

Wibbly wobbly timey wimey stuff

Uso delle timeline nell'analisi forense





Wibbly wobbly timey wimey stuff

Chi sono

Davide 'Rebus' Gabrini

Per chi lavoro non è un mistero.

Oltre a ciò:

- ▶ Perito informatico
- ▶ Consulente tecnico e Perito forense
- ▶ Collaboratore UniPV
- ▶ Docente di sicurezza informatica e digital forensics per privati e P.A.
- ▶ Certificazioni CIFI, ACE, AME
- ▶ Socio IISFA, DEFTA, Tech&Law fellow
- ▶ Proud fellow of Italian Hacker Embassy

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



➡ Chi

Cosa

Dove

Come

Raccolta

Elaborazione

Visualizzazione

Problemi

Credits



Wibbly wobbly timey wimey stuff

Timeline

Chi

▶ Una timeline è una rappresentazione di eventi ordinati cronologicamente

▶ Cosa

▶ Gli eventi possono provenire da un'unica fonte o, più sovente, da una pluralità di fonti

Dove

Come

▶ Per le finalità di oggi, ci interessano solo gli eventi di natura digitale, ma un'indagine spesso attinge da fonti molto eterogenee

Raccolta

Elaborazione

Visualizzazione

▶ Metodo rapido e intuitivo per avere immediata contezza di quanto occorso in un sistema in una determinata finestra temporale

Problemi

Credits



Wibbly wobbly timey wimey stuff

Timeline

▶ Utilizzi:

Chi

▶ Ricostruire le attività di un utente....

▶ Cosa

▶ ...o di un intruso.

Dove

▶ Ricostruire le fasi di un attacco/infezione

Come

▶ Individuare il punto di compromissione originale

▶ Individuare le cause di un incidente

Raccolta

▶ Evidenziare incongruenze che siano sintomo di attività illecite e antiforensics

Elaborazione

Visualizzazione

▶ 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.

Problemi

Credits



Wibbly wobbly timey wimey stuff

Da dove arrivano i riferimenti temporali?

Chi

Cosa

→ Dove

Come

Raccolta

Elaborazione

Visualizzazione

Problemi

Credits

▶ 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?



Wibbly wobbly timey wimey stuff

Dove sono registrati

Chi ▶ Il primo posto dove guardare è il filesystem: attributi MAC(B) di ogni file/cartella e altre strutture come p.e. il journal

Cosa ▶ Il filesystem non basta: un sistema operativo registra innumerevoli eventi cronologicamente referenziati

⇒ Dove ▶ File di log (sistema e applicazioni) e registri degli eventi

Come ▶ Registro di Windows (contenuto e metadati delle chiavi)

Raccolta ▶ Feature proprie del sistema operativo (Prefetch, Restore Points, Link, Cestino, thumbs.db, ShellBag, Volume Shadow Copy...)

Elaborazione ▶ Cronologia, Cache e Cookies dei browser

Visualizzazione ▶ Cache e database applicativi

Problemi ▶ Metadati interni ai documenti (Office, EXIF, pagine HTML...)

Credits ▶ Eventi temporali recuperabili tramite carving da aree deallocate, slack space, memory dump, partizioni di swap, file di ibernazione (record \$MFT, chiavi di registro, chat...)



Wibbly wobbly timey wimey stuff

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.

Chi

Cosa

Dove

→ Come

Raccolta

Elaborazione

Visualizzazione

Problemi

Credits



Wibbly wobbly timey wimey stuff

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

Chi

Cosa

Dove

→ Come

Raccolta

Elaborazione

Visualizzazione

Problemi

Credits



Wibbly wobbly timey wimey stuff

Filesystem e S.O.

▶ **FAT** registra gli attributi MAC in localtime

Chi

▶ **NTFS** registra 2 serie di attributi MACB in UTC

Cosa

▶ Da NT in poi è possibile disabilitare

Dove

l'aggiornamento dell'attributo Access (per Vista è default)

→ Come

▶ HKLM\SYSTEM\CurrentSet\Control\FileSystem\NtfsDisableLastAccessUpdate

Raccolta

▶ Linux registra in Unix time (secondi trascorsi dal 1 / 1 / 1970 00:00:00 UTC) attributi MAC su **Ext2/3**.

Elaborazione

Con **Ext4** arriva l'attributo Birth e la granularità al nanosecondo.

Visualizzazione

Problemi

L'aggiornamento degli attributi può essere inibito in fase di mount.

Credits

▶ **HFS+** registra i secondi trascorsi da 1 / 1 / 1904 00:00:00 GMT



Wibbly wobbly timey wimey stuff

NTFS: dove sono i timestamp?

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

Chi

Cosa

▶ **\$STANDARD_INFO**

→ Dove

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

Come

Raccolta

Elaborazione

Modificabile in **user space**.

Visualizzazione

▶ **\$FILE_NAME**

Problemi

Contiene il nome file in Unicode e un ulteriore set di timestamp MACB.

Credits

Modificabile solo in **kernel space**.



Wibbly wobbly timey wimey stuff

Quando cambiano i timestamp? (NTFS)

	\$FILE_NAME	Rename	Local Move	Volume Move	Copy	Access	Modify	Create	Delete
Chi	Modification		X	X	X			X	X
Cosa	Accessed			X	X			X	
Dove	Change (meta)		X	X	X			X	X
	Born			X	X			X	
→ Come									
	\$STANDARD_INFO	Rename	Local Move	Volume Move	Copy	Access	Modify	Create	Delete
Raccolta	Modification						X	X	
Elaborazione	Accessed			X	X	X	X	X	
Visualizzazione	Change (meta)	X	X	X	X			X	X
	Born				X			X	

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



Wibbly wobbly timey wimey stuff

Comportamento in Windows 7

Chi

Windows 7 File System \$STDInfo and \$Filename Properties

Cosa

Dove

→ Come

Raccolta

Elaborazione

Visualizzazione

Problemi

Credits

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



Wibbly wobbly timey wimey stuff

Applicazioni

Chi

▶ Singole applicazioni, però, possono adottare timestamp alternativi:

Cosa

Dove

▶ Nel registro di Windows, i valori

→ Come

FILETIME riportano il numero di intervalli da 100 nanosecondi trascorsi dal 1/1/1601 00:00:00 UTC

Raccolta

Elaborazione

Visualizzazione

▶ da MacOSX 10 le applicazioni (p.e.

