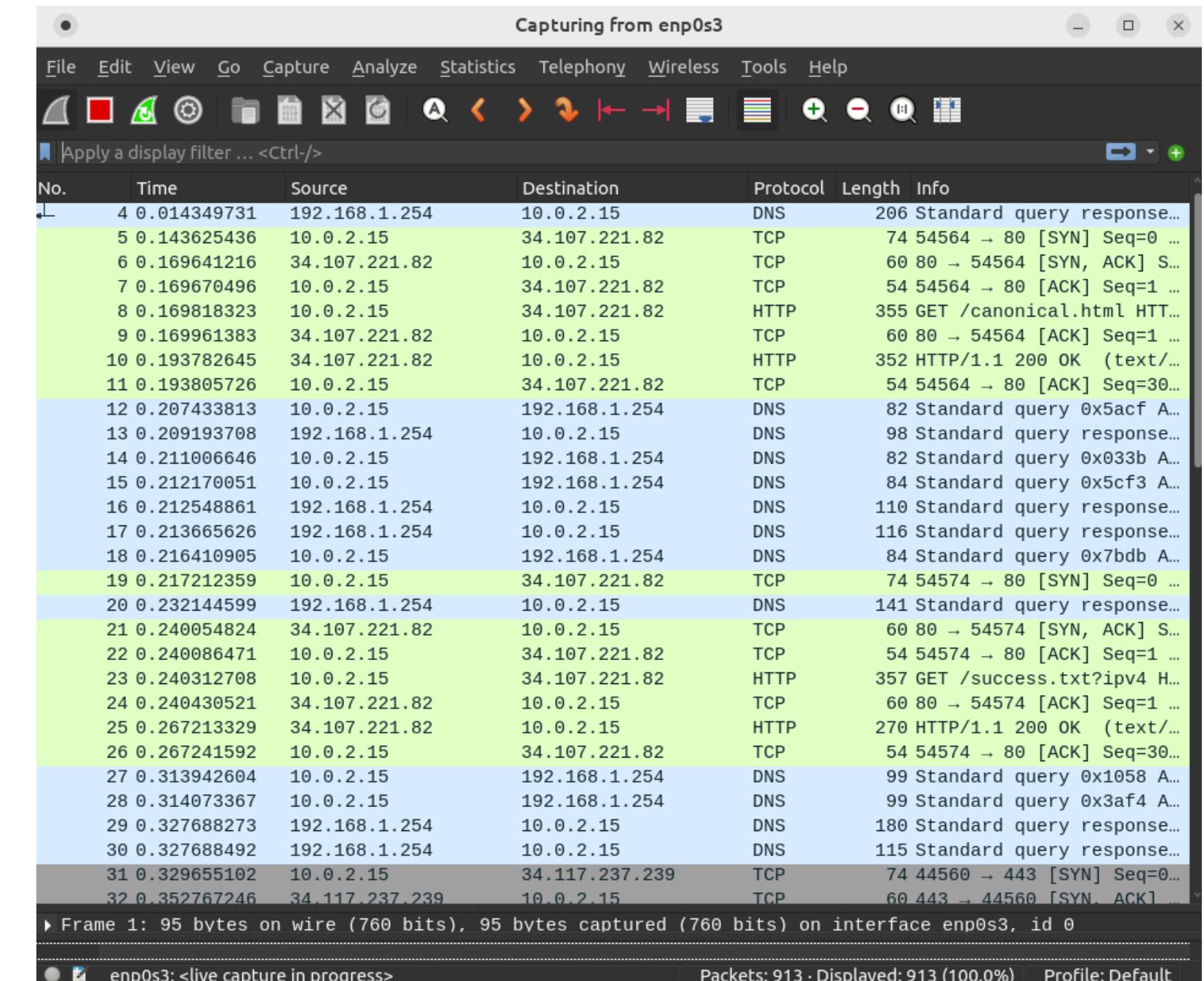
- 1 Scansione dei pacchetti **IPv6** ad esclusione di quelli **ICMP6**:
tcpdump -i enp0s3 ip6 and not icmp6
- 2 Scansione dei pacchetti provenienti dall'IP address **192.168.1.100**:
tcpdump -i enp0s3 host 192.168.1.100
- 3 Scansione dei pacchetti **HTTP** e visualizzazione **ASCII** del **contenuto**:
tcpdump -i enp0s3 port 80 -X

