(un)fooling timelines

in forensic analysis

EndSummerCamp
3.9.2011

Chi

Cosa

Dove

Come

Raccolta

Elaborazione

Visualizzazione

Problemi

Credits

End Summer Camp

Venezia, 3 settembre 2011

Rebus
Human, Forensicator,
Chaotic Good

(un)fooling timelines

EndSummerCamp
3.9.2011

Rebus
Human, Forensicator,
Chaotic Good

Chi sono

Davide ‘Rebus’ Gabrini

- Per chi lavoro non è un mistero
- Consulente tecnico e Perito forense
- Docente di sicurezza informatica e computer forensics per Corsisoftware srl
- Socio istituzionale IISFA
- Certificazioni CIFI, ACE

Come vedete **non** sono qui in divisa ☺

(un)fooling timelines

EndSummerCamp
3.9.2011

Rebus
Human, Forensicator,
Chaotic Good

Timeline

- Una timeline è una rappresentazione di eventi ordinati cronologicamente
- Gli eventi possono provenire da un'unica fonte o, più sovente, da una pluralità di fonti
- Per le finalità di oggi, ci interessano solo gli eventi di natura digitale, ma un'indagine spesso attinge da fonti molto eterogenee
- Metodo rapido e intuitivo per avere immediata contezza di quanto occorso in un sistema in una determinata finestra temporale

(un)fooling timelines

EndSummerCamp
3.9.2011

Rebus
Human, Forensicator,
Chaotic Good

Timeline

- Utilizzi:
  - Ricostruire le attività di un utente….
  - …o di un intruso.
  - Ricostruire le fasi di un attacco/infezione
  - Individuare il punto di compromissione originale
  - Individuare le cause di un incidente
  - Evidenziare incongruenze che siano sintomo di attività illecite e antiforensics
- Vedere in una rappresentazione lineare la sequenza di creazione di file, chiavi di registro, installazione di servizi ecc. rende comprensibile le modalità di intrusione e permette di individuarne tutti i componenti.

(un)fooling timelines

EndSummerCamp
3.9.2011

Rebus
Human, Forensicator,
Chaotic Good

Da dove arrivano i riferimenti temporali?

- E' importante individuare la fonte dei timestamp: locale (orologio CMOS) o esterna?
- Attendibilità?
- Configurazione Timezone
- Configurazione NTP (server, frequenza di update, ultimo update eseguito ecc.)
- L'applicazione che ha registrato l'evento che tipo di timestamp utilizza?

(un)fooling timelines

EndSummerCamp
3.9.2011

Rebus
Human, Forensicator,
Chaotic Good

Dove sono registrati

- Il primo posto dove guardare è il filesystem, con gli attributi MAC(B) di ogni file/cartella
- Il filesystem non basta: un sistema operativo registra innumerevoli eventi cronologicamente referenziati
- File di log (sistema e applicazioni) e registri degli eventi
- Registro di Windows (contenuto e metadati delle chiavi)
- Feature proprie del sistema operativo (Prefetch, Restore Points, Link, Cestino, thumbs.db, ShellBag, Volume Shadow Copy…)
- Cronologia, Cache e Cookies dei browser
- Cache e database applicativi
- Metadati interni ai documenti (Office, EXIF, pagine HTML…)
- Eventi temporali recuperabili tramite carving da aree deallocate, slack space, memory dump, partizioni di swap, file di ibernazione (record $MFT, chiavi di registro, chat…)

(un)fooling timelines

EndSummerCamp
3.9.2011

Rebus
Human, Forensicator,
Chaotic Good

MAC(B) timestamp

- I timestamp MAC(B) presenti in un filesystem riguardano gli eventi:
  - **M**odified (modifica dei dati)
  - **A**ccessed (lettura dei dati)
  - **C**hanged (modifica dei metadati)
  - **B**irth (creazione del file)
- Non tutti i filesystem registrano le stesse informazioni.
- Non tutti i sistemi operativi sfruttano le possibilità del filesystem.

(un)fooling timelines

EndSummerCamp
3.9.2011

Rebus
Human, Forensicator,
Chaotic Good

MAC(B) Meaning by File System

File System	M	A	C	B
Ext2/3	Modified	Accessed	Changed	N/A
Ext4	Modified	Accessed	Changed	Created
FAT	Written	Accessed	N/A	Created
NTFS	File Modified	Accessed	MFT Modified	Created
UFS	Modified	Accessed	Changed	N/A

(un)fooling timelines

EndSummerCamp
3.9.2011

Rebus
Human, Forensicator,
Chaotic Good

Filesystem e S.O.

- **FAT** registra gli attributi MAC in localtime
- **NTFS** registra 2 serie di attributi MACB in UTC
- Da NT in poi è possibile disabilitare l'aggiornamento dell'attributo Access (per Vista è default)
  - HKLM\SYSTEM\CurrentSet\Control\FileSystem\NtfsDisableLastAccessUpdate
- Linux registra in Unix time (secondi trascorsi dal 1/1/1970 00:00:00 UTC) attributi MAC su **Ext2/3**. Con **Ext4** arriva l'attributo Birth e la granularità al nanosecondo.
  L'aggiornamento degli attributi può essere inibito in fase di mount.
- **HFS+** registra i secondi trascorsi da 1/1/1904 00:00:00 GMT

(un)fooling timelines

EndSummerCamp
3.9.2011

Chi

Cosa

Dove

Come

Raccolta

Elaborazione

Visualizzazione

Problemi

Credits

Rebus
Human, Forensicator,
Chaotic Good

NTFS: dove sono i timestamp?

Per ogni file, la Master File Table ($MFT) registra **due** serie di timestamp:

- **$STANDARD_INFO**

Contiene metadati come SID, owner, flags e un set di timestamp MACB. Sono i timestamp che vedete da Esplora Risorse. Modificabile in **user space**.

- **$FILE_NAME**

Contiene il nome file in Unicode e un ulteriore set di timestamp MACB. Modificabile solo in **kernel space**.

(un)fooling timelines

Quando cambiano i timestamp? (NTFS)

$FILE_NAME	Rename	Local Move	Volume Move	Copy	Access	Modify	Create	Delete
Modification		X	X	X			X	X
Accessed			X	X			X	
Change (meta)		X	X	X			X	X
Born			X	X			X	

$STANDARD_INFO	Rename	Local Move	Volume Move	Copy	Access	Modify	Create	Delete
Modification						X	X	
Accessed			X	X	X	X	X	
Change (meta)	X	X	X	X			X	X
Born				X			X	

- Le regole sulla modifica o preservazione dei timestamp nel casi di copia e spostamento di file tra partizioni FAT e NTFS sono riportate alla pagina http://support.microsoft.com/kb/299648/en-us

(un)fooling timelines

EndSummerCamp
3.9.2011

Chi

Cosa

Dove

Come

Raccolta

Elaborazione

Visualizzazione

Problemi

Credits

Comportamento in Windows 7

Windows 7 File System $STDInfo and $Filename Properties

Timevalue Type	File Rename	Local File Move	Volume File Move	File Copy	File Access	File Modify	File Creation	File Deletion
$STD Info Modification Time						Changed	Changed	
$STD Info Access Time			Changed	Changed	Changed (No Change on VISTA/Win7)	Changed	Changed	
$STD Info Creation Time				Changed			Changed	
$STD Info MFT Entry Modified	Change	Changes	Changed	Changed			Changed	Changed
$Filename Modification Time		Updated to $STDINFO Modification Time		Changed			Changed	Updated to $STDINFO Modification Time
$Filename Access Time			Changed	Changed			Changed	
$Filename Creation Time				Changed			Changed	
$Filename MFT Entry Modified		Updated to $STDINFO Metadata Time		Changed			Changed	Updated to $STDINFO Metadata Time

