



Di chi sono i miei dati

20 Settembre 2013, Bologna

Sicurezza all'ombra delle Torri

Concorrenza sleale da parte di dipendenti e collaboratori infedeli nell'epoca della crisi

Paolo Dal Checco
Consulente Informatico Forense



Chi sono

- PhD in Informatica a Torino (Computer & Network Security)
- Consulente Informatico Forense
- Perizie Informatiche per Procure, Tribunali, Forze dell'Ordine, Avvocati, Aziende, Privati
- Founder DEFT Association
- Socio IISFA Italian Chapter





Un problema di percezione

- “*Di chi sono i miei dati*”... un controsenso o un problema di percezione reale?
- Scarsa percezione del reato informatico rispetto al reato “ordinario”, perché:
 - Facilità nel commetterlo
 - Errata sensazione di anonimato e impunità
 - I dati digitali vengono percepiti come immateriali
 - Poca chiarezza su proprietà intellettuale



La dura realtà...

- Accesso abusivo a sistema telematico (art. 615 ter): **da 1 a 5 anni**
- Detenzione e diffusione abusiva di codici di accesso (615 quater): **da 1 a 2 anni**
- Diffusione di apparecchiature, dispositivi o programmi informatici diretti a danneggiare o interrompere un sistema informatico o telematico (art. 615 quinquies): **da 1 a 2 anni**
- Installazione di apparecchiature atte ad intercettare od impedire comunicazioni o conversazioni telegrafiche o telefoniche (art. 617 bis): **da 1 a 5 anni**
- Falsificazione, alterazione o soppressione del contenuto di comunicazioni o conversazioni telegrafiche o telefoniche (art. 617 ter): **da 1 a 4 anni**
- Intercettazione, impedimento o interruzione illecita di comunicazioni informatiche o telematiche (art. 617 quater): **da 1 a 5 anni**
- Installazione di apparecchiature atte ad intercettare, impedire od interrompere comunicazioni informatiche o telematiche (art. 617 quinquies): **da 1 a 5 anni**



La dura realtà...

- Falsificazione, alterazione o soppressione del contenuto di comunicazioni informatiche o telematiche (art. 617 sexies): **da 1 a 5 anni**
- Rivelazioni del contenuto di corrispondenza (art. 618): **fino a 6 mesi**
- Rivelazione del contenuto di documenti segreti (art. 621): **fino a 3 anni**
- Rivelazione di segreto professionale (art. 622): **fino a 1 anno**
- Rivelazione di segreti scientifici o industriali (art. 623): **fino a 2 anni**
- Danneggiamento informatico (art. 635 bis): **da 1 a 5 anni**
- Installazione di apparecchiature atte ad intercettare od impedire comunicazioni o conversazioni telegrafiche o telefoniche: **da 1 a 5 anni**
- Intercettazione, impedimento o interruzione illecita di comunicazioni informatiche o telematiche: **da 1 a 5 anni**



Cosa è l'incidente informatico

- “Expectations for Computer Security Incident Response” (RFC 2350, ma vedere anche ISO 27035, ISO 27037 e ISO 27041-42-43)
- L'incidente informatico, un evento che compromette aspetti della sicurezza dei computer e delle reti, con almeno uno fra:
 - perdita di confidenzialità delle informazioni
 - compromissione dell'integrità delle informazioni
 - interruzione di servizio
 - utilizzo inappropriato di servizi, sistemi, informazioni
 - danneggiamento di sistemi





Come gestire l'incidente informatico

- “Guidelines for Evidence Collection and Archiving” (RFC 3227)
- Procedere metodicamente
- Catturare un'immagine completa del sistema
- Minimizzare le modifiche ai dati
- Isolare se necessario il sistema
- Prima si raccoglie, poi si analizza
- Procedere in ordine di volatilità
- Garantire la catena di custodia



Come non gestire l'incidente informatico

- Mancata copia forense (bitstream) dei supporti
- Accensione e utilizzo del PC originale
- Mancata conservazione dei supporti originali
- Mancata apposizione di data certa
- Monitoraggio del dipendente in tempo reale
- Violazione Privacy
- Errata repertazione (hash, sigilli, catena di conservazione)
- Uso di strumenti di duplicazione inadeguati (es. Norton Ghost)
- Utilizzo di strumenti di analisi o metodologie non adeguate (es. RegExp malformate)
- Per l'Avvocato: non chiamare il CT all'ultimo momento
- Per il CT: non fare l'Avvocato (vale anche il viceversa)



