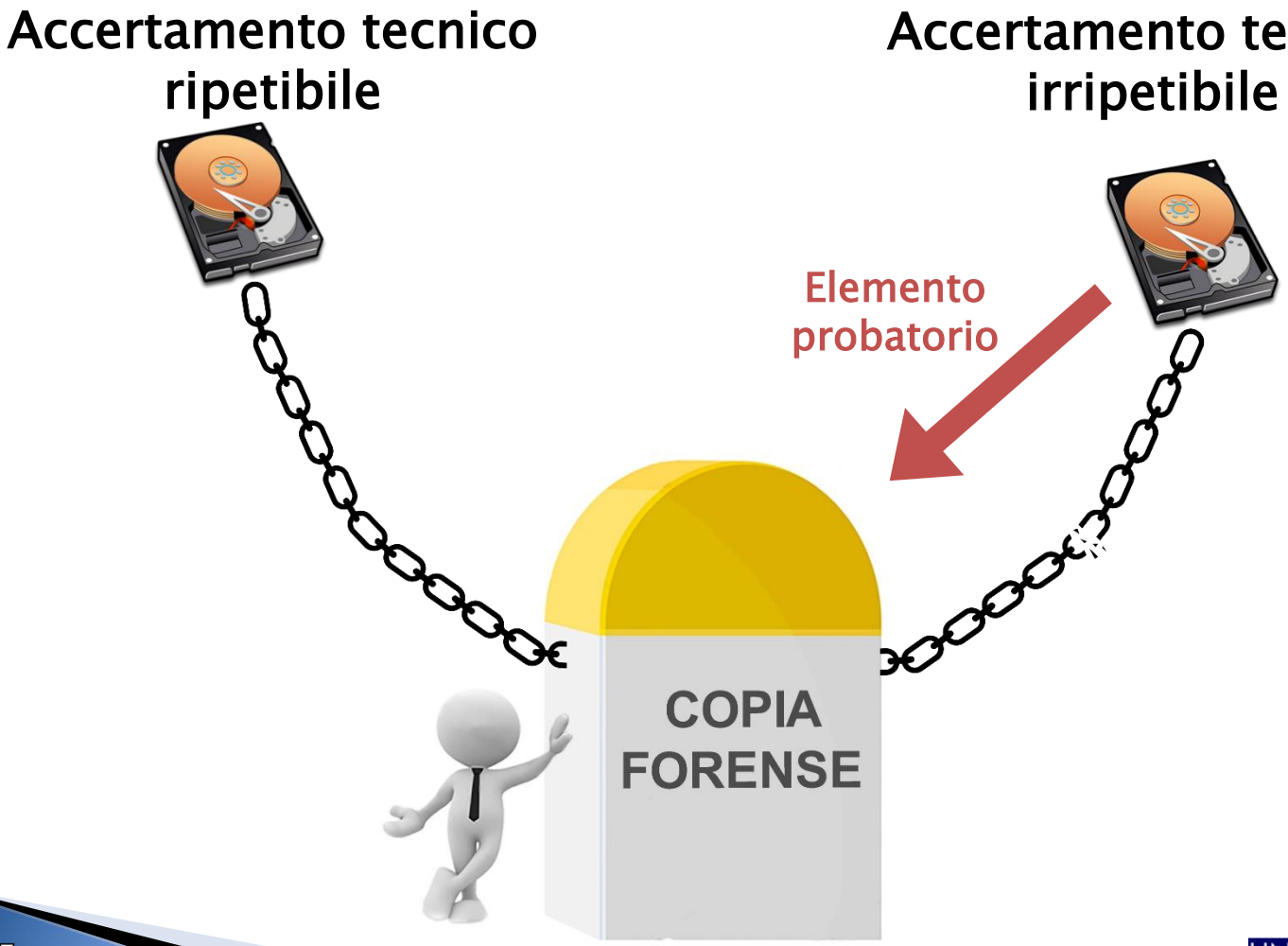
COMPUTER FORENSICS

Lezione 12: L'Analisi
gli strumenti
(1ª parte)

A.A. 2021/22
Dott. Lorenzo LAURATO

Nelle puntate precedenti…



Fasi

- Identificazione
- Raccolta
- Validazione
- Preservazione
- **Analisi**
- Interpretazione
- Documentazione
- Presentazione

L'analisi

- Va eseguita su una copia
- Riproducibilità
- Stesso risultato ottenibile da diverse operazioni/strumenti di analisi
- Ricostruzione di eventi passati mediante la lettura di dati digitali

L'analisi

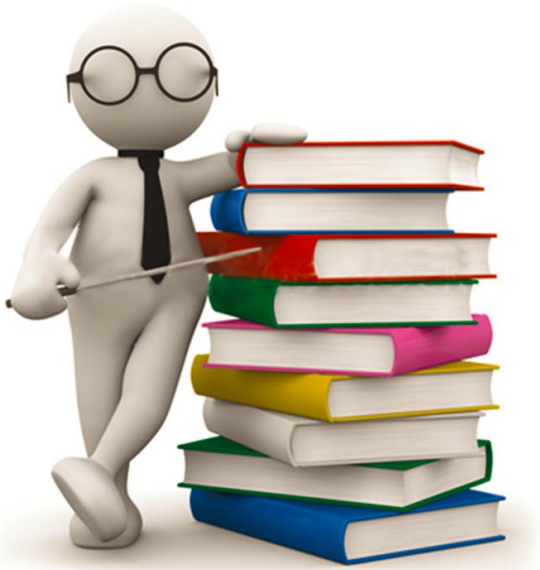
Riscontro delle informazioni

Nuove informazioni

Contro-analisi

L'analisi

- Il primo strumento di analisi è il proprio bagaglio di conoscenze informatiche.



L'Analisi

- montare un file immagine

L'Analisi

montare un file immagine: linux

- Analizziamo il file immagine

```
root@caine:/# fdisk -l /mnt/dest/dd_image/sda.dd

Disk /mnt/dest/dd_image/sda.dd: 4 GiB, 4294967296 bytes, 8388608 sectors
Units: sectors of 1 * 512 = 512 bytes
Sector size (logical/physical): 512 bytes / 512 bytes
I/O size (minimum/optimal): 512 bytes / 512 bytes
Disklabel type: dos
Disk identifier: 0x72a3c36c

Device                          Boot   Start     End Sectors Size Id Type
/mnt/dest/dd_image/sda.ddp1             2048 2099199 2097152   1G  b W95 FAT32
/mnt/dest/dd_image/sda.ddp2          2099200 8388607 6289408   3G  b W95 FAT32
```

Il file immagine rappresenta una memoria con due partizioni: **p1** e **p2**

L'Analisi

montare un file immagine: linux

- montiamo la partizione p2

```
Device                          Boot    Start      End  Sectors Size  Id Type
/mnt/dest/dd_image/sda.ddp1             2048  2099199  2097152   1G  b  W95 FAT32
/mnt/dest/dd_image/sda.ddp2          2099200  8388607  6289408   3G  b  W95 FAT32
```

```
root@caine:/# mount -o ro,loop,offset=1074790400 /mnt/dest/dd_image/sda.dd /mnt/sda_dd
```

- **ro**: read-only
- **loop**: crea un *virtual block device* da un file (*character device*)
- **offset**=*byte*: punto di inizio della partizione da montare (*2099200 • 512*)

Solo immagini DD/RAW non segmentate

L'Analisi

montare un file immagine: linux

- merge immagine segmentata DD\RAW (**AFFLIBv3**)

```
root@caine:/# ls -l /mnt/dest/dd_image/
total 4194308
-rwxrwxrwx 1 root root 2147483648 apr  8 01:16 sda.000
-rwxrwxrwx 1 root root 2147483648 apr  8 01:23 sda.001
-rwxrwxrwx 1 root root        823 apr  8 01:23 sda.log
```

```
root@caine:/# affuse /mnt/dest/dd_image/sda.000 /mnt/sda_fuse
root@caine:/# ls -l /mnt/sda_fuse/
total 0
-r--r--r-- 1 root root 4294967296 gen  1 1970 sda.000.raw

root@caine:/# fdisk -l /mnt/sda_fuse/sda.000.raw
Disk /mnt/sda_fuse/sda.000.raw: 4 GiB, 4294967296 bytes, 8388608 sectors
Units: sectors of 1 * 512 = 512 bytes
Sector size (logical/physical): 512 bytes / 512 bytes
I/O size (minimum/optimal): 512 bytes / 512 bytes
Disklabel type: dos
Disk identifier: 0x72a3c36c
Device                        Boot   Start     End Sectors Size Id Type
/mnt/sda_fuse/sda.000.raw1            2048 2099199 2097152   1G  b W95 FAT32
/mnt/sda_fuse/sda.000.raw2         2099200 8388607 6289408   3G  b W95 FAT32
```

L'Analisi

montare un file immagine: linux

- merge immagine segmentata EWF (**libewf**)

```
root@caine:/# ls -l /mnt/dest/e01_image/
total 235526
-rw-r--r-- 1 root root 104857600 apr  8 02:26 sda.E01
-rw-r--r-- 1 root root 104857600 apr  8 02:28 sda.E02
-rw-r--r-- 1 root root  31457280 apr  8 02:29 sda.E03
-rw-r--r-- 1 root root      7161 apr  8 02:29 sda.info
```