Rebus
Human, Forensicator, Chaotic Good

(un)fooling timelines

EndSummerCamp
3.9.2011

Rebus
Human, Forensicator,
Chaotic Good

Applicazioni

- Singole applicazioni, però, possono adottare timestamp alternativi:
- Nel registro di Windows, i valori FILETIME riportano il numero di intervalli da 100 nanosecondi trascorsi dal 1/1/1601 00:00:00 UTC
- da MacOSX 10 le applicazioni (p.e. Safari) possono usare il Mac Absolute Time, o CFDate: secondi trascorsi dal 1/1/2001 00:00:00 GMT

(un)fooling timelines

EndSummerCamp
3.9.2011

Rebus
Human, Forensicator,
Chaotic Good

Normalizzazione

Quindi è necessario verificare ogni fonte e uniformare tra loro i diversi timestamp

- Conversione fuso orario
- Compensazione eventuali time skew
- Normalizzazione del formato data-ora
- Ricorso a formati standardizzati
  - Body_file

    MD5|name|inode|mode_as_string|UID|GID|size|atime|mtime|ctime|crtime
  - TLN

    Time|Source|Host|User|Description

(un)fooling timelines

EndSummerCamp
3.9.2011

Rebus
Human, Forensicator,
Chaotic Good

Raccolta dati

(un)fooling timelines

EndSummerCamp
3.9.2011

Rebus
Human, Forensicator,
Chaotic Good

Filesystem - fls

Estrazione MAC(B) tramite fls (SleuthKit) da un'immagine forense:

```
$ fls -f ntfs -o 63 -r -m C: /images/suspect.dd > fs_body_file
```

- **-f**ilesystem-type
- **-o**ffset
- **-r**ecursive
- **-m**ountpoint

Il body_file è un formato intermedio per le timeline previsto dallo SleuthKit:

```
MD5|name|inode|mode_as_string|UID|GID|size|atime|mtime|ctime|crtime
```

I comandi **fls**, **ils** e **mac-robber** generano output in formato body_file; il tool **mactime** legge i body_file e ordina i contenuti in un comodo CSV:

```
$mactime -d -b fs_body_file >fs_timeline.csv
```

(un)fooling timelines

EndSummerCamp
3.9.2011

Chi

Cosa

Dove

Come

Raccolta

Elaborazione

Visualizzazione

Problemi

Credits

Rebus
Human, Forensicator, Chaotic Good

body_file

0|C:/Bootfont.bin|1862-128-3|r/r--x--x--x|0|0|4952|1276960801|1141300800|1141300800|1141300800
0|C:/$AttrDef|4-128-4|r/rr-xr-xr-x|48|0|2560|1276960582|1276960582|1276960582|1276960582
0|C:/$BadClus|8-128-2|r/rr-xr-xr-x|0|0|0|1276960582|1276960582|1276960582|1276960582
0|C:/$BadClus:$Bad|8-128-1|r/rr-xr-xr-x|0|0|49532633088|1276960582|1276960582|1276960582|1276960582
0|C:/$Bitmap|6-128-1|r/rr-xr-xr-x|0|0|1511616|1276960582|1276960582|1276960582|1276960582
0|C:/$Boot|7-128-1|r/rr-xr-xr-x|48|0|8192|1276960582|1276960582|1276960582|1276960582
0|C:/$Extend|11-144-4|d/dr-xr-xr-x|0|0|344|1276960582|1276960582|1276960582|1276960582
0|C:/$LogFile|2-128-1|r/rr-xr-xr-x|0|0|67108864|1276960582|1276960582|1276960582|1276960582
0|C:/$MFT|0-128-1|r/rr-xr-xr-x|0|0|57950208|1276960582|1276960582|1276960582|1276960582
0|C:/$MFTMirr|1-128-1|r/rr-xr-xr-x|0|0|4096|1276960582|1276960582|1276960582|1276960582
0|C:/$Secure:$SDH|9-144-17|r/rr-xr-xr-x|0|0|56|1276960582|1276960582|1276960582|1276960582
0|C:/$Secure:$SII|9-144-16|r/rr-xr-xr-x|0|0|56|1276960582|1276960582|1276960582|1276960582
0|C:/$Secure:$SDS|9-128-0|r/rr-xr-xr-x|0|0|887276|1276960582|1276960582|1276960582|1276960582
0|C:/$UpCase|10-128-1|r/rr-xr-xr-x|0|0|131072|1276960582|1276960582|1276960582|1276960582
0|C:/$Volume|3-128-3|r/rr-xr-xr-x|48|0|0|1276960582|1276960582|1276960582|1276960582
0|C:/AUTOEXEC.BAT|7420-128-1|r/rrwxrwxrwx|0|0|0|1276955179|1276955179|1276955179|1276955179
0|C:/boot.ini|3528-128-10|r/r--x--x--x|0|0|212|1292187989|1276955625|1276955625|1276960966
0|C:/Config.Msi|29593-144-6|d/dr-xr-xr-x|0|0|48|1292189987|1292183363|1292183363|1292180848

(un)fooling timelines

EndSummerCamp
3.9.2011

Chi

Cosa

Dove

Come

Raccolta

Elaborazione

Visualizzazione

Problemi

Credits

Rebus
Human, Forensicator, Chaotic Good

FTK Imager ed Encase

In alternativa a fls, sia FTK Imager che Encase possono esportare CSV contenenti i timestamp di ogni singolo oggetto del filesystem

```
Date,Size,Type,Mode,UID,GID,Meta,File Name
Wed Nov 21 2001 13:13:36,6178,m...,r/rrwxrwxrwx,0,0,51150-128-3,C:/Forensics/Browser/ndphlpr.vxd
Tue Apr 23 2002 20:11:00,261082,m...,r/rrwxrwxrwx,0,0,50090-128-3,C:/IrfanView/Plugins/PopArt.8bf
Thu Oct 17 2002 21:23:14,8200,m..b,r/rrwxrwxrwx,0,0,16305-128-3,C:/Microsoft/OFFICE/DATA/OPA12.BAK
Thu Feb 13 2003 10:43:22,4860,m...,r/rrwxrwxrwx,0,0,50978-128-4,C:/BETA/MFL-FA/RemovableMask.pct
Thu Feb 13 2003 10:44:20,14504,m...,r/rrwxrwxrwx,0,0,50977-128-4,C:/BETA/MFL-FA/RemovableImage.pct
Wed Oct 01 2003 20:40:00,366592,m...,r/rrwxrwxrwx,0,0,51003-128-3,C:/ClamWinPortable/lib/wxc.pyd
Wed Oct 01 2003 20:40:02,35840,m...,r/rrwxrwxrwx,0,0,50988-128-3,C:/ClamWinPortable/lib/htmlc.pyd
Wed Oct 01 2003 20:40:38,71168,m...,r/rrwxrwxrwx,0,0,50987-128-3,C:/ClamWinPortable/lib/gizmosc.pyd
Fri Nov 07 2003 09:42:00,7434,m...,r/rrwxrwxrwx,0,0,44594-128-3,C:/XnView/Masks/PF-Brush.jpg
Fri Nov 07 2003 09:42:00,6445,m...,r/rrwxrwxrwx,0,0,44595-128-4,C:/XnView/Masks/PF-Camera.jpg
Fri Nov 07 2003 09:42:00,11681,m...,r/rrwxrwxrwx,0,0,44596-128-4,C:/XnView/Masks/PF-Diffuse.jpg
Fri Nov 07 2003 09:42:00,5021,m...,r/rrwxrwxrwx,0,0,44597-128-4,C:/XnView/Masks/PF-Ellipse.jpg
Fri Nov 07 2003 09:42:00,5459,m...,r/rrwxrwxrwx,0,0,44598-128-3,C:/XnView/Masks/PF-Fog.jpg
```

(un)fooling timelines

EndSummerCamp
3.9.2011

Chi

Cosa

Dove

Come

Raccolta

Elaborazione

Visualizzazione

Problemi

Credits

Rebus
Human, Forensicator,
Chaotic Good

Registro di Windows - regtime

- Ogni chiave di registro ha un attributo temporale LastWrite
- Lo script regtime.pl di Harlan Carvey permette di estrarre i valori LastWrite dai singoli hive:

```
$ regtime.pl –m HKLM-SYSTEM –r /mnt/target/WINDOWS/system32/config/system  > body
$ regtime.pl –m HKLM-SAM –r /mnt/target/WINDOWS/system32/config/SAM >> body
$ regtime.pl –m HKLM-SECURITY–r /mnt/target/WINDOWS/system32/config/SECURITY >> body
$ regtime.pl –m HKLM-SOFTWARE–r /mnt/target/WINDOWS/system32/config/software >> body
$ regtime.pl –m HKCU-USERNAME –r /mnt/target/Users/USERNAME/NTUSER.DAT >> body
```

- Sempre con mactime.pl si può ottenere un più pratico e ordinato CSV.