Case study

**Alcuni casi reali
opportunamente anonimizzati**



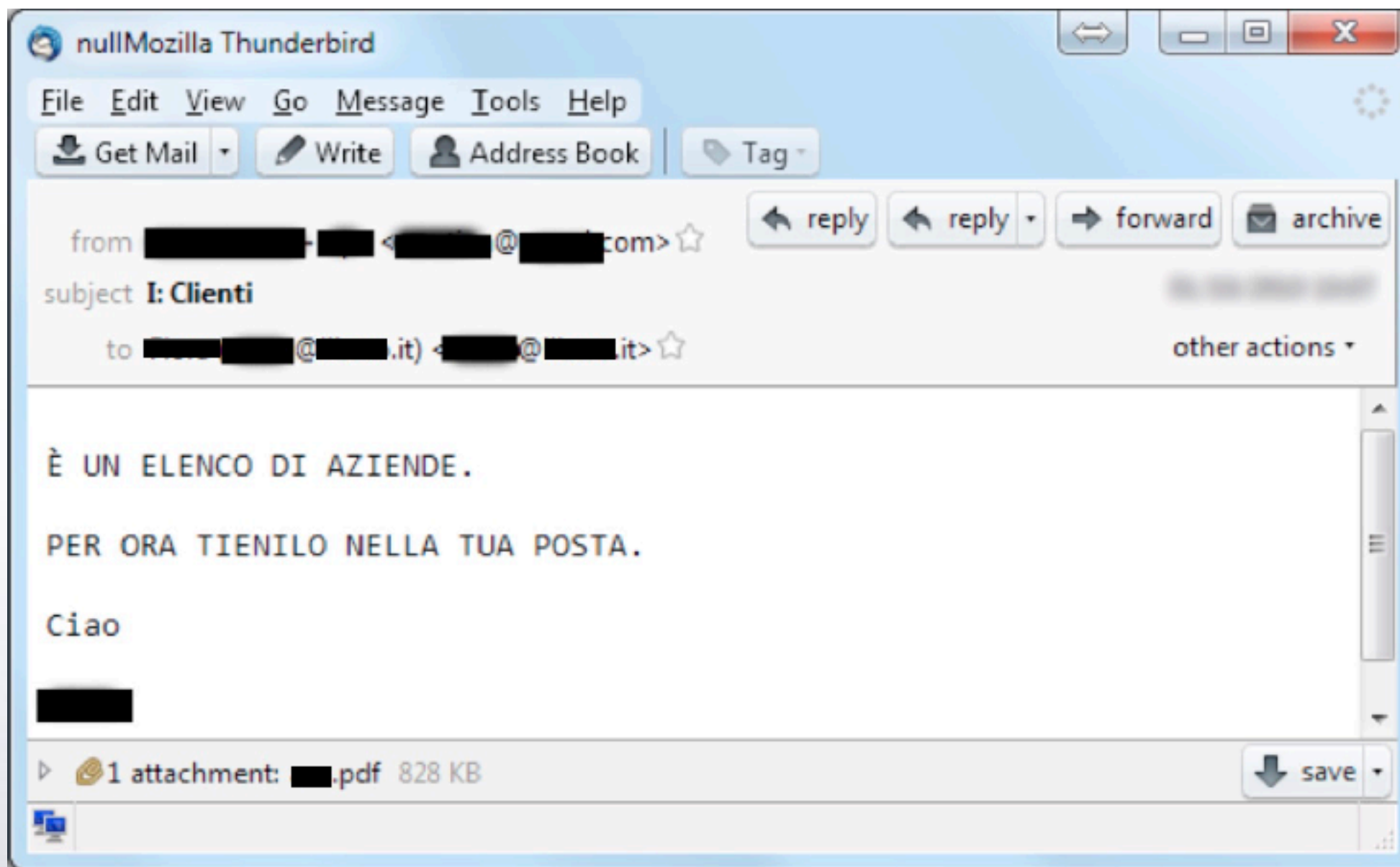


Case study: “Cosa è il cestino”

- Un’azienda ci segnala che un dipendente li ha lasciati improvvisamente, aprendo nuova attività
- Sono sicuri abbia una copia del database clienti di proprietà aziendale
- Hanno solo il computer dell’ex dipendente



Case study: “Cosa è il cestino?”





Case study: “il DB fantasma”

- Un’azienda ci segnala che un dipendente li ha lasciati improvvisamente, aprendo nuova attività
- Sono sicuri abbia una copia del database clienti di proprietà aziendale
- Hanno solo il computer dell’ex dipendente





Case study: “il DB fantasma”

- Una veloce **timeline** realizzata tramite fls (TSK o Autopsy) ci serve per inquadrare i giorni in cui il PC è stato utilizzato maggiormente

```
fls -o 63 -r -m C: /dev/sda > c-timeline.body  
  
mactime -y -m -d -i day c-timeline-daily.csv -z  
Europe/Rome -b c-timeline.body > c-timeline.csv
```





Case study: “il DB fantasma”

- Tramite il daily summary notiamo che in una certa data, prossima alla dipartita, vi sono stati numerosi accessi in lettura a file (compreso il DB dei clienti)