Problemi

Safari) possono usare il Mac Absolute

Credits

Time, o CFDate: secondi trascorsi dal 1/1/2001 00:00:00 GMT



Wibbly wobbly timey wimey stuff

Normalizzazione

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

Chi

Cosa

Dove

→ Come

Raccolta

Elaborazione

Visualizzazione

Problemi

Credits

▶ 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



Wibbly wobbly timey wimey stuff

Chi

Cosa

Dove

Come

➡ Raccolta

Elaborazione

Visualizzazione

Problemi

Credits

Raccolta dati





Wibbly wobbly timey wimey stuff

Filesystem - fls

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

Chi

Cosa

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

Dove

-**f**filesystem-type

Come

-**o**offset

-**r**recursive

► Raccolta

-**m**mountpoint

Elaborazione

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

Visualizzazione

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

Problemi

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:

Credits

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




Wibbly wobbly timey wimey stuff

body_file

O|C:/Bootfont.bin|1862-128-3|r/r--x--x--x|0|0|4952|1276960800||141300800||141300800||141300800
 Chi O|C:/AttrDef|4-128-4|r/rr-xr-xr-x|48|0|2560|1276960582|1276960582|1276960582|1276960582
 Cosa O|C:/BadClus|8-128-2|r/rr-xr-xr-x|0|0|0|1276960582|1276960582|1276960582|1276960582
 Dove O|C:/BadClus:\$Bad|8-128-1|r/rr-xr-xr-x|0|0|49532633088|1276960582|1276960582|1276960582|1276960582
 Come O|C:/Bitmap|6-128-1|r/rr-xr-xr-x|0|0|1511616|1276960582|1276960582|1276960582|1276960582
 Raccolta O|C:/Boot|7-128-1|r/rr-xr-xr-x|48|0|8192|1276960582|1276960582|1276960582|1276960582
 Elaborazione O|C:/Extend|1-144-4|d/dr-xr-xr-x|0|0|344|1276960582|1276960582|1276960582|1276960582
 Visualizzazione O|C:/LogFile|2-128-1|r/rr-xr-xr-x|0|0|67108864|1276960582|1276960582|1276960582|1276960582
 Problemi O|C:/MFT|0-128-1|r/rr-xr-xr-x|0|0|57950208|1276960582|1276960582|1276960582|1276960582
 Credits O|C:/MFTMirr|1-128-1|r/rr-xr-xr-x|0|0|4096|1276960582|1276960582|1276960582|1276960582
 O|C:/Secure:\$SDH|9-144-17|r/rr-xr-xr-x|0|0|56|1276960582|1276960582|1276960582|1276960582
 O|C:/Secure:\$SI|9-144-16|r/rr-xr-xr-x|0|0|56|1276960582|1276960582|1276960582|1276960582
 O|C:/Secure:\$SDS|9-128-0|r/rr-xr-xr-x|0|0|887276|1276960582|1276960582|1276960582|1276960582
 O|C:/UpCase|10-128-1|r/rr-xr-xr-x|0|0|131072|1276960582|1276960582|1276960582|1276960582
 O|C:/Volume|3-128-3|r/rr-xr-xr-x|48|0|0|1276960582|1276960582|1276960582|1276960582
 O|C:/AUTOEXEC.BAT|7420-128-1|r/rrwxrwxrwx|0|0|0|1276955179|1276955179|1276955179|1276955179
 O|C:/boot.ini|3528-128-10|r/r--x--x--x|0|0|212|1292187989|1276955625|1276955625|1276960966
 O|C:/Config.Msi|29593-144-6|d/dr-xr-xr-x|0|0|48|1292189987|1292183363|1292183363|1292180848



Wibbly wobbly timey wimey stuff

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

Chi

Date,Size,Type,Mode,UID,GID,Meta,File Name

Cosa

Wed Nov 21 2001 13:13:36,6178,m...,r/rwxrwxrwx,0,0,51150-128-3,C:/Forensics/Browser/ndphlpr.vxd

Dove

Tue Apr 23 2002 20:11:00,261082,m...,r/rwxrwxrwx,0,0,50090-128-3,C:/IrfanView/Plugins/PopArt.8bf

Come

Thu Oct 17 2002 21:23:14,8200,m..b,r/rwxrwxrwx,0,0,16305-128-3,C:/Microsoft/OFFICE/DATA/OPA12.BAK

Thu Feb 13 2003 10:43:22,4860,m...,r/rwxrwxrwx,0,0,50978-128-4,C:/BETA/MFL-FA/RemovableMask.pct

➡ Raccolta

Thu Feb 13 2003 10:44:20,14504,m...,r/rwxrwxrwx,0,0,50977-128-4,C:/BETA/MFL-FA/RemovableImage.pct

Elaborazione

Wed Oct 01 2003 20:40:00,366592,m...,r/rwxrwxrwx,0,0,51003-128-3,C:/ClamWinPortable/lib/wxc.pyd

Wed Oct 01 2003 20:40:02,35840,m...,r/rwxrwxrwx,0,0,50988-128-3,C:/ClamWinPortable/lib/htmlc.pyd

Visualizzazione

Wed Oct 01 2003 20:40:38,71168,m...,r/rwxrwxrwx,0,0,50987-128-3,C:/ClamWinPortable/lib/gizmosc.pyd

Problemi

Fri Nov 07 2003 09:42:00,7434,m...,r/rwxrwxrwx,0,0,44594-128-3,C:/XnView/Masks/PF-Brush.jpg

Fri Nov 07 2003 09:42:00,6445,m...,r/rwxrwxrwx,0,0,44595-128-4,C:/XnView/Masks/PF-Camera.jpg

Credits

Fri Nov 07 2003 09:42:00,11681,m...,r/rwxrwxrwx,0,0,44596-128-4,C:/XnView/Masks/PF-Diffuse.jpg

