

# COMPUTER FORENSICS

## Lezione 13: L'Analisi *gli strumenti* (2<sup>a</sup> parte)



A.A. 2021/22

Dott. Lorenzo LAURATO



# 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

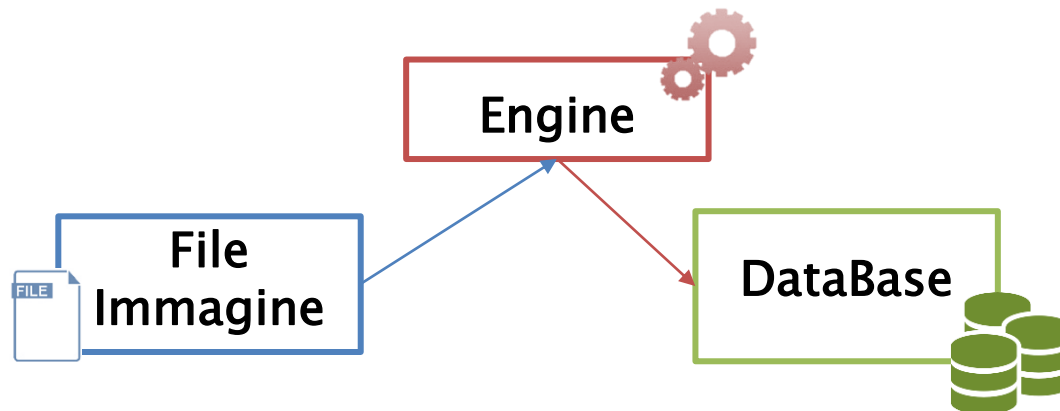
# I Toolkit: overview

## Forensic ToolKit (FTK)

- ▶ Commerciale
- ▶ Microsoft Windows

## Autopsy

- ▶ Free e OpenSource
- ▶ Multiplatforma



Multi-utente / Scalabile

# I Toolkit

## Formati File Immagine

### Forensic ToolKit (FTK)

- ▶ Encase E01
- ▶ Encase L01 Logical Image
- ▶ Expert Witness
- ▶ SnapBack
- ▶ Safeback 2.0 and under
- ▶ ICS
- ▶ Linux DD
- ▶ SMART
- ▶ Ghost (forensic images only)
- ▶ MSVHD (MS Virtual Hard Disk)
- ▶ AccessData Logical Image (AD1)
- ▶ Lx0, Lx01
- ▶ DMG (Mac)
- ▶ VMDK (VmWare Disk)

### Autopsy

- ▶ Encase E01
- ▶ Raw (DD, BIN, IMG)
- ▶ Virtual Disk (VMDK, VHD)

# I Toolkit

## File System

### Forensic ToolKit (FTK)

- ▶ FAT
- ▶ exFAT
- ▶ NTFS
- ▶ Ext2FS
- ▶ Ext3FS
- ▶ Ext4FS
- ▶ APFS
- ▶ HFS, HFS+
- ▶ CDFS
- ▶ ReiserFS 3
- ▶ VxFS (Veritas File System)

### Autopsy

- ▶ FAT
- ▶ ExFAT
- ▶ NTFS
- ▶ EXT2FS
- ▶ EXT3FS
- ▶ EXT4FS
- ▶ APFS
- ▶ HFS, HFS+
- ▶ YAFFS2

# I Toolkit

## Le Viste

Offrono più visualizzazioni delle informazioni  
contenute nella copia forense

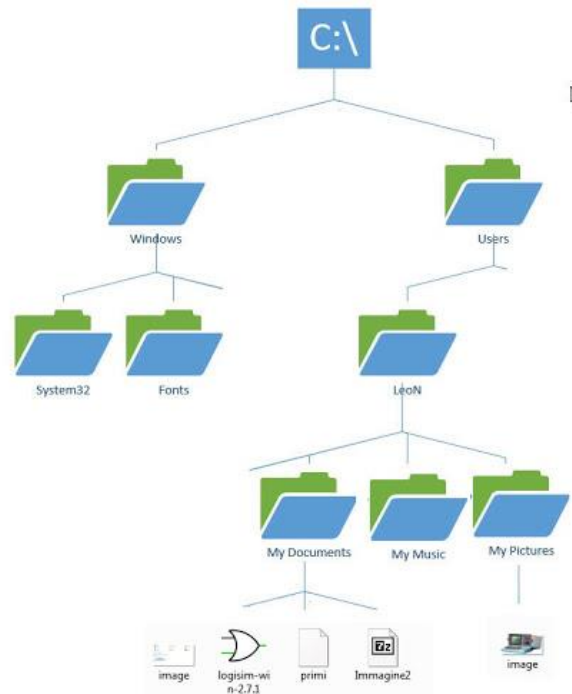


Elaborazione di file e artefatti

# I Toolkit

## Le Viste

### Albero



Rappresentazione gerarchica dei file

# I Toolkit

## Le Viste

### File Type

- ▶ **Catalogazione:** analisi dei file per
  - *estensione*: suffisso del file
    - .docx, .jpg, .pdf, . zip, etc.
  - *signature (magic number)*: sequenza di bit posta in punto ben preciso del file (offset), normalmente prima della sequenza di dati, che serve per definire il formato in cui i dati sono memorizzati.

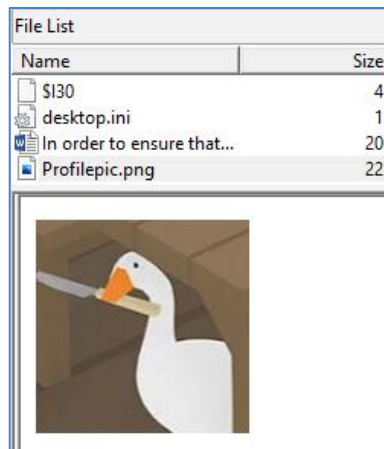


# I Toolkit

## Le Viste

### Signature

Hex signature	89 50 4E 47 0D 0A 1A 0A
ASCII	.PNG....
Offset	0
Ext	PNG



File List				
Name	Size	Type	Date Modified	
\$I30	4	NTFS Index All...	12/11/2019 20:...	
desktop.ini	1	Regular File	05/11/2019 22:...	
In order to ensure that...	20	Regular File	05/11/2019 00:...	
Profilepic.png	22	Regular File	29/10/2019 17:...	

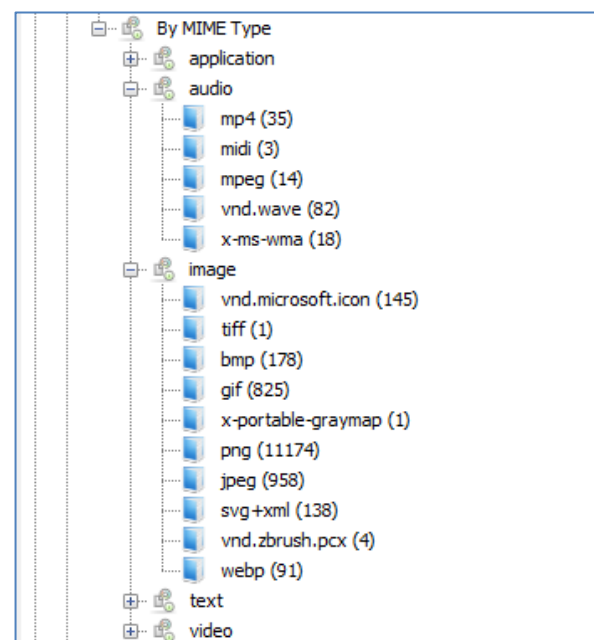
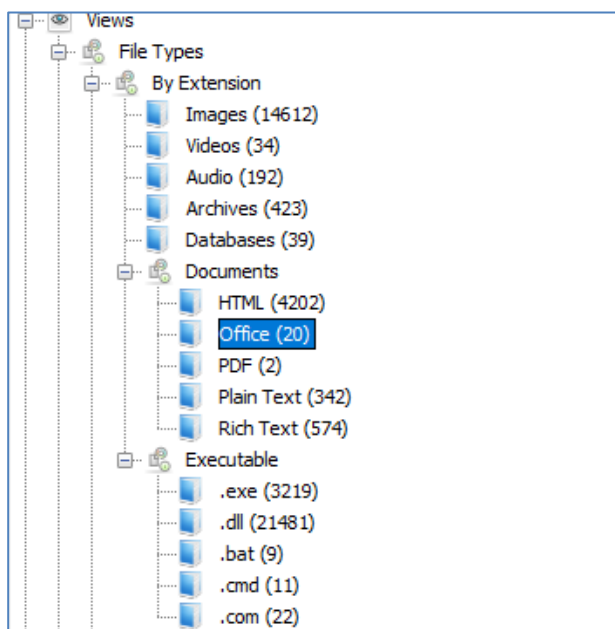
0000	89 50 4E 47 0D 0A 1A 0A	00 00 0D 49 48 44 52	.PNG . . . . .	IHDR
0010	00 00 00 8C 00 00 00 8C	08 02 00 00 00 21 A2 D6	. . . . .	leÖ
0020	69 00 00 00 03 73 42 49	54 08 08 08 DB E1 4F E0	i . . . . sBIT . . . .	ÛäOà
0030	00 00 00 97 7A 54 58 74	52 61 77 20 70 72 6F 66	. . . . zTXtRaw prof	
0040	69 6C 65 20 74 79 70 65	20 41 50 50 31 00 00 18	ile type APPl . . .	

