



Corso di Digital Forensics

CdLM in Informatica

Università degli Studi di Salerno

Docente: Ugo Fiore

3 – File Recovery

- Dopo aver visto come creare immagini forensi di un supporto di memorizzazione (ad esempio, un disco fisso), ci concentreremo su come effettuare le operazioni di **file recovery** (*ripristino di file*) e **data carving** (*carving = intaglio*)
- I vari sistemi operativi, utilizzano i propri **file system**, ai fini di permettere l'**accesso**, la **memorizzazione** e la **modifica** dei dati
 - Allo stesso modo, i **supporti di memorizzazione, permettono le suddette operazioni**, in accordo al file system utilizzato

- Con l'aiuto di specifici **metadati**, il sistema operativo è in grado di **identificare la tipologia dei dati**
- I metadati contengono diverse informazioni tecniche utili, fra cui:
 - Data/ora di creazione
 - Nome del file
 - Dimensione del file
 - Ecc.
- **Grazie ai metadati** è anche possibile migliorare **l'indicizzazione e la ricerca**, nei sistemi operativi

- Senza considerare, invece, i metadati (poiché potrebbero non essere disponibili, *maggiori dettagli in seguito*), ma sfruttando alcune **caratteristiche della struttura dei file**, è possibile effettuare un processo di **recupero di dati e file (file recovery e data carving)**, dai seguenti punti:
 - **Slack space** (letteralmente, *spazio allentato*)
 - **Unallocated space** (*spazio non allocato*)
- Nelle prossime slide, vedremo quali sono le caratteristiche principali dello *slack space* e dell'*unallocated space*

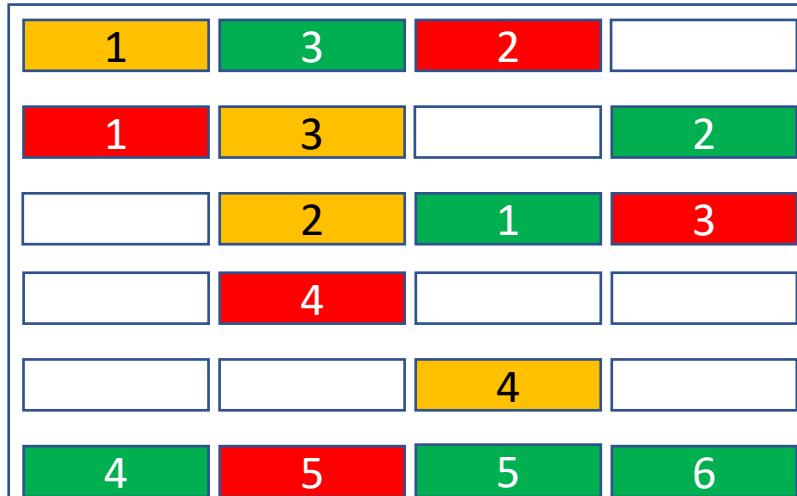
Caratteristiche Principali | Slack space | 1/4

- Il **cluster** (tipicamente di 4 KB) è l'**unità più piccola che è possibile indirizzare** da un file system
- Per la memorizzazione di un file possono servire più cluster

Caratteristiche Principali | Slack space | 1/4

- Il **cluster** (tipicamente di 4 KB) è l'unità più piccola che è possibile indirizzare da un file system
- Per la memorizzazione di un file **possono servire più cluster**

Esempio (Grafico)



- Ogni rettangolo rappresenta un cluster
- I cluster bianchi non sono allocati
- Nei cluster aventi lo stesso colore è memorizzato lo stesso file, esempio:
 - *File 1* (cluster in **ocra**)
 - *File 2* (cluster in **verde**)
 - *File 3* (cluster in **rosso**)

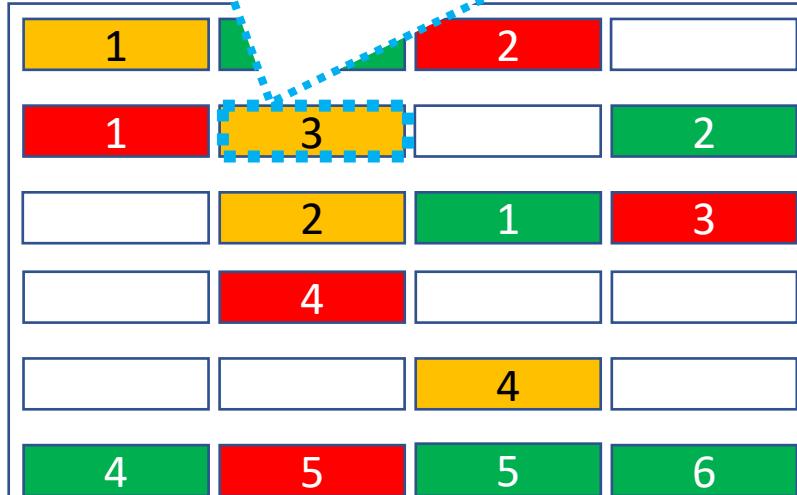
Nozioni Introduttive | 5/15

Caratteristiche Principali | Slack space | 1/4

Ad ogni cluster colorato, è associato un numero, il quale indica la parte di file memorizzata da tale cluster

Ad esempio, il *cluster evidenziato* è riferito alla parte 3, del *File 1*

Esempio (Grajico)



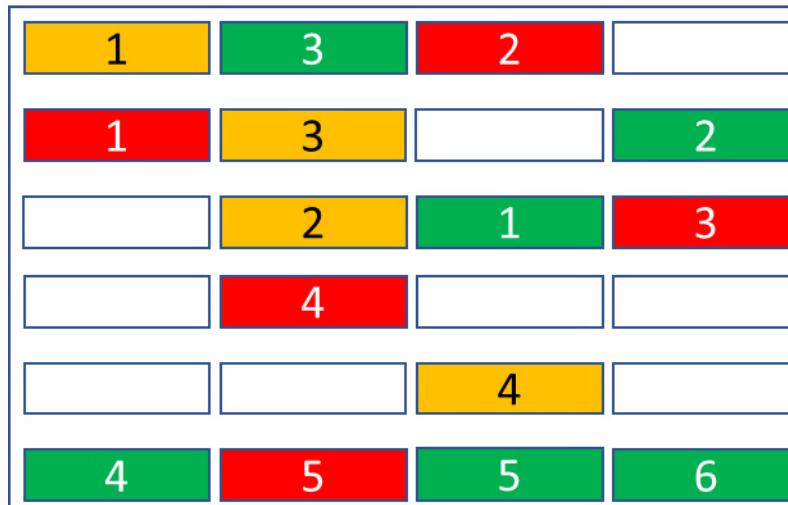
- Ogni rettangolo rappresenta un cluster
- I cluster bianchi non sono allocati
- Nei cluster aventi lo stesso colore è memorizzato lo stesso file, esempio:
 - *File 1* (cluster in **ocra**)
 - *File 2* (cluster in **verde**)
 - *File 3* (cluster in **rosso**)

Caratteristiche Principali | Slack space | 2/4

- Il **cluster** (tipicamente di 4 KB) è l'unità più piccola che è possibile indirizzare da un file system
- Per la memorizzazione di un file possono servire più cluster
 - **OSSERVAZIONE:** Il cluster che memorizza l'ultima parte di un file, potrebbe essere non completamente utilizzato
- Lo spazio che intercorre dalla **fine del file** alla **fine dell'ultimo cluster** è chiamato **slack space**
 - *Esempio (grafico) nelle prossime slide*

Caratteristiche Principali | Slack space | 2/4

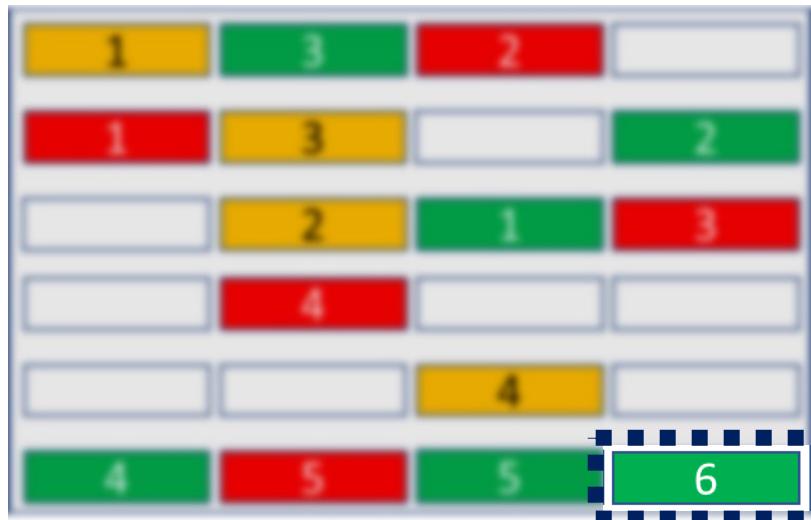
Esempio (Grafico)



- Consideriamo, ad esempio, il cluster **6** (in **verde**), il quale memorizza l'ultima parte del File 2
- Supponiamo che i dati dell'ultima parte del *File 2*, occupino solo parzialmente il suddetto cluster

Caratteristiche Principali | Slack space | 2/4

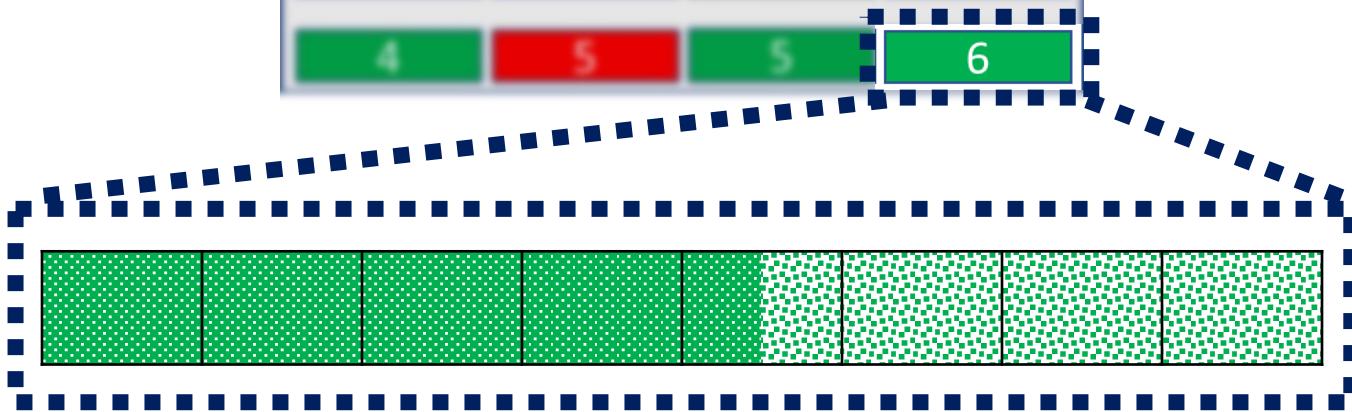
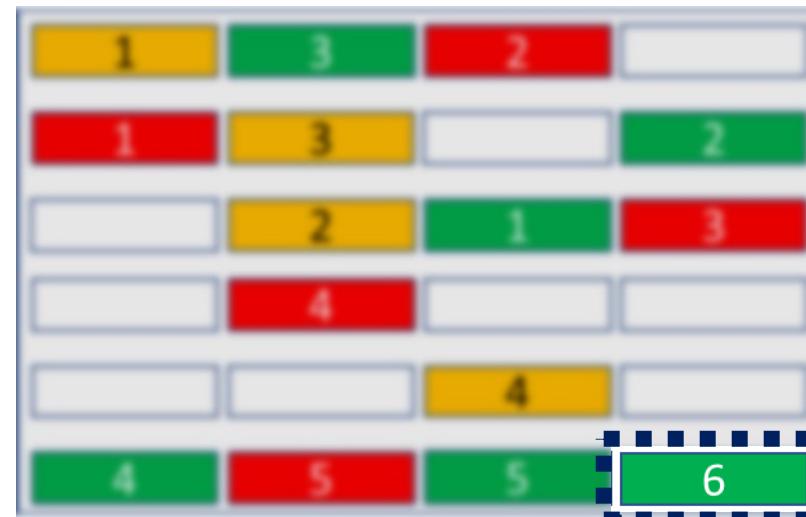
Esempio (Grafico)



- Consideriamo, ad esempio, il cluster 6 (in verde), il quale memorizza l'ultima parte del *File 2*
- Supponiamo che i dati dell'ultima parte del *File 2*, occupino solo parzialmente il suddetto cluster

Caratteristiche Principali | Slack space | 2/4

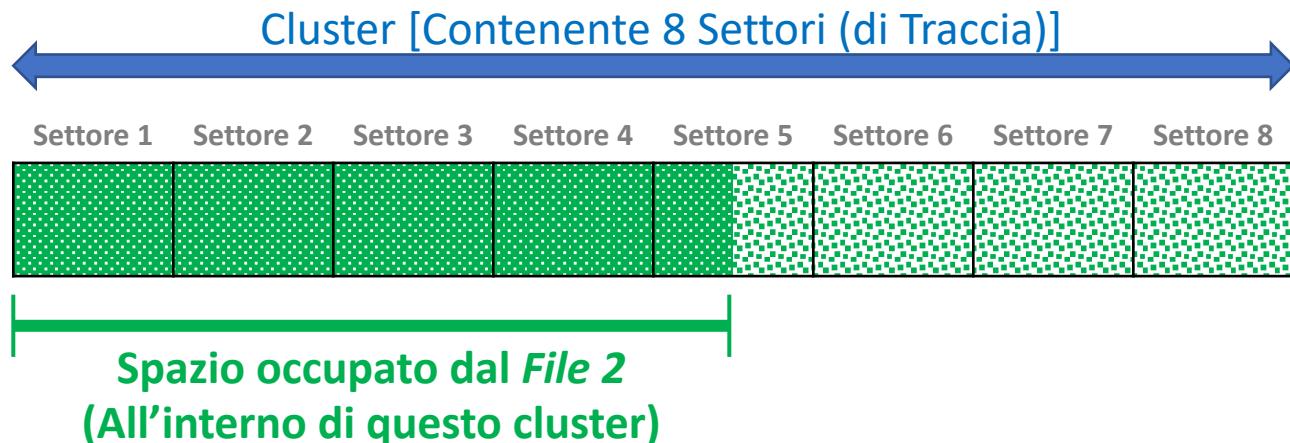
Esempio (Grafico)



Nozioni Introduttive | 5/15

Caratteristiche Principali | Slack space | 3/4

Esempio (Grafico)

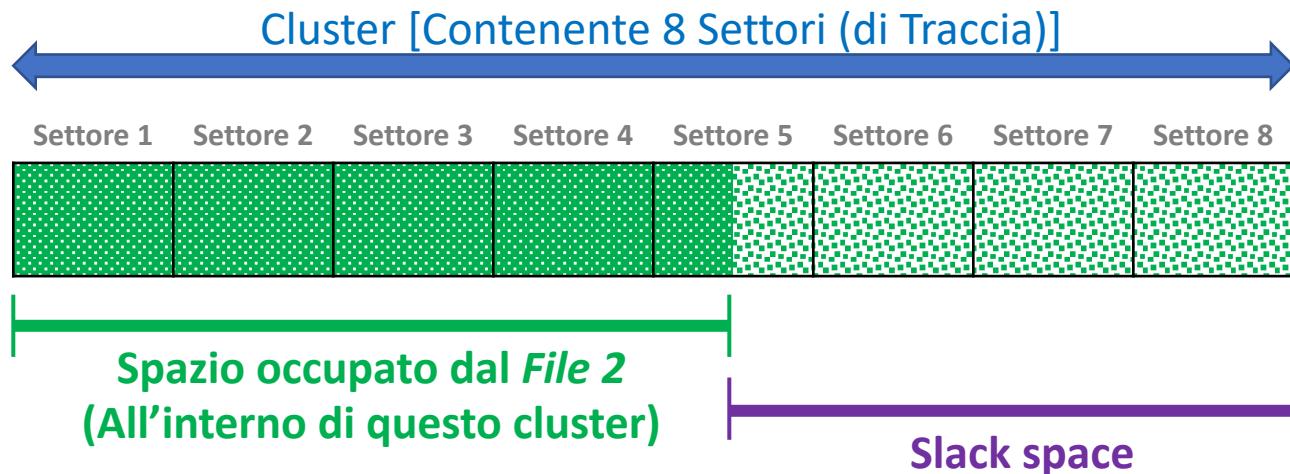


Ingrandimento del cluster 6 (in verde), relativo al *File 2*

Nozioni Introduttive | 5/15

Caratteristiche Principali | Slack space | 3/4

Esempio (Grafico)



Ingrandimento del cluster 6 (in verde), relativo al File 2

Caratteristiche Principali | Slack space | 4/4

- Il **cluster** (tipicamente di 4 KB) è l'unità più piccola che è possibile indirizzare da un file system
- Per la memorizzazione di un file possono servire più cluster
 - **OSSERVAZIONE:** Il cluster che memorizza l'ultima parte di un file, potrebbe essere non completamente utilizzato
- Lo spazio che intercorre dalla fine del file alla fine dell'ultimo cluster è chiamato **slack space**

Lo **slack space** è importante nelle indagini forensi, poiché, al suo interno possono **esservi dati** appartenenti a **file cancellati** precedentemente

Caratteristiche Principali | Unallocated space

- Quando un **file** viene **eliminato**, i **cluster allocati** per esso, **divengono non allocati** (si tratta quindi di **spazio non allocato** o **unallocated space**)
 - Tali cluster sono quindi contrassegnati come **liberi (non allocati/unallocated)** e **non saranno modificati finché non saranno riallocati**, per memorizzare il contenuto di altri file
 - Tramite i metadati, qualora disponibili, è possibile comunque provare a recuperare file eliminati
 - Ad esempio, in NTFS, quando un file viene eliminato, la relativa entry nella Master File Table (MFT) viene contrassegnata come **unallocated**
 - Tuttavia, tale entry conterrà ancora i metadati relativi al file eliminato, finché non verrà sovrascritta
 - L'**unallocated space** diviene quindi **potenzialmente importante**, per quanto riguarda la digital forensics

Nozioni Introduttive | 8/15



- All'interno dell'unallocated space, i metadati dei file, però, potrebbero non essere presenti o potrebbero essere corrotti
 - Ad esempio, in NTFS, i metadati sono contenuti nelle entry della MFT, le quali, molto probabilmente, sono state riutilizzate per altri file (di conseguenza, i metadati sono stati sovrascritti)
 - In questi scenari, è comunque possibile sfruttare alcune caratteristiche strutturali del contenuto dei file (nello specifico, gli *header* e/o i *footer*), al fine di provare a ricostruire i file eliminati
 - Queste considerazioni, sono sfruttate nei processi di data carving e file recovery



Nozioni Introduttive | 8/15

HEADER E FOOTER DI UN FILE

Ogni file appartiene generalmente ad una certa tipologia (ad esempio, documenti di Microsoft Word, fogli di calcolo di Microsoft Excel, filmati AVI, ecc.)

La tipologia di un file non è identificata dall'estensione del file stesso (ad esempio, .docx, .xlsx, .avi, ecc.)