Fri Nov 07 2003 09:42:00,5021,m...,r/rwxrwxrwx,0,0,44597-128-4,C:/XnView/Masks/PF-Ellipse.jpg

Fri Nov 07 2003 09:42:00,5459,m...,r/rwxrwxrwx,0,0,44598-128-3,C:/XnView/Masks/PF-Fog.jpg



Wibbly wobbly timey wimey stuff

Registro di Windows - regtime

Chi ▶ Ogni chiave di registro ha un attributo temporale LastWrite

Cosa

Dove ▶ Lo script regtime.pl di Harlan Carvey permette di estrarre i valori LastWrite dai singoli hive:

Come

→ Raccolta

Elaborazione

```
$ 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
```

Visualizzazione

```
$ regtime.pl -m HKLM-SECURITY -r /mnt/target/WINDOWS/system32/config/SECURITY >> body
```

Problemi

```
$ regtime.pl -m HKLM-SOFTWARE -r /mnt/target/WINDOWS/system32/config/software >> body
```

Credits

```
$ 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.



Wibbly wobbly timey wimey stuff

log2timeline - Input

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

Chi Dispone di numerosissimi moduli ed è in continua espansione:

Cosa ▶ Apache2 Access/Error logs

▶ Google Chrome history

Dove ▶ Encase e FTK Imager dirlisting

▶ Windows Event Log files (EVT e EVTX)

Come ▶ EXIF e metadati da vari formati multimediali

▶ Firefox bookmark e history

➡ Raccolta

▶ Generic Linux log file

Elaborazione ▶ Internet Explorer history (file index.dat)

▶ Windows IIS W3C log files

Visualizzazione

▶ ISA server text export.

Problemi ▶ Mactime e TLN body files

▶ McAfee AntiVirus Log files

Credits

▶ MS-SQL Error log

▶ Opera Global and Direct browser history

▶ OpenXML metadata (metadati dei documenti Office 2007)

▶ PCAP files



Wibbly wobbly timey wimey stuff

log2timeline - Input

▶ PDF metadata

Chi ▶ Windows Prefetch directory

Cosa ▶ Windows Recycle Bin (INFO2 or I\$)

▶ Windows Restore Points

Dove ▶ Safari Browser history files

Come ▶ Skype main.db file

▶ Windows XP SetupAPI.log file

➡ Raccolta ▶ Adobe Local Shared Object files (SOL/LSO), aka Flash Cookies

Elaborazione ▶ Squid Access Logs (httpd_emulate off)

▶ Windows Registry Hives

Visualizzazione ▶ UserAssist key of the Windows registry

Problemi ▶ Windows Shortcut files (LNK)

▶ Windows WMIProv log file

Credits

▶ Windows XP Firewall Log files (W3C format)

▶ Volatility: the output file from the psscan and psscan2 modules



Wibbly wobbly timey wimey stuff

log2timeline - Output

Chi ▶ BeeDocs (visualization tool per Mac)

Cosa ▶ CEF (Common Event Format)

Dove ▶ CFTL (XML per CyberForensics
Come TimeLab)

→ Raccolta ▶ CSV e TSV (ideali per fogli di calcolo,
Elaborazione database, grep e script)

Visualizzazione ▶ Mactime, TLN e TLNX

Problemi ▶ SIMILE (XML per SIMILE widget)

Credits

▶ SQLite



Wibbly wobbly timey wimey stuff

Altri strumenti

▶ System Combo Timeline

Chi (analogo a log2timeline, ma con meno feature)

▶ NFI Aftertime

Cosa (analogo a log2timeline, ma con una strana licenza)

Dove ▶ prefs.pl, evtparse.pl, jobparse.pl, AnalyzeMFT...
(parser specifici)

→ Raccolta

Elaborazione ▶ 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 impegnato con gli altri strumenti di analisi.

Visualizzazione

Problemi

Credits





Wibbly wobbly timey wimey stuff

Chi

Cosa

Dove

Come

Raccolta

⇒ Elaborazione

Visualizzazione

Problemi

Credits

Elaborazione





Wibbly wobbly timey wimey stuff

Elaborazione dati

► Excel e Calc, o eventualmente un DBMS

Chi

Cosa

Dove

Come

Raccolta

► Elaborazione

Visualizzazione

Problemi

Credits

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.Ink point
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.Ink
Fri Jan 16 2009 18:25:13	335	..cb	7848	[LNK] /mnt/hack/windows_mount/Documents and Settings/Donald Blake/Recent/SECRET.Ink point
Fri Jan 16 2009 18:25:13	254	.acb	8253	[LNK] /mnt/hack/windows_mount/Documents and Settings/Donald Blake/Recent/SECRET (2).Ink 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/Dona
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



Wibbly wobbly timey wimey stuff

Encase

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

Chi

Cosa

Dove

Come

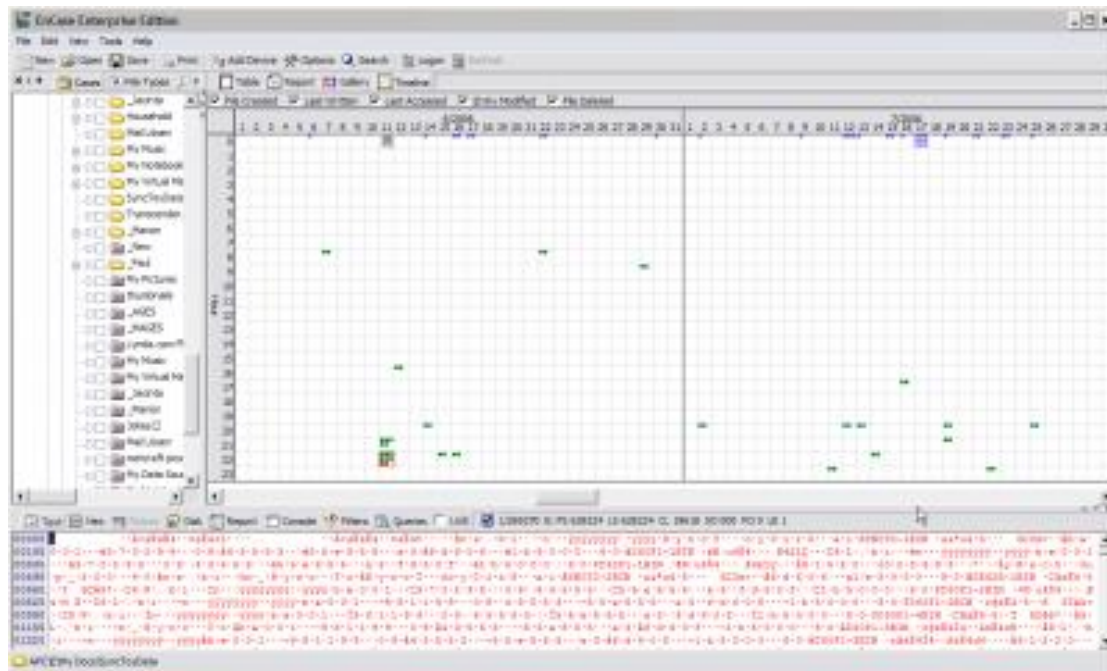
Raccolta

➡ Elaborazione

Visualizzazione

Problemi

Credits





