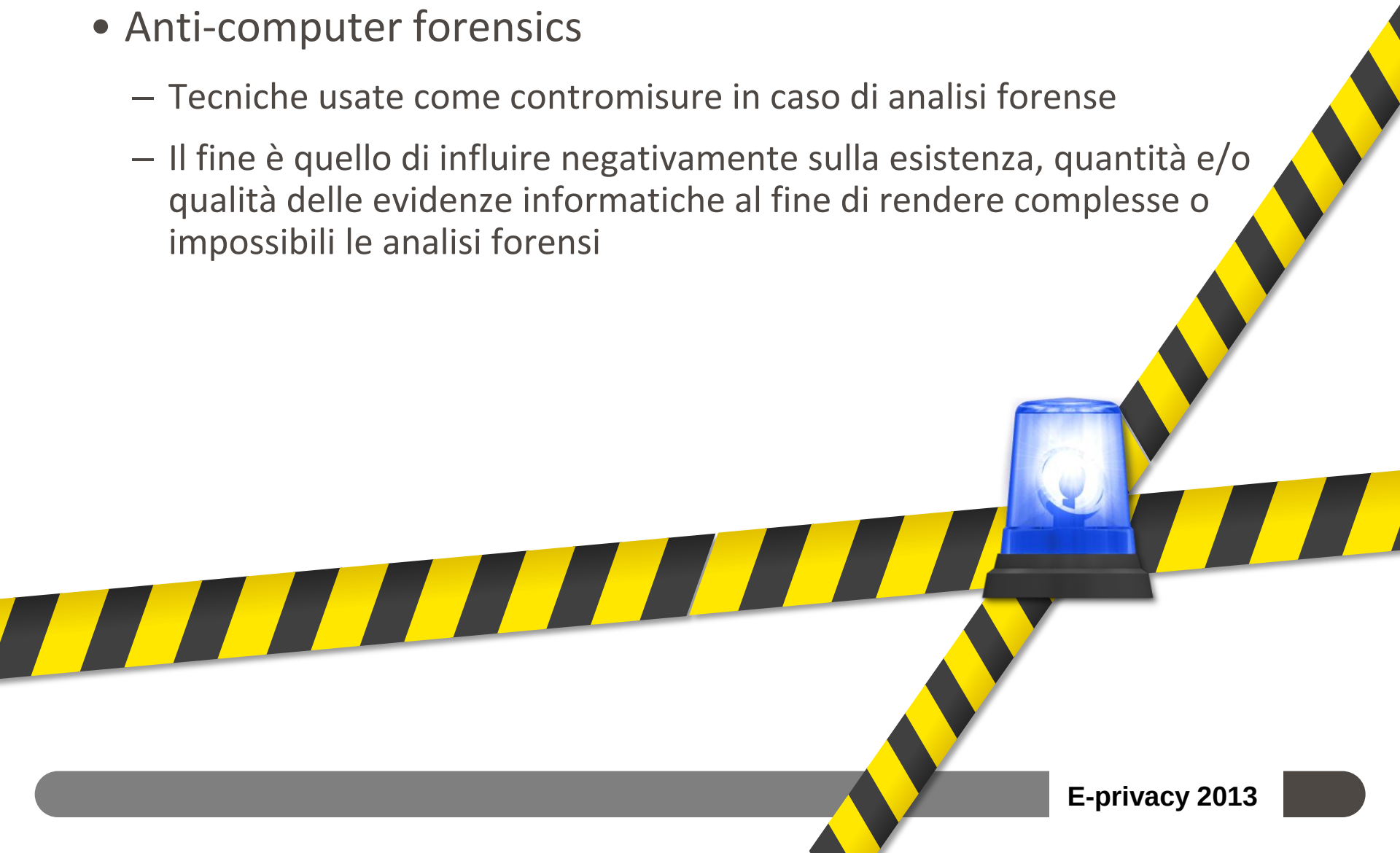
Pratiche di Anti-computer forensics per la postazione personale