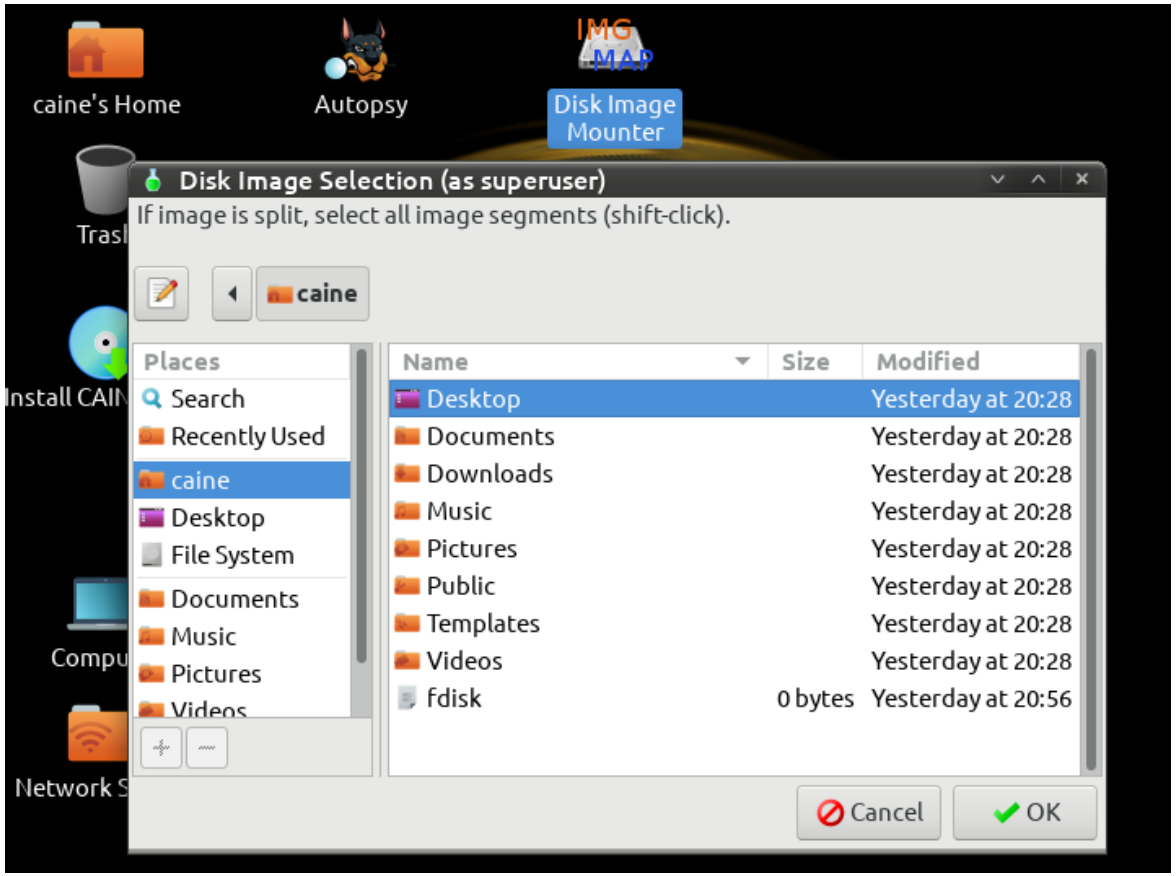
```
root@caine:/# ewfmount /mnt/dest/e01_image/sda.E01 /mnt/sda_fuse
root@caine:/# ls -l /mnt/sda_fuse/
total 0
-r--r--r-- 1 root root 4294967296 apr  8 02:31 ewf1

root@caine:/# fdisk -l /mnt/sda_fuse/ewf1
Disk /mnt/sda_fuse/ewf1: 4 GiB, 4294967296 bytes, 8388608 sectors
Units: sectors of 1 * 512 = 512 bytes
Sector size (logical/physical): 512 bytes / 512 bytes
I/O size (minimum/optimal): 512 bytes / 512 bytes
Disklabel type: dos
Disk identifier: 0x72a3c36c
Device                 Boot   Start     End Sectors Size Id Type
/mnt/sda_fuse/ewf1p1           2048 2099199 2097152   1G  b W95 FAT32
/mnt/sda_fuse/ewf1p2        2099200 8388607 6289408   3G  b W95 FAT32
```

L'Analisi

montare un file immagine: linux

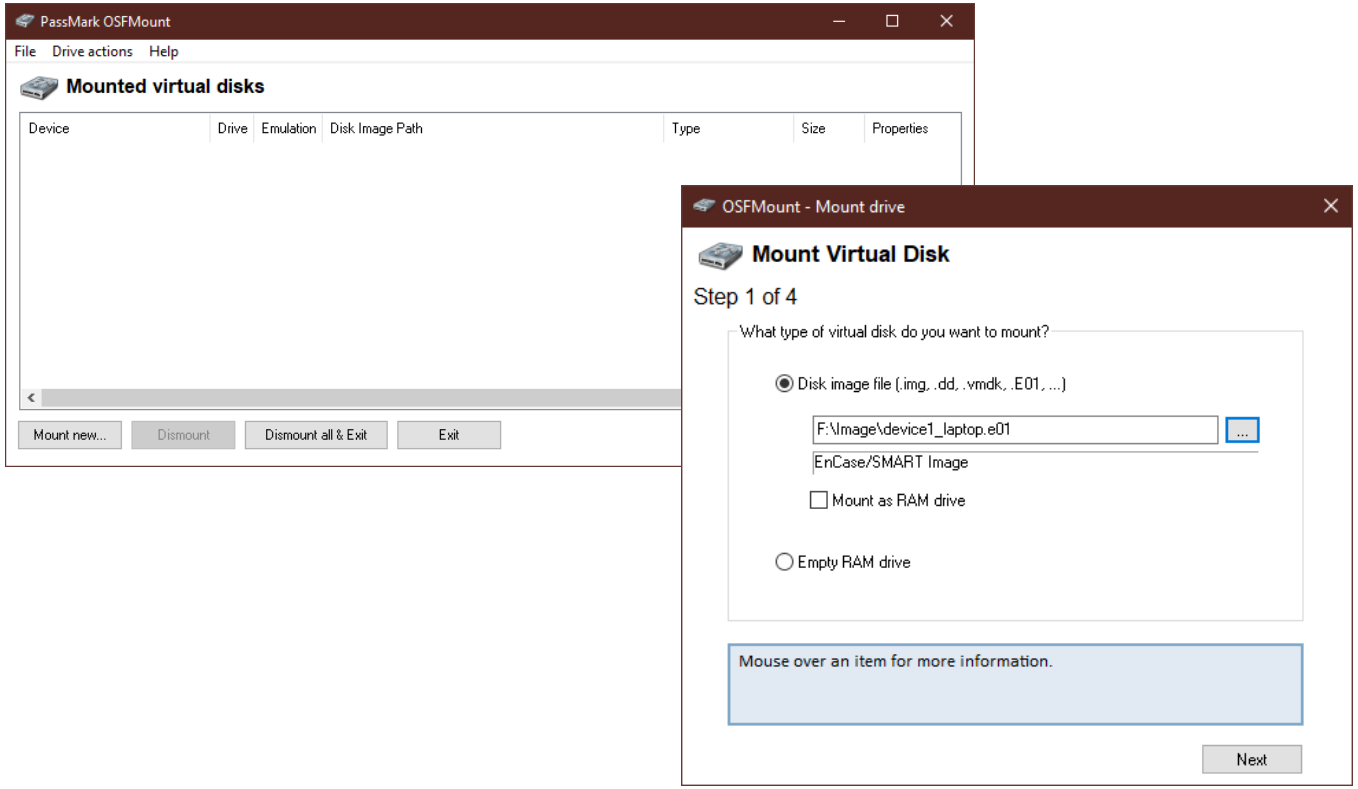
- tramite GUI: tool «**IMG_MAP**»