Wibbly wobbly timey wimey stuff

NFI Aftertime (per windows e linux)

► Supporta timestamp di diversa provenienza:

Chi

E-mail

MBox

Cosa

Files

MAC-times, Shortcuts

Dove

Internet history

Internet Explorer cookies / history

Come

Safari cookies / history

Raccolta

Opera cookies

Mozilla/Firefox cookies / history

► Elaborazione

Logs

MSN, Zone alarm, Gator

Visualizzazione

WTMP

Problemi

Console kit

setupapi.log, WBEM

Credits

Multimedia

Exif

Operating System

Windows Event log, Registry, Prefetch, Shadow-files

Linux / Macintosh logs



Wibbly wobbly timey wimey stuff

Aftertime Consumer02 [Consumer02]

File Edit Layout Scan Report Help

Presentation timezone: GMT+00:00 GMT

Date	Time	Scanner	Type	Filename	Path	URL
2006-11-23	10:33:33	FileScanner	changed	07-TiGas-02-0[1].jpg	/Consumer02.E01_0/Documents and Settings/Darth Vader/Local ...	
2006-11-23	10:33:33	FileScanner	accessed	07-TiGas-02-0[1].jpg	/Consumer02.E01_0/Documents and Settings/Darth Vader/Local ...	
2006-11-23	10:33:33	FileScanner	modified	KimFireballs[1].jpg	/Consumer02.E01_0/Documents and Settings/Darth Vader/Local ...	
2006-11-23	10:33:33	FileScanner	changed	KimFireballs[1].jpg	/Consumer02.E01_0/Documents and Settings/Darth Vader/Local ...	
2006-11-23	10:33:33	FileScanner	accessed	KimFireballs[1].jpg	/Consumer02.E01_0/Documents and Settings/Darth Vader/Local ...	

Name : Consumer02

Time Zone : Greenwich Mean Time

Description : <description>

Last Scan : 2010-02-09 06:31

Found : 187204

Scan

Timelines

From: 2006-11-23 00:00

To: 2006-11-23 23:59

Unit: Year #bars

- E-mail
- Files Management
- Internet History
- Logs
- Multimedia
- Operating System

- E-mail
- Files Management
- Internet History
- Logs
- Multimedia
- Operating System
 - Eventlogscanner
 - PrefetchFileScanner
 - Linux / Mac LogScanner
 - RegistryScanner
 - ShadowScanner

Aftertime Consumer04 [Consumer04]

File Edit Layout Scan Report Help

Presentation timezone: GMT+00:00 GMT

Project: Consumer04

Name : Consumer04

Time Zone : Coordinated Universal Time

Description : <description>

Last Scan : 2010-02-08 12:29

Found : 443452

Scan

Timelines

From: 2004-10-23 09:40:11

To: 2011-11-06 02:36:19

Unit: Month #bars ~ 1560 Reset

#events

Date

- Exif:Original
- Exif:Digitized
- Exif:Changed
- Shortcut:Created
- Shortcut:Accessed
- Shortcut:Modified
- MSNLog:Invitation
- MSNLog:InvitationResponse
- MSNLog:Message
- WTMP:Generated
- ConsoleKit:Generated
- ZoneAlarmLog:Generated
- Eventlog:Generated
- Eventlog:Written
- PrefetchFile:Last run
- Linux / Mac Log:Generated
- Registry:Modified
- IECookie:Created
- IECookie:Expired
- SafariCookie:Created
- SafariCookie:Expired
- Gator:Generated
- Shadow:Submitted
- SafariHistory:Last Visited
- SetupAPI:Generated
- OperaCookie:Created
- OperaCookie:Expired
- MozillaCookie:Created
- MozillaCookie:Expired
- IECache:Modified
- IECache:Accessed
- File:Created
- File:Accessed
- File:Modified
- File:Entry modified
- File:Deleted
- MBox:Sender time
- MBox:SMTP time
- WBEMLog:Generated
- MozillaHistory:Last Visited
- MozillaHistory:First Visited

Show legend Logarithmic Multi-chart Stacked Bars

Apply + New Edit Delete

Apply + New Edit Delete



Wibbly wobbly timey wimey stuff

4n6time

The screenshot shows the 4n6time application interface. On the left, there are several panels for filtering and searching: 'Selected Filtering Criteria (click to remove)', 'Field and Value(s)', 'Data and Time', 'String Search', 'Select Logic, Color Code, and Filter', and 'Saved Queries'. The main area features a bar chart titled 'All Database Activity' showing frequency over time (2010-05-19 to 2010-05-20). Below the chart is a table of event logs with columns: row#, datetime, timezone, MACB, source, sourcetype, type, user, host, class, filename, inode, and notes. The table shows several entries for 'Time generated/written' events. At the bottom, there is a 'Backview' section showing details for a selected event.

row#	datetime	timezone	MACB	source	sourcetype	type	user	host	class	filename	inode	notes
1	2010-05-19...	ESTSEDT	MACB	EVT	Event Log	Time gene...	5-1-5-18	WINXPWS...	Security/86...	C:/WINDO...	2898	URL...
