Advanced time-lining using open source tools

Using time-line principles, tools and forensic techniques we establish the context necessary to reconstruct a incident

About me

- Christian Prickaerts
    - prickaerts@fox-it.com

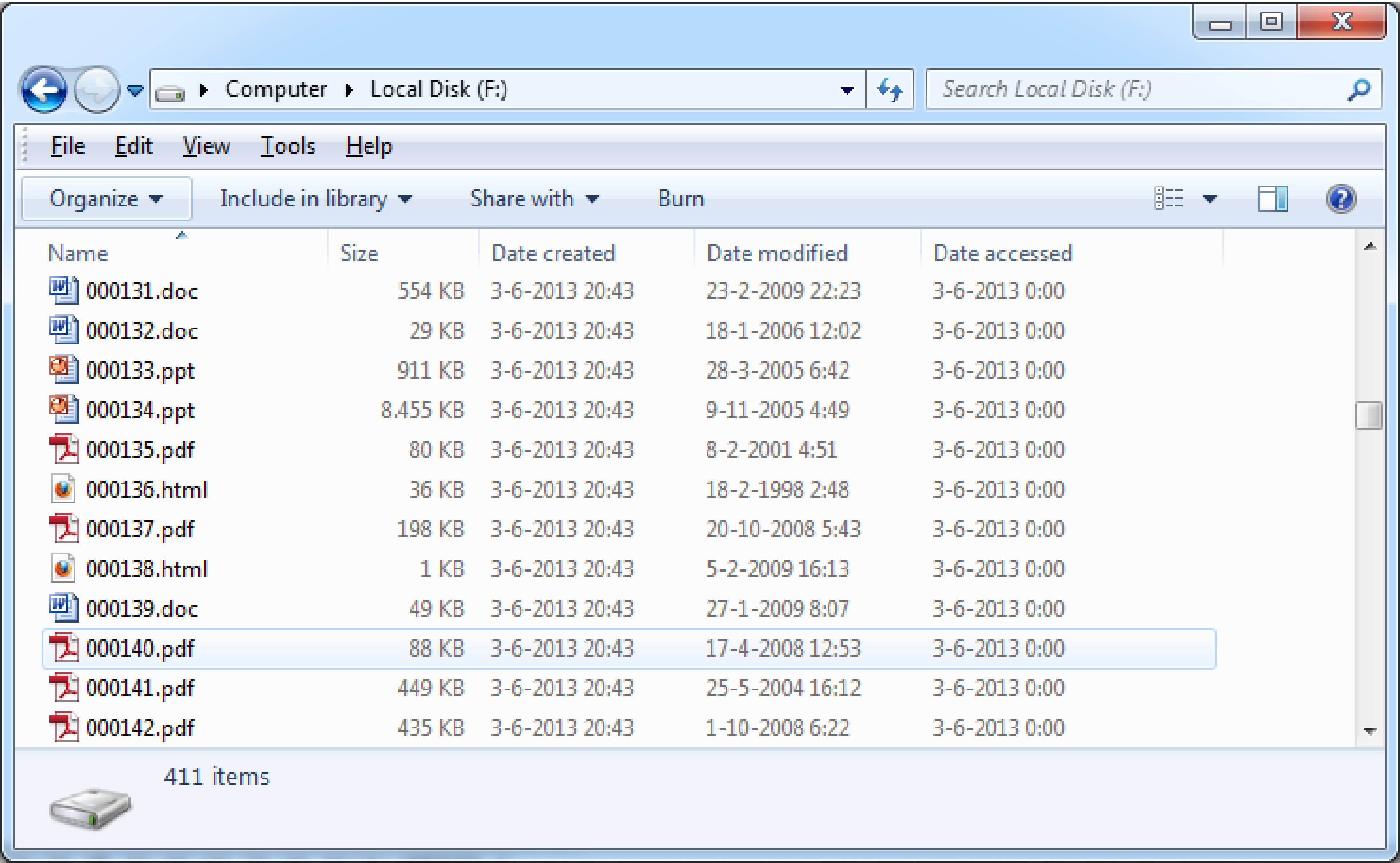
- My day job
    - In charge of DFIR @Fox-IT
    - Providing expert witness testimony
    - SANS Institute instructor

Time is of the essence

- You are using timelines in your investigation, are you not?

- Talking about time
  - Timelining is ***hot!***
  - Combine temporal data from multiple sources
  - New artifacts (sources) added constantly

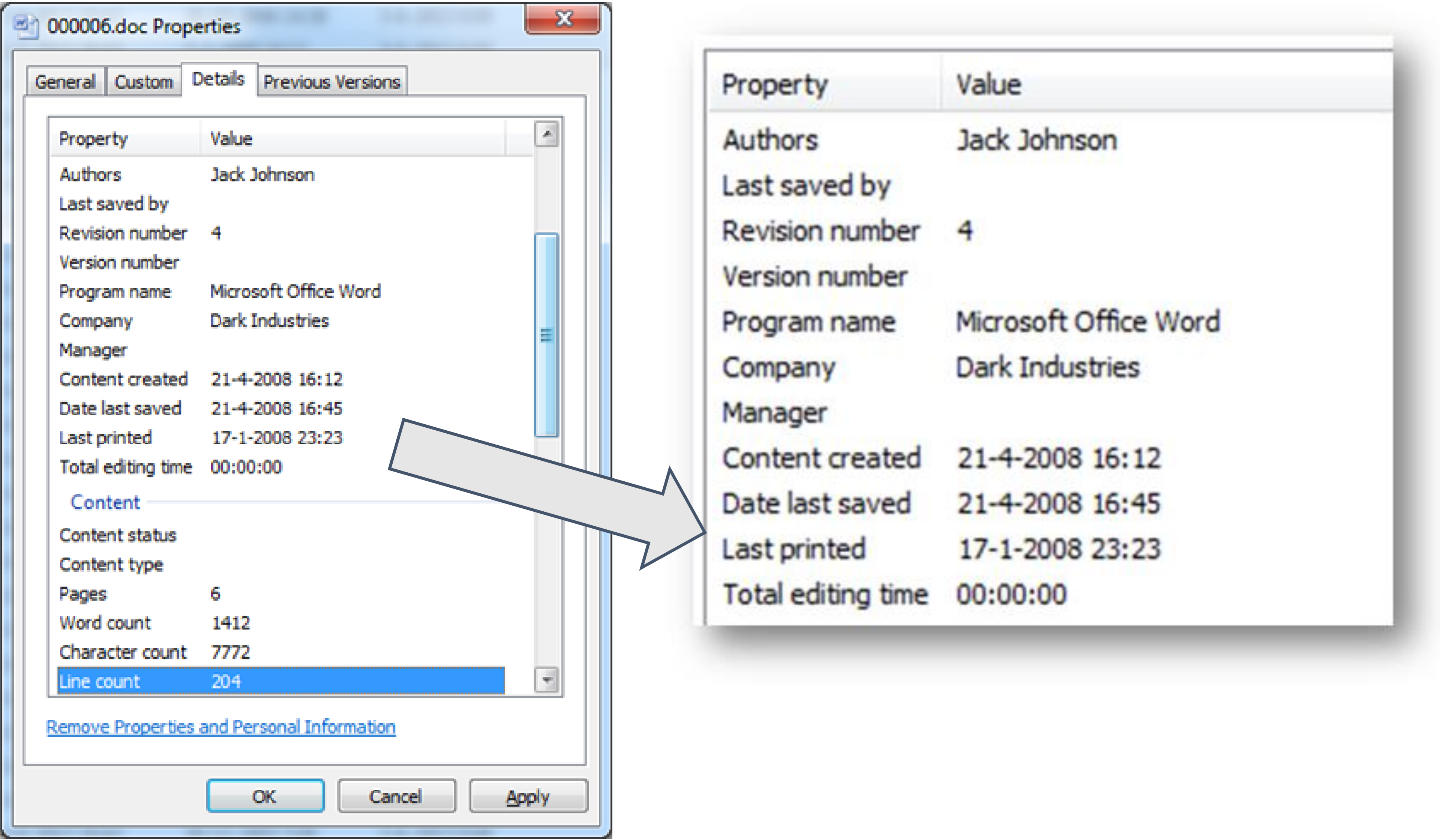
Timestamp example



Name	Size	Date created	Date modified	Date accessed
000131.doc	554 KB	3-6-2013 20:43	23-2-2009 22:23	3-6-2013 0:00
000132.doc	29 KB	3-6-2013 20:43	18-1-2006 12:02	3-6-2013 0:00
000133.ppt	911 KB	3-6-2013 20:43	28-3-2005 6:42	3-6-2013 0:00
000134.ppt	8.455 KB	3-6-2013 20:43	9-11-2005 4:49	3-6-2013 0:00
000135.pdf	80 KB	3-6-2013 20:43	8-2-2001 4:51	3-6-2013 0:00
000136.html	36 KB	3-6-2013 20:43	18-2-1998 2:48	3-6-2013 0:00
000137.pdf	198 KB	3-6-2013 20:43	20-10-2008 5:43	3-6-2013 0:00
000138.html	1 KB	3-6-2013 20:43	5-2-2009 16:13	3-6-2013 0:00
000139.doc	49 KB	3-6-2013 20:43	27-1-2009 8:07	3-6-2013 0:00
000140.pdf	88 KB	3-6-2013 20:43	17-4-2008 12:53	3-6-2013 0:00
000141.pdf	449 KB	3-6-2013 20:43	25-5-2004 16:12	3-6-2013 0:00
000142.pdf	435 KB	3-6-2013 20:43	1-10-2008 6:22	3-6-2013 0:00

411 items

When was document last printed?

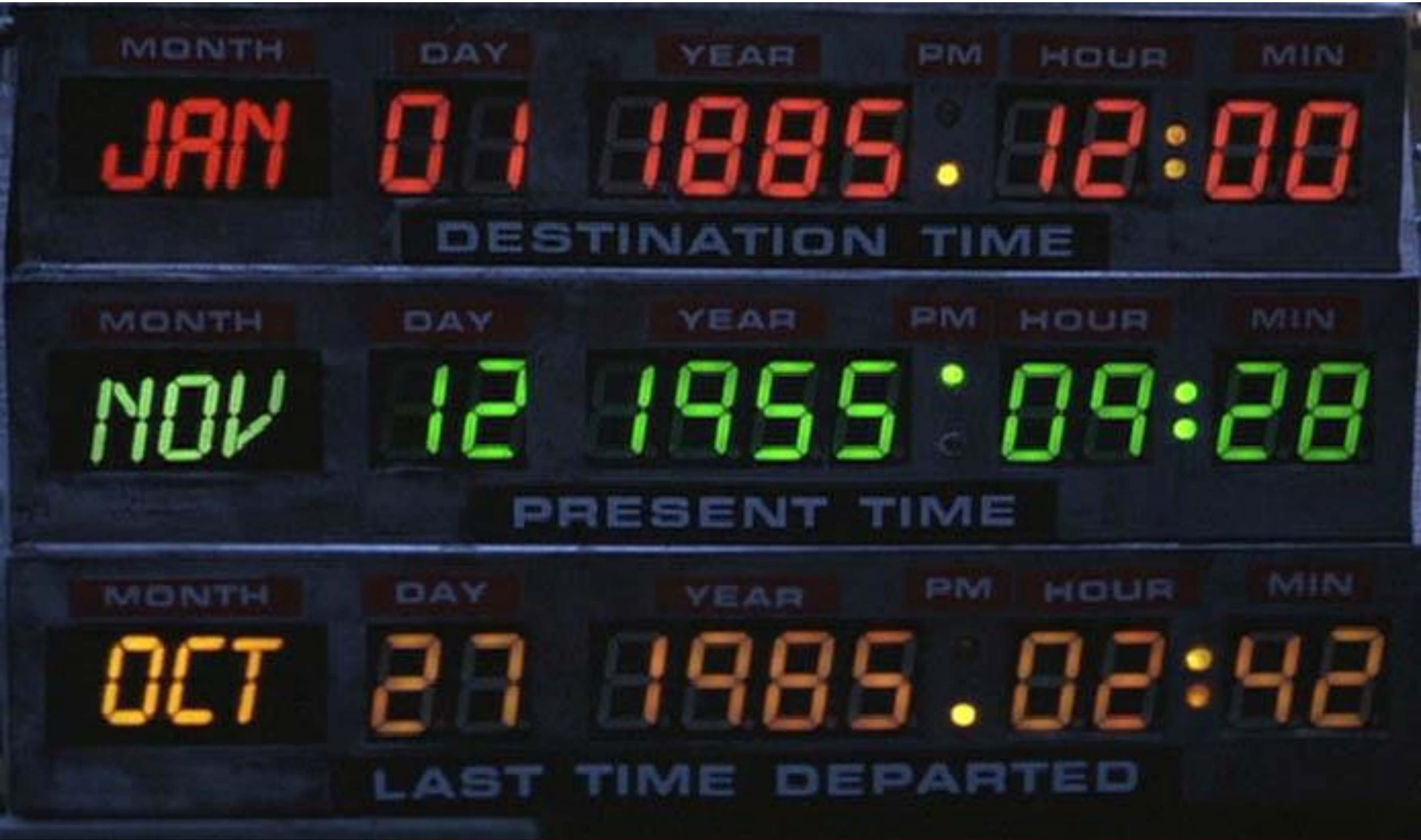


Property	Value
Authors	Jack Johnson
Last saved by	
Revision number	4
Version number	
Program name	Microsoft Office Word
Company	Dark Industries
Manager	
Content created	21-4-2008 16:12
Date last saved	21-4-2008 16:45
Last printed	17-1-2008 23:23
Total editing time	00:00:00
Content	
Content status	
Content type	
Pages	6
Word count	1412
Character count	7772
Line count	204