L'Analisi

montare un file immagine: windows

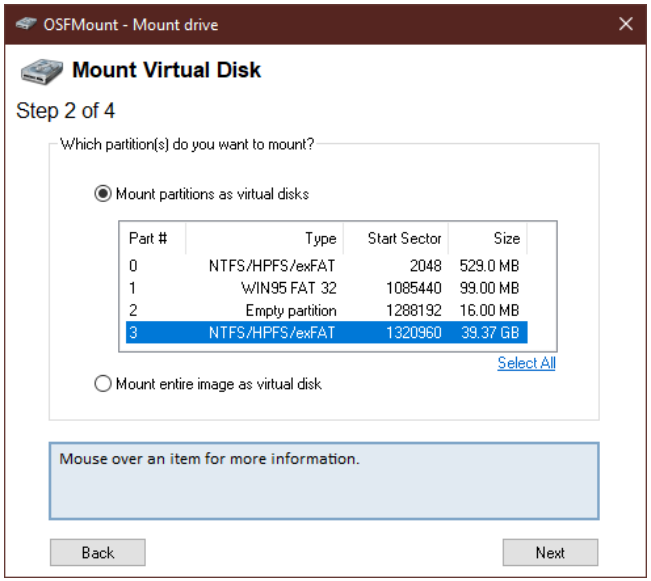
PassMark OFSMount

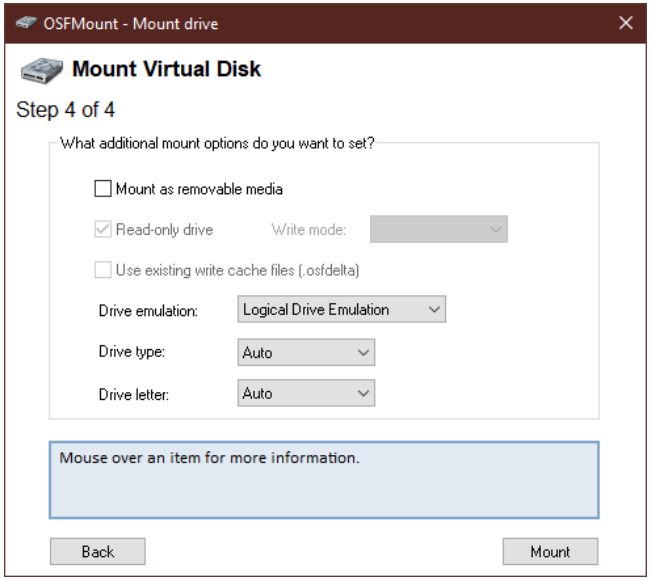


L'Analisi

montare un file immagine: windows

PassMark **OFSMount**

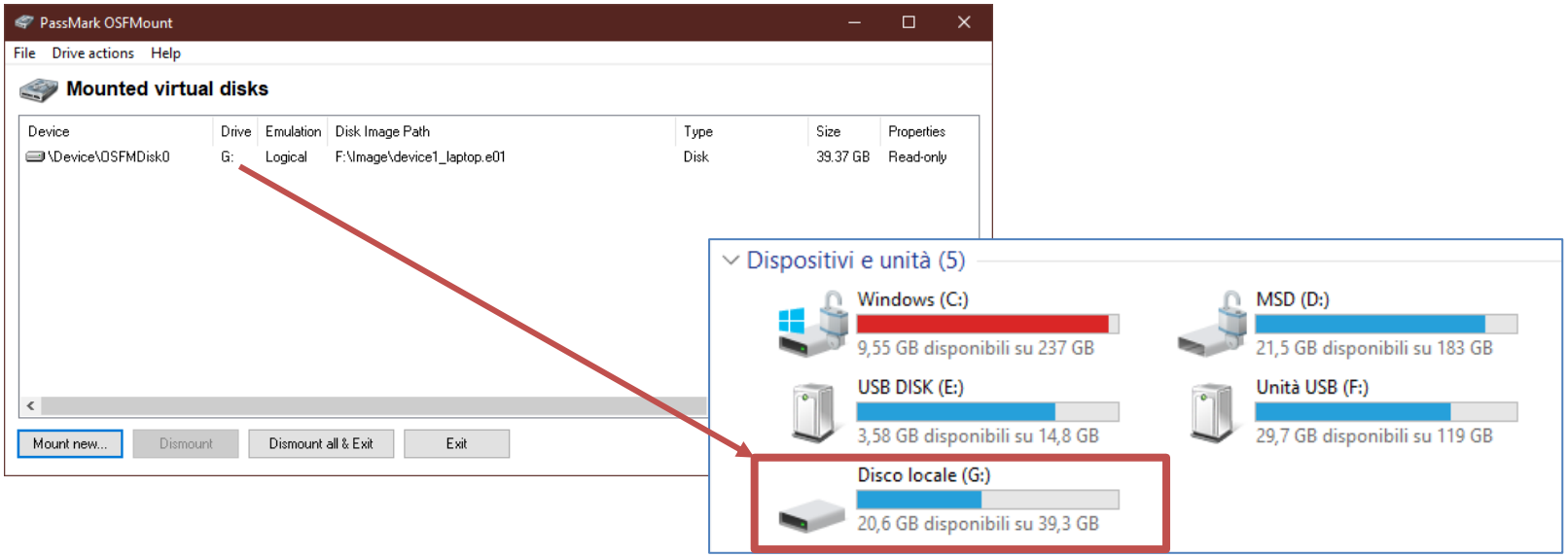




L'Analisi

montare un file immagine: windows

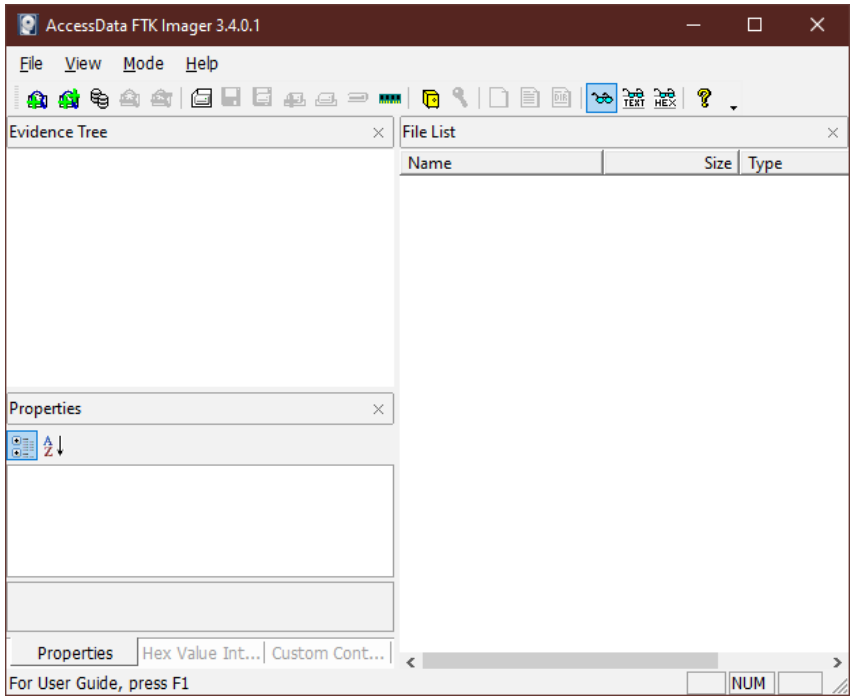
PassMark OFSMount

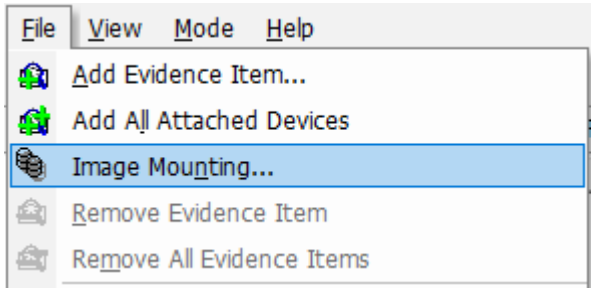


L'Analisi

montare un file immagine: windows

AccessData FTK Imager

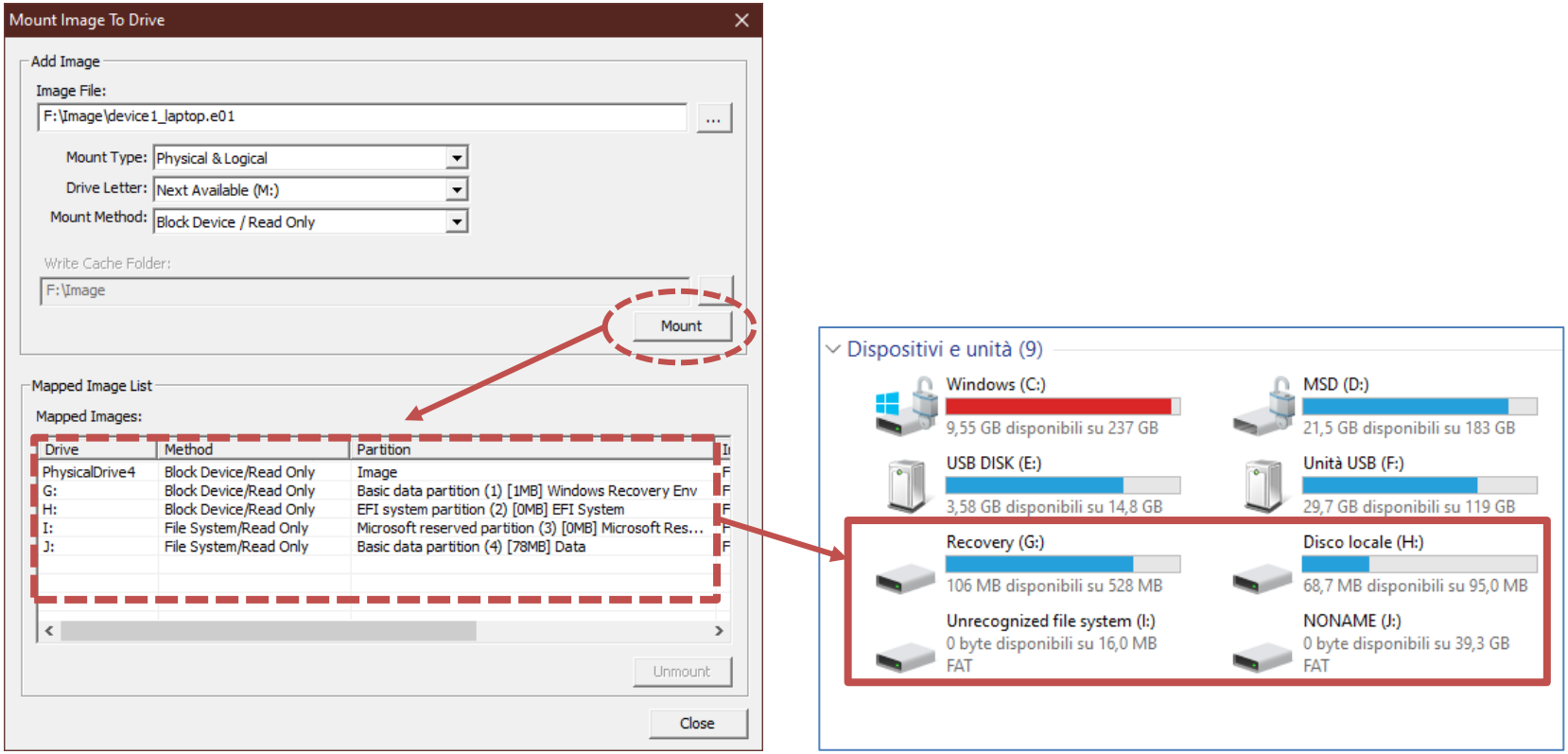




L'Analisi

montare un file immagine: windows

AccessData FTK Imager



L'Analisi

montare un file immagine

Pro

- veloce per operazioni semplici
- Utilizzo di tool non forensic oriented

Contro

- Farraginoso
- Solo file residenti
- Riconoscimento del FileSystem dell'immagine demandata al nostro S.O.