Wireshark



1

Selezioniamo la scheda di rete **enp0s3**



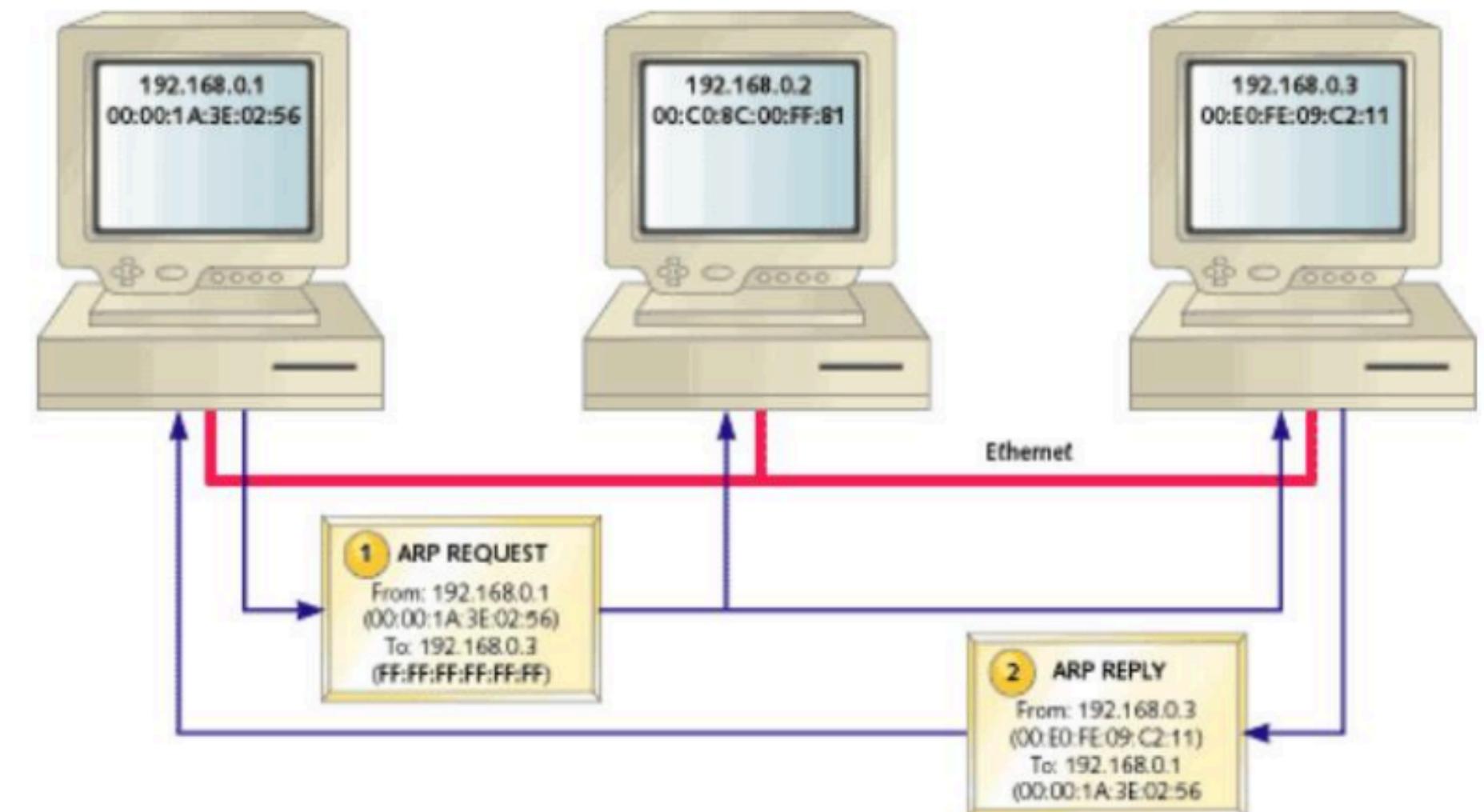
2

Iniziamo la scansione e l'analisi dei **pacchetti**

Address Resolution Protocol

ARP è un protocollo utilizzato nelle reti informatiche per mappare gli indirizzi IP (Internet Protocol) agli indirizzi fisici (MAC address) dei dispositivi di rete.

ARP aiuta i dispositivi a trovare l'indirizzo MAC di un altro dispositivo nella stessa rete quando conoscono solo il suo indirizzo IP.



ARP Request

No.	Time	Source	Destination	Protocol	Length	Info
1	0.0000000000	Dell_if:af:3f	Broadcast	ARP	42	Who has 192.168.10.102? Tell 192.168.10.100
2	0.001074383	PcsCompu_cd:05:65	Dell_if:af:3f	ARP	60	192.168.10.102 is at 08:00:27:cd:05:65
3	0.001083418	192.168.10.100	192.168.10.102	TCP	74	52934 → 80 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 SACK_PERM=1 T...
4	0.001767226	192.168.10.102	192.168.10.100	TCP	74	80 → 52934 [SYN, ACK] Seq=0 Ack=1 Win=65160 Len=0 MSS=1460 SA...
5	0.001796525	192.168.10.100	192.168.10.102	TCP	66	52934 → 80 [ACK] Seq=1 Ack=1 Win=64256 Len=0 TSval=1594247221...
6	0.001975373	192.168.10.100	192.168.10.102	HTTP	417	GET /bluemonkey4n6.html HTTP/1.1
7	0.002504172	192.168.10.102	192.168.10.100	TCP	66	80 → 52934 [ACK] Seq=1 Ack=352 Win=64896 Len=0 TSval=11938045...
8	0.002913826	192.168.10.102	192.168.10.100	HTTP	781	HTTP/1.1 200 OK (text/html)
9	0.002926559	192.168.10.100	192.168.10.102	TCP	66	52934 → 80 [ACK] Seq=352 Ack=716 Win=64128 Len=0 TSval=159424...
10	0.002926559	192.168.10.100	192.168.10.102	HTTP	271	GET /favicon.ico HTTP/1.1

Address Resolution Protocol (request)
Hardware type: Ethernet (1)
Protocol type: IPv4 (0x0800)
Hardware size: 6
Protocol size: 4

Sender MAC address: Dell_if:af:3f (84:7b:eb:1f:af:3f)
Sender IP address: 192.168.10.100
Target MAC address: 00:00:00:00:00:00 (00:00:00:00:00:00)
Target IP address: 192.168.10.102

0000	ff ff ff ff ff 84 7b eb 1f af 3f 08 06 00 01{ . . . ? . . . }
0010	08 00 06 04 00 01 84 7b eb 1f af 3f c0 a8 0a 64{ . . . ? . . . d
0020	00 00 00 00 00 00 c0 a8 0a 66 f