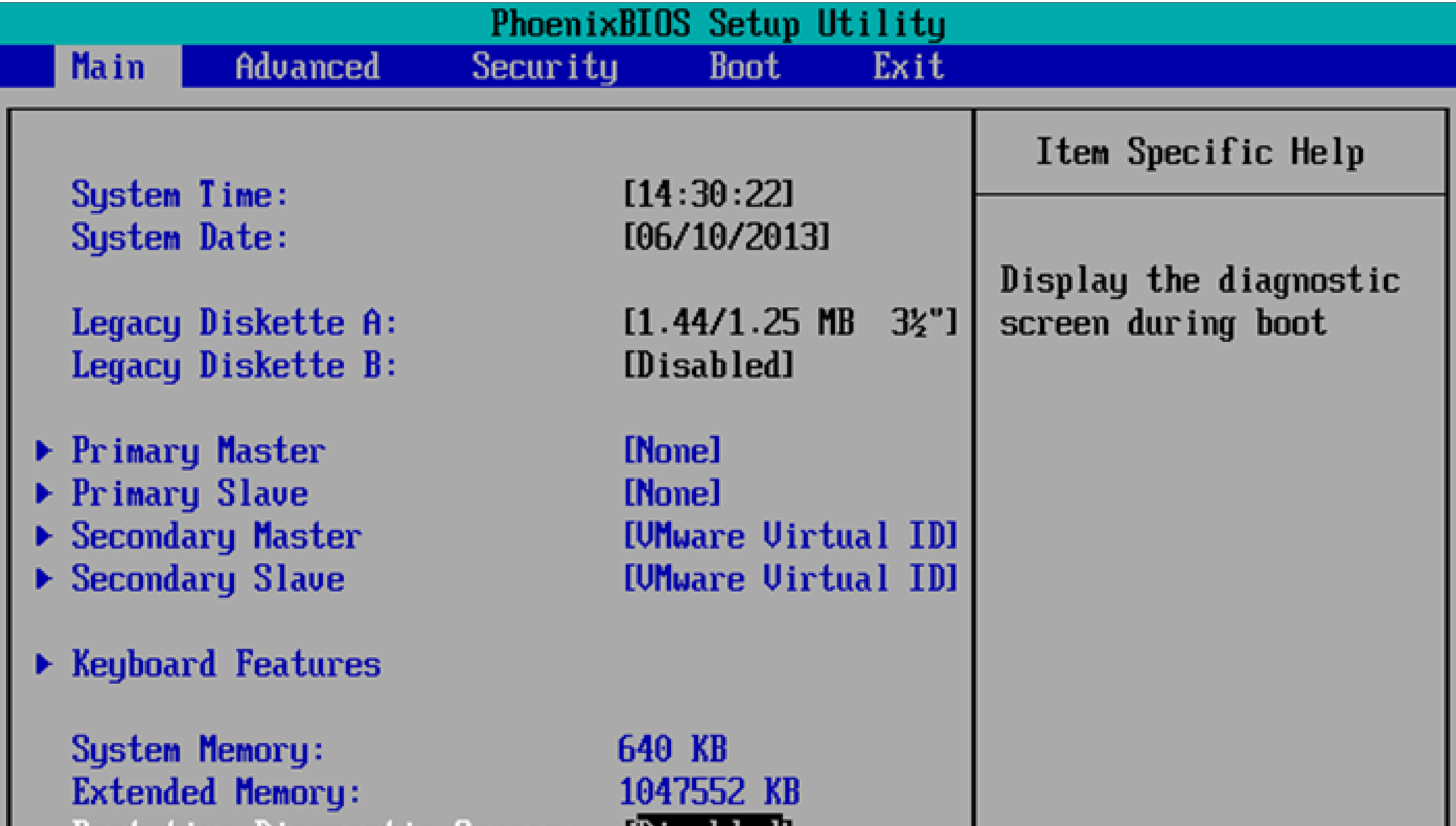
Property	Value
Authors	Jack Johnson
Last saved by	
Revision number	4
Version number	
Program name	Microsoft Office Word
Company	Dark Industries
Manager	
Content created	21-4-2008 16:12
Date last saved	21-4-2008 16:45
Last printed	17-1-2008 23:23
Total editing time	00:00:00

It's a
Trap!

What time is it?



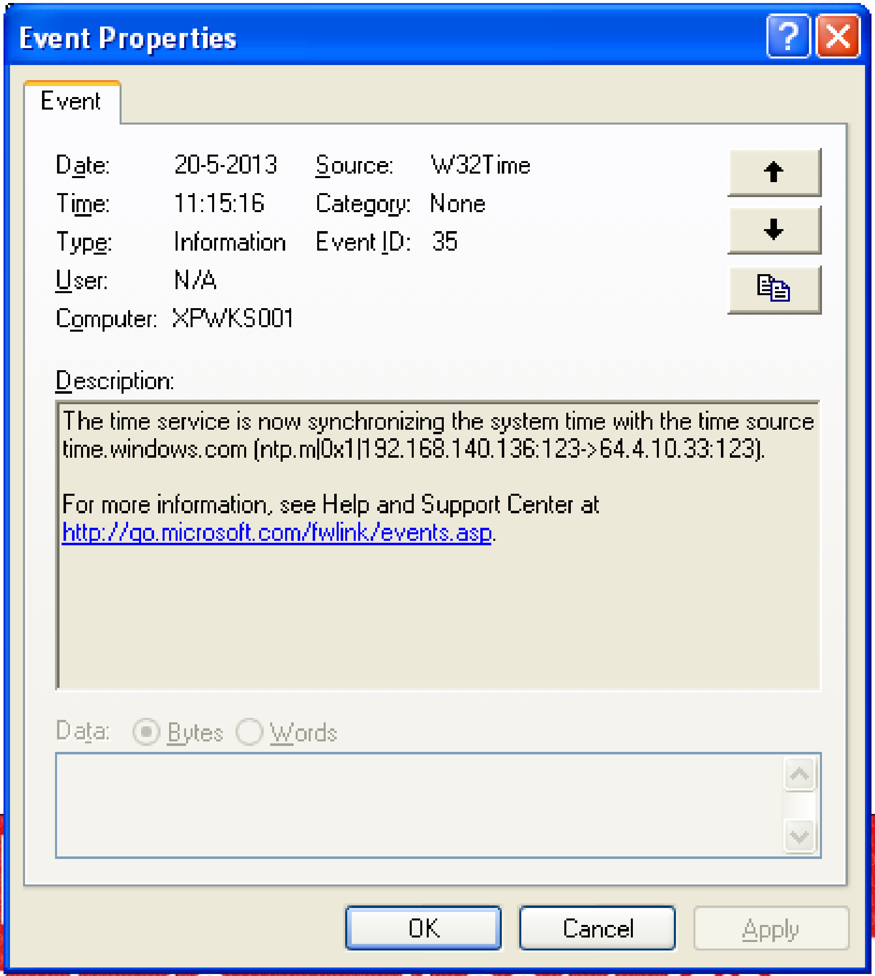
System time at acquisition



```
                    PhoenixBIOS Setup Utility
  Main     Advanced     Security     Boot     Exit

                                                   Item Specific Help

  System Time:               [14:30:22]
  System Date:               [06/10/2013]
                                                Display the diagnostic
  Legacy Diskette A:         [1.44/1.25 MB  3½"]  screen during boot
  Legacy Diskette B:         [Disabled]

▶ Primary Master             [None]
▶ Primary Slave              [None]
▶ Secondary Master           [VMware Virtual ID]
▶ Secondary Slave            [VMware Virtual ID]

▶ Keyboard Features

  System Memory:             640 KB
  Extended Memory:           1047552 KB
```

W32Time / Windows Time Service

- Automatic time sync
  - ID 35 = Good
  - ID 17, 29 (XP) = Bad
  - ID 134 (Win7) = Bad



Event Properties

Event

Date: 20-5-2013
Source: W32Time
Time: 11:15:16
Category: None
Type: Information
Event ID: 35
User: N/A
Computer: XPWKS001

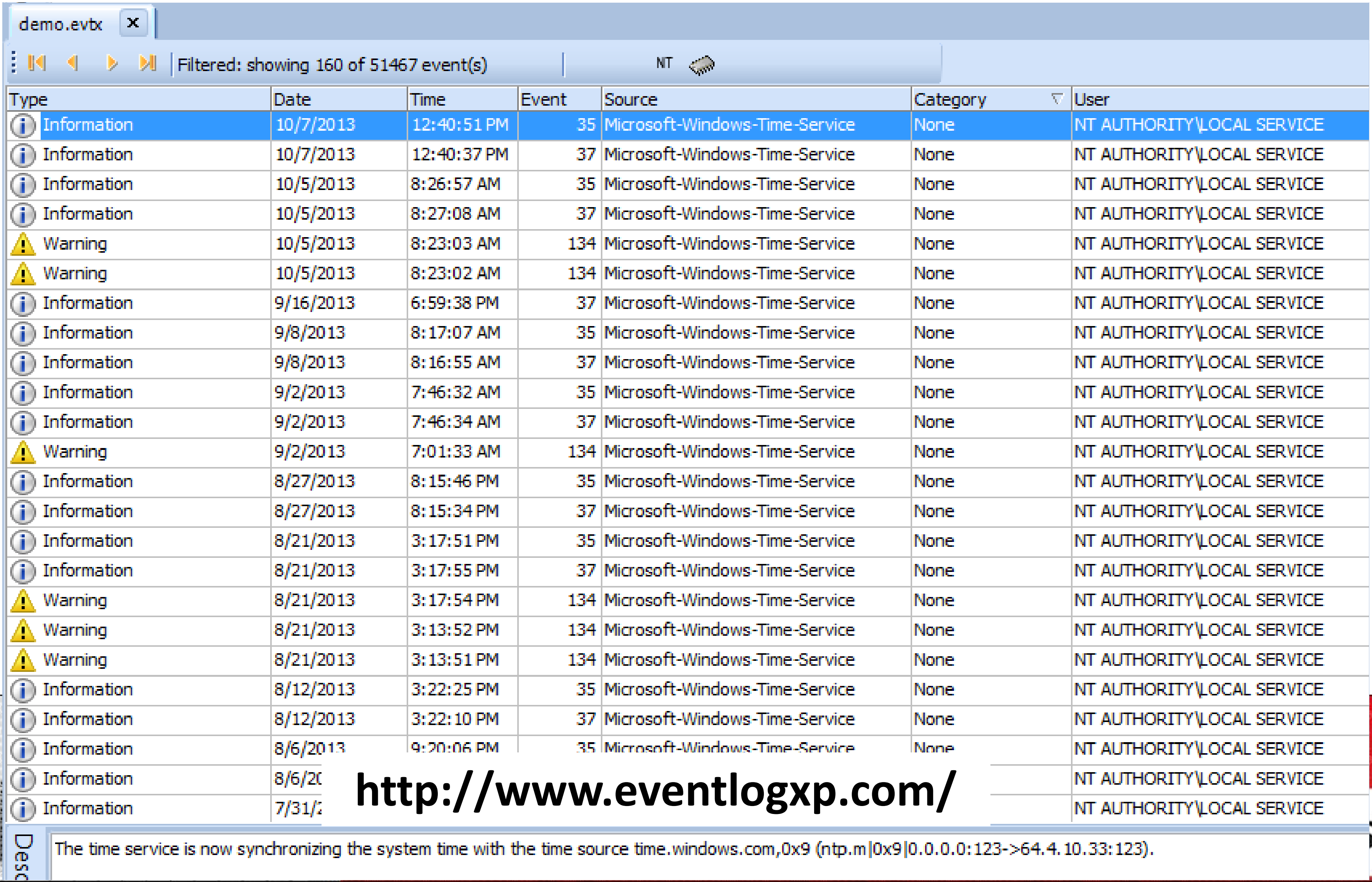
Description:

The time service is now synchronizing the system time with the time source time.windows.com (ntp.m|0x1|192.168.140.136:123->64.4.10.33:123).