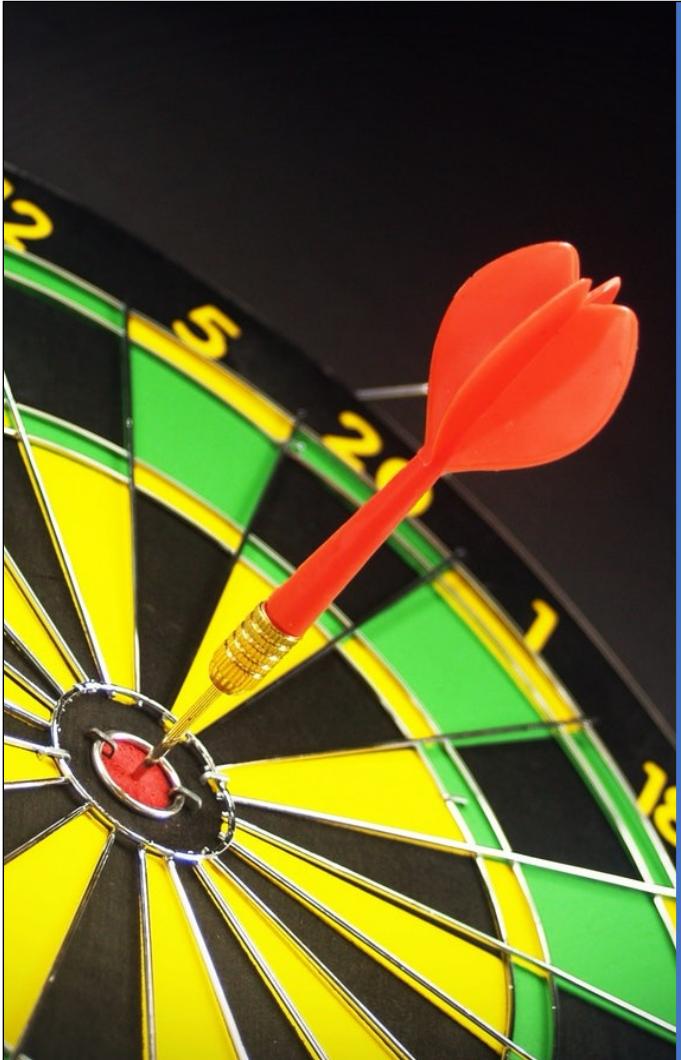
Nel contenuto di un file, sono presenti un **header** (ovvero, una sequenza di particolari byte, all'inizio del file; *alcuni esempi di header verranno riportati nelle prossime slide*) e un **footer** (una sequenza di particolari byte, alla fine del file; **NOTA:** il footer può essere generalmente omesso), i quali caratterizzano la tipologia di tale file

specifico, gli **header** e/o i **footer**), al fine di provare a ricostruire i file eliminati

- Queste considerazioni, sono sfruttate nei processi di data carving e file recovery



Nozioni Introduttive | 9/15



OBIETTIVI

I processi di **file recovery** e **data carving** consistono proprio nell'individuare ed estrarre dati significativi dallo *slack space* e dall'*unallocated space*

Nozioni Introduttive | 10/15

- Per cui, **anche in caso di modifica dell'estensione del file** (ad esempio, da .jpg a .ppp), tramite l'analisi dell'header e/o del footer **è possibile provare ad effettuare il recupero**

- Per cui, anche in caso di modifica dell'estensione del file (ad esempio, da .jpg a .ppp), tramite l'analisi dell'header e/o del footer è possibile provare ad effettuare il recupero



OSSERVAZIONE 1

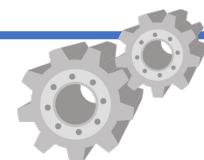
Il processo di recupero è un processo **particolarmente oneroso**,
in termini di tempo di esecuzione

- Per cui, anche in caso di modifica dell'estensione del file (ad esempio, da .jpg a .ppp), tramite l'analisi dell'header e/o del footer è possibile provare ad effettuare il recupero



OSSERVAZIONE 1

Il processo di recupero è un processo **particolarmente oneroso**,
in termini di tempo di esecuzione



OSSERVAZIONE 2

È consigliabile utilizzare **strumenti automatizzati**, al fine di
risparmiare tempo

- Per cui, anche in caso di modifica dell'estensione del file (ad esempio, da .jpg a .ppp), tramite l'analisi dell'header e/o del footer è possibile provare ad effettuare il recupero

OSSERVAZIONE 3

Può essere **particolarmente significativo**, per migliorare l'efficacia del recupero e, conseguentemente, migliorare l'investigazione, l'**utilizzo di più di un tool** di file recovery e data carving



Nozioni Introduttive | 11/15

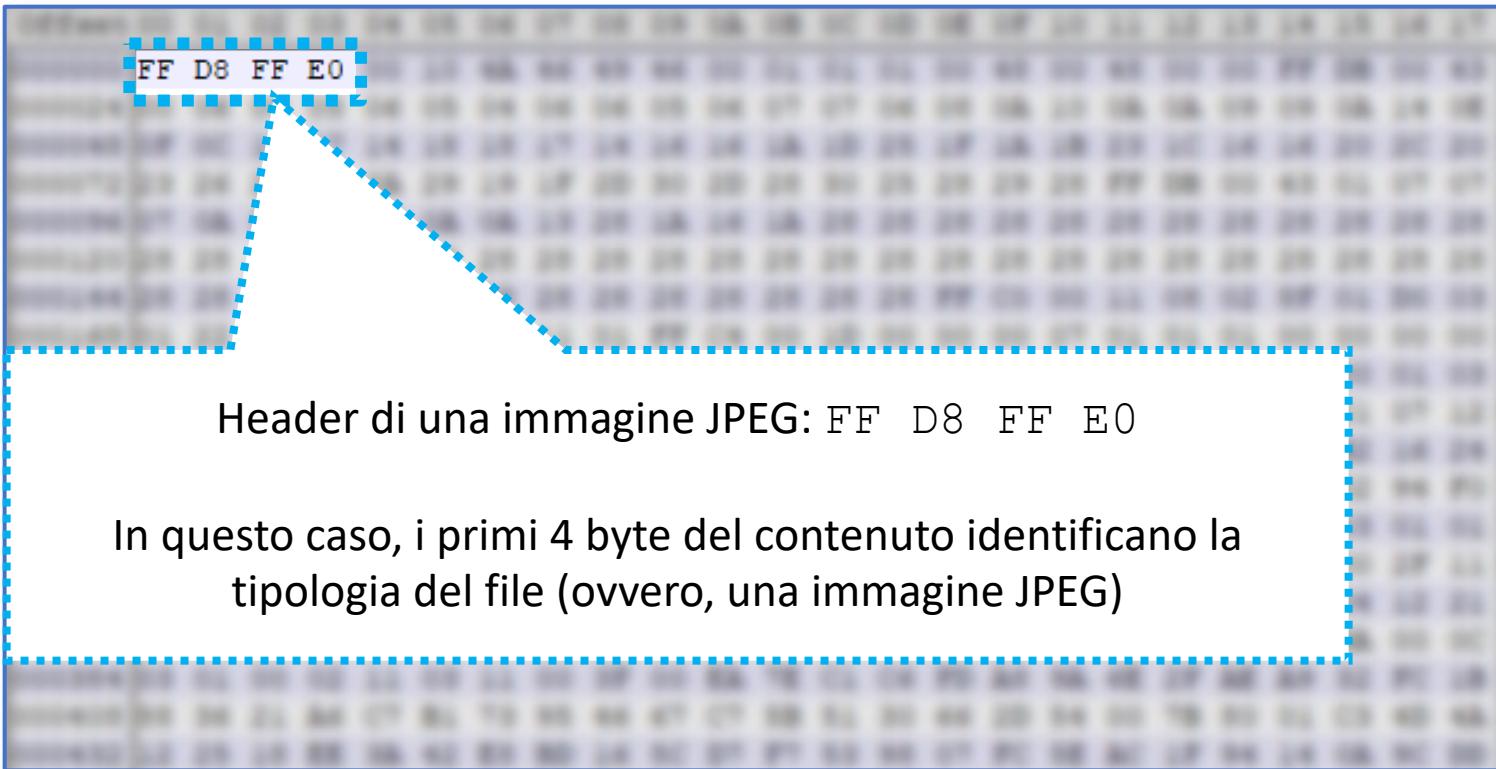
- *Esempio di Header | File JPEG (Immagine)*

Offset	00 01 02 03 04 05 06 07 08 09 0A 0B 0C 0D 0E 0F 10 11 12 13 14 15 16 17
000000	FF D8 FF E0 00 10 4A 46 49 46 00 01 01 01 01 00 48 00 48 00 00 FF DB 00 43
000024	00 06 04 05 06 05 04 06 06 05 06 07 07 06 08 0A 10 0A 0A 09 09 0A 14 0E
000048	0F 0C 10 17 14 18 18 17 14 16 16 1A 1D 25 1F 1A 1B 23 1C 16 16 20 2C 20
000072	23 26 27 29 2A 29 19 1F 2D 30 2D 28 30 25 28 29 28 FF DB 00 43 01 07 07
000096	07 0A 08 0A 13 0A 0A 13 28 1A 16 1A 28 28 28 28 28 28 28 28 28 28 28 28 28
000120	28 28
000144	28 28 28 28 28 28 28 28 28 28 28 28 28 28 28 28 FF C0 00 11 08 02 8F 01 D0 03
000168	01 22 00 02 11 01 03 11 01 FF C4 00 1D 00 00 00 07 01 01 01 00 00 00 00
000192	00 00 00 00 00 00 00 01 02 03 04 05 06 08 07 09 FF C4 00 5C 10 00 01 03
000216	02 03 04 05 04 0B 0B 09 06 06 02 01 05 01 00 02 03 04 11 05 06 21 07 12
000240	31 41 13 22 51 61 71 14 32 91 B1 08 15 17 23 33 52 72 73 81 A1 B2 16 24
000264	25 34 35 36 42 56 62 93 C1 26 37 53 55 63 74 92 C2 D1 18 43 45 82 94 F0
000288	44 46 54 95 A2 D2 27 F1 83 57 75 85 A4 E1 FF C4 00 1B 01 00 02 03 01 01
000312	01 00 00 00 00 00 00 00 00 00 01 02 03 04 05 06 07 FF C4 00 2F 11
000336	00 02 02 01 04 01 03 03 05 00 03 01 00 00 00 00 01 02 03 11 04 12 21
000360	31 05 13 32 41 06 22 51 14 15 61 16 42 71 91 A1 23 52 C1 F1 FF DA 00 0C
000384	03 01 00 02 11 03 11 00 3F 00 EA 7E C1 C6 FD A8 9A 6E 2F AE A9 32 FC 1B
000408	88 36 21 A6 C7 B1 73 95 46 67 C7 5B 51 30 66 2D 54 00 7B 80 01 C3 4D 4A
000432	12 25 18 EE 3A 42 E8 BD 16 5C D7 F7 53 98 07 FC 5E AC 1F 94 14 0A 9C DD

Rappresentazione esadecimale byte per byte, del
contenuto di un file

Nozioni Introduttive | 11/15

- *Esempio di Header | File JPEG (Immagine)*



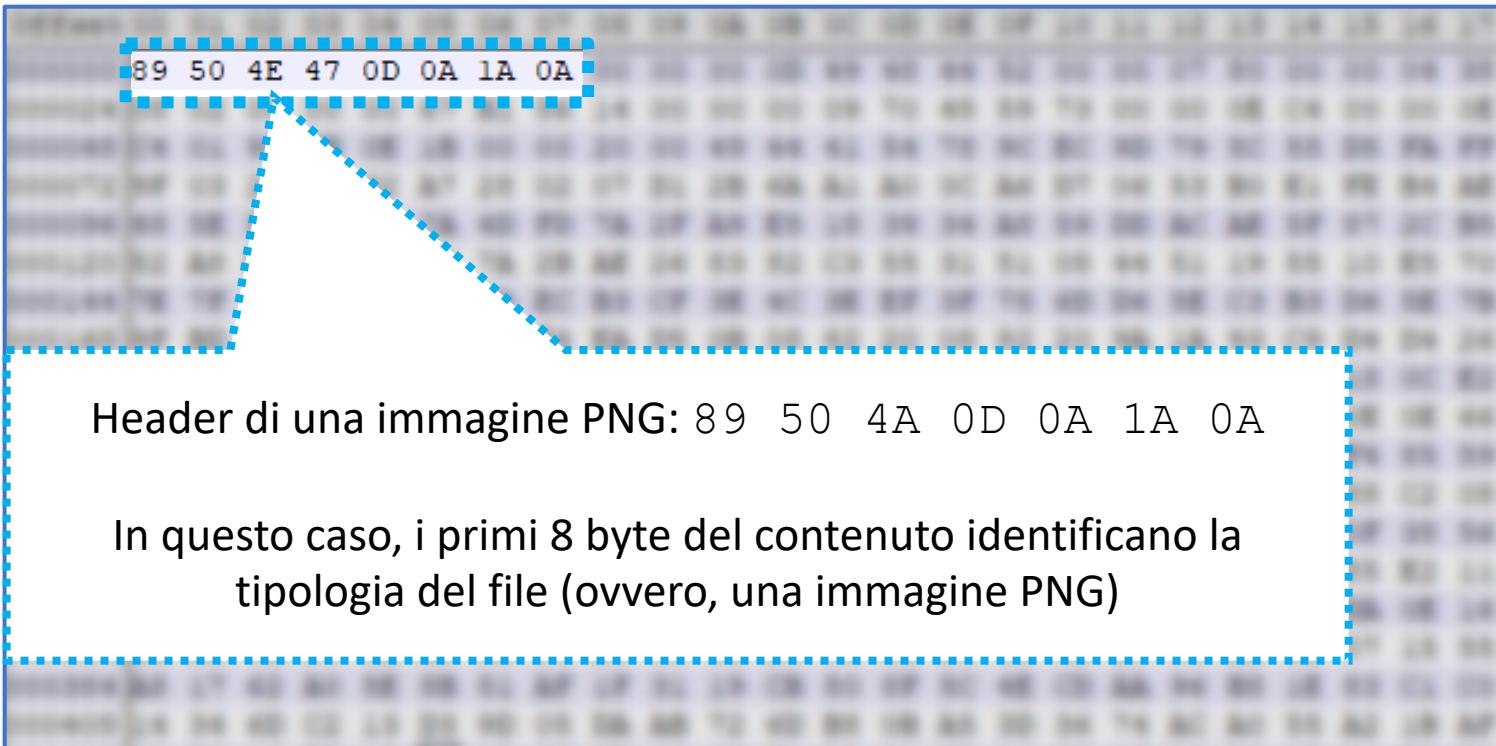
Nozioni Introduttive | 12/15

- *Esempio di Header | File PNG (Immagine)*

Offset	00	01	02	03	04	05	06	07	08	09	0A	0B	0C	0D	0E	0F	10	11	12	13	14	15	16	17	
000000	89	50	4E	47	0D	0A	1A	0A	00	00	00	0D	49	48	44	52	00	00	07	80	00	00	04	38	
000024	08	02	00	00	00	67	B1	56	14	00	00	00	09	70	48	59	73	00	00	0E	C4	00	00	0E	
000048	C4	01	95	2B	0E	1B	00	00	20	00	49	44	41	54	78	9C	EC	9D	79	5C	55	D5	FA	FF	
000072	9F	03	2A	88	32	A7	28	02	07	D1	2B	6A	A1	A0	0C	A6	D7	06	53	B0	E1	FE	B4	AE	
000096	48	5E	87	34	F4	7A	4D	FD	7A	2F	A9	E5	18	39	34	A8	59	DD	AC	AE	5F	87	2C	B5	
000120	52	A8	B4	6F	65	92	7A	2B	AE	26	83	82	C3	55	31	51	08	44	51	19	55	10	E5	70	
000144	7E	7F	3C	B2	5A	EC	E9	EC	B3	CF	3E	4C	3E	EF	3F	78	6D	D6	5E	C3	B3	D6	5E	7B	
000168	9F	BD	3F	FB	D9	CF	32	F4	EA	D5	0B	08	82	20	08	82	20	9A	1A	93	C9	D4	D4	26	
000192	B4	6C	1C	1D	1D	9B	DA	04	82	20	08	82	20	AC	83	BF	FF	71	70	70	30	18	0C	E2	
000216	3C	75	75	75	66	B3	59	97	1F	7A	73	3D	72	6D	A9	01	ED	31	18	0C	0E	0E	0E	66	
000240	B3	B9	AE	AE	8E	ED	C2	44	85	A6	0D	06	03	B6	CB	17	44	7B	E4	0A	2A	F4	85	59	
000264	82	29	CA	03	A8	90	41	0D	75	75	75	75	75	8E	8E	8E	82	1A	58	E5	88	C2	08		
000288	08	32	B3	A3	60	AD	49	E2	8E	AB	6C	5D	A1	36	F6	AF	F2	10	E1	20	28	0F	38	56	
000312	68	CB	50	B3	93	42	6E	CE	0B	6C	B6	68	B6	C5	4A	F0	FC	E2	67	A6	42	85	E2	11	
000336	C3	44	00	D0	70	34	19	FC	69	A5	AD	06	C9	0A	15	C6	D0	64	32	A1	B5	DA	0E	16	
000360	EB	B2	CA	FC	6D	AC	6D	80	20	08	82	20	08	82	20	08	82	20	08	E2	1E	07	15	55	
000384	A8	17	62	A0	5E	8B	51	AF	1F	31	19	CB	50	8F	5C	4E	CD	AA	96	B8	1E	83	C1	CO	
000408	14	34	6D	C2	13	D3	9D	05	DA	AB	72	6D	B8	0B	A5	3D	36	74	AC	A0	55	A2	1B	AF	

Nozioni Introduttive | 12/15

- *Esempio di Header | File PNG (Immagine)*



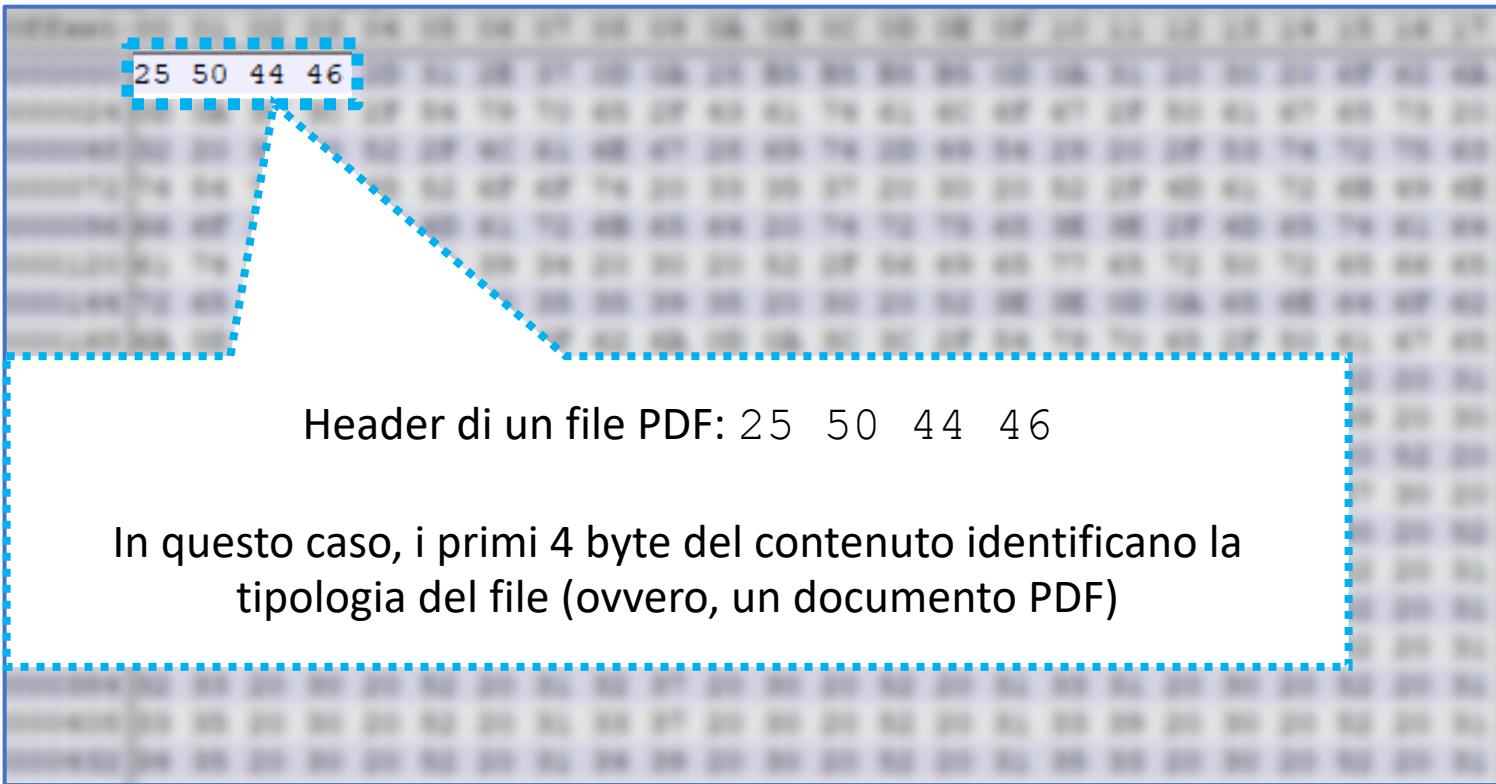
Nozioni Introduttive | 13/15

- *Esempio di Header | File PDF (Documento)*

Offset	00 01 02 03 04 05 06 07 08 09 0A 0B 0C 0D 0E 0F 10 11 12 13 14 15 16 17
000000	25 50 44 46 2D 31 2E 37 0D 0A 25 B5 B5 B5 B5 0D 0A 31 20 30 20 6F 62 6A
000024	0D 0A 3C 3C 2F 54 79 70 65 2F 43 61 74 61 6C 6F 67 2F 50 61 67 65 73 20
000048	32 20 30 20 52 2F 4C 61 6E 67 28 69 74 2D 49 54 29 20 2F 53 74 72 75 63
000072	74 54 72 65 65 52 6F 6F 74 20 33 35 37 20 30 20 52 2F 4D 61 72 6B 49 6E
000096	66 6F 3C 3C 2F 4D 61 72 6B 65 64 20 74 72 75 65 3E 3E 2F 4D 65 74 61 64
000120	61 74 61 20 35 35 39 34 20 30 20 52 2F 56 69 65 77 65 72 50 72 65 66 65
000144	72 65 6E 63 65 73 20 35 35 39 35 20 30 20 52 3E 3E 0D 0A 65 6E 64 6F 62
000168	6A 0D 0A 32 20 30 20 6F 62 6A 0D 0A 3C 3C 2F 54 79 70 65 2F 50 61 67 65
000192	73 2F 43 6F 75 6E 74 20 39 39 2F 4B 69 64 73 5B 20 33 20 30 20 52 20 31
000216	36 20 30 20 52 20 32 33 20 30 20 52 20 32 35 20 30 20 52 20 32 39 20 30
000240	20 52 20 33 31 20 30 20 52 20 35 30 20 30 20 52 20 35 33 20 30 20 52 20
000264	36 30 20 30 20 52 20 36 34 20 30 20 52 20 36 37 20 30 20 52 20 37 30 20
000288	30 20 52 20 37 34 20 30 20 52 20 37 39 20 30 20 52 20 38 33 20 30 20 52
000312	20 39 35 20 30 20 52 20 39 37 20 30 20 52 20 31 30 30 20 30 20 52 20 31
000336	30 34 20 30 20 52 20 31 30 39 20 30 20 52 20 31 31 31 20 30 20 52 20 31
000360	31 35 20 30 20 52 20 31 31 39 20 30 20 52 20 31 32 31 20 30 20 52 20 31
000384	32 33 20 30 20 52 20 31 32 37 20 30 20 52 20 31 33 31 20 30 20 52 20 31
000408	33 35 20 30 20 52 20 31 33 37 20 30 20 52 20 31 33 39 20 30 20 52 20 31
000432	34 35 20 30 20 52 20 31 34 39 20 30 20 52 20 31 35 33 20 30 20 52 20 31

Nozioni Introduttive | 13/15

- *Esempio di Header | File PDF (Documento)*



Nozioni Introduttive | 14/15

- *Header di file | Online | 1/2*
 - <https://www.filesignatures.net/>

The screenshot shows the homepage of File Signatures. The title "File Signatures" is at the top, followed by a binary string and some hex values. Below is a navigation bar with links: Search, All Signatures, Submit Sigs, My Favorites, and Control Panel. The main area contains a search form with a checkbox for "Disable autocomplete", a text input field, and a "submit" button. Below the input field are two radio buttons: "Extension" and "Signature". A dashed blue line connects the bottom right corner of the QR code area to the "Extension" radio button on the website's search form.