(un)fooling timelines

EndSummerCamp
3.9.2011

Rebus
Human, Forensicator,
Chaotic Good

log2timeline - Input

Creato da Kristinn Gudjonsson, è il punto di riferimento del settore.

Dispone di numerosissimi moduli ed è in continua espansione:

- Apache2 Access/Error logs
- Google Chrome history
- Encase e FTK Imager dirlisting
- Windows Event Log files (EVT e EVTX)
- EXIF e metadati da vari formati multimediali
- Firefox bookmark e history
- Generic Linux log file
- Internet Explorer history (file index.dat)
- Windows IIS W3C log files
- ISA server text export.
- Mactime e TLN body files
- McAfee AntiVirus Log files
- MS-SQL Error log
- Opera Global and Direct browser history
- OpenXML metadata (metadati dei documenti Office 2007)
- PCAP files

(un)fooling timelines

EndSummerCamp
3.9.2011

Chi

Cosa

Dove

Come

Raccolta

Elaborazione

Visualizzazione

Problemi

Credits

Rebus
Human, Forensicator,
Chaotic Good

log2timeline - Input

- PDF metadata
- Windows Prefetch directory
- Windows Recycle Bin (INFO2 or I$)
- Windows Restore Points
- Safari Browser history files
- Skype main.db file
- Windows XP SetupAPI.log file
- Adobe Local Shared Object files (SOL/LSO), aka Flash Cookies
- Squid Access Logs (httpd_emulate off)
- Windows Registry Hives
- UserAssist key of the Windows registry
- Windows Shortcut files (LNK)
- Windows WMIProv log file
- Windows XP Firewall Log files (W3C format)
- Volatility: the output file from the psscan and psscan2 modules

(un)fooling timelines

EndSummerCamp
3.9.2011

Rebus
Human, Forensicator,
Chaotic Good

log2timeline e timescanner

- Il metodo più pratico per usare log2timeline e tramite il front-end timescanner
- Si può scansionare un intero filesystem per estrarre timestamp da ogni tipo di file supportato
- Timescanner normatizza i timestamp in UTC. Si può indicare un diverso fuso orario con -z

```
$ timescanner -z local -d /mnt/analisi -w ./body_file
```

(un)fooling timelines

EndSummerCamp
3.9.2011

Rebus
Human, Forensicator,
Chaotic Good

log2timeline - Output

- BeeDocs (visualization tool per Mac)
- CEF (Common Event Format)
- CFTL (XML per CyberForensics TimeLab)
- CSV e TSV (ideali per fogli di calcolo, database, grep e script)
- Mactime, TLN e TLNX
- SIMILE (XML per SIMILE widget)
- SQLite

(un)fooling timelines

EndSummerCamp
3.9.2011

Rebus
Human, Forensicator,
Chaotic Good

Altri strumenti

- System Combo Timeline
(analogo a log2timeline, ma con meno feature)
- NFI Aftertime
(analogo a log2timeline, ma con una strana licenza)
- prefs.pl, evtparse.pl, jobparse.pl, AnalyzeMFT…
(parser specifici)
- Log Parser di Microsoft consente di eseguire query su log testuali, file XML e CSV, eventi, Registro di sistema, file system e Active Directory. Può produrre output testuali ed essere quindi impegato con gli altri strumenti di analisi.

(un)fooling timelines

EndSummerCamp
3.9.2011

Rebus
Human, Forensicator,
Chaotic Good

Elaborazione

(un)fooling timelines

EndSummerCamp
3.9.2011

Chi

Cosa

Dove

Come

Raccolta

Elaborazione

Visualizzazione

Problemi

Credits

Rebus
Human, Forensicator,
Chaotic Good

Elaborazione dati

- Excel e Calc, o eventualmente un DBMS

Date	Size	Type	Meta	File Name
Thu Jan 15 2009 01:10:22	451	.a..	12888-128	C:/Documents and Settings/Donald Blake/Cookies/donald blake@aol[2].txt
Thu Jan 15 2009 10:27:09	0	m...	0	DBlake-NTSUER/Software/Microsoft/Windows/CurrentVersion/Explorer/RunMRU
Thu Jan 15 2009 10:27:09	0	macb	0	[UserAssist] User: Donald Blake - UEME_RUNPATH:C:\WINDOWS\system32\secedit.exe [Count: 1]
Thu Jan 15 2009 10:27:09	11372	macb	7842	[Prefetch] SECEDIT.EXE-160D449D.pf created - run 1 times
Thu Jan 15 2009 10:27:09	11372	macb	7842-128-	C:/WINDOWS/Prefetch/SECEDIT.EXE-160D449D.pf
Thu Jan 15 2009 10:27:10	0	macb	0	[IE History] User connected to URL:Visited: Donald Blake@mk:@MSITStore:C:\WINDOWS\Help\sec
Thu Jan 15 2009 23:59:59	335	m...	7848	[LNK] /mnt/hack/windows_mount/Documents and Settings/Donald Blake/Recent/SECRET.lnk points
Thu Jan 15 2009 23:59:59	376	m...	8180	[LNK] /mnt/hack/windows_mount/Documents and Settings/Donald Blake/Recent/TIVO Research - C
Fri Jan 16 2009 18:15:16	163840	.a..	2280-128-	C:/WINDOWS/system32/credui.dll
Fri Jan 16 2009 18:15:16	176	.a..	45-144-6	C:/WINDOWS/inf
Fri Jan 16 2009 18:15:19	56	.a..	31-144-6	C:/WINDOWS/system32/drivers
Fri Jan 16 2009 18:15:20	0	m...	0	SYSTEM/ControlSet001/Enum/USBSTOR/Disk&Ven_M-Sys&Prod_Dell_Memory_Key&Rev_4.50/086
Fri Jan 16 2009 18:15:20	0	m...	0	SYSTEM/ControlSet001/Enum/USBSTOR/Disk&Ven_M-Sys&Prod_Dell_Memory_Key&Rev_4.50/086
Fri Jan 16 2009 18:18:10	449	..cb	8178	[LNK] /mnt/hack/windows_mount/Documents and Settings/Donald Blake/Recent/Blue Harvest Bus
Fri Jan 16 2009 18:18:19	290	.a..	9121	[LNK] /mnt/hack/windows_mount/Documents and Settings/Donald Blake/Recent/DBlake Personal (
Fri Jan 16 2009 18:18:25	449	m...	8178	[LNK] /mnt/hack/windows_mount/Documents and Settings/Donald Blake/Recent/Blue Harvest Bus
Fri Jan 16 2009 18:18:26	0	macb	0	[IE History] User connected to URL:Visited: Donald Blake@file:///E:/Blue Harvest Business Plan v1.c
Fri Jan 16 2009 18:18:26	449	m.c.	8178-128-	C:/Documents and Settings/Donald Blake/Recent/Blue Harvest Business Plan v1.lnk
Fri Jan 16 2009 18:25:13	335	..cb	7848	[LNK] /mnt/hack/windows_mount/Documents and Settings/Donald Blake/Recent/SECRET.lnk points
Fri Jan 16 2009 18:25:13	254	.acb	8253	[LNK] /mnt/hack/windows_mount/Documents and Settings/Donald Blake/Recent/SECRET (2).lnk po
Fri Jan 16 2009 18:25:28	0	macb	0	[IE History] User connected to URL:Visited: Donald Blake@file:///C:/Documents and Settings/Donal
Fri Jan 16 2009 18:25:28	0	macb	0	[UserAssist] User: Donald Blake - UEME_RUNPATH:C:\PROGRA~1\WINZIP\winzip32.exe [Count: 5]
Fri Jan 16 2009 18:25:28	56	.a..	3715-144-	C:/Documents and Settings/All Users/Documents