2	2010-05-19...	ESTSEDT	MACB	EVT	Event Log	Time gene...	5-1-5-20	WINXPWS...	Security/86...	C:/WINDO...	2898	URL...
3	2010-05-19...	ESTSEDT	MACB	EVT	Event Log	Time gene...	5-1-5-18	WINXPWS...	Security/80...	C:/WINDO...	2898	URL...
4	2010-05-19...	ESTSEDT	MACB	EVT	Event Log	Time gene...	5-1-5-20	WINXPWS...	Security/80...	C:/WINDO...	2898	URL...
5	2010-05-19...	ESTSEDT	MACB	EVT	Event Log	Time gene...	5-1-5-18	WINXPWS...	Security/80...	C:/WINDO...	2898	URL...
6	2010-05-19...	ESTSEDT	MACB	EVT	Event Log	Time gene...	5-1-5-20	WINXPWS...	Security/87...	C:/WINDO...	2898	URL...
7	2010-05-19...	ESTSEDT	MACB	EVT	Event Log	Time gene...	5-1-5-20	WINXPWS...	Security/82...	C:/WINDO...	2898	URL...

- Chi
- Cosa
- Dove
- Come
- Raccolta
- Elaborazione
- Visualizzazione
- Problemi
- Credits



Wibbly wobbly timey wimey stuff

Coming soon: TimeShark

► Progetto italiano di Federico Grattirio per UniPV

Chi

Cosa

Dove

Come

Raccolta

Elaborazione

Visualizzazione

Problemi

Credits

Attività MainGui.py mer 5 giu, 18.09 Timeshark

File Modifica Visualizza ?

Load file: /home/fede/Scrivania/SysEvent.csv

Elenco eventi x Sessioni x Timeline x Statistiche x Preferiti x Aggregazioni x

	date	time	timezone	offset	md5 file	event type	
1	03/01/2013	13:25:40	Europe/Rome	2	b24be2c442de2cf5065fccc06f2787be	7035	03/01/2013,13:25:40,Europe/Rome,MACB,EVT,Event Log,Time generated/written,S-1-5-18,FEDE-B32F088125,Service Control Manag
2	03/01/2013	13:22:30	Europe/Rome	3	b24be2c442de2cf5065fccc06f2787be	14200	03/01/2013,13:22:30,Europe/Rome,MACB,EVT,Event Log,Time generated/written,-,FEDE-B32F088125,WMPNetworkSvc/14200;Info;V
3	03/01/2013	15:00:23	Europe/Rome	4	b24be2c442de2cf5065fccc06f2787be	1074	03/01/2013,15:00:23,Europe/Rome,MACB,EVT,Event Log,Time generated/written,S-1-5-18,FEDE-B32F088125,USER32/1074;Info;win
4	03/01/2013	13:29:10	Europe/Rome	5	b24be2c442de2cf5065fccc06f2787be	7035	03/01/2013,13:29:10,Europe/Rome,MACB,EVT,Event Log,Time generated/written,S-1-5-18,FEDE-B32F088125,Service Control Manag
5	03/01/2013	13:25:07	Europe/Rome	6	b24be2c442de2cf5065fccc06f2787be	7036	03/01/2013,13:25:07,Europe/Rome,MACB,EVT,Event Log,Time generated/written,-,FEDE-B32F088125,Service Control Manager/7036;
6	03/01/2013	15:02:22	Europe/Rome	7	b24be2c442de2cf5065fccc06f2787be	7035	03/01/2013,15:02:22,Europe/Rome,MACB,EVT,Event Log,Time generated/written,S-1-5-21-73586283-606747145-682003330-100;
7	03/06/2013	18:03:57	Europe/Rome	8	b24be2c442de2cf5065fccc06f2787be	7035	03/06/2013,18:03:57,Europe/Rome,MACB,EVT,Event Log,Time generated/written,S-1-5-18,FEDE-B32F088125,Service Control Manag
8	03/13/2013	15:04:22	Europe/Rome	9	b24be2c442de2cf5065fccc06f2787be	6009	03/13/2013,15:04:22,Europe/Rome,MACB,EVT,Event Log,Time generated/written,-,FEDE-B32F088125,EventLog/6009;Info;5.01. - 26C
9	03/12/2013	17:02:50	Europe/Rome	10	b24be2c442de2cf5065fccc06f2787be	7036	03/12/2013,17:02:50,Europe/Rome,MACB,EVT,Event Log,Time generated/written,-,FEDE-B32F088125,Service Control Manager/7036;
10	03/01/2013	13:25:30	Europe/Rome	11	b24be2c442de2cf5065fccc06f2787be	7036	03/01/2013,13:25:30,Europe/Rome,MACB,EVT,Event Log,Time generated/written,-,FEDE-B32F088125,Service Control Manager/7036;
11	03/10/2013	20:17:10	Europe/Rome	12	b24be2c442de2cf5065fccc06f2787be	7035	03/10/2013,20:17:10,Europe/Rome,MACB,EVT,Event Log,Time generated/written,S-1-5-18,FEDE-B32F088125,Service Control Manag
12	03/13/2013	15:11:41	Europe/Rome	13	b24be2c442de2cf5065fccc06f2787be	7035	03/13/2013,15:11:41,Europe/Rome,MACB,EVT,Event Log,Time generated/written,S-1-5-21-73586283-606747145-682003330-100;
13	03/01/2013	14:52:25	Europe/Rome	14	b24be2c442de2cf5065fccc06f2787be	7036	03/01/2013,14:52:25,Europe/Rome,MACB,EVT,Event Log,Time generated/written,-,FEDE-B32F088125,Service Control Manager/7036;
14	03/10/2013	15:08:48	Europe/Rome	15	b24be2c442de2cf5065fccc06f2787be	7036	03/10/2013,15:08:48,Europe/Rome,MACB,EVT,Event Log,Time generated/written,-,FEDE-B32F088125,Service Control Manager/7036;
15	03/01/2013	14:52:25	Europe/Rome	16	b24be2c442de2cf5065fccc06f2787be	7036	03/01/2013,14:52:25,Europe/Rome,MACB,EVT,Event Log,Time generated/written,-,FEDE-B32F088125,Service Control Manager/7036;