ARP Reply

No.	Time	Source	Destination	Protocol	Length	Info
1	0.000000000	Dell_1f:af:3f	Broadcast	ARP	42	Who has 192.168.10.102? Tell 192.168.10.100
2	0.001074383	PcsCompu_cd:05:65	Dell_1f:af:3f	ARP	60	192.168.10.102 is at 08:00:27:cd:05:65
3	0.001083418	192.168.10.100	192.168.10.102	TCP	74	52934 → 80 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 SACK_PERM=1 T...
4	0.001767226	192.168.10.102	192.168.10.100	TCP	74	80 → 52934 [SYN, ACK] Seq=0 Ack=1 Win=65160 Len=0 MSS=1460 SA...
5	0.001796525	192.168.10.100	192.168.10.102	TCP	66	52934 → 80 [ACK] Seq=1 Ack=1 Win=64256 Len=0 TSval=1594247221...
6	0.001975373	192.168.10.100	192.168.10.102	HTTP	417	GET /bluemonkey4n6.html HTTP/1.1
7	0.002504172	192.168.10.102	192.168.10.100	TCP	66	80 → 52934 [ACK] Seq=1 Ack=352 Win=64896 Len=0 TSval=11938045...
8	0.002913826	192.168.10.102	192.168.10.100	HTTP	781	HTTP/1.1 200 OK (text/html)
9	0.002926559	192.168.10.100	192.168.10.102	TCP	66	52934 → 80 [ACK] Seq=352 Ack=716 Win=64128 Len=0 TSval=159424...
10	0.074752891	192.168.10.100	192.168.10.102	HTTP	371	GET /favicon.ico HTTP/1.1

▼ Address Resolution Protocol (reply)

Hardware type: Ethernet (1)
Protocol type: IPv4 (0x0800)
Hardware size: 6
Protocol size: 4

Sender MAC address: PcsCompu_cd:05:65 (08:00:27:cd:05:65)
Sender IP address: 192.168.10.102
Target MAC address: Dell_1f:af:3f (84:7b:eb:1f:af:3f)
Target IP address: 192.168.10.100

0000	84	7b	eb	1f	af	3f	08	00	27	cd	05	65	08	06	00	01	· { . . . ? . . ' . . e . . .
0010	08	00	06	04	00	02	08	00	27	cd	05	65	c0	a8	0a	66	· ' . . e . . .
0020	84	7b	eb	1f	af	3f	c0	a8	0a	64	00	00	00	00	00	00	· { . . . ? . . ' . . d . . .
0030	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	·

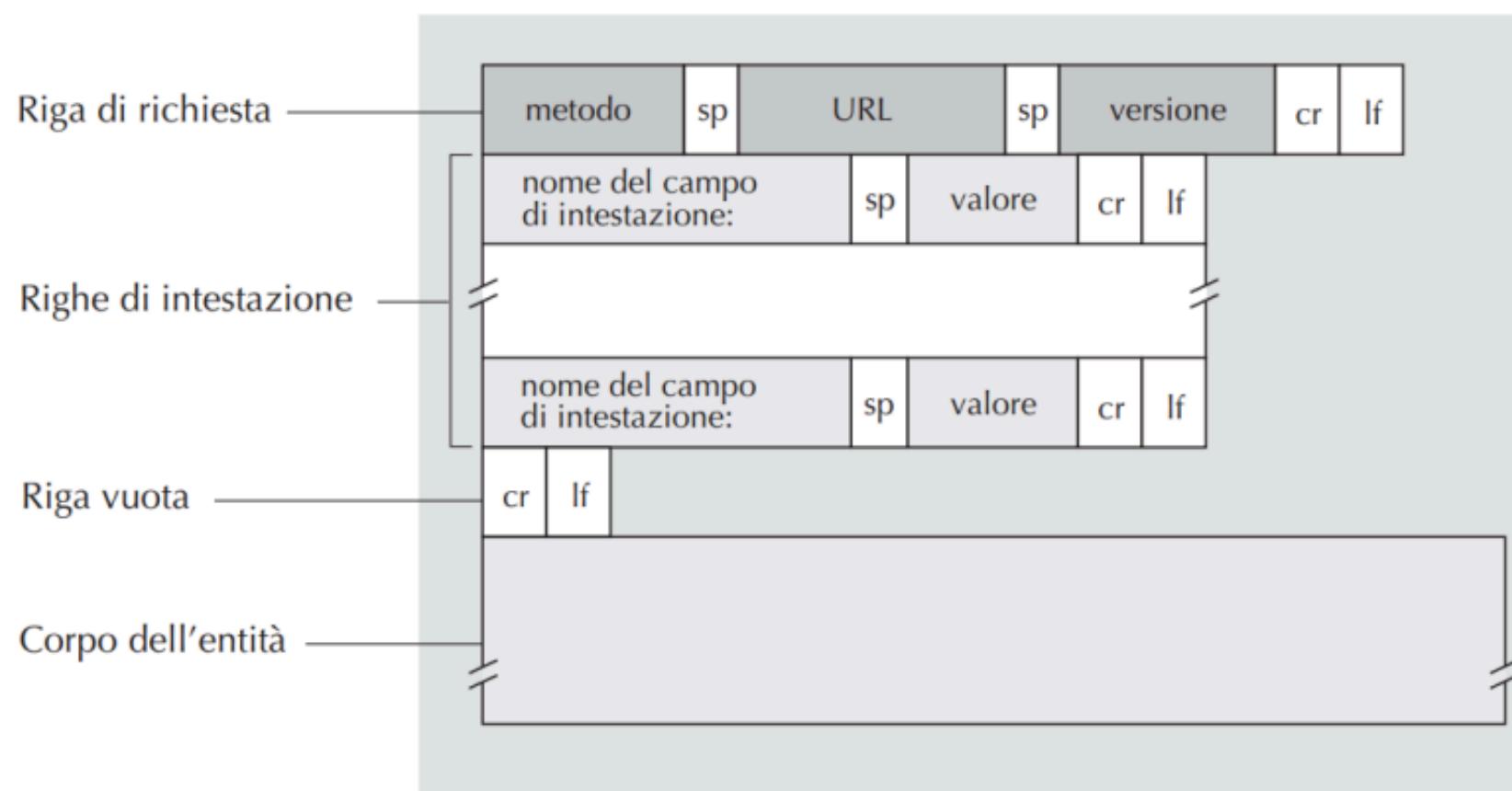
HyperText Transfer Protocol

HTTP è il protocollo di comunicazione utilizzato per trasferire dati su Internet.