# I Toolkit

## Le Viste

### File Type

### Autopsy

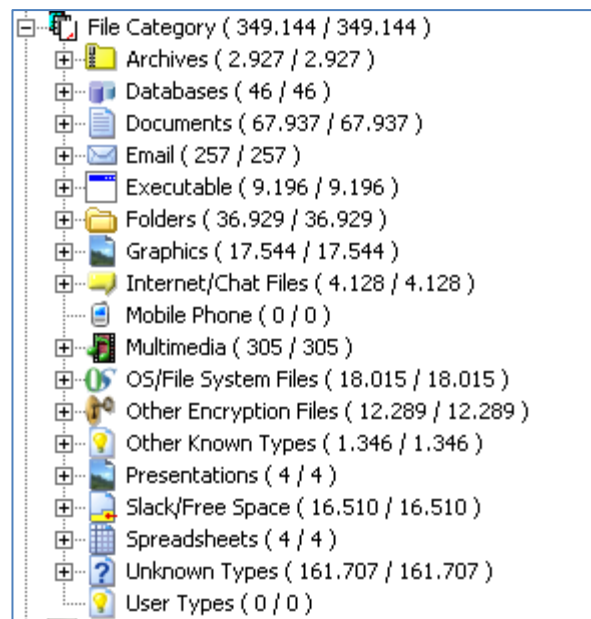
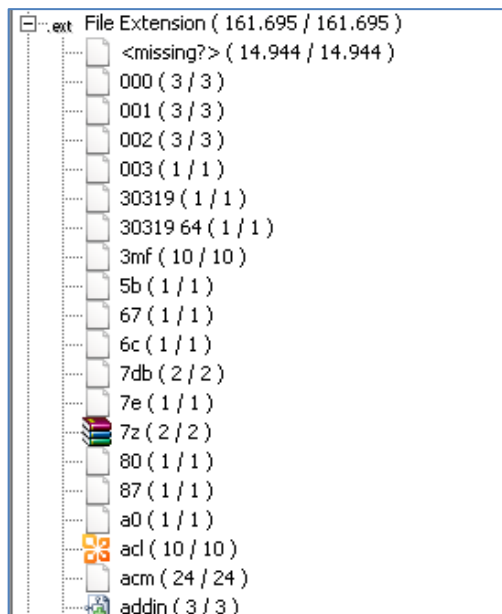


# I Toolkit

## Le Viste

### File Type

#### FTK

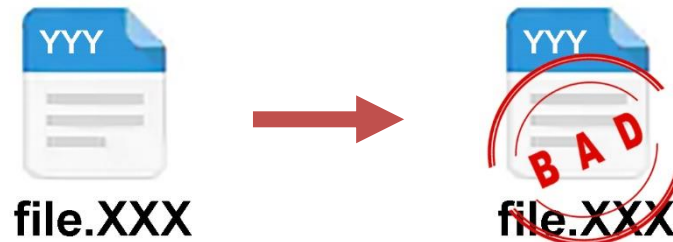


# I Toolkit

## Le Viste

### File Type

- ▶ **Classificazione:** i file vengono analizzati ed arricchiti di alcuni attributi:
  - Bad Extension: estensione vs signature



- Delete file: file marcati come cancellati dal file system

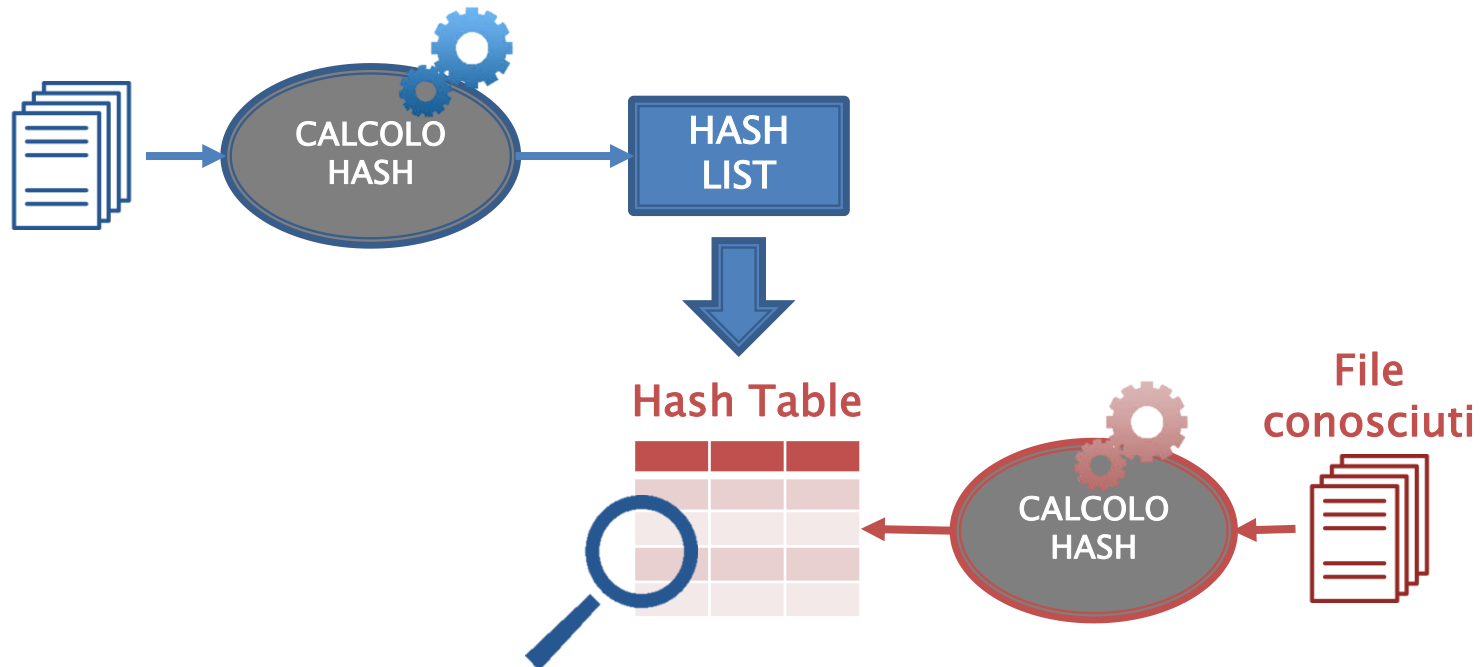


# I Toolkit

## Le Viste

### Known File

- Riconoscimento del file basato sull'HASH



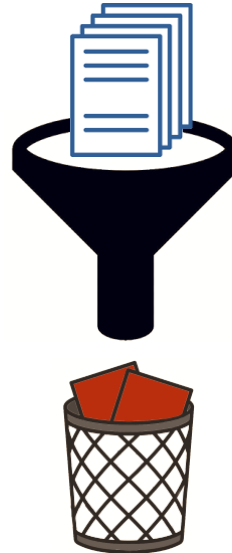
Ignorable File / Notable File

# I Toolkit

## Le Viste

### Known File: *Ignorable File*

- ▶ File conosciuti come di non interesse:
  - Sottrazione di migliaia di File dall'analisi
  - Es: file di sistema/programmi (National Software Reference Library)