- Excel Template; Pivoting

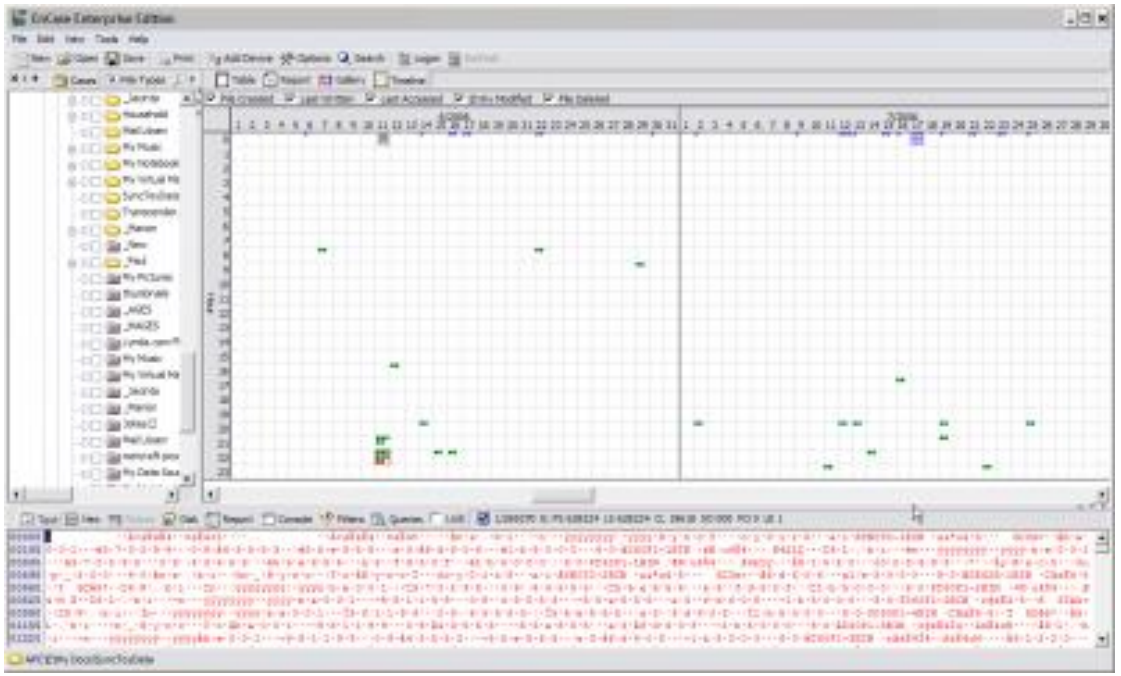
(un)fooling timelines

EndSummerCamp
3.9.2011

Rebus
Human, Forensicator,
Chaotic Good

Encase

- Encase permette di muoversi nella timeline molto rapidamente, ma è limitato nell'interfaccia, nella reportistica e soprattutto nella base dati



(un)fooling timelines

EndSummerCamp
3.9.2011

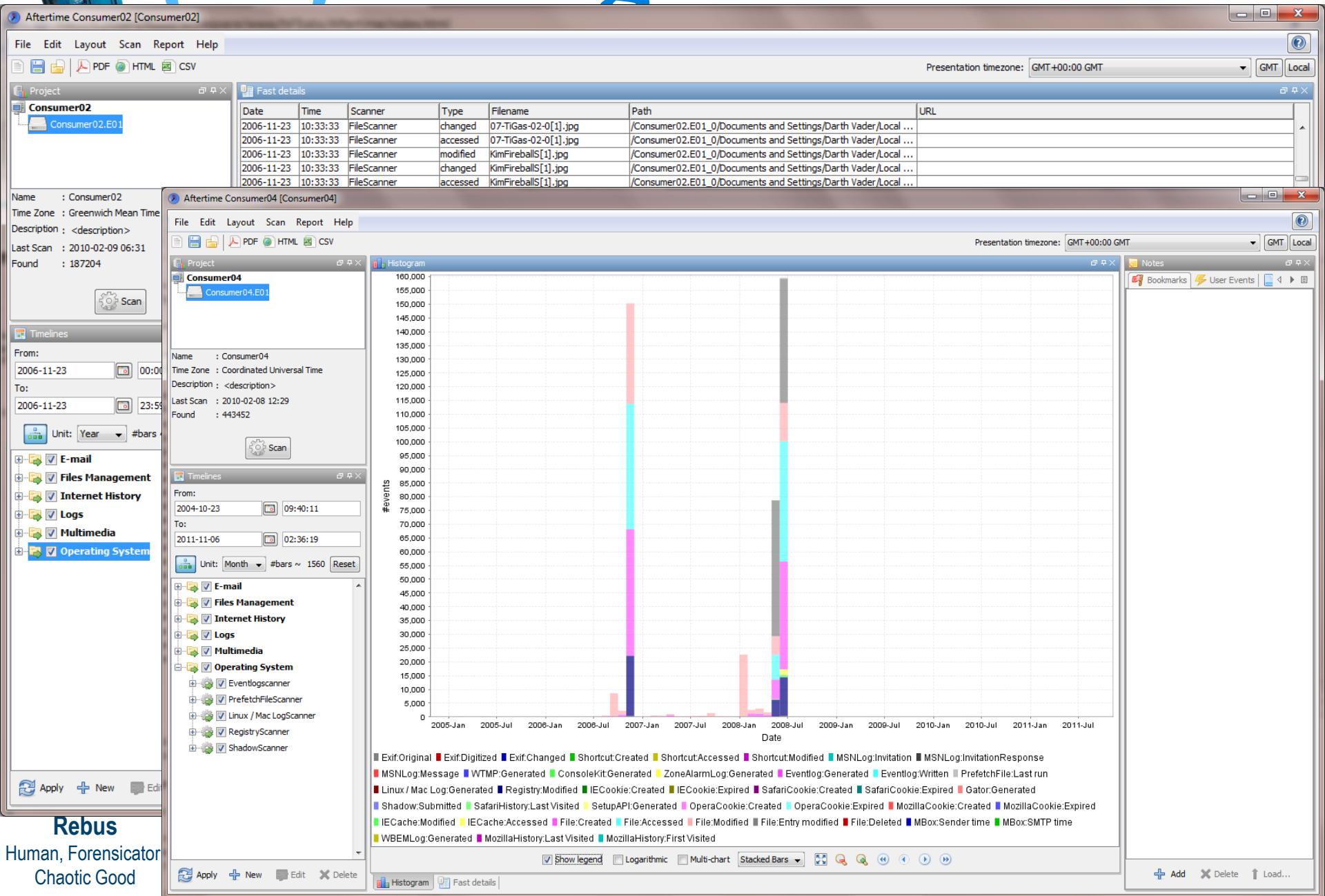
Rebus
Human, Forensicator,
Chaotic Good

NFI Aftertime (per windows e linux)

Supporta timestamp di diversa provenienza:

E-mail	MBox
Files	MAC-times, Shortcuts
Internet history	Internet Explorer cookies / history
	Safari cookies / history
	Opera cookies
	Mozilla/Firefox cookies / history
Logs	MSN, Zone alarm, Gator
	WTMP
	Console kit
	setupapi.log, WBEM
Multimedia	Exif
Operating System	Windows Event log, Registry, Prefetch, Shadow-files
	Linux / Macintosh logs

(un)fooling timelines



Rebus
Human, Forensicator
Chaotic Good

(un)fooling timelines

EndSummerCamp
3.9.2011

Rebus
Human, Forensicator,
Chaotic Good

Altri strumenti

- CyberForensics TimeLab
- Zeitline
- ex-Tip Framework

Chi li ha visti?