È responsabile della trasmissione di pagine web, immagini, video e altri contenuti da un server web a un browser, consentendo agli utenti di accedere e visualizzare informazioni online.

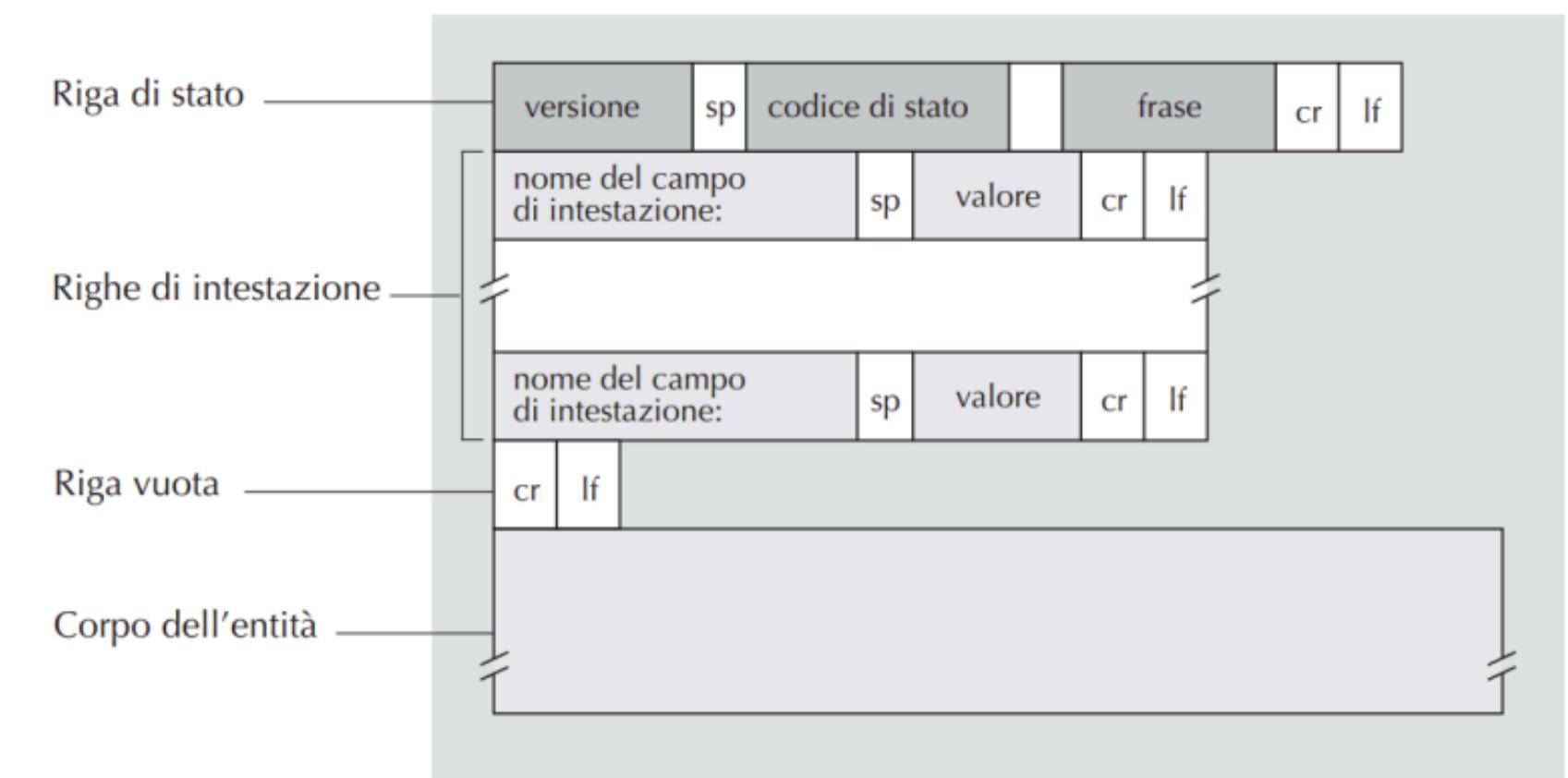


HTTP Request & Response



1

Messaggio di Richiesta HTTP



2

Messaggio di Risposta HTTP

HTTP Request

Wireshark - Packet 22 · enp0s3

► Frame 22: 415 bytes on wire (3320 bits), 415 bytes captured (3320 bits) on interface enp0s3, id 0

► Ethernet II, Src: PcsCompu_df:e0:54 (08:00:27:df:e0:54), Dst: RealtekU_12:35:02 (52:54:00:12:35:02)

► Internet Protocol Version 4, Src: 10.0.2.15, Dst: 168.119.8.211

► Transmission Control Protocol, Src Port: 59204, Dst Port: 80, Seq: 1, Ack: 1, Len: 361

▼ Hypertext Transfer Protocol

► GET / HTTP/1.1\r\n

Host: pediconegiulio.altervista.org\r\n

User-Agent: Mozilla/5.0 (X11; Ubuntu; Linux x86_64; rv:124.0) Gecko/20100101 Firefox/124.0\r\n

Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,*/*;q=0.8\r\n

Accept-Language: en-US,en;q=0.5\r\n

Accept-Encoding: gzip, deflate\r\n

Connection: keep-alive\r\n

Upgrade-Insecure-Requests: 1\r\n

\r\n

Hex	Dec	Text
0030	fa f0 be dc 00 00 47 45	GET / HTTP
0040	54 20 2f 20 48 54 54 50	/1.1 Host: pedi
0050	2f 31 2e 31 0d 0a 48 6f	cone giul io.alter
0060	73 74 3a 20 70 65 64 69	vista.or g User-
0070	63 6f 6e 65 67 69 75 6c	Agent: Mozilla/5
0080	69 6f 2e 61 6c 74 65 72	.0 (X11; Ubuntu;
0090	76 69 73 74 61 2e 6f 72	Linux x 86_64; r
00a0	76 3a 31 32 34 2e 30 29	v:124.0) Gecko/2

?