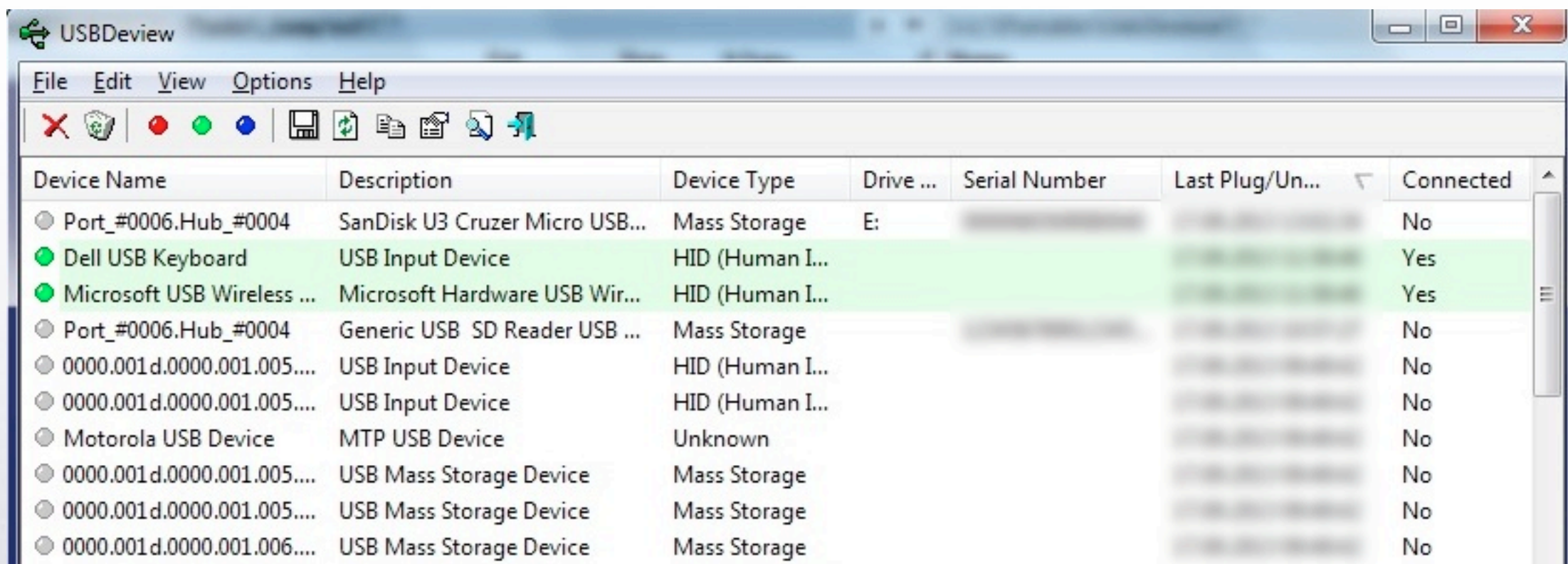
```
Tue 03 02 2010, 6616
Wed 03 03 2010, 3990
Thu 03 04 2010, 62239
Fri 03 05 2010, 315
Sat 03 06 2010, 5
Sun 03 07 2010, 178
```

```
Wed 03 03 2010 17:00:00, 63
Wed 03 03 2010 18:00:00, 94
Thu 03 04 2010 01:00:00, 2
Thu 03 04 2010 02:00:00, 1
Thu 03 04 2010 09:00:00, 294
Thu 03 04 2010 10:00:00, 46
Thu 03 04 2010 11:00:00, 13874
Thu 03 04 2010 12:00:00, 44408
Thu 03 04 2010 13:00:00, 3478
Thu 03 04 2010 16:00:00, 3
Thu 03 04 2010 17:00:00, 98
Thu 03 04 2010 18:00:00, 1
Thu 03 04 2010 19:00:00, 2
Thu 03 04 2010 20:00:00, 3
Thu 03 04 2010 23:00:00, 29
Fri 03 05 2010 01:00:00, 6
Fri 03 05 2010 06:00:00, 1
Fri 03 05 2010 08:00:00, 10
```




Case study: “il DB fantasma”

- Dal registro di sistema (Windows) con il tool gratuito UsbDeview rileviamo che poco prima degli accessi è stata inserita una pendrive USB



The screenshot shows the UsbDeview application window. The title bar reads 'USBDeview'. The menu bar includes 'File', 'Edit', 'View', 'Options', and 'Help'. Below the menu bar is a toolbar with various icons. The main area contains a table with the following columns: 'Device Name', 'Description', 'Device Type', 'Drive ...', 'Serial Number', 'Last Plug/Un...', and 'Connected'. The table lists several USB devices, with the first three rows highlighted in green.

Device Name	Description	Device Type	Drive ...	Serial Number	Last Plug/Un...	Connected
Port_#0006.Hub_#0004	SanDisk U3 Cruzer Micro USB...	Mass Storage	E:			No
● Dell USB Keyboard	USB Input Device	HID (Human I...				Yes
● Microsoft USB Wireless ...	Microsoft Hardware USB Wir...	HID (Human I...				Yes
Port_#0006.Hub_#0004	Generic USB SD Reader USB ...	Mass Storage				No
0000.001d.0000.001.005....	USB Input Device	HID (Human I...				No
0000.001d.0000.001.005....	USB Input Device	HID (Human I...				No
Motorola USB Device	MTP USB Device	Unknown				No
0000.001d.0000.001.005....	USB Mass Storage Device	Mass Storage				No
0000.001d.0000.001.005....	USB Mass Storage Device	Mass Storage				No
0000.001d.0000.001.006....	USB Mass Storage Device	Mass Storage				No



Case study: “il DB fantasma”