(un)fooling timelines

EndSummerCamp
3.9.2011

Rebus
Human, Forensicator,
Chaotic Good

Visualizzazione

(un)fooling timelines

EndSummerCamp
3.9.2011

Chi

Cosa

Dove

Come

Raccolta

Elaborazione

Visualizzazione

Problemi

Credits

Rebus
Human, Forensicator, Chaotic Good

Timeline visuali

- Autopsy e l'enscript Timeline Report di Geoff Black generano report HTML
  - Spartani, limitati, ma talvolta pratici

	\change.log.1	Indexed					
45	\C\System Volume Information_restore{D2674A2A-0500-4E46-BC0C-00D162391AE9}\RP380	Folder, Compressed, Not Indexed	16384	12/01/10 08:54:26AM	12/06/10 02:41:23PM	12/02/10 09:23:37AM	12/02/10 09:23:37AM
46	\C\System Volume Information_restore{D2674A2A-0500-4E46-BC0C-00D162391AE9}\RP380\snapshot	Folder, Compressed, Not Indexed	4096	12/01/10 08:54:26AM	12/01/10 08:54:30AM	12/01/10 08:54:29AM	12/01/10 08:54:29AM
47	\C\System Volume Information_restore{D2674A2A-0500-4E46-BC0C-00D162391AE9}\RP380 \snapshot_REGISTRY_USER_NTUSER_S-1-5-18	File, Archive, Compressed, Not Indexed	270336	12/01/10 08:54:26AM	12/01/10 08:54:26AM	12/01/10 08:54:26AM	12/01/10 08:54:26AM
48	\C\System Volume Information_restore{D2674A2A-0500-4E46-BC0C-00D162391AE9}\RP380 \snapshot_REGISTRY_USER_NTUSER_S-1-5-18	File, Archive, Compressed, Not Indexed	270336	12/01/10 08:54:26AM	12/01/10 08:54:26AM	12/01/10 08:54:26AM	12/01/10 08:54:26AM
49	\C\System Volume Information_restore{D2674A2A-0500-4E46-BC0C-00D162391AE9}\RP380 \snapshot_REGISTRY_USER_NTUSER_S-1-5-18	File, Archive, Compressed, Not Indexed	270336	12/01/10 08:54:26AM	12/01/10 08:54:26AM	12/01/10 08:54:26AM	12/01/10 08:54:26AM
50	\C\System Volume Information_restore{D2674A2A-0500-4E46-BC0C-00D162391AE9}\RP380 \snapshot_REGISTRY_USER_NTUSER_S-1-5-18	File, Archive, Compressed, Not Indexed	270336	12/01/10 08:54:26AM	12/01/10 08:54:26AM	12/01/10 08:54:26AM	12/01/10 08:54:26AM
51	\C\System Volume Information_restore{D2674A2A-0500-4E46-BC0C-00D162391AE9}\RP380 \snapshot_REGISTRY_USER_NTUSER_S-1-5-19	File, Archive, Compressed, Not Indexed	241664	12/01/10 08:54:26AM	12/01/10 08:54:26AM	12/01/10 08:54:26AM	12/01/10 08:54:26AM
52	\C\System Volume Information_restore{D2674A2A-0500-4E46-BC0C-00D162391AE9}\RP380 \snapshot_REGISTRY_USER_NTUSER_S-1-5-19	File, Archive, Compressed, Not Indexed	241664	12/01/10 08:54:26AM	12/01/10 08:54:26AM	12/01/10 08:54:26AM	12/01/10 08:54:26AM
53	\C\System Volume Information_restore{D2674A2A-0500-4E46-BC0C-00D162391AE9}\RP380 \snapshot_REGISTRY_USER_NTUSER_S-1-5-19	File, Archive, Compressed, Not Indexed	241664	12/01/10 08:54:26AM	12/01/10 08:54:26AM	12/01/10 08:54:26AM	12/01/10 08:54:26AM
54	\C\System Volume Information_restore{D2674A2A-0500-4E46-BC0C-00D162391AE9}\RP380 \snapshot_REGISTRY_USER_NTUSER_S-1-5-19	File, Archive, Compressed, Not Indexed	241664	12/01/10 08:54:26AM	12/01/10 08:54:26AM	12/01/10 08:54:26AM	12/01/10 08:54:26AM
55	\C\System Volume Information_restore{D2674A2A-0500-4E46-BC0C-00D162391AE9}\RP380 \snapshot_REGISTRY_USER_USRCLASS_S-1-5-19	File, Archive, Compressed, Not Indexed	8192	12/01/10 08:54:26AM	12/01/10 08:54:26AM	12/01/10 08:54:26AM	12/01/10 08:54:26AM
56	\C\System Volume Information_restore{D2674A2A-0500-4E46-BC0C-00D162391AE9}\RP380 \snapshot_REGISTRY_USER_USRCLASS_S-1-5-19	File, Archive, Compressed, Not Indexed	8192	12/01/10 08:54:26AM	12/01/10 08:54:26AM	12/01/10 08:54:26AM	12/01/10 08:54:26AM
57	\C\System Volume Information_restore{D2674A2A-0500-4E46-BC0C-00D162391AE9}\RP380 \snapshot_REGISTRY_USER_USRCLASS_S-1-5-19	File, Archive, Compressed, Not Indexed	8192	12/01/10 08:54:26AM	12/01/10 08:54:26AM	12/01/10 08:54:26AM	12/01/10 08:54:26AM