Help

Close

HTTP Response

Wireshark - Packet 32 · enp0s3

► Frame 32: 74 bytes on wire (592 bits), 74 bytes captured (592 bits) on interface enp0s3, id 0
► Ethernet II, Src: RealtekU_12:35:02 (52:54:00:12:35:02), Dst: PcsCompu_df:e0:54 (08:00:27:df:e0:54)
► Internet Protocol Version 4, Src: 168.119.8.211, Dst: 10.0.2.15
► Transmission Control Protocol, Src Port: 80, Dst Port: 59204, Seq: 10130, Ack: 362, Len: 20
► [4 Reassembled TCP Segments (10149 bytes): #26(2920), #28(4380), #30(2829), #32(20)]
▼ Hypertext Transfer Protocol
► HTTP/1.1 200 OK\r\nDate: Fri, 12 Apr 2024 07:15:19 GMT\r\nServer: Apache\r\n[truncated]Link: <http://pediconegiulio.altervista.org/wp-json/>; rel="https://api.w.org/", <http://pedi
Vary: Accept-Encoding\r\nContent-Encoding: gzip\r\nKeep-Alive: timeout=1, max=100\r\nConnection: Keep-Alive\r\nTransfer-Encoding: chunked\r\nContent-Type: text/html; charset=UTF-8\r\n.
0000 08 00 27 df e0 54 52 54 00 12 35 02 08 00 45 00 .T.RT .5 .E.
0010 00 3c 4c de 00 00 40 06 70 85 a8 77 08 d3 0a 00 .<L .@. p .w .
0020 02 0f 00 50 e7 44 10 97 39 93 56 02 9d b4 50 18 .P.D .9 .V .P .
0030 ff ff 1a 5d 00 00 61 0d 0a 03 00 59 3e d9 47 f8 .].a .Y> .G .
0040 9c 00 00 0d 0a 30 0d 0a 0d 0a .0 .

Sniffing di dati inviati tramite form HTML

Wireshark

Sniffing dei dati

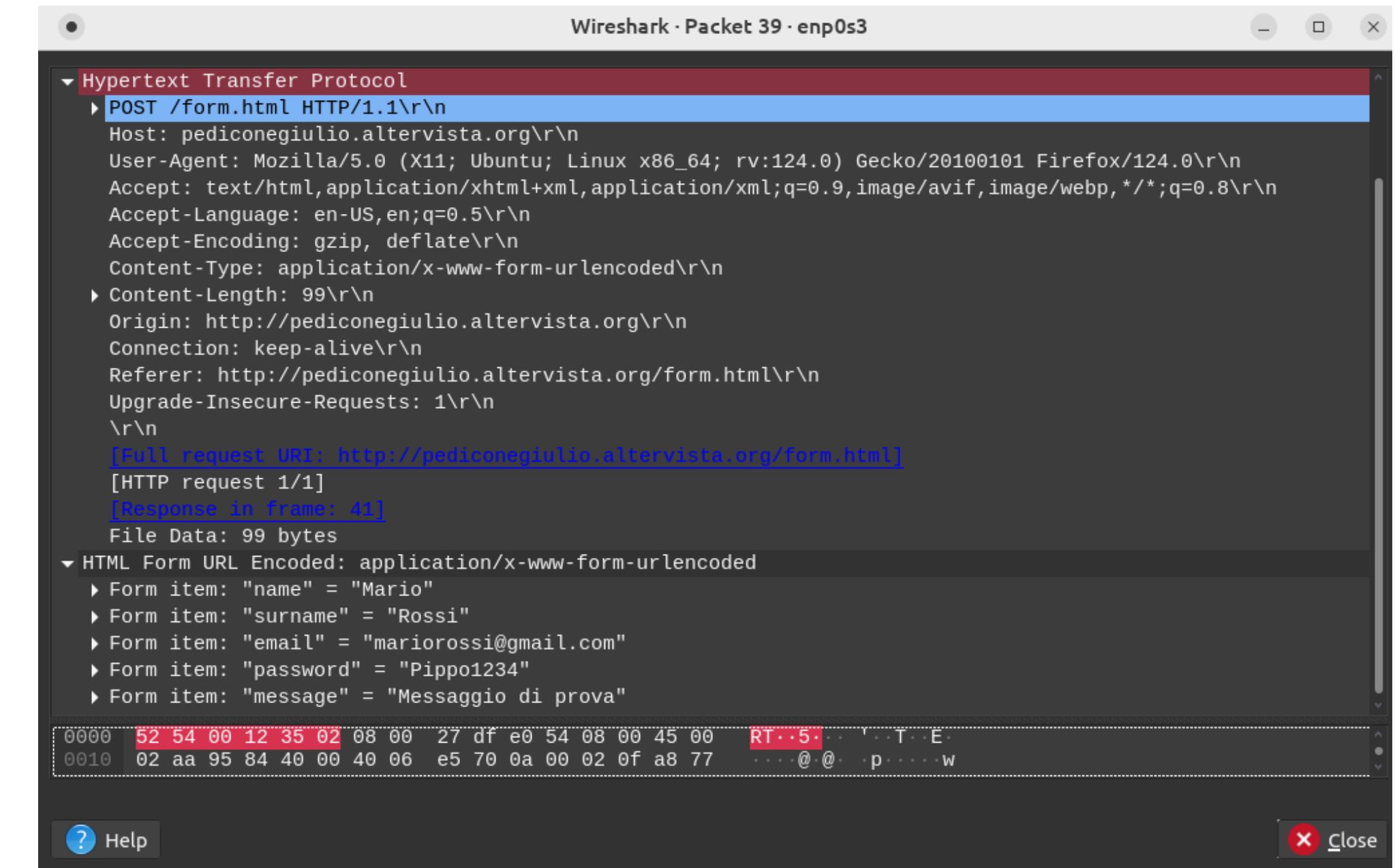
Nome:

Cognome:

Email:

Password:

Message:



1 Form HTML con method POST

2 Contenuto del pacchetto catturato da Wireshark

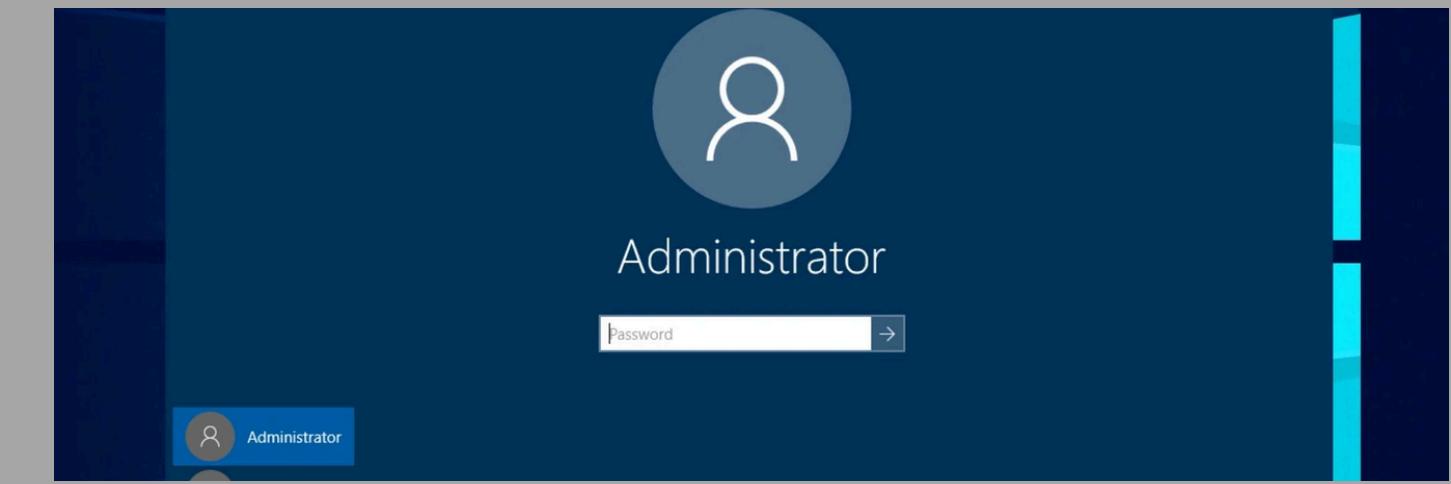


chntpw

chntpw

Rimuovi la password di Windows

E' un tool che ci permette di rimuovere la password sul Sistema Operativo Windows con una serie di passaggi dopo aver richiamato il comando chntpw



Potremmo aver bisogno del PIN per accedere al profilo dell'utente del laptop

POSSIBILE CASO REALE

Dopo aver sequestrato gli effetti personali di un possibile indagato di un reato, contenenti informazioni utili per l'indagine sull'evento



Quello che ci servirà



Sistema Operativo
Linux Caine

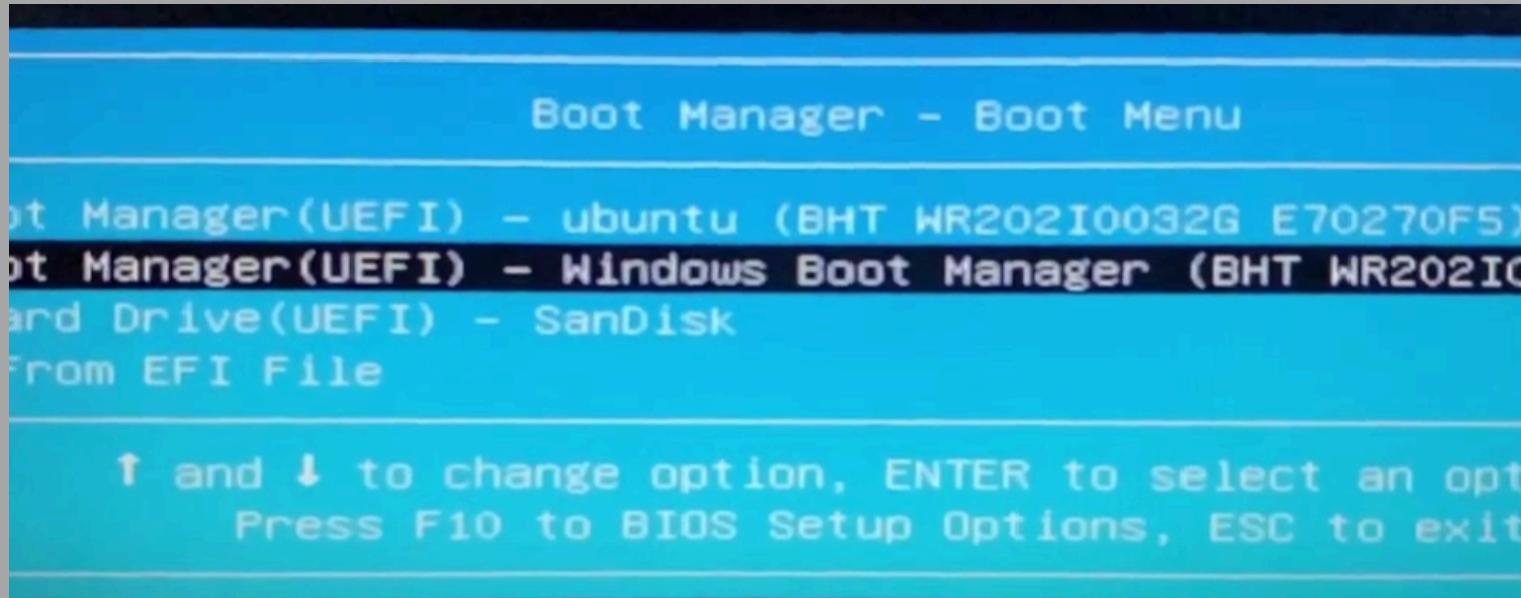


Chiavetta USB con
eseguibile CAINE

PASSAGGI - chntpw (1)