E-privacy 2013 – Firenze

Gabriele Zanoni

Definizione

- Anti-computer forensics
  - Tecniche usate come contromisure in caso di analisi forense
  - Il fine è quello di influire negativamente sulla esistenza, quantità e/o qualità delle evidenze informatiche al fine di rendere complesse o impossibili le analisi forensi



Macro categorie

- **Nascondere** -> cifrare, cartelle nascoste..
- **Cancellare** -> wiping, distruzione dischi…
- **Offuscare** -> creare confusione, falsificare date, cancellare log, cambiare header ai file…
- **Anti-CF-Tools** -> attaccare i tool che fanno analisi forense

Lo scenario in questione

- Immaginiamo di costruire un PC Windows «a prova di analisi forense»…
- Presenteremo le tecniche che realisticamente possiamo adottare (senza perderci nelle tecniche avanzate che tipicamente hanno tipicamente lo svantaggio di essere time-consuming)

Windows®

Partiamo dal disco

- Quale disco? [1] [2]

- O usiamo una SD/CF facile da rimuovere? [3]

[1] http://www.tomshardware.com/news/solid-state-flash-translation-layer-NAND-FAST-11-Sanitization,12252.html
[2] http://www.kingston.com/us/community/articledetail?articleid=10
[3] http://www.thinkwiki.org/wiki/CompactFlash_boot_drive

Hai detto RAID?

- Ricostruire il RAID spesso senza saperne la configurazione originaria (tipologia, dimensioni settori, etc…) è un terno al lotto
- Esistono software che mettono insieme le immagini dei singoli dischi del RAID e ne fanno l'analisi. Valutano l'entropia della relativa combinazione generata cercando in questo modo di indentificare quella più probabile [1]
- RAID non standard (spesso su SAN/NAS etc…) [2]

[1] http://www.runtime.org/raid.htm
[2] http://www.synology.com/support/tutorials_show.php?lang=ita&q_id=492

Scelta del File System

- File System particolari potrebbero non essere ben supportati dai tool di analisi forense
- Problemi riscontrati nel corso tempo:
  - Alcune distribuzioni forensi non supportavano Ext4
  - Tool per analizzare o recuperare file da un File System NTFS compresso
  - Anche all'uscita di exFat si sono riscontrati problemi di supporto per la lettura e per il recupero di file cancellati

Spesso il supporto (o meno) di certe tecnologie dipende da problemi legati ai relativi brevetti o alla scarsa diffusione di queste tecnologie. Nella maggior parte dei casi è stato sufficiente aspettare ed il supporto anche per le tecnologie più nuove o di nicchia è stato raggiunto.

Password HDD

- Password sul disco (!= password sul Bios)
- Diverse compagnie di recovery dei dati affermano di poter bypassare questa password [1] [2]

[1] http://www.hddunlock.com/
[2] http://www.pwcrack.com/harddisk.shtml

Cifratura

- Disco
  - WDE - PGP: per la cifratura del disco e della posta
  - TrueCrypt Hidden Partition
  - BitLocker

- Dati:
  - Potete anche cifrare i singoli documenti o archivi all'interno di un file system cifrato.
  - Non lasciare email critiche in chiaro sul server di posta -> scaricarle soprattutto se non sono cifrate. E sul telefono ?
  - Ricordiamoci che anche per i backup è importante la cifratura

Ricordatevi della sicurezza fisica!