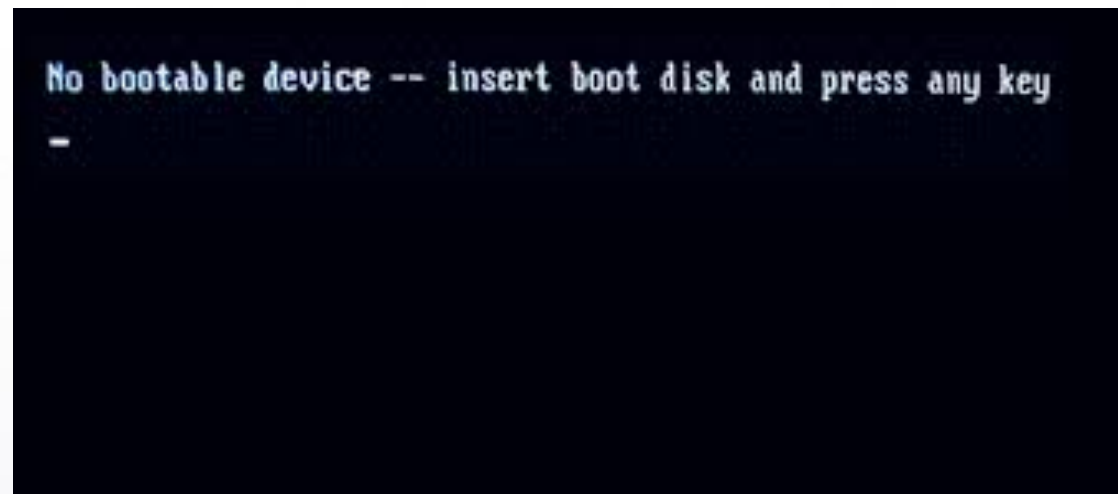
- Tramite analisi del registro, dalle ShellBag/MRU notiamo che sulla pendrive (non aziendale e non in possesso dell'azienda) esisteva un folder chiamato... “**DB CLIENTI**” aperto sulla pendrive
- Tool per analisi ShellBag/MRU Streams: Registry Report (Gaijin), RegRipper (H. Carvey), Sbag (TzWorks)
- Bingo! :-)





Case study: “la storia non si cancella”

Il server dell'azienda Snake Oil Spa viene trovato con schermata nera e un “*no bootable device*” sullo schermo *



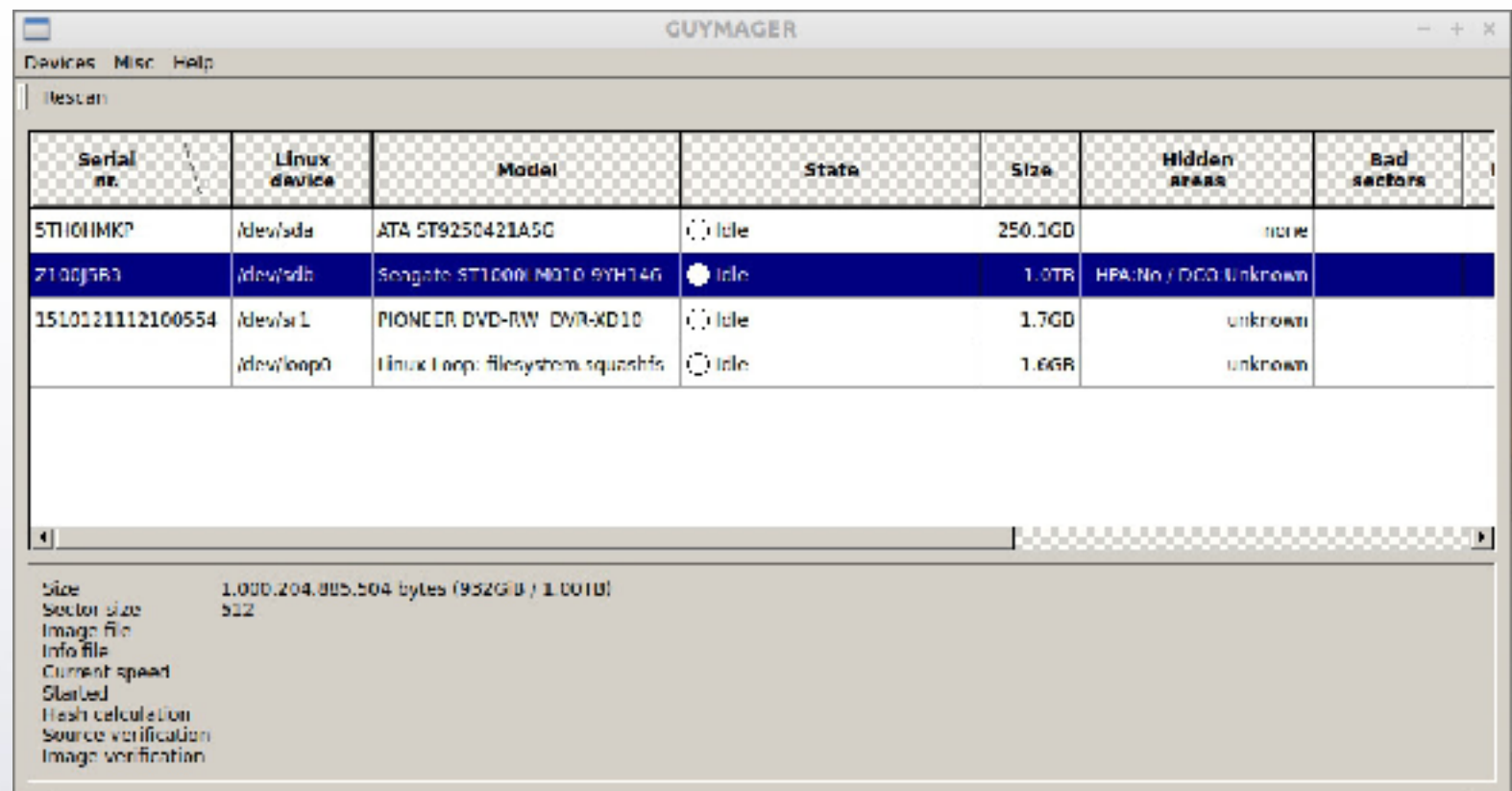
Errore software/hardware o danneggiamento informatico?

