



Time Line Analysis

Using Free & Open Source Tools

Let's go back in time...

```
Oct 03 2000 16:01:30      484 .a. -rw----- root      root      /etc/ftpaccess
                        153488 .a. -rwxr-xr-x root      root      /usr/sbin/in.ftpd
Oct 03 2000 16:01:33      456 .a. -rw----- root      root      /etc/ftpconversions
Oct 03 2000 16:01:34      104 .a. -rw----- root      root      /etc/ftphosts
                        79 .a. -rw----- root      root      /etc/ftpusers
                        4096 mac -rw-r--r-- root      root      /var/run/ftp.pids-
all
Oct 03 2000 16:01:54     42736 .a. -rwxr-xr-x root      root      /sbin/ifconfig
                        11868 .a. -rwxr-xr-x root      root      /usr/bin/cut
Oct 03 2000 16:01:55      3070 m.c -rw-r--r-- root      root      /etc/inetd.conf
                        10160 .a. -rwxr-xr-x root      root      /usr/bin/killall
                        8860 .a. -r-xr-xr-x root      root      /usr/bin/w
Oct 03 2000 16:20:37     20452 m.c -rwxr-xr-x root      root      /bin/systat
```

... state of the art circa 2000

```
Oct 03 2000 16:20:53 166416 .a. -rwxr-xr-x root    root    /usr/bin/pico
                    1143 .a. -rw-r--r-- root    root    /usr/share/terminfo/v/vt100
                    1143 .a. -rw-r--r-- root    root    /usr/share/terminfo/v/vt100-am
Oct 03 2000 16:21:04 63376  .a. -rwxr-xr-x root    root    /usr/bin/egcs
                    63376 .a. -rwxr-xr-x root    root    /usr/bin/gcc
Oct 03 2000 16:21:05 207600 .a. -rwxr-xr-x root    root    /usr/bin/as
                    2315 .a. -rw-r--r-- root    root    /usr/include/_G_config.h
                    1297 .a. -rw-r--r-- root    root    /usr/include/bits/stdio_lim.h
                    4680 .a. -rw-r--r-- root    root    /usr/include/bits/types.h
                    9512 .a. -rw-r--r-- root    root    /usr/include/features.h
                    1021 .a. -rw-r--r-- root    root    /usr/include/gnu/stubs.h
                    11673 .a. -rw-r--r-- root    root    /usr/include/libio.h
                    20926 .a. -rw-r--r-- root    root    /usr/include/stdio.h
                    4951 .a. -rw-r--r-- root    root    /usr/include/sys/cdefs.h
```

The background of the slide is a screenshot of an Ubuntu desktop environment. At the top, there is a taskbar with various application icons including Firefox, LibreOffice, and a terminal. The desktop has several icons on the left side, including a monitor icon labeled 'SIFTWORKSTATION', a folder icon, and a PDF file icon labeled 'SIFT Workstation Cheat Sheet 1.5.pdf'. In the center, a terminal window titled 'sansforensics@SIFT-Workstation: ~' is open, showing a command prompt 'sansforensics@SIFT-Workstation:~\$'.

SANS Investigative Forensics Toolkit

- <http://computer-forensics.sans.org/community>
- Linux virtual machine (VMWare)
- Dozens of FOSS forensics tools
- Enables “hybrid” investigations



HolisticInfoSec.org



Monday, January 31, 2011

2010 Toolsmith Tool of the Year: SIFT 2.0

As voted by you, the readers, the 2010 [Toolsmith](#) Tool of the Year is [SIFT 2.0](#). The SANS Investigative Forensic Toolkit (SIFT) Workstation Version 2.0, as discussed in May's ISSA Journal, is a Linux distribution that is preconfigured for forensic investigations. Created by Rob Lee for the [SANS 508 track](#), SIFT 2.0 includes all the tools a forensic analyst/incident responder would require to conduct a thorough system investigation. I particularly favor it for memory analysis - grab a memory image from your victim system; pull it back to your SIFT VM and get down to business in no time flat.

Of 76 votes, SIFT 2.0 came in first with 24 votes (31.6%).

Rounding out the top five:


- 2) [Firefox Addons for Security Practitioners](#) with 20 votes (26.3%)
- 3) [SamuraiWTF](#) with 18 votes (23.7%)
- 4) [NetWitness Investigator](#) with 12 votes (15.8%)
- 5) [Confessor and MOLE](#) with 8 votes (10.5%)




Disclaimer

The views expressed here are mine alone unless clearly cited as those of others.