Solo per specifiche analisi

L'Analisi

- FTK Imager

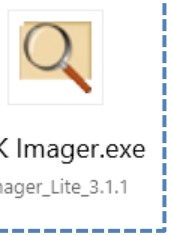
FTK Imager

Analisi copia forense

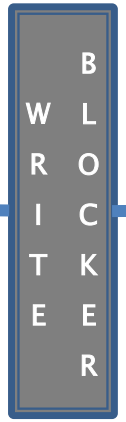
Preview
(Perquisizione)

LIVE

Dispositivo Target

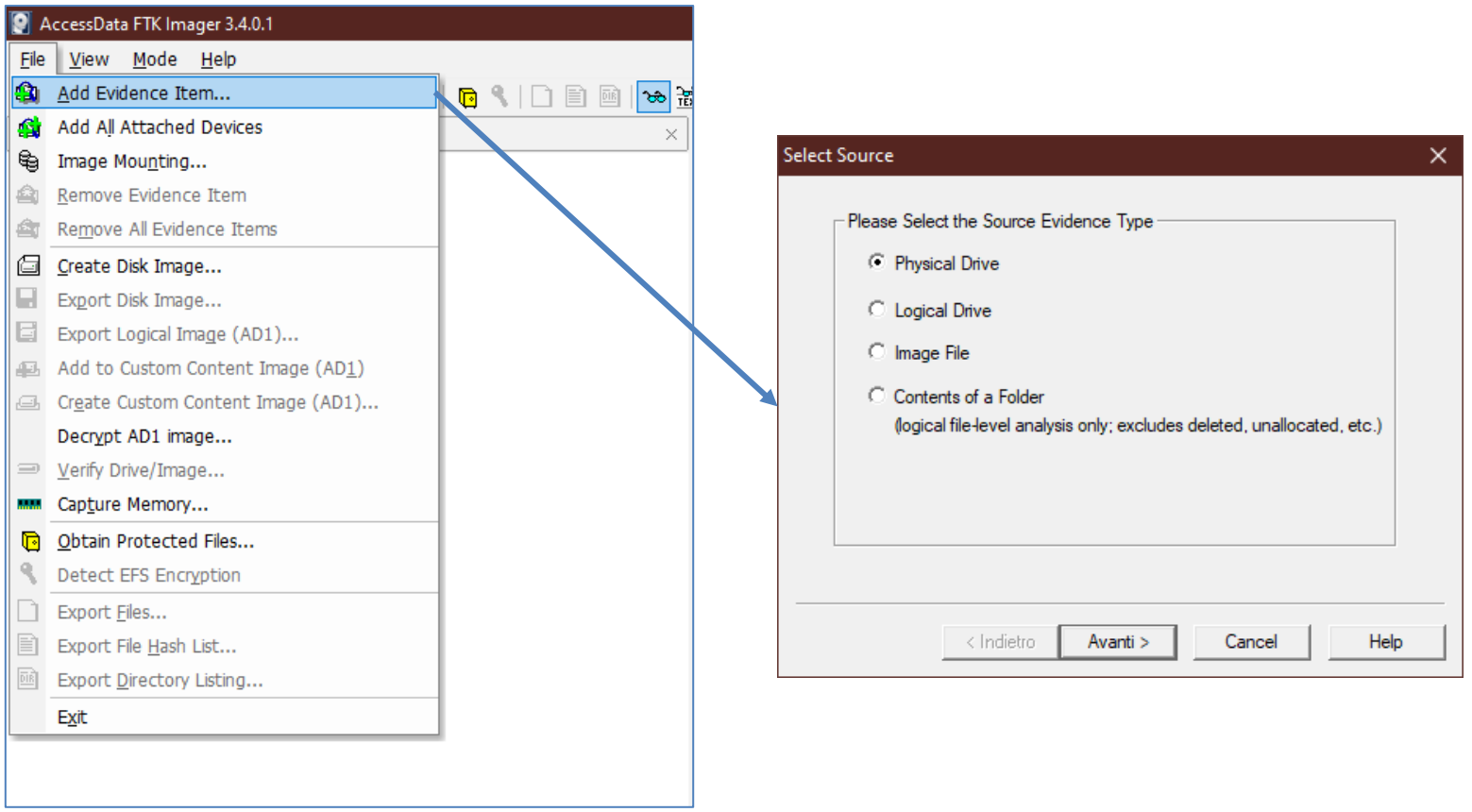


DEAD



Dispositivo Target

FTK Imager


AccessData FTK Imager 3.4.0.1
File
View
Mode
Help
Add Evidence Item...
Add All Attached Devices
Image Mounting...
Remove Evidence Item
Remove All Evidence Items
Create Disk Image...
Export Disk Image...
Export Logical Image (AD1)...
Add to Custom Content Image (AD1)
Create Custom Content Image (AD1)...
Decrypt AD1 image...
Verify Drive/Image...
Capture Memory...
Obtain Protected Files...
Detect EFS Encryption
Export Files...
Export File Hash List...
Export Directory Listing...
Exit
Select Source
Please Select the Source Evidence Type
Physical Drive
Logical Drive
Image File
Contents of a Folder
(logical file-level analysis only; excludes deleted, unallocated, etc.)
< Indietro
Avanti >
Cancel
Help

FTK Imager

Hard Disk Image Formats

The following table lists AccessData Imager-identified and analyzed hard disk image formats:

Identified and Analyzed Hard Disk Image Formats	
• Encase, including 6.12	• SnapBack
• Safeback 2.0 and under	• Expert Witness
• Linux DD	• ICS
• Ghost (forensic images only)	• SMART
• AccessData Logical Image (AD1)	• Advanced Forensics Format (AFF)

FTK Imager

CD and DVD Image Formats

The following table lists AccessData Imager-identified and analyzed CD and DVD image formats:

Identified and Analyzed CD and DVD File Systems and Formats	
• Alcohol (*.mds)	• IsoBuster CUE
• PlexTools (*.pxi)	• CloneCD (*.ccd)
• Nero (*.nrg)	• Roxio (*.cif)
• ISO	• Pinnacle (*.pdi)
• Virtual CD (*.vc4)	• CD-RW,
• VCD	• CD-ROM
• DVD+MRW	• DVCD
• DVD-RW	• DVD-VFR
• DVD+RW Dual Layer	• DVD-VR
• BD-R SRM-POW	• BD-R DL
• BD-R SRM	• CloneCD (*.ccd)
• HD DVD-R	• HD DVD-RW DL
• SVCD	• HD DVD