Ricerca della tipologia di un file, mediante la sua **estensione** o
mediante il suo **header/footer**

Nozioni Introduttive | 15/15

- *Header di file | Online | 2/2*
 - <https://www.filesignatures.net/>

The screenshot shows the homepage of File Signatures. At the top, there is a navigation bar with links for Search, All Signatures, Submit Sigs, My Favorites, and Control Panel. Below the navigation bar is a search form with a text input field containing the hex string "89504E470D0A1A0A". There is also a checkbox labeled "Disable autocomplete" and a "submit" button. Below the search form, there is a radio button group for "Extension" and "Signature", with "Signature" selected. The main content area displays a table titled "1 Results Found For 89504E470D0A1A0A". The table has three columns: Extension, Signature, and Description. One result is listed:

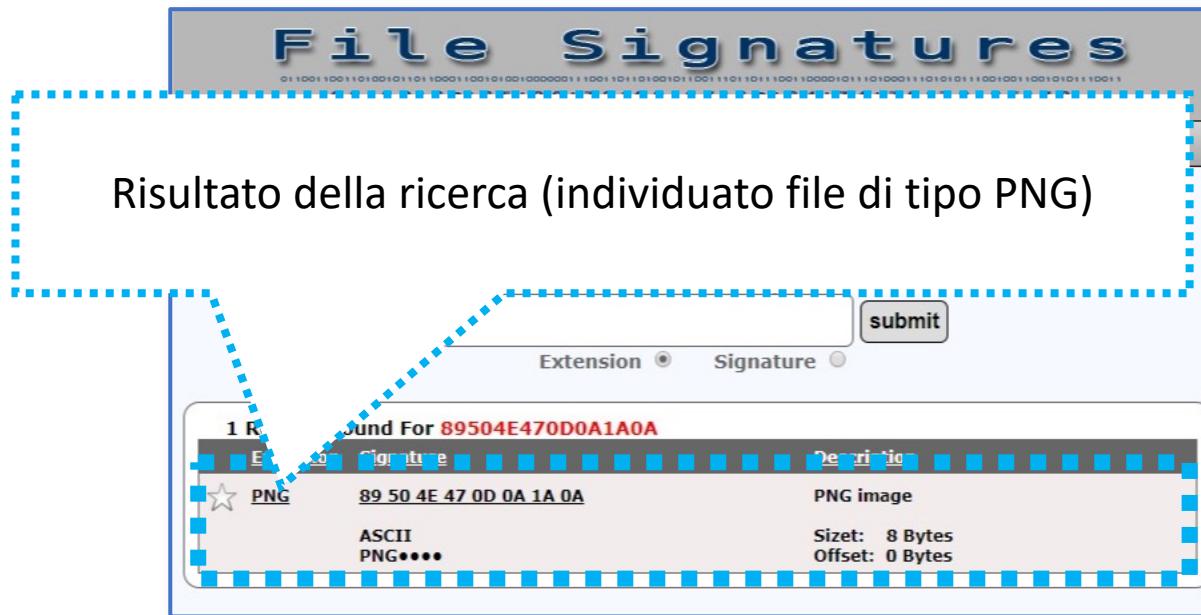
Extension	Signature	Description
PNG	89 50 4E 47 0D 0A 1A 0A	PNG image
	ASCII PNG.....	Size: 8 Bytes Offset: 0 Bytes

- Stringa di ricerca: 89504E470D0A1A0A
 - 8 bytes rappresentati in esadecimale (senza spazi)
- Opzione di ricerca: Signature

File Recovery e Data Carving

Concetti Preliminari | 14/14

- *Header di file | Online | 2/2*
 - <https://www.filesignatures.net/>



Il tool Foremost

Il tool Foremost

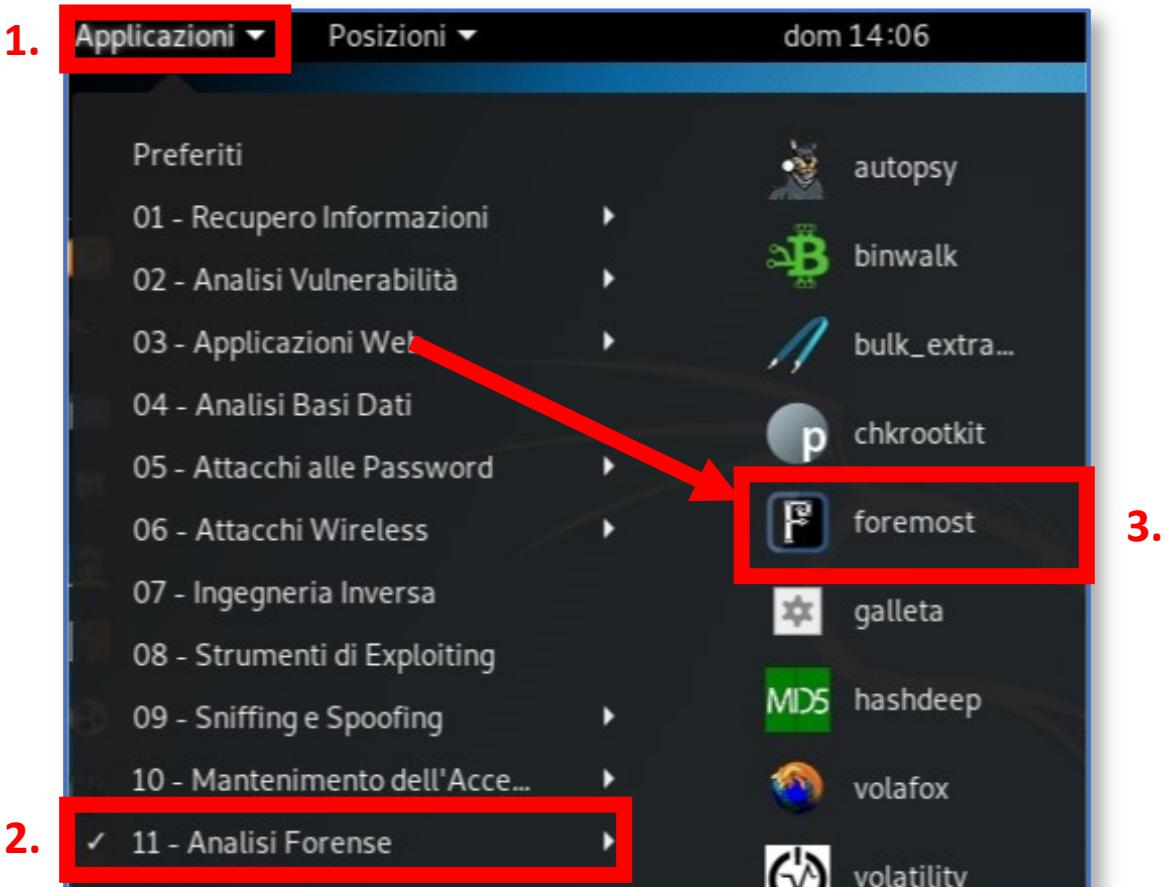
Caratteristiche

- Il tool **Foremost** è presente in Kali Linux
- **Open-Source** per sistemi Linux-based
- Utilizzabile tramite **linea di comando** (CLI – Command Line Interface)
- Utilizzabile per il recupero dei file
 - È in grado di **leggere l'header e/o il footer** dei file, al fine di **individuarne la relativa tipologia e recuperarli**
- **Semplice ed efficace**
- Maggiori Dettagli:
 - <http://foremost.sourceforge.net/>

Il tool Foremost

Avvio del Tool | 1/2

- Avvio tramite Interfaccia Grafica



Il tool Foremost

Avvio del Tool | 2/2

- *Avvio tramite Interfaccia Grafica*

```
foremost version 1.5.7 by Jesse Kornblum, Kris Kendall, and Nick Mikus.  
$ foremost [-v|-V|-h|-T|-Q|-q|-a|-w-d] [-t <type>] [-s <blocks>] [-k <size>]  
      [-b <size>] [-c <file>] [-o <dir>] [-i <file>]  
  
-V  - display copyright information and exit  
-t  - specify file type. (-t jpeg,pdf ...)  
-d  - turn on indirect block detection (for UNIX file-systems)  
-i  - specify input file (default is stdin)  
-a  - Write all headers, perform no error detection (corrupted files)  
-w  - Only write the audit file, do not write any detected files to the disk  
-o  - set output directory (defaults to output)  
-c  - set configuration file to use (defaults to foremost.conf)  
-q  - enables quick mode. Search are performed on 512 byte boundaries.  
-Q  - enables quiet mode. Suppress output messages.  
-v  - verbose mode. Logs all messages to screen  
root@kali:~# █
```

- All'avvio di Foremost, si avvierà il terminale di Kali Linux e ci verranno mostrate informazioni sulla versione (nell'esempio, la versione è la 1.5.7) e alcune delle principali opzioni (ad esempio, `-i`, `-o`, ecc.)

Il tool Foremost

Utilizzo su Kali Linux | 1/3

- Per avere maggiori informazioni su come utilizzare il tool Foremost, è possibile visionare il relativo manuale, mediante il seguente comando:

```
man foremost
```

- L'output del manuale è suddiviso in varie sezioni, fra cui, è possibile individuare le seguenti:
 - Sintassi
 - File supportati
 - Opzioni
 - Esempi

Il tool Foremost

Utilizzo su Kali Linux | 2/3

```
man foremost
```

- Sintassi

```
foremost [-h] [-v] [-d] [-vqwQT] [-b <blocksize>] [-o <dir>] [-t  
<type>] [-s <num>] [-i <file>]
```

- File supportati (*Parziale*)

```
jpg Support for the JFIF and Exif formats including implementations  
used in modern digital cameras.
```

```
gif
```

```
png
```

```
bmp Support for windows bmp format.
```

Il tool Foremost

Utilizzo su Kali Linux | 2/3

```
man foremost
```

- Opzioni (*Parziale*)

```
-h      Show a help screen and exit.  
-V      Show copyright information and exit.  
-d      Turn on indirect block detection, this works well for Unix file  
        systems.  
-T      Time stamp the output directory so you don't have to delete the  
        output dir when running multiple times.  
-v      Enables verbose mode. This causes more information regarding the  
        current state of the program to be displayed on the screen, and  
        is highly recommended.
```

- Esempi (*Parziale*)

```
Search for jpeg format skipping the first 100 blocks  
foremost -s 100 -t jpg -i image.dd
```

```
Only generate an audit file, and print to the screen (verbose mode)  
foremost -av image.dd
```

Il tool Foremost

Utilizzo su Kali Linux | 3/3

- Sintassi Semplificata (*Descrizione*)

```
foremost -i <file> -o <dir> [options]
```

Il tool Foremost

Utilizzo su Kali Linux | 3/3

- Sintassi Semplificata (*Descrizione*)

```
foremost -i <file> -o <dir> [options]
```

- **-i**: Permette di specificare il percorso del **file di input**
 - **OSSERVAZIONE**: il file di input deve essere una immagine forense, precedentemente acquisita, con gli appositi tool (ad esempio, con il tool DC3DD)

Il tool Foremost

Utilizzo su Kali Linux | 3/3

- Sintassi Semplificata (*Descrizione*)

```
foremost -i <file> -o <dir> [options]
```

- **-i**: Permette di specificare il percorso del **file di input**
 - **OSSERVAZIONE**: il file di input deve essere una immagine forense, precedentemente acquisita, con gli appositi tool (ad esempio, con il tool DC3DD)
- **-o**: Permette di specificare la directory di output, dove verranno memorizzati i file, recuperati mediante il processo di file recovering
 - *Esempio nelle prossime slide*

Il tool Foremost

Utilizzo su Kali Linux | 3/3

- Sintassi Semplificata (*Descrizione*)

```
foremost -i <file> -o <dir> [options]
```

- **-i**: Permette di specificare il percorso del **file di input**
 - **OSSERVAZIONE**: il file di input deve essere una immagine forense, precedentemente acquisita, con gli appositi tool (ad esempio, con il tool DC3DD)
- **-o**: Permette di specificare la directory di output, dove verranno memorizzati i file, recuperati mediante il processo di file recovering
 - *Esempio nelle prossime slide*
- **[options]**: Eventuali opzioni (facoltative), da specificare solo se necessarie

Il tool Foremost

Esempio di Utilizzo | 1/9

- Per effettuare un esempio di utilizzo del tool Foremost, è stata utilizzata **una immagine forense**, denominata 11-carve-fat.dd
- Tale immagine è stata creata, per fini di testing, ecc., da Nick Micus (uno dei contributor di Foremost)
 - Contiene diversi file (anche eliminati), inoltre, il **boot sector della partizione** è stato volutamente **danneggiato** (ciò rende impossibile effettuare un mounting dell'immagine, per visionarne il contenuto)
- L'immagine 11-carve-fat.dd è scaricabile gratuitamente dal seguente link (dove è possibile trovare ulteriori dettagli):
 - <http://dfft.sourceforge.net/test11/>
 - **NOTA 1:** L'immagine è scaricata in formato ZIP ed è necessario estrarla prima di procedere (dimensioni del file: ~11MB, in formato ZIP, e ~65MB una volta estratto)
 - **NOTA 2:** Il File System dell'immagine è di tipo FAT32

Il tool Foremost

Esempio di Utilizzo | 1/9

OSSERVAZIONE

Alla pagina **Digital Forensics Tool Testing Images**, ospitata su Sourceforge, al link <http://dftt.sourceforge.net/> (ottenibile anche mediante il relativo QR Code), sono presenti ulteriori immagini forensi (come si può vedere dallo screenshot), su cui è possibile effettuare testing, con il tool Foremost (e non solo)

Test Images:

1. [Extended Partition Test](#) (July '03)
2. [FAT Keyword Search Test](#) (Aug '03)
3. [NTFS Keyword Search Test #1](#) (Oct '03)
4. [EXT3FS Keyword Search Test #1](#) (Nov '03)
5. [FAT Daylight Savings Test](#) (Jan '04)
6. [FAT Undelete Test #1](#) (Feb '04)
7. [NTFS Undelete \(and leap year\) Test #1](#) (Feb '04)
8. [JPEG Search Test #1](#) (Jun '04)
9. [FAT Volume Label Test #1](#) (Aug '04)
10. [NTFS Autodetect Test #1](#) (Jan '05)
11. [Basic Data Carving Test #1](#) (Mar '05) (by Nick Mikus)
12. [Basic Data Carving Test #2](#) (Mar '05) (by Nick Mikus)
13. [Windows Memory Analysis #1](#) (Jan '06) (by Jesse Kornblum)
14. [ISO9660 Interpretation Test #1](#) (Aug '10)



Il tool Foremost

Esempio di Utilizzo | 2/9

- Per avviare il processo di recovery sull'immagine 11-carve-fat.dd, effettuiamo i seguenti step:
 1. Posizioniamoci nella cartella che contiene il file dell'immagine (ad esempio, la *Scrivania*)
 2. Digitiamo il seguente comando:

```
foremost -i 11-carve-fat.dd -o Ripristinati
```

- 3. L'output del processo verrà riportato nella cartella specificata, ovvero, Ripristinati

Il tool Foremost

Esempio di Utilizzo | 3/9

- *Processo terminato*

```
root@kali:~/Scrivania# foremost -i 11-carve-fat.dd -o Ripristinati/
Processing: 11-carve-fat.dd
| foundat=wword60.txt
[...]
root@kali:~/Scrivania#
```

Il tool Foremost

Esempio di Utilizzo | 3/9

- *Processo terminato*

```
root@kali:~/Scrivania# foremost -i 11-carve-fat.dd -o Ripristinati/
Processing: 11-carve-fat.dd
| foundat=wword60.txt
| r00(0W00kN10a0EI)0:05 0o00%0I00000~0000Ve00D@=0%80#00000000K0E^00*0) /F08/000l0f0=0
| 0 000.:I' It0000~0! 000w000<0$00x"/00WI0000Mp000000:0800>z{zq00000000ov00g00JF
QY0a5/020308+0Q0K 00y00M_000080(X00^T$003|S$002T00q0000$000uE0|:Z00hxgWI00v\00
000mT0iosk}00s0d0% 0|<.000n0AZ]0i0V00ma|000`}000000000
0// 0-102y9:0G0E0.0Y0'00000
0>02 Viene elaborato il file di input (11-carve-fat.dd)
* |
root@kali:~/Scrivania#
```

Il tool Foremost

Esempio di Utilizzo | 3/9

- *Processo terminato*

```
root@kali:~/Scrivania# foremost -i 11-carve-fat.dd -o Ripristinati/
Processing: 11-carve-fat.dd
| foundat=wword60.txt
| 050nEK0o00%0I0000~0000Ve00D@=0%80#00000000K0E^00*0) /F08/000L0F0=0
| 0 000.:I'It0y000~0|{0000000w000<0$00x"/00WI0000Mp000000:0800>z{zq00000000ov00g00JF
| QY0a5/020308+0Q0K00:[0X00o?0y00M_000080(X00^T$003|S$002T00q0000$000uE0|:Z00hxgWI00v\00
| 000mT00sk}00s0d0%0t0000/0E0
| Cestino q0|<.000n0AZ]0i0V00ma|000`}000000000
| 0~J00y9:0G0E0.0Y0'00000
| 0//)&Z007t0p+~00000000Ky0V00
| 0>0a
| *|
root@kali:~/Scrivania#
```

Nonostante i caratteri «strani» mostrati a video, il processo è terminato correttamente

Il tool Foremost

Esempio di Utilizzo | 3/9

- *Processo terminato*

```
root@kali:~/Scrivania# foremost -i 11-carve-fat.dd -o Ripristinati/
Processing: 11-carve-fat.dd
| foundat=wword60.txt
| r00(050nEK0o00%0I0000~0000Ve00D@=0%80#00
| 000.:I'It000~0|{0000000w000<0$00x"/00WI000Mp000000
QY0a5/020308+0Q0K00:[0X00o?0y00M_000080(X00^T$003|S$002T
000mT0iosk}00s0d0%0t0000/0E0
| Cestino q0|<.000n0AZ]0i0V00ma|000`0
0//)&Z007t0p+~0000000Ky0V00
0>0a
*|
root@kali:~/Scrivania#
```

OSSERVAZIONE IMPORTANTE

È necessario che la cartella di output (in questo esempio: Ripristinati) sia vuota, altrimenti verrà mostrato un messaggio di errore, simile a quello mostrato in figura:

```
root@kali:~/Scrivania# foremost -i 11-carve-fat.dd -o Ripristinati
ERROR: /root/Scrivania/Ripristinati is not empty
Please specify another directory or run with -T.
```

Il tool Foremost

Esempio di Utilizzo | 4/9

- *Processo terminato*

```
root@kali:~/Scrivania# foremost -i 11-carve-fat.dd -o Ripristinati/
Processing: 11-carve-fat.dd
| foundat=wword60.txt
[...]
root@kali:~/Scrivania#
```

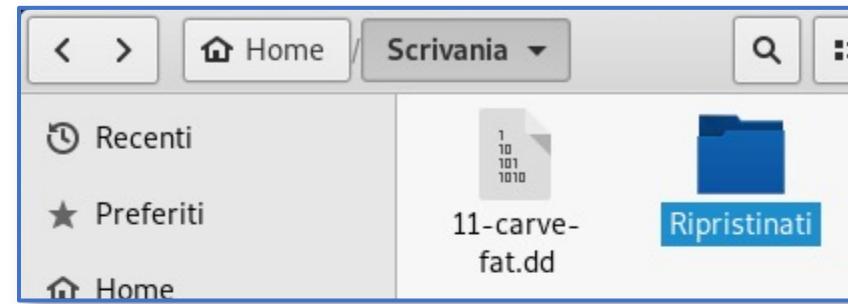
- **Durata del processo di recovering:** Date le dimensioni ridotte dell'immagine forense, in input, il processo di recovering impiegherà pochi secondi

Il tool Foremost

Esempio di Utilizzo | 5/9

- *File Prodotti | 1/5*

- Al termine del processo, sarà possibile accedere alla cartella Ripristinati (nell'esempio, sulla *Scrivania*)



Il tool Foremost

Esempio di Utilizzo | 5/9

- *File Prodotti | 1/5*

- Al termine del processo, sarà possibile accedere alla cartella Ripristinati (nell'esempio, sulla *Scrivania*)