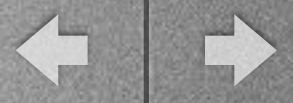


Case study: “la storia non si cancella”

- Si avvia il server con DEFT e con Guymager si crea un'immagine forense del disco, in EWF

deft





Case study: “la storia non si cancella”

- Tentiamo di montare la copia forense ma, come immaginabile, non ci sono partizioni

```
deft8vm /mnt/hgfs/Shared % fdisk -l img.dd

Disk img.dd: 74 MB, 74560000 bytes
255 heads, 63 sectors/track, 9 cylinders, total 145625 sectors
Units = sectors of 1 * 512 = 512 bytes
Sector size (logical/physical): 512 bytes / 512 bytes
I/O size (minimum/optimal): 512 bytes / 512 bytes
Disk identifier: 0x00000000

Disk img.dd doesn't contain a valid partition table
```

- Apriamo l'immagine EWF in un hex editor (FTK Imager) e verifichiamo se ci sono dati...





Case study: “la storia non si cancella”

- La parte iniziale del disco è piena di 0x00
- Ad un certo punto però dei dati sembrano esserci
- Questo è quello che troviamo...

0000000000	01 01 01 03 00 00 C0 20 20 20 20 20 20 00 00
0000000010	02 02 02 03 00 00 C0 20-20 20 20 20 20 20 00 00
0000000020	02 02 02 03 00 00 C0 20 20 20 20 20 20 20 00 00
0000000030	02 02 02 03 00 00 C0 20-20 20 20 20 20 20 00 00
0000000040	02 02 02 03 00 00 C0 20-20 20 20 20 20 20 00 00
0000000050	02 02 02 03 00 00 C0 20-20 20 20 20 20 20 00 00
0000000060	02 02 02 03 00 00 C0 20-20 20 20 20 20 20 00 00
0000000070	02 02 02 03 00 00 C0 20-20 20 20 20 20 20 00 00
0000000080	02 02 02 03 00 00 C0 20-20 20 20 20 20 20 00 00
0000000090	02 02 02 03 00 00 C0 20 20 20 20 20 20 20 00 00
00000000a0	02 02 02 03 00 00 C0 20-20 20 20 20 20 20 00 00
00000000b0	02 02 02 03 00 00 C0 20 20 20 20 20 20 20 00 00
00000000c0	02 02 02 03 00 00 C0 20-20 20 20 20 20 20 00 00
00000000d0	02 02 02 03 00 00 C0 20 20 20 20 20 20 20 00 00
00000000e0	02 02 02 03 00 00 C0 20-20 20 20 20 20 20 00 00
00000000f0	02 02 02 03 00 00 C0 20-20 20 20 20 20 20 00 00
0000000100	02 02 02 03 00 00 C0 20-20 20 20 20 20 20 00 00
0000000110	02 02 02 03 00 00 C0 20-20 20 20 20 20 20 00 00
0000000120	02 02 02 03 00 00 C0 20-20 20 20 20 20 20 00 00
0000000130	02 02 02 03 00 00 C0 20-20 20 20 20 20 20 00 00
0000000140	02 02 02 03 00 00 C0 20 20 20 20 20 20 20 00 00
0000000150	02 02 02 03 00 00 C0 20-20 20 20 20 20 20 00 00
0000000160	02 02 02 03 00 00 C0 20 20 20 20 20 20 20 00 00
0000000170	02 02 02 03 00 00 C0 20-20 20 20 20 20 20 00 00
0000000180	02 02 02 03 00 00 C0 20 20 20 20 20 20 20 00 00
0000000190	02 02 02 03 00 00 C0 20-20 20 20 20 20 20 00 00
00000001a0	02 02 02 03 00 00 C0 20-20 20 20 20 20 20 00 00
00000001b0	02 02 02 03 00 00 C0 20-20 20 20 20 20 20 00 00
00000001c0	02 02 02 03 00 00 C0 20-20 20 20 20 20 20 00 00
00000001d0	02 02 02 03 00 00 C0 20-20 20 20 20 20 20 00 00
00000001e0	02 02 02 03 00 00 C0 20-20 20 20 20 20 20 00 00
00000001f0	02 02 02 03 00 00 C0 20 20 20 20 20 20 20 00 00
0000000200	02 02 02 03 00 00 C0 20 20 20 20 20 20 20 00 00
0000000210	02 02 02 03 00 00 C0 20-20 20 20 20 20 20 00 00
0000000220	02 02 02 03 00 00 C0 20-20 20 20 20 20 20 00 00
0000000230	02 02 02 03 00 00 C0 20 20 20 20 20 20 20 00 00
0000000240	02 02 02 03 00 00 C0 20-20 20 20 20 20 20 00 00
0000000250	02 02 02 03 00 00 C0 20-20 20 20 20 20 20 00 00



Case study: “la storia non si cancella”

- Questo è quello che avremmo dovuto trovare...
- Un MBR, o settore di avvio, con qualcosa all'interno dei primi 512 byte