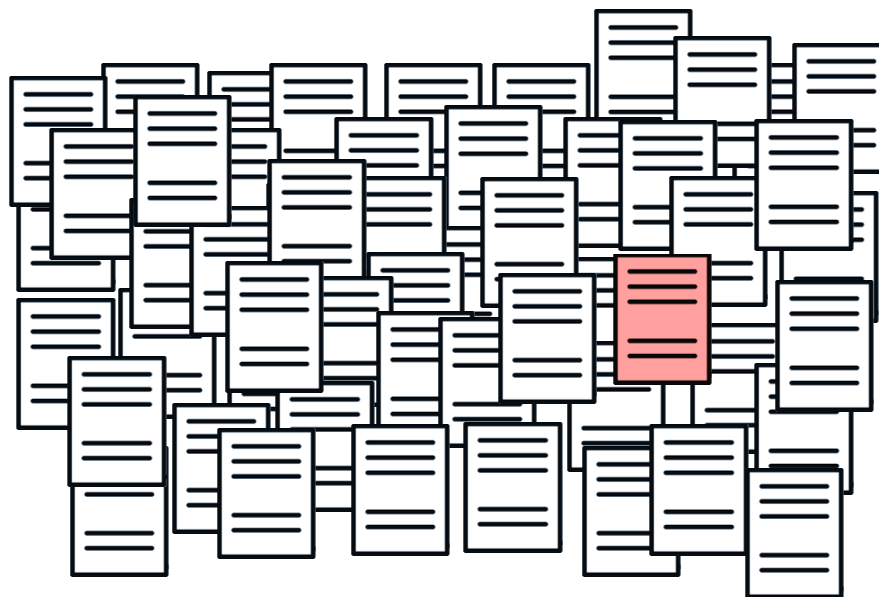


# I Toolkit

## Le Viste

### Known File: *Notable File*

- ▶ File conosciuti come di notevole interesse:
  - Ricerca mirata di determinati file
  - Es: Pedopornografia (Project VIC)

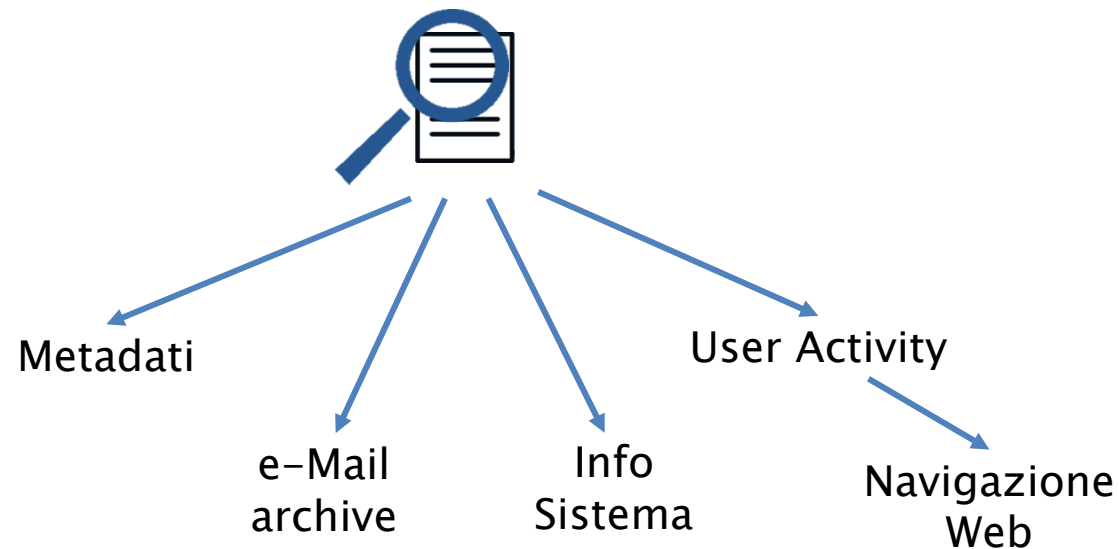


# I Toolkit

## Le Viste

### Artefatti

- ▶ Analisi del contenuto del file:
  - Estrazione ed elaborazione delle informazioni presenti in uno o più file





# I Toolkit

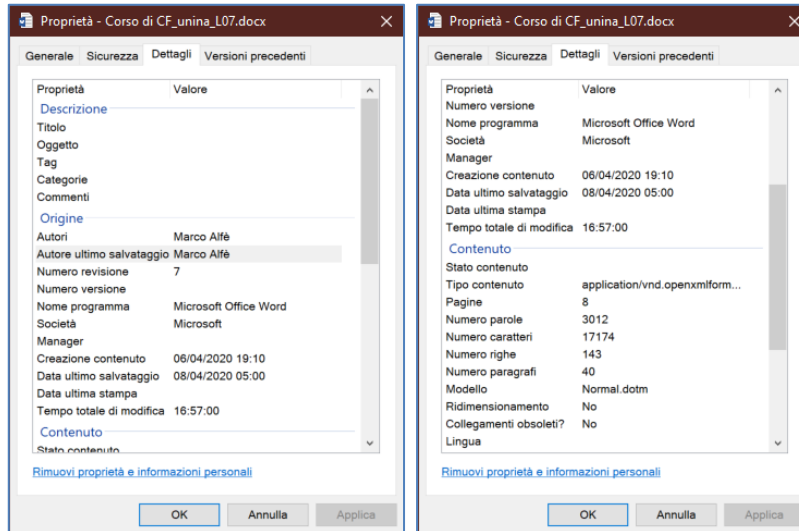
## Le Viste

### Artefatti: *Metadati*

- ▶ dati strutturati contenenti informazioni aggiuntive sul file

Documenti  
(Office, PDF, etc)

FTK



Properties	
Name	Corso di CF_unina_L07.docx
Item Number	351001
File Type	Microsoft Word 2016 XML
Path	Corso di CF_unina_L07.docx
General Info	
Microsoft Office Metadata	
Author	Marco Alfè
Template	Normal.dotm
Last saved by	Marco Alfè
Revision number	7
Total editing time	16 minutes 57 seconds
Create time	06/04/2020 19:10:00 (2020-04-06 17:10:00 UTC)
Last saved time	08/04/2020 05:00:00 (2020-04-08 03:00:00 UTC)
Number of pages	8
Number of words	3.012
Number of characters	17.174
Creating application	Microsoft Office Word
Security	0
Line Count	143
Paragraphs	40
Crop or Scale	False
Document Sections Count	Titolo=1
Company	Microsoft

# I Toolkit

## Le Viste

### Artefatti: *Metadati*

Exif: informazioni sulla fotografia  
(JPEG, TIFF, RIFF)



IMG\_20191023\_170347.jpg

### Autopsy

Type	Value
Date Created	2019-10-23 17:03:47
Latitude	29.950344083333334
Longitude	-90.06626891666666
Altitude	10.0
Device Model	BLU R1 HD
Device Make	BLU

### FTK

EXIF Entries	
Exif.Image.Make	BLU
Exif.Image.Model	BLU R1 HD
Exif.Image.Orientation	1
Exif.Image.XResolution	72/1
Exif.Image.YResolution	72/1
Exif.Image.ResolutionUnit	2
Exif.Image.Software	MediaTek Camera Application
Exif.Image.DateTime	2019:10:23 17:03:47
Exif.Image.YCbCrPositioning	2
Exif.Image.ExifTag	426
Exif.Image.GPSTag	812
Exif.Photo.ExposureTime	2327/1000000
Exif.Photo.FNumber	20/10
Exif.Photo.ExposureProgram	0
Exif.Photo.ISOSpeedRatings	106
Exif.Photo.ExifVersion	48 50 50 48

Exif.Photo.DateTimeOriginal	2019:10:23 17:03:47
Exif.Photo.DateTimeDigitized	2019:10:23 17:03:47
Exif.Photo.ComponentsConfiguration	1 2 3 0
Exif.Photo.ExposureBiasValue	0/10
...	...
Exif.GPSInfo.GPSVersionID	2 2 0 0
Exif.GPSInfo.GPSLatitudeRef	N
Exif.GPSInfo.Latitude	29/1 57/1 12387/10000
Exif.GPSInfo.LongitudeRef	W
Exif.GPSInfo.Longitude	90/1 3/1 585681/10000
Exif.GPSInfo.AltitudeRef	0
Exif.GPSInfo.Altitude	10/1
Exif.GPSInfo.GPSTimeStamp	22/1 3/1 20/1
Exif.GPSInfo.GPSProcessingMethod	65 83 67 73 73 0 0 0 78 69 84 87 79 82 75
Exif.GPSInfo.GPSDateStamp	2019:10:23

# I Toolkit

## Le Viste

### Artefatti: *e-Mail Archive*

► Analisi degli archivi/database e-Mail:

- Visualizzazione delle e-Mail
- Estrazione degli allegati



Autopsy  $\approx$  FTK

**File List**

Subject	Submit Time	From	To
Photos	01/11/2019 21:12:46 ...	Peacock Leprechaun <peacockleprechaun@gmail.com>	antirenzik@gmail.com
ARG questions	01/11/2019 21:24:57 ...	Peacock Leprechaun <peacockleprechaun@gmail.com>	Goose Honkerson <antirenzik@gmail.com>
Undelivered Mail Returned to Sender	01/11/2019 21:30:43 ...	MAILER-DACMON@malstream-east.morecord.io (...)	antirenzik@gmail.com
Fareed: The Middle East Is Still Fertile Ground for Terror Groups	01/11/2019 23:27:26 ...	Fareed's Global Briefing <GlobalBriefing@cnn.com>	<antirenzik@gmail.com>
Re: ARG questions	01/11/2019 23:27:26 ...	Goose Honkerson <antirenzik@gmail.com>	Peacock Leprechaun <peacockleprechaun@gmail.com>
We Have Renzik	01/11/2019 23:30:33 ...	Goose Honkerson <antirenzik@gmail.com>	briancarmen@basistech.com
Re: ARG questions	01/11/2019 23:32:01 ...	Goose Honkerson <antirenzik@gmail.com>	Peacock Leprechaun <peacockleprechaun@gmail.com>
The Point: The impeachment vote had no tricks -- and no treats	01/11/2019 23:32:56 ...	Chris Gilliza <cgilliza@cnn.com>	<antirenzik@gmail.com>
We Have Renzik	01/11/2019 23:33:11 ...	Goose Honkerson <antirenzik@gmail.com>	info@basistech.com
Re: ARG questions	01/11/2019 23:35:10 ...	Goose Honkerson <antirenzik@gmail.com>	Peacock Leprechaun <peacockleprechaun@gmail.com>
235 days; McHenry and Fox; Deadspin's future; Warzel's remin...	02/11/2019 02:22:57 ...	Brian Stelter <brian.stelter@cnn.com>	<antirenzik@gmail.com>
What happens when dreams come true?	02/11/2019 13:08:50 ...	CNN's Good Stuff <TheGoodStuff@cnn.com>	
Day 9 - What The Heck Is Mining?	02/11/2019 19:32:29 ...	"The Bitcoin.com Team" <team@bitcoin.com>	

**File Content**

Hex Text Filtered Natural

**From:** Goose Honkerson <antirenzik@gmail.com>  
**Sent:** 01/11/2019 15:33:11 -0700  
**To:** info@basistech.com  
**Subject:** We Have Renzik  
**Attachments:** RN.jpg; IMG\_20191023\_092858.jpg

My dearest Mr Carrier,

We have Renzik, and we have had him for a few days. Do not try to find him, we have specifically ensured that he is safely hidden. You will hear from us in 24 hours with more details.

All Hail Hash

**Email Attachments**

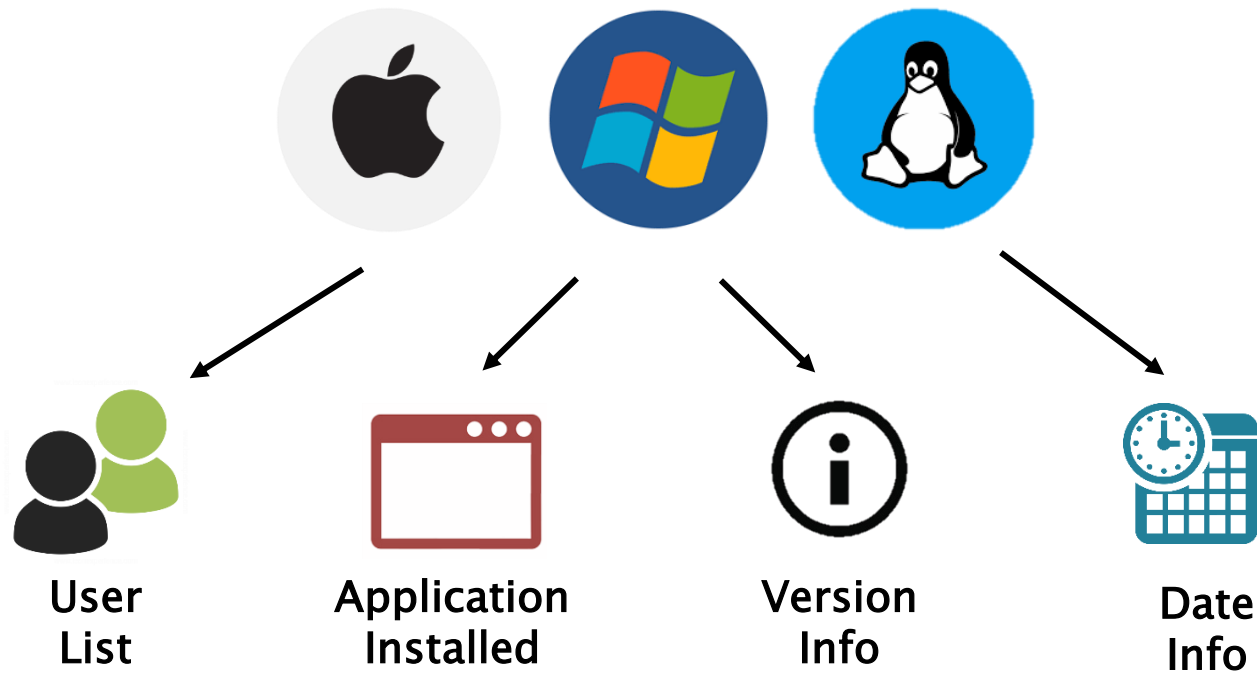
- entry #23494986.eml
- RN.jpg
- IMG\_20191023\_092858.jpg

