

SuperTimeline+Splunk



dorumugs

<http://malware.co.kr>

And yet it does move



1. SIFT(SANS Investigate Forensic Toolkit)
2. Install Splunk
3. Create Timeline
4. Splunk + SuperTimeline

SIFT

(SANS Investigate Forensic Toolkit)

- SIFT?
- SIFT Download
- SIFT Information



SIFT?

- SIFT is Toolkit for forensic investigator.
- It has a lot of tools about forensics like dd, sleuthkit, autopsy and so on.
- SANS supports this OS for free.





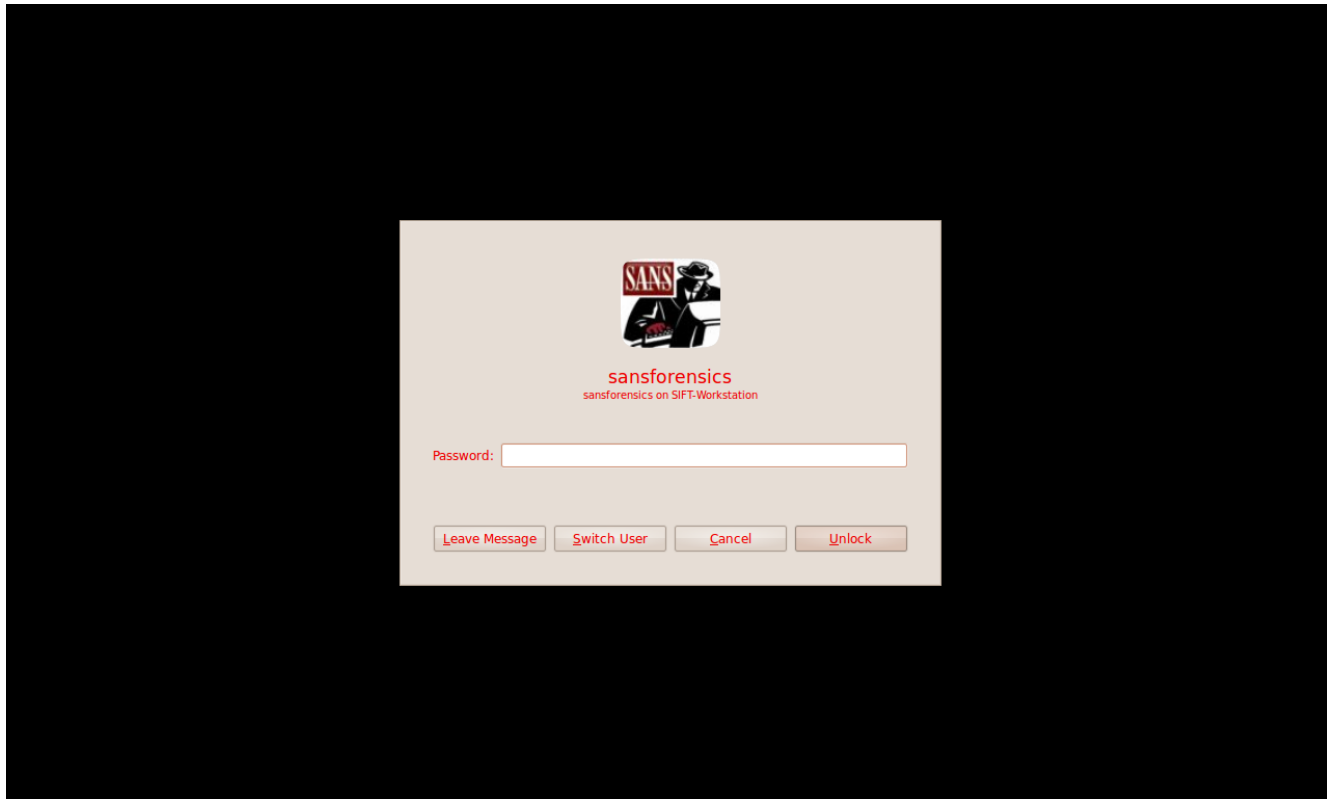
SIFT Download

- URL : <http://computer-forensics.sans.org/community/downloads#over>
- You can download a couple of SIFT version.
 - VMware
 - ✓ <https://computer-forensics12.sans.org/community/download-sift-kit/2.1>
 - ISO
 - ✓ <https://computer-forensics12.sans.org/community/download-sift-kit/2.1/iso>
- Password
 - SIFT Default Password : sansforensics / forensics
 - PTK Default Password : admin / forensics



SIFT Download

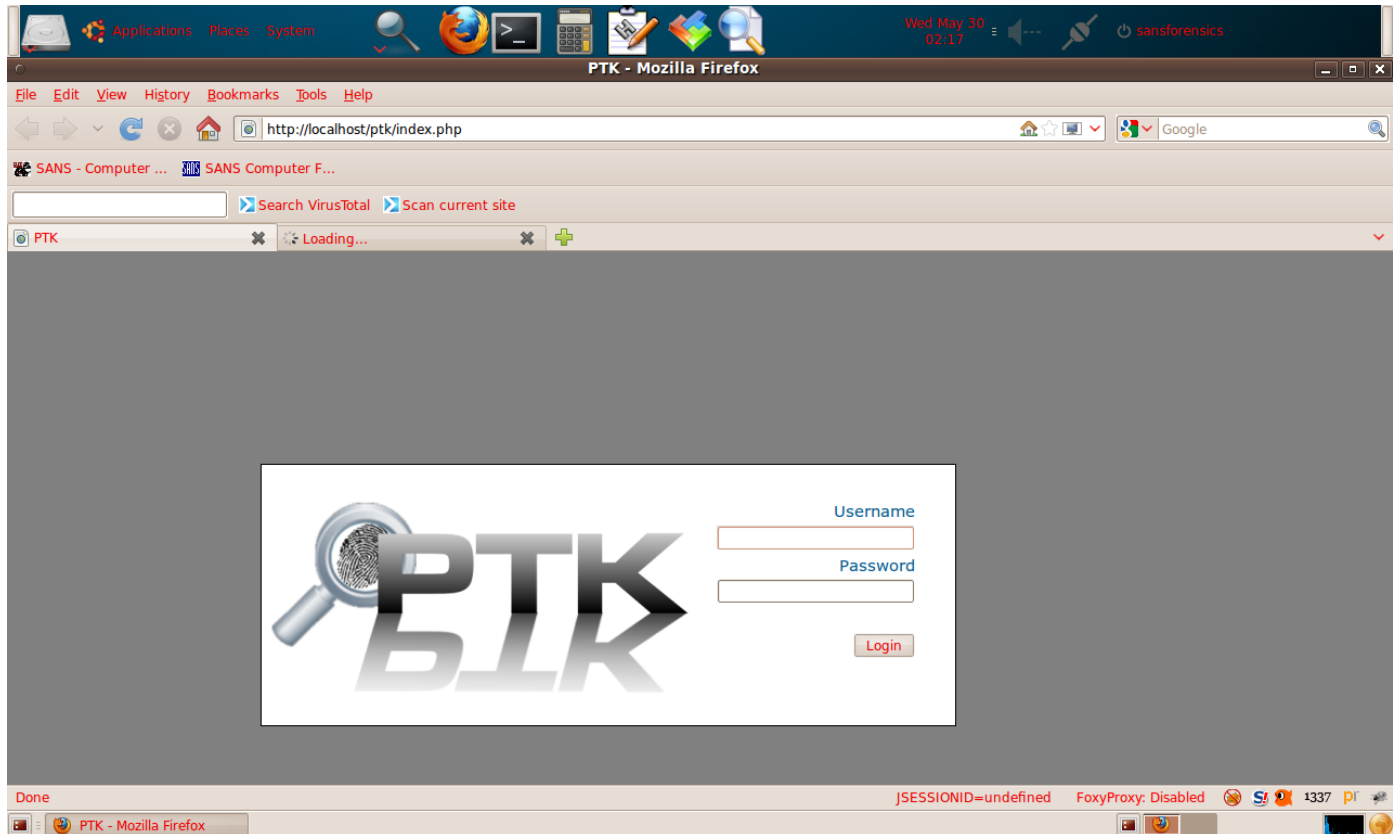
- SIFT Default Password : sansforensics / forensics





SIFT Download

- PTK Default Password : admin / forensics





SIFT Information

▪ SIFT Layout

- `/forensics`
 - ✓ Location of the files used for the Autopsy Toolset.
- `/usr/local/src`
 - ✓ Source files for autopsy, The Sleuthkit, and other tools.
- `/usr/local/bin`
 - ✓ Location of the forensic pre-compiled binaries.
- `/cases`
 - ✓ Location of the images that were seized from your compromised system.
- `/mnt`
 - ✓ Location of the mount points for the file system images.