00000000	EB 40 90 00 00 00 00 00-00	00 00 00 00 00 00 00 00	00 00 00 00 00 00 00 00	00 00 00 00 00 00 00 00	00 00 00 00 00 00 00 00	00 00 00 00 00 00 00 00	00 00 00 00 00 00 00 00
00000001	00 00 00 00 00 00 00 00	00 00 00 00 00 00 00 00	00 00 00 00 00 00 00 00	00 00 00 00 00 00 00 00	00 00 00 00 00 00 00 00	00 00 00 00 00 00 00 00	00 00 00 00 00 00 00 00
00000002	00 00 00 00 00 00 00 00	00 00 00 00 00 00 00 00	00 00 00 00 00 00 00 00	00 00 00 00 00 00 00 00	00 00 00 00 00 00 00 00	00 00 00 00 00 00 00 00	00 00 00 00 00 00 00 00
00000003	00 00 00 00 00 00 00 00	00 00 00 00 00 00 00 00	00 00 00 00 00 00 00 00	00 00 00 00 00 00 00 00	00 00 00 00 00 00 00 00	00 00 00 00 00 00 00 00	00 00 00 00 00 00 00 00
00000004	FF 00 00 80 80 00 EB 03-00	08 FA 80 CB 80 EB 58	00 00 00 00 00 00 00 00	00 00 00 00 00 00 00 00	00 00 00 00 00 00 00 00	00 00 00 00 00 00 00 00	00 00 00 00 00 00 00 00
00000005	7C 00 00 31 C0 8E 08 8E 00	8C 00 2C FB AD 40 7C	00 00 00 00 00 00 00 00	00 00 00 00 00 00 00 00	00 00 00 00 00 00 00 00	00 00 00 00 00 00 00 00	00 00 00 00 00 00 00 00
00000006	5C EF 74 02 88 C2 52 BE-79	7D E8 34 01 F6 C2 8C	00 00 00 00 00 00 00 00	00 00 00 00 00 00 00 00	00 00 00 00 00 00 00 00	00 00 00 00 00 00 00 00	00 00 00 00 00 00 00 00
00000007	74 54 B4 41 EB AA 55 CD 13	5A 52 72 45 81 FB 55	00 00 00 00 00 00 00 00	00 00 00 00 00 00 00 00	00 00 00 00 00 00 00 00	00 00 00 00 00 00 00 00	00 00 00 00 00 00 00 00
00000008	AA 75 43 A0 41 7C 84 C0-75	05 83 E1 01 74 37 66	00 00 00 00 00 00 00 00	00 00 00 00 00 00 00 00	00 00 00 00 00 00 00 00	00 00 00 00 00 00 00 00	00 00 00 00 00 00 00 00
00000009	EB 4C 10 BE 05 7C C6 44 FF	01 66 8E 1E 44 7C C7	00 00 00 00 00 00 00 00	00 00 00 00 00 00 00 00	00 00 00 00 00 00 00 00	00 00 00 00 00 00 00 00	00 00 00 00 00 00 00 00
0000000A	14 10 00 C7 44 02 01 00-66	89 5C 0E C7 44 0E 0C	00 00 00 00 00 00 00 00	00 00 00 00 00 00 00 00	00 00 00 00 00 00 00 00	00 00 00 00 00 00 00 00	00 00 00 00 00 00 00 00
0000000B	70 66 31 C0 09 44 04 56-09	44 0C D4 42 CD 12 72	00 00 00 00 00 00 00 00	00 00 00 00 00 00 00 00	00 00 00 00 00 00 00 00	00 00 00 00 00 00 00 00	00 00 00 00 00 00 00 00
0000000C	15 BB 00 70 EB 7D B4 08-CD	13 73 0A F6 C3 8C 0F	00 00 00 00 00 00 00 00	00 00 00 00 00 00 00 00	00 00 00 00 00 00 00 00	00 00 00 00 00 00 00 00	00 00 00 00 00 00 00 00
0000000D	74 F0 00 F9 0D 00 DE 05-7C	C6 44 FF 00 60 01 00	00 00 00 00 00 00 00 00	00 00 00 00 00 00 00 00	00 00 00 00 00 00 00 00	00 00 00 00 00 00 00 00	00 00 00 00 00 00 00 00
0000000E	E8 F0 10 56 89 14 04 31-D2	88 C7 C1 E2 02 8E EB	00 00 00 00 00 00 00 00	00 00 00 00 00 00 00 00	00 00 00 00 00 00 00 00	00 00 00 00 00 00 00 00	00 00 00 00 00 00 00 00
0000000F	00 F4 40 09 44 00 31 C0-00	D0 C0 EF 02 60 09 04	00 00 00 00 00 00 00 00	00 00 00 00 00 00 00 00	00 00 00 00 00 00 00 00	00 00 00 00 00 00 00 00	00 00 00 00 00 00 00 00
00000010	E6 A1 14 7C 66 31 D2 66-F7	34 88 54 0A 66 31 D2	00 00 00 00 00 00 00 00	00 00 00 00 00 00 00 00	00 00 00 00 00 00 00 00	00 00 00 00 00 00 00 00	00 00 00 00 00 00 00 00
00000011	E6 F7 74 04 88 54 0B 89-44	0C 3B 44 0F 7D 3C 8A	00 00 00 00 00 00 00 00	00 00 00 00 00 00 00 00	00 00 00 00 00 00 00 00	00 00 00 00 00 00 00 00	00 00 00 00 00 00 00 00
00000012	E4 0D C0 E2 06 8A 4C 0A FE	C1 08 D1 8A 6C 0C 5A	00 00 00 00 00 00 00 00	00 00 00 00 00 00 00 00	00 00 00 00 00 00 00 00	00 00 00 00 00 00 00 00	00 00 00 00 00 00 00 00
00000013	EA 74 0B EB 00 70 8E C3-31	DB B8 01 02 CD 1E 72	00 00 00 00 00 00 00 00	00 00 00 00 00 00 00 00	00 00 00 00 00 00 00 00	00 00 00 00 00 00 00 00	00 00 00 00 00 00 00 00