HolisticInfoSec.org needs your help choosing the 2010 [Toolsmith](#) Tool of the Year. We covered a lot of excellent information security-related tools in 2010; which one did you believe was the best? We appreciate you taking the time to make your choice [here](#).

 [Subscribe](#)

 [Follow](#)

with Google Friend Connect

Followers (30) [More »](#)



SIFT Workstation 2.0 Capabilities

Ability to securely examine raw disks, multiple file systems, evidence formats. Places strict guidelines on how evidence is examined (read-only) verifying that the evidence has not changed

File system support

- Windows (MSDOS, FAT, VFAT, NTFS)
- MAC (HFS)
- Solaris (UFS)
- Linux (EXT2/3)

Evidence Image Support

- Expert Witness (E01)
- RAW (dd)
- Advanced Forensic Format (AFF)

Software Includes

- The Sleuth Kit (File system Analysis Tools)
- log2timeline (Timeline Generation Tool)
- ssdeep & md5deep (Hashing Tools)
- Foremost/Scalpel (File Carving)
- WireShark (Network Forensics)
- Vinetto (thumbs.db examination)
- Pasco (IE Web History examination)
- Rifiuti (Recycle Bin examination)
- Volatility Framework (Memory Analysis)
- DFLabs PTK (GUI Front-End for Sleuthkit)
- Autopsy (GUI Front-End for Sleuthkit)
- PyFLAG (GUI Log/Disk Examination)

Key Directories in SANS SIFT Workstation



THE OLD SCHOOL

M is for Modification



Photo By Nick Ares



A is for Access



C is for Metadata Change



B is for Born



File System Time Lines

🔍 Brian Carrier's The Sleuthkit

- fls
- mactime

fls

🔍 Creates a “bodyfile”

```
0|C:$AttrDef|4-128-4|r/rr-xr-xr-x|48|0|2560|1296631049|1296631049|1296631049|1296631049
0|C:$BadClus|8-128-2|r/rr-xr-xr-x|0|0|0|1296631049|1296631049|1296631049|1296631049
0|C:$Bitmap|6-128-4|r/rr-xr-xr-x|0|0|1310656|1296631049|1296631049|1296631049|1296631049
0|C:$Boot|7-128-1|r/rr-xr-xr-x|48|0|8192|1296631049|1296631049|1296631049|1296631049
0|C:$Extend|11-144-4|d/dr-xr-xr-x|0|0|552|1296631049|1296631049|1296631049|1296631049
...
```

```
fls -r -m mount_point -r -z time_zone -s clock_skew image > output_file
```

Can't remember the syntax? Run the command.

mactime

- 🔍 Takes a bodyfile and makes it legible
 - Like the first two slides in this presentation

```
mactime -b bodyfile -d -y -m -z time_zone > output_file
```

Can't remember the syntax? Run the command!



Muhahaha, I haz timestomp!

regwin.exe?

Date	Size	Type	Meta	File Name
2008 04 14 Mon 07:00:00	115713	m..b	18851-128-3	C/WINDOWS/regwin.exe
2010 10 23 Sat 14:32:21	115713	.a..	18851-128-3	C/WINDOWS/regwin.exe
2010 10 29 Fri 22:12:33	115713	..c.	18851-128-3	C/WINDOWS/regwin.exe
2010 10 29 Fri 22:36:12	73802	m..b	18803-128-4	C/Documents and Settings/Administrator/My Documents/kids_games.exe
2010 10 29 Fri 22:36:23	73802	.ac.	18803-128-4	C/Documents and Settings/Administrator/My Documents/kids_games.exe
2010 10 29 Fri 22:36:33	10732	macb	18804-128-4	C/WINDOWS/Prefetch/KIDS_GAMES.EXE-28036ABA.pf
2010 10 29 Fri 22:41:36	13624	macb	18856-128-4	C/WINDOWS/Prefetch/REGWIN.EXE-30A6EFE7.pf

NTFS gets complicated

- 🔑 Time is recorded in two places
 - \$STANDARD_INFORMATION Attribute
 - \$FILE_NAME_INFORMATION Attribute

- 🔑 Credit Rob Lee of SANS & Mandiant for his research into NTFS time stamps

\$STDINFO

	Rename	Local Move	Volume Move	Copy	Access	Modify	Create	Delete
M						X	X	
A			X	X	X Not Vista Not Win7	X	X	
C	X	X	X	X			X	X
B				X			X	