SIFT Information

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

- **Evidence Image Support**
 - Expert Witness (EO1)
 - RAW (dd)
 - Advanced Forensic Format (AFF)



SIFT Information

▪ 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)
- 100s more tools -> See Detailed Tool Listing



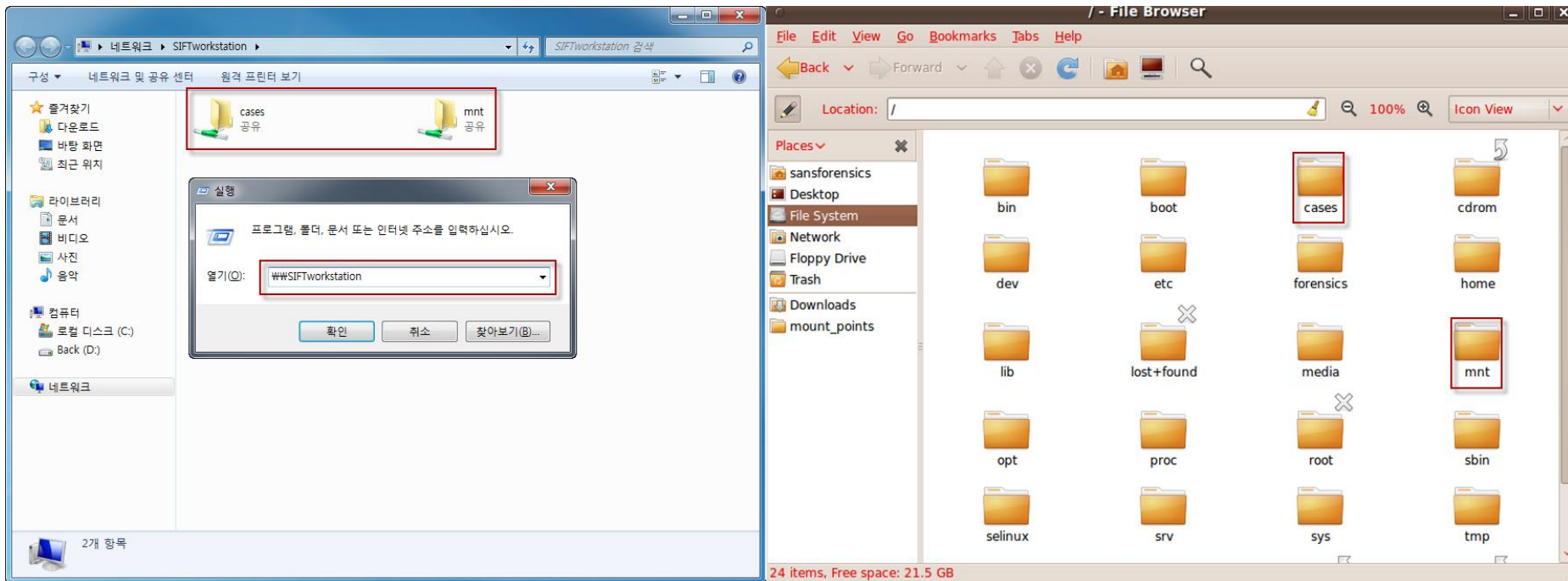
SIFT Information

- **New in SIFT 2.13**
 - iPhone, Blackberry, and Android Forensic Capabilities
 - Registry Viewer (YARU)
 - Compatibility with F-Response Tactical, Standard, and Enterprise
 - PTK 2.0 (Special Release - Not Available for Download)
 - Automated Timeline Generation via log2timeline
 - Many Firefox Investigative Plugins
 - Windows Journal Parser and Shellbags Parser (jp and sbag)
 - Many Windows Analysis Utilities (prefetch, usbstor, event log, and more)
 - Complete Overhaul of Regripper Plugins (added over 80 additional plugins)



SIFT Information

- SIFT shares folder
 - `\\WSIFTWORKSTATION`



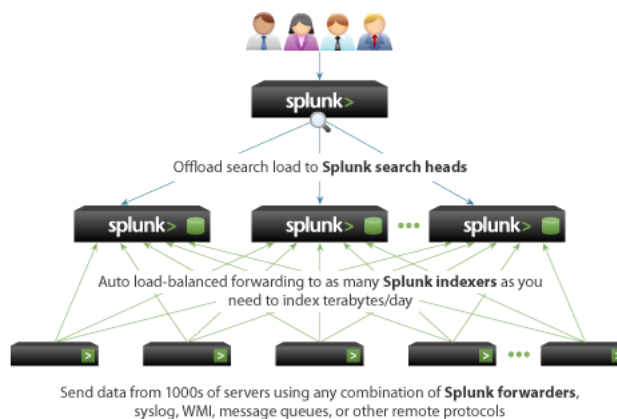
Install Splunk

- **Splunk?**
- **Splunk Download**
- **Splunk Information**

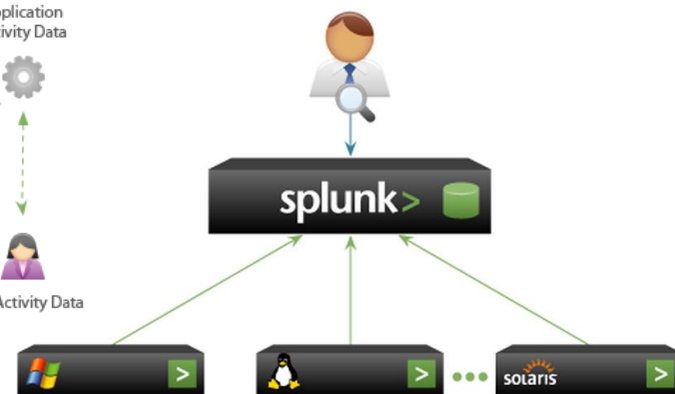
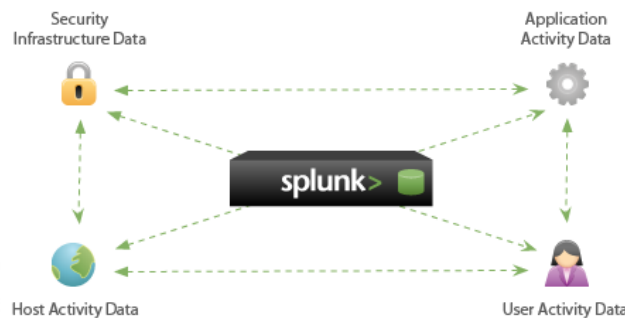
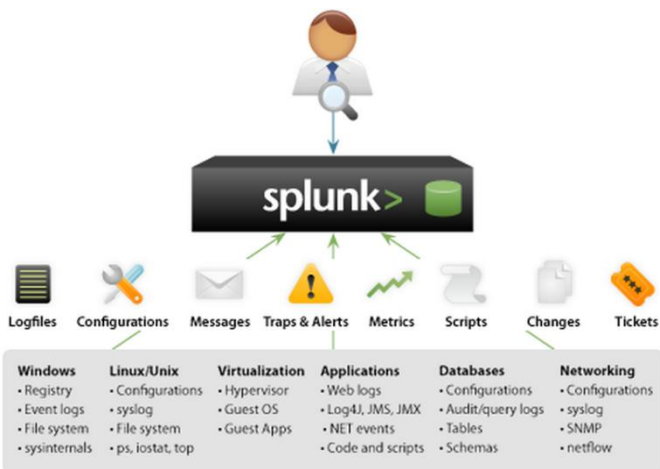


Splunk?