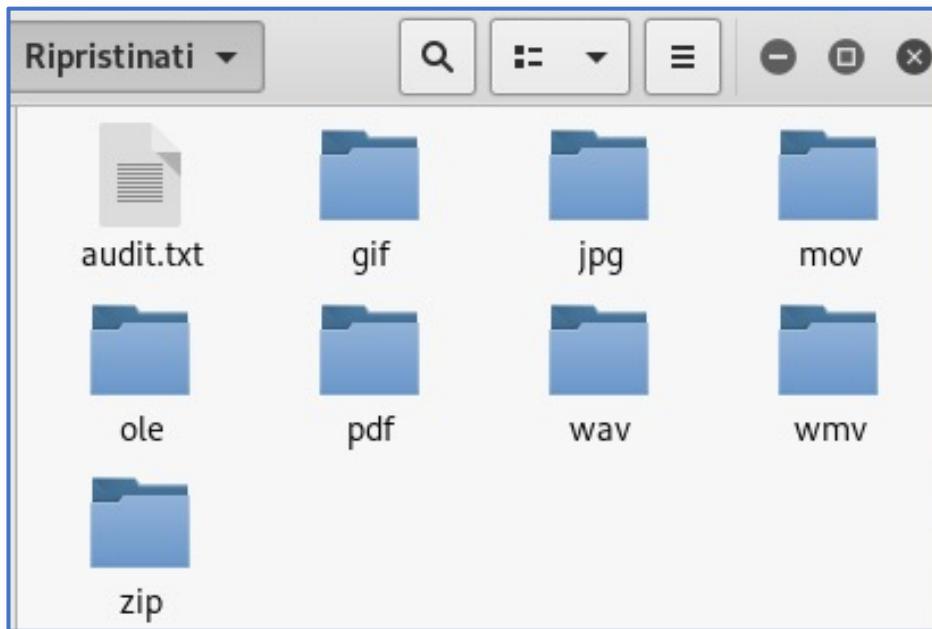


La cartella Ripristinati, generata da Foremost

Il tool Foremost

Esempio di Utilizzo | 6/9

- *File Prodotti | 2/5*
 - Il contenuto della cartella Ripristinati

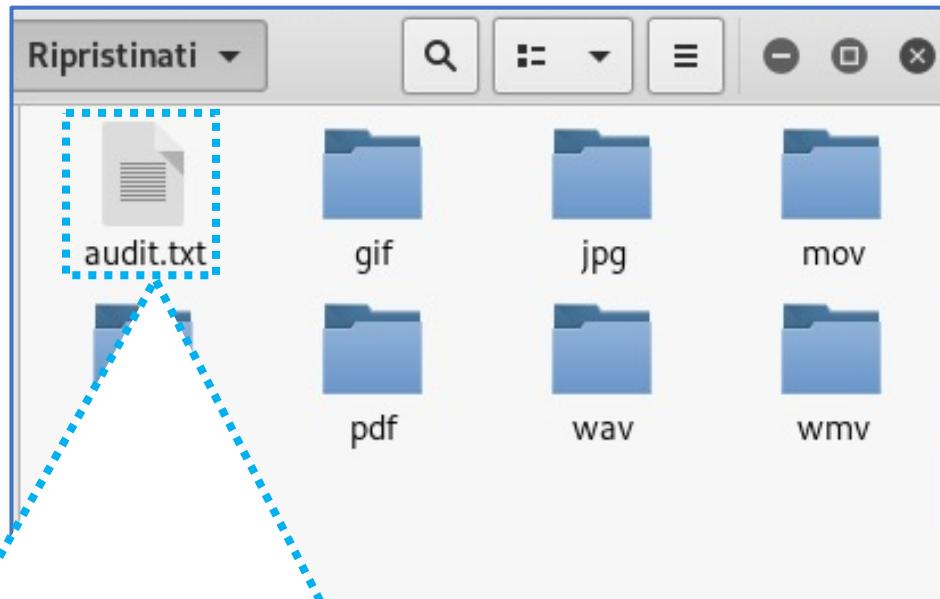


- Gli elementi ripristinati sono stati inseriti in apposite sottocartelle, in base alla loro tipologia (ad esempio, le immagini JPEG sono state inserite nella sottocartella jpg)

Il tool Foremost

Esempio di Utilizzo | 6/9

- *File Prodotti | 2/5*
 - Il contenuto della cartella Ripristinati



È possibile inoltre notare anche la presenza di un file testuale, denominato `audit.txt` (*maggiori dettagli nella prossima slide*)

Il tool Foremost

Esempio di Utilizzo | 7/9

- *File Prodotti | 3/5*

- Il contenuto (*parziale*) del file testuale audit.txt

Num	Name (bs=512)	Size	File Offset	Comment
0:	00019717.jpg	29 KB	10095104	
1:	00019777.jpg	433 KB	10125824	
2:	00020645.jpg	96 KB	10570240	
3:	00020841.gif	5 KB	10670592	(88 x 31)
4:	00000321.wmv	7 MB	164352	
5:	00021929.wmv	1012 KB	11227648	
6:	00020853.mov	537 KB	10676736	
7:	00016021.wav	311 KB	8202752	
8:	00000281.ole	20 KB	143872	
9:	00016693.ole	24 KB	8546816	
10:	00023957.ole	6 MB	12265984	
11:	00023981.zip	77 KB	12278272	
12:	00016741.pdf	1 MB	8571392	(PDF is Linearized)
13:	00019477.pdf	119 KB	9972224	

Il tool Foremost

Esempio di Utilizzo | 7/9

- *File Prodotti | 3/5*

- Il contenuto (*parziale*) del file testuale audit.txt

Num	Name (bs=512)	Size	File Offset	Comment
0:	00019717.jpg	29 KB	10095104	
1:	00019777.jpg	433 KB	10125824	
2:	00020645.jpg	96 KB	10570240	
3:	00020841.gif	5 KB	10670592	(88 x 31)
4:	00000321.wmv	7 MB	164352	
5:	00021929.wmv	1012 KB	11227648	
6:	00020853.mov	537 KB	10676736	
7:	00016021.wav	311 KB	8202752	
8:	00000281.ole	20 KB	143872	
9:	00016693.ole	24 KB	8546816	
10:	00023957.ole	6 MB	12265984	
11:	00023981.zip	77 KB	12278272	
12:	00016741.pdf	1 MB	8571392	(PDF is Linearized)
13:	00019477.pdf	119 KB	9972224	

Viene riportata **una lista dei file ripristinati**. Per ciascuno di tali file, viene riportato il **nome associato** (colonna Name), la **dimensione** (colonna Size) ed **altre informazioni** (fra cui eventuali commenti, nella colonna Comment)

Il tool Foremost

Esempio di Utilizzo | 8/9

- *File Prodotti | 4/5*

- Il contenuto (*parziale*) del file testuale audit.txt

```
14 FILES EXTRACTED

jpg:= 3
gif:= 1
wmv:= 2
mov:= 1
rif:= 1
ole:= 3
zip:= 1
pdf:= 2
```

Il tool Foremost

Esempio di Utilizzo | 8/9

- *File Prodotti | 4/5*

- Il contenuto (*parziale*) del file testuale audit.txt

```
14 FILES EXTRACTED

jpg:= 3
gif:= 1
wmv:= 2
mov:= 1
rif:= 1
ole:= 3
zip:= 1
pdf:= 2
```

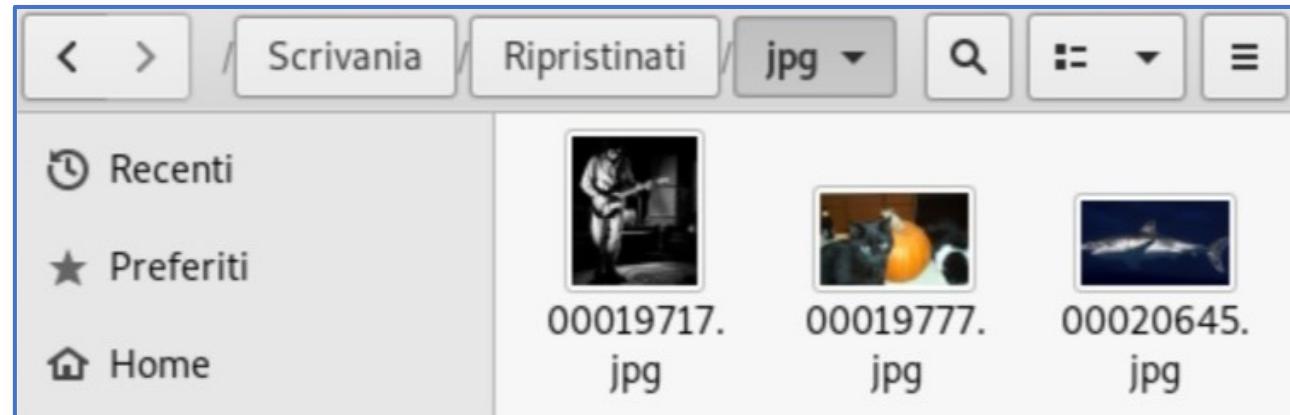
Viene poi riportata una **sintesi** dei file ripristinati, mostrando il **numero totale dei file ripristinati** ed il **numero di file ripristinati, per ciascuna categoria** (ad esempio, sono state ripristinate 3 immagine JPEG, denotate dalla voce jpg)

Il tool Foremost

Esempio di Utilizzo | 9/9

- *File Prodotti | 5/5*

- Il contenuto della cartella Ripristinati/jpg (contenente le tre immagini JPEG ripristinate)



Il tool Foremost

Osservazioni | 1/3

- **Foremost** è uno strumento **abbastanza potente ed efficace**
- L'intero **processo, nell'esempio, è durato pochi secondi** (anche testandolo su configurazioni più lente)
- Il **tempo di elaborazione** tuttavia può coprire un **arco temporale anche molto lungo**, in base alla dimensione del file di input ed altri fattori
 - Se si conosce la tipologia di file che si intende ripristinare, è possibile utilizzare l'opzione `-t` (*esempio nella prossima slide*), in modo da ridurre le tempistiche elaborate

Il tool Foremost

Osservazioni | 2/3

- *Esempio utilizzo opzione -t di Foremost*

```
root@kali:~/Scrivania# foremost -i 11-carve-fat.dd -o RiprJPEG/ -t jpeg
Processing: 11-carve-fat.dd
[*]
root@kali:~/Scrivania#
```

Il tool Foremost

Osservazioni | 2/3

- *Esempio utilizzo opzione -t di Foremost*

```
root@kali:~/Scrivania# foremost -i 11-carve-fat.dd -o RiprJPEG/ -t jpeg  
Processing: 11-carve-fat.dd  
|*|  
root@kali:~/Scrivania#
```

Con l'opzione `-t jpeg`, verranno ripristinati esclusivamente le immagini JPEG

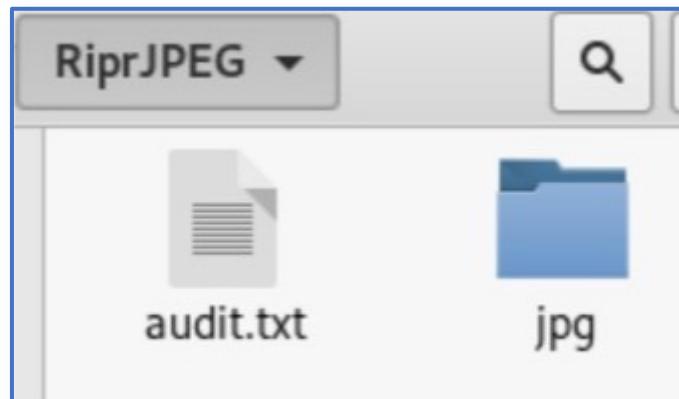
Il tool Foremost

Osservazioni | 3/3

- *Esempio utilizzo opzione -t di Foremost*

```
root@kali:~/Scrivania# foremost -i 11-carve-fat.dd -o RiprJPEG/ -t jpeg
Processing: 11-carve-fat.dd
[*]
root@kali:~/Scrivania#
```

- *File Prodotti | 1/2*



Il tool Foremost

Osservazioni | 3/3

- *Esempio utilizzo opzione -t di Foremost*

```
root@kali:~/Scrivania# foremost -i 11-carve-fat.dd -o RiprJPEG/ -t jpeg
Processing: 11-carve-fat.dd
|*|
root@kali:~/Scrivania#
```

- *File Prodotti | 2/2 | Contenuto (parziale) di audit.txt*

Num	Name (bs=512)	Size	File Offset	Comment
0:	00019717.jpg	29 KB	10095104	
1:	00019777.jpg	433 KB	10125824	
2:	00020645.jpg	96 KB	10570240	

3 FILES EXTRACTED

jpg:= 3

II tool Scalpel

Il tool Scalpel

Caratteristiche

- Il tool **Scalpel** (letteralmente, *scalpello*) è presente in Kali Linux
- **Open-Source** per sistemi Linux-based ed utilizzabile tramite **linea di comando**
- Originariamente basato su Foremost, tuttavia, significativamente più efficiente di quest'ultimo
 - Scalpel risolve i problemi di Foremost, relativi all'utilizzo elevato di CPU e RAM, durante la fase di recovering



Il tool Scalpel

Configurazione | 1/3

- A differenza di Foremost, con Scalpel **è necessario specificare le tipologie di file** che si intende cercare di ripristinare
- Scalpel deve essere configurato mediante il relativo file di configurazione, denominato `scalpel.conf`, individuabile nella directory `/etc/scalpel`

```
kali@linux# ls /etc/scalpel
scalpel.conf
#
```

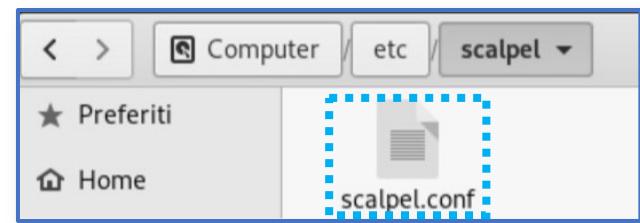


Il tool Scalpel

Configurazione | 1/3

- A differenza di Foremost, con Scalpel **è necessario specificare le tipologie di file** che si intende cercare di ripristinare
- Scalpel deve essere configurato mediante il relativo file di configurazione, denominato `scalpel.conf`, individuabile nella directory `/etc/scalpel`

```
kali@linux# ls /etc/scalpel
scalpel.conf
#
```



Il tool Scalpel

Configurazione | 2/3

- Contenuto (parziale) del file di configurazione scalpel.conf

```
# GIF and JPG files (very common)
#      gif      y      5000000          \x47\x49\x46\x38\x37\x61      \x00\x3b
#      gif      y      5000000          \x47\x49\x46\x38\x39\x61      \x00\x3b
#      jpg      y      5242880          \xff\xd8\xff???Exif        \xff\xd9
```

Il tool Scalpel

Configurazione | 2/3

- Contenuto (parziale) del file di configurazione `scalpel.conf`

```
# GIF and JPG files (very common)
#      gif      y      5000000          \x47\x49\x46\x38\x37\x61      \x00\x3b
#      gif      y      5000000          \x47\x49\x46\x38\x39\x61      \x00\x3b
#      jpg      y      5242880          \xff\xd8\xff???Exif      \xff\xd9
```

- Per ciascuna tipologia di file, `scalpel.conf` contiene le seguenti informazioni:

Il tool Scalpel

Configurazione | 2/3

- Contenuto (parziale) del file di configurazione `scalpel.conf`

```
# GIF and JPG files (very common)
# gif      y      5000000  \x47\x49\x46\x38\x37\x61  \x00\x3b
# gif      y      5000000  \x47\x49\x46\x38\x39\x61  \x00\x3b
# jpg      y      5242880  \xff\xd8\xff???Exif  \xff\xd9
```

- Per ciascuna tipologia di file, `scalpel.conf` contiene le seguenti informazioni:
 - Estensione, associata alla tipologia

Il tool Scalpel

Configurazione | 2/3

- Contenuto (parziale) del file di configurazione `scalpel.conf`

```
# GIF and JPG files (very common)
#      gif      y      5000000
#      gif      y      5000000
#      jpg      y      5242880
\x47\x49\x46\x38\x37\x61
\x47\x49\x46\x38\x39\x61
\xff\xd8\xff???Exif
\x00\x3b
\x00\x3b
\xff\xd9
```

- Per ciascuna tipologia di file, `scalpel.conf` contiene le seguenti informazioni:
 - Estensione, associata alla tipologia
 - Header rappresentato in esadecimale

Il tool Scalpel

Configurazione | 2/3

- Contenuto (parziale) del file di configurazione `scalpel.conf`

```
# GIF and JPG files (very common)
#     gif      y      5000000          \x47\x49\x46\x38\x37\x61          \x00\x3b
#     gif      y      5000000          \x47\x49\x46\x38\x39\x61          \x00\x3b
#     jpg      y      5242880          \xff\xd8\xff???Exif          \xff\xd9
```

- Per ciascuna tipologia di file, `scalpel.conf` contiene le seguenti informazioni:
 - Estensione, associata alla tipologia
 - Header rappresentato in esadecimale
 - Footer rappresentato in esadecimale

Il tool Scalpel

Configurazione | 2/3

- Contenuto (parziale) del file di configurazione scalpel.conf

```
# GIF and JPG files (very common)
# gif      y      5000000          \x47\x49\x46\x38\x37\x61      \x00\x3b
# gif      y      5000000          \x47\x49\x46\x38\x39\x61      \x00\x3b
# jpg      y      5242880         \xff\xd8\xff???Exif        \xff\xd9
```

- Per ciascuna tipologia di file, scalpel.conf contiene le seguenti informazioni:
 - Estensione, associata alla tipologia
 - Header rappresentato in esadecimale
 - Footer rappresentato in esadecimale
- **OSSERVAZIONE IMPORTANTE:** Tutte le tipologie di file sono **commentate** (lo si denota dal carattere #), pertanto, è strettamente necessario rimuovere i commenti (rimuovendo il carattere #) per almeno una tipologia

Il tool Scalpel

Configurazione | 2/3

Qualora non venisse modificato il file `scalpel.conf`, verrebbe fornito un errore, simile al seguente:

```
root@kali:~/Scrivania# scalpel 11-carve-fat.dd
Scalpel version 1.60
Written by Golden G. Richard III, based on Foremost 0.69.

Opening target "/root/Scrivania/11-carve-fat.dd"

ERROR: The configuration file didn't specify any file types to carve.
(If you're using the default configuration file, you'll have to
uncomment some of the file types.)

See /etc/scalpel/scalpel.conf.
```

- **OSSERVAZIONE IMPORTANTE:** Tutte le tipologie di file sono **commentate** (lo si denota dal carattere `#`), pertanto, è strettamente necessario rimuovere i commenti (rimuovendo il carattere `#`) per almeno una tipologia

Il tool Scalpel

Configurazione | 3/3

- Contenuto (parziale) del file di configurazione `scalpel.conf`

```
# GIF and JPG files (very common)
#     gif      y      5000000          \x47\x49\x46\x38\x37\x61      \x00\x3b
#     gif      y      5000000          \x47\x49\x46\x38\x39\x61      \x00\x3b
#     jpg      y      5242880          \xff\xd8\xff???Exif          \xff\xd9
```



```
# GIF and JPG files (very common)
#     gif      y      5000000          \x47\x49\x46\x38\x37\x61      \x00\x3b
#     gif      y      5000000          \x47\x49\x46\x38\x39\x61      \x00\x3b
    jpg      y      5242880          \xff\xd8\xff???Exif          \xff\xd9
```

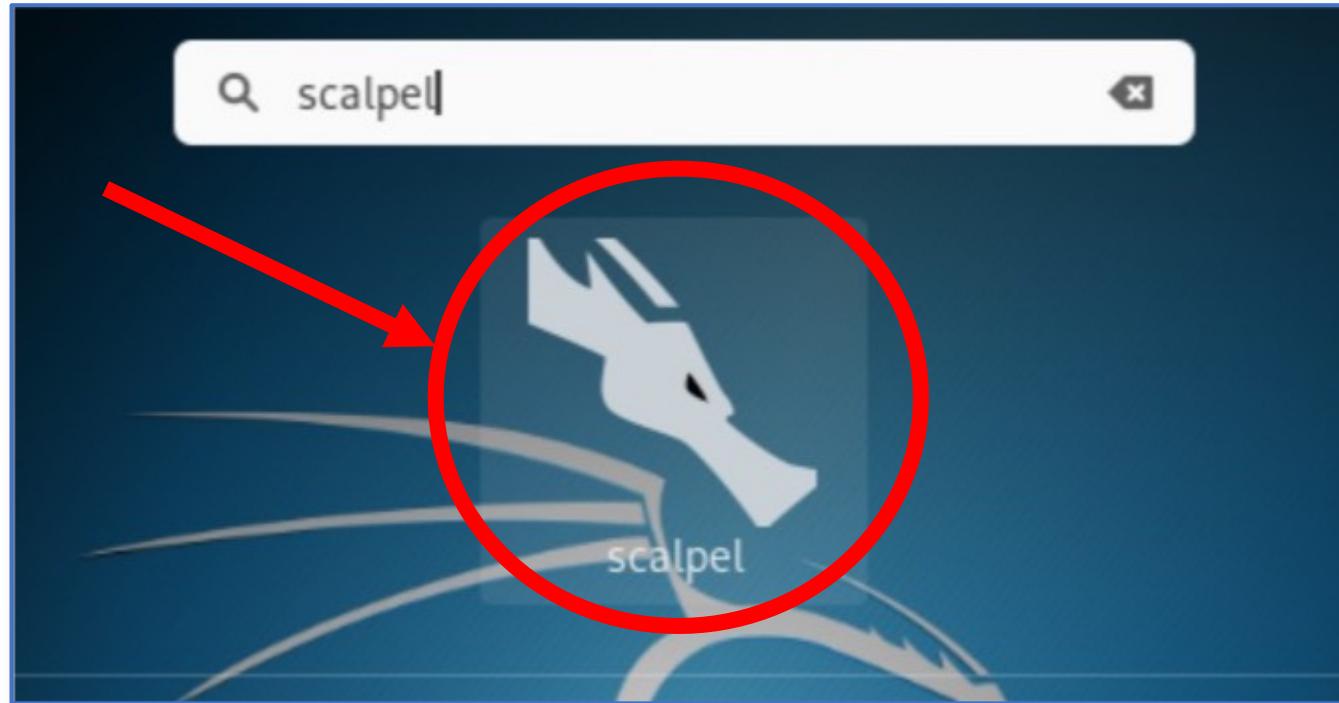
Versione modificata del file, dove è stato rimosso un commento, in corrispondenza della riga, relativa alla tipologia `jpg`

Pertanto, Scalpel effettuerà il recupero di immagini JPEG

Il tool Scalpel

Avvio del Tool | 1/2

- Avvio tramite Interfaccia Grafica



Il tool Scalpel

Avvio del Tool | 2/2

- *Avvio tramite Interfaccia Grafica*

```
Scalpel version 1.60
Written by Golden G. Richard III, based on Foremost 0.69.
Carves files from a disk image based on file headers and footers.

Usage: scalpel [-b] [-c <config file>] [-d] [-h|V] [-i <file>]
           [-m blocksize] [-n] [-o <outputdir>] [-O num] [-q clustersize]
           [-r] [-s num] [-t <blockmap file>] [-u] [-v]
           <imgfile> [<imgfile>] ...

-b Carve files even if defined footers aren't discovered within
maximum carve size for file type [foremost 0.69 compat mode].
-c Choose configuration file.
-d Generate header/footer database; will bypass certain optimizations
and discover all footers, so performance suffers. Doesn't affect
the set of files carved. **EXPERIMENTAL**
-h Print this help message and exit.
-i Read names of disk images from specified file.
```