\$Filename

	Rename	Local Move	Volume Move	Copy	Access	Modify	Create	Delete
M		X	X	X			X	X
A			X	X			X	
C		X	X	X			X	X
B			X	X			X	

\$Filename times

Date	Size	Type	Meta	File Name
2008 04 14 Mon 07:00:00	115713	m..b	18851-128-3	C:/WINDOWS/regwin.exe
2010 10 23 Sat 14:32:21	115713	.a..	18851-128-3	C:/WINDOWS/regwin.exe
2010 10 29 Fri 22:12:33	115713	..c.	18851-128-3	C:/WINDOWS/regwin.exe
2010 10 29 Fri 22:36:12	0	macb	18803	C:FN/Documents and Settings/Administrator/My Documents/kids_games.exe
2010 10 29 Fri 22:36:12	73802	m..b	18803-128-4	C/Documents and Settings/Administrator/My Documents/kids_games.exe
2010 10 29 Fri 22:36:23	73802	.ac.	18803-128-4	C/Documents and Settings/Administrator/My Documents/kids_games.exe
2010 10 29 Fri 22:36:33	0	macb	18804	C:FN/WINDOWS/Prefetch/KIDS_GAMES.EXE-28036ABA.pf
2010 10 29 Fri 22:36:33	10732	macb	18804-128-4	C/WINDOWS/Prefetch/KIDS_GAMES.EXE-28036ABA.pf
2010 10 29 Fri 22:41:17	0	macb	18851	C:FN/WINDOWS/regwin.exe
2010 10 29 Fri 22:41:36	0	macb	18856	C:FN/WINDOWS/Prefetch/REGWIN.EXE-30A6EFE7.pf
2010 10 29 Fri 22:41:36	13624	macb	18856-128-4	C/WINDOWS/Prefetch/REGWIN.EXE-30A6EFE7.pf

Mark McKinnon's MFT Parser

🔍 Windows

- <http://j.mp/jq129c>

🔍 Linux

- <http://j.mp/m4Q2er>

🔍 Mac

- <http://j.mp/iRKR8t>

Timestomp clones

Date	Size	Type	Meta	File Name
2008 04 14 Mon 07:00:00	115713	m..b	18851-128-3	C/WINDOWS/regwin.exe
2008 04 14 Mon 07:00:00	146432	m..b	2114-128-3	C/WINDOWS/regedit.exe
2010 10 23 Sat 14:32:21	115713	.a..	18851-128-3	C/WINDOWS/regwin.exe
2010 10 23 Sat 14:32:21	146432	.a..	2114-128-3	C/WINDOWS/regedit.exe
2010 10 29 Fri 22:12:33	115713	..c.	18851-128-3	C/WINDOWS/regwin.exe
2010 10 29 Fri 22:12:33	146432	..c.	2114-128-3	C/WINDOWS/regedit.exe



But Wait...
**THERE'S
MORE!**

*Tighten Your Abs, Make Millions,
and Learn How the \$100 Billion Infomercial
Industry Sold Us Everything but the Kitchen Sink*



"A wholly fascinating
account of a wholly
fascinating industry."
—Robert B. Cialdini,
bestselling author of *Influence:
Science and Practice*



Circa 2008

🔍 “The Windows Registry is a log file.”

– Harlan Carvey author of Windows Forensic Analysis and Windows Registry Forensics

- Regtime.pl can pull Registry “last write” times and put them in “bodyfile” format.

Registry Times

Date	Type	File Name
2010 10 29 Fri 22:36:12	m...	NTUSER/Software/Microsoft/Internet Explorer
2010 10 29 Fri 22:36:12	m...	NTUSER/Software/Microsoft/Windows/CurrentVersion/Explorer
2010 10 29 Fri 22:36:12	m...	NTUSER/Software/Microsoft/Windows/CurrentVersion/Explorer/ComDlg32
2010 10 29 Fri 22:36:12	m...	NTUSER/Software/Microsoft/Windows/CurrentVersion/Explorer/ComDlg32/LastVisitedMRU
2010 10 29 Fri 22:36:12	m...	NTUSER/Software/Microsoft/Windows/CurrentVersion/Explorer/ComDlg32/OpenSaveMRU
2010 10 29 Fri 22:36:12	m...	NTUSER/Software/Microsoft/Windows/CurrentVersion/Explorer/ComDlg32/OpenSaveMRU/*
2010 10 29 Fri 22:36:12	m...	NTUSER/Software/Microsoft/Windows/CurrentVersion/Explorer/ComDlg32/OpenSaveMRU/exe
2010 10 29 Fri 22:36:12	m...	C/Documents and Settings/Administrator/My Documents
2010 10 29 Fri 22:36:12	.a..	C/Documents and Settings/Administrator/Local Settings/Temporary Internet Files/Content.IE5/IBWFEF2T