00000014	2A 9C C3 8E 06 48 7C 60 1E	E9 00 01 8E D5 31 F6	00 00 00 00 00 00 00 00	00 00 00 00 00 00 00 00	00 00 00 00 00 00 00 00	00 00 00 00 00 00 00 00	00 00 00 00 00 00 00 00
00000015	51 FF 5C F3 A5 1F 51 FF-26	42 7C BE 7F 7D EB 4C	00 00 00 00 00 00 00 00	00 00 00 00 00 00 00 00	00 00 00 00 00 00 00 00	00 00 00 00 00 00 00 00	00 00 00 00 00 00 00 00
00000016	00 EB 0E BE 84 7D E8 38 00	EB 06 BE 8E 7D EB 3C	00 00 00 00 00 00 00 00	00 00 00 00 00 00 00 00	00 00 00 00 00 00 00 00	00 00 00 00 00 00 00 00	00 00 00 00 00 00 00 00
00000017	10 BE 93 7D E8 2A 00 EB-FE	47 52 55 42 2C 0C 47	00 00 00 00 00 00 00 00	00 00 00 00 00 00 00 00	00 00 00 00 00 00 00 00	00 00 00 00 00 00 00 00	00 00 00 00 00 00 00 00
00000018	05 GF 5D 00 40 51 72 54-20	44 69 7C 6D 0C 52 6C	00 00 00 00 00 00 00 00	00 00 00 00 00 00 00 00	00 00 00 00 00 00 00 00	00 00 00 00 00 00 00 00	00 00 00 00 00 00 00 00
00000019	61 64 00 20 15 72 72 5F-72	00 BB 01 0C B4 0E CD	00 00 00 00 00 00 00 00	00 00 00 00 00 00 00 00	00 00 00 00 00 00 00 00	00 00 00 00 00 00 00 00	00 00 00 00 00 00 00 00
0000001A	10 AC 3C 00 75 74 C3 00-00	00 00 00 00 00 00 00 00	00 00 00 00 00 00 00 00	00 00 00 00 00 00 00 00	00 00 00 00 00 00 00 00	00 00 00 00 00 00 00 00	00 00 00 00 00 00 00 00
0000001B	10 00 00 00 00 00 00 00	00 00 00 00 00 00 00 00	00 00 00 00 00 00 00 00	00 00 00 00 00 00 00 00	00 00 00 00 00 00 00 00	00 00 00 00 00 00 00 00	00 00 00 00 00 00 00 00
0000001C	02 00 03 FE FF FF 01 00-00	00 9F CA 9C 04 00 FE	00 00 00 00 00 00 00 00	00 00 00 00 00 00 00 00	00 00 00 00 00 00 00 00	00 00 00 00 00 00 00 00	00 00 00 00 00 00 00 00
0000001D	FF FF 8E 1E FF FF A0 CA-90	04 A0 D6 6B 1E 00 00	00 00 00 00 00 00 00 00	00 00 00 00 00 00 00 00	00 00 00 00 00 00 00 00	00 00 00 00 00 00 00 00	00 00 00 00 00 00 00 00
0000001E	10 00 00 00 00 00 00 00	00 00 00 00 00 00 00 00	00 00 00 00 00 00 00 00	00 00 00 00 00 00 00 00	00 00 00 00 00 00 00 00	00 00 00 00 00 00 00 00	00 00 00 00 00 00 00 00
0000001F	10 00 00 00 00 00 00 00	00 00 00 00 00 00 00 00	00 00 00 00 00 00 00 00	00 00 00 00 00 00 00 00	00 00 00 00 00 00 00 00	00 00 00 00 00 00 00 00	00 00 00 00 00 00 00 00
00000020	10 00 00 00 00 00 00 00	00 00 00 00 00 00 00 00	00 00 00 00 00 00 00 00	00 00 00 00 00 00 00 00	00 00 00 00 00 00 00 00	00 00 00 00 00 00 00 00	00 00 00 00 00 00 00 00
00000021	10 00 00 00 00 00 00 00	00 00 00 00 00 00 00 00	00 00 00 00 00 00 00 00	00 00 00 00 00 00 00 00	00 00 00 00 00 00 00 00	00 00 00 00 00 00 00 00	00 00 00 00 00 00 00 00
00000022	10 00 00 00 00 00 00 00	00 00 00 00 00 00 00 00	00 00 00 00 00 00 00 00	00 00 00 00 00 00 00 00	00 00 00 00 00 00 00 00	00 00 00 00 00 00 00 00	00 00 00 00 00 00 00 00
00000023	10 00 00 00 00 00 00 00	00 00 00 00 00 00 00 00	00 00 00 00 00 00 00 00	00 00 00 00 00 00 00 00	00 00 00 00 00 00 00 00	00 00 00 00 00 00 00 00	00 00 00 00 00 00 00 00
00000024	10 00 00 00 00 00 00 00	00 00 00 00 00 00 00 00	00 00 00 00 00 00 00 00	00 00 00 00 00 00 00 00	00 00 00 00 00 00 00 00	00 00 00 00 00 00 00 00	00 00 00 00 00 00 00 00
00000025	10 00 00 00 00 00 00 00	00 00 00 00 00 00 00 00	00 00 00 00 00 00 00 00	00 00 00 00 00 00 00 00	00 00 00 00 00 00 00 00	00 00 00 00 00 00 00 00	00 00 00 00 00 00 00 00
00000026	10 00 00 00 00 00 00 00	00 00 00 00 00 00 00 00	00 00 00 00 00 00 00 00	00 00 00 00 00 00 00 00	00 00 00 00 00 00 00 00	00 00 00 00 00 00 00 00	00 00 00 00 00 00 00 00



