Creazione ed accesso alle immagini forensi

Cosa sono?

Perché?

Come fare?

Michele Ferrazzano

15 marzo 2011

Le 5 fasi dell'informatica forense

- Identificazione
- Acquisizione (e conservazione)
- Analisi
- Valutazione
- Presentazione

Immagine forense

- Un'immagine forense è una **copia bit a bit** di un supporto originale.
- È anche nota come *bit stream image*
- **Un "copia e incolla" o un "drag&drop" NON sono una copia forense. Perché?**
- Una copia forense include anche lo spazio non allocato
  - File cancellati
  - Slack space
  - Spazio libero

Gestione dei file sul filesystem

Promessi sposi.txt	1
Il Cinque Maggio.txt	7

1	Quel ram	1	2
2	o del la	1	3
3	go di Co	1	4
4	mo che v	1	5
5	olge a m	1	5
5	ezzogior	1	6
6	noX	1	/
7	Ei fu. S	1	8
8	iccome i	1	9
9	mmobile,	1	10
10	dato il	1	11
11	mortal	1	12
12	sospiroX	1	/
13		0	/
14		0	/
15		0	/
16		0	/

Cancellazione di un file

~~Promessi sposi.txt~~	~~1~~
Il Cinque Maggio.txt	7

1	**Quel ram**	**0**	2
2	**o del la**	**0**	3
3	**go di Co**	**0**	4
4	**mo che v**	**0**	5
5	**olge a m**	**0**	5
5	**ezzogior**	**0**	6
6	**noX**	**0**	/
7	Ei fu. S	1	8
8	iccome i	1	9
9	mmobile,	1	10
10	dato il	1	11
11	mortal	1	12
12	sospiroX	1	/
13		0	/
14		0	/
15		0	/
16		0	/

Salvataggio di un nuovo file

Divina commedia.txt	**1**
Il Cinque Maggio.txt	7

1	**Nel mezz**	**1**	**2**
2	**o del ca**	**1**	**3**
3	**mmin di**	**1**	**4**
4	**nostra v**	**1**	**5**
5	**itaX a m**	**1**	/
5	**ezzogior**	**0**	**6**
6	**noX**	**0**	/
7	Ei fu. S	1	8
8	iccome i	1	9
9	mmobile,	1	10
10	dato il	1	11
11	mortal	1	12
12	sospiroX	1	/
13		0	/
14		0	/
15		0	/
16		0	/

Slack space

Divina commedia.txt	1
Il Cinque Maggio.txt	7

1	Nel mezz	1	2
2	o del ca	1	3
3	mmin di	1	4
4	nostra v	1	5
5	itaX **a m**	1	/
5	**ezzogior**	0	6
6	**noX**	0	/
7	Ei fu. S	1	8
8	iccome i	1	9
9	mmobile,	1	10
10	dato il	1	11
11	mortal	1	12
12	sospiroX	1	/
13		0	/
14		0	/
15		0	/
16		0	/

Perché creare immagini forensi

- **Preservare le evidenze**
  - Hash
- Lavorare con copie fedeli all'originale
- Produrre diverse copie per dividere il lavoro tra più persone
- **Rendere ripetibili operazioni irripetibili**
  - Ad esempio, esecuzione di macchine virtuali per mostrare comportamento di un trojan

Acquisizione di immagini forensi

Cosa non fare

- Usare direttamente la macchina oggetto di indagine
  - Valgono dovute eccezioni (ad esempio, recupero password su pc acceso)
  - Tool: DEFT Extra
- Acquisire con Windows senza protezioni (write block)

Acquisizione di immagini forensi

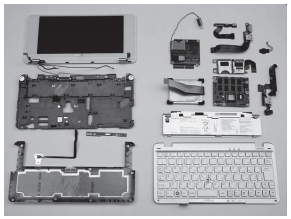
Cosa fare

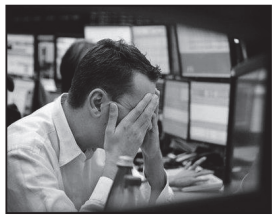
- Utilizzare direttamente la macchina oggetto di indagine *solo* quando è necessario acquisire dati dalla RAM, quindi spegnere immediatamente
- Utilizzare write block
- Scrivere su dischi di destinazione vergini (*wiped*)
- Utilizzare Windows solo con protezioni (write block) oppure fare uso di Forensic CD
- Utilizzare hardware dedicato alla copia

Acquisizione di immagini forensi

ATTENZIONE

- RAID
- Dischi cifrati
- Difficoltà a rimuovere i dischi
- Server in esecuzione





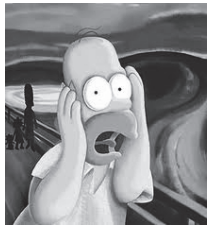
Cosa estrarre?

Breve elenco *assolutamente* non esaustivo… solo per avere un'idea!

- Residenti su disco
- File cancellati
- Slack space
- File di swap o memoria virtuale
- File temporanei creati dalle applicazioni
- File gestiti dai browser
  - Cronologia
  - Cookie
  - Cache
- File di log
- […]

Cosa acquisire

- Classico
  - Personal computer e server
- Quasi classico
  - Palmari, cellulari, smartphone
- Ma anche
  - Automobili
  - Console videogame
  - Slot machine
  - […]



Formati di acquisizione

- DD
  - Compressione assente
- Encase
  - Compressione dei dati
- FTK Imager
  - A scelta (compressione dei dati o compressione assente)
- …

Hash

- L'algoritmo di hash elabora una qualunque mole di bit e restituisce in output una stringa di bit di dimensione fissa. L'output è detto *digest*
- La stringa di output è univoca per ogni documento e ne è un identificatore
- L'algoritmo non è invertibile, ossia non è possibile ricostruire il documento originale a partire dalla stringa che viene restituita in output
  - In realtà “per tentativi” **(infiniti)** è possibile
    - Per ogni digest esistono infiniti input che la generano (collisioni)!

Hash MD5

- L'acronimo MD5 (*Message Digest algorithm 5*) indica un algoritmo crittografico di hashing realizzato da Ronald Rivest nel 1991 e standardizzato con la RFC 1321
- Questo tipo di codifica prende in input una stringa di lunghezza arbitraria e ne produce in output un'altra a 128 bit (ovvero con lunghezza fissa di 32 valori esadecimali) che può essere usata per calcolare la firma digitale dell'input