But Wait...
**THERE'S
MORE!**

**Tighten Your Abs, Make Millions,
and Learn How the \$100 Billion Infomercial
Industry Sold Us Everything but the Kitchen Sink**



"A wholly fascinating
account of a wholly
fascinating industry."
—**Robert B. Cialdini**,
bestselling author of *Influence:
Science and Practice*



More time stamps

- 🔑 Windows Event logs
- 🔑 EXIF metadata
- 🔑 Browser history & other artifacts
- 🔑 Anti-virus logs
- 🔑 PCAP files
- 🔑 PDF files
- 🔑 Windows Prefetch files
- 🔑 Windows Recycle Bin
- 🔑 Restore Points
- 🔑 Volume Shadows
- 🔑 Windows SetupAPI.log
- 🔑 Memory dumps
- 🔑 Windows Shortcuts
- 🔑 ...

How to collect them all?

Mastering the Super Timeline With log2timeline

GIAC (GCFA) Gold Certification

Author: Kristinn Guðjónsson, kristinn@log2timeline.net

Advisor: Charles Hornat

Accepted: June 29, 2010

Abstract

Traditional timeline analysis can be extremely useful yet it sometimes misses important events that are stored inside files or OS artifacts on the suspect. By solely depending on traditional filesystem timeline the investigator misses context that is necessary to get a complete and accurate description of the events that took place. To achieve this goal of enlightenment we need to dig deeper and incorporate information found inside artifacts

Super time line

Date	Type	Meta	File Name
2008 04 14 Mon 07:00:00	m..b	18851-128-3	C:/WINDOWS/regwin.exe
2010 10 23 Sat 14:32:21	.a..	18851-128-3	C:/WINDOWS/regwin.exe
2010 10 29 Fri 22:12:33	..c.	18851-128-3	C:/WINDOWS/regwin.exe
2010 10 29 Fri 22:36:12	macb	18803	C:/FN/Documents and Settings/Administrator/My Documents/kids_games.exe
2010 10 29 Fri 22:36:12	m..b	18803-128-4	C:/Documents and Settings/Administrator/My Documents/kids_games.exe
2010 10 29 Fri 22:36:23	.ac.	18803-128-4	C:/Documents and Settings/Administrator/My Documents/kids_games.exe
2010 10 29 Fri 22:36:23	macb	9644	[Prefetch] KIDS_GAMES.EXE-28036ABA.pf - [KIDS_GAMES.EXE] was executed - run count [1]
2010 10 29 Fri 22:36:33	macb	18804	C:/FN/WINDOWS/Prefetch/KIDS_GAMES.EXE-28036ABA.pf
2010 10 29 Fri 22:36:33	macb	18804-128-4	C:/WINDOWS/Prefetch/KIDS_GAMES.EXE-28036ABA.pf
2010 10 29 Fri 22:41:17	macb	18851	C:/FN/WINDOWS/regwin.exe
2010 10 29 Fri 22:41:26	macb	9618	[Prefetch] REGWIN.EXE-30A6EFE7.pf - [REGWIN.EXE] was executed - run count [1]
2010 10 29 Fri 22:41:36	macb	18856	C:/FN/WINDOWS/Prefetch/REGWIN.EXE-30A6EFE7.pf
2010 10 29 Fri 22:41:36	macb	18856-128-4	C:/WINDOWS/Prefetch/REGWIN.EXE-30A6EFE7.pf

Conclusions

- 🔍 Timestomp upped the attacker's game
- 🔍 We can do better...
 - Mark McKinnon's MFT Parser
 - David Kovar's analyzeMFT.py
 - Harlan Carvey's Regtime
 - Kristinn Gudjonsson Log2Timeline

Questions

Additional reading:

computer-forensics.sans.org/blog

Contact:

davehull@trustedsignal.com