- All'avvio di Scalpel, si aprirà il terminale di Kali Linux e verranno riportate informazioni in merito alla versione (nell'esempio, la versione è la 1.60) ed alcune opzioni del tool

Il tool Scalpel

Utilizzo su Kali Linux | 1/3

- Sintassi Semplificata (*Descrizione*)

```
scalpel -o <dir> <file>
```

Il tool Scalpel

Utilizzo su Kali Linux | 2/3

- Sintassi Semplificata (*Descrizione*)

```
scalpel -o <dir> <file>
```

- **-o**: Permette di specificare la directory di output, dove verranno memorizzati i file, recuperati mediante il processo di file recovering

Il tool Scalpel

Utilizzo su Kali Linux | 3/3

- Sintassi Semplificata (*Descrizione*)

```
scalpel -o <dir> <file>
```

- **-o**: Permette di specificare la directory di output, dove verranno memorizzati i file, recuperati mediante il processo di file recovering
- **<file>**: Permette di specificare il percorso del **file di input**
 - **OSSERVAZIONE**: il file di input deve essere una immagine forense, precedentemente acquisita, con gli appositi tool (ad esempio, con il tool DC3DD)

Il tool Scalpel

Utilizzo su Kali Linux | 3/3

- Sintassi Semplificata (*Descrizione*)

```
scalpel -o <dir> <file>
```

- **-o**: Permette di specificare la directory di output, dove verranno memorizzati i file, recuperati mediante il processo di file recovering
- **<file>**: Permette di specificare il percorso del **file di input**
 - **OSSERVAZIONE**: il file di input deve essere una immagine forense, precedentemente acquisita, con gli appositi tool (ad esempio, con il tool DC3DD)
 - *Esempio di utilizzo nelle prossime slide*

Il tool Scalpel

Esempio di Utilizzo | 1/9

- Per avviare il processo di recovery sull'immagine forense 11-carve-fat.dd (la medesima utilizzata anche con Foremost), effettuiamo i seguenti step:
 1. Posizioniamoci nella cartella che contiene il file dell'immagine (ad esempio, la *Scrivania*)
 2. Digitiamo il seguente comando:
- ```
scalpel -o RipristinatiScalpel/ 11-carve-fat.dd
```
- 3. L'output del processo verrà riportato nella cartella specificata, ovvero, RipristinatiScalpel

# Il tool Scalpel

## Esempio di Utilizzo | 2/9

- *Processo terminato*

```
root@kali:~/Scrivania# scalpel -o RipristinatiScalpel/ 11-carve-fat.dd
Scalpel version 1.60
Written by Golden G. Richard III, based on Foremost 0.69.

Opening target "/root/Scrivania/11-carve-fat.dd"

Image file pass 1/2.
11-carve-fat.dd: 100.0% |*****| 62.0 MB 00:00 ETAAllocat
[...]

Image file pass 2/2.
11-carve-fat.dd: 100.0% |*****| 62.0 MB 00:00 ETAProcess
ing of image file complete. Cleaning up...
Done.
Scalpel is done, files carved = 19, elapsed = 3 seconds.
root@kali:~/Scrivania#
```

# Il tool Scalpel

## Esempio di Utilizzo | 2/9

- *Processo terminato*

```
root@kali:~/Scrivania# scalpel -o RipristinatiScalpel/ 11-carve-fat.dd
Scalpel version 1.60
Written by Golden G. Richard III, based on Foremost 0.69.

Opening target "/root/Scrivania/11-carve-fat.dd"

Image file pass 1/2.
11-carve-fat.dd: 100.0% |*****| 62.0 MB 00:00 ETAAllocat
[...]

Image file pass 2/2.
11-carve-fat.dd: 100.0% |*****| 62.0 MB 00:00 ETAProcess
ing of image file complete. Cleaning up...
Done.
Scalpel is done, files carved = 19, elapsed = 3 seconds.
root@kali:~/Scrivania#
```

### OSSERVAZIONE IMPORTANTE

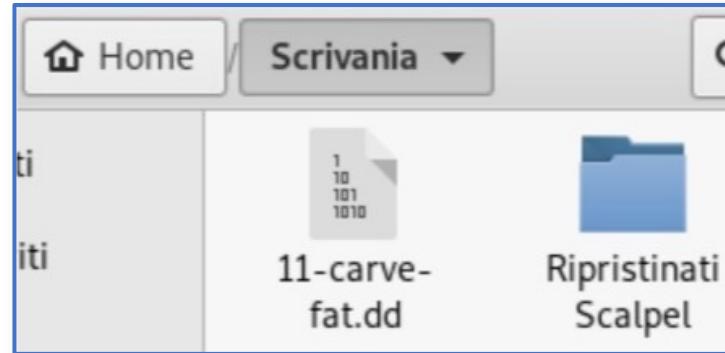
Scalpel ha ripristinato **19 file**, invece di **14**, come avvenuto per Foremost

# Il tool Scalpel

## Esempio di Utilizzo | 3/9

- *File Prodotti | 1/4*

- Al termine del processo, sarà possibile accedere alla cartella RipristinatiScalpel (nell'esempio, sulla *Scrivania*)

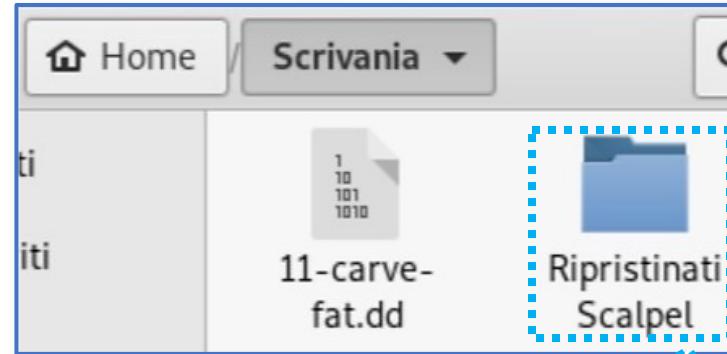


# Il tool Scalpel

## Esempio di Utilizzo | 3/9

- *File Prodotti | 1/4*

- Al termine del processo, sarà possibile accedere alla cartella RipristinatiScalpel (nell'esempio, sulla *Scrivania*)



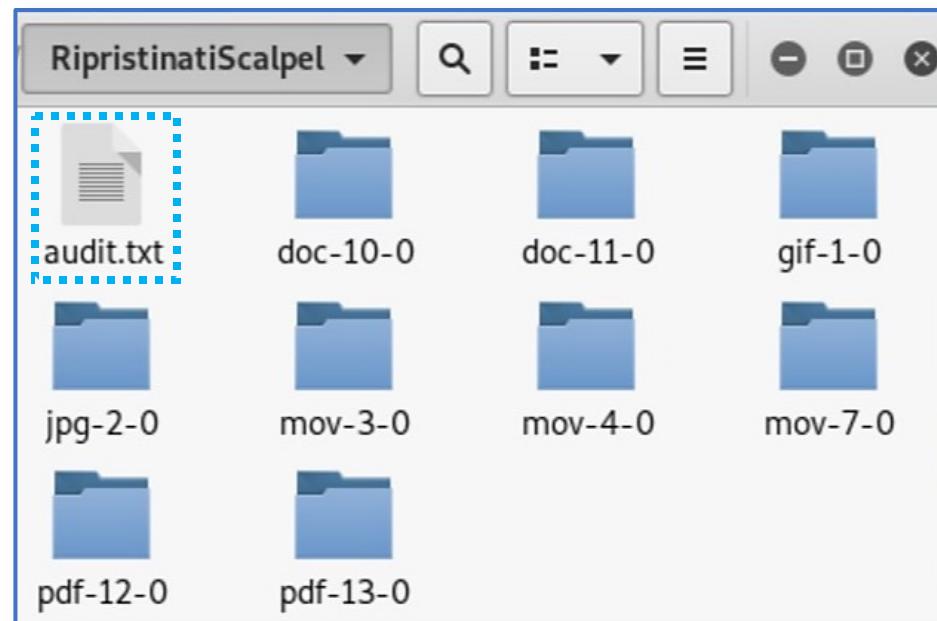
La cartella RipristinatiScalpel, generata da Scalpel

# Il tool Scalpel

## Esempio di Utilizzo | 4/9

- *File Prodotti | 2/4*

- Il contenuto della cartella RipristinatiScalpel



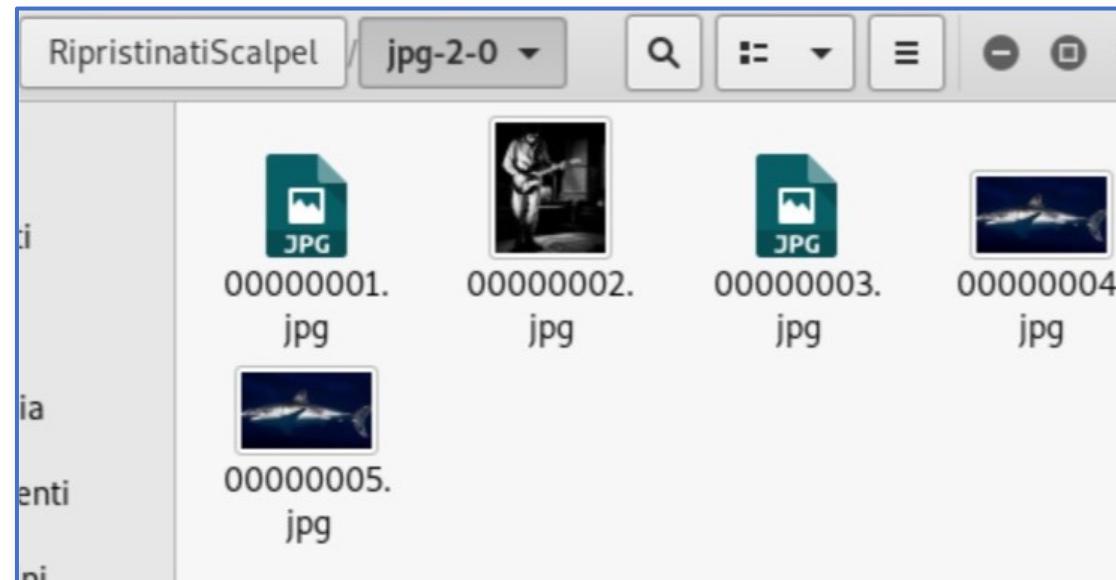
- L'output è molto simile a quello di Foremost, inoltre, è possibile notare la presenza del file audit.txt

# Il tool Scalpel

## Esempio di Utilizzo | 5/9

- *File Prodotti | 3/4*

- Il contenuto della cartella RipristinatiScalpel/jpg-2-0 (contenente cinque file JPEG ripristinate)



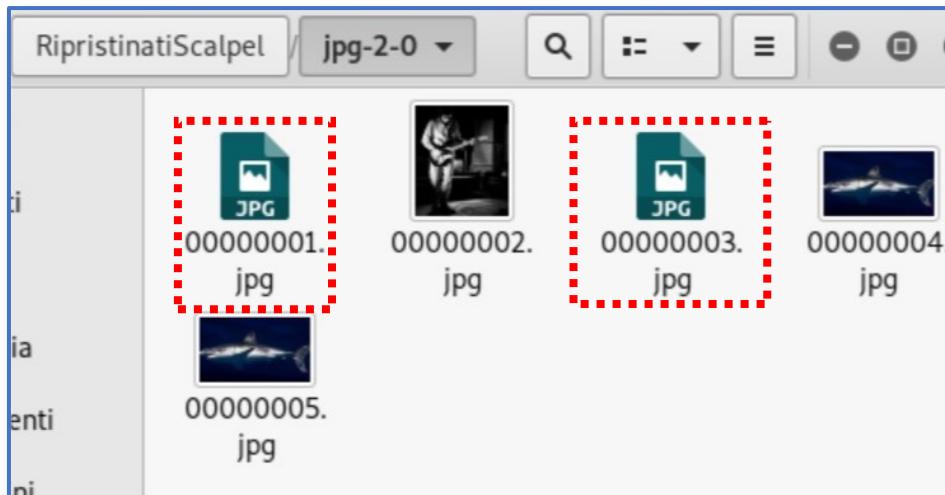
# Il tool Scalpel

## Esempio di Utilizzo | 6/9

### OSSERVAZIONI IMPORTANTI | 1/2

Scalpel ha individuato 5 file JPEG (in base al relativo header e/o footer), tuttavia, come si può notare visivamente, dalla figura, solo tre mostrano un'anteprima (00000002.jpg, 00000004.jpg e 00000005.jpg), mentre gli altri due (00000001.jpg e 00000003.jpg) non mostrano alcuna anteprima

I file, per i quali non è mostrata anteprima, sono corrotti: Scalpel ha verosimilmente ripristinato dei «**FALSI POSITIVI**»



# Il tool Scalpel

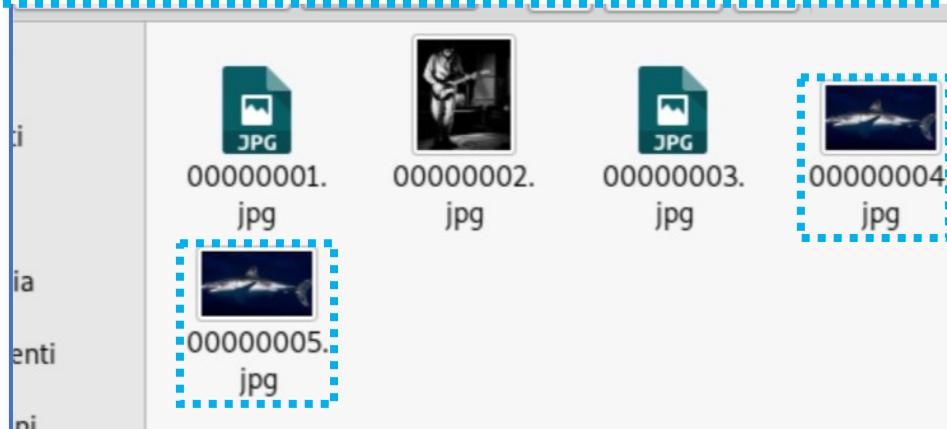
## Esempio di Utilizzo | 7/9

### OSSERVAZIONI IMPORTANTI | 2/2

Inoltre è possibile osservare che i file 00000004.jpg e 00000005.jpg sono identici (stesso valore di hash, per entrambi i file)

In questo caso, in pratica, Scalpel ha ripristinato un numero minore di immagini JPEG (ovvero, 2), rispetto a Foremost (il quale ne aveva ripristinate 3)

In virtù di queste osservazioni, risulta ancor più evidente l'importanza di **considerare più tool, i quali potrebbero NON restituire il medesimo risultato**  
[operando sulla medesima immagine forense]



# Il tool Scalpel

## Esempio di Utilizzo | 8/9

- *File Prodotti | 4/4*
  - Il contenuto (parziale) del file audit.txt

| The following files were carved: |          |      |          |                 |
|----------------------------------|----------|------|----------|-----------------|
| File                             | Start    | Chop | Length   | Extracted From  |
| 00000010.doc                     | 143872   | NO   | 8402944  | 11-carve-fat.dd |
| 00000002.jpg                     | 10095104 | NO   | 29885    | 11-carve-fat.dd |
| 00000001.jpg                     | 8522240  | NO   | 24367    | 11-carve-fat.dd |
| 00000013.doc                     | 143872   | YES  | 10000000 | 11-carve-fat.dd |
| 00000016.pdf                     | 8571392  | NO   | 1399508  | 11-carve-fat.dd |
| 00000017.pdf                     | 8571392  | NO   | 1523266  | 11-carve-fat.dd |
| 00000018.pdf                     | 9972224  | NO   | 122434   | 11-carve-fat.dd |
| 00000011.doc                     | 8546816  | NO   | 3719168  | 11-carve-fat.dd |
| 00000014.doc                     | 8546816  | YES  | 10000000 | 11-carve-fat.dd |
| 00000009.mov                     | 10677985 | YES  | 10000000 | 11-carve-fat.dd |
| 00000008.mov                     | 10678017 | YES  | 10000000 | 11-carve-fat.dd |
| 00000007.mov                     | 10678001 | YES  | 10000000 | 11-carve-fat.dd |
| 00000006.mov                     | 10676736 | YES  | 10000000 | 11-carve-fat.dd |
| 00000005.jpg                     | 10574693 | NO   | 2655     | 11-carve-fat.dd |
| 00000004.jpg                     | 10570636 | NO   | 2655     | 11-carve-fat.dd |
| 00000003.jpg                     | 10570240 | NO   | 3051     | 11-carve-fat.dd |
| 00000000.gif                     | 10670592 | NO   | 5498     | 11-carve-fat.dd |
| 00000015.doc                     | 12265984 | YES  | 10000000 | 11-carve-fat.dd |
| 00000012.doc                     | 12265984 | NO   | 10000000 | 11-carve-fat.dd |

# Il tool Scalpel

## Esempio di Utilizzo | 9/9

- *File Prodotti | 4/4*
  - Il contenuto (*parziale*) del file audit.txt

### OSSERVAZIONE

A differenza del file audit.txt, prodotto da Foremost, nel file audit.txt, prodotto da Scalpel, non viene riportata alcuna sintesi in relazione al numero di file estratti per ciascuna tipologia

# Il tool PhotoRec

# Il tool PhotoRec

## Caratteristiche

- Il tool **PhotoRec** è un software di file recovery (supporta circa 100 tipologie di file) da **immagini forensi** e da **vari tipi di supporti** (dischi fissi, memory card, ecc.)
- Il nome PhotoRec deriva dalla contrazione delle due parole: **Photo Recovery**
  - Capacità del software di recuperare fotografie dalla memoria di macchine fotografiche
- **Open-Source** e **multi-piattaforma** (Windows, Linux, macOS/ OS X)
  - Preinstallato su Kali Linux e Parrot Linux
- Funziona anche nel caso di **supporti particolarmente danneggiati o formattati**
- Maggiori informazioni al seguente link:
  - [https://www.cgsecurity.org/wiki/PhotoRec\\_IT](https://www.cgsecurity.org/wiki/PhotoRec_IT)

# Il tool PhotoRec

## Utilizzo su Kali Linux | 1/3

- PhotoRec è utilizzabile mediante il **comando** è photorec e può essere eseguito dal terminale di Kali Linux
- Digitando il seguente comando, verrà mostrato l'help del tool

```
photorec -h
```

- *Output*

```
PhotoRec 7.0, Data Recovery Utility, April 2015
Christophe GRENIER <grenier@cgsecurity.org>
http://www.cgsecurity.org

Usage: photorec [/log] [/debug] [/d recuper_dir] [file.dd|file.e01|device]
 photorec /version

/log : create a photorec.log file
/debug : add debug information

PhotoRec searches various file formats (JPEG, Office...), it stores them
in recuper_dir directory.
```

# Il tool PhotoRec

## Utilizzo su Kali Linux | 2/3

- Sintassi Semplificata (*Descrizione*)

```
photorec [input]
```

# Il tool PhotoRec

## Utilizzo su Kali Linux | 3/3

- Sintassi Semplificata (*Descrizione*)

```
photorec [input]
```

- **[input]**: Parametro opzionale che permette di specificare il percorso del **file di input**
  - **OSSERVAZIONE 1**: il file di input può essere una immagine forense (formato .DD oppure .E01) oppure un device

# Il tool PhotoRec

## Utilizzo su Kali Linux | 3/3

- Sintassi Semplificata (*Descrizione*)

```
photorec [input]
```

- **[input]**: Parametro opzionale che permette di specificare il percorso del **file di input**
  - **OSSERVAZIONE 1**: il file di input può essere una immagine forense (formato .DD oppure .E01) oppure un device
  - **OSSERVAZIONE 2**: Se non viene specificato il parametro **[input]**, il tool richiede all'utente di selezionare un device (fra quelli disponibili), da cui effettuare il recupero

# Il tool PhotoRec

## Esempio di Utilizzo | 1/15

- Per avviare il processo di recovery sull'immagine 11-carve-fat.dd (la stessa utilizzata anche con Foremost e Scalpel), effettuiamo i seguenti step:
  1. Posizioniamoci nella cartella che contiene il file dell'immagine (ad esempio, la *Scrivania*)
  2. Digitiamo il seguente comando:

```
photorec 11-carve-fat.dd
```

3. L'output del processo verrà riportato nella cartella `recup_dir`

# Il tool PhotoRec

## Esempio di Utilizzo | 1/15

- Per avviare il processo di recovery sull'immagine 11-carve-fat.dd (la stessa utilizzata anche con Foremost e Scalpel), effettuiamo i seguenti step:
  1. Posizioniamoci nella cartella che contiene il file dell'immagine (ad esempio, la *Scrivania*)
  2. Digitiamo il seguente comando:

```
photorec 11-carve-fat.dd
```