16	03/01/2013	15:20:00	Europe/Rome	17	b24be2c442de2cf5065fccc06f2787be	7035	03/01/2013,15:20:00,Europe/Rome,MACB,EVT,Event Log,Time generated/written,S-1-5-18,FEDE-B32F088125,Service Control Manag
17	03/13/2013	14:38:07	Europe/Rome	18	b24be2c442de2cf5065fccc06f2787be	7036	03/13/2013,14:38:07,Europe/Rome,MACB,EVT,Event Log,Time generated/written,-,FEDE-B32F088125,Service Control Manager/7036;
18	03/13/2013	14:38:07	Europe/Rome	19	b24be2c442de2cf5065fccc06f2787be	7035	03/13/2013,14:38:07,Europe/Rome,MACB,EVT,Event Log,Time generated/written,S-1-5-18,FEDE-B32F088125,Service Control Manag
19	03/01/2013	15:24:32	Europe/Rome	20	b24be2c442de2cf5065fccc06f2787be	7036	03/01/2013,15:24:32,Europe/Rome,MACB,EVT,Event Log,Time generated/written,-,FEDE-B32F088125,Service Control Manager/7036;
20	03/01/2013	15:01:06	Europe/Rome	21	b24be2c442de2cf5065fccc06f2787be	7036	03/01/2013,15:01:06,Europe/Rome,MACB,EVT,Event Log,Time generated/written,-,FEDE-B32F088125,Service Control Manager/7036;
21	03/12/2013	17:02:49	Europe/Rome	22	b24be2c442de2cf5065fccc06f2787be	7035	03/12/2013,17:02:49,Europe/Rome,MACB,EVT,Event Log,Time generated/written,S-1-5-18,FEDE-B32F088125,Service Control Manag
22	03/01/2013	13:29:10	Europe/Rome	23	b24be2c442de2cf5065fccc06f2787be	7035	03/01/2013,13:29:10,Europe/Rome,MACB,EVT,Event Log,Time generated/written,S-1-5-18,FEDE-B32F088125,Service Control Manag
23	03/10/2013	15:08:49	Europe/Rome	24	b24be2c442de2cf5065fccc06f2787be	7036	03/10/2013,15:08:49,Europe/Rome,MACB,EVT,Event Log,Time generated/written,-,FEDE-B32F088125,Service Control Manager/7036;
24	03/12/2013	17:02:49	Europe/Rome	25	b24be2c442de2cf5065fccc06f2787be	7036	03/12/2013,17:02:49,Europe/Rome,MACB,EVT,Event Log,Time generated/written,-,FEDE-B32F088125,Service Control Manager/7036;
25	03/01/2013	14:16:34	Europe/Rome	26	b24be2c442de2cf5065fccc06f2787be	6009	03/01/2013,14:16:34,Europe/Rome,MACB,EVT,Event Log,Time generated/written,-,MA CHINENAME,EventLog/6009;Info;5.01. - 2600-
26	03/13/2013	15:11:43	Europe/Rome	27	b24be2c442de2cf5065fccc06f2787be	7036	03/13/2013,15:11:43,Europe/Rome,MACB,EVT,Event Log,Time generated/written,-,FEDE-B32F088125,Service Control Manager/7036;
27	03/01/2013	15:06:23	Europe/Rome	28	b24be2c442de2cf5065fccc06f2787be	7035	03/01/2013,15:06:23,Europe/Rome,MACB,EVT,Event Log,Time generated/written,S-1-5-18,FEDE-B32F088125,Service Control Manag
28	03/01/2013	15:24:33	Europe/Rome	29	b24be2c442de2cf5065fccc06f2787be	7035	03/01/2013,15:24:33,Europe/Rome,MACB,EVT,Event Log,Time generated/written,S-1-5-18,FEDE-B32F088125,Service Control Manag

Applied filters:



Wibbly wobbly timey wimey stuff

Chi

Cosa

Dove

Come

Raccolta

Elaborazione

➡ Visualizzazione

Problemi

Credits

Visualizzazione



Wibbly wobbly timey wimey stuff

Timeline visuali

► Autopsy e l'enscript Timeline Report di Geoff Black generano report HTML

► Spartani, limitati, ma talvolta pratici

Chi

Cosa

Dove

Come

Raccolta

Elaborazione

► Visualizzazione

Problemi

Credits

ID	File Name	Type	Size	Created	Modified	Accessed	Deleted
	change.log.1	Indexed					
45	\\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	\\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	\\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	\\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	\\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	\\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	\\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	\\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	\\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	\\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	\\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	\\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	\\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



Wibbly wobbly timey wimey stuff

Timeline visuali

► Matchware Timelines, LexisNexis TimeMap, TimelineMaker, SmartDraw, Beedocs...

Chi

Cosa

Dove

Come

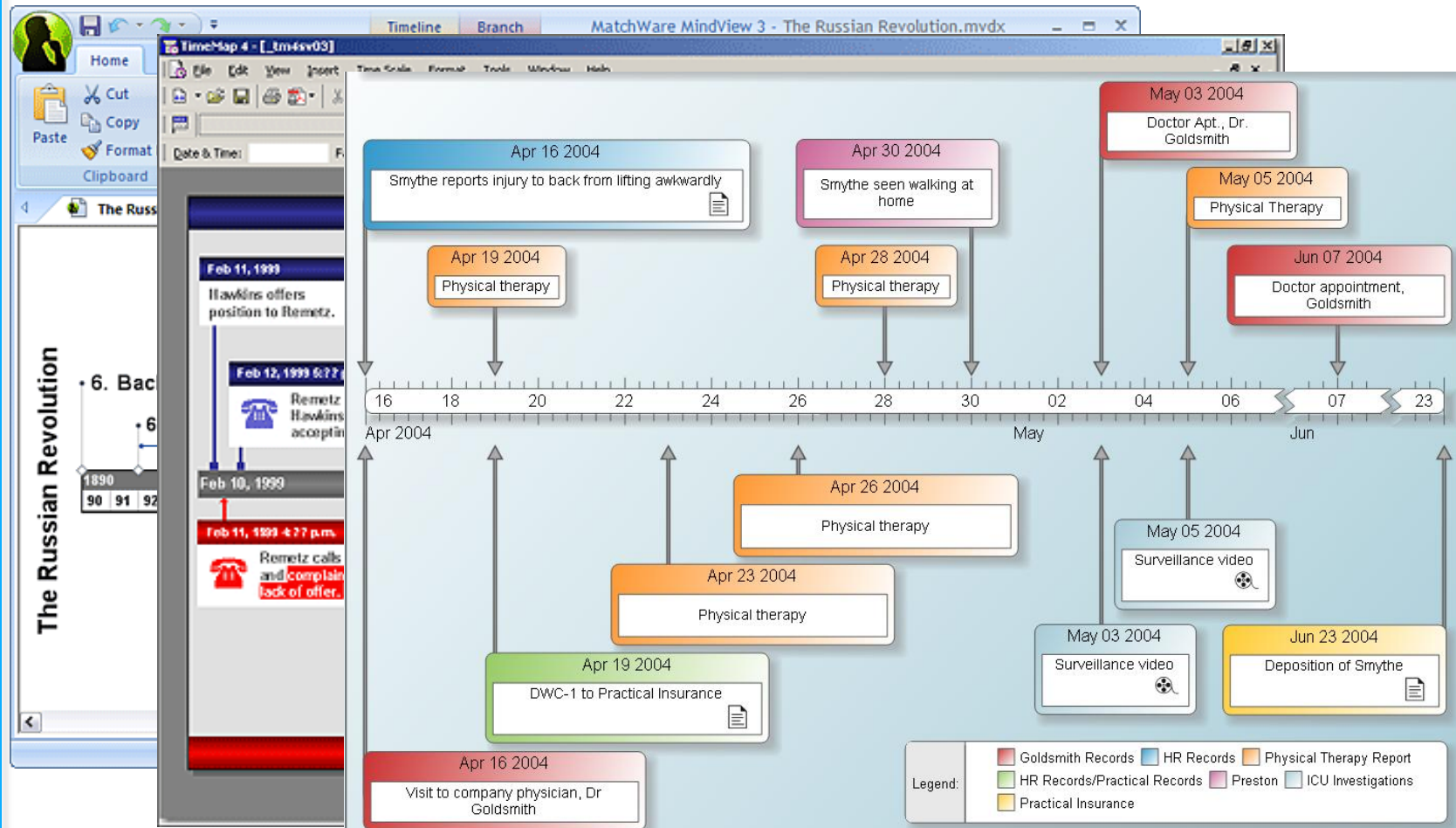
Raccolta

Elaborazione

Visualizzazione

Problemi

Credits