For more information, see Help and Support Center at http://go.microsoft.com/fwlink/events.asp.

Data: ● Bytes ○ Words

Look for a bunch of those



Filtered: showing 160 of 51467 event(s)

Type	Date	Time	Event	Source	Category	User
Information	10/7/2013	12:40:51 PM	35	Microsoft-Windows-Time-Service	None	NT AUTHORITY\LOCAL SERVICE
Information	10/7/2013	12:40:37 PM	37	Microsoft-Windows-Time-Service	None	NT AUTHORITY\LOCAL SERVICE
Information	10/5/2013	8:26:57 AM	35	Microsoft-Windows-Time-Service	None	NT AUTHORITY\LOCAL SERVICE
Information	10/5/2013	8:27:08 AM	37	Microsoft-Windows-Time-Service	None	NT AUTHORITY\LOCAL SERVICE
Warning	10/5/2013	8:23:03 AM	134	Microsoft-Windows-Time-Service	None	NT AUTHORITY\LOCAL SERVICE
Warning	10/5/2013	8:23:02 AM	134	Microsoft-Windows-Time-Service	None	NT AUTHORITY\LOCAL SERVICE
Information	9/16/2013	6:59:38 PM	37	Microsoft-Windows-Time-Service	None	NT AUTHORITY\LOCAL SERVICE
Information	9/8/2013	8:17:07 AM	35	Microsoft-Windows-Time-Service	None	NT AUTHORITY\LOCAL SERVICE
Information	9/8/2013	8:16:55 AM	37	Microsoft-Windows-Time-Service	None	NT AUTHORITY\LOCAL SERVICE
Information	9/2/2013	7:46:32 AM	35	Microsoft-Windows-Time-Service	None	NT AUTHORITY\LOCAL SERVICE
Information	9/2/2013	7:46:34 AM	37	Microsoft-Windows-Time-Service	None	NT AUTHORITY\LOCAL SERVICE
Warning	9/2/2013	7:01:33 AM	134	Microsoft-Windows-Time-Service	None	NT AUTHORITY\LOCAL SERVICE
Information	8/27/2013	8:15:46 PM	35	Microsoft-Windows-Time-Service	None	NT AUTHORITY\LOCAL SERVICE
Information	8/27/2013	8:15:34 PM	37	Microsoft-Windows-Time-Service	None	NT AUTHORITY\LOCAL SERVICE
Information	8/21/2013	3:17:51 PM	35	Microsoft-Windows-Time-Service	None	NT AUTHORITY\LOCAL SERVICE
Information	8/21/2013	3:17:55 PM	37	Microsoft-Windows-Time-Service	None	NT AUTHORITY\LOCAL SERVICE
Warning	8/21/2013	3:17:54 PM	134	Microsoft-Windows-Time-Service	None	NT AUTHORITY\LOCAL SERVICE
Warning	8/21/2013	3:13:52 PM	134	Microsoft-Windows-Time-Service	None	NT AUTHORITY\LOCAL SERVICE
Warning	8/21/2013	3:13:51 PM	134	Microsoft-Windows-Time-Service	None	NT AUTHORITY\LOCAL SERVICE
Information	8/12/2013	3:22:25 PM	35	Microsoft-Windows-Time-Service	None	NT AUTHORITY\LOCAL SERVICE
Information	8/12/2013	3:22:10 PM	37	Microsoft-Windows-Time-Service	None	NT AUTHORITY\LOCAL SERVICE
Information	8/6/2013	9:20:06 PM	35	Microsoft-Windows-Time-Service	None	NT AUTHORITY\LOCAL SERVICE
Information	8/6/20					NT AUTHORITY\LOCAL SERVICE
Information	7/31/2					NT AUTHORITY\LOCAL SERVICE

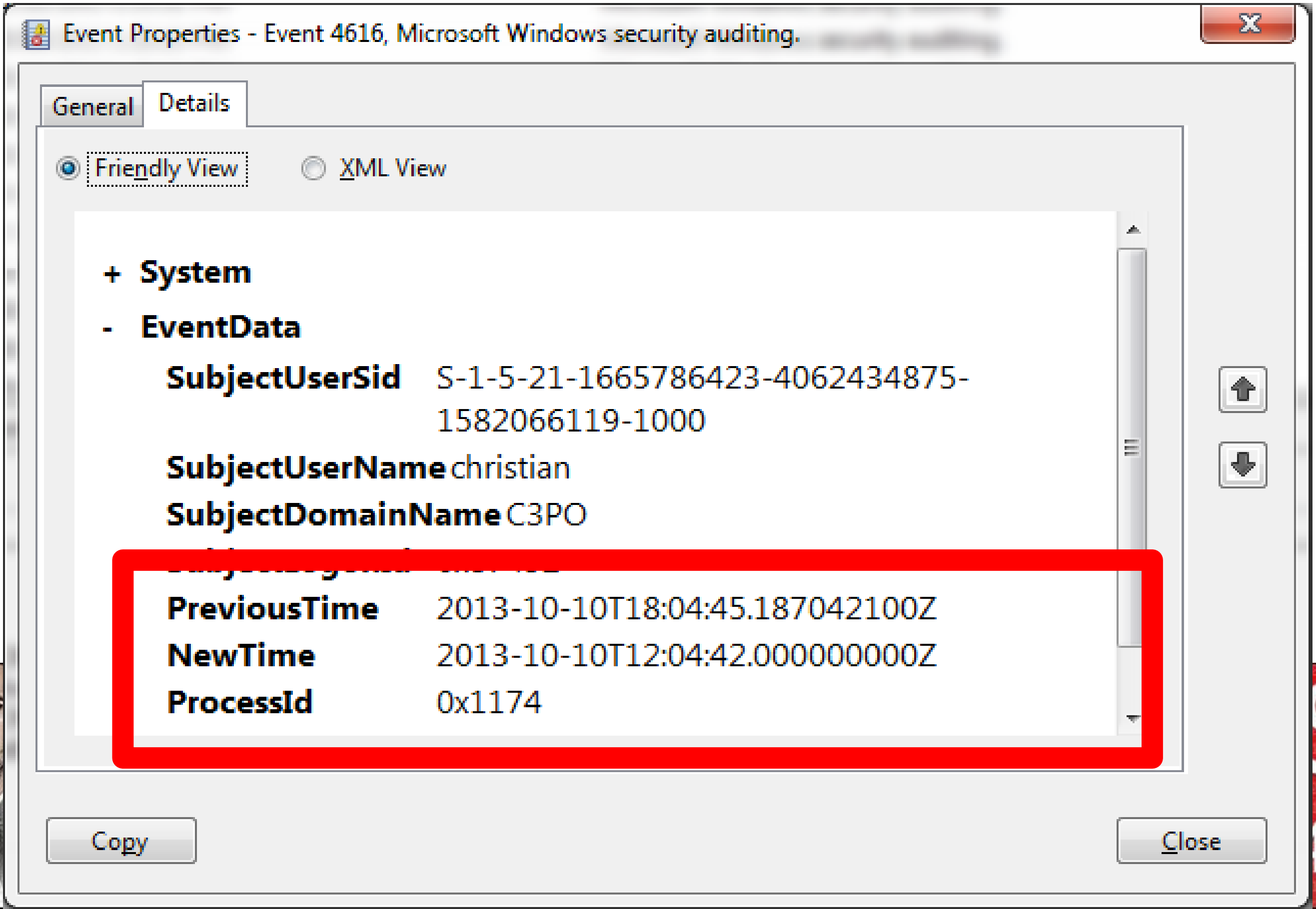
Desc

The time service is now synchronizing the system time with the time source time.windows.com,0x9 (ntp.m|0x9|0.0.0.0:123->64.4.10.33:123).

http://www.eventlogxp.com/

Times, they are changing

- Look for system time change events: event 4616



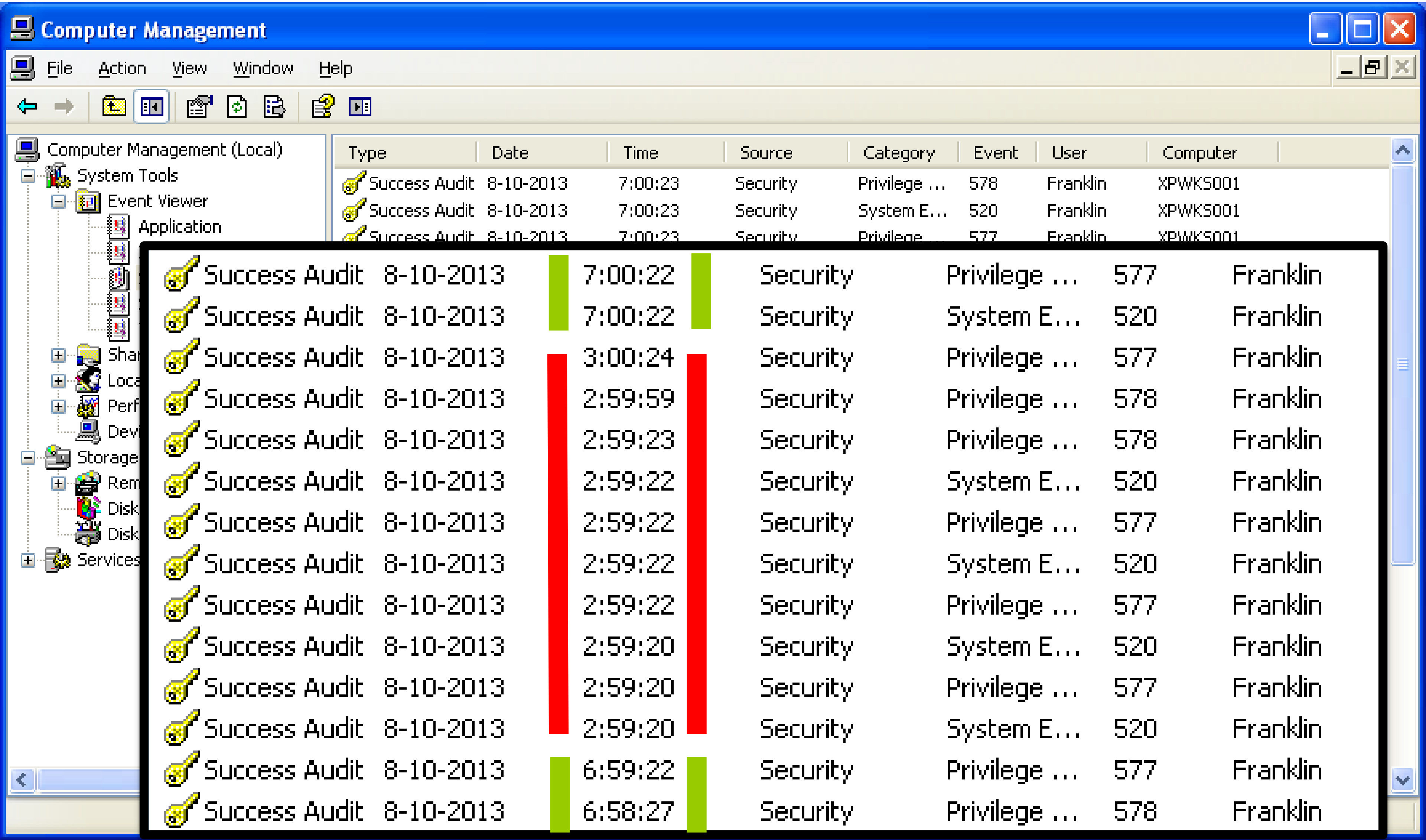
Event Properties - Event 4616, Microsoft Windows security auditing.