- Indexes any data from any source
- Forwards data from remote systems
- Correlates complex events
- Engineered for big data



splunk>
















Deploy Splunk forwarders on remote systems and send data to a central Splunk server

<http://www.splunk.com/product>



Splunk Download

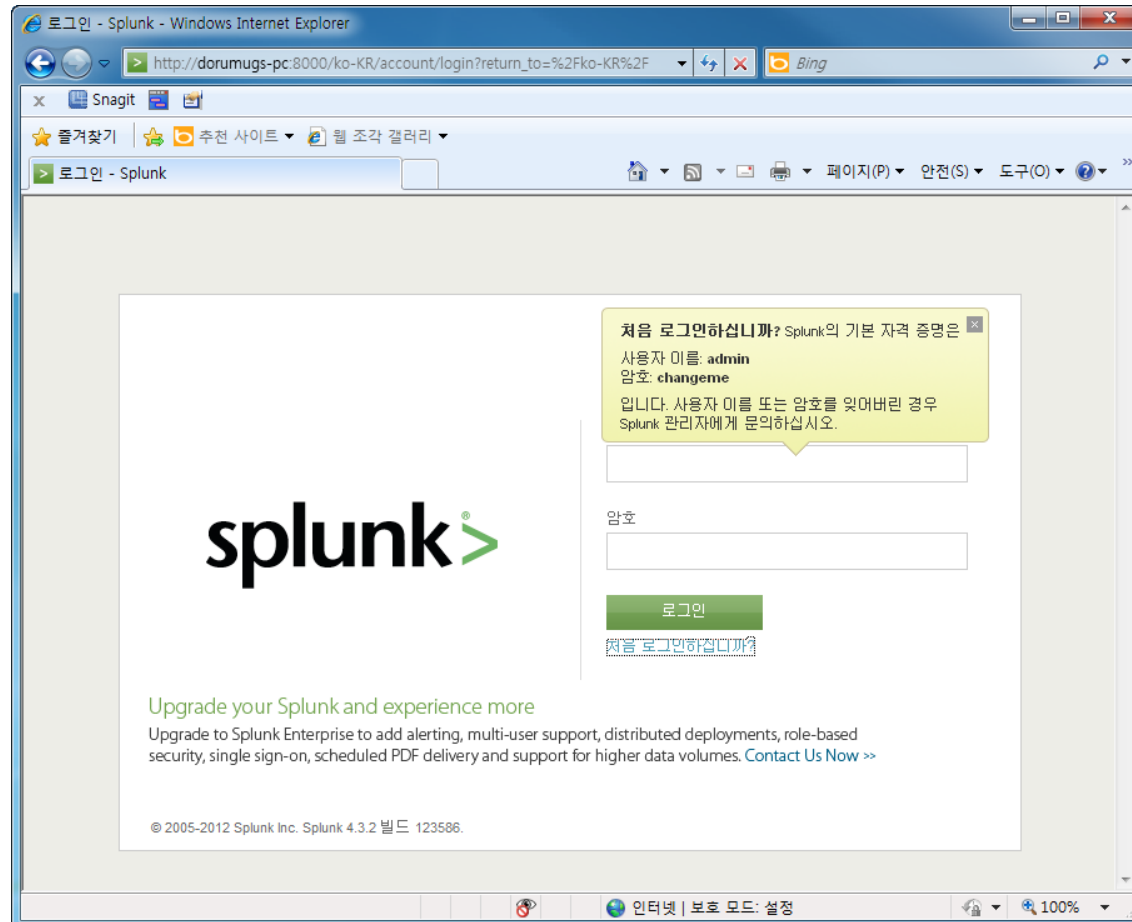
- URL : <http://www.splunk.com/download?r=header>

Platform	Version	Installer	Notes
	Windows XP, 2003, Vista, Windows 7, 2008, 2008 R2 (64-bit)	4.3.2: splunk-4.3.2-123586-x64-release.msi	Release Notes
	Windows XP, 2003, Vista, Windows 7, 2008	4.3.2: splunk-4.3.2-123586-x86-release.msi	Release Notes
	2.6+ kernel Linux distributions (64-bit)	4.3.2: splunk-4.3.2-123586-linux-2.6-x86_64.rpm splunk-4.3.2-123586-linux-2.6-amd64.deb splunk-4.3.2-123586-Linux-x86_64.tgz	Release Notes
	2.4+ kernel Linux distributions with NPTL (32-bit) 2.6+ kernel Linux distributions (32-bit)	4.3.2: splunk-4.3.2-123586-i386.rpm splunk-4.3.2-123586-linux-2.6-intel.deb splunk-4.3.2-123586-Linux-i686.tgz	Release Notes
	Solaris 9, 10 (64-bit)	4.3.2: splunk-4.3.2-123586-solaris-10-intel.pkg.Z splunk-4.3.2-123586-SunOS-x86_64.tar.Z	Release Notes
	Solaris 9, 10 (32-bit)	4.3.2: splunk-4.3.2-123586-solaris-9-intel.pkg.Z splunk-4.3.2-123586-SunOS-i386.tar.Z	Release Notes
	Solaris 8, 9, 10 (SPARC)	4.3.2: splunk-4.3.2-123586-solaris-8-sparc.pkg.Z splunk-4.3.2-123586-SunOS-sparc.tar.Z	Release Notes
	OSX 10.5 (Universal) OSX 10.6 (Universal)	4.3.2: splunk-4.3.2-123586-macosx-10.5-universal.dmg splunk-4.3.2-123586-Darwin-universal.tgz	Release Notes
	FreeBSD 6.2, 7.x, 8.x (64-bit) (freebsd-6.2 is a native package)	4.3.2: splunk-4.3.2-123586-freebsd-7.3-amd64.tgz splunk-4.3.2-123586-freebsd-6.2-amd64.tgz splunk-4.3.2-123586-FreeBSD7-amd64.tgz	Release Notes
	FreeBSD 6.2, 7.x, 8.x (32-bit) (Intel is a native package)	4.3.2: splunk-4.3.2-123586-freebsd-7.3-intel.tgz splunk-4.3.2-123586-FreeBSD7-i386.tgz splunk-4.3.2-123586-freebsd-6.1-intel.tgz	Release Notes
	AIX 5.2, 5.3, 6.1	4.3.2: splunk-4.3.2-123586-AIX-powerpc.tgz	Release Notes
	HP-UX 11i v2 (11.22 PA-RISC) HP-UX 11i v3 (11.31 PA-RISC)	4.3.2: splunk-4.3.2-123586-HPUX-PARISC.tgz	Release Notes
	HP-UX 11i v2 (11.22 Itanium) HP-UX 11i v3 (11.31 Itanium)	4.3.2: splunk-4.3.2-123586-HPUX-ia64.tgz	Release Notes



Splunk Download

- First Login : admin / changeme





Splunk Information

▪ Free License limit

- Use Enterprise features for 60 days.
- Index up to 500megabytes of data per day.
 - ✓ **U can index data over 500megabytes for 6 days.**



<http://www.splunk.com/product>

▪ What's New in Splunk 4.3

- Mobile
 - ✓ New non-Flash UI delivers the power of splunk anywhere.
- Dashboard
 - ✓ Dashboards that business users can define and edit on the fly.
- More concurrent user & faster search
- Complex security policies

Make SuperTimeline

- SuperTimeline?
- Creating SuperTimeline

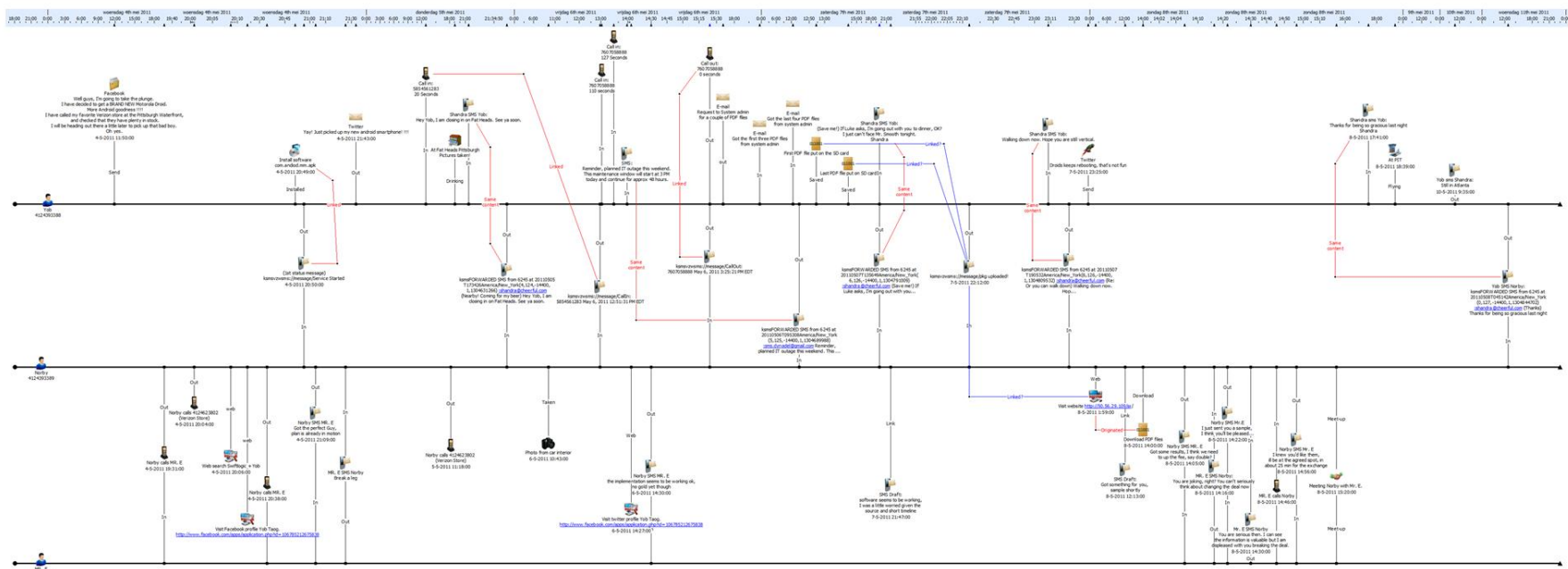


SuperTimeline?