# I Toolkit

## Le Viste

### Artefatti: *System Information*

- Estrazione delle informazioni dell'ambiente di lavoro

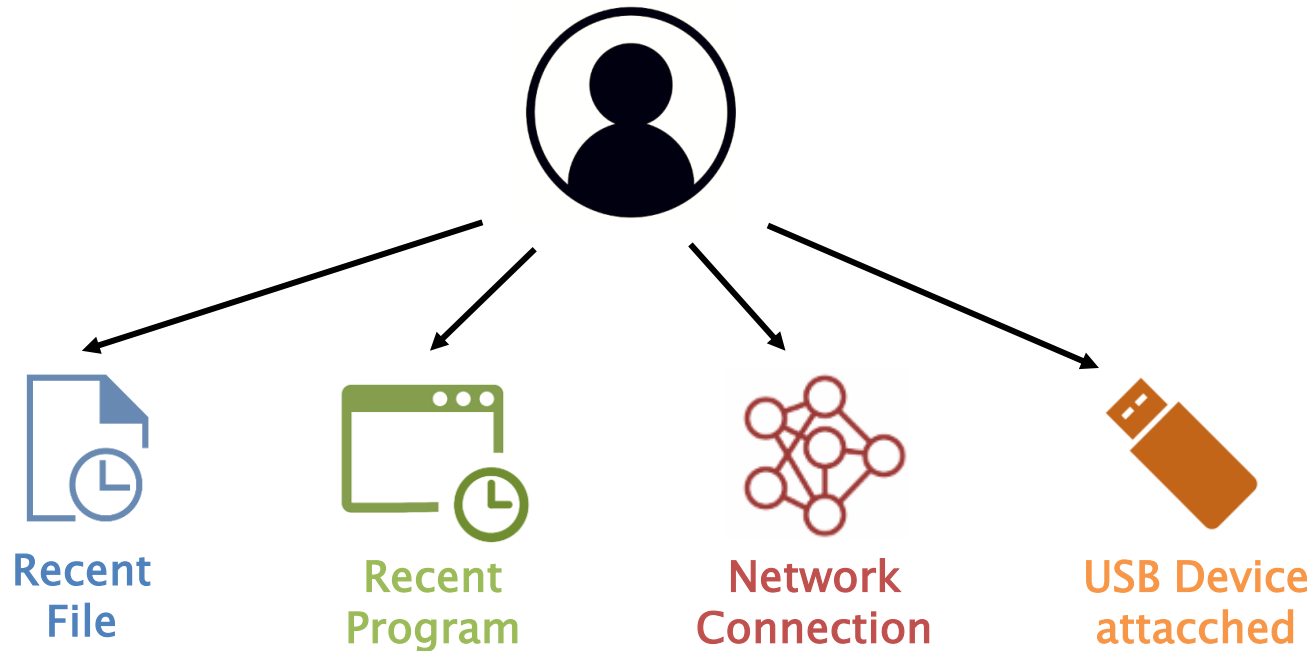


# I Toolkit

## Le Viste

### Artefatti: *User Activity*

- ▶ Analisi delle attività eseguite dall'utente: *File di registro, log, etc.*

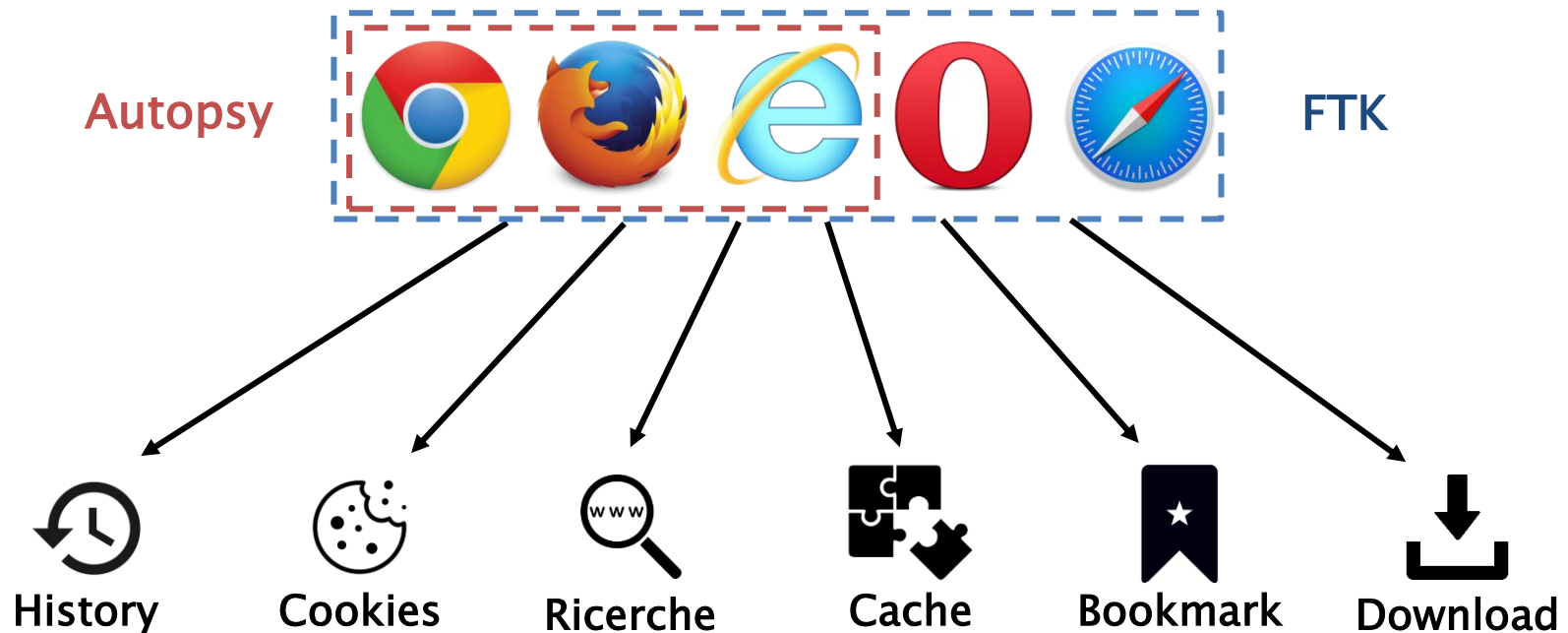


# I Toolkit

## Le Viste

### Artefatti: *Navigazione WEB*

- Analisi dei file dei browser web: *history, cookies, cache, download, search, autofill.*