EVIL MAID ATTACK

[1] https://www.trustedcomputinggroup.org/resources/evil_maid_attacks_on_encrypted_hard_drives
[2] http://theinvisiblethings.blogspot.it/2009/10/evil-maid-goes-after-truecrypt.html

Password

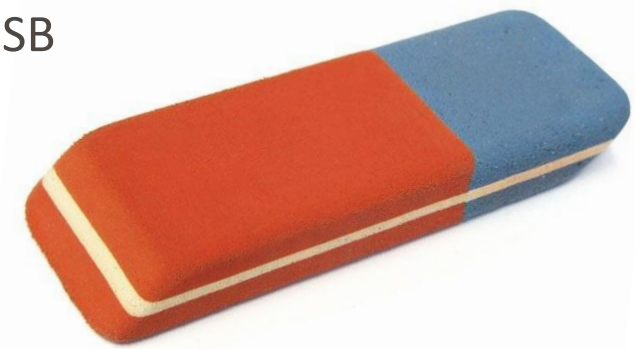
- All'accesso
- Dopo lo screensaver [1]
- Conservate con sistemi sicuri come KeePass [2]
- Password diverse per diversi servizi!
- 2FA

"I needed a password eight characters long, so I picked Snow White and the Seven Dwarfs"

[1] http://www.microsoft.com/resources/documentation/windows/xp/all/proddocs/en-us/display_assign_screensaver_password.mspx?mfr=true
[2] http://keepass.info/

Cancellare… bene

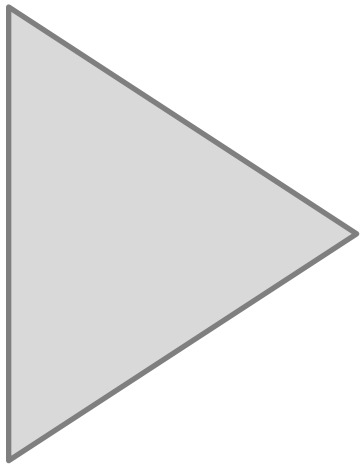
- Deframmentare spesso
- Da Vista in poi i job di deframmentazione e chkdisk sono automatici e in background (Self-Healing File System) [1]
- Sovrascrivere quando si cancella (CCleaner, Eraser etc..)[2] [3]
- Usare le nuove opzioni di zeroing a più passate del comando «Format» [4]
- Cancellare bene… anche gli HD esterni e le penne USB



[1] http://technet.microsoft.com/en-us/library/cc771388(v=ws.10).aspx
[2] http://security.stackexchange.com/questions/10464/why-is-writing-zeros-or-random-data-over-a-hard-drive-multiple-times-better-th
[3] http://www.infosecisland.com/blogview/16130-The-Urban-Legend-of-Multipass-Hard-Disk-Overwrite.html
[4] http://technet.microsoft.com/en-us/library/51ec7423-9a01-4219-868a-25d69cdcc832

Cancellare i dati bene e velocemente?

VIDEO



http://www.youtube.com/watch?v=_42QugHuWfs

USB security

- Setupapi.log
- HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Enum\USB STOR
- Usare USBhistory/UsbLogView per controllare che non sia rimasto nulla [1]
- Le penne Cruzer U3 creano altri file in posizioni diverse da quelle standard [2]

[1] http://www.nirsoft.net/utils/usb_log_view.html
[2] http://forums.sandisk.com/t5/All-SanDisk-USB-Flash-Drives/Pass-protected-cruzer-not-accessible-on-win7-and-xp-Any-help-is/td-p/186623

Minimizzare le informazioni lasciate sul sistema 1/2

- Disabilitare l'ibernazione ('Change advanced power settings' -> 'Sleep' -> 'Hibernate After' -> 'Never') [1]
- Disabilitare i "System Restore Points" [2]
- Disabilitare il "Send Error Report to Microsoft" [3]
- Disabilitare le informazioni di debug "Disable Debugging Upon Failure" [4]

[1] http://support.microsoft.com/kb/920730
[2] http://support.microsoft.com/kb/264887
[3] http://www.microsoft.com/resources/documentation/windows/xp/all/proddocs/en-us/sysdm_advancd_exception_reporting.mspx?mfr=true
[4] "Right click on Computer and go to Advanced System Settings, now go to Start Up and Recovery. Now, set Debugging Information to None"