Timeline

- Wikipedia

- ✓ **timeline** is a way of displaying a list of events in chronological order, sometimes described as a project artifact. It is typically a graphic design showing a long bar labeled with dates alongside itself and (usually) events labeled on points where they would have happened.



http://sandbox.dfrws.org/2011/fox-it/DFRWS2011_results/Report/DFRWS%202011%20-%20timeline.png



SuperTimeline?

■ Create Timeline

• Sleuthkit

✓ URL : <http://www.sleuthkit.org/sleuthkit/download.php>

✓ Timeline

- Command : `fls -r -m <mountpoint> <image/device>`
- Command : `mactime <options> -b bodyfile <date-range> -z timezone(Seoul/Asia)`

timeline_ntfs_c.txt									
Thu May 24 2001 00:26:00	20398080	m...	r/r-wx-wx-wx	0	0	53-128-1	c:/SNL/SNL - Celebrity Jeopardy - Lucy Liu - Connery, Jones, W#286.mpeg		
Tue Jun 26 2001 12:48:34	26348294	m...	r/rwxrwxrwx	0	0	48-128-1	c:/SNL/SNL - Celebrity Jeopardy - Robin Williams, Catherine Zet#4db.avi		
Tue Jun 26 2001 14:17:50	25308530	m...	r/r-wx-wx-wx	0	0	59-128-1	c:/RECYCLE.BIN/S-1-5-21-3029248715-2331915947-3066867013-1000/\$RY8BZGE.avi		
Thu May 09 2002 16:49:58	24653187	m...	r/r-wx-wx-wx	0	0	43-128-1	c:/SNL/SNL - Celebrity Jeopardy - The Rapists.mpg		
Thu Aug 05 2004 22:32:14	1027979	m...	r/r-wx-wx-wx	0	0	50-128-1	c:/Media/TrunkMonkey1-high.wmv		
	1027979	m...	r/r-wx-wx-wx	0	0	57-128-1	c:/RECYCLE.BIN/S-1-5-21-3029248715-2331915947-3066867013-1000/\$RNS18KH.wmv		
Thu Aug 05 2004 22:35:07	2236865	m...	r/r-wx-wx-wx	0	0	47-128-1	c:/Media/TrunkMonkey5-high.wmv		
Sat Aug 18 2007 01:01:07	131072	macb	r/r-r-xr-xr-x	0	0	0-128-1	c:/SMFT		
	4096	macb	r/r-r-xr-xr-x	0	0	1-128-1	c:/SMFTMirr		
	131072	macb	r/r-r-xr-xr-x	0	0	10-128-1	c:/UpCase		
	552	macb	d/dr-xr-xr-x	0	0	11-144-4	c:/Extend		
	10141696	macb	r/r-r-xr-xr-x	0	0	2-128-1	c:/LogFile		
	0	macb	r/r-r-xr-xr-x	48	0	3-128-3	c:/Volume		
	2560	macb	r/r-r-xr-xr-x	48	0	4-128-4	c:/AttrDef		
	49088	macb	r/r-r-xr-xr-x	0	0	6-128-1	c:/SBitmap		
	8192	macb	r/r-r-xr-xr-x	48	0	7-128-1	c:/SBoot		
	1608511488	macb	r/r-r-xr-xr-x	0	0	8-128-1	c:/SBadClus:\$Bad		
	0	macb	r/r-r-xr-xr-x	0	0	8-128-2	c:/SBadClus		
	265572	macb	r/r-r-xr-xr-x	0	0	9-128-8	c:/Secure:\$SDS		
	56	macb	r/r-r-xr-xr-x	0	0	9-144-11	c:/Secure:\$SDH		
	56	macb	r/r-r-xr-xr-x	0	0	9-144-14	c:/Secure:\$SII		
Sat Aug 18 2007 01:01:14	208	macb	r/r-r-xr-xr-x	0	0	24-144-2	c:/Extend/\$Quota:\$Q		
	88	macb	r/r-r-xr-xr-x	0	0	24-144-3	c:/Extend/\$Quota:\$Q		
	56	macb	r/r-r-xr-xr-x	0	0	25-144-5	c:/Extend/\$ObjId:\$Q		
	48	macb	r/r-r-xr-xr-x	0	0	26-144-2	c:/Extend/\$Reparse:\$R		
	336	macb	d/dr-xr-xr-x	0	0	27-144-2	c:/Extend/\$RmMetadata		
	8	macb	r/r-r-xr-xr-x	0	0	28-128-2	c:/Extend/\$RmMetadata/\$Repair:\$Config		
	0	macb	r/r-r-xr-xr-x	0	0	28-128-4	c:/Extend/\$RmMetadata/\$Repair		
	56	macb	d/dr-xr-xr-x	0	0	29-144-5	c:/Extend/\$RmMetadata/\$TxFlog		



SuperTimeline?

- **Create Timeline**

- **Log2timeline**

- ✓ **URL :** <http://log2timeline.net/#download>

- ✓ **Timeline**

- **Find Partition starting sector**

- » `mmls image.dd`

- **Extact \$MFT**

- » `icat -I raw -f ntfs -o 63 image.dd 0 > image.mft`

- **Convert \$MFT to CSV**

- » `log2timeline -f mft -z Seoul/Asia -m c: image.mft -w timeline.csv`

- **Mount image for processing**

- » `mount -o ro,noexec,show_sys_files,loop,offset=32256 image.dd /mnt/windows_mount`

- **Create Comprehensive Timeline**

- » `log2timeline -p -r -f winxp -z Seoul/Asia /mnt/windows_mount -w timeline.csv`

- **Filter and Keyword WhiteList**

- » `l2t_process -b timeline.csv -k keywords.txt MM-DD-YYYY..MM-DD-YYYY`



SuperTimeline?

- Create Timeline

- SuperTimeline(SIFT)

- ✓ Script File that log2timeline is used

- ✓ URL : <http://computer-forensics.sans.org/community/downloads>

- ✓ Timeline

- Create Comprehensive Timeline for partition

- » Log2timeline-sift -z Seoul/Asia -p 0 -I partition.dd

- Create Comprehensive Timeline for disk

- » Log2timeline-sift -z Seoul/Asia -I disk.dd

- Creating a Whitelist

- » kedit whitelist.txt

- Content.IE5
 - TemporaryW InternetW Files

- Filter and Keyword WhiteList

- » l2t_process -b timeline.csv -w whitelist.txt MM-DD-YYYY..MM-DD-YYYY > timeline.csv



SuperTimeline?

- Create Timeline
 - SuperTimeline(SIFT)