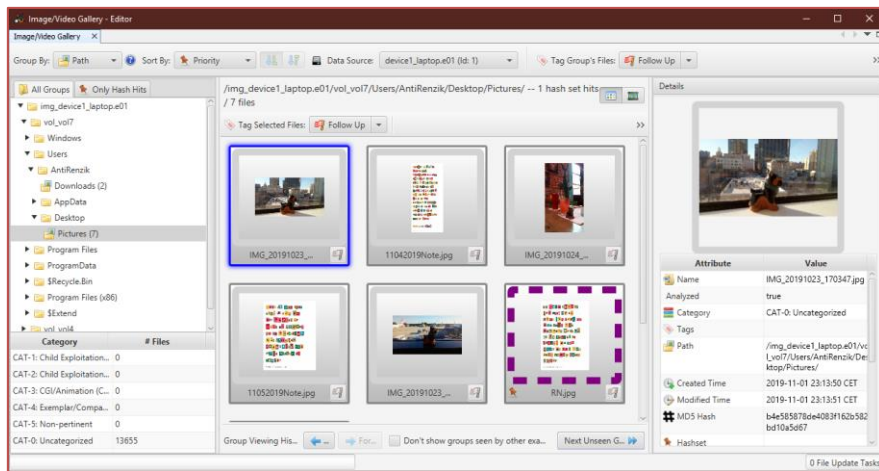
# I Toolkit

## Le viste specializzate

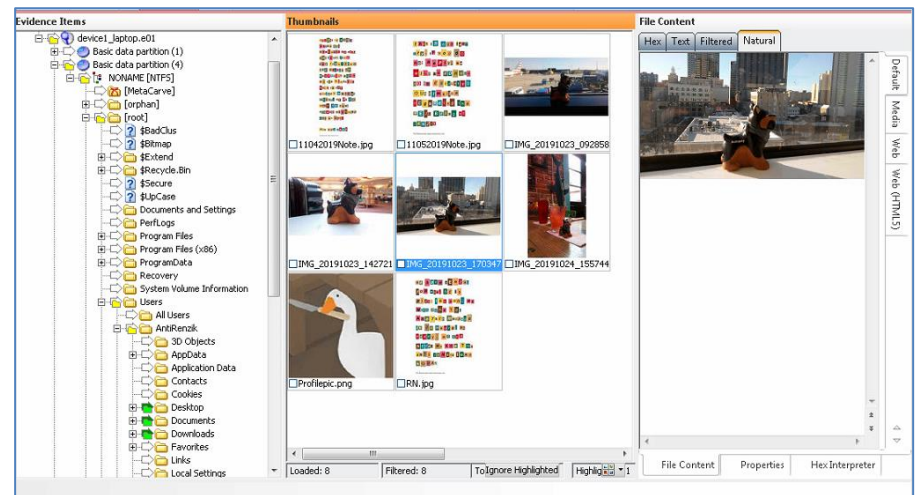
### Image Gallery

- Generazione e visualizzazione di *thumbnail* dei file grafici

### Autopsy



### FTK



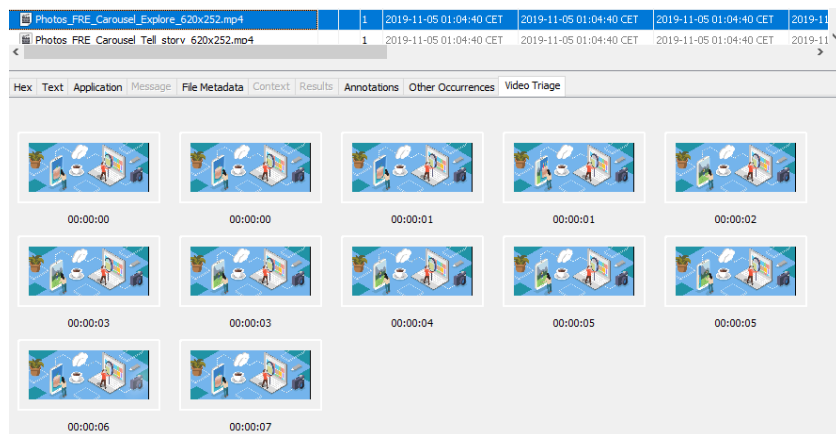


# I Toolkit

## Le viste specializzate

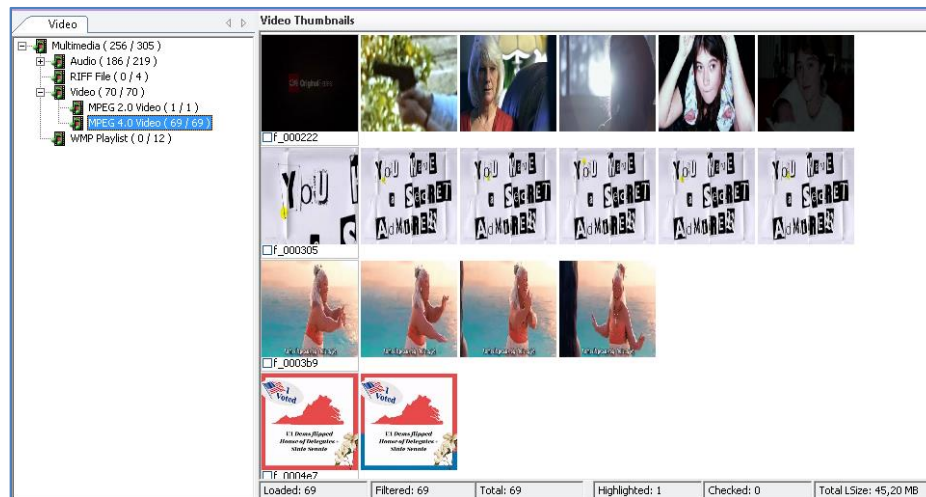
### Video Gallery

- ▶ Processo di elaborazione per l'estrazione e la visualizzazione di frame dai video:
  - Ogni valore % del video (5%, 10%, etc)
  - Ogni intervallo di tempo (1min, 5min, etc.)



Autopsy

FTK





# I Toolkit

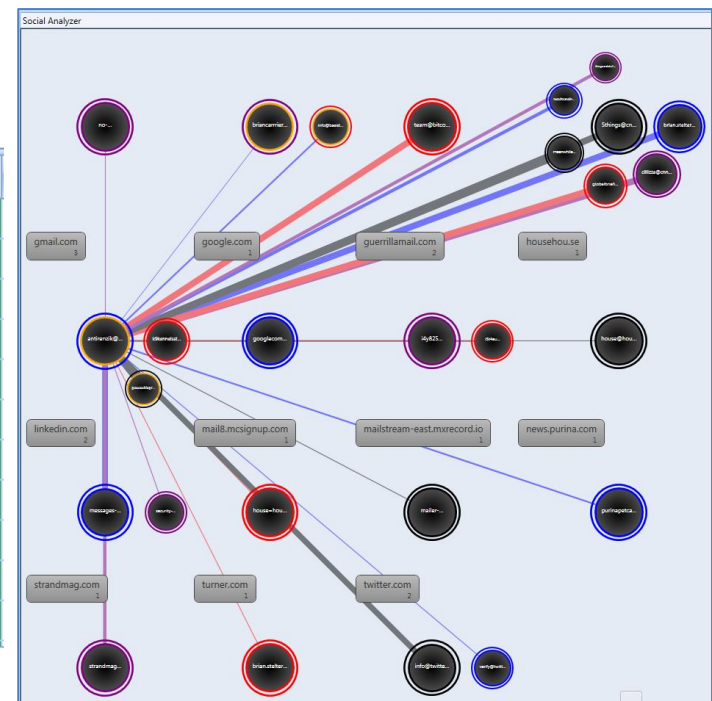
## Le viste specializzate

### Social Analyzer

- Visualizzazione delle relazioni/connessioni avvenute tra i diversi soggetti (*eMail*)

### FTK

Display Name	Email Address	Traffic Count	Sent	Received
(mail delivery system)		1	1	0
good morning from cnn	5things@cnn.com	13	13	0
	antirenzik@gmail.com	139	12	127
brian stelter	brian.stelter@cnn.com	12	12	0
brian stelter	brian.stelter@turner.com	1	1	0
	briancarrier@basistech.com	1	0	1
chris cillizza	cillizza@cnn.com	13	13	0
cnn's global briefing	globalbriefing@cnn.com	13	13	0
google community team	googlecommunityteam-noreply@g	1	1	0
house house	house@househou.se	1	1	0
house house	house=househou.se@mail8.mcsign	1	1	0



# I Toolkit











## Le viste specializzate

### Social Analyzer

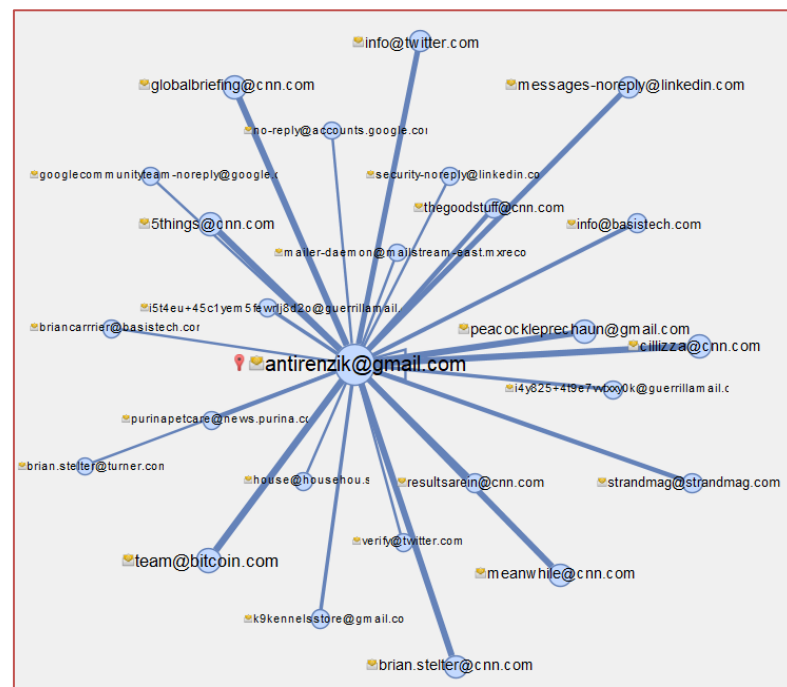
- Visualizzazione delle relazioni/connessioni avvenute tra i diversi soggetti (*eMail*)

Browse

Visualize

Account	Device	Type	▼ Items
 antirenzik@gmail.com	device1_laptop.e01	Email	276
 team@bitcoin.com	device1_laptop.e01	Email	34
 5things@cnn.com	device1_laptop.e01	Email	26
 peacockleprechaun@gmail.com	device1_laptop.e01	Email	26
 globalbriefing@cnn.com	device1_laptop.e01	Email	26
 cillizza@cnn.com	device1_laptop.e01	Email	26
 brian.stelter@cnn.com	device1_laptop.e01	Email	24
 meanwhile@cnn.com	device1_laptop.e01	Email	22
 messages-noreply@linkedin.com	device1_laptop.e01	Email	14
 info@twitter.com	device1_laptop.e01	Email	14