1) Inseriamo la chiavetta USB nel PC

2) Dal Boot Loader , facciamo partire CAINE



3) Dopo aver digitato il comando “lsblk”, individuiamo la partizione del SO Windows

```
caine@caine:~$ lsblk
NAME  MAJ:MIN RM  SIZE RO TYPE MOUNTPOINT
loop0  7:0    0  3,8G  1 loop /rofs
sda   8:0    0 150G  1 disk
└─sda1 8:1    0 148,7G 1 part
  └─sda2 8:2    0  527M 1 part
  └─sda3 8:3    0  842M 1 part
sdb   8:16   0 250G  1 disk
└─sdb1 8:17   0 128M 1 part
  └─sdb2 8:18   0 249,9G 1 part
sr0   11:0   1  3,9G  1 rom  /cdrom
caine@caine:~$
```

Windows System partition

```
caine@caine:~$ sudo blockdev --report
RO  RA  SSZ  BSZ  StartSec          Size  Device
ro  256  512  1024      0  4023779328  /dev/loop0
ro  256  512  4096      0  161061273600  /dev/sda
ro  256  512  4096     2048  159622782976  /dev/sda1
ro  256  512  4096  311767040      552599552  /dev/sda2
ro  256  512  4096  312848384      882900992  /dev/sda3
ro  256  2048 2048      0  4137680896  /dev/sr0
ro  256  512  4096      0  268435456000  /dev/sdb
ro  256  512  4096      34  134217728  /dev/sdb1
ro  256  512  4096  264192  268299141120  /dev/sdb2
caine@caine:~$ sudo blockdev --setrw /dev/sda*
caine@caine:~$ sudo blockdev --report
RO  RA  SSZ  BSZ  StartSec          Size  Device
ro  256  512  1024      0  4023779328  /dev/loop0
rw  256  512  4096      0  161061273600  /dev/sda
rw  256  512  4096     2048  159622782976  /dev/sda1
rw  256  512  4096  311767040      552599552  /dev/sda2
rw  256  512  4096  312848384      882900992  /dev/sda3
ro  256  2048 2048      0  4137680896  /dev/sr0
ro  256  512  4096      0  268435456000  /dev/sdb
ro  256  512  4096      34  134217728  /dev/sdb1
```

PASSAGGI - chntpw (2)

DIGITAL FORENSICS
A.A 2023/24

4) Montiamo nella chiavetta USB il file System Windows

```
caine@caine:~$  
caine@caine:~$ sudo mount /dev/sda1 /mnt/usb  
caine@caine:~$ cd /mnt/usb/Windows/System32/config/  
caine@caine:/mnt/usb/Windows/System32/config$ ls -l SAM*  
-rwxrwxrwx 1 root root 131072 gen 7 2022 SAM  
-rwxrwxrwx 1 root root 65536 dic 7 2019 SAM.LOG1  
-rwxrwxrwx 1 root root 81920 dic 7 2019 SAM.LOG2
```

Il file SAM (Security Accounts Manager) su Windows è un componente critico che memorizza le informazioni sugli account degli utenti, inclusi nomi utente e password hash. Il file SAM non è direttamente accessibile dall'utente

5) Eseguiamo il comando "chntpw -i SAM"

```
caine@caine:/mnt/usb/Windows/System32/config$ chntpw -i SAM  
chntpw version 1.00 140201, (c) Petter N Hagen  
Hive <SAM> name (from header): <\SystemRoot\System32\Config\SAM>  
ROOT KEY at offset: 0x001020 * Subkey indexing type is: 686c <lh>  
File size 131072 [20000] bytes, containing 10 pages (+ 1 headerpage)  
Used for data: 319/63336 blocks/bytes, unused: 10/18264 blocks/bytes.
```

```
<=====> chntpw Main Interactive Menu <=====>
```

```
Loaded hives: <SAM>
```

```
1 - Edit user data and passwords  
2 - List groups  
- - -  
9 - Registry editor, now with full write support!  
q - Quit (you will be asked if there is something to save)
```

```
What to do? [1] ->
```

Comandi chntpw

-i: Interfaccia interattiva che guida attraverso il processo di modifica della password.