Minimizzare le informazioni lasciate sul sistema 2/2

- Disabilitare il “Windows Event Logging” [1] [2]
- No Standby

```
Windows Registry Editor Version 5.00

[HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Servic es\ACPI\Parameters]
"AMLIMaxCTObjs"=hex:04,00,00,00 "Attributes"=dword:0070
[HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Servic es\ACPI\Parameters\WakeUp]
"FixedEventMask"=hex:20,05 "FixedEventStatus"=hex:00,84 "GenericEventMask"=hex:18,50,00,10
"GenericEventStatus"=hex:10,00,ff,00
```

[1] http://technet.microsoft.com/en-us/library/dd315601(v=ws.10).aspx
[2] http://www.windows-commandline.com/2011/03/enable-disable-event-log-service.html

Timeline

Timestomp e touch per cambiare MACE/MAC aka Modified, Accessed, Changed, Entry Changed (valore di controllo di NTFS)

LastAccess time can be disabled in two ways:

HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Control\FileSystem

Set DWORD NtfsDisableLastAccessUpdate = 1

OR open Command Prompt as Administrator:

FSUTIL behavior set disablelastaccess 1

Traffico rete

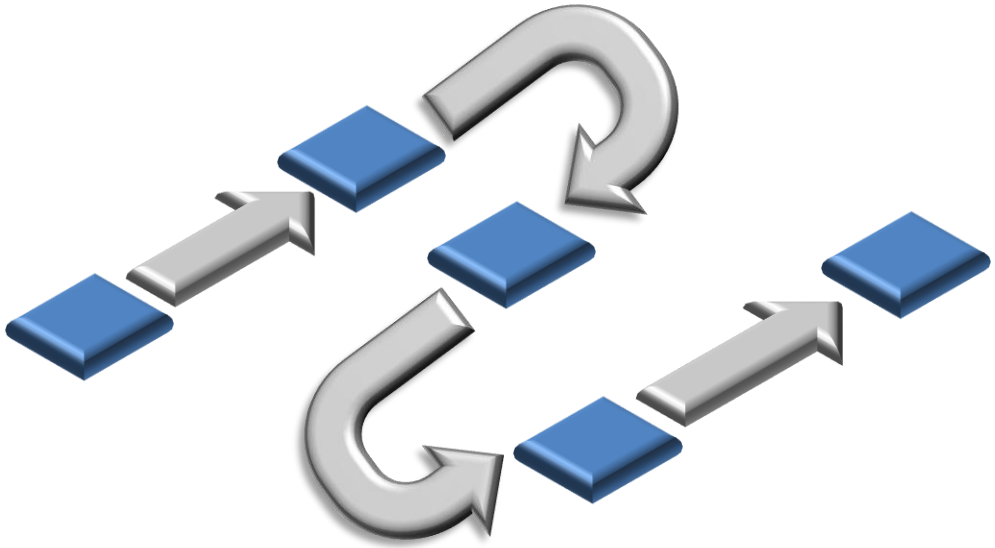
- Contro le intercettazioni del traffico di rete possiamo usare Sniffjoke per cercare di rendere difficile la ricostruzione dei pacchetti e mandare in errore gli sniffer di rete
- Usare SSL sempre!
  (e.g. Plugin per forzare SSL sul browser) [2]
- Tenere presente i controlli di base per verificare che SSL sia implementato correttamente. Oppure controllare con Qualys SSLLabs.

QUALYS® SSL LABS

[1] http://www.delirandom.net/sniffjoke/
[2] https://www.eff.org/https-everywhere
[3] https://www.ssllabs.com/

Dati in transito

- Se si usano degli alias per l'email fare attenzione a come transita il flusso ed i possibili punti dove potrebbe essere intercettato
- Usare SSL, SSH, SCP, SFTP, PGP etc..
- I dati critici dovrebbero essere cifrati prima di essere mandati o conservati nel Cloud (e.g. Dropbox etc..)