	A	B	C	D	E	F	G	H	I	J	K	
1	date	time	timezone	MACB	source	sourcetype	type	user	host	short	desc	versi
2	03/11/2002	23:06:30	Asia/Seoul	M...	FILE	NTFS SMFT	\$\$I [M...] time	-	-	C:/Program Files/Adobe/Acrobat 7.0/Setup Files/RdrBig708/ENU_/_ir	C:/Program Files/Adobe/Acrobat 7.0/Setup Files/RdrBig708/ENU_/_instmsiw.exe	
3	03/11/2002	23:06:30	Asia/Seoul	M.B	FILE	NTFS SMFT	\$\$I [M.B] time	-	-	C:/System Volume Information/_restore(ACE7F36F-07FA-4780-9F43-	C:/System Volume Information/_restore(ACE7F36F-07FA-4780-9F43-E1304183A	
4	05/24/2002	12:22:16	Asia/Seoul	M...	FILE	NTFS SMFT	\$\$I [M...] time	-	-	C:/WINDOWS/\$NTServicePackUninstall\$/msdaipp.dll	C:/WINDOWS/\$NTServicePackUninstall\$/msdaipp.dll	
5	05/24/2002	12:22:16	Asia/Seoul	..B	FILE	NTFS SMFT	\$\$I [..B] time	-	-	C:/Program Files/Common Files/System/OLEDDB~1/msdaipp.dll	C:/Program Files/Common Files/System/OLEDDB~1/msdaipp.dll	
6	05/24/2002	12:22:16	Asia/Seoul	M.B	FILE	NTFS SMFT	\$\$I [M.B] time	-	-	C:/System Volume Information/_restore(ACE7F36F-07FA-4780-9F43-	C:/System Volume Information/_restore(ACE7F36F-07FA-4780-9F43-E1304183A	
7	07/31/2002	21:46:52	Asia/Seoul	M.B	FILE	NTFS SMFT	\$\$I [M.B] time	-	-	C:/Program Files/Adobe/READER~1.0/Reader/atl.dll	C:/Program Files/Adobe/READER~1.0/Reader/atl.dll	
8	12/01/2002	16:01:08	Asia/Seoul	M.B	FILE	NTFS SMFT	\$\$I [M.B] time	-	-	C:/Program Files/Adobe/READER~1.0/Resource/ENUtxt.pdf	C:/Program Files/Adobe/READER~1.0/Resource/ENUtxt.pdf	
9	12/20/2002	0:20:38	Asia/Seoul	M.B	FILE	NTFS SMFT	\$\$I [M.B] time	-	-	C:/Program Files/Adobe/READER~1.0/Reader/plug_ins/AcroSign.prc	C:/Program Files/Adobe/READER~1.0/Reader/plug_ins/AcroSign.prc	
10	02/19/2003	8:58:08	Asia/Seoul	M.B	FILE	NTFS SMFT	\$\$I [M.B] time	-	-	C:/System Volume Information/_restore(ACE7F36F-07FA-4780-9F43-	C:/System Volume Information/_restore(ACE7F36F-07FA-4780-9F43-E1304183A	
11	02/19/2003	8:58:08	Asia/Seoul	M...	FILE	NTFS SMFT	\$\$I [M...] time	-	-	C:/Program Files/Adobe/Acrobat 7.0/Setup Files/RdrBig708/ENU_/_0	C:/Program Files/Adobe/Acrobat 7.0/Setup Files/RdrBig708/ENU_/_0x0409.ini	
12	02/21/2003	4:42:22	Asia/Seoul	M.B	FILE	NTFS SMFT	\$\$I [M.B] time	-	-	C:/WINDOWS/system32/msvc71.dll	C:/WINDOWS/system32/msvc71.dll	
13	03/18/2003	21:05:50	Asia/Seoul	M.B	FILE	NTFS SMFT	\$\$I [M.B] time	-	-	C:/WINDOWS/system32/atl71.dll	C:/WINDOWS/system32/atl71.dll	
14	03/18/2003	21:12:12	Asia/Seoul	M.B	FILE	NTFS SMFT	\$\$I [M.B] time	-	-	C:/WINDOWS/system32/mfc71u.dll	C:/WINDOWS/system32/mfc71u.dll	
15	03/18/2003	21:19:59	Asia/Seoul	M.B	FILE	NTFS SMFT	\$\$I [M.B] time	-	-	C:/WINDOWS/system32/mfc71.dll	C:/WINDOWS/system32/mfc71.dll	
16	03/18/2003	22:14:52	Asia/Seoul	M.B	FILE	NTFS SMFT	\$\$I [M.B] time	-	-	C:/WINDOWS/system32/msvc71.dll	C:/WINDOWS/system32/msvc71.dll	
17	03/24/2003	16:53:43	Asia/Seoul	M...	FILE	NTFS SMFT	\$\$I [M...] time	-	-	C:/WINDOWS/\$NTServicePackUninstall\$/fpencode.dll	C:/WINDOWS/\$NTServicePackUninstall\$/fpencode.dll	
18	03/24/2003	16:53:43	Asia/Seoul	M...	FILE	NTFS SMFT	\$\$I [M...] time	-	-	C:/WINDOWS/\$NTServicePackUninstall\$/fp4avss.dll	C:/WINDOWS/\$NTServicePackUninstall\$/fp4avss.dll	
19	03/24/2003	16:53:43	Asia/Seoul	M...	FILE	NTFS SMFT	\$\$I [M...] time	-	-	C:/WINDOWS/\$NTServicePackUninstall\$/shtml.dll	C:/WINDOWS/\$NTServicePackUninstall\$/shtml.dll	
20	03/24/2003	16:53:43	Asia/Seoul	M...	FILE	NTFS SMFT	\$\$I [M...] time	-	-	C:/WINDOWS/\$NTServicePackUninstall\$/tcpctest.exe	C:/WINDOWS/\$NTServicePackUninstall\$/tcpctest.exe	
21	03/24/2003	16:53:43	Asia/Seoul	M...	FILE	NTFS SMFT	\$\$I [M...] time	-	-	C:/WINDOWS/\$NTServicePackUninstall\$/fpexedll.dll	C:/WINDOWS/\$NTServicePackUninstall\$/fpexedll.dll	
22	03/24/2003	16:53:43	Asia/Seoul	M...	FILE	NTFS SMFT	\$\$I [M...] time	-	-	C:/WINDOWS/\$NTServicePackUninstall\$/fpadmdll.dll	C:/WINDOWS/\$NTServicePackUninstall\$/fpadmdll.dll	
23	03/24/2003	16:53:43	Asia/Seoul	M...	FILE	NTFS SMFT	\$\$I [M...] time	-	-	C:/WINDOWS/\$NTServicePackUninstall\$/fpcount.exe	C:/WINDOWS/\$NTServicePackUninstall\$/fpcount.exe	
24	03/24/2003	16:53:43	Asia/Seoul	M...	FILE	NTFS SMFT	\$\$I [M...] time	-	-	C:/System Volume Information/_restore(ACE7F36F-07FA-4780-9F43-	C:/System Volume Information/_restore(ACE7F36F-07FA-4780-9F43-E1304183A	
25	03/24/2003	16:53:43	Asia/Seoul	M...	FILE	NTFS SMFT	\$\$I [M...] time	-	-	C:/System Volume Information/_restore(ACE7F36F-07FA-4780-9F43-	C:/System Volume Information/_restore(ACE7F36F-07FA-4780-9F43-E1304183A	
26	03/24/2003	16:53:43	Asia/Seoul	M...	FILE	NTFS SMFT	\$\$I [M...] time	-	-	C:/System Volume Information/_restore(ACE7F36F-07FA-4780-9F43-	C:/System Volume Information/_restore(ACE7F36F-07FA-4780-9F43-E1304183A	
27	03/24/2003	16:53:43	Asia/Seoul	M...	FILE	NTFS SMFT	\$\$I [M...] time	-	-	C:/WINDOWS/\$NTServicePackUninstall\$/admin.dll	C:/WINDOWS/\$NTServicePackUninstall\$/admin.dll	
28	03/24/2003	16:53:43	Asia/Seoul	M...	FILE	NTFS SMFT	\$\$I [M...] time	-	-	C:/WINDOWS/\$NTServicePackUninstall\$/admin.exe	C:/WINDOWS/\$NTServicePackUninstall\$/admin.exe	
29	03/24/2003	16:53:43	Asia/Seoul	M...	FILE	NTFS SMFT	\$\$I [M...] time	-	-	C:/System Volume Information/_restore(ACE7F36F-07FA-4780-9F43-	C:/System Volume Information/_restore(ACE7F36F-07FA-4780-9F43-E1304183A	
30	03/24/2003	16:53:43	Asia/Seoul	M...	FILE	NTFS SMFT	\$\$I [M...] time	-	-	C:/WINDOWS/\$NTServicePackUninstall\$/fpremadm.exe	C:/WINDOWS/\$NTServicePackUninstall\$/fpremadm.exe	
31	03/24/2003	16:53:43	Asia/Seoul	M...	FILE	NTFS SMFT	\$\$I [M...] time	-	-	C:/WINDOWS/\$NTServicePackUninstall\$/fp4avnb.dll	C:/WINDOWS/\$NTServicePackUninstall\$/fp4avnb.dll	
32	03/24/2003	16:53:43	Asia/Seoul	M...	FILE	NTFS SMFT	\$\$I [M...] time	-	-	C:/System Volume Information/_restore(ACE7F36F-07FA-4780-9F43-	C:/System Volume Information/_restore(ACE7F36F-07FA-4780-9F43-E1304183A	
33	03/24/2003	16:53:43	Asia/Seoul	M...	FILE	NTFS SMFT	\$\$I [M...] time	-	-	C:/WINDOWS/\$NTServicePackUninstall\$/author.dll	C:/WINDOWS/\$NTServicePackUninstall\$/author.dll	
34	03/24/2003	16:53:43	Asia/Seoul	M...	FILE	NTFS SMFT	\$\$I [M...] time	-	-	C:/WINDOWS/\$NTServicePackUninstall\$/cfgwiz.exe	C:/WINDOWS/\$NTServicePackUninstall\$/cfgwiz.exe	
35	03/24/2003	16:53:43	Asia/Seoul	M...	FILE	NTFS SMFT	\$\$I [M...] time	-	-	C:/WINDOWS/\$NTServicePackUninstall\$/fp4areg.dll	C:/WINDOWS/\$NTServicePackUninstall\$/fp4areg.dll	
36	03/24/2003	16:53:43	Asia/Seoul	M...	FILE	NTFS SMFT	\$\$I [M...] time	-	-	C:/WINDOWS/\$NTServicePackUninstall\$/fp4anscp.dll	C:/WINDOWS/\$NTServicePackUninstall\$/fp4anscp.dll	
37	03/24/2003	16:53:43	Asia/Seoul	M...	FILE	NTFS SMFT	\$\$I [M...] time	-	-	C:/WINDOWS/\$NTServicePackUninstall\$/fp98swin.exe	C:/WINDOWS/\$NTServicePackUninstall\$/fp98swin.exe	
38	03/24/2003	16:53:43	Asia/Seoul	M...	FILE	NTFS SMFT	\$\$I [M...] time	-	-	C:/WINDOWS/\$NTServicePackUninstall\$/fp98sadm.exe	C:/WINDOWS/\$NTServicePackUninstall\$/fp98sadm.exe	
39	03/24/2003	16:53:43	Asia/Seoul	M...	FILE	NTFS SMFT	\$\$I [M...] time	-	-	C:/WINDOWS/\$NTServicePackUninstall\$/fp4atst.dll	C:/WINDOWS/\$NTServicePackUninstall\$/fp4atst.dll	



SuperTimeline?