Autopsy



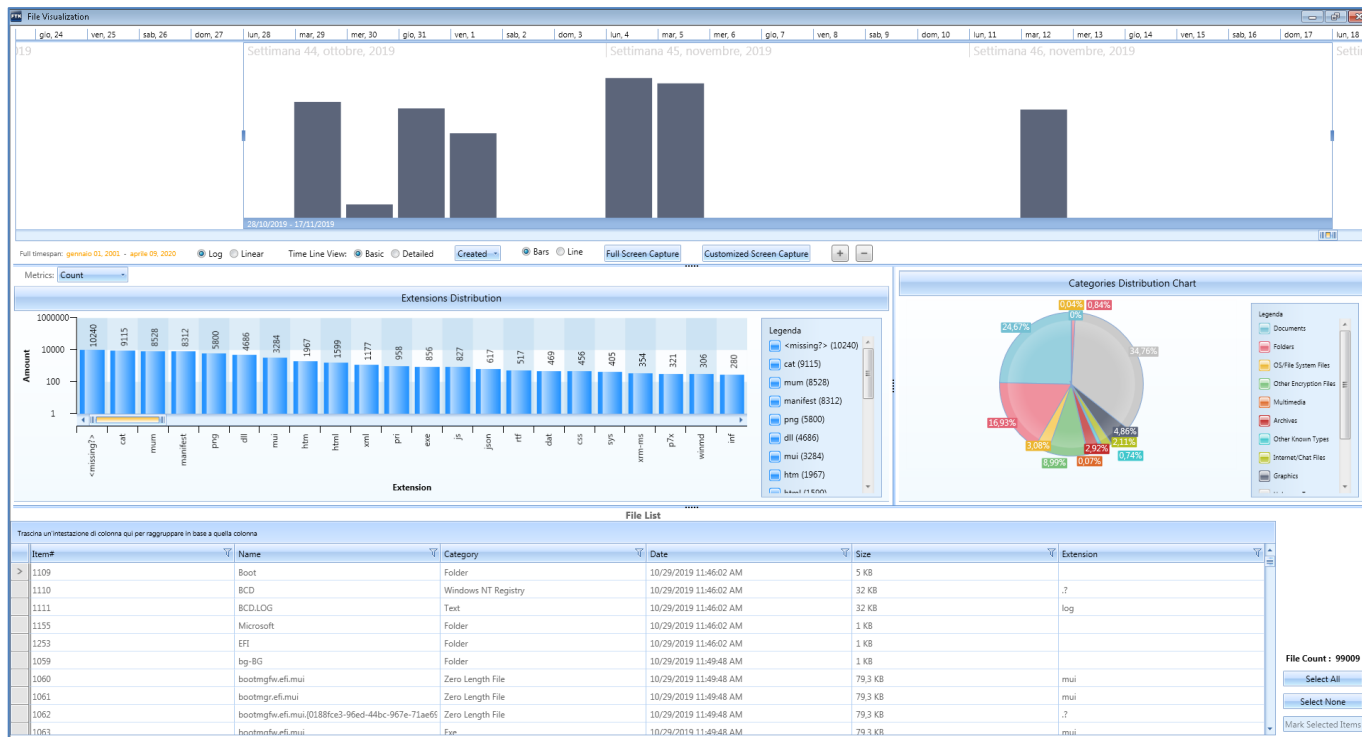
# I Toolkit

## Le viste specializzate

### TimeLine

## ► Visualizzazione temporale dei file

FTK



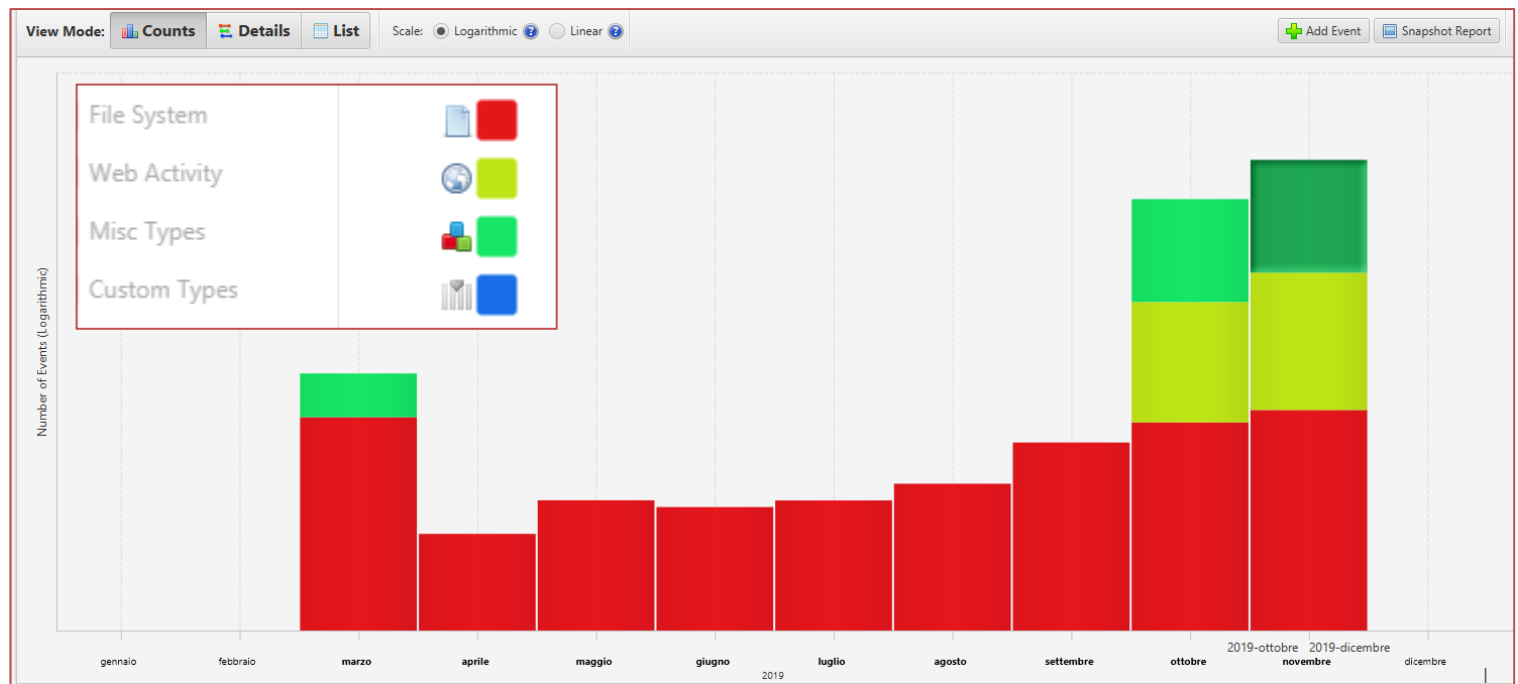
# I Toolkit

## Le viste specializzate

### TimeLine

- Visualizzazione temporale dei file

### Autopsy

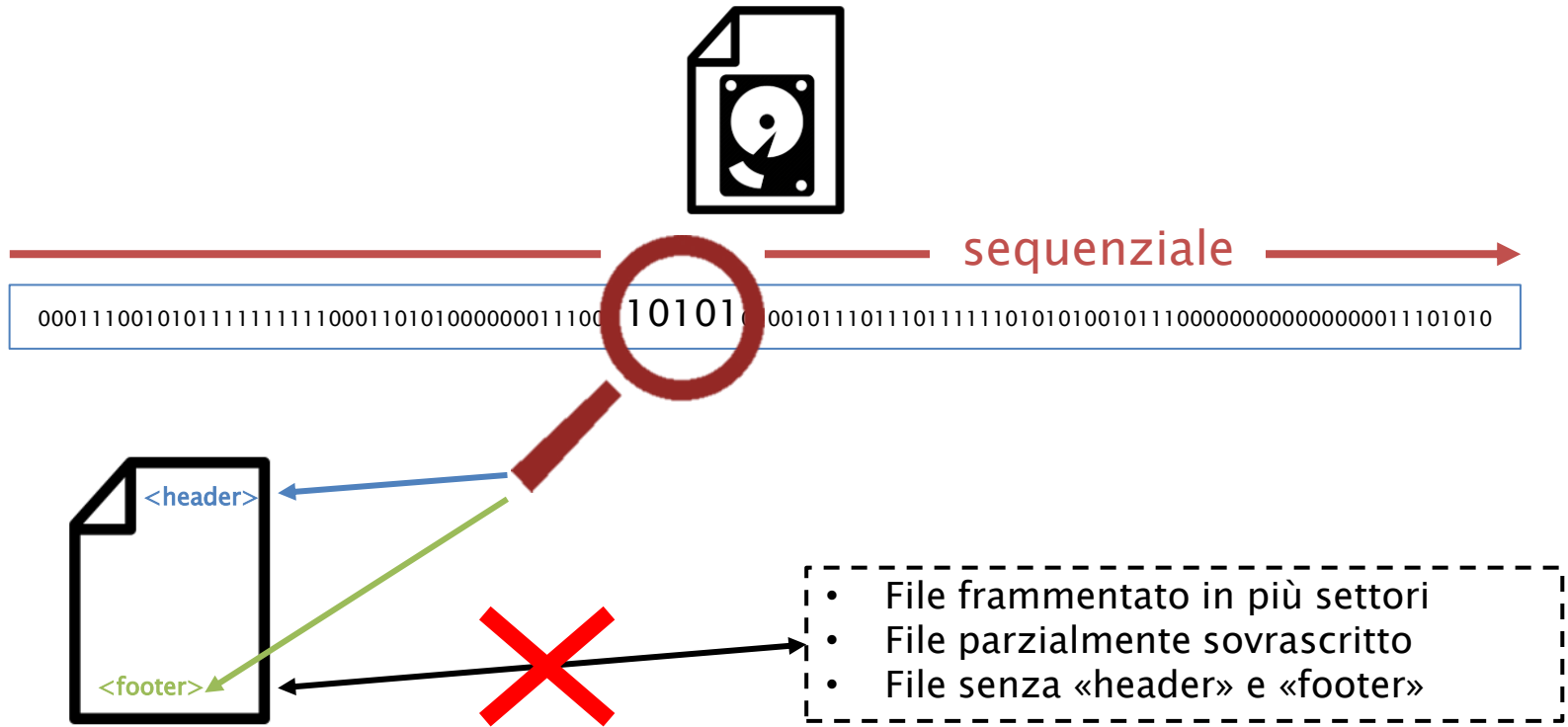


# I Toolkit

## Altri strumenti

# File Carving

- ▶ Recupero dei file non più residenti nel file system



# I Toolkit

## Altri strumenti

### Ricerche semi manuali

#### ► Ricerca tramite attributi

- Es.: immagini presenti nel profilo utente di CAIO che si riferiscono al periodo gennaio 2019.