Cronologie

- I moderni Windows quando cancellano la cronologia wipano a zero il file .dat di Internet Explorer [1]
- Usare le modalità di navigazione anonima che creano meno log e lasciano meno informazioni agli esaminatori
- Usare sistemi di DoNotTrack [2]
- Informazioni private potrebbero essere usate dalle funzioni avanzate dei browser [3]

[1] http://blogs.msdn.com/b/wndp/archive/2006/08/04/wininet-index-dat.aspx
[2] http://donottrack.us/
[3] http://support.google.com/chromeos/bin/answer.py?hl=it&answer=114836

Rinominare o…

- Mismatch tra estensioni e contenuto.
- Iniettare un header ed un footer in un file? [1]

```
if opt.type =="jpg":
        header = "\xFF\xD8\xFF\xE0\x00\x10"
        footer = "\xFF\xD9"
elif opt.type =="gif":
        header = "\x47\x49\x46\x38\x37\x61"
        footer = "\x00\x3B"
elif opt.type =="png":
        header = "\x50\x4E\x47?"
        footer = "\xFF\xFC\xFD\xFE"
elif opt.type =="bmp":
        header = "BM??\x00\x00\x00"
        footer = ""
elif opt.type =="tif":
        header = "\x49\x49\x2A\x00"
        footer = ""
```

[1] python bee.py -t gif -i php-backdoor.php -o my-shell.gif
https://github.com/bee-project/core

Oltre la cifratura: nascondere

- Sicuramente usabili:
  - Steganografia [1] [2]
  - ADS
- Storicamente [3]:
  - RuneFS scrive nell'inode dei bad block
  - WaffenFS finto journal di EXT3 ad EXT2 (fino a 32 MB)
  - KY FS inode delle directory
  - Data Mule FS: dati nel padding e nelle strutture dei metadati

[1] http://www.silenteye.org/index.html?i1s1
[2] http://www.pentagonpost.com/steganography-now-on-facebook/8346042
[3] http://www.blackhat.com/presentations/bh-asia-03/bh-asia-03-grugq/bh-asia-03-grugq.pdf

NSRL VS Hash Collision

- National Software Reference Library (NSRL):
  - Collezione di hash di file noti [1]
  - Centinaia di Giga possono essere ridotti a poche centinaia di Mega