3. L'output del processo verrà riportato nella cartella `recup_dir`

**OSSERVAZIONE:** Il nome della cartella di output (`recup_dir`), non può essere modificato

# Il tool PhotoRec

## Esempio di Utilizzo | 2/15

- *Comando:*

```
photorec 11-carve-fat.dd
```

- *Selezione del supporto | 1/2*

```
PhotoRec 7.0, Data Recovery Utility, April 2015
Christophe GRENIER <grenier@cgsecurity.org>
http://www.cgsecurity.org

PhotoRec is free software, and
comes with ABSOLUTELY NO WARRANTY.

Select a media (use Arrow keys, then press Enter):
>Disk 11-carve-fat.dd - 64 MB / 61 MiB (R0)

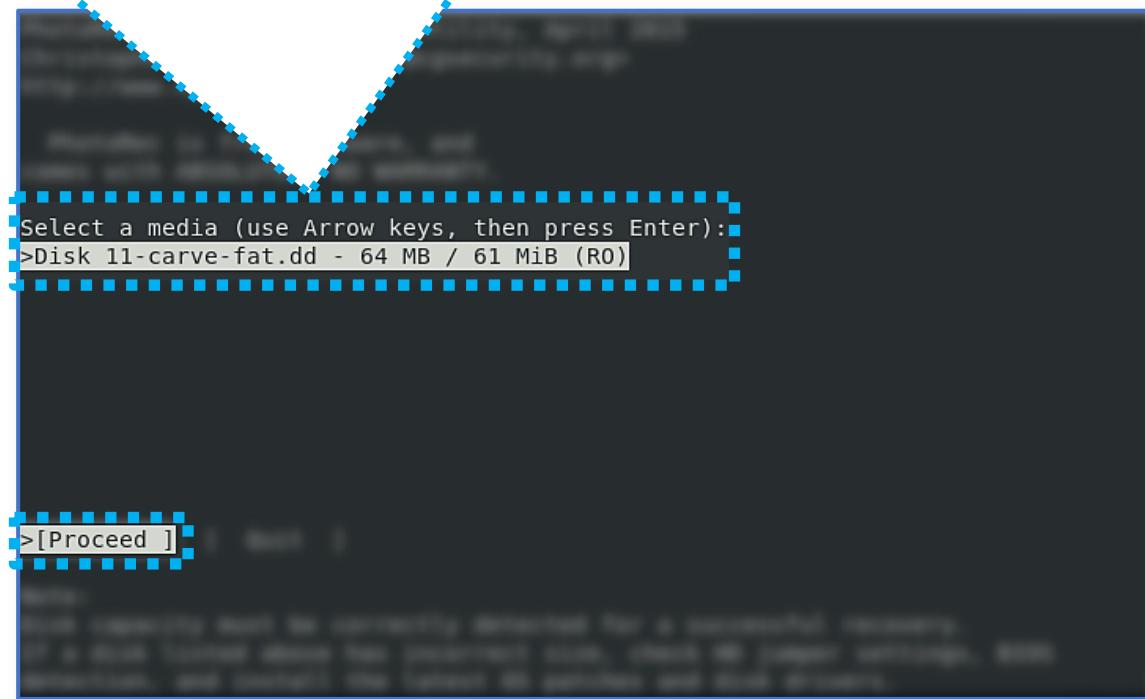
>[Proceed] [Quit]

Note:
Disk capacity must be correctly detected for a successful recovery.
If a disk listed above has incorrect size, check HD jumper settings, BIOS
detection, and install the latest OS patches and disk drivers.
```

# Il tool PhotoRec

## Esempio di Utilizzo | 2/15

Selezioniamo il supporto di origine (nell'esempio, ve n'è solo uno), selezioniamo l'opzione [ Proceed ] e confermiamo con il tasto Invio



# Il tool PhotoRec

## Esempio di Utilizzo | 3/15

- *Comando:*

```
photorec 11-carve-fat.dd
```

- *Selezione del supporto | 2/2*

```
PhotoRec 7.0, Data Recovery Utility, April 2015
Christophe GRENIER <grenier@cgsecurity.org>
http://www.cgsecurity.org

Disk 11-carve-fat.dd - 64 MB / 61 MiB (R0)

 Partition Start End Size in sectors
> P Unknown 0 0 1 7 229 31 126913

>[Search] [Options] [File Opt] [Quit]
 Start file recovery
```

# Il tool PhotoRec

## Esempio di Utilizzo | 3/15

Successivamente, PhotoRec richiede di selezionare la partizione dalla quale effettuare il recupero (nell'esempio, è presente un'unica partizione)

```
Partition Start End Size in sectors
> P Unknown 0 1 7 229 31 126913
```

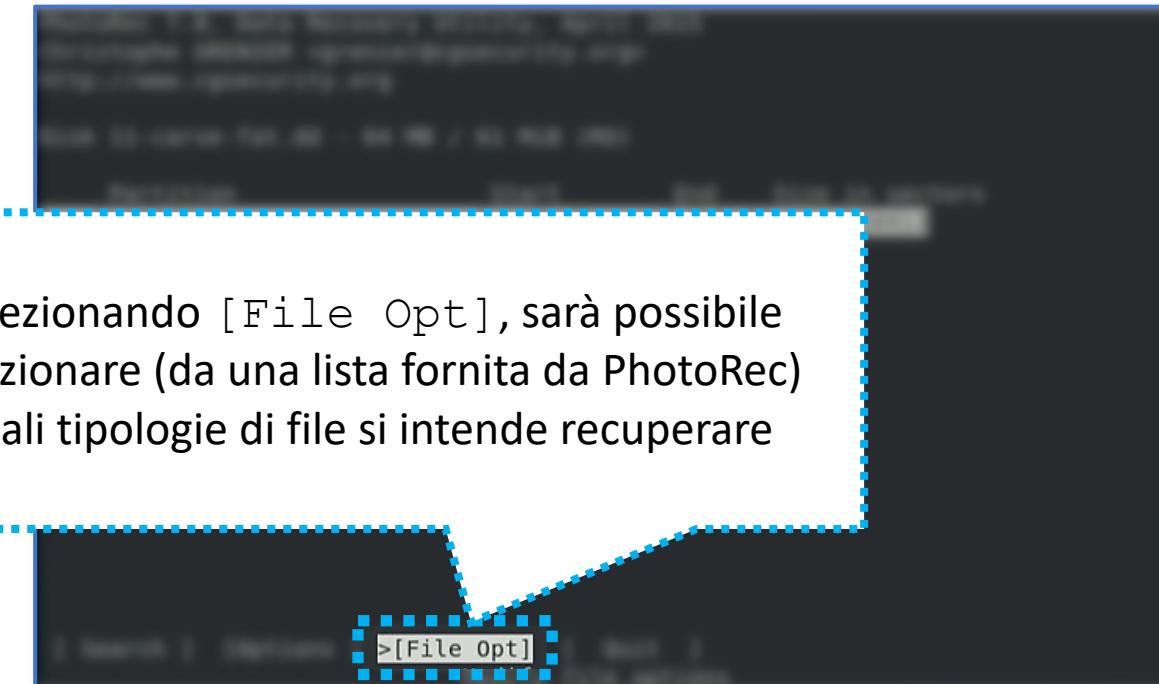
# Il tool PhotoRec

## Esempio di Utilizzo | 4/15

- *Comando:*

```
photorec 11-carve-fat.dd
```

- *Selezione delle tipologie di file che si intende recuperare | 1/2*



Selezionando [File Opt], sarà possibile selezionare (da una lista fornita da PhotoRec) quali tipologie di file si intende recuperare

# Il tool PhotoRec

## Esempio di Utilizzo | 5/15

- *Comando:*

**photorec** 11-carve-fat.dd

- *Selezione delle tipologie di file che si intende recuperare | 2/2*

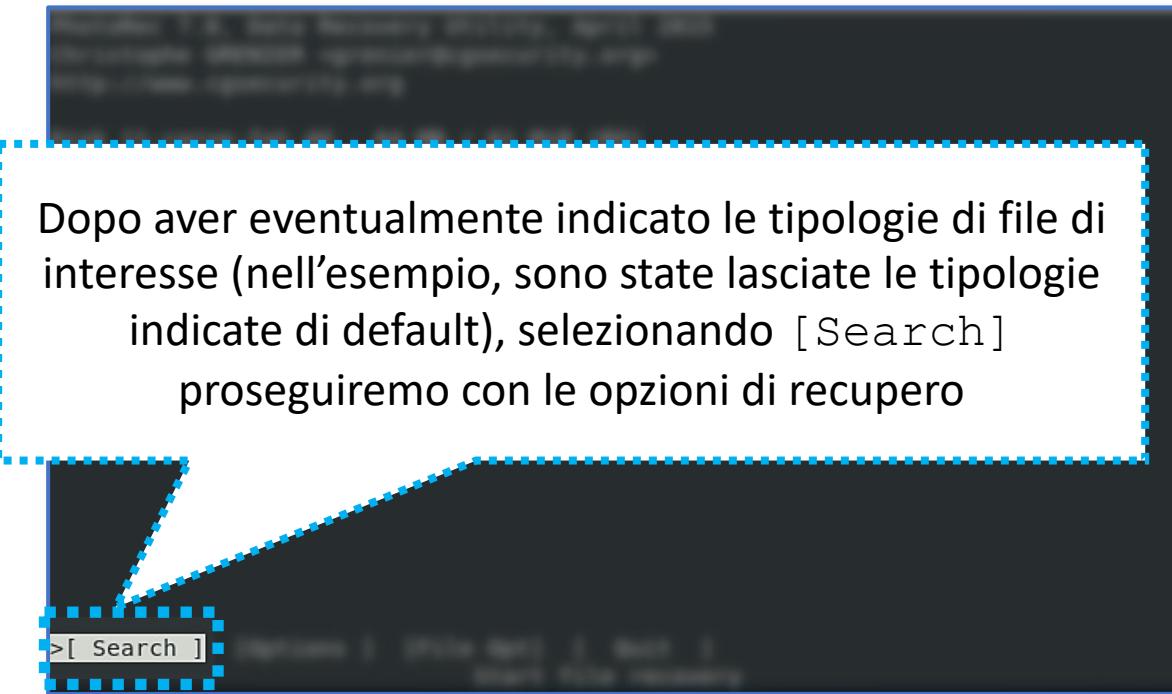
# Il tool PhotoRec

## Esempio di Utilizzo | 6/15

- *Comando:*

```
photorec 11-carve-fat.dd
```

- *Recupero dei file | 1/3*



Dopo aver eventualmente indicato le tipologie di file di interesse (nell'esempio, sono state lasciate le tipologie indicate di default), selezionando [ Search ] proseguiremo con le opzioni di recupero

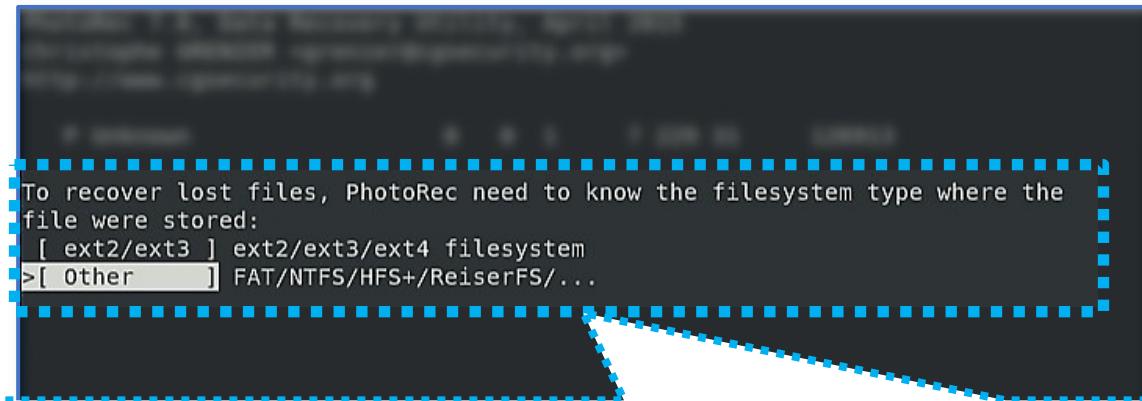
# Il tool PhotoRec

## Esempio di Utilizzo | 7/15

- *Comando:*

```
photorec 11-carve-fat.dd
```

- *Recupero dei file | 2/3*



Nel passo successivo, PhotoRec chiede di indicare il file system dell'immagine, fra le due seguenti opzioni:

- ext2, ext3 o ext4
- FAT, NTFS, HFS+, ecc.

Nell'esempio, il file system dell'immagine è di tipo FAT (nello specifico, FAT32), pertanto, è necessario indicare la seconda opzione

# Il tool PhotoRec

## Esempio di Utilizzo | 8/15

- *Comando:*

```
photorec 11-carve-fat.dd
```

- *Recupero dei file | 3/4*

```
PhotoRec 7.0, Data Recovery Utility, April 2015

Please select a destination to save the recovered files.
Do not choose to write the files to the same partition they were stored on.
Keys: Arrow keys to select another directory
 C when the destination is correct
 Q to quit

Directory /root/Scrivania
>drwxr-xr-x 0 0 4096 4-Feb-2019 09:15 .
drwxr-xr-x 0 0 4096 4-Feb-2019 07:54 ..
drwxr-xr-x 0 0 4096 4-Feb-2019 08:30 11-carve-fat
-rw-r--r-- 501 501 64979456 9-Mar-2005 19:34 11-carve-fat.dd
-rw-r--r-- 0 0 40960 4-Feb-2019 09:15 photorec.ses
```

Verrà poi chiesta conferma in merito al percorso della cartella di output (è necessario premere il tasto C per proseguire)

# Il tool PhotoRec

## Esempio di Utilizzo | 9/15

- *Comando:*

```
photorec 11-carve-fat.dd
```

- *Recupero dei file | 4/4 | Terminata*

```
PhotoRec 7.0, Data Recovery Utility, April 2015
Christophe GRENIER <grenier@cgsecurity.org>
http://www.cgsecurity.org

Disk 11-carve-fat.dd - 64 MB / 61 MiB (R0)
 Partition Start End Size in sectors
 P Unknown 0 1 7 229 31 126913

14 files saved in /root/Scrivania/recup_dir directory.
Recovery completed.

You are welcome to donate to support further development and encouragement
http://www.cgsecurity.org/wiki/Donation
```

[ Quit ]

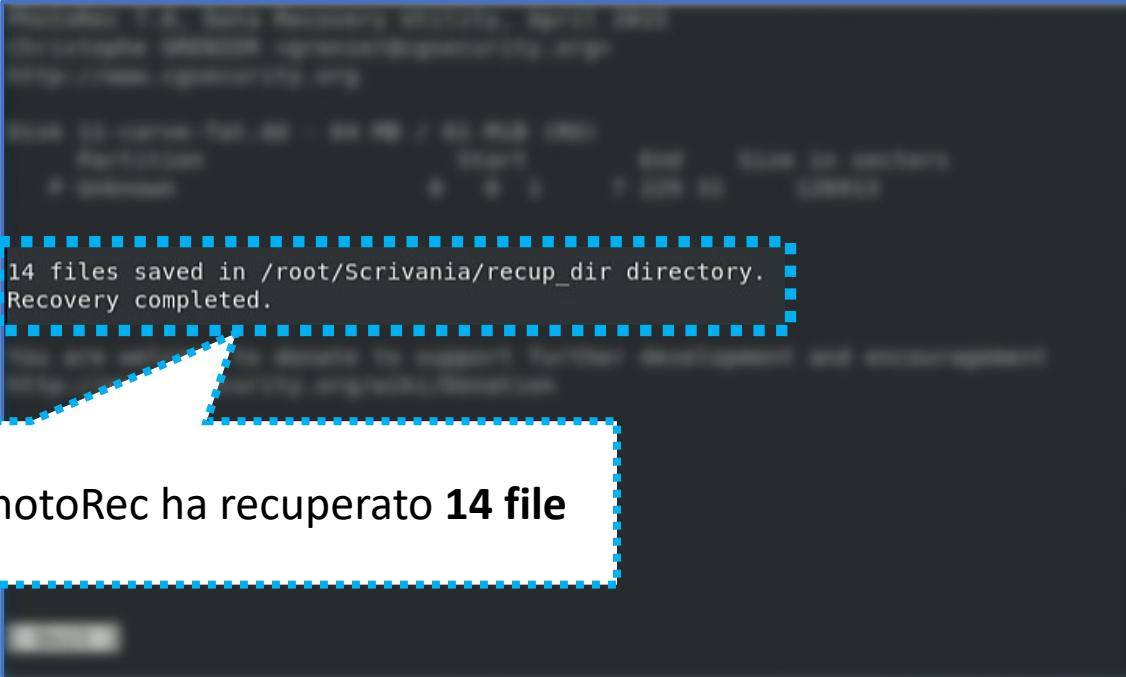
# Il tool PhotoRec

## Esempio di Utilizzo | 9/15

- *Comando:*

```
photorec 11-carve-fat.dd
```

- *Recupero dei file | 4/4 | Terminata*



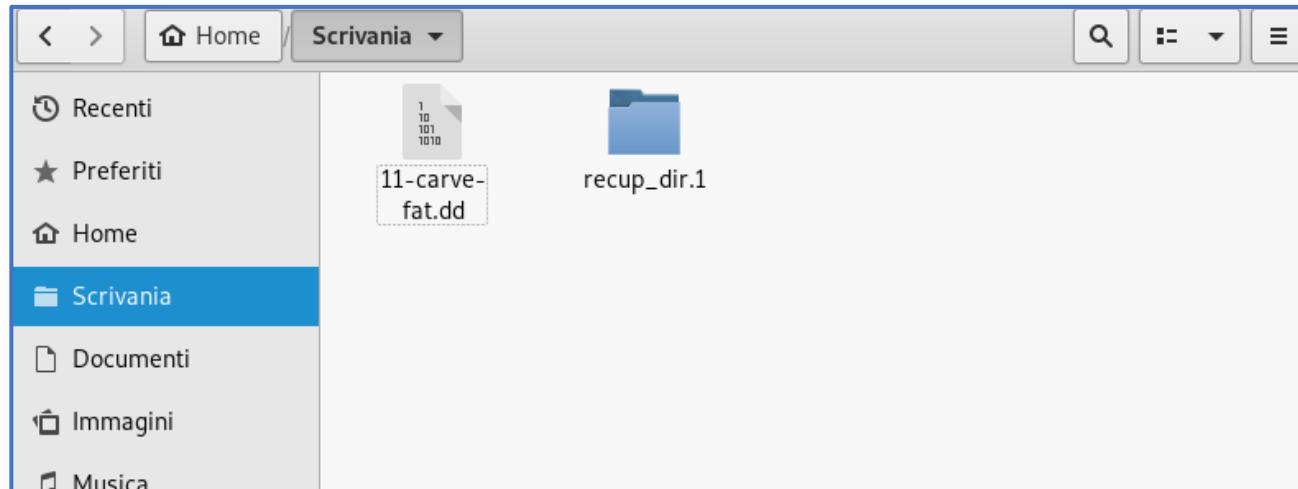
A screenshot of a terminal window with a dark background. In the center, there is a message in white text: "14 files saved in /root/Scrivania/recup\_dir directory. Recovery completed." This message is highlighted with a blue dashed rectangular box. At the bottom left of the terminal window, another blue dashed box contains the text "PhotoRec ha recuperato **14** file".

# Il tool PhotoRec

## Esempio di Utilizzo | 10/15

- *File Prodotti | 1/4*

- Al termine del processo, dopo aver chiuso PhotoRec (selezionando [Quit], nelle varie schermate), sarà possibile accedere alla cartella `recup_dir.1` (nell'esempio, sulla *Scrivania*)

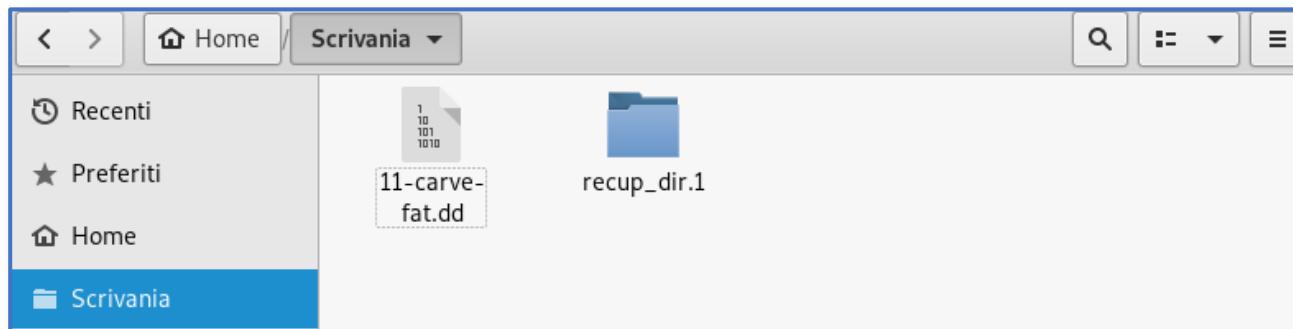


# Il tool PhotoRec

## Esempio di Utilizzo | 11/15

- *File Prodotti | 1/4*

- Al termine del processo, dopo aver chiuso PhotoRec (selezionando [Quit], nelle varie schermate), sarà possibile accedere alla cartella `recup_dir.1` (nell'esempio, sulla *Scrivania*)
  - **NOTA:** PhotoRec aggiunge automaticamente il suffisso `.N` al nome della cartella `recup_dir` (nell'esempio, `recup_dir.1`), per permettere eventuali ulteriori recuperi successivi (ad esempio, un recupero successivo darà luogo ad una cartella `recup_dir.2` e così via)

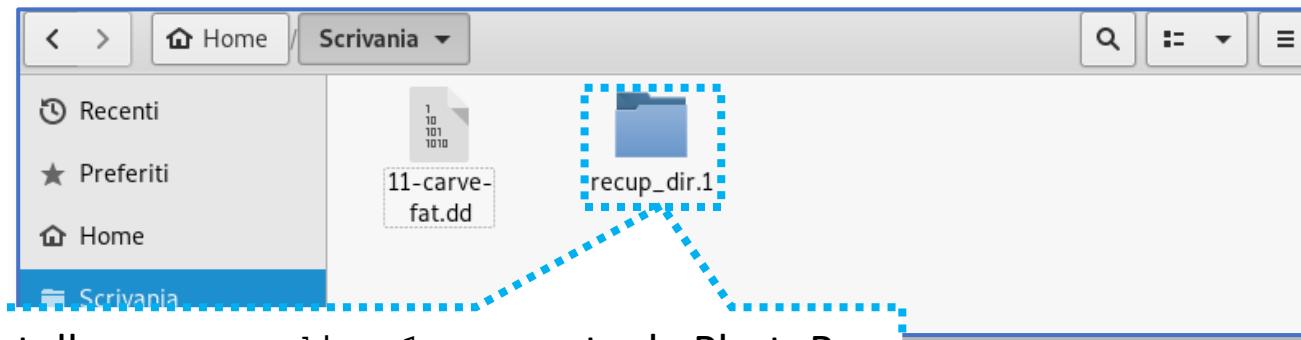


# Il tool PhotoRec

## Esempio di Utilizzo | 11/15

- *File Prodotti | 1/4*

- Al termine del processo, dopo aver chiuso PhotoRec (selezionando [Quit], nelle varie schermate), sarà possibile accedere alla cartella `recup_dir.1` (nell'esempio, sulla *Scrivania*)
  - **NOTA:** PhotoRec aggiunge automaticamente il suffisso `.N` al nome della cartella `recup_dir` (nell'esempio, `recup_dir.1`), per permettere eventuali ulteriori recuperi successivi (ad esempio, un recupero successivo darà luogo ad una cartella `recup_dir.2` e così via)