-l: Elenco le informazioni sugli account utente nel file SAM. " chntpw -l SAM "

-u: Specifica un nome utente per il quale si desidera modificare la password " chntpw -u username SAM "

-d : Abilita o disabilita un account utente. " chntpw -d username SAM "

-e: Modifica le proprietà avanzate di un account utente. "chntpw -e username SAM"



PASSAGGI - chntpw (3)

6) Digitiamo 1 per modificare i dati utente e password ed il suo RID

```
Loaded hives: <SAM>

1 - Edit user data and passwords
2 - List groups
...
9 - Registry editor, now with full write support!
q - Quit (you will be asked if there is something to save)

What to do? [1] -> 1

===== chntpw Edit User Info & Passwords =====

RID - ----- Username ----- Admin? |- Lock? --|
01f4 | Administrator           | ADMIN   | dis/lock |
03eb | BlueMonkey4n6          | ADMIN   | dis/lock |
01f7 | DefaultAccount          | ADMIN   | dis/lock |
03ea | FOR585                 | ADMIN   | dis/lock |
01f5 | Guest                   |         | dis/lock |
01f8 | WDAGUtilityAccount      |         | dis/lock |

Please enter user number (RID) or 0 to exit: [3ea] 3eb
```

8) Usciamo e salviamo

```
What to do? [1] -> q

Hives that have changed:
#  Name
0  <SAM>

Write hive files? (y/n) [n] : y
0  <SAM> - OK
```

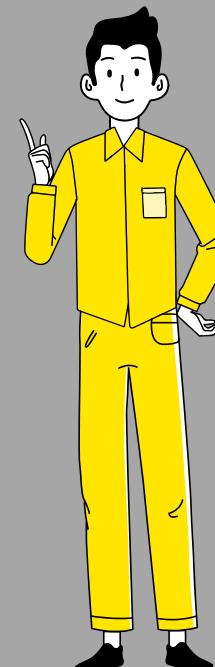
```
caine@caine:/mnt/usb/Windows/System32/config$ cd
caine@caine:~$ sudo umount /mnt/usb
caine@caine:~$ shutdown -
```

7) Digitiamo 1 per "pulire" la password

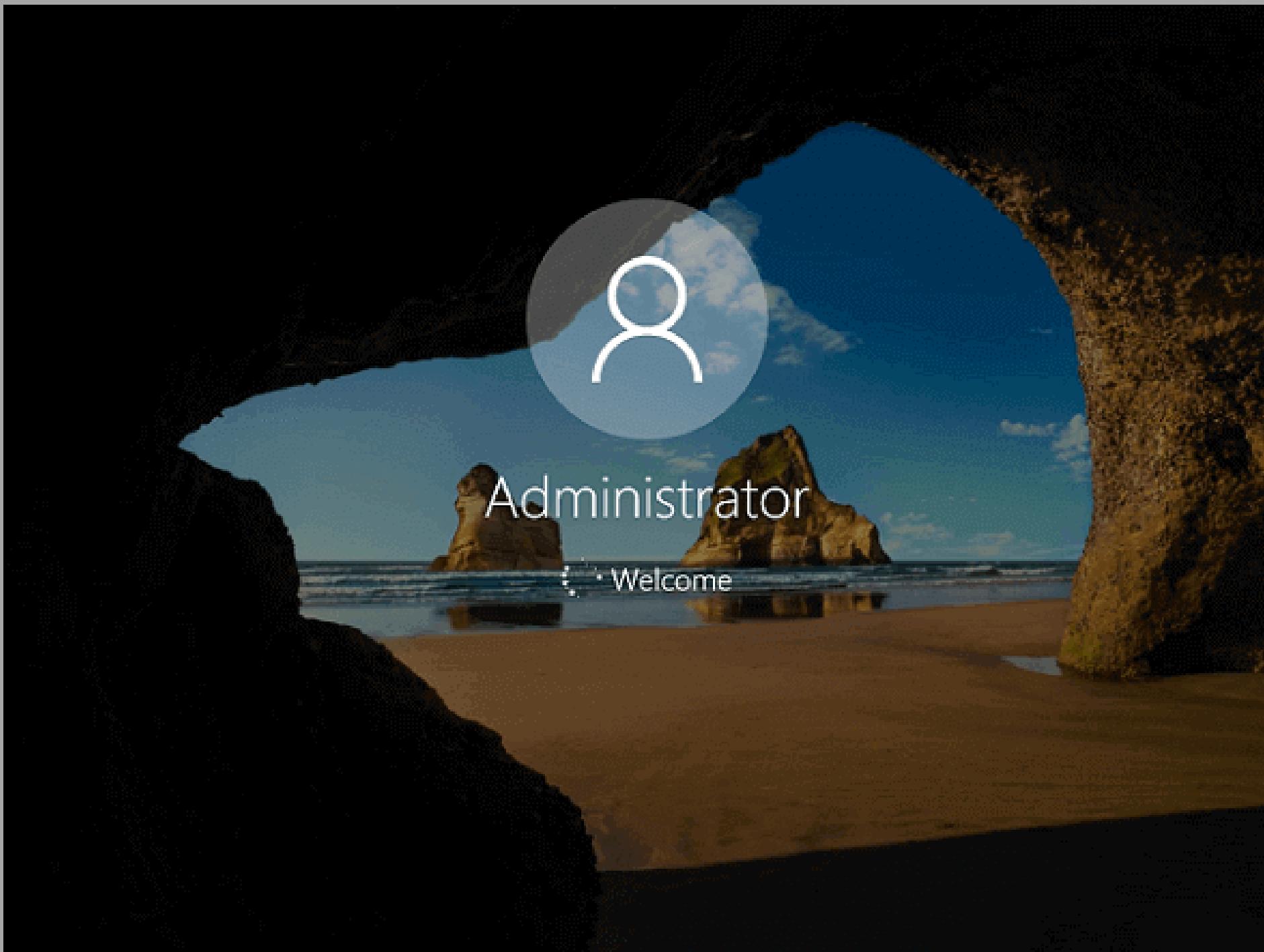
```
----- User Edit Menu:
1 - Clear (blank) user password
2 - Unlock and enable user account [probably locked now]
3 - Promote user (make user an administrator)
4 - Add user to a group
5 - Remove user from a group
q - Quit editing user, back to user select

Select: [q] > 1
```

9)Scolleghiamo la chiavetta ed Avviamo Windows



chntpw (finale)



Come per magia il Sistema Operativo Windows si avvierà normalmente come se non avesse nessun PIN o Password .

Alcune versioni di Windows richiedono la creazione di una nuova password