- Create Timeline

- SuperTimeline(SIFT) – Template

- ✓ Link

- <http://computer-forensics.sans.org/blog/2012/01/25/digital-forensic-sifting-colored-super-timeline-template-for-log2timeline-output-files>

- ✓ Download

- http://blogs.sans.org/computer-forensics/files/2012/01/TIMELINE_COLOR_TEMPLATE.zip



SuperTimeline?

- **Create Timeline**

- **SuperTimeline(SIFT) – Template**

- ✓ **The way to import timeline in template**

- 1) Download it - Open Timeline Color Template
- 2) Switch to Color Timeline worksheet/tab
- 3) Click on Cell A-1
- 4) Select 'DATA' Ribbon
- 5) Import Data "FROM TEXT"
- 6) Select log2timeline.csv file
- 7) TEXT IMPORT WIZARD Will Start
- 8) Step 1 -> Select Delimited ->Select NEXT
- 9) Step 2 -> Unselect Tab under Delimiters -> Select Comma under Delimiters -> Select NEXT >
- 10) Step 3 ->Select Finish
- 11) Where do you want to put the data? Simply Select OK.
- 12) Once imported View -> Freeze Panes -> Freeze Top Row
- 13) Optional Hide Columns Timzone, User, Host, Short or Desc (keep one of these), Version
- 14) Select HOME Ribbon
- 15) Select all Cells "CTRL-A"
- 16) In Home Ribbon -> Sort and Filter - Filter



SuperTimeline?

- Create Timeline
 - SuperTimeline(SIFT) – Template

The screenshot shows a Microsoft Excel spreadsheet titled 'TIMELINE_COLOR_TEMPLATE.xlsx'. The spreadsheet is a template for creating a timeline. It has columns labeled A through J. Column A is 'date', B is 'time', D is 'MACB', E is 'source', F is 'sourcetype', G is 'type', and J is 'short'. The rows contain example data. A red arrow points to the 'type' column. A legend is visible at the bottom left of the spreadsheet.

	A	B	D	E	F	G	J
1	date	time	MACB	source	sourcetype	type	short
4147	08/04/2004	0:53:30	M..B	FILE	NTFS \$MFT	\$SI [M..B] time	C:/System Volume Information/_restore(ACE7F36F-07FA-4780-9F43-E1304183A4A1)/Fifoec
4148	08/04/2004	0:53:30	M..B	FILE	NTFS \$MFT	\$SI [M..B] time	C:/System Volume Information/_restore(ACE7F36F-07FA-4780-9F43-E1304183A4A1)/Fifoec
4149	08/04/2004	0:53:30	...B	FILE	NTFS \$MFT	\$SI [...] time	C:/WINDOWS/system32/syssetup.dll
4150	08/04/2004	0:53:30	M...	FILE	NTFS \$MFT	\$SI [M...] time	C:/WINDOWS/\$NtServicePackUninstall\$/usbmon.dll
4151	08/04/2004	0:53:30	M...	FILE	NTFS \$MFT	\$SI [M...] time	C:/WINDOWS/\$NtServicePackUninstall\$/upnphost.dll
4152	08/04/2004	0:53:30	M...	FILE	NTFS \$MFT	\$SI [M...] time	C:/WINDOWS/\$NtServicePackUninstall\$/usbui.dll
4153	08/04/2004	0:53:30	...B	FILE	NTFS \$MFT	\$SI [...] time	C:/WINDOWS/system32/urmon.dll
4154	08/04/2004					\$SI [M..B] time	C:/System Volume Information/_restore(ACE7F36F-07FA-4780-9F43-E1304183A4A1)/Fifoec
4155	08/04/2004					\$SI [...] time	C:/WINDOWS/system32/w3ssl.dll
4156	08/04/2004					\$SI [...] time	C:/WINDOWS/system32/syncui.dll
4157	08/04/2004					\$SI [M..B] time	C:/System Volume Information/_restore(ACE7F36F-07FA-4780-9F43-E1304183A4A1)/Fifoec
4158	08/04/2004					\$SI [...] time	C:/WINDOWS/system32/upnphost.dll
4159	08/04/2004					\$SI [M...] time	C:/WINDOWS/\$NtServicePackUninstall\$/bdflog.dll
4160	08/04/2004					\$SI [...] time	C:/WINDOWS/system32/umandlg.dll
4161	08/04/2004					\$SI [M..B] time	C:/System Volume Information/_restore(ACE7F36F-07FA-4780-9F43-E1304183A4A1)/Fifoec
4162	08/04/2004					\$SI [M...] time	C:/WINDOWS/\$NtServicePackUninstall\$/tcpmib.dll
4163	08/04/2004					\$SI [M...] time	C:/System Volume Information/_restore(ACE7F36F-07FA-4780-9F43-E1304183A4A1)/Fifoec
4164	08/04/2004	0:53:30	M..B	FILE	NTFS \$MFT	\$SI [M..B] time	C:/System Volume Information/_restore(ACE7F36F-07FA-4780-9F43-E1304183A4A1)/Fifoec
4165	08/04/2004	0:53:30	M..B	FILE	NTFS \$MFT	\$SI [M..B] time	C:/System Volume Information/_restore(ACE7F36F-07FA-4780-9F43-E1304183A4A1)/Fifoec
4166	08/04/2004	0:53:30	M...	FILE	NTFS \$MFT	\$SI [M...] time	C:/WINDOWS/\$NtServicePackUninstall\$/wbemcore.dll
4167	08/04/2004	0:53:30	M...	FILE	NTFS \$MFT	\$SI [M...] time	C:/WINDOWS/\$NtServicePackUninstall\$/tapi32.dll
4168	08/04/2004	0:53:30	M..B	FILE	NTFS \$MFT	\$SI [M..B] time	C:/System Volume Information/_restore(ACE7F36F-07FA-4780-9F43-E1304183A4A1)/Fifoec
4169	08/04/2004	0:53:30	M...	FILE	NTFS \$MFT	\$SI [M...] time	C:/WINDOWS/\$NtServicePackUninstall\$/tsoc.dll
4170	08/04/2004	0:53:30	...B	FILE	NTFS \$MFT	\$SI [...] time	C:/WINDOWS/system32/version.dll
4171	08/04/2004	0:53:30	M...	FILE	NTFS \$MFT	\$SI [M...] time	C:/WINDOWS/\$NtServicePackUninstall\$/tapi3.dll
4172	08/04/2004	0:53:30	M...	FILE	NTFS \$MFT	\$SI [M...] time	C:/System Volume Information/_restore(ACE7F36F-07FA-4780-9F43-E1304183A4A1)/Fifoec
4173	08/04/2004	0:53:30	M...	FILE	NTFS \$MFT	\$SI [M...] time	C:/WINDOWS/\$NtServicePackUninstall\$/version.dll

Legend:

- FILE OPENING
- WEB HISTORY
- DELETED DATA
- EXECUTION
- DEVICE or USB USAGE
- FOLDER OPENING
- LOG FILE

Splunk + SuperTimeline

- Splunk Configuration
- Splunk + SuperTimeline
- Splunk Queries



Splunk Configuration

- Configuration files

- URL

- ✓ <https://files.me.com/nick.klein/844rxi> => props.conf
 - ✓ <https://files.me.com/nick.klein/46lcln> => transforms.conf

- Copy

- ✓ C:\Program Files\Splunk\etc\system\local\props.conf
 - ✓ C:\Program Files\Splunk\etc\system\local\transforms.conf
 - ✓ Rerun splunk after copying above files.