+ System

- EventData

SubjectUserSid	S-1-5-21-1665786423-4062434875-1582066119-1000
SubjectUserName	christian
SubjectDomainName	C3PO
[illegible]	[illegible]
PreviousTime	2013-10-10T18:04:45.187042100Z
NewTime	2013-10-10T12:04:42.000000000Z
ProcessId	0x1174

Sorting by logical order

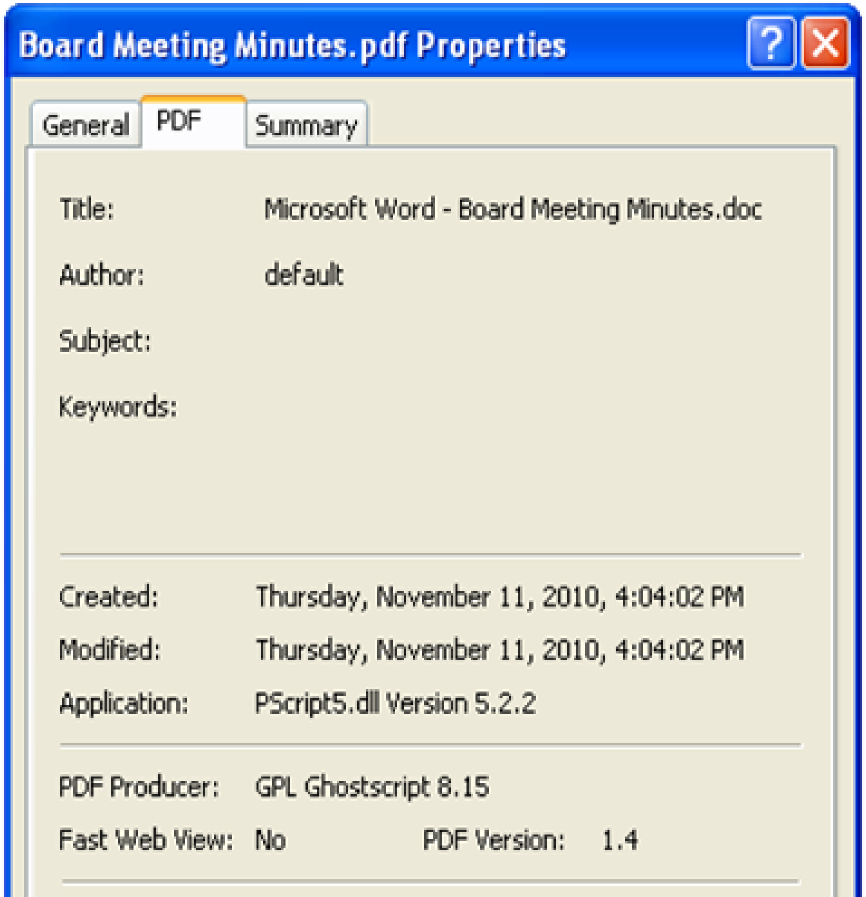


Type	Date	Time	Source	Category	Event	User	Computer
Success Audit	8-10-2013	7:00:23	Security	Privilege ...	578	Franklin	XPWKS001
Success Audit	8-10-2013	7:00:23	Security	System E...	520	Franklin	XPWKS001
Success Audit	8-10-2013	7:00:23	Security	Privilege ...	577	Franklin	XPWKS001

Success Audit	8-10-2013	7:00:22	Security	Privilege ...	577	Franklin
Success Audit	8-10-2013	7:00:22	Security	System E...	520	Franklin
Success Audit	8-10-2013	3:00:24	Security	Privilege ...	577	Franklin
Success Audit	8-10-2013	2:59:59	Security	Privilege ...	578	Franklin
Success Audit	8-10-2013	2:59:23	Security	Privilege ...	578	Franklin
Success Audit	8-10-2013	2:59:22	Security	System E...	520	Franklin
Success Audit	8-10-2013	2:59:22	Security	Privilege ...	577	Franklin
Success Audit	8-10-2013	2:59:22	Security	System E...	520	Franklin
Success Audit	8-10-2013	2:59:22	Security	Privilege ...	577	Franklin
Success Audit	8-10-2013	2:59:20	Security	System E...	520	Franklin
Success Audit	8-10-2013	2:59:20	Security	Privilege ...	577	Franklin
Success Audit	8-10-2013	2:59:20	Security	System E...	520	Franklin
Success Audit	8-10-2013	6:59:22	Security	Privilege ...	577	Franklin
Success Audit	8-10-2013	6:58:27	Security	Privilege ...	578	Franklin

Summertime, and the living is… well, whatever

Viewed on November 11



Board Meeting Minutes.pdf Properties

Title: Microsoft Word - Board Meeting Minutes.doc

Author: default

Subject:

Keywords:

Created: Thursday, November 11, 2010, 4:04:02 PM

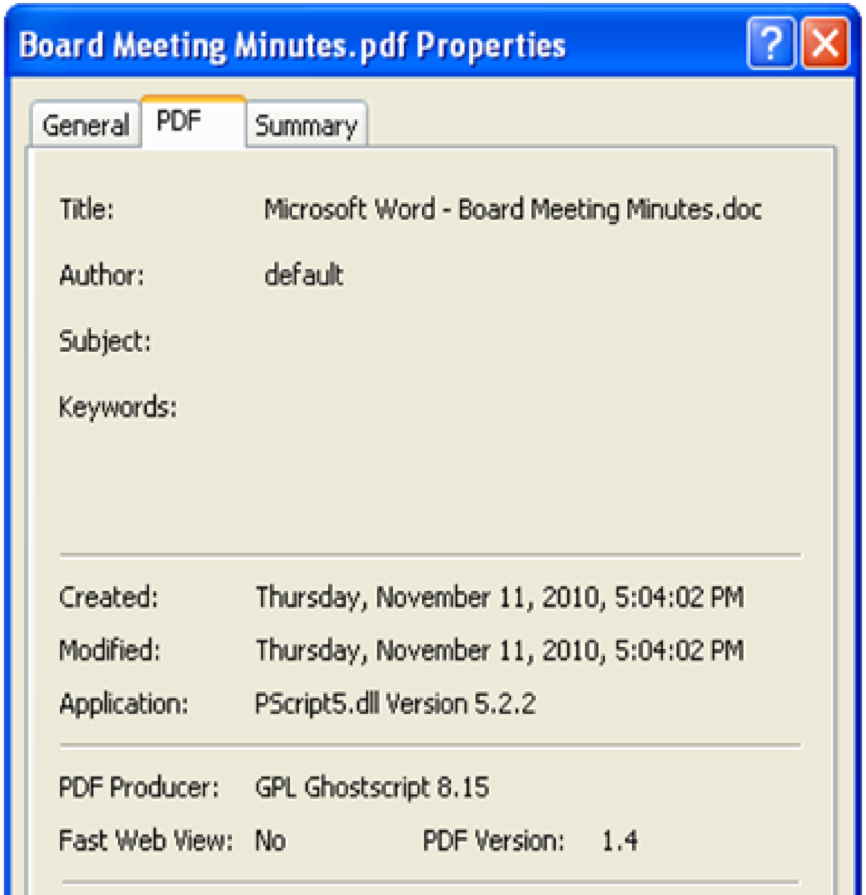
Modified: Thursday, November 11, 2010, 4:04:02 PM

Application: PScript5.dll Version 5.2.2

PDF Producer: GPL Ghostscript 8.15

Fast Web View: No PDF Version: 1.4

Viewed on May 28



Board Meeting Minutes.pdf Properties

Title: Microsoft Word - Board Meeting Minutes.doc

Author: default

Subject:

Keywords:

Created: Thursday, November 11, 2010, 5:04:02 PM

Modified: Thursday, November 11, 2010, 5:04:02 PM

Application: PScript5.dll Version 5.2.2

PDF Producer: GPL Ghostscript 8.15

Fast Web View: No PDF Version: 1.4

Timeline Utopia

The Reality

Logic dictates

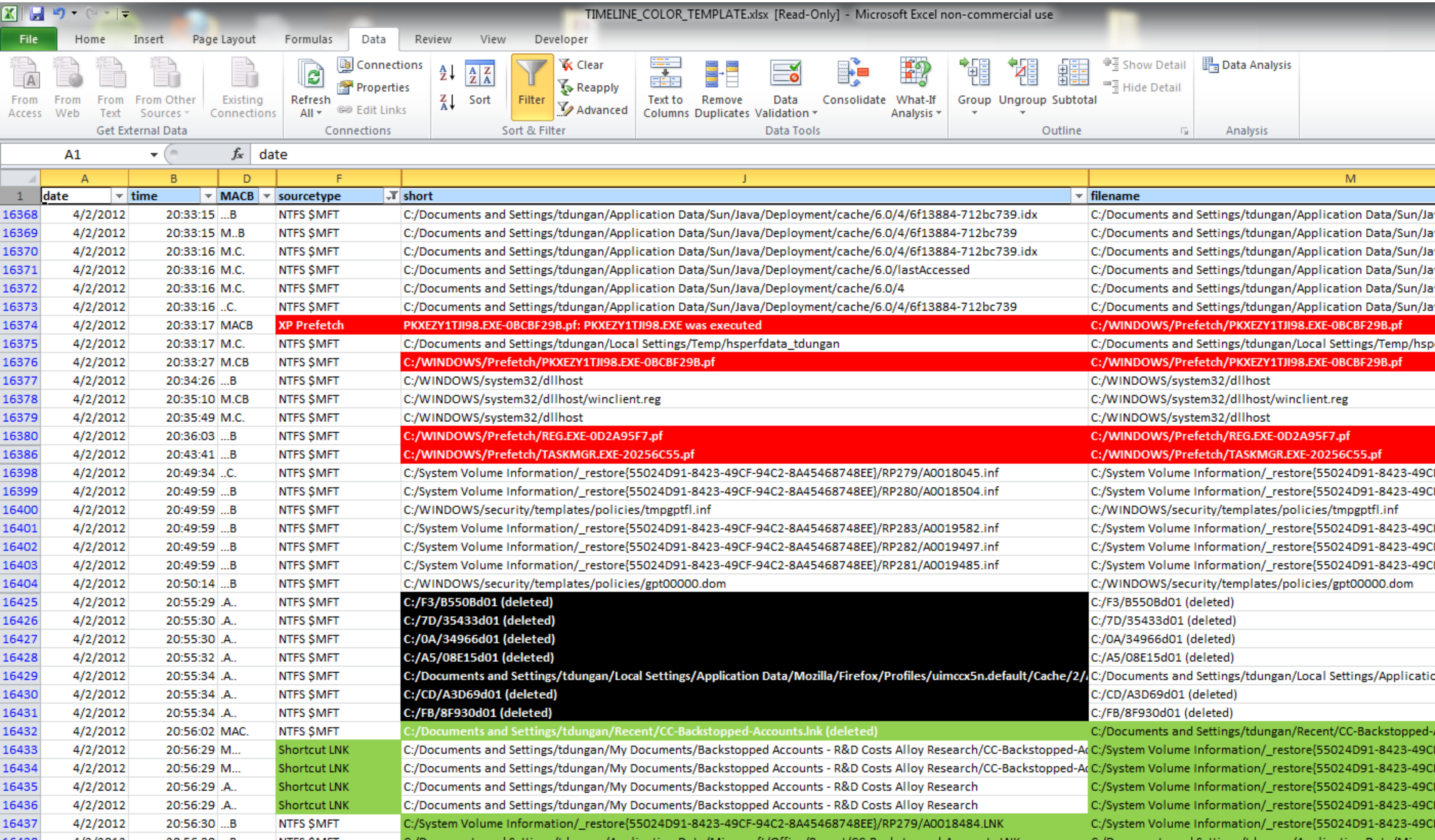
- You have lots of tools at your disposal
- But they are <u>not</u> intelligent (enough)