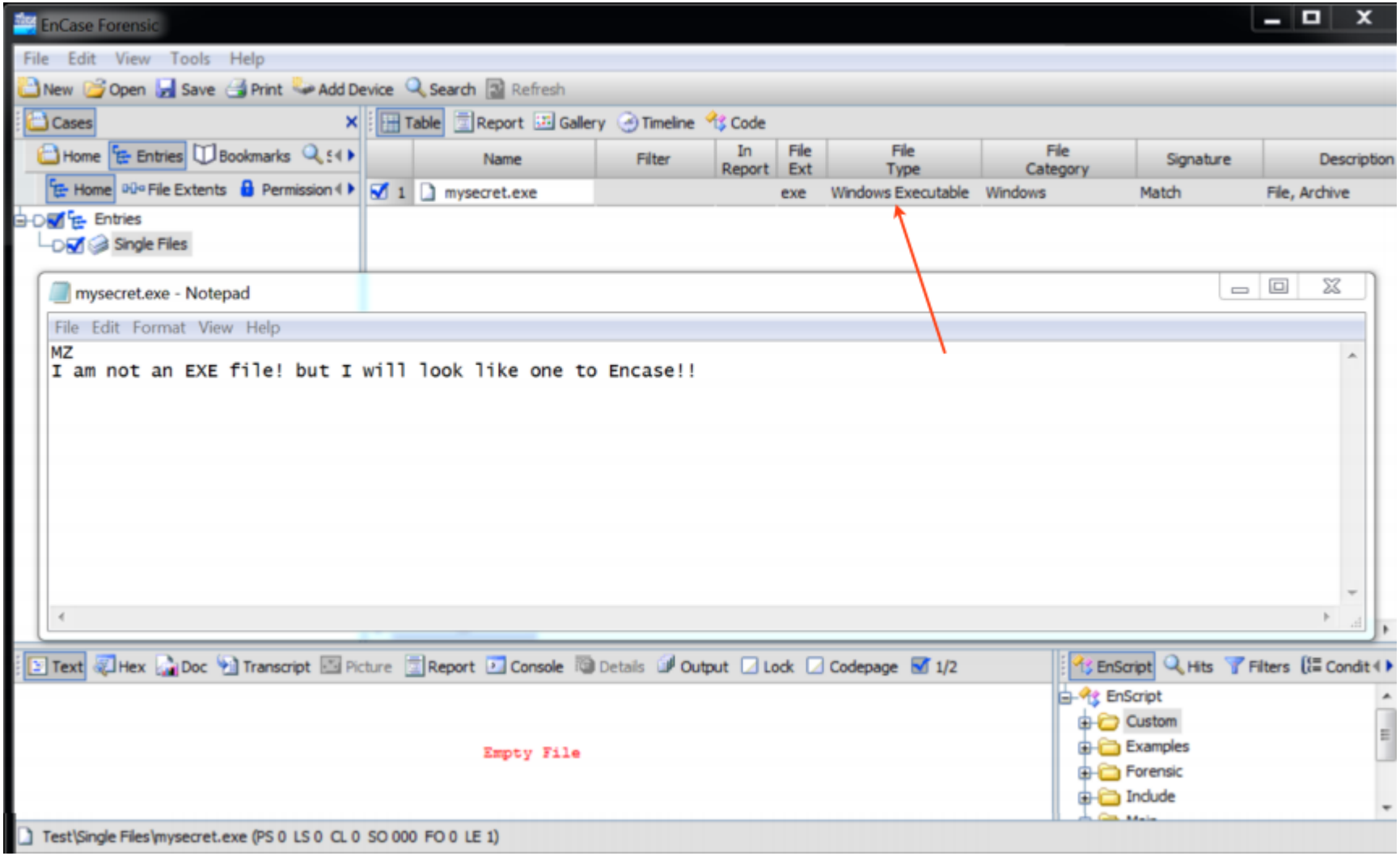
- Hash Collision [2]:
  - Cosa succede quando il vostro file Word ha lo stesso MD5 di rundll.dll ?
  - HashClash [3]

[1] http://www.nsrl.nist.gov/Downloads.htm
[2] http://www.win.tue.nl/hashclash/On%20Collisions%20for%20MD5%20-%20M.M.J.%20Stevens.pdf
[3] https://code.google.com/p/hashclash/

Anti-CF-Tools

- Uso di exploit per tool forensi (EnCase, PTK etc..)
- E.g.
  - Generare n partizioni nell'estesa: per valori di n sufficientemente grande i tool si siedono
  - Remote Code in PTK [1] [2]
- Tools evasion (ZIP Files: PK, EXE Files: MZ, PDF Files: PDF)

[1] http://vimeo.com/2161045
[2] http://www.securityfocus.com/archive/1/498081



http://www.perklin.ca/~defcon20/perklin_antiforensics.pdf

Finezze

- Disabilitare le Jump List dalla scheda Start Menù del pannello Taskbar e Start Menù properties.
- Controllo delle JumpList:
- - Jump Lists - sono le miniature nello Start menu o le icone dei programmi nella Taskbar. Ogni Jump List può contenere Task, link ai documenti recenti, o link a documenti.
- - I dati delle Jump List sono messi per tutte le applicazioni in modo centralizzato nel profilo utente.
- - C:\Users\<username>\AppData\Roaming\Microsoft \Windows\Recent\CustomDestinations
- - C:\Users\<username>\AppData\Roaming\Microsoft \Windows\Recent\AutomaticDestinations

PS: non si vedono da explorer ed il contenuto ha estensione "-ms"

Domande ?

Thank you!

gabriele.zanoni@gmail.com

https://www.twitter.com/infoshaker