Case study: “la storia non si cancella”

- Tentiamo di ricostruire le partizioni
- Non possiamo lavorare sull'immagine EWF che è “congelata” per non alterare i dati e mantenere la catena di conservazione
- Come possiamo procedere?





Case study: “la storia non si cancella”

- Due alternative almeno per “scongellare” la copia forense EWF, vediamo come fare in DEFT:
- Riverso l'EWF su un disco creando un “clone” di quello originario

```
ewfmount img.ewf /mnt/ewf
```

```
dcfldd if=/mnt/ewf/ewf1 of=/dev/sdb
```

- Uso “xmount” da DEFT per convertire virtualmente in real time l'EWF in un DD, utilizzando il caching

```
xmount -in ewf -out dd -cache img.cache img.ewf /mnt/ewf
```





Case study: “la storia non si cancella”

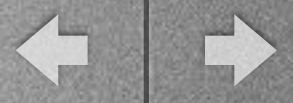
- Una volta che ho una copia modificabile (ovviamente l'originale in entrambi i casi rimarrà integro) procedo con un tool di partition recovery, sul disco clone o sul virtual raw dd
- Utilizziamo “testdisk”, presente in DEFT, che ovviamente conferma che manca la chiusura dell'MBR, cioè i byte “0xAA55”

```
TestDisk 6.11, Data Recovery Utility, April 2009
Christophe GRENIER <grenier@cgsecurity.org>
http://www.cgsecurity.org

Disk /mnt/ewf/ewf1 - 1000 GB / 931 GiB - CHS 121602 255 63 (R0)
Current partition structure:
    Partition                Start          End      Size in sectors

Partition sector doesn't have the endmark 0xAA55
```





Case study: “la storia non si cancella”

- Testdisk propone alcune alternative, le testiamo e riusciamo a ricostruire le partizioni così da poterle visualizzare con “mmls” e montare su una directory

```
# mmls /mnt/ewf/img.dd
DOS Partition Table
Offset Sector: 0
Units are in 512-byte sectors
```

	Slot	Start	End	Length	Description
00:	Meta	0000000000	0000000000	0000000001	Primary Table (#0)
01:	-----	0000000000	0000000062	0000000063	Unallocated
02:	00:00	0000000063	1145234556	1145234552	Linux (0x83)
03:	-----	1145334624	1145643544	0000004124	Unallocated

```
# mount -o ro,loop,offset=$((63*512)) /mnt/ewf/img.dd /mnt/p2
```




Case study: “la storia non si cancella”

- Andiamo a visualizzare il contenuto della partizione e cominciamo a esplorare il folder /var/log
- Trovo i file wtmp (last access, runlevel switch, reboot, shutdown) e btmp (come wtmp ma per tentativi falliti)
- Non si possono leggere i file direttamente perché sono strutturati: uso i comandi “last” e “lastb” con opportuni parametri

last -wix -f wtmp lastb -wix -f btmp





Case study: “la storia non si cancella”

Parametri utilizzati per “last” e “lastb” (man last):

- w: Display full user and domain names in the output.
- i: This option is like -d in that it displays the IP number of the remote host, but it displays the IP number in numbers-and-dots notation.
- x: Display the system shutdown entries and run level changes.
- f file: Specifies a file to search other than /var/log/wtmp.





Case study: “la storia non si cancella”

- Andiamo in /root e vediamo se c'è traccia degli ultimi comandi digitati in “.bash_history” e... sorpresa!

```
# cat .bash_history

fdisk -l
dd if=/dev/sda of=/root/sda.bin bs=512 count=1
dd if=/dev/zero of=/dev/sda bs=512 count=1
rm .bash_history
reboot
```

- Ciò che è avvenuto pare ovvio ma la domanda è: perché nonostante il “rm .bash_history” la history è rimasta? :-)





Case study: “la storia non si cancella”

- La history di ogni sessione viene regolata tramite le seguenti variabili

```
deft8vm /var/log % set | grep HIS  
HISTCONTROL=ignoredups:ignorespace  
HISTFILE=/root/.bash_history  
HISTFILESIZE=2000  
HISTSIZE=1000  
deft8vm /var/log %
```

- Cancellando il file `.bash_history` quindi si elimina la history vecchia, ma al logout viene scritta quella della sessione corrente!





Q & A

Grazie per l'attenzione!