- No. 1 tool?
  - (Your) grey mass
- No. 2 tool
  - Log2Timeline/Plaso

Log2timeline aka Plaso

https://code.google.com/p/plaso/

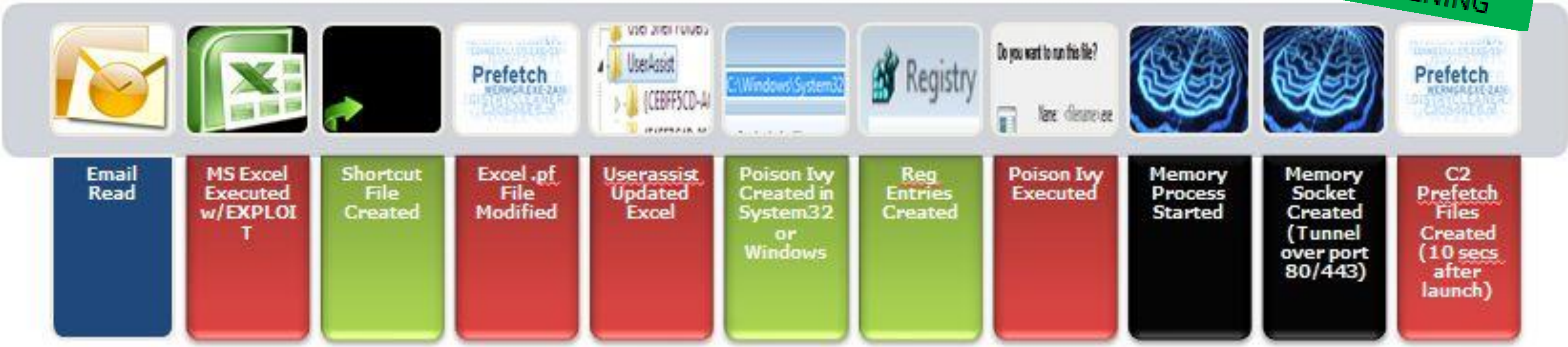
Super Timeline



	A	B	D	F	J	M
1	date	time	MACB	sourcetype	short	filename
16368	4/2/2012	20:33:15	...B	NTFS $MFT	C:/Documents and Settings/tdungan/Application Data/Sun/Java/Deployment/cache/6.0/4/6f13884-712bc739.idx	C:/Documents and Settings/tdungan/Application Data/Sun/Ja
16369	4/2/2012	20:33:15	M..B	NTFS $MFT	C:/Documents and Settings/tdungan/Application Data/Sun/Java/Deployment/cache/6.0/4/6f13884-712bc739	C:/Documents and Settings/tdungan/Application Data/Sun/Ja
16370	4/2/2012	20:33:16	M.C.	NTFS $MFT	C:/Documents and Settings/tdungan/Application Data/Sun/Java/Deployment/cache/6.0/4/6f13884-712bc739.idx	C:/Documents and Settings/tdungan/Application Data/Sun/Ja
16371	4/2/2012	20:33:16	M.C.	NTFS $MFT	C:/Documents and Settings/tdungan/Application Data/Sun/Java/Deployment/cache/6.0/lastAccessed	C:/Documents and Settings/tdungan/Application Data/Sun/Ja
16372	4/2/2012	20:33:16	M.C.	NTFS $MFT	C:/Documents and Settings/tdungan/Application Data/Sun/Java/Deployment/cache/6.0/4	C:/Documents and Settings/tdungan/Application Data/Sun/Ja
16373	4/2/2012	20:33:16	..C.	NTFS $MFT	C:/Documents and Settings/tdungan/Application Data/Sun/Java/Deployment/cache/6.0/4/6f13884-712bc739	C:/Documents and Settings/tdungan/Application Data/Sun/Ja
16374	4/2/2012	20:33:17	MACB	XP Prefetch	PKXEZY1TJI98.EXE-0BCBF29B.pf: PKXEZY1TJI98.EXE was executed	C:/WINDOWS/Prefetch/PKXEZY1TJI98.EXE-0BCBF29B.pf
16375	4/2/2012	20:33:17	M.C.	NTFS $MFT	C:/Documents and Settings/tdungan/Local Settings/Temp/hsperfdata_tdungan	C:/Documents and Settings/tdungan/Local Settings/Temp/hsp
16376	4/2/2012	20:33:27	M.CB	NTFS $MFT	C:/WINDOWS/Prefetch/PKXEZY1TJI98.EXE-0BCBF29B.pf	C:/WINDOWS/Prefetch/PKXEZY1TJI98.EXE-0BCBF29B.pf
16377	4/2/2012	20:34:26	...B	NTFS $MFT	C:/WINDOWS/system32/dllhost	C:/WINDOWS/system32/dllhost
16378	4/2/2012	20:35:10	M.CB	NTFS $MFT	C:/WINDOWS/system32/dllhost/winclient.reg	C:/WINDOWS/system32/dllhost/winclient.reg
16379	4/2/2012	20:35:49	M.C.	NTFS $MFT	C:/WINDOWS/system32/dllhost	C:/WINDOWS/system32/dllhost
16380	4/2/2012	20:36:03	...B	NTFS $MFT	C:/WINDOWS/Prefetch/REG.EXE-0D2A95F7.pf	C:/WINDOWS/Prefetch/REG.EXE-0D2A95F7.pf
16386	4/2/2012	20:43:41	...B	NTFS $MFT	C:/WINDOWS/Prefetch/TASKMGR.EXE-20256C55.pf	C:/WINDOWS/Prefetch/TASKMGR.EXE-20256C55.pf
16398	4/2/2012	20:49:34	..C.	NTFS $MFT	C:/System Volume Information/_restore{55024D91-8423-49CF-94C2-8A45468748EE}/RP279/A0018045.inf	C:/System Volume Information/_restore{55024D91-8423-49C
16399	4/2/2012	20:49:59	...B	NTFS $MFT	C:/System Volume Information/_restore{55024D91-8423-49CF-94C2-8A45468748EE}/RP280/A0018504.inf	C:/System Volume Information/_restore{55024D91-8423-49C
16400	4/2/2012	20:49:59	...B	NTFS $MFT	C:/WINDOWS/security/templates/policies/tmpgptfl.inf	C:/WINDOWS/security/templates/policies/tmpgptfl.inf
16401	4/2/2012	20:49:59	...B	NTFS $MFT	C:/System Volume Information/_restore{55024D91-8423-49CF-94C2-8A45468748EE}/RP283/A0019582.inf	C:/System Volume Information/_restore{55024D91-8423-49C
16402	4/2/2012	20:49:59	...B	NTFS $MFT	C:/System Volume Information/_restore{55024D91-8423-49CF-94C2-8A45468748EE}/RP282/A0019497.inf	C:/System Volume Information/_restore{55024D91-8423-49C
16403	4/2/2012	20:49:59	...B	NTFS $MFT	C:/System Volume Information/_restore{55024D91-8423-49CF-94C2-8A45468748EE}/RP281/A0019485.inf	C:/System Volume Information/_restore{55024D91-8423-49C
16404	4/2/2012	20:50:14	...B	NTFS $MFT	C:/WINDOWS/security/templates/policies/gpt00000.dom	C:/WINDOWS/security/templates/policies/gpt00000.dom
16425	4/2/2012	20:55:29	.A..	NTFS $MFT	C:/F3/B550Bd01 (deleted)	C:/F3/B550Bd01 (deleted)
16426	4/2/2012	20:55:30	.A..	NTFS $MFT	C:/7D/35433d01 (deleted)	C:/7D/35433d01 (deleted)
16427	4/2/2012	20:55:30	.A..	NTFS $MFT	C:/0A/34966d01 (deleted)	C:/0A/34966d01 (deleted)
16428	4/2/2012	20:55:32	.A..	NTFS $MFT	C:/A5/08E15d01 (deleted)	C:/A5/08E15d01 (deleted)
16429	4/2/2012	20:55:34	.A..	NTFS $MFT	C:/Documents and Settings/tdungan/Local Settings/Application Data/Mozilla/Firefox/Profiles/uimccx5n.default/Cache/2/	C:/Documents and Settings/tdungan/Local Settings/Applicatio
16430	4/2/2012	20:55:34	.A..	NTFS $MFT	C:/CD/A3D69d01 (deleted)	C:/CD/A3D69d01 (deleted)
16431	4/2/2012	20:55:34	.A..	NTFS $MFT	C:/FB/8F930d01 (deleted)	C:/FB/8F930d01 (deleted)
16432	4/2/2012	20:56:02	MAC.	NTFS $MFT	C:/Documents and Settings/tdungan/Recent/CC-Backstopped-Accounts.lnk (deleted)	C:/Documents and Settings/tdungan/Recent/CC-Backstopped-
16433	4/2/2012	20:56:29	M...	Shortcut LNK	C:/Documents and Settings/tdungan/My Documents/Backstopped Accounts - R&D Costs Alloy Research/CC-Backstopped-Ac	C:/System Volume Information/_restore{55024D91-8423-49C
16434	4/2/2012	20:56:29	M...	Shortcut LNK	C:/Documents and Settings/tdungan/My Documents/Backstopped Accounts - R&D Costs Alloy Research/CC-Backstopped-Ac	C:/System Volume Information/_restore{55024D91-8423-49C
16435	4/2/2012	20:56:29	.A..	Shortcut LNK	C:/Documents and Settings/tdungan/My Documents/Backstopped Accounts - R&D Costs Alloy Research	C:/System Volume Information/_restore{55024D91-8423-49C
16436	4/2/2012	20:56:29	.A..	Shortcut LNK	C:/Documents and Settings/tdungan/My Documents/Backstopped Accounts - R&D Costs Alloy Research	C:/System Volume Information/_restore{55024D91-8423-49C
16437	4/2/2012	20:56:30	...B	NTFS $MFT	C:/System Volume Information/_restore{55024D91-8423-49CF-94C2-8A45468748EE}/RP279/A0018484.LNK	C:/System Volume Information/_restore{55024D91-8423-49C

Case Study - Phishing Attack

FILE OPENING
WEB HISTORY
DELETED DATA
EXECUTION
USB USAGE
FOLDER OPENING



Email Read

MS Excel Executed w/EXPLOIT

Shortcut File Created

Excel .pf File Modified

Userassist Updated Excel

Poison Ivy Created in System32 or Windows

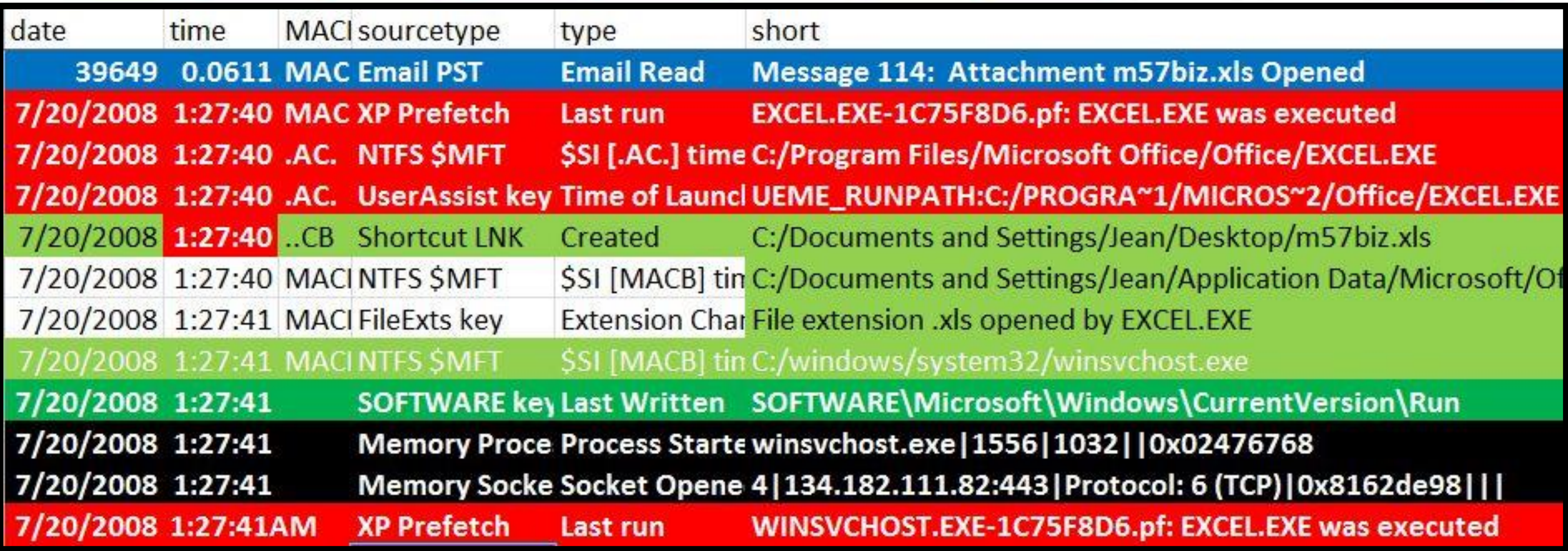
Reg Entries Created

Poison Ivy Executed

Memory Process Started

Memory Socket Created (Tunnel over port 80/443)