Wibbly wobbly timey wimey stuff

Timeline visuali

▶ Web Scavator, IEF, TimeFlow

Chi

Cosa

Dove

Come

Raccolta

Elaborazione

▶ Visualizzazione

Problemi

Credits

The screenshot displays a web application interface for a timeline visualization. The interface is divided into several sections:

- Navigation Sidebar (Left):** Contains a menu with options: All Results, Refined Results, Chat, Cloud, Email, Web Related, Peer to Peer, Social Networks, Mobile Backups, and Media.
- Timeline Controls (Top Left):** Includes 'Display' and 'Filter' tabs, 'Timeline Controls' with zoom options (zoom out 2X, zoom out 100%), and 'Layout' options (loose, diagonal, graph).
- Global Controls (Middle Left):** Shows 'Showing All 392 Events', 'Not filtering', and a 'clear all' button. Below are dropdown menus for 'Label', 'Groups', 'Color', and 'Dot Size'.
- Color Legend (Bottom Left):** Lists event categories and their counts: Remarks - 96, Meeting - 90, In-town event - 77, Call - 35, Memorandum - 25, Trip - 22, Executive order - 18, Out-of-town event - 13, Bill signing - 10, Down time - 5, Proclamation - 1.
- Main Timeline Area (Right):** Displays a horizontal bar chart representing a timeline from February 2009 to March 2009. The chart is populated with colored dots representing individual events. The events are categorized into sections: Remarks, Meeting, In-town event, Call, Memorandum, Trip, Executive order, Out-of-town event, Bill signing, Down time, and Proclamation.



Wibbly wobbly timey wimey stuff

Chi

Cosa

Dove

Come

Raccolta

Elaborazione

Visualizzazione

⇒ Problemi

Credits

Problemi, intralci, attacchi

Conoscerli, identificarli e sopravvivere





Wibbly wobbly timey wimey stuff

Dispersività

Chi

▶ Troppi dati sono difficili da gestire

Cosa

▶ Troppo pochi potrebbe non essere abbastanza descrittivi

Dove

Come

▶ ...o più facilmente falsati

Raccolta

▶ Servono scanner automatizzati e strumenti di ricerca e filtering efficienti

Elaborazione

Visualizzazione

▶ La rappresentazione è spesso problematica

⇒ Problemi

Credits





Wibbly wobbly timey wimey stuff

Intralci

Chi ► I programmi che eseguono scansioni massive di file (antivirus, antispyware, indicizzatori ecc.) facilmente ne alterano la data di accesso, rendendo l'informazione poco significativa

Elaborazione ► Alcuni antivirus possono essere istruiti a riguardo (p.e. Preserve Filetime in NAV Corporate)

⇒ Problemi

Credits





Wibbly wobbly timey wimey stuff

Intralci intenzionali

Chi

▶ Le manipolazioni possono ovviamente essere intenzionali

Cosa

Dove

▶ Strategia attuata da taluni malware per confondere le acque e rendere difficoltoso individuare il punto di compromissione e le azioni successive

Come

Raccolta

Elaborazione

Visualizzazione

▶ Problemi

Credits

▶ Strategia alla portata degli utenti grazie a strumenti come touch, timestomp, SetMACE e tanti altri





Wibbly wobbly timey wimey stuff

“Ma io cambio l’ora di sistema!”

Chi

▶ Se fatto da Windows Vista o 7, ne troverò traccia nel registro degli eventi (ID 1)

Cosa

▶ Con Linux dipende, con Mac OS X non lo so, ma con BSD sì!

Dove

▶ Se fatto da BIOS, ho ancora qualche speranza di accorgermene dalle incongruenze negli artefatti:

Come

▶ accessi a file che non avrebbero dovuto esistere

Raccolta

▶ uso di applicazioni o servizi non installati

Elaborazione

▶ File LNK in Windows XP (hanno un contatore!)

Visualizzazione

▶ Restore Point (RP## è incrementale per XP, Vista e 7)

▶ Problemi

▶ Sequenzialità dei log (soprattutto su eventi continui) e delle cache applicative

Credits

▶ Confronto con dati esterni al sistema

▶ Pagine HTML salvare, e-mail ricevute, altri metadati con riferimenti temporali esterni





Wibbly wobbly timey wimey stuff

CAT Detect

► Progetto interessante, ma fermo dal 2011

Chi ► Ricerca incongruenze nella sequenza temporale degli eventi

Cosa ► Nato per Windows, ma su principi adattabili ad altri O.S.

Dove

Come

Raccolta

Elaborazione

Visualizzazione

► Problemi

Credits

CAT Detect - Version 1 - Temporal Inconsistency Checking

Enter the query to select a timeline for consistency checking