(un)fooling timelines

EndSummerCamp
3.9.2011

Chi

Cosa

Dove

Come

Raccolta

Elaborazione

Visualizzazione

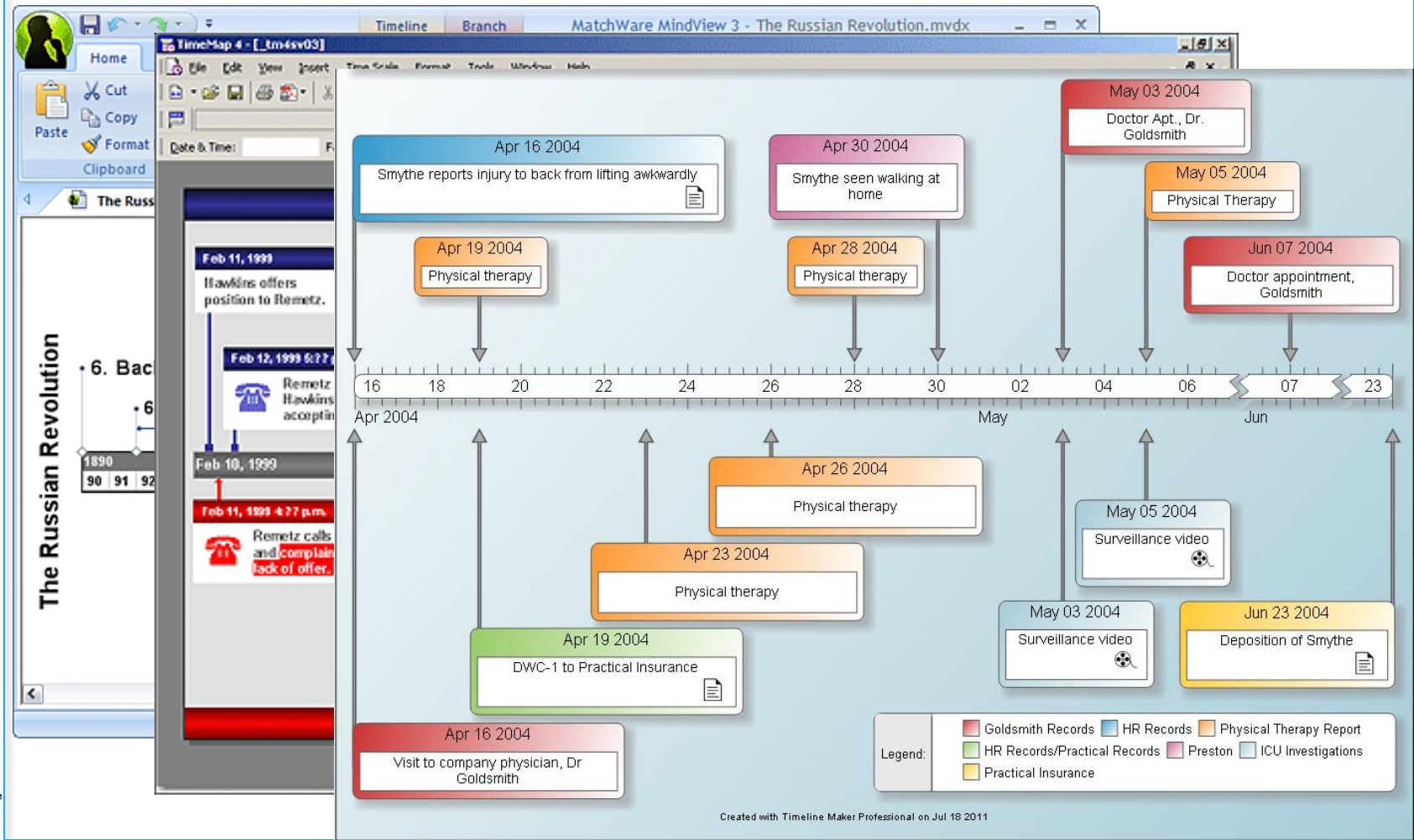
Problemi

Credits

Rebus
Human, Forensicator,
Chaotic Good

Timeline visuali

- Matchware Timelines, LexisNexis TimeMap, TimelineMaker, SmartDraw, Beedocs…



(un)fooling timelines

EndSummerCamp
3.9.2011

Chi

Cosa

Dove

Come

Raccolta

Elaborazione

Visualizzazione

Problemi

Credits

Rebus
Human, Forensicator,
Chaotic Good

Timeline visuali: Webscavator

- Open Source
- Solo navigazione web
- Importa report da Fox Analysis, Net Analysis, Web Historian, Pasco, Chrome Cache Viewer
- Espandibile (sapendo un po' di Python)
- Dispone di diverse modalità di visualizzazione
- Non è solo un visualizzatore: offre strumenti di ricerca, filtri e funzioni statistiche

WEBSCAVATOR

Filters

	Google searches	Web Email	Local Files	News URLs	Work hours	Advert URLs
✔	○	○	○	○	○	○
✘	○	○	○	○	○	○

Overview | Timeline | Websites visited | Online Searches | Files

Overview for sen2b

Heat Map of Internet Usage

	Mon	Tue	Wed	Thu	Fri	Sat	Sun
00:00 - 00:59							
01:00 - 01:59							
02:00 - 02:59							
03:00 - 03:59							
04:00 - 04:59							
05:00 - 05:59							
06:00 - 06:59							
07:00 - 07:59							
08:00 - 08:59							
09:00 - 09:59						20	
10:00 - 10:59						33	
11:00 - 11:59						34	
12:00 - 12:59						47	
13:00 - 13:59						25	
14:00 - 14:59						1	53
15:00 - 15:59						20	36
16:00 - 16:59						24	21
17:00 - 17:59							19
18:00 - 18:59	89	157	152	162		52	73
19:00 - 19:59	37	19	15	21	119	7	10
20:00 - 20:59	49	5	11		85		
21:00 - 21:59	24	53	12				
22:00 - 22:59	29	3	17				
23:00 - 23:59							

Browser St

Internet Usage Statistics

Average amount of web pages visited daily: 13

Peak time of usage: 18:00 - 18:59

Case Information

Case name: sen2b

Date created: 07:36PM 11 Aug 2010

Web Files

Name: test file

Program used: Web Historian

File uploaded: Scenario2_B.xml

WEBSCAVATOR

Home | Edit case | Load case | New case | Help | About

Search Term: vin

vin has been searched twice.

vin was used in the following searches:

car vin number [On Sat May 08 2010 12:22:53]

get rid of vin [On Sat May 08 2010 12:22:49]

Filters

Reset filters

Add New Filter

Social Networking URLs

Overview | Timeline | Websites visited | Online Searches | Files

Search Engine Usage for sen2b

Top 20 | AOL | Bing | Yahoo! | Google | Ask Jeeves

Google

The top 20 searched terms are below.

hire away car beating van cheap robbery removal tinted edinburgh get vin vin number windows rid security number white points weak

(un)fooling timelines

EndSummerCamp
3.9.2011

Chi

Cosa

Dove

Come

Raccolta

Elaborazione

Visualizzazione

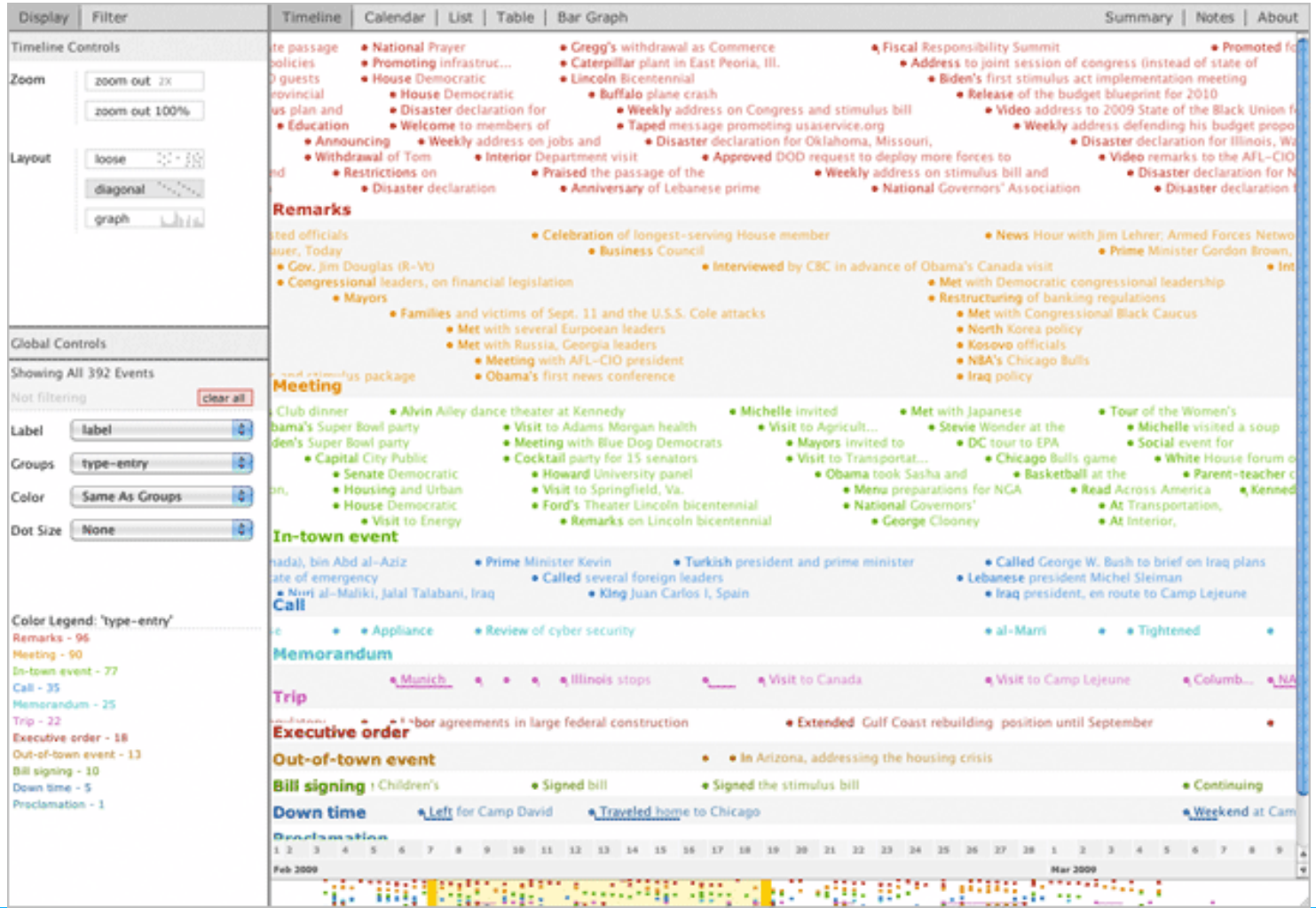
Problemi

Credits

Rebus
Human, Forensicator,
Chaotic Good

Timeline visuali: TimeFlow

- https://github.com/FlowingMedia/TimeFlow



(un)fooling timelines

EndSummerCamp
3.9.2011

Rebus
Human, Forensicator,
Chaotic Good

Problemi, intralci, attacchi

Conoscerli, identificarli e sopravvivere

(un)fooling timelines

EndSummerCamp
3.9.2011

Rebus
Human, Forensicator,
Chaotic Good

Dispersività

- Troppi dati sono difficili da gestire
- Troppo pochi potrebbe non essere abbastanza descrittivi
- …o più facilmente falsati
- Servono scanner automatizzati e strumenti di ricerca e filtering efficienti
- La rappresentazione è spesso problematica