Splunk + SuperTimeline

- Data Import

« 검색(으)로 돌아가기

Administrator | 앱 | 관리자 | 경고 | 작업 | 로그아웃

splunk> 관리자 » 인덱스 » 새로 추가

도움말 | 정보

새로 추가

인덱스 설정

인덱스 이름 *

케이스명 : case_test

인덱스 이름(예: INDEX_NAME)을 설정하십시오. index=INDEX_NAME을 사용하여 검색하십시오.

홈 경로

Hot/warm db 경로입니다. 기본적으로 바꿔 두십시오(\$SPLUNK_DB/INDEX_NAME/db).

Cold 경로

Cold db 경로입니다. 기본적으로 바꿔 두십시오(\$SPLUNK_DB/INDEX_NAME/colddb).

Thawed 경로

Thawed/resurrected db 경로입니다. 기본적으로 바꿔 두십시오(\$SPLUNK_DB/INDEX_NAME/thaweddb).

전체 인덱스의 최대 크기(MB)

500000

전체 인덱스의 최대 대상 크기입니다.

hot/warm/cold 버킷의 최대 크기(MB)

auto

버킷의 최대 대상 크기입니다. 높은 볼륨의 인덱스인 경우 'auto_high_volume'를 입력하십시오.

등결된 아카이브 경로

등결된 버킷 아카이브 경로입니다. Splunk가 등결된 버킷을 자동으로 아카이브하도록 하려면 이 항목을 설정하십시오.

취소

저장



Splunk + SuperTimeline

- Data Import

« 검색(으)로 돌아가기

Administrator | 앱 | 관리자 | 경고 | 작업 | 로그아웃

splunk> 관리자 » 인덱스

"case_test"을(를) 성공적으로 저장되었습니다.

도움말 | 정보

인덱스

새로 만들기

9개 항목 중 1-9 표시

페이지당 결과 25

인덱스 이름	전체 인덱스의 최대 크기(MB)	동결된 아카이브 경로	현재 크기(MB)	이벤트 카운트	최초 이벤트	최신 이벤트	홈
_audit	500,000	None	1	1,964	2012. 5. 16. 오전 9:40:40	2012. 5. 16. 오후 3:23:27	C:\File
_blocksignature	0	None	1	0	N/A	N/A	C:\File
_internal	500,000	None	8	152,807	2012. 4. 23. 오후 12:17:38	2012. 5. 17. 오후 12:11:33	C:\File
_thefishbucket	500,000	None	1	0	N/A	N/A	C:\File
case_test	500,000	None	1	0	N/A	N/A	C:\File
history	500,000	None	1	0	N/A	N/A	C:\File
main	500,000	None	1	0	N/A	N/A	C:\File
splunklogger	500,000	None	0	0	N/A	N/A	C:\File
summary	500,000	None	1	0	N/A	N/A	C:\File



Splunk + SuperTimeline

- Data Import

The screenshot shows the Splunk Data Import wizard interface. At the top, the breadcrumb navigation reads: « Search(으)로 돌아가기 | Administrator | 앱 | 관리자 | 경고 | 작업 | 로그아웃. The main header shows the path: splunk> 관리자 » 데이터 추가 » 파일 및 디렉터리 » Data preview. Below this, there are two steps: 1 Preview data and 2 Add data input. The first step, 'Preview data before indexing', is selected and highlighted with a red box. It contains the text: 'Preview data before indexing 자세히 알아보기', 'Point Splunk at a single file representative of the data you want to index.', 'Note: Splunk will only preview the first 1.91 MB of the file.', 'Path to file on the server', and a text input field containing 'C:\Timeline\Image.csv' with a 'Browse server' button. Below this, there is a 'Skip preview' option. A 'File browser' window is open, showing a tree view of the file system. The 'Timeline' folder is expanded, and 'Image.csv' is selected, highlighted with a red box. A 'Set source type' dialog is also open, showing the 'Use auto-detected sourcetype: csv' option selected, with a 'Continue' button. At the bottom, a status bar shows '선택된 경로: C:\Timeline\Image.csv'.

« Search(으)로 돌아가기 | Administrator | 앱 | 관리자 | 경고 | 작업 | 로그아웃

splunk> 관리자 » 데이터 추가 » 파일 및 디렉터리 » Data preview | 도움말 | 정보

1 Preview data — 2 Add data input

☒ Preview data before indexing 자세히 알아보기
Point Splunk at a single file representative of the data you want to index.
Note: Splunk will only preview the first 1.91 MB of the file.
Path to file on the server
C:\Timeline\Image.csv Browse server
On Windows: c:\apache\apache.error.log, On Unix: /var/log/foo.log

☐ Skip preview
Skip preview and manually configure your input.

Continue

File browser

C:\
├── PerfLogs
├── Program Files
├── Program Files (x86)
├── Temp
├── Timeline
│ └── Image.csv
├── Users
├── Windows
└── .rnd
D:\

Set source type

☒ Use auto-detected sourcetype: csv
Start with an existing sourcetype (you can make changes)

☐ Start a new sourcetype

☐ Apply an existing sourcetype
Choose a sourcetype...

Learn more about source types

Continue

선택된 경로: C:\Timeline\Image.csv



Splunk + SuperTimeline

■ Data Import

« 홈(으)로 돌아가기 Administrator 앱 관리자 경고 작업 로그아웃

splunk> 홈 » 데이터 추가 » 파일 및 디렉터리 » 새로 추가 도움말 정보

새로 추가

Splunk에서 파일 또는 디렉터리로부터 데이터를 계속 수집하거나(데이터를 가져온 그대로 인덱스함) 정적 파일을 인덱스한 후 중지할 수 있습니다.

원본

데이터를 가져온 위치와 이 데이터로 수행할 작업을 Splunk에 알려주십시오.

원본 지정

- 이 Splunk 인스턴스가 액세스할 수 있는 파일 또는 디렉터리에서 데이터 계속 인덱스

« 홈(으)로 돌아가기 Administrator 앱 관리자 경고 작업 로그아웃

splunk> 홈 » 데이터 추가 도움말 정보

성공! 데이터가 Splunk로 인덱스되는 중입니다.

현재까지 관리자 > 데이터 입력으로 이동하여 이 데이터 입력에 대한 구성에 액세스할 수 있습니다.

- > 검색 시작
- 더 많은 데이터 추가
- 시작으로 돌아가기

관련 기능

데이터 종류를 Splunk에 알려주면 검색할 때 동일한 유형의 다른 데이터와 해당 데이터를 그룹화할 수 있습니다. Splunk가 자동으로 이 작업을 수행하지만 Splunk에서 오류가 발생한 경우 사용자가 원하는 작업을 지정할 수 있습니다.

원본 유형 설정

목록에서

자동으로 설정할 경우 Splunk는 원본 유형을 자동으로 분류하고 활동한 후 알 수 없는 원본 유형에 위치 표시자 이름을 제공합니다.

목록에서 원본 유형 선택

log2timeline

Splunk에서는 모든 경우 데이터 유형을 자동으로 분류하지만 특정 유형을 찾고 있는 경우 Splunkbase 앱 브라우저 또는 www.splunkbase.com에서 온라인으로 원본 유형을 더 찾을 수 있습니다.

인덱스

Splunk가 데이터를 사용하면 이 데이터는 인덱스화됩니다. 기본적으로 Splunk는 '기본' 인덱스에 데이터를 저장하지만 사용자가 다른 인덱스를 지정할 수 있습니다.