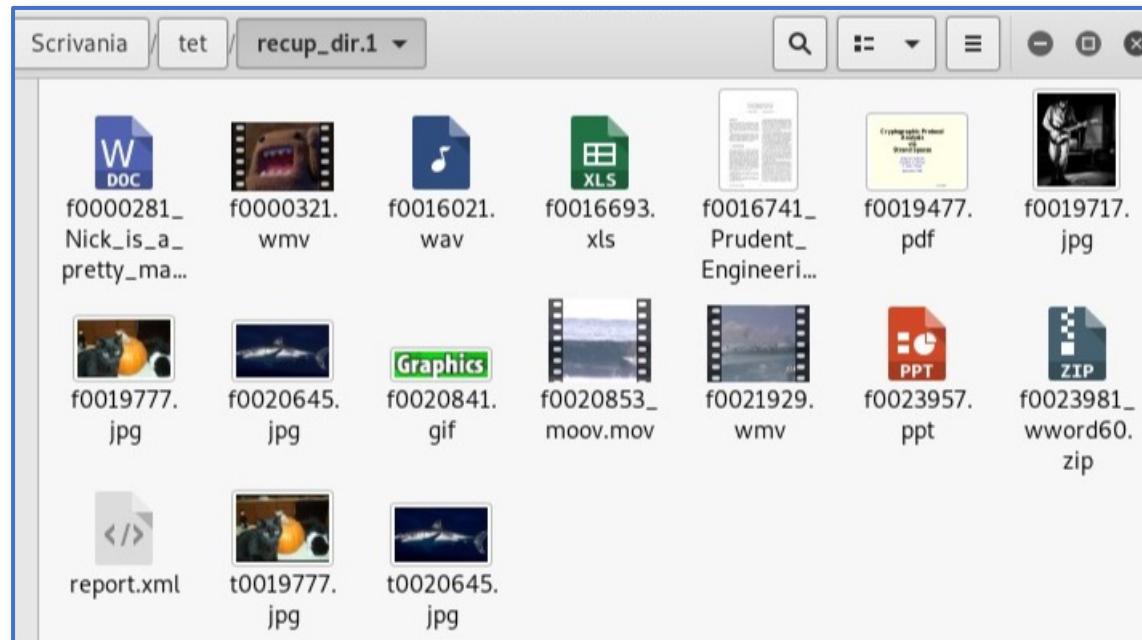


La cartella `recup_dir.1`, generata da PhotoRec

# Il tool PhotoRec

## Esempio di Utilizzo | 12/15

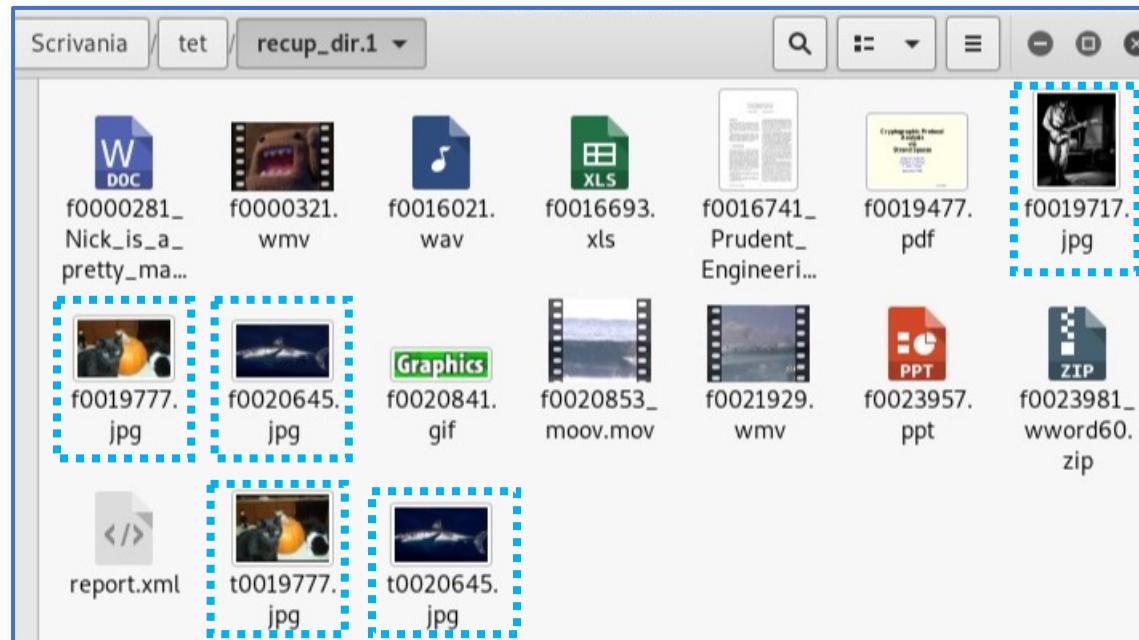
- *File Prodotti | 2/4*
  - Il contenuto della cartella `recup_dir.1`



# Il tool PhotoRec

## Esempio di Utilizzo | 12/15

- *File Prodotti | 2/4*
  - Il contenuto della cartella `recup_dir.1`

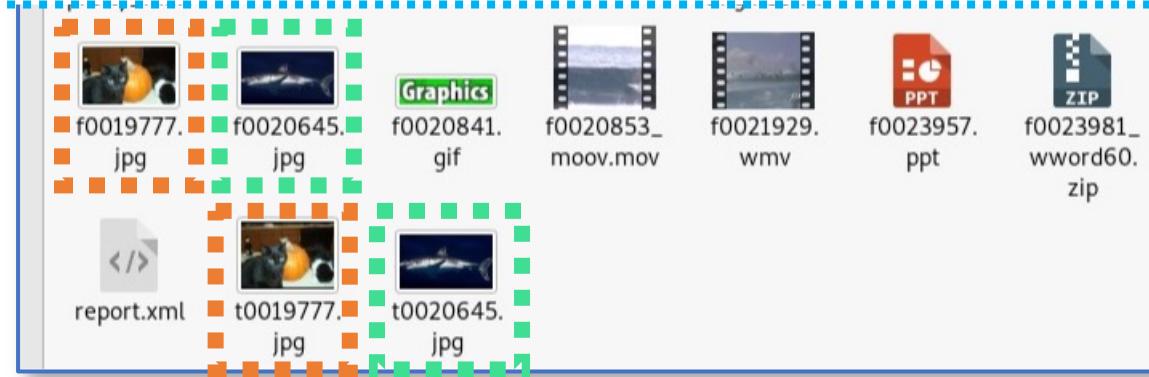


- Sono presenti 5 file JPG

## OSSERVAZIONE IMPORTANTE

PhotoRec ha individuato 5 file JPEG, tuttavia, è possibile effettuare le seguenti osservazioni:

- I file f0019777.jpg e t0019777.jpg (evidenziati in **arancio**), fanno riferimento alla stessa immagine
  - Le due immagini, contenute nei suddetti file, hanno risoluzioni diverse ed una di esse ha una risoluzione particolarmente bassa (potrebbe trattarsi di un ripristino parziale)
- I file f0020645.jpg e t0020645.jpg (evidenziati in **verde**), fanno riferimento alla stessa immagine
  - Le due immagini, contenute nei suddetti file, hanno risoluzioni diverse ed una di esse ha una risoluzione particolarmente bassa (potrebbe trattarsi di un ripristino parziale)
- Alcuni tool di file recovery e data carving, potrebbero recuperare (o tentare di recuperare) solo parzialmente un file

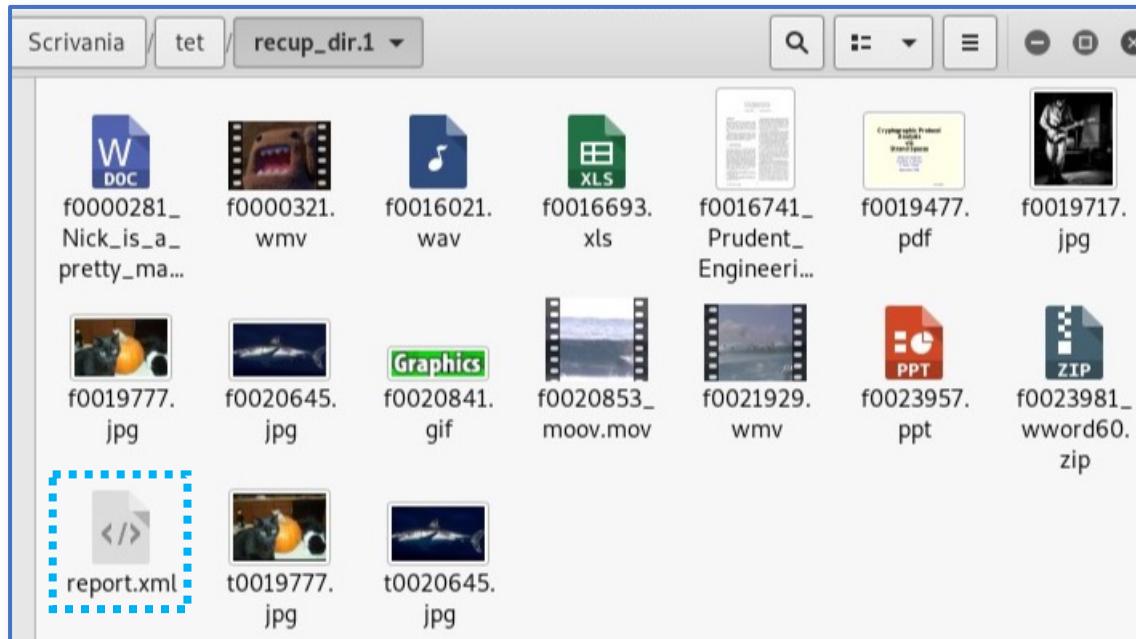


- Sono presenti 5 file JPG

# Il tool PhotoRec

## Esempio di Utilizzo | 13/15

- *File Prodotti | 3/4*
  - Il contenuto della cartella `recup_dir.1`



- PhotoRec ha memorizzato un report, in formato XML, nel file `report.xml`, contenente dettagli sui file e sulla fase di recupero

# Il tool PhotoRec

## Esempio di Utilizzo | 14/15

- *File Prodotti | 4/4*

- Contenuto (parziale) del file report.xml | 1/2

```
<?xml version='1.0' encoding='UTF-8'?>
<dfxml xmloutputversion='1.0'>
 <metadata
 xmlns='http://www.forensicswiki.org/wiki/Category:Digital_Forensics_XML'
 xmlns:xsi='http://www.w3.org/2001/XMLSchema-instance'
 xmlns:dc='http://purl.org/dc/elements/1.1/'>
 <dc:type>Carve Report</dc:type>
 </metadata>
 <creator>
 <package>PhotoRec</package>
 <version>7.0</version>
 <build_environment>
 <compiler>GCC 7.3</compiler>
 <library name='libext2fs' version='1.44.4'/>
 <library name='libewf' version='none'/>
 <library name='libjpeg' version='libjpeg-turbo-1.5.2'/>
 <library name='libntfs' version='libntfs-3g'/>
 </build_environment>
 <execution_environment>
 <os_sysname>Linux</os_sysname>
 <os_release>4.18.0-kali2-amd64</os_release>
 <os_version>#1 SMP Debian 4.18.10-2kali1 (2018-10-09)</os_version>
 <host>kali</host>
 <arch>x86_64</arch>
 <uid>0</uid>
 <start_time>2019-02-04T09:20:24+0100</start_time>
 </execution_environment>
 </creator>
 <source>
 <image_filename>11-carve-fat.dd</image_filename>
 <sectorsize>512</sectorsize>
 <image_size>64979456</image_size>
 <volume>
 <byte_runs>
 <byte_run offset='0' img_offset='0' len='64979456'/>
 </byte_runs>
 </volume>
 </source>
```

Nella prima parte del report, vengono indicate informazioni sulla **versione di PhotoRec**, sull'**immagine sorgente**, sulla **versione del Sistema Operativo** sui cui si è svolta la fase di recupero, ecc.

# Il tool PhotoRec

## Esempio di Utilizzo | 15/15

- *File Prodotti | 4/4*

- Contenuto (parziale) del file report.xml | 2/2

Nella seconda parte del report, per ciascun file recuperato, vengono diverse informazioni, fra cui:

- Nome assegnato da PhotoRec
- Dimensione del file (espressa in byte)
- Ecc.

```
</configuration>
<fileobject>
 <filename>f0000281.doc</filename>
 <filesize>19968</filesize>
 <byte_runs>
 <byte_run offset='0' img_offset='143872' len='20480'/>
 </byte_runs>
</fileobject>
<fileobject>
 <filename>f0000321.wmv</filename>
 <filesize>8037267</filesize>
 <byte_runs>
 <byte_run offset='0' img_offset='164352' len='8038400'/>
 </byte_runs>
</fileobject>
<fileobject>
 <filename>f0016021.wav</filename>
 <filesize>318894</filesize>
 <byte_runs>
 <byte_run offset='0' img_offset='8202752' len='319488'/>
 </byte_runs>
</fileobject>
<fileobject>
 <filename>f0016693.xls</filename>
 <filesize>23040</filesize>
 <byte_runs>
 <byte_run offset='0' img_offset='8546816' len='24576'/>
 </byte_runs>
</fileobject>
<fileobject>
 <filename>f0016741.pdf</filename>
 <filesize>1399508</filesize>
 <byte_runs>
 <byte_run offset='0' img_offset='8571392' len='1400832'/>
 </byte_runs>
</fileobject>
<fileobject>
```

# **II tool Bulk Extractor**

# Il tool Bulk Extractor

## Caratteristiche | 1/3

- I tool Foremost, Scalpel e PhotoRec, visti in precedenza, sono abbastanza potenti, negli ambiti del file recovery e del data carving
  - **OSSERVAZIONE:** I succitati tool sono orientati, principalmente, al recovery di file, in accordo alle tipologie specificate o supportate
  - In alcuni scenari, potrebbe essere estremamente utile recuperare direttamente dati significativi (ad esempio, indirizzi email, numeri di telefono, ecc.), piuttosto che recuperare interi file eliminati (i quali, potrebbero anche non essere recuperati, dai tool di file recovery, ad esempio, a causa di alterazioni del contenuto, ecc.)
    - Per far ciò, è possibile utilizzare il tool **Bulk Extractor**

# Il tool Bulk Extractor

## Caratteristiche | 2/3

- Bulk Extractor è comunque abbastanza performante anche nell'ambito dell'estrazioni di video, immagini, documenti, ecc.
- Mediante Bulk Extractor, possono essere individuati ed estratti diverse tipologie di dati, fra cui:
  - Numero di carte di credito (Credit Card Number – CCN)
  - Indirizzi email
  - URL
  - Ricerche online
  - Informazioni di Siti Web
  - Profili di Social Network ed informazioni provenienti dai Social Network
  - Ecc.

# Il tool Bulk Extractor

## Caratteristiche | 3/3

- Il tool Bulk Extractor (letteralmente: *estrattore di massa*) è presente in Kali Linux
  - Proposto da Simson L. Garfinkel
- Disponibile per diversi Sistemi Operativi:
  - Linux/Unix
  - Microsoft Windows
- Efficiente e multi-thread
- Utilizzabile tramite **linea di comando** (CLI – Command Line Interface)
- Download per Linux/Windows:
  - [http://downloads.digitalcorpora.org/downloads/bulk\\_extractor/](http://downloads.digitalcorpora.org/downloads/bulk_extractor/)
- Maggiori Dettagli:
  - [https://simson.net/clips/academic/2013.COSE.bulk\\_extractor.pdf](https://simson.net/clips/academic/2013.COSE.bulk_extractor.pdf)

# Il tool Bulk Extractor

## Utilizzo su Kali Linux | 1/4

- Bulk Extractor è utilizzabile mediante il **comando bulk\_extractor** e può essere eseguito dal terminale di Kali Linux
- Digitando il seguente comando, verrà mostrato l'help del tool

```
bulk_extractor -h
```

- Output (*parziale*):

```
root@kali:~/Documenti# bulk_extractor -h
bulk_extractor version 1.6.0-dev
Usage: bulk_extractor [options] imagefile
 runs bulk extractor and outputs to stdout a summary of what was found where

Required parameters:
 imagefile - the file to extract
 or -R filedir - recurse through a directory of files
 HAS SUPPORT FOR E01 FILES
 HAS SUPPORT FOR AFF FILES
 -o outdir - specifies output directory. Must not exist.
 bulk_extractor creates this directory.

Options:
 -i - INFO mode. Do a quick random sample and print a report.
 -b banner.txt - Add banner.txt contents to the top of every output file.
```

# Il tool Bulk Extractor

## Utilizzo su Kali Linux | 2/4

- Sintassi Semplificata (*Descrizione*)

```
bulk_extractor -o <dir> <file>
```

# Il tool Bulk Extractor

## Utilizzo su Kali Linux | 3/4

- Sintassi Semplificata (*Descrizione*)

```
bulk_extractor -o <dir> <file>
```

- **-o**: Permette di specificare la directory di output, dove verranno memorizzati i file, contenenti i dati estratti, tramite il processo di data carving, operato da Bulk Extractor

# Il tool Bulk Extractor

## Utilizzo su Kali Linux | 4/4

- Sintassi Semplificata (*Descrizione*)

```
bulk_extractor -o <dir> <file>
```

- **-o**: Permette di specificare la directory di output, dove verranno memorizzati i file, contenenti i dati estratti, tramite il processo di data carving, operato da Bulk Extractor
- **<file>**: Permette di specificare il percorso del **file di input**
  - **OSSERVAZIONE**: il file di input deve essere una immagine forense, precedentemente acquisita

# Il tool Bulk Extractor

## Utilizzo su Kali Linux | 4/4

- Sintassi Semplificata (*Descrizione*)

```
bulk_extractor -o <dir> <file>
```

- **-o**: Permette di specificare la directory di output, dove verranno memorizzati i file, contenenti i dati estratti, tramite il processo di data carving, operato da Bulk Extractor
- **<file>**: Permette di specificare il percorso del **file di input**
  - **OSSERVAZIONE**: il file di input deve essere una immagine forense, precedentemente acquisita
  - *Esempio di utilizzo nelle prossime slide*

# Il tool Bulk Extractor

## Esempio di Utilizzo | 1/8

- Per effettuare un esempio di utilizzo del tool Bulk Extractor, è stata utilizzata **una immagine forense**, denominata terry-work-usb-2009-12-11.E01
- L'immagine terry-work-usb-2009-12-11.E01 è scaricabile gratuitamente dal seguente link (ottenibile anche dal QR Code):
  - <http://downloads.digitalcorpora.org/corpora/scenarios/2009-m57-patents/drives-redacted/>



- **NOTA:** La dimensione della suddetta immagine è di circa 32 MB
- Al suddetto link, sono presenti diverse immagini, per effettuare ulteriori test

# Il tool Bulk Extractor

## Esempio di Utilizzo | 2/8

- Per avviare il processo di recovery sull'immagine terry-work-usb-2009-12-11.E01, effettuiamo i seguenti step:

1. Posizioniamoci nella cartella che contiene il file dell'immagine
2. Digitiamo il seguente comando:

```
bulk_extractor -o bulk_output terry-work-usb-2009-12-11.E01
```

3. L'output del processo verrà riportato nella cartella specificata, ovvero, bulk\_output

# Il tool Bulk Extractor

## Esempio di Utilizzo | 3/8

- *Processo terminato*

```
root@kali:~/Documenti# bulk_extractor -o bulk_output terry-work-usb-2009-12-11.E01
bulk_extractor version: 1.6.0-dev
Hostname: kali
Input file: terry-work-usb-2009-12-11.E01
Output directory: bulk_output
Disk Size: 2097152000
Threads: 1
21:16:35 Offset 67MB (3.20%) Done in 0:10:26 at 21:27:01
21:16:41 Offset 150MB (7.20%) Done in 0:05:33 at 21:22:14
21:16:42 Offset 234MB (11.20%) Done in 0:03:35 at 21:20:17
21:16:43 Offset 318MB (15.20%) Done in 0:02:38 at 21:19:21
21:16:44 Offset 402MB (19.20%) Done in 0:02:05 at 21:18:49

[...]

MD5 of Disk Image: e07f26954b23db1a44dfd28ecd717da9
Phase 2. Shutting down scanners
Phase 3. Creating Histograms
Elapsed time: 59.3214 sec.
Total MB processed: 2097
Overall performance: 35.3524 MBytes/sec (35.3524 MBytes/sec/thread)
Total email features found: 3
root@kali:~/Documenti#
```

# Il tool Bulk Extractor

## Esempio di Utilizzo | 3/8

- *Processo terminato*

```
root@kali:~/Documenti# bulk_extractor -o bulk_output terry-work-usb-2009-12-11.E01
bulk_extractor version: 1.6.0-dev
Hostname: kali
Input file: terry-work-usb-2009-12-11.E01
Output directory: bulk_output
Disk Size: 2097152000
```

Al termine del processo, Bulk Extractor mostra alcune informazioni utili, fra cui:

- Numero di MB elaborati
- Valore di Hash (MD5) dell'immagine elaborata
- Numero di indirizzi email individuate

```
MD5 of Disk Image: e07f26954b23db1a44dfd28ecd717da9
Phase 2. Shutting down scanners
Phase 3. Creating Histograms
Elapsed time: 59.3214 sec.
Total MB processed: 2097
Overall performance: 35.3524 MBytes/sec (35.3524 MBytes/sec/thread)
Total email features found: 3
root@kali:~/Documenti#
```