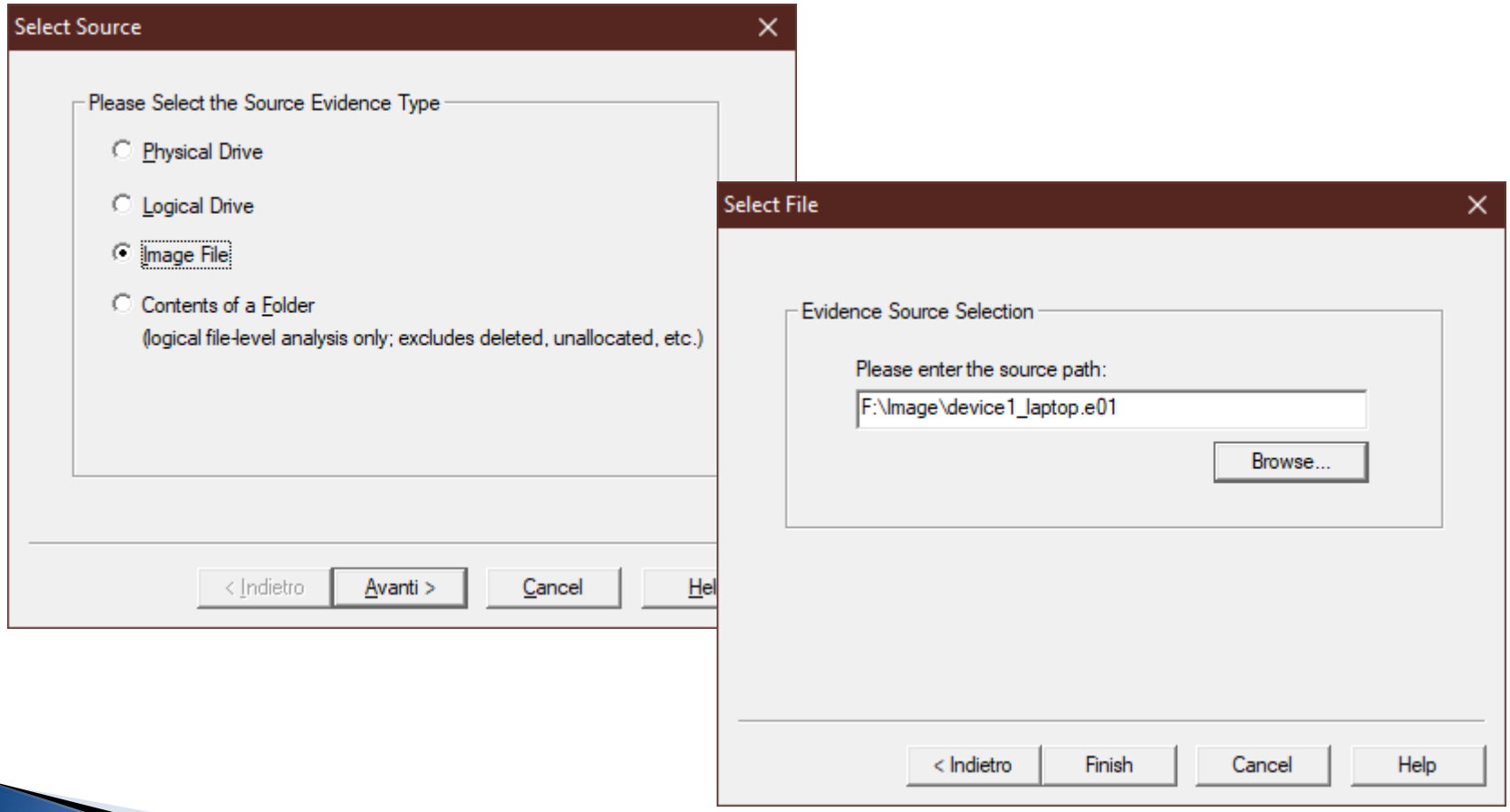
FTK Imager

File Systems

The following table lists AccessData Imager-identified and analyzed file systems:

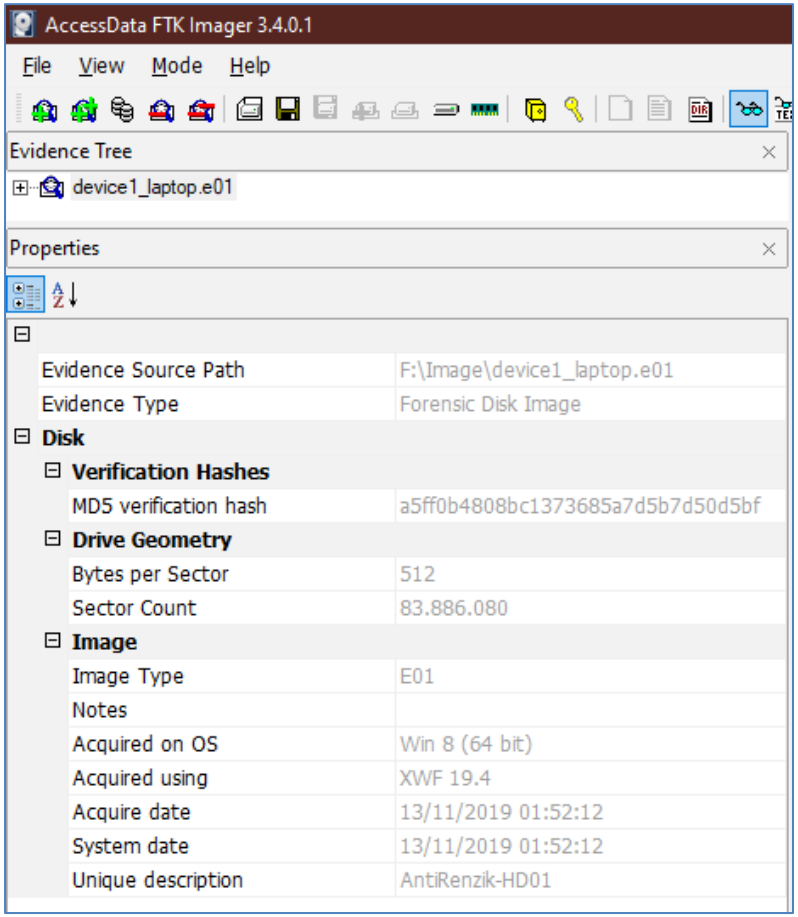
Identified and Analyzed File Systems	
• APFS	• HFS
• CDFS	• HFS+
• exFAT	• NTFS
• Ext2FS	• ReiserFS3
• Ext3FS	• VXFS
• Ext4FS	• XFS
• FAT12, FAT16, FAT32	

FTK Imager:
analisi file immagine



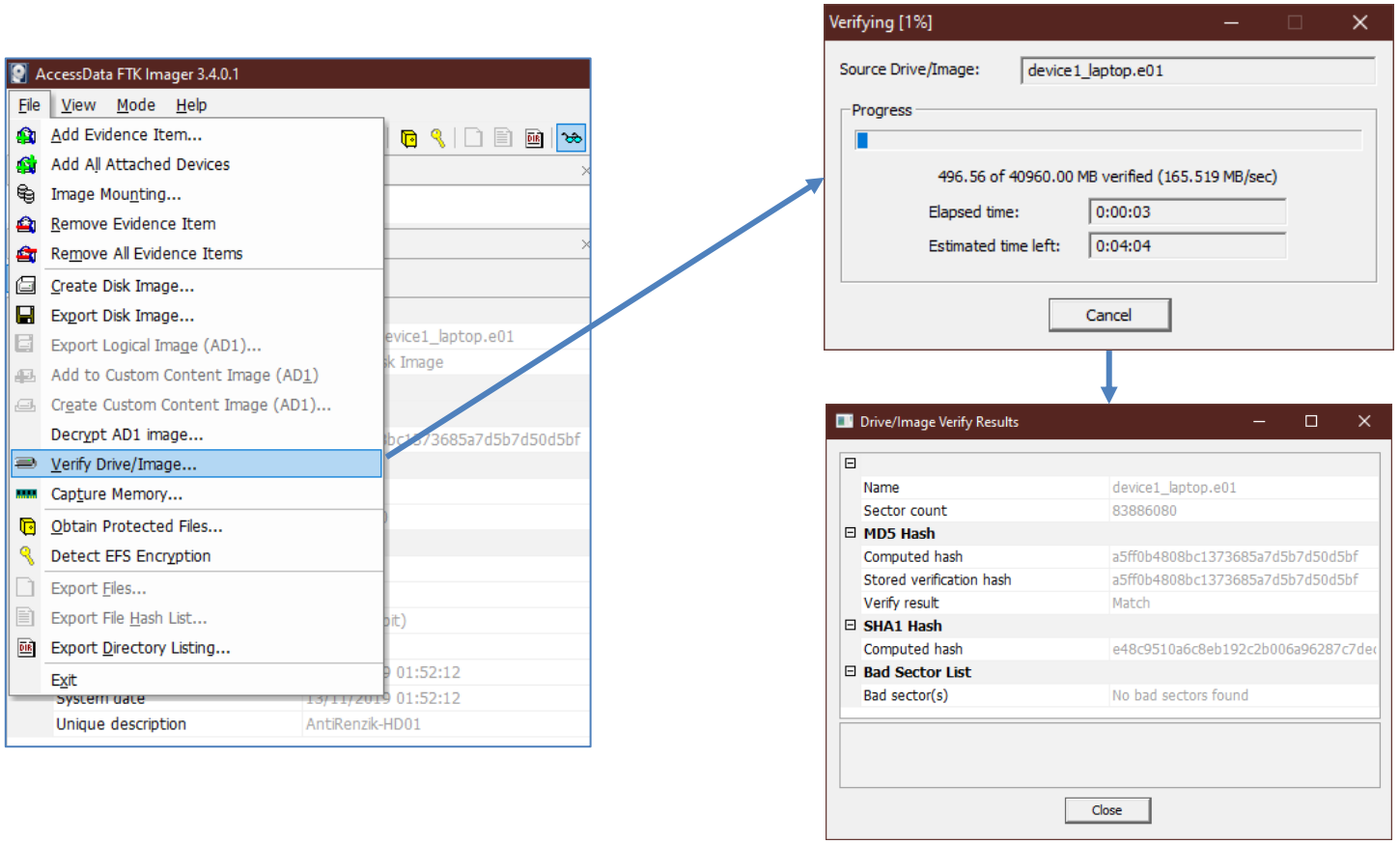
FTK Imager:

analisi file immagine: header info



FTK Imager:

analisi file immagine: verifica



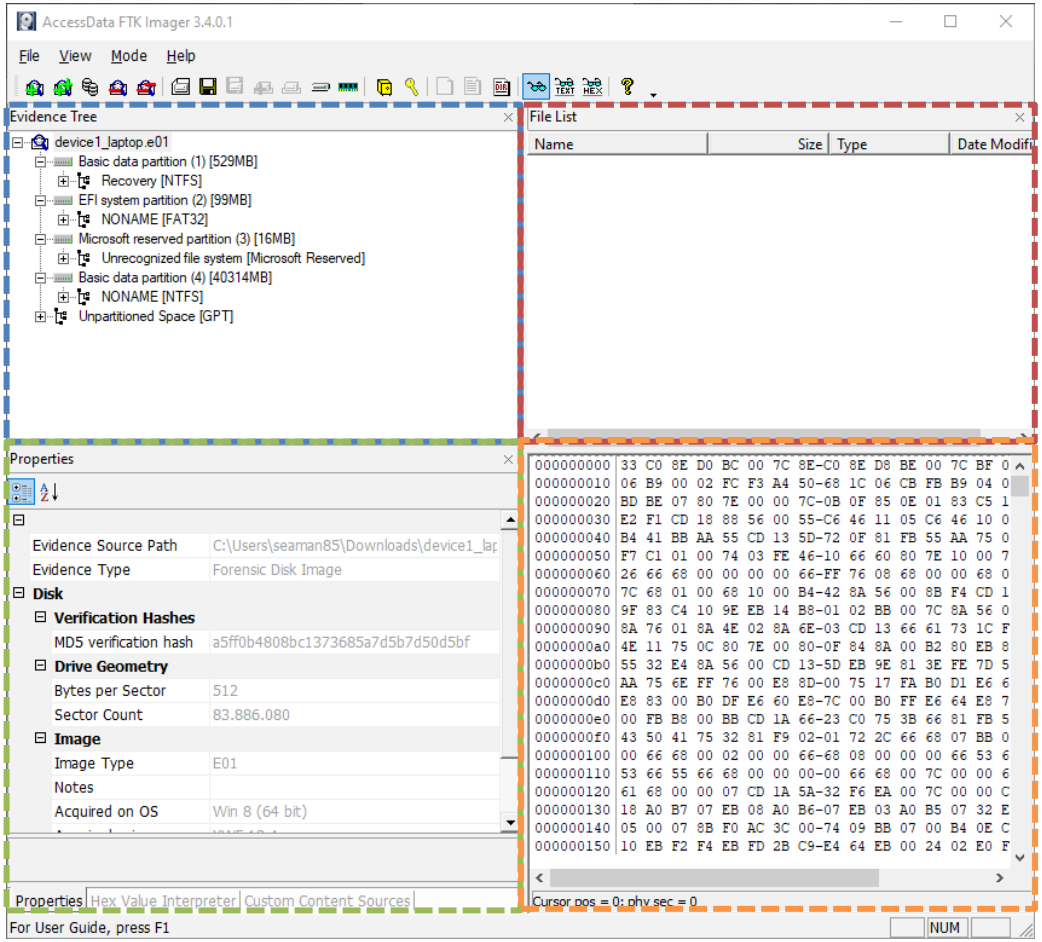
FTK Imager:
analisi file immagine: GUI

Evidence Tree

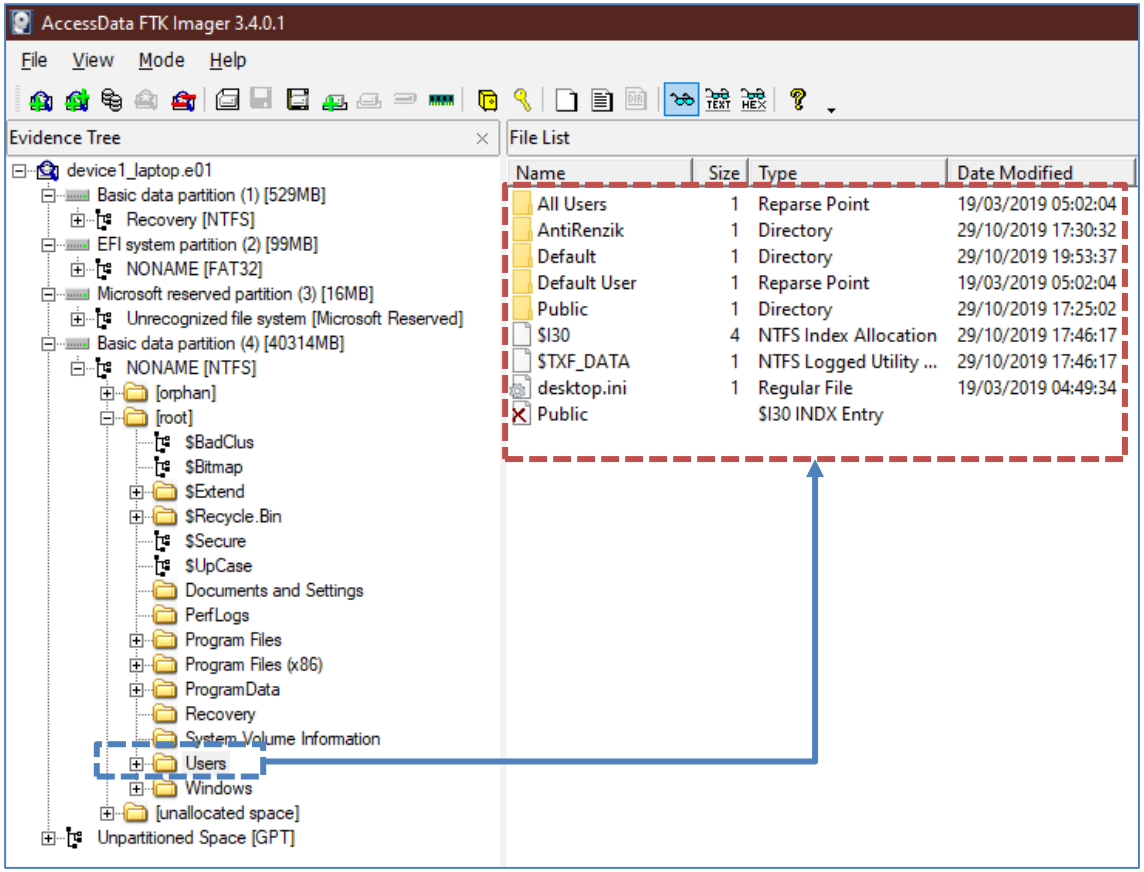
File List

Properties

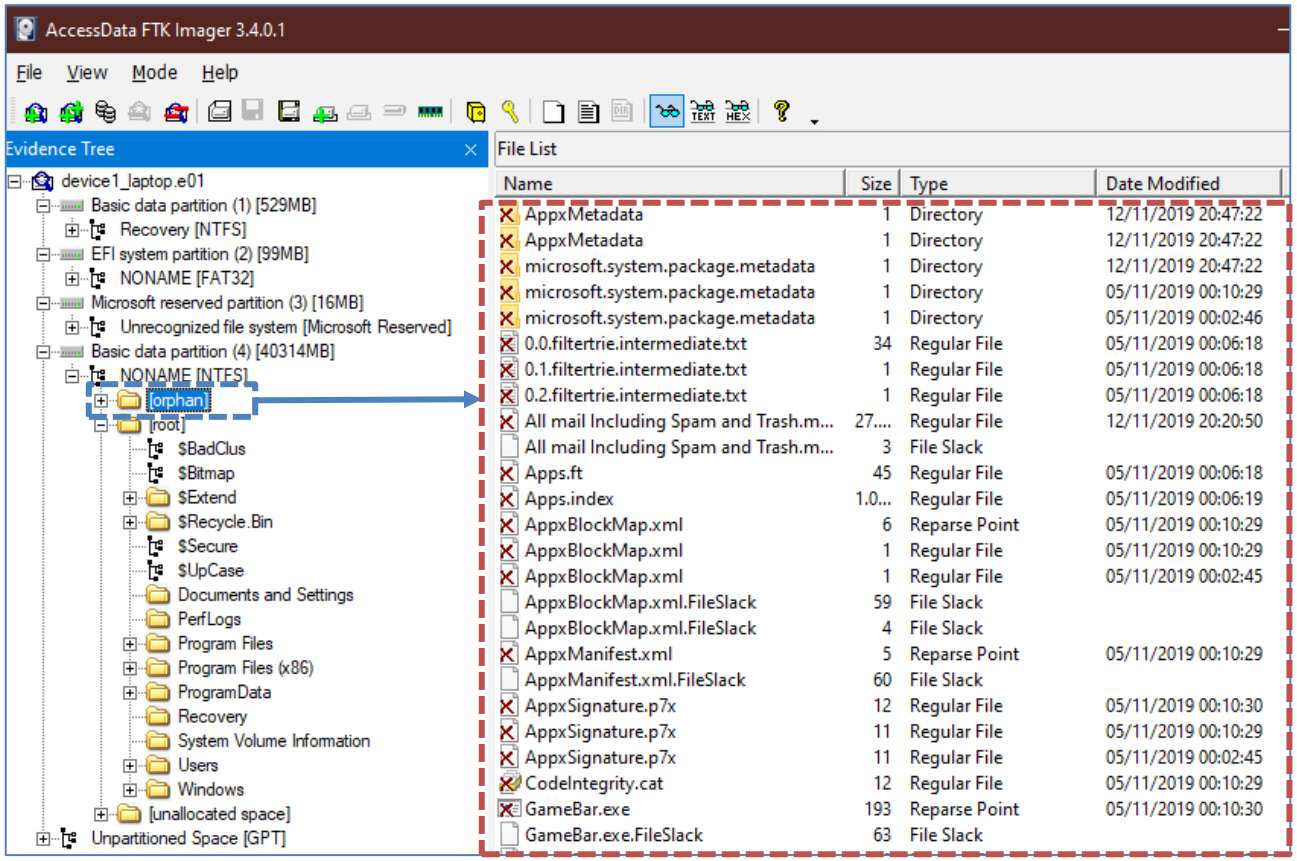
Viewer



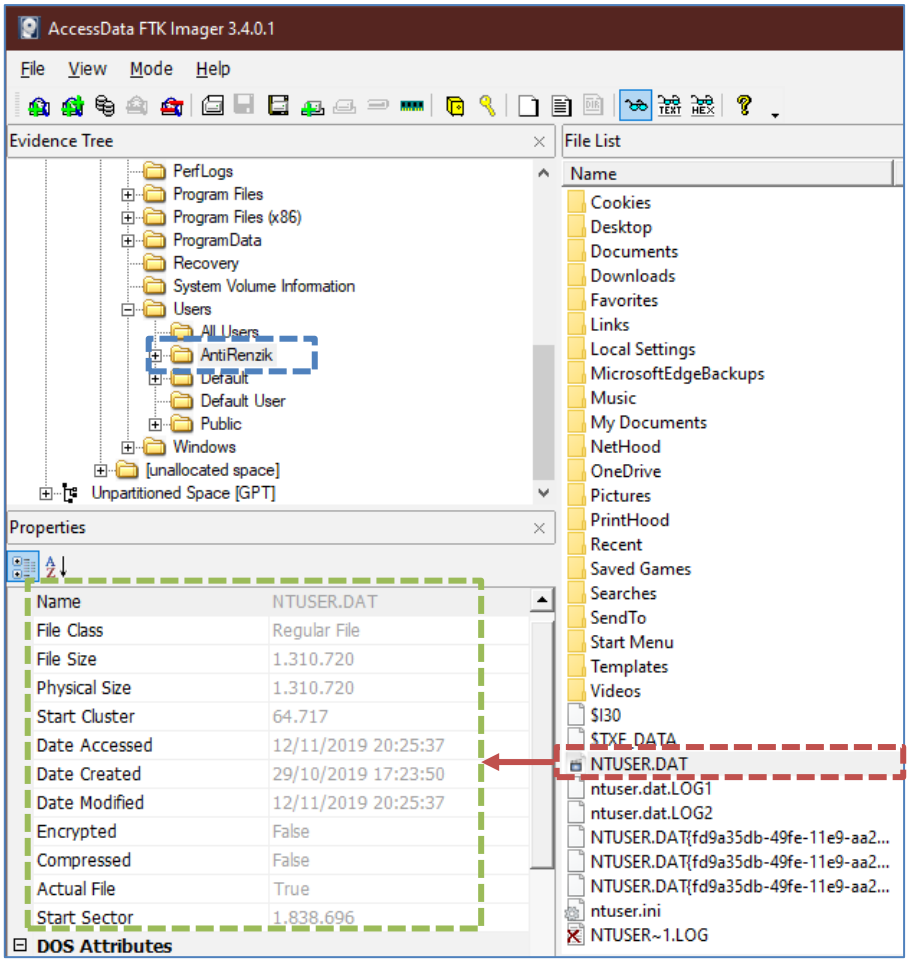