Filter Definition: Temp

Properties:

Name: 00 Description:

Rules: ☐ Live Preview

	Properties	Operators	Criteria
<input type="checkbox"/>	<input checked="" type="checkbox"/> Path	<input type="checkbox"/> Contains	<input type="checkbox"/> /Users/Caio/
<input type="checkbox"/>	<input checked="" type="checkbox"/> File Category	<input type="checkbox"/> Is a Member of	<input type="checkbox"/> [Graphics]
<input type="checkbox"/>	<input checked="" type="checkbox"/> Modified Date	<input type="checkbox"/> Is Between	<input type="checkbox"/> 01/01/2019 00:00:00 - 01/02/2019 00:00:00

☐ Match Any  
☒ Match All

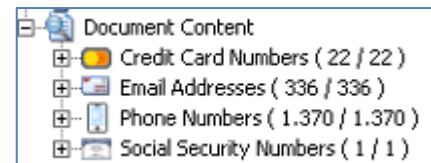
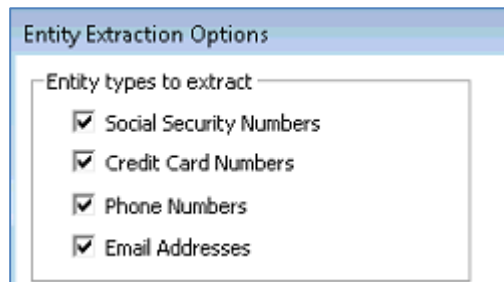
Save Close

# I Toolkit

## Altri strumenti

### Ricerche semi manuali

- ▶ **Document Content:** estrazione di determinate informazioni mediante regular expression



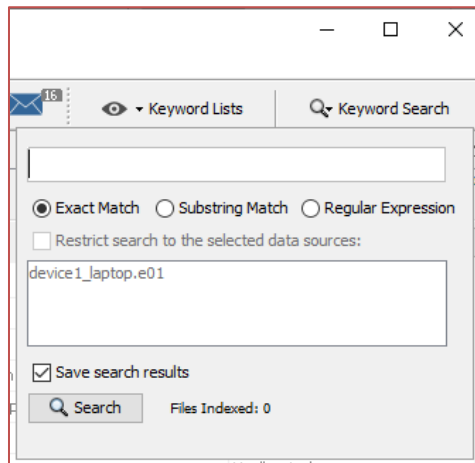
# I Toolkit

## Altri strumenti

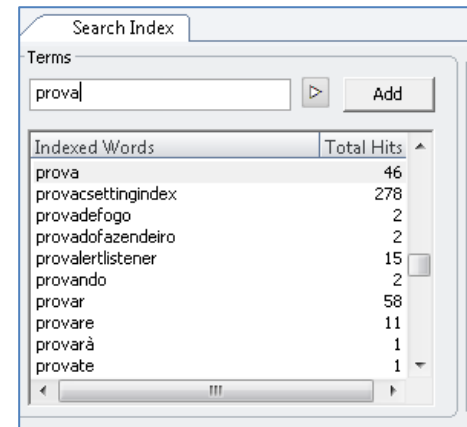
Ricerche semi manuali

- **Indexing:** ricerche di determinate parole chiave

Autopsy  
Solr



FTK  
dtSearch®





# I Toolkit

## Altri strumenti



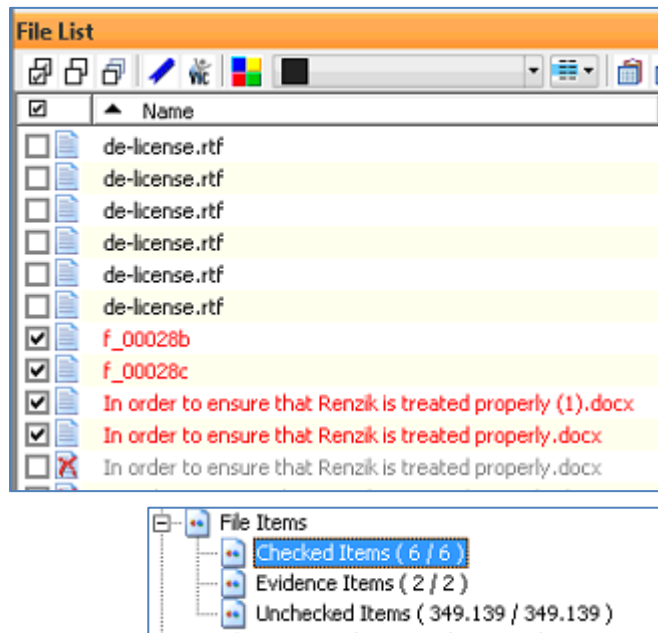
- ▶ Decrypt
- ▶ Malware Analysis
- ▶ Processing Image:
  - PhotoDNA
  - Riconoscimento Immagine/Viso
- ▶ Traduttore

# I Toolkit

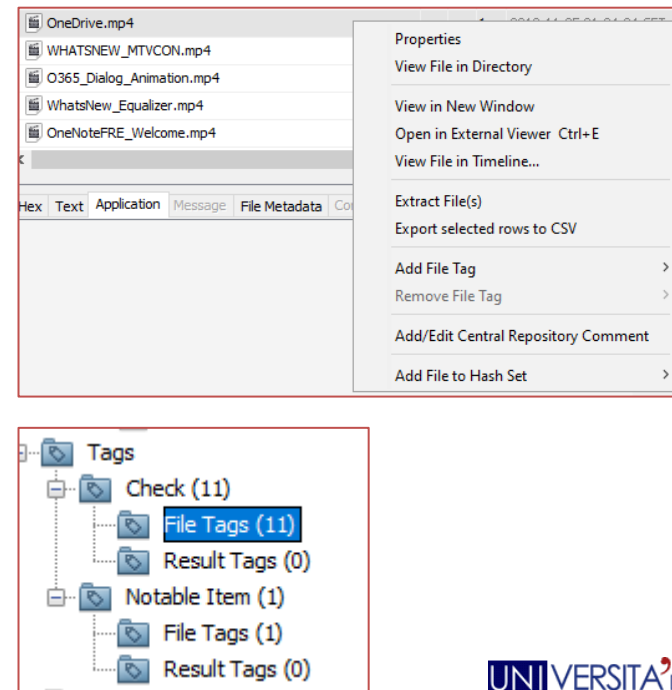
## Export/Report

- ▶ Esportare i file di interesse:
  - Etichette/Tag
  - Checkbox

### FTK



### Autopsy



# I Toolkit

## Export/Report

### Autopsy

**Report Navigation**

- Case Summary
- Hashset Hits (0)
- Keyword Hits (0)
- Tagged Files (11)
- Tagged Images (11)
- Tagged Results (0)

### Autopsy Forensic Report

HTML Report Generated on 2020/05/08 02:06:05

Case: Case1  
Number of Images: 3  
Examiner: Marco

**Image Information:**

device1\_laptop.e01

FTK

**FTK**  
CASE REPORT

**Case Summary**

- Case Information
- File Overview
- Evidence List

**Bookmarks**

**Graphics**

**Videos**

- Page 1

**File Paths**

- Checked Items

**File Properties**

- Checked Items

**Selected Registry Types**

**Case Information**

Time zone for display: ora legale Europa occidentale

<b>Version</b>	AccessData Forensic Toolkit Version: 7.2.0.4127
<b>Case Owner</b>	AD-SSRILAB\FTK
<b>Case Name</b>	case1
<b>Case Reference</b>	
<b>Case Description</b>	
<b>Report Created</b>	08/05/2020 02:05:59
<b>Agency/Company</b>	
<b>Investigator's Name</b>	
<b>Address</b>	
<b>Phone</b>	
<b>Fax</b>	
<b>Email</b>	
<b>Comments</b>	

AccessData Forensic Toolkit®

Fine seconda 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](http://www.docenti.unina.it/lorenzo.laurato)

[www.computerforensicsunina.forumcommunity.net](http://www.computerforensicsunina.forumcommunity.net)