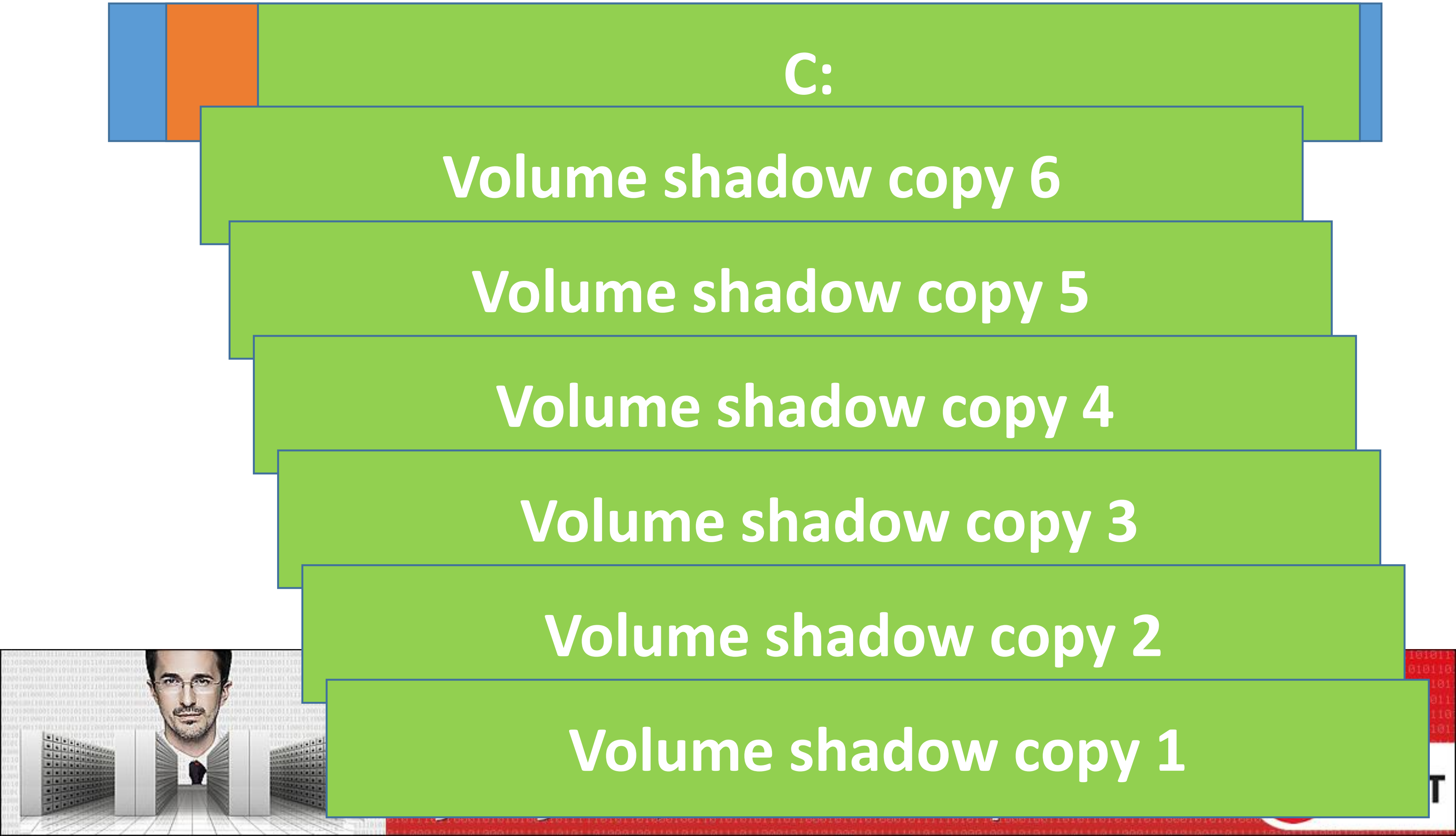
C2 Prefetch Files Created (10 secs after launch)



date	time	MACB	sourcetype	type	short
39649	0.0611	MAC	Email PST	Email Read	Message 114: Attachment m57biz.xls Opened
7/20/2008	1:27:40	MAC	XP Prefetch	Last run	EXCEL.EXE-1C75F8D6.pf: EXCEL.EXE was executed
7/20/2008	1:27:40	.AC.	NTFS $MFT	$SI [.AC.] time	C:/Program Files/Microsoft Office/Office/EXCEL.EXE
7/20/2008	1:27:40	.AC.	UserAssist key	Time of Launcl	UEME_RUNPATH:C:/PROGRA~1/MICROS~2/Office/EXCEL.EXE
7/20/2008	1:27:40	..CB	Shortcut LNK	Created	C:/Documents and Settings/Jean/Desktop/m57biz.xls
7/20/2008	1:27:40	MACI	NTFS $MFT	$SI [MACB] tin	C:/Documents and Settings/Jean/Application Data/Microsoft/Of
7/20/2008	1:27:41	MACI	FileExts key	Extension Char	File extension .xls opened by EXCEL.EXE
7/20/2008	1:27:41	MACI	NTFS $MFT	$SI [MACB] tin	C:/windows/system32/winsvchost.exe
7/20/2008	1:27:41		SOFTWARE key	Last Written	SOFTWARE\Microsoft\Windows\CurrentVersion\Run
7/20/2008	1:27:41		Memory Proce	Process Starte	winsvchost.exe|1556|1032||0x02476768
7/20/2008	1:27:41		Memory Socke	Socket Opene	4|134.182.111.82:443|Protocol: 6 (TCP)|0x8162de98|||
7/20/2008	1:27:41AM		XP Prefetch	Last run	WINSVCHOST.EXE-1C75F8D6.pf: EXCEL.EXE was executed

Picture is never complete, ever…

Volume shadow copy



C:

Volume shadow copy 6

Volume shadow copy 5

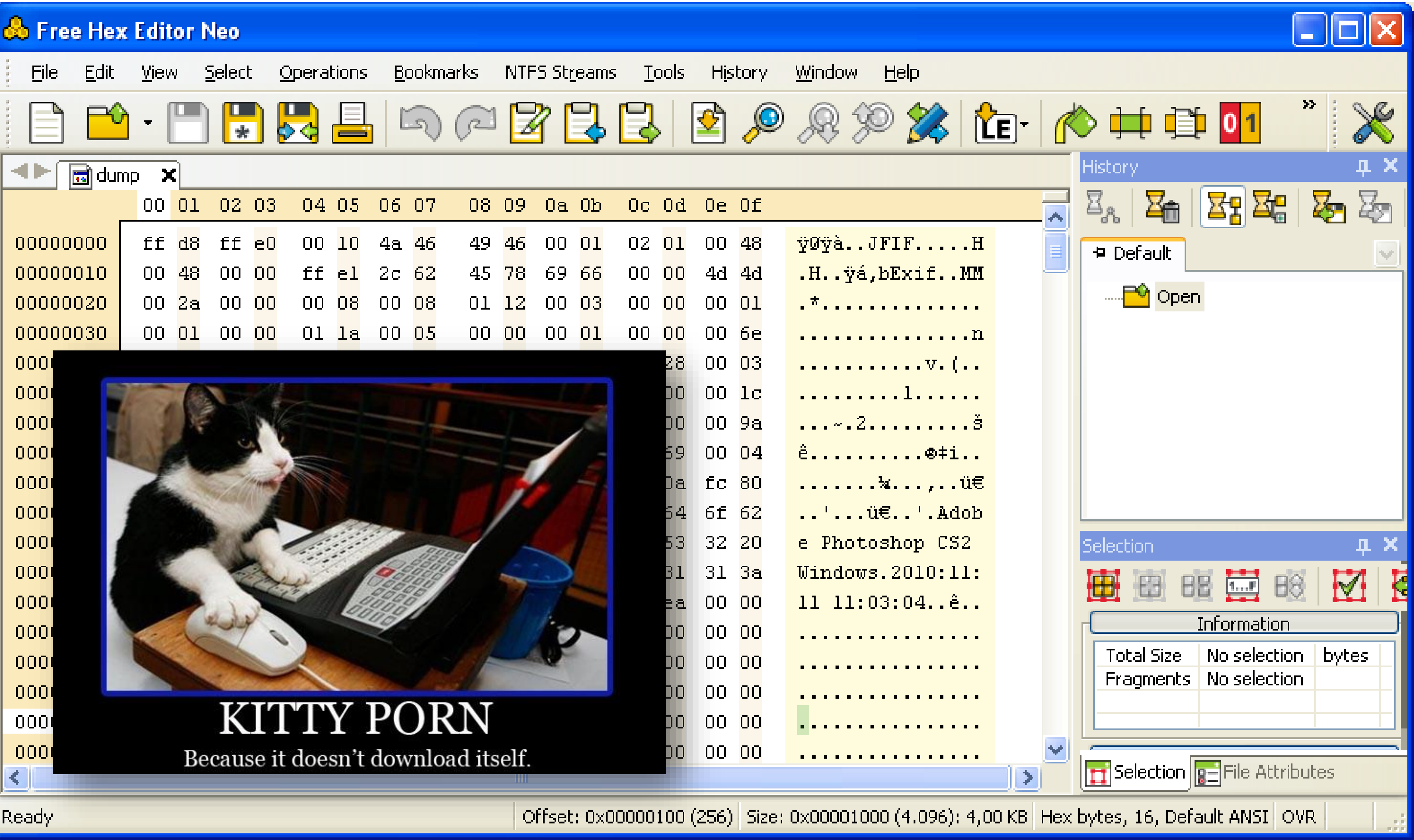
Volume shadow copy 4

Volume shadow copy 3

Volume shadow copy 2

Volume shadow copy 1

Unallocated space



```
           00 01  02 03  04 05  06 07  08 09  0a 0b  0c 0d  0e 0f
00000000   ff d8  ff e0  00 10  4a 46  49 46  00 01  02 01  00 48   ÿØÿà..JFIF.....H
00000010   00 48  00 00  ff e1  2c 62  45 78  69 66  00 00  4d 4d   .H..ÿá,bExif..MM
00000020   00 2a  00 00  00 08  00 08  01 12  00 03  00 00  00 01   .*..............
00000030   00 01  00 00  01 1a  00 05  00 00  00 01  00 00  00 6e   ...............n
000                                               28  00 03   ...........v.(..
000                                               00  00 1c   .........l......
000                                               00  00 9a   ...~.2.........š
000                                               59  00 04   ê..........®‡i..
000                                               0a  fc 80   .......¼...,..ü€
000                                               54  6f 62   ..'...ü€..'.Adob
000                                               53  32 20   e Photoshop CS2
000                                               31  31 3a   Windows.2010:11:
000                                               ea  00 00   11 11:03:04..ê..
000                                               00  00 00   ................
000                                               00  00 00   ................
000                                               00  00 00   ................
000                                               00  00 00   ................
000                                               00  00 00   ................
```

Total Size	No selection	bytes
Fragments	No selection	

Ready | Offset: 0x00000100 (256) | Size: 0x00001000 (4.096): 4,00 KB | Hex bytes, 16, Default ANSI | OVR

Exiftool metadata example

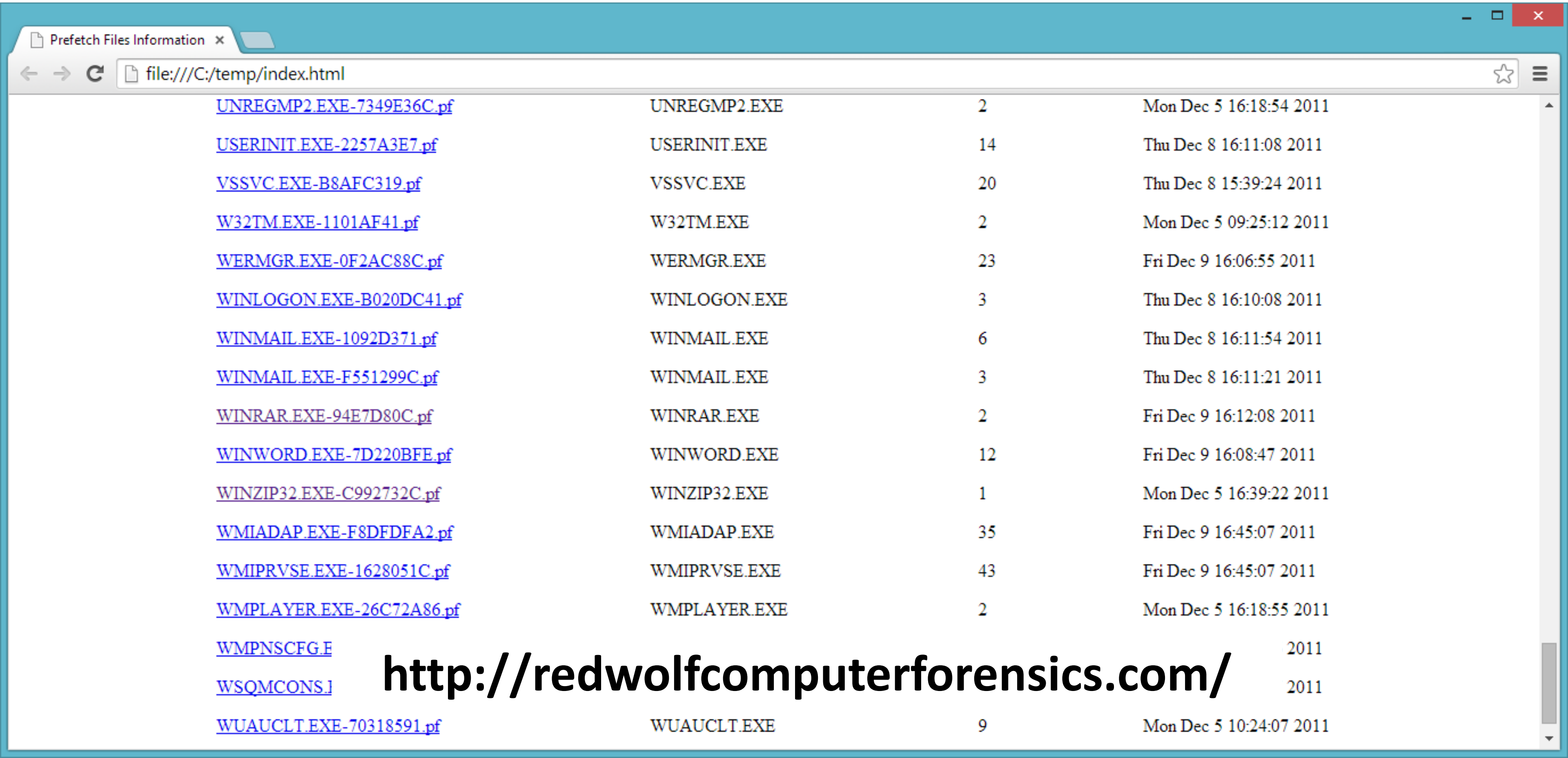
http://www.sno.phy.queensu.ca/~phil/exiftool/