(un)fooling timelines

EndSummerCamp
3.9.2011

Rebus
Human, Forensicator,
Chaotic Good

Intralci

- I programmi che eseguono scansioni massive di file (antivirus, antispyware, indicizzatori ecc.) facilmente ne alterano la data di accesso, rendendo l'informazione poco significativa
- Alcuni antivirus possono essere istruiti a riguardo (p.e. Preserve Filetime in NAV Corporate)

(un)fooling timelines

EndSummerCamp
3.9.2011

Rebus
Human, Forensicator,
Chaotic Good

Filesystem tunneling

- Windows effettua un tunneling del filesystem (default 15 sec.) che può causare fastidi…
  - Creare un file denominato file1.
  - Attendere uno o due minuti.
  - Creare un file denominato file2.
  - Effettuare un'operazione DIR /TC. Notare le date di creazione.
  - Rinominare file1 in file.
  - Rinominare file2 in file1.
  - Effettuare un'operazione DIR /TC. Si noterà che le date di creazione sono identiche.
  - Per entrambi i file è indicata la stessa data e ora di creazione, che è identica a quella del file originale file1 e corrisponde al comportamento previsto con il tunneling attivato.
- La funzione è disattivabile o estendibile

(un)fooling timelines

EndSummerCamp
3.9.2011

Rebus
Human, Forensicator,
Chaotic Good

Intralci intenzionali

- Le manipolazioni possono ovviamente essere intenzionali
- Strategia attuata da taluni malware per confondere le acque e rendere difficoltoso individuare il punto di compromissione e le azioni successive
- Strategia alla portata degli utenti grazie a strumenti come touch, timestomp e tanti altri tool scriptabili
- Come tecnica di antiforensics non funziona tanto bene, dipende molto dal filesystem in uso…

(un)fooling timelines

EndSummerCamp
3.9.2011

Chi

Cosa

Dove

Come

Raccolta

Elaborazione

Visualizzazione

Problemi

Credits

Rebus
Human, Forensicator, Chaotic Good

Timestomp vs Encase

- In condizioni normali su NTFS:

AUTOEXEC.BAT	06/30/05 11:57:13AM	12/02/04 09:43:29AM	12/02/04 09:43:29AM	12/02/04 09:43:29AM

- Dopo timestomp (-z "Monday 05/05/2005 05:05:05 AM")

AUTOEXEC.BAT	05/05/05 05:05:05AM	05/05/05 05:05:05AM	05/05/05 05:05:05AM	05/05/05 05:05:05AM

- Dopo timestomp (-b)

AUTOEXEC.BAT				

(un)fooling timelines

EndSummerCamp
3.9.2011

Chi

Cosa

Dove

Come

Raccolta

Elaborazione

Visualizzazione

Problemi

Credits

Rebus
Human, Forensicator,
Chaotic Good

Timestomp vs Encase

	Name	Last Accessed	File Created	Last Written	Entry Modified
14	$UpCase	12/02/04 02:16:52AM	12/02/04 02:16:52AM	12/02/04 02:16:52AM	12/02/04 02:16:52AM
15	$Volume	12/02/04 02:16:52AM	12/02/04 02:16:52AM	12/02/04 02:16:52AM	12/02/04 02:16:52AM
16	3584 byte bob.txt	07/09/05 04:09:20PM	07/09/05 04:09:20PM	06/18/05 09:11:39PM	07/09/05 04:09:09PM
17	AUTOEXEC.BAT				
18	boot.ini	07/22/05 09:00:01AM	12/02/04 02:20:31AM	12/02/04 11:25:05AM	12/02/04 11:25:05AM
19	CONFIG.SYS	01/17/05 11:48:45PM	12/02/04 09:43:29AM	12/02/04 09:43:29AM	12/02/04 09:43:29AM
20	DELL	07/20/05 02:37:53PM	12/02/04 09:47:17AM	12/02/04 10:07:18AM	12/02/04 10:07:18AM
21	devicetable.log	07/08/05 03:54:12PM	01/11/05 09:45:55AM	07/08/05 03:54:12PM	07/08/05 03:54:12PM
22	Documents and Settings	07/22/05 12:00:03PM	12/02/04 02:21:18AM	12/02/04 09:55:27AM	12/02/04 09:55:27AM
23	hpfr5550.xml	02/12/05 12:23:59AM	02/06/05 01:56:24PM	02/12/05 12:23:59AM	02/12/05 12:23:59AM
24	Install.log	06/06/05 02:11:04AM	04/18/05 09:02:35AM	04/18/05 09:02:36AM	04/18/05 09:02:35AM
25	IO.SYS	12/02/04 09:43:29AM	12/02/04 09:43:29AM	12/02/04 09:43:29AM	12/02/04 09:43:29AM
26	legalese_l0_001.txt	07/19/05 01:31:43PM	03/29/05 04:19:12PM	03/29/05 04:19:12PM	03/29/05 04:19:12PM

(un)fooling timelines

EndSummerCamp
3.9.2011

Chi

Cosa

Dove

Come

Raccolta

Elaborazione

Visualizzazione

Problemi

Credits

Rebus
Human, Forensicator,
Chaotic Good

Timestomp vs Encase

	Name	Last Accessed	File Created	Last Written	Entry Modified
☐ 62	ODBCINST.INI				
☐ 63	iis5.log				
☐ 64	comsetup.log				
☐ 65	imsins.log				
☐ 66	ockodak.log				
☐ 67	ocgen.log				
☐ 68	mmdet.log				
☐ 69	ModemDet.txt				
☐ 70	Blue Lace 16.bmp				
☐ 71	Soap Bubbles.bmp				
☐ 72	Coffee Bean.bmp				
☐ 73	FeatherTexture.bmp				
☐ 74	Gone Fishing.bmp				
☐ 75	Greenstone.bmp				
☐ 76	Prairie Wind.bmp				
☐ 77	Rhododendron.bmp				
☐ 78	River Sumida.bmp				
☐ 79	Santa Fe Stucco.bmp				
☐ 80	Zapotec.bmp				
☐ 81	vb.ini				
☐ 82	vbaddin.ini				
☐ 83	COM+.log				
☐ 84	folder.htt				
☐ 85	desktop.ini				

(un)fooling timelines

EndSummerCamp
3.9.2011

Chi

Cosa

Dove

Come

Raccolta

Elaborazione

Visualizzazione

Problemi

Credits

Rebus
Human, Forensicator, Chaotic Good

Defeating Timestomp

- Sembra divertente, ma "Timestomp is for suckers"
- Altera a piacere gli attributi $SI, ma non gli attributi $FN
- Al momento, **nessun** tool di antiforensics noto interviene su $FN!
- Encase di suo lavora solo con $SI, ma dispone di script che parsano $MFT ed eseguono verifiche di coerenza tra $SI e $FN
- Anche mft.pl di Harlan Carvey e altri tool di parsing dell'MFT consentono la verifica
- Per SleuthKit, istat e icat consentono di estrarre $FN; fls invece no (o non ancora)
- Tutto ciò ovviamente ha senso solo su NTFS

(un)fooling timelines

EndSummerCamp
3.9.2011

Chi

Cosa

Dove

Come

Raccolta

Elaborazione

Visualizzazione

Problemi

Credits

Rebus
Human, Forensicator,
Chaotic Good

log2timeline

L'ultima recente versione di log2timeline ha nuove feature a riguardo:

- Rimuove automaticamente entry duplicate nella timeline
- Può eseguire il parsing di $MFT e verificare automaticamente le entry sospette di alterazione
- Può eseguire contestualmente alla scansione delle fonti una ricerca per keyword
- Analizzando $MFT, può creare un grafico dei file in windows/system32, riportante il numero della entry MFT sull'asse X e i timestamp di creazione del file ($SI e $FN) sull'asse Y, così da rendere immediatamente visibili incongruenze che possono essere rivelatrici di malware.