```

SELECT * FROM (
  (SELECT * FROM RecordedEvents) UNION
  (SELECT * FROM InferredEvents))
AS AllEvents
WHERE Time >=
  (SELECT Time FROM RecordedEvents
   WHERE EventID = 180)
AND Time <=
  ( SELECT Time FROM RecordedEvents
   WHERE EventID = 146)

ORDER BY Time:

```

Launch Query

EventID	Time	Subject	Object	Action	Results
176	2008-10-09T18:47:14	APPLICATION LOCAL SERVICE17605128	SYSTEM	Privilege Use	Success
178	2008-10-09T18:47:14	APPLICATION C:\WINDOWS\explorer.exe18972263	SYSTEM	Detailed Tracking	Success
179	2008-10-09T18:47:14	APPLICATION C:\WINDOWS\system32\winlogon.exe30836417	SYSTEM	Detailed Tracking	Success
180	2008-10-09T18:47:14	APPLICATION C:\WINDOWS\system32\userinit.exe16886931	SYSTEM	Detailed Tracking	Success
181	2008-10-09T18:47:14	USER TARGETBOX\$14098944	SYSTEM	Privilege Use	Success
182	2008-10-09T18:47:14	USER TARGETBOX\$14098944	SYSTEM	Privilege Use	Success
183	2008-10-09T18:47:14	USER TARGETBOX\$14098944	SYSTEM	Privilege Use	Success
184	2008-10-09T18:47:14	USER TARGETBOX\$14098944	SYSTEM	Privilege Use	Success
173	2008-10-09T18:47:15	APPLICATION C:\WINDOWS\system32\svchost.exe28732166	SYSTEM	System Event	Success
174	2008-10-09T18:47:15	USER Domain:40717	SYSTEM	Logon/Logoff	Success
175	2008-10-09T18:47:15	APPLICATION C:\WINDOWS\system32\svchost.exe28732166	SYSTEM	System Event	Success
170	2008-10-09T18:47:16	APPLICATION C:\WINDOWS\system32\logonui.exe26903574	SYSTEM	Detailed Tracking	Success
171	2008-10-09T18:47:16	APPLICATION Files\Messenger\msmsgs.exe29616570	SYSTEM	Detailed Tracking	Success
172	2008-10-09T18:47:16	APPLICATION C:\WINDOWS\system32\ctfmon.exe17591548	SYSTEM	Detailed Tracking	Success
169	2008-10-09T18:47:18	USER baddie27660658	SYSTEM	Privilege Use	Success
167	2008-10-09T18:47:22	APPLICATION LOCAL SERVICE17605128	SYSTEM	Privilege Use	Success

Inconsistent Events

Event ID	Rule Broken
940	(tA in T,x in O,SYSTEM, LOGON, Success) happened-before (tB in T,x in O,, CREATED, r in {Success,Failure,unknown}) && preconditional((tA in T,x in O,SYSTEM, LOGON, Success) , (tB in T,x in O,, CRE...
916	(tA in T,x in O,SYSTEM, LOGON, Success) happened-before (tB in T,x in O,, CREATED, r in {Success,Failure,unknown}) && preconditional((tA in T,x in O,SYSTEM, LOGON, Success) , (tB in T,x in O,, CRE...
917	(tA in T,x in O,SYSTEM, LOGON, Success) happened-before (tB in T,x in O,, MODIFIED, r in {Success,Failure,unknown}) && preconditional((tA in T,x in O,SYSTEM, LOGON, Success) , (tB in T,x in O,, MO...
941	(tA in T,x in O,SYSTEM, LOGON, Success) happened-before (tB in T,x in O,, MODIFIED, r in {Success,Failure,unknown}) && preconditional((tA in T,x in O,SYSTEM, LOGON, Success) , (tB in T,x in O,, MO...
918	(tA in T,x in O,SYSTEM, LOGON, Success) happened-before (tB in T,x in O,, OPENED, r in {Success,Failure,unknown}) && preconditional((tA in T,x in O,SYSTEM, LOGON, Success) , (tB in T,x in O,, OPEN...
942	(tA in T,x in O,SYSTEM, LOGON, Success) happened-before (tB in T,x in O,, OPENED, r in {Success,Failure,unknown}) && preconditional((tA in T,x in O,SYSTEM, LOGON, Success) , (tB in T,x in O,, OPEN...





Wibbly wobbly timey wimey stuff

Teniamoci in contatto...

Daide **Rebus Gabrini**

e-mail: rebus@tipiloschi.net

GPG Public Key: www.tipiloschi.net/rebus.asc
KeyID: 0x176560F7



Chi

Cosa

Dove

Come

Raccolta

Elaborazione

Visualizzazione

Problemi

⇒ Credits



facebook.com/gabrini



twitter.com/therebus



it.linkedin.com/in/rebus

Queste e altre cazzate (come **Rebus'Digest** ed **EventiLoschi**)
su <http://www.tipiloschi.net>