Windows – Prefetch files

- When executing a program Windows automatically generates a prefetch file
  - To further enhance performance
  - Existence proves execution
- Location:
  - C:\Windows\Prefetch\
- Name:
  - [application].[ext]-[hash].pf

Prefetch (2)

- Executables that ran on the system:

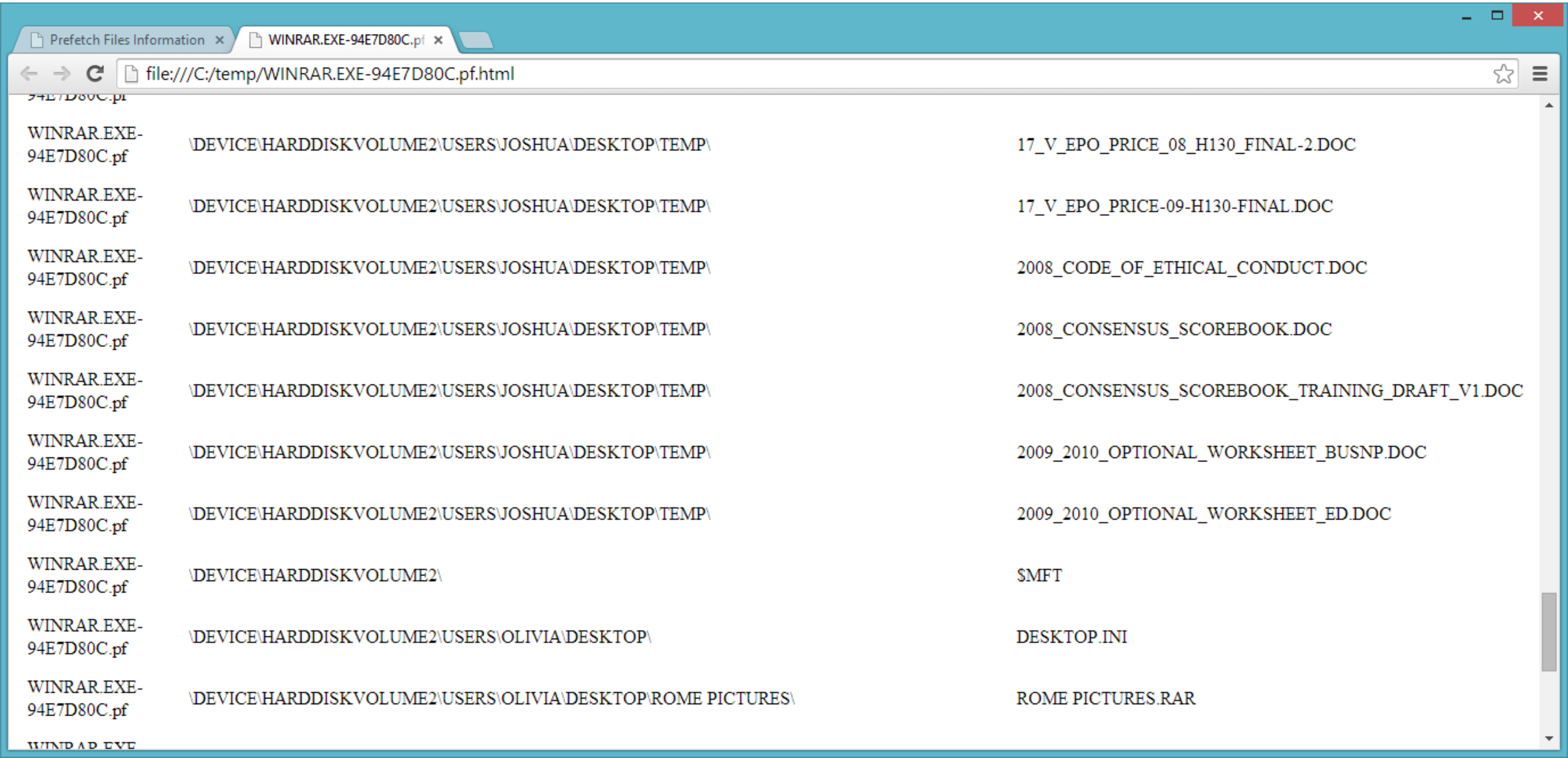


UNREGMP2.EXE-7349E36C.pf	UNREGMP2.EXE	2	Mon Dec 5 16:18:54 2011
USERINIT.EXE-2257A3E7.pf	USERINIT.EXE	14	Thu Dec 8 16:11:08 2011
VSSVC.EXE-B8AFC319.pf	VSSVC.EXE	20	Thu Dec 8 15:39:24 2011
W32TM.EXE-1101AF41.pf	W32TM.EXE	2	Mon Dec 5 09:25:12 2011
WERMGR.EXE-0F2AC88C.pf	WERMGR.EXE	23	Fri Dec 9 16:06:55 2011
WINLOGON.EXE-B020DC41.pf	WINLOGON.EXE	3	Thu Dec 8 16:10:08 2011
WINMAIL.EXE-1092D371.pf	WINMAIL.EXE	6	Thu Dec 8 16:11:54 2011
WINMAIL.EXE-F551299C.pf	WINMAIL.EXE	3	Thu Dec 8 16:11:21 2011
WINRAR.EXE-94E7D80C.pf	WINRAR.EXE	2	Fri Dec 9 16:12:08 2011
WINWORD.EXE-7D220BFE.pf	WINWORD.EXE	12	Fri Dec 9 16:08:47 2011
WINZIP32.EXE-C992732C.pf	WINZIP32.EXE	1	Mon Dec 5 16:39:22 2011
WMIADAP.EXE-F8DFDFA2.pf	WMIADAP.EXE	35	Fri Dec 9 16:45:07 2011
WMIPRVSE.EXE-1628051C.pf	WMIPRVSE.EXE	43	Fri Dec 9 16:45:07 2011
WMPLAYER.EXE-26C72A86.pf	WMPLAYER.EXE	2	Mon Dec 5 16:18:55 2011
WMPNSCFG.E			2011
WSQMCONS.I			2011
WUAUCLT.EXE-70318591.pf	WUAUCLT.EXE	9	Mon Dec 5 10:24:07 2011

http://redwolfcomputerforensics.com/

Prefetch (3)

- Files associated with the execution of WINRAR.EXE:


Prefetch Files Information
WINRAR.EXE-94E7D80C.pf
file:///C:/temp/WINRAR.EXE-94E7D80C.pf.html

94E7D80C.pf		
WINRAR.EXE-94E7D80C.pf	\DEVICE\HARDDISKVOLUME2\USERS\JOSHUA\DESKTOP\TEMP\	17_V_EPO_PRICE_08_H130_FINAL-2.DOC
WINRAR.EXE-94E7D80C.pf	\DEVICE\HARDDISKVOLUME2\USERS\JOSHUA\DESKTOP\TEMP\	17_V_EPO_PRICE-09-H130-FINAL.DOC
WINRAR.EXE-94E7D80C.pf	\DEVICE\HARDDISKVOLUME2\USERS\JOSHUA\DESKTOP\TEMP\	2008_CODE_OF_ETHICAL_CONDUCT.DOC
WINRAR.EXE-94E7D80C.pf	\DEVICE\HARDDISKVOLUME2\USERS\JOSHUA\DESKTOP\TEMP\	2008_CONSENSUS_SCOREBOOK.DOC
WINRAR.EXE-94E7D80C.pf	\DEVICE\HARDDISKVOLUME2\USERS\JOSHUA\DESKTOP\TEMP\	2008_CONSENSUS_SCOREBOOK_TRAINING_DRAFT_V1.DOC
WINRAR.EXE-94E7D80C.pf	\DEVICE\HARDDISKVOLUME2\USERS\JOSHUA\DESKTOP\TEMP\	2009_2010_OPTIONAL_WORKSHEET_BUSNP.DOC
WINRAR.EXE-94E7D80C.pf	\DEVICE\HARDDISKVOLUME2\USERS\JOSHUA\DESKTOP\TEMP\	2009_2010_OPTIONAL_WORKSHEET_ED.DOC
WINRAR.EXE-94E7D80C.pf	\DEVICE\HARDDISKVOLUME2\	$MFT
WINRAR.EXE-94E7D80C.pf	\DEVICE\HARDDISKVOLUME2\USERS\OLIVIA\DESKTOP\	DESKTOP.INI
WINRAR.EXE-94E7D80C.pf	\DEVICE\HARDDISKVOLUME2\USERS\OLIVIA\DESKTOP\ROME PICTURES\	ROME PICTURES.RAR
WINRAR.EXE		

Analyze recovered prefetch

- Foremost signature for carving PF files:

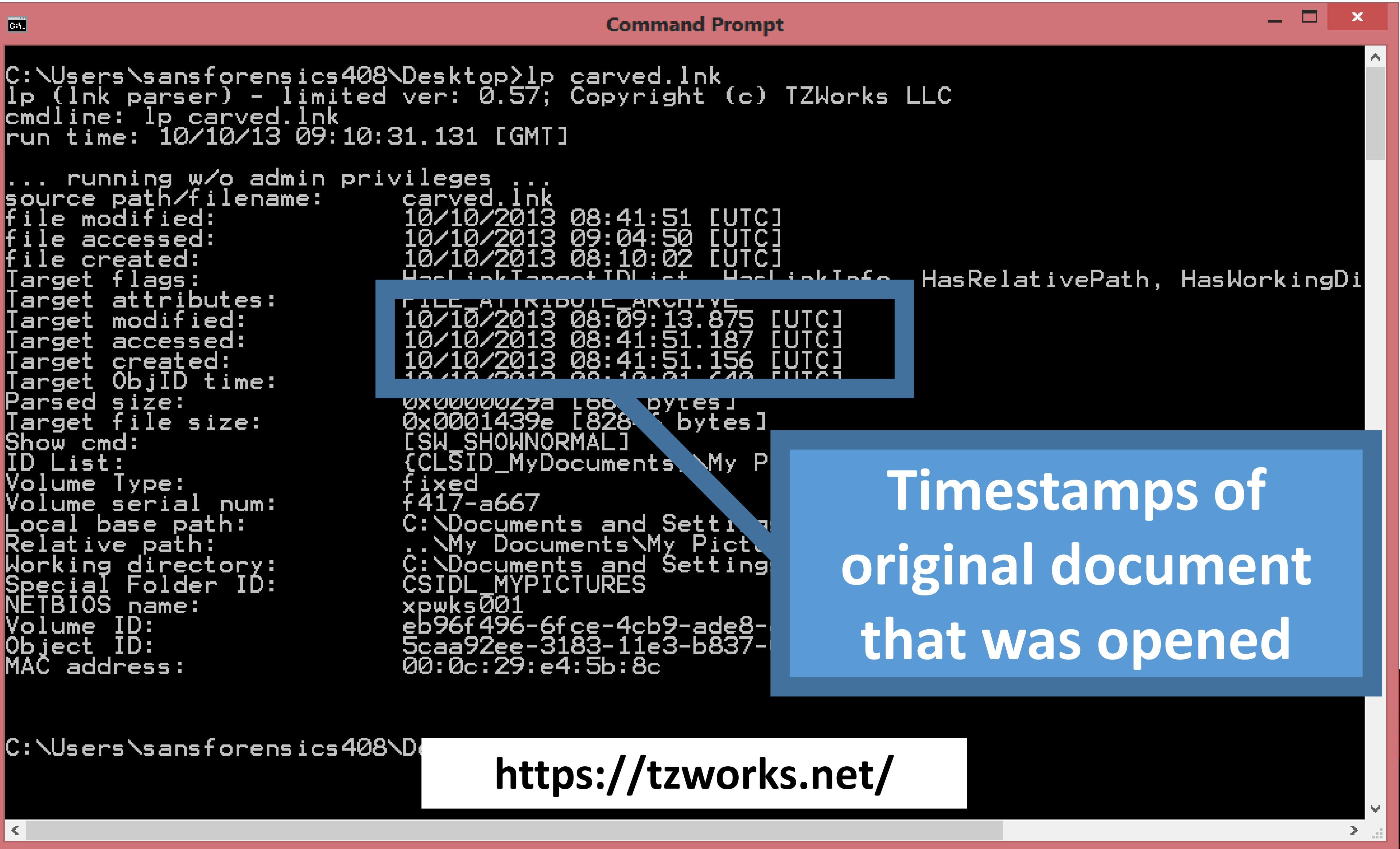
```
pf    y   80000   ?\x00\x00\x00\x53\x43\x43\x41
```