FTK Imager:
analisi file immagine: GUI



FTK Imager:
analisi file immagine: GUI



FTK Imager:
analisi file immagine: GUI



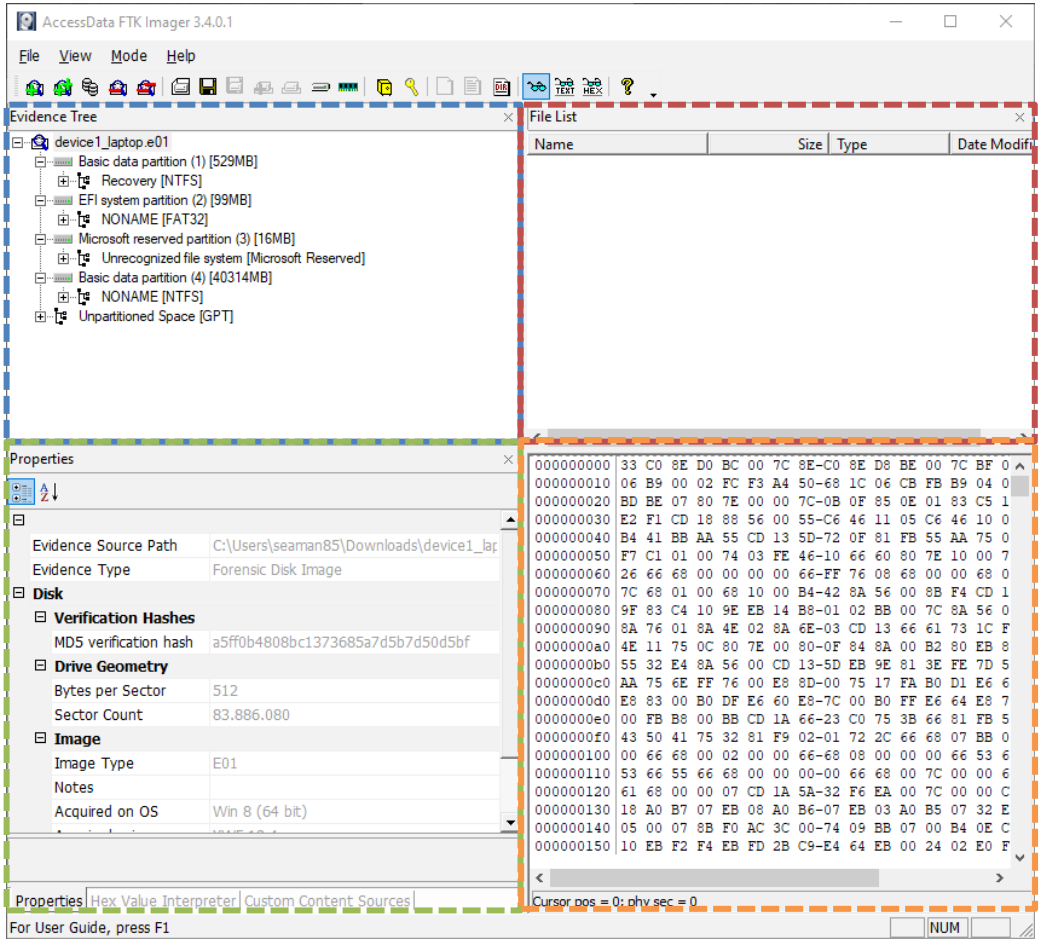
FTK Imager:
analisi file immagine: GUI

Evidence Tree

File List

Properties

Viewer



FTK Imager:

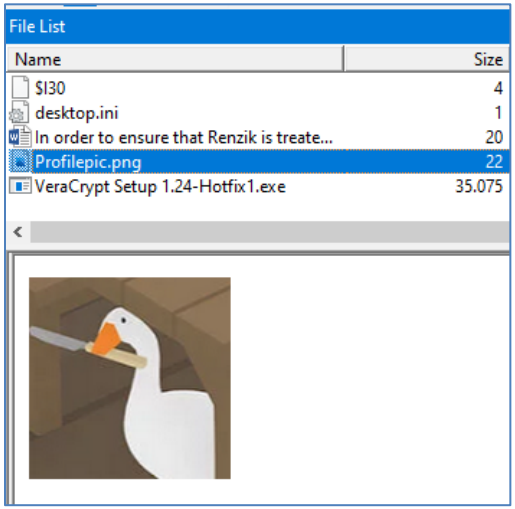
analisi file immagine: GUI

Viewer

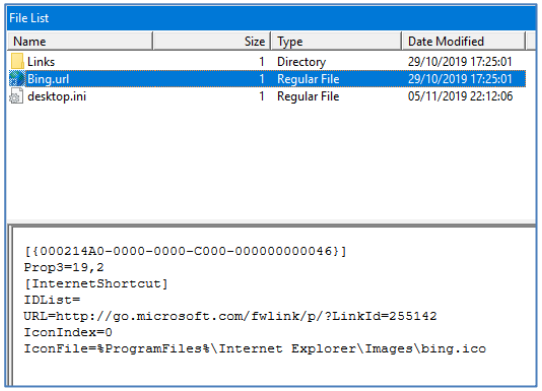
Automatic Mode

Manual Mode

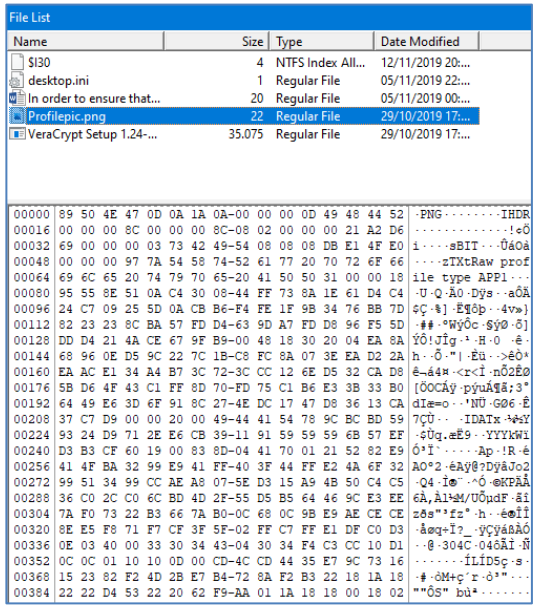
Internet Explorer Mode



Text Mode



Hex Mode



SSRI
Sicurezza Sistemi Reti Informatiche

UNIVERSITÀ DEGLI STUDI DI NAPOLI FEDERICO II

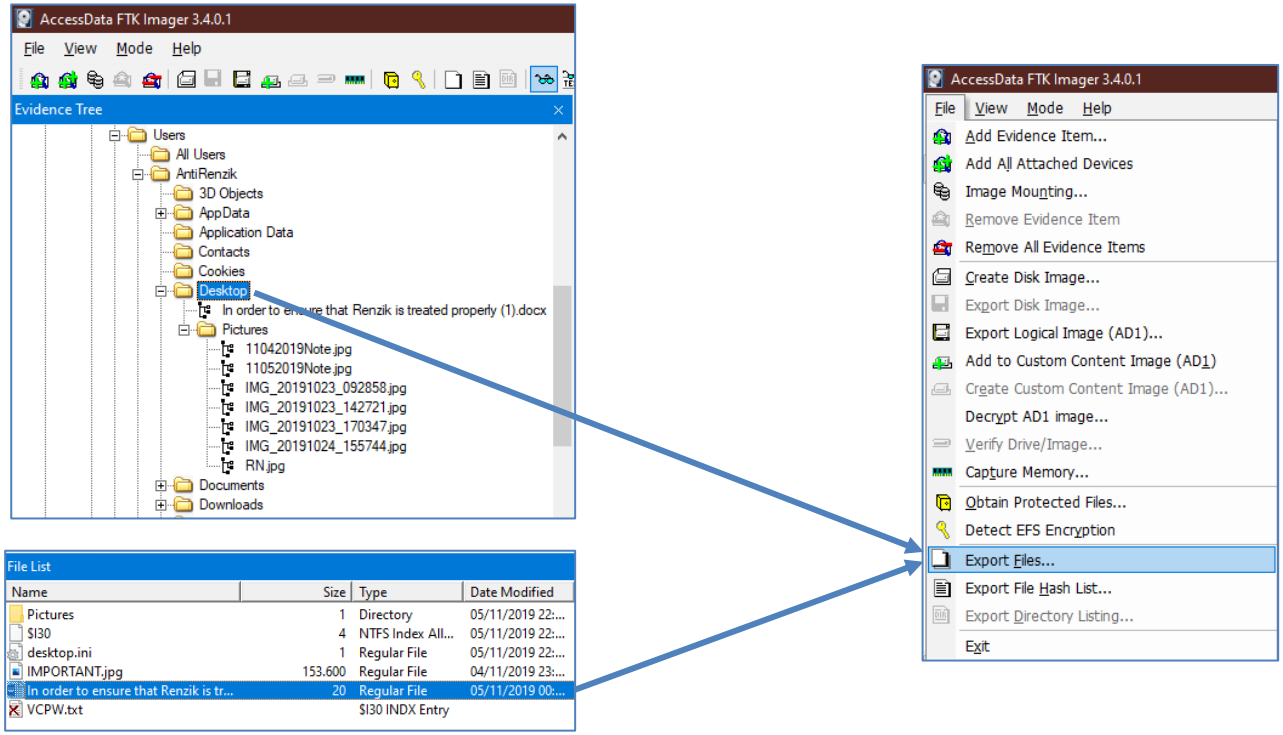
a.a. 2021/22

FTK Imager:

analisi file immagine: Export

Export Files

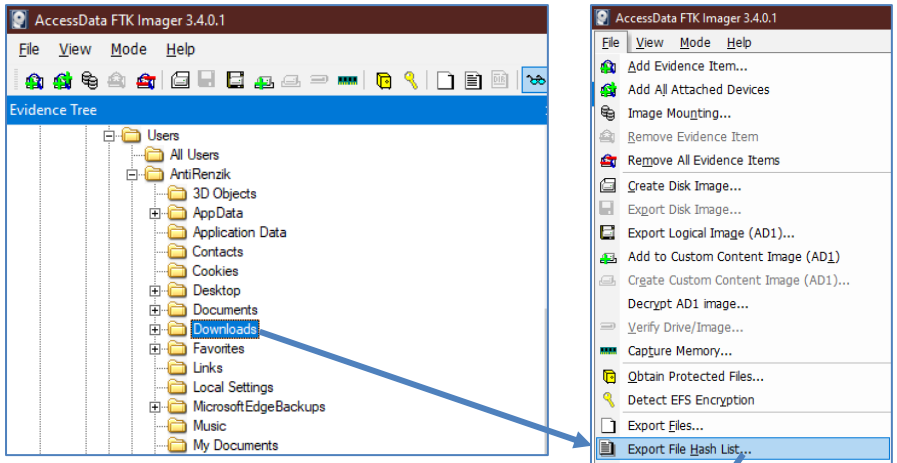
- Esportazione di un file o di un nodo di cartelle



FTK Imager:
analisi file immagine: Export

Export File Hash List

- Esportazione del calcolo Hash (*MD5/SHA1*) di un file o di un nodo di cartelle



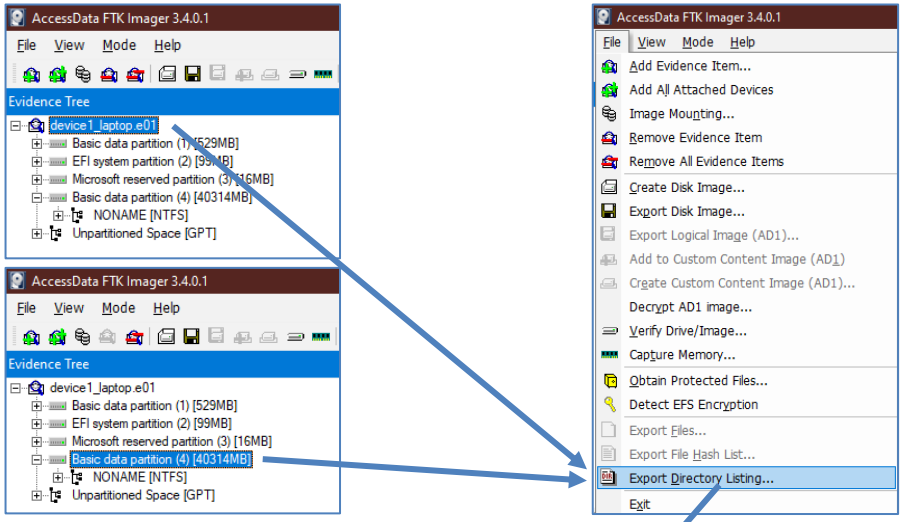
File CSV

A	B	C
MD5	SHA1	FileNames
738f48afad501c7cf52c1517097e2344	2f1adfff64f38fa9c4a98f1f0e05b5050801fcb6	[...]\[root]\Users\AntiRenzik\Downloads\$I30
1a3f1f429a63557547f8a6e837f7f9c0	ba5b15d5995201eacd4af11b734937673bddf903	[...]\[root]\Users\AntiRenzik\Downloads\Profilepic.png
f64c13dedf35213a61ad6975d97f551a	85d92c4fc9120e592d4ed14165e8bfecca2f6c18	[...]\[root]\Users\AntiRenzik\Downloads\Profilepic.png\Zone.Identifier
8dfd9415855c0dd2243b760883d3b53a	432bc364ea5f64c67723c2a1d10c1e9d924da61f	[...]\[root]\Users\AntiRenzik\Downloads\VeraCrypt Setup 1.24-Hotfix1.exe
3a37312509712d4e12d27240137ff377	30ced927e23b584725cf16351394175a6d2a9577	[...]\[root]\Users\AntiRenzik\Downloads\desktop.ini
fea63c9d66768dbb5b23b2f2b3795961	6799557a5e9ed75ba3824e823b705cb320499d4a	[...]\[root]\Users\AntiRenzik\Downloads\In order to ensure that Renzik is treated properly.docx
b883edd4ccb08965c6983dd632a45b1e	91f645b465dbfe1589a76848fd4ed03a0ca1f7cb	[...]\[root]\Users\AntiRenzik\Downloads\In order to ensure that Renzik is treated properly.docx\Zone.Identifier

FTK Imager:
analisi file immagine: Export

Export Directory Listing

- Esportazione dell'elenco di file e cartelle presenti nell'interno dispositivo/partizione



	A	B	C	D	E	F	G
1	Filename	Full Path	Size (bytes)	Created	Modified	Accessed	Is Deleted
2	[root]	NONAME [NTFS]\[root]\	56	2019-Mar-19 04:37:21.986161 UTC	2019-Nov-05 22:24:31.294968 UTC	2019-Nov-12 20:25:40.264356 UTC	no
3	[unallocated space]	NONAME [NTFS]\[unallocated space]\	0				no
4	[orphan]	NONAME [NTFS]\[orphan]\	0				no
5	file system slack	NONAME [NTFS]\file system slack	3584				no
6	backup boot sector	NONAME [NTFS]\backup boot sector	512				no
7	$I30	NONAME [NTFS]\[root]\$I30	4096	2019-Mar-19 04:37:21.986161 UTC	2019-Nov-05 22:24:31.294968 UTC	2019-Nov-12 20:25:40.264356 UTC	no
8	$TXF_DATA	NONAME [NTFS]\[root]\$TXF_DATA	56	2019-Mar-19 04:37:21.986161 UTC	2019-Nov-05 22:24:31.294968 UTC	2019-Nov-12 20:25:40.264356 UTC	no
9	Recovery	NONAME [NTFS]\[root]\Recovery\	48	2019-Oct-29 19:53:43.804763 UTC	2019-Oct-29 19:53:43.804763 UTC	2019-Oct-29 19:53:43.804763 UTC	no
10	Documents and Settings	NONAME [NTFS]\[root]\Documents and Settings\	60	2019-Oct-29 19:53:37.151795 UTC	2019-Oct-29 19:53:37.151795 UTC	2019-Oct-29 19:53:37.151795 UTC	no
11	...	...	...	...	...	...	...

L'Analisi

- Strumenti Software

L'Analisi
strumenti software

Toolkit

- Supporto all'intera fase di analisi

Es.:
- AccessData FTK
- Autopsy
- Encase Forensics
- BlackLight
- X-Ways Forensics
- PassMark OS Forensics

Tools Forensic Oriented

- Esecuzione di un specifico task

Es.:
- Internet Evidence Finder
- Amped Five
- Log2Timeline

Tool Generici

- Non progettati per la C.F.

Es.:
- USBdeview
- Diff-PDF
- VMWare

Fine prima parte…

SSRI Lorenzo Laurato s.r.l.

Via Coroglio nr. 57/D (BIC- Città della Scienza)
80124 Napoli

Tel. 081.19804755
Fax 081.19576037

lorenzo.laurato@unina.it
lorenzo.laurato@ssrilab.com

www.docenti.unina.it/lorenzo.laurato
www.computerforensicsunina.forumcommunity.net