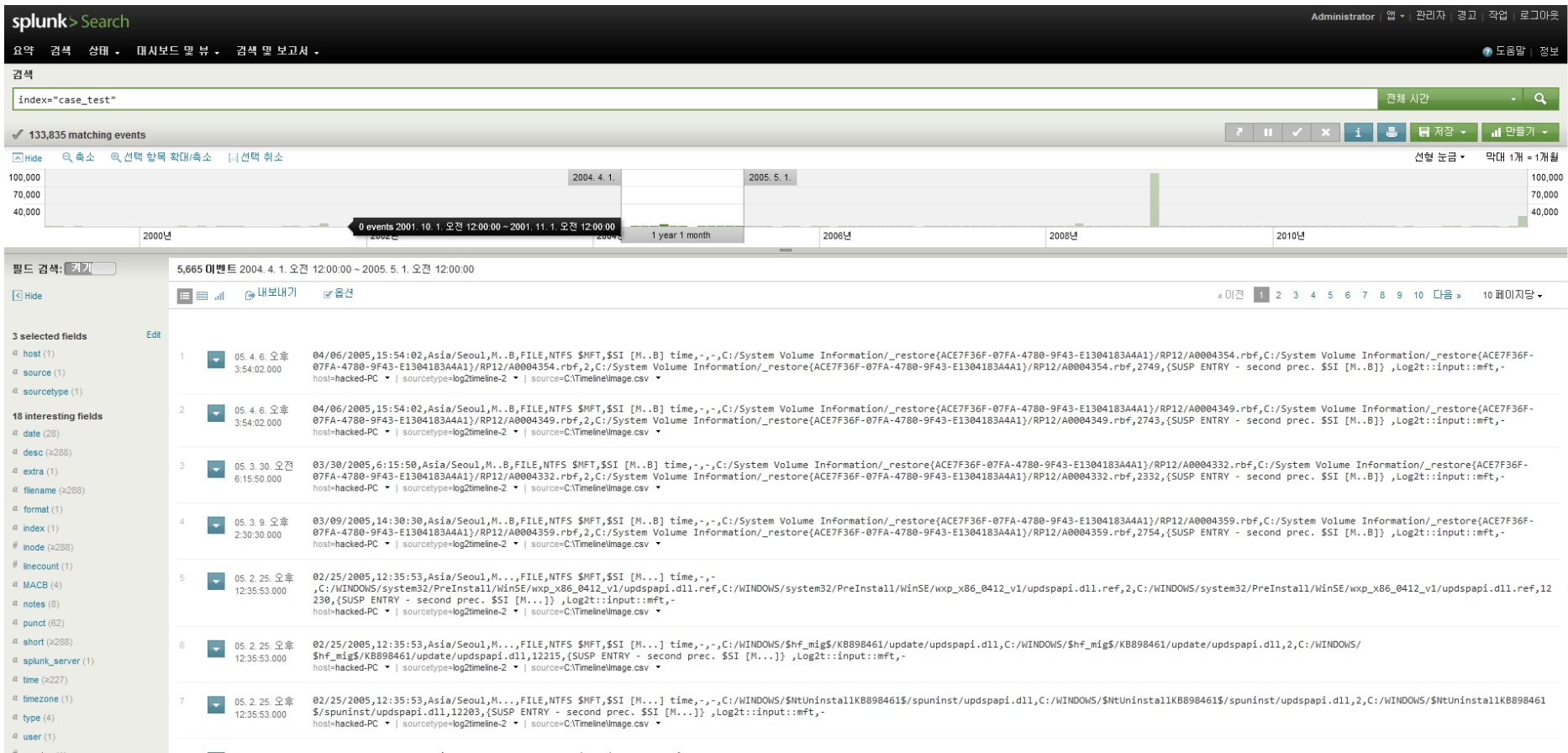
대상 인덱스 설정

case_test



Splunk + SuperTimeline

Data Import





Splunk Queries

▪ Column

- **date** - 02/21/2003
- **time** - 4:42:22
- **timezone** - Asia/Seoul
- **MACB** - M..B
- **source** - FILE
- **sourcetype** - NTFS \$MFT
- **type** - \$SI [M..B] time
- **user** - -
- **host** - -
- **short** - C:/WINDOWS/system32/msvcr71.dll
- **desc** - C:/WINDOWS/system32/msvcr71.dll
- **version** - 2
- **filename** - C:/WINDOWS/system32/msvcr71.dll
- **inode** - 10740
- **notes** - {SUSP ENTRY - second prec. \$SI [M..B]}
- **format** - Log2t::input::mft
- **extra** -



Splunk Queries

- **Search 2011 Records**
 - `index=case_test date_year=2011`
- **Search 2011 year 11 month Records**
 - `index=case_test date_year=2011 date_month=november`
- **Search Birth time and sort filename ascending**
 - `index=case_test MACB="*B" | sort filename`
- **Search Birth time and sort filename descending**
 - `index=case_test MACB="*B" | sort filename desc`
- **Search NTUSER.dat's Record start time**
 - `index=case_test type="time of launch" | sort filename`



Splunk Queries

- Search PDF and Sort date descending
 - `index=case_test filename="*.pdf*" | sort date_year, date_month, time desc`

- Search administrator or user and dat extension and Sort date descending
 - `index=case_test (user="administrator" OR user="user") filename="*.dat" | sort date_year, date_month, time desc`

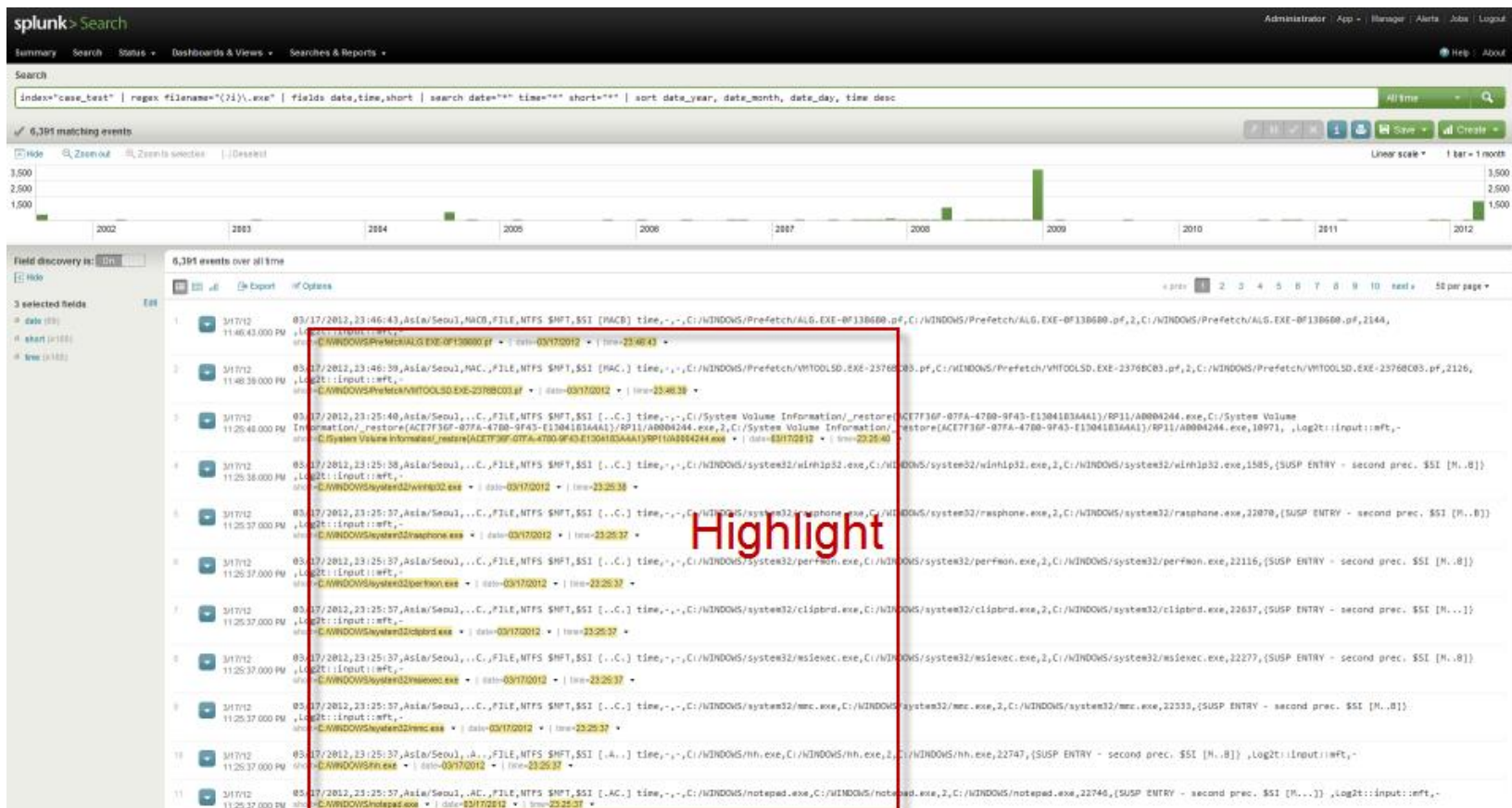
- Search visited URL and Sort date descending
 - `index=case_test short="visited*" | sort date_year, date_month, time desc`

- Search all files in C drive and Sort date descending
 - `index=case_test filename="*c:w*" | sort date_year, date_month, time desc`



Splunk Example

- `index="case_test" | regex filename="(?!)\W.exe" | fields date,time,short | search date="*" time="*" short="*" | sort date_year, date_month, date_day, time desc`
 - `(?!)` is case insensitive function. / `date="*" time="*" short="*"` is highlight function.





Splunk Queries

- **Advantage**
 - ✓ Investigator can Search faster All data.
 - ✓ Investigator can use splunk for free. Although it has limit by 500 megabyte.
 - ✓ Splunk Maintains 500 megabyte over for 6 days.
- **Disadvantage**
 - ✓ Splunk is very expensive for user.
 - ✓ Investigator can research 10 records at the same time.