- Use pf to parse recovered files:

```
pf -v recovered_file.pf
```

- **Use Foremost or Photorec**

Carved LNK file



```
C:\Users\sansforensics408\Desktop>lp carved.lnk
lp (lnk parser) - limited ver: 0.57; Copyright (c) TZWorks LLC
cmdline:  lp carved.lnk
run time:  10/10/13 09:10:31.131 [GMT]

... running w/o admin privileges ...
source path/filename:       carved.lnk
file modified:              10/10/2013 08:41:51 [UTC]
file accessed:              10/10/2013 09:04:50 [UTC]
file created:               10/10/2013 08:10:02 [UTC]
Target flags:               HasLinkTargetIDList, HasLinkInfo, HasRelativePath, HasWorkingDi
Target attributes:          FILE_ATTRIBUTE_ARCHIVE
Target modified:            10/10/2013 08:09:13.875 [UTC]
Target accessed:            10/10/2013 08:41:51.187 [UTC]
Target created:             10/10/2013 08:41:51.156 [UTC]
Target ObjID time:          10/10/2013 08:10:01.640 [UTC]
Parsed size:                0x0000029a [666 bytes]
Target file size:           0x0001439e [82846 bytes]
Show cmd:                   [SW_SHOWNORMAL]
ID List:                    {CLSID_MyDocuments}\My P
Volume Type:                fixed
Volume serial num:          f417-a667
Local base path:            C:\Documents and Setti
Relative path:              ..\My Documents\My Pict
Working directory:          C:\Documents and Setting
Special Folder ID:          CSIDL_MYPICTURES
NETBIOS name:               xpwks001
Volume ID:                  eb96f496-6fce-4cb9-ade8-
Object ID:                  5caa92ee-3183-11e3-b837-
MAC address:                00:0c:29:e4:5b:8c


C:\Users\sansforensics408\D
```

Timestamps of original document that was opened

https://tzworks.net/

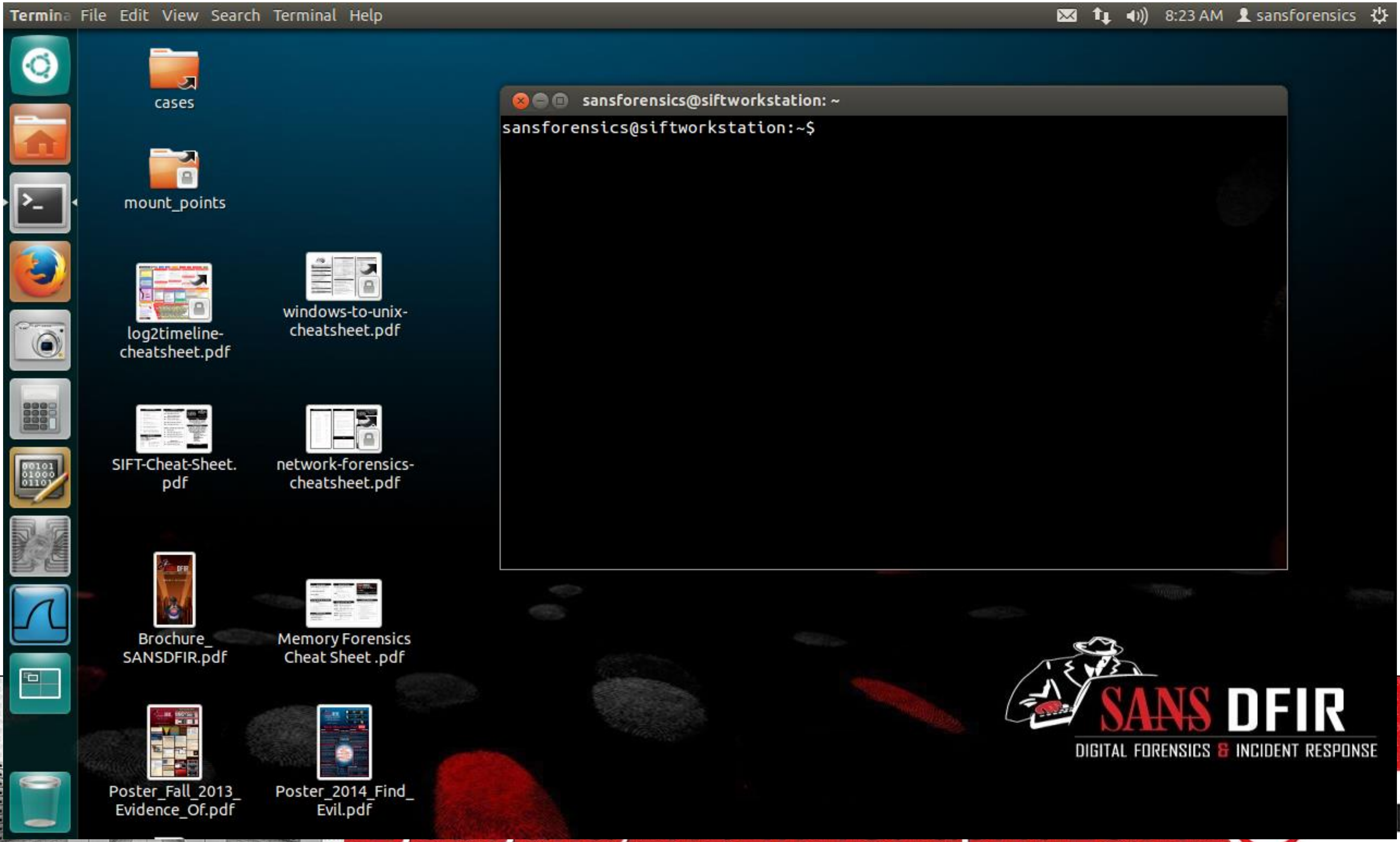
Volatility: timeliner plugin

- Many memory artifacts have embedded timestamps:
  - Processes, threads
  - Portable Executable Files
    - Process EXEs, DLLs, and Drivers
  - Network Sockets, Registry Keys, Event Logs

- Timeliner consolidates artifacts into delimited file that can be easily converted to a timeline

https://code.google.com/p/volatility/

SANS SIFT Workstation

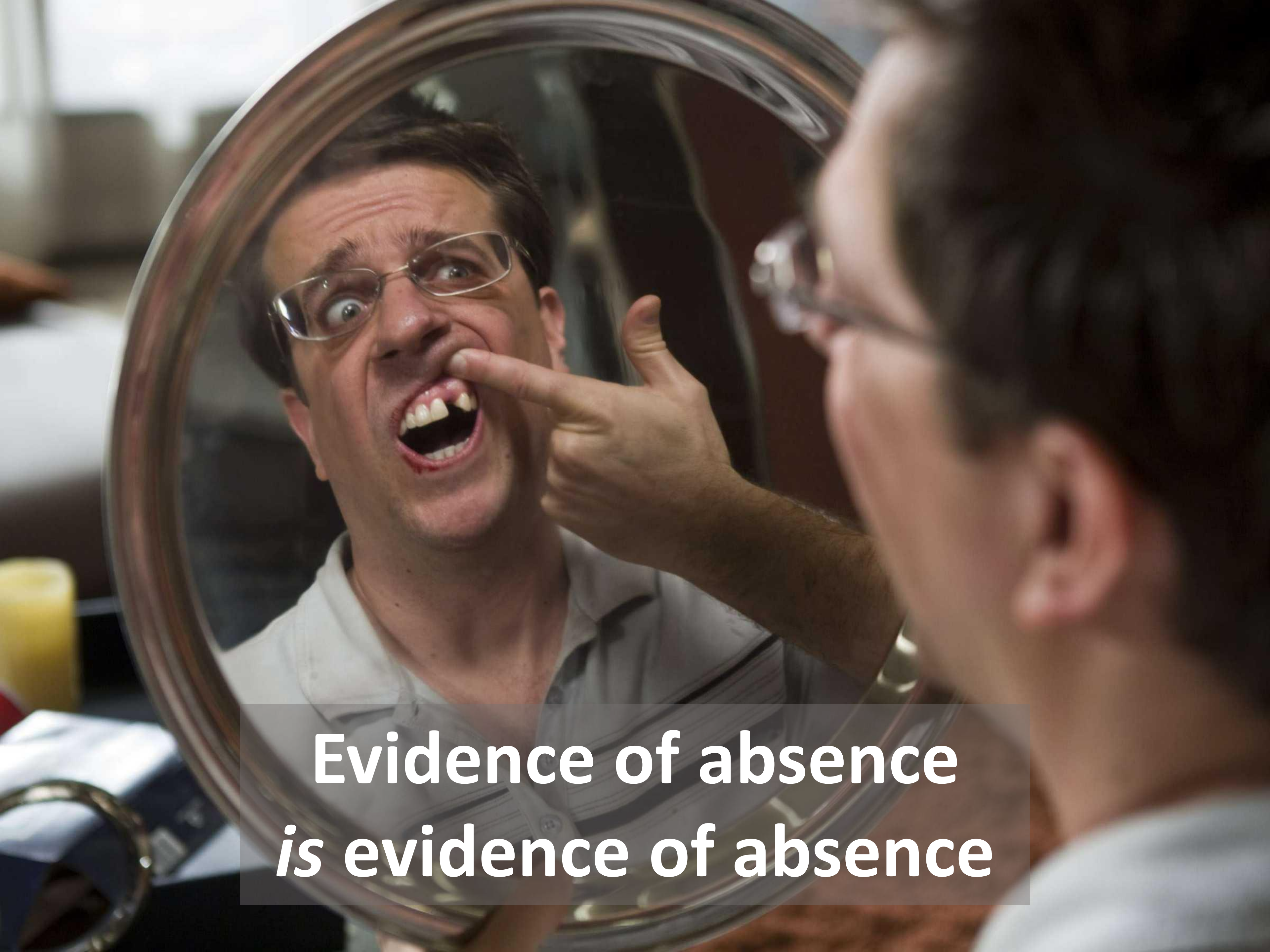


Terminal File Edit View Search Terminal Help
8:23 AM
sansforensics
cases
mount_points
log2timeline-cheatsheet.pdf
windows-to-unix-cheatsheet.pdf
SIFT-Cheat-Sheet.pdf
network-forensics-cheatsheet.pdf
Brochure_SANSDFIR.pdf
Memory Forensics Cheat Sheet .pdf
Poster_Fall_2013_Evidence_Of.pdf
Poster_2014_Find_Evil.pdf
sansforensics@siftworkstation: ~
SANS DFIR
DIGITAL FORENSICS & INCIDENT RESPONSE

```
sansforensics@siftworkstation:~$
```

Absence of evidence
isn’t evidence of absence

- Carl Sagan



Evidence of absence
is evidence of absence

Test your hypotheses

Final thoughts

- You are looking at the **result** of certain activity, not at the activity itself
- There might be an alternative scenario that produces that specific pattern

FOX IT

Christian Prickaerts

prickaerts@fox-it.com