# Il tool Bulk Extractor

## Esempio di Utilizzo | 4/8

- *File Prodotti | 1/3*

- Al termine del processo, sarà possibile visionare i file, generati da Bulk Extractor, i quali sono contenuti nella cartella bulk\_output
  - **NOTA:** Viene generato anche un report, in formato XML, relativo al processo di estrazione, denominato report.xml

Parte 1 di 3

```
root@kali:~/Documenti/bulk_output# ls -l
totale 30600
-rw-r--r-- 1 root root 0 feb 22 21:16 aes_keys.txt
-rw-r--r-- 1 root root 0 feb 22 21:16 alerts.txt
-rw-r--r-- 1 root root 0 feb 22 21:17 ccn_histogram.txt
-rw-r--r-- 1 root root 0 feb 22 21:17 ccn_track2_histogram.txt
-rw-r--r-- 1 root root 0 feb 22 21:16 ccn_track2.txt
-rw-r--r-- 1 root root 0 feb 22 21:16 ccn.txt
-rw-r--r-- 1 root root 68140 feb 22 21:17 domain_histogram.txt
-rw-r--r-- 1 root root 7603392 feb 22 21:16 domain.txt
-rw-r--r-- 1 root root 0 feb 22 21:16 elf.txt
-rw-r--r-- 1 root root 0 feb 22 21:17 email_domain_histogram.txt
-rw-r--r-- 1 root root 260 feb 22 21:17 email_histogram.txt
-rw-r--r-- 1 root root 1116 feb 22 21:16 email.txt
-rw-r--r-- 1 root root 0 feb 22 21:17 ether_histogram.txt
-rw-r--r-- 1 root root 0 feb 22 21:16 ether.txt
-rw-r--r-- 1 root root 517 feb 22 21:16 exif.txt
```

# Il tool Bulk Extractor

## Esempio di Utilizzo | 4/8

- *File Prodotti | 1/3*

- Al termine del processo, sarà possibile visionare i file, generati da Bulk Extractor, i quali sono contenuti nella cartella bulk\_ouput
  - **NOTA:** Viene generato anche un report, in formato XML, relativo al processo di estrazione, denominato report.xml

Parte 2 di 3

```
-rw-r--r-- 1 root root 0 feb 22 21:17 find_histogram.txt
-rw-r--r-- 1 root root 0 feb 22 21:16 find.txt
-rw-r--r-- 1 root root 0 feb 22 21:16 gps.txt
-rw-r--r-- 1 root root 0 feb 22 21:16 httplogs.txt
-rw-r--r-- 1 root root 0 feb 22 21:17 ip_histogram.txt
-rw-r--r-- 1 root root 0 feb 22 21:16 ip.txt
-rw-r--r-- 1 root root 0 feb 22 21:16 jpeg_carved.txt
-rw-r--r-- 1 root root 0 feb 22 21:16 json.txt
-rw-r--r-- 1 root root 0 feb 22 21:16 kml.txt
-rw-r--r-- 1 root root 0 feb 22 21:17 pii_teamviewer.txt
-rw-r--r-- 1 root root 0 feb 22 21:16 pii.txt
-rw-r--r-- 1 root root 0 feb 22 21:16 rar.txt
-rw-r--r-- 1 root root 31088 feb 22 21:17 report.xml
-rw-r--r-- 1 root root 0 feb 22 21:16 rfc822.txt
-rw-r--r-- 1 root root 0 feb 22 21:16 sqlite_carved.txt
-rw-r--r-- 1 root root 238 feb 22 21:17 telephone_histogram.txt
-rw-r--r-- 1 root root 740 feb 22 21:16 telephone.txt
```

# Il tool Bulk Extractor

## Esempio di Utilizzo | 4/8

- *File Prodotti | 1/3*

- Al termine del processo, sarà possibile visionare i file, generati da Bulk Extractor, i quali sono contenuti nella cartella bulk\_output
  - **NOTA:** Viene generato anche un report, in formato XML, relativo al processo di estrazione, denominato report.xml

Parte 3 di 3

```
-rw-r--r-- 1 root root 0 feb 22 21:16 unrar_carved.txt
-rw-r--r-- 1 root root 0 feb 22 21:16 unzip_carved.txt
-rw-r--r-- 1 root root 0 feb 22 21:17 url_facebook-address.txt
-rw-r--r-- 1 root root 0 feb 22 21:17 url_facebook-id.txt
-rw-r--r-- 1 root root 3118516 feb 22 21:17 url_histogram.txt
-rw-r--r-- 1 root root 0 feb 22 21:17 url_microsoft-live.txt
-rw-r--r-- 1 root root 0 feb 22 21:17 url_searches.txt
-rw-r--r-- 1 root root 68107 feb 22 21:17 url_services.txt
-rw-r--r-- 1 root root 18809144 feb 22 21:16 url.txt
-rw-r--r-- 1 root root 0 feb 22 21:16 vcard.txt
-rw-r--r-- 1 root root 1483960 feb 22 21:16 windirs.txt
-rw-r--r-- 1 root root 0 feb 22 21:16 winlnk.txt
drwxr-xr-x 3 root root 4096 feb 22 21:16 winpe_carved
-rw-r--r-- 1 root root 6192 feb 22 21:16 winpe_carved.txt
-rw-r--r-- 1 root root 76280 feb 22 21:16 winpe.txt
-rw-r--r-- 1 root root 0 feb 22 21:16 winprefetch.txt
-rw-r--r-- 1 root root 24457 feb 22 21:16 zip.txt
root@kali:~/Documenti/bulk_output#
```

# Il tool Bulk Extractor

## Esempio di Utilizzo | 4/8

- *File Prodotti | 1/3*

- Al termine del processo, sarà possibile visionare i file, generati da Bulk Extractor, i quali sono contenuti nella cartella bulk\_ouput
  - **NOTA:** Viene generato anche un report, in formato XML, relativo al processo di estrazione, denominato report.xml

Parte 3 di 3

### OSSERVAZIONI

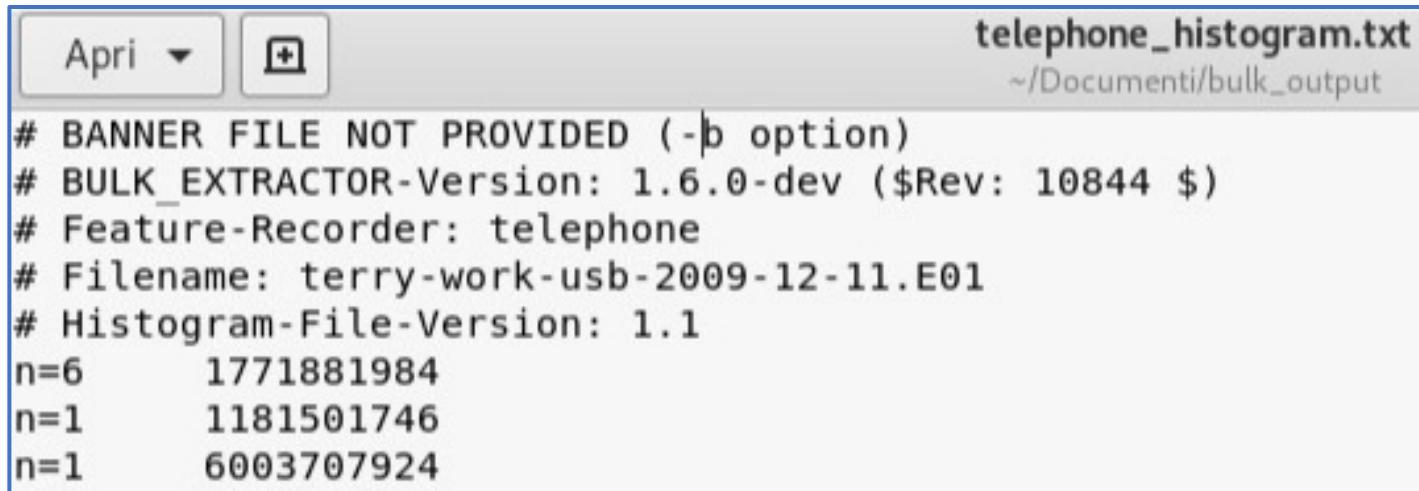
- I file che contengono la sottostringa ccn (ad esempio, ccn.txt, ccn\_histogram.txt, ecc.) sono riferiti a numeri di carte di credito
- Non tutti i file contengono dati
  - I file contenenti dati hanno dimensione > 0 byte

# Il tool Bulk Extractor

## Esempio di Utilizzo | 7/8

- *File Prodotti | 2/3*

- Contenuto del file telephone\_histogram.txt



The screenshot shows a text editor window with a blue border. The title bar reads "telephone\_histogram.txt" and " ~/Documenti/bulk\_output". The main area contains the following text:

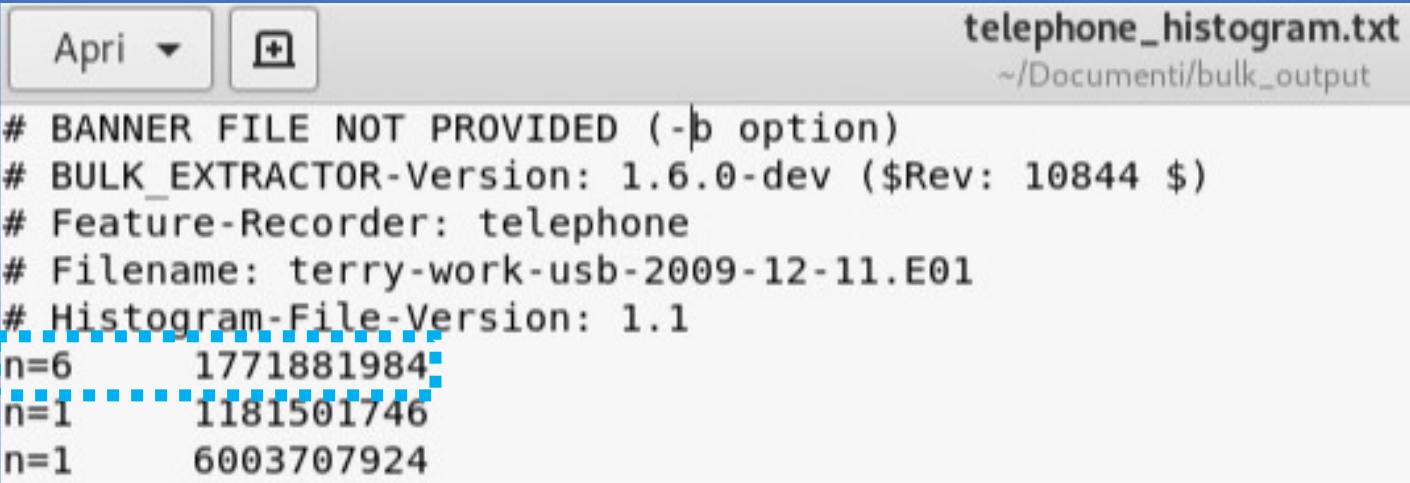
```
BANNER FILE NOT PROVIDED (-b option)
BULK_EXTRACTOR-Version: 1.6.0-dev ($Rev: 10844 $)
Feature-Recorder: telephone
Filename: terry-work-usb-2009-12-11.E01
Histogram-File-Version: 1.1
n=6 1771881984
n=1 1181501746
n=1 6003707924
```

# Il tool Bulk Extractor

## Esempio di Utilizzo | 7/8

- *File Prodotti | 2/3*

- Contenuto del file telephone\_histogram.txt



```
BANNER FILE NOT PROVIDED (-b option)
BULK_EXTRACTOR-Version: 1.6.0-dev ($Rev: 10844 $)
Feature-Recorder: telephone
Filename: terry-work-usb-2009-12-11.E01
Histogram-File-Version: 1.1
n=6 1771881984
n=1 1181501746
n=1 6003707924
```

### OSSERVAZIONE | 1/2

Questo file riporta i numeri di telefono individuati ed il relativo numero di occorrenze (per ciascun numero di telefono)

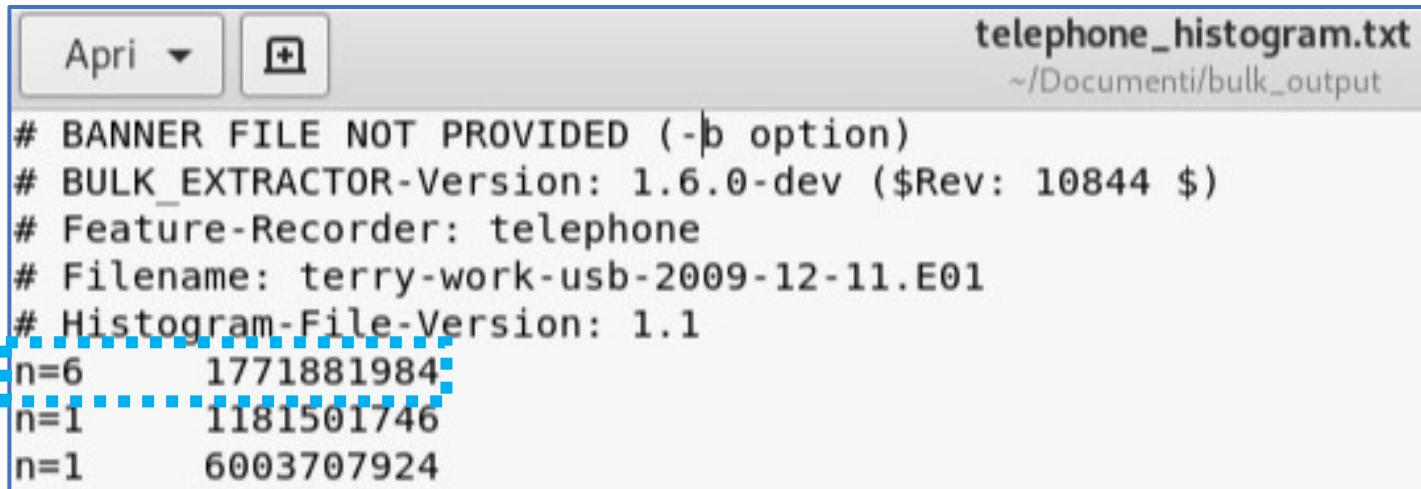
**Esempio:** Il numero di telefono 1771881984 è apparso 6 volte nei dati estratti (numero di telefono apparso più frequentemente)

# Il tool Bulk Extractor

## Esempio di Utilizzo | 7/8

- *File Prodotti | 2/3*

- Contenuto del file telephone\_histogram.txt



```
telephone_histogram.txt
~/Documenti/bulk_output

BANNER FILE NOT PROVIDED (-b option)
BULK_EXTRACTOR-Version: 1.6.0-dev ($Rev: 10844 $)
Feature-Recorder: telephone
Filename: terry-work-usb-2009-12-11.E01
Histogram-File-Version: 1.1
n=6 1771881984
n=1 1181501746
n=1 6003707924
```

### OSSERVAZIONE | 2/2

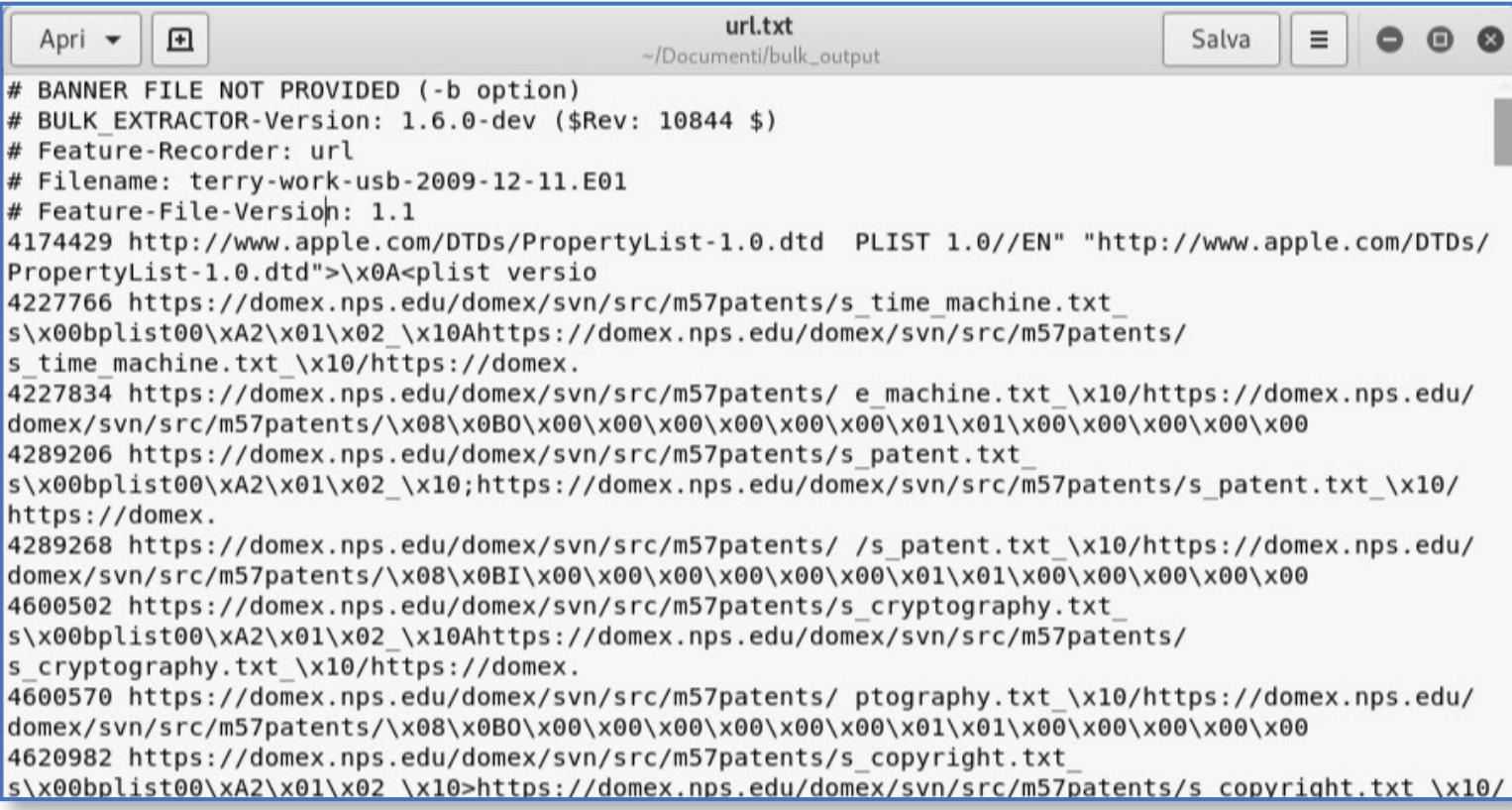
Da questo file è possibile realizzare un **istogramma**, il quale riporta, per ciascun numero di telefono individuato (riportato sull'asse X), il relativo numero di occorrenze (sull'asse Y)

# Il tool Bulk Extractor

## Esempio di Utilizzo | 8/8

- *File Prodotti | 3/3*

- Contenuto (*parziale*) del file url.txt, il quale riporta tutti siti web e i link visitati, estratti da Bulk Extractor



The screenshot shows a text editor window titled "url.txt" located at the path "~/Documenti/bulk\_output". The window has standard operating system controls (Minimize, Maximize, Close) and a "Salva" (Save) button. The content of the file is a list of URLs, mostly in hex format, representing links found during a bulk extraction process. The file starts with a banner and version information, followed by a large list of URLs.

```
BANNER FILE NOT PROVIDED (-b option)
BULK_EXTRACTOR-Version: 1.6.0-dev ($Rev: 10844 $)
Feature-Recorder: url
Filename: terry-work-usb-2009-12-11.E01
Feature-File-Version: 1.1
4174429 http://www.apple.com/DTDs/PropertyList-1.0.dtd PLIST 1.0//EN "http://www.apple.com/DTDs/PropertyList-1.0.dtd">\x0A<plist versio
4227766 https://domex.nps.edu/domex svn/src/m57patents/s_time_machine.txt
s\x00bplist00\xA2\x01\x02_\x10Ahttps://domex.nps.edu/domex svn/src/m57patents/
s_time_machine.txt_\x10/https://domex.
4227834 https://domex.nps.edu/domex svn/src/m57patents/ e_machine.txt_\x10/https://domex.nps.edu/
domex svn/src/m57patents/\x08\x0B0\x00\x00\x00\x00\x00\x01\x01\x00\x00\x00\x00\x00
4289206 https://domex.nps.edu/domex svn/src/m57patents/s_patent.txt
s\x00bplist00\xA2\x01\x02_\x10;https://domex.nps.edu/domex svn/src/m57patents/s_patent.txt_\x10/
https://domex.
4289268 https://domex.nps.edu/domex svn/src/m57patents/ /s_patent.txt_\x10/https://domex.nps.edu/
domex svn/src/m57patents/\x08\x0B1\x00\x00\x00\x00\x01\x01\x00\x00\x00\x00\x00
4600502 https://domex.nps.edu/domex svn/src/m57patents/s_cryptography.txt
s\x00bplist00\xA2\x01\x02_\x10Ahttps://domex.nps.edu/domex svn/src/m57patents/
s_cryptography.txt_\x10/https://domex.
4600570 https://domex.nps.edu/domex svn/src/m57patents/ ptography.txt_\x10/https://domex.nps.edu/
domex svn/src/m57patents/\x08\x0B0\x00\x00\x00\x00\x00\x01\x01\x00\x00\x00\x00\x00
4620982 https://domex.nps.edu/domex svn/src/m57patents/s_copyright.txt
s\x00bplist00\xA2\x01\x02_\x10>https://domex.nps.edu/domex svn/src/m57patents/s_copyright.txt_\x10/
```

# Riferimenti Bibliografici

- **Digital Forensics with Kali Linux, Shiva V.N. Parasram, Packt Publishing, 2017**
  - Capitolo 3 (*Parziale*)
  - Capitolo 5
- **PhotoRec**
  - [https://www.cgsecurity.org/wiki/PhotoRec\\_IT](https://www.cgsecurity.org/wiki/PhotoRec_IT)