(un)fooling timelines

EndSummerCamp
3.9.2011

Rebus
Human, Forensicator,
Chaotic Good

“Ma io cambio l’ora di sistema!”

- Se fatto da Windows Vista o 7, ne troverò traccia nel registro degli eventi (ID 1)
- Con Linux dipende, con Mac OS X non lo so (BSD lo faceva!)
- Se fatto da BIOS, ho ancora qualche speranza di accorgermene dalle incongruenze negli artefatti:
  - accessi a file che non avrebbero dovuto esistere
  - uso di applicazioni o servizi non installati
  - File LNK in Windows XP (hanno un contatore!)
  - Restore Point (RP## è incrementale per XP, Vista e 7)
  - Sequenzialità dei log (soprattutto su eventi continui) e delle cache applicative
  - Confronto con dati esterni al sistema
  - Pagine HTML salvare, e-mail ricevute, altri metadati con riferimenti temporali esterni

(un)fooling timelines

EndSummerCamp
3.9.2011

Chi

Cosa

Dove

Come

Raccolta

Elaborazione

Visualizzazione

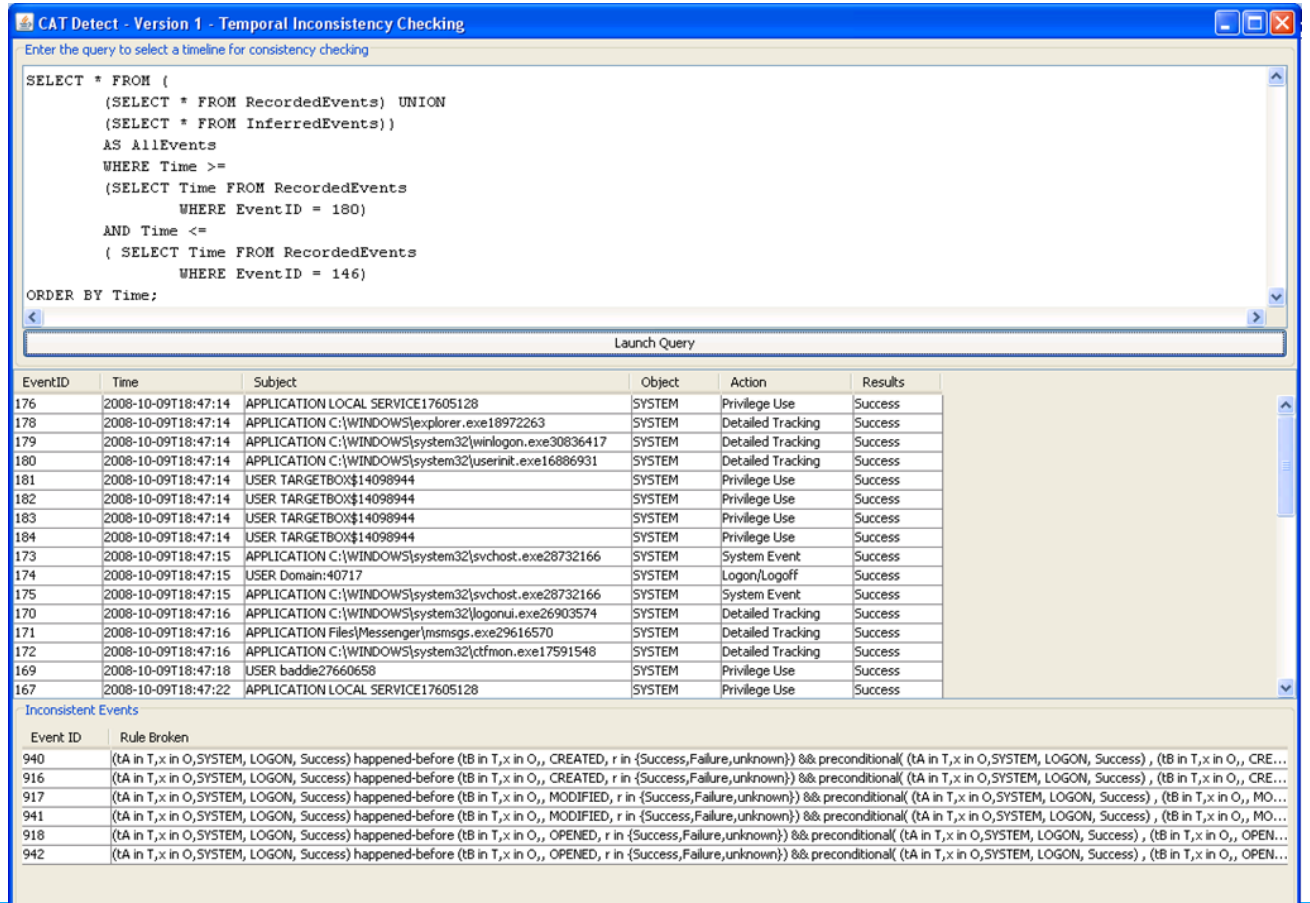
Problemi

Credits

Rebus
Human, Forensicator,
Chaotic Good

CAT Detect

- Progetto ancora sperimentale, ma molto promettente
- Ricerca incongruenze nella sequenza temporale degli eventi
- Nato per Windows, ma su principi adattabili ad altri O.S.



(un)fooling timelines

EndSummerCamp
3.9.2011

Rebus
Human, Forensicator,
Chaotic Good

Bibliografia

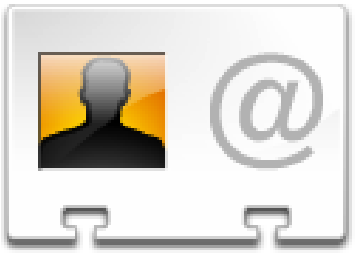
- http://www.timeforensics.com
- http://www.log2timeline.net
- http://www.sans.org/reading_room/whitepapers/logging/mastering-super-timeline-log2timeline_33438
- http://www.sans.org/reading_room/whitepapers/forensics/ex-tip-extensible-timeline-analysis-framework-perl_32767
- http://computer-forensics.sans.org/blog
- http://computerforensics.parsonage.co.uk/downloads/TheMeaningofLIFE.pdf
- http://www.vertex42.com/ExcelArticles/create-a-timeline.html
- http://journeyintoir.blogspot.com/2010/11/reviewing-timelines-with-excel.html
- http://journeyintoir.blogspot.com/2010/11/reviewing-timelines-with-calc.html
- http://www.forensic4cast.com/2011/01/detecting-cmos-clock-changes
- CAT Detect: http://www.dfrws.org/2011/proceedings/11-343.pdf

(un)fooling timelines

EndSummerCamp
3.9.2011

Rebus
Human, Forensicator,
Chaotic Good

Teniamoci in contatto...



Davide Rebus Gabrini

e-mail:
rebus@mensa.it
davide.gabrini@poliziadistato.it

GPG Public Key: (available on keyserver.linux.it)
www.tipiloschi.net/rebus.asc
KeyID: 0x176560F7

Instant Messaging:

MSN	therebus@hotmail.com
ICQ	115159498
Yahoo!	therebus
Skype	therebus

Mi trovate anche su Facebook, Twitter e **LinkedIn**.

Queste e altre cazzate su **http://www.tipiloschi.net**