타임라인 분석

JK Kim

@pr0neer

forensic-proof.com

proneer@gmail.com

개요

1. 타임라인 분석 소개

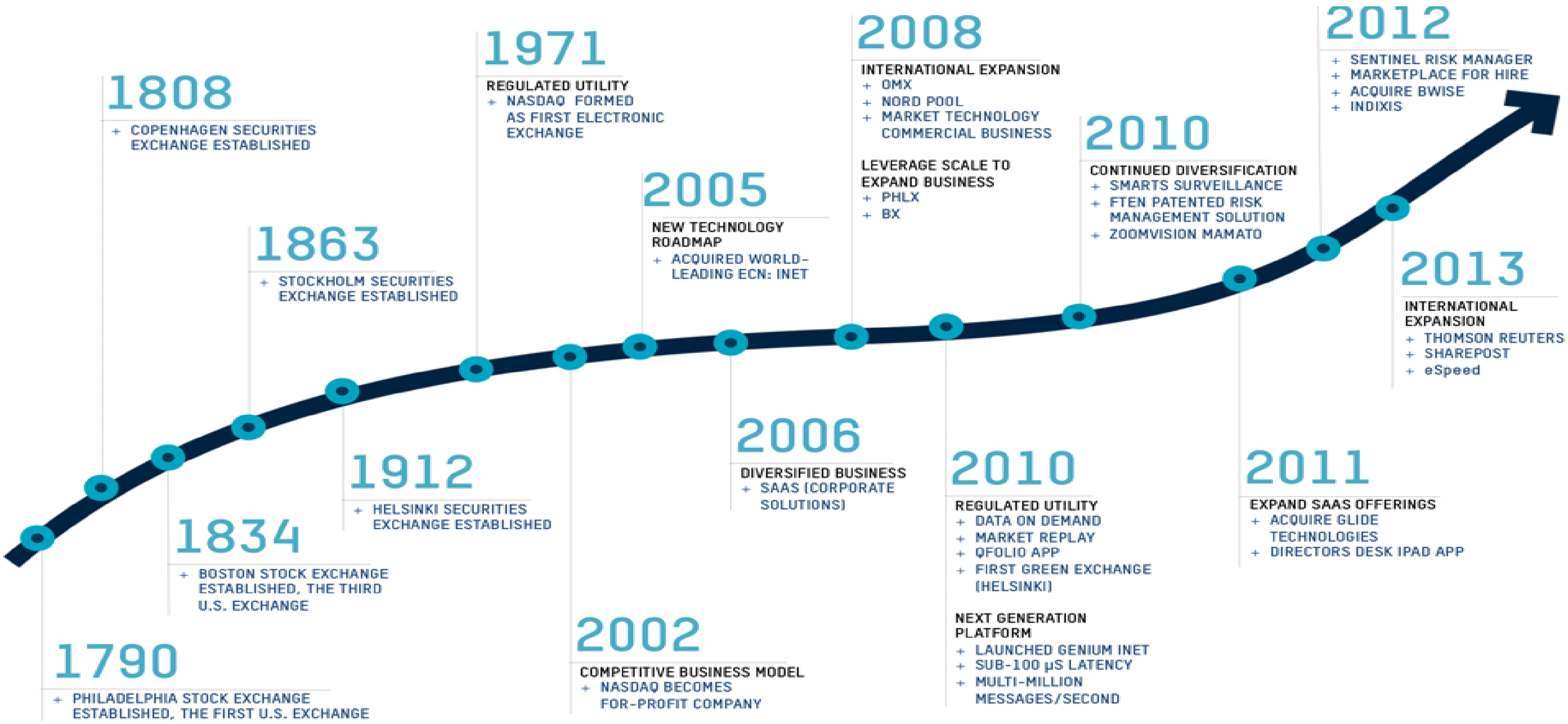
2. 타임라인 분석 실전

타임라인 분석 소개

타임라인 분석 소개

타임라인 분석이란?

- 분석 데이터를 시간 순으로 나열하여 분석하는 방법



1790
+ PHILADELPHIA STOCK EXCHANGE ESTABLISHED, THE FIRST U.S. EXCHANGE

1808
+ COPENHAGEN SECURITIES EXCHANGE ESTABLISHED

1834
+ BOSTON STOCK EXCHANGE ESTABLISHED, THE THIRD U.S. EXCHANGE

1863
+ STOCKHOLM SECURITIES EXCHANGE ESTABLISHED

1912
+ HELSINKI SECURITIES EXCHANGE ESTABLISHED

1971
REGULATED UTILITY
+ NASDAQ FORMED AS FIRST ELECTRONIC EXCHANGE

2002
COMPETITIVE BUSINESS MODEL
+ NASDAQ BECOMES FOR-PROFIT COMPANY

2005
NEW TECHNOLOGY ROADMAP
+ ACQUIRED WORLD-LEADING ECN: INET

2006
DIVERSIFIED BUSINESS
+ SAAS [CORPORATE SOLUTIONS]

2008
INTERNATIONAL EXPANSION
+ OMX
+ NORD POOL
+ MARKET TECHNOLOGY COMMERCIAL BUSINESS

LEVERAGE SCALE TO EXPAND BUSINESS
+ PHLX
+ BX

2010
CONTINUED DIVERSIFICATION
+ SMARTS SURVEILLANCE
+ FTEN PATENTED RISK MANAGEMENT SOLUTION
+ ZOOMVISION MAMATO

2010
REGULATED UTILITY
+ DATA ON DEMAND
+ MARKET REPLAY
+ QFOLIO APP
+ FIRST GREEN EXCHANGE (HELSINKI)

NEXT GENERATION PLATFORM
+ LAUNCHED GENIUM INET
+ SUB-100 µS LATENCY
+ MULTI-MILLION MESSAGES/SECOND

2011
EXPAND SAAS OFFERINGS
+ ACQUIRE GLIDE TECHNOLOGIES
+ DIRECTORS DESK IPAD APP

2012
+ SENTINEL RISK MANAGER
+ MARKETPLACE FOR HIRE
+ ACQUIRE BWISE
+ INDIXIS

2013
INTERNATIONAL EXPANSION
+ THOMSON REUTERS
+ SHAREPOST
+ eSpeed

타임라인 분석 소개

- **활용 방안**
  - **타임라인 분석을 왜 하는가?**
    - ✓ 특정 이벤트 발생 시점 전, 후로 시스템 상에서 어떤 일이 발생했는지 쉽게 파악 가능
    - ✓ 정밀 분석 대상을 빠르게 선별 가능
  - **타임라인 분석의 필요 요소**
    - ✓ 상관관계
    - ✓ 맥락, 전후 사정
    - ✓ 신뢰성
    - ✓ 근접한 시간 분석
    - ✓ 시간에 기반한 정확한 정렬

타임라인 분석 소개

- **활용 방안**
  - **시점 *KNOWN***
    - ✓ 타임라인 추출 후 해당 시점을 기준으로 분석
  - **시점 *UNKNOWN***
    - ✓ 사건 성격이나 분석 대상에 따른 분석 지표를 조사하여 시점 파악
    - ✓ 정보 유출 사고
      - 사용자 이상 행위, 외장저장매체 연결 시각, 외부 서비스 접속 시간 등
    - ✓ 침해사고
      - 침해 지표 생성 시점, 프로그램 실행 시점 등

타임라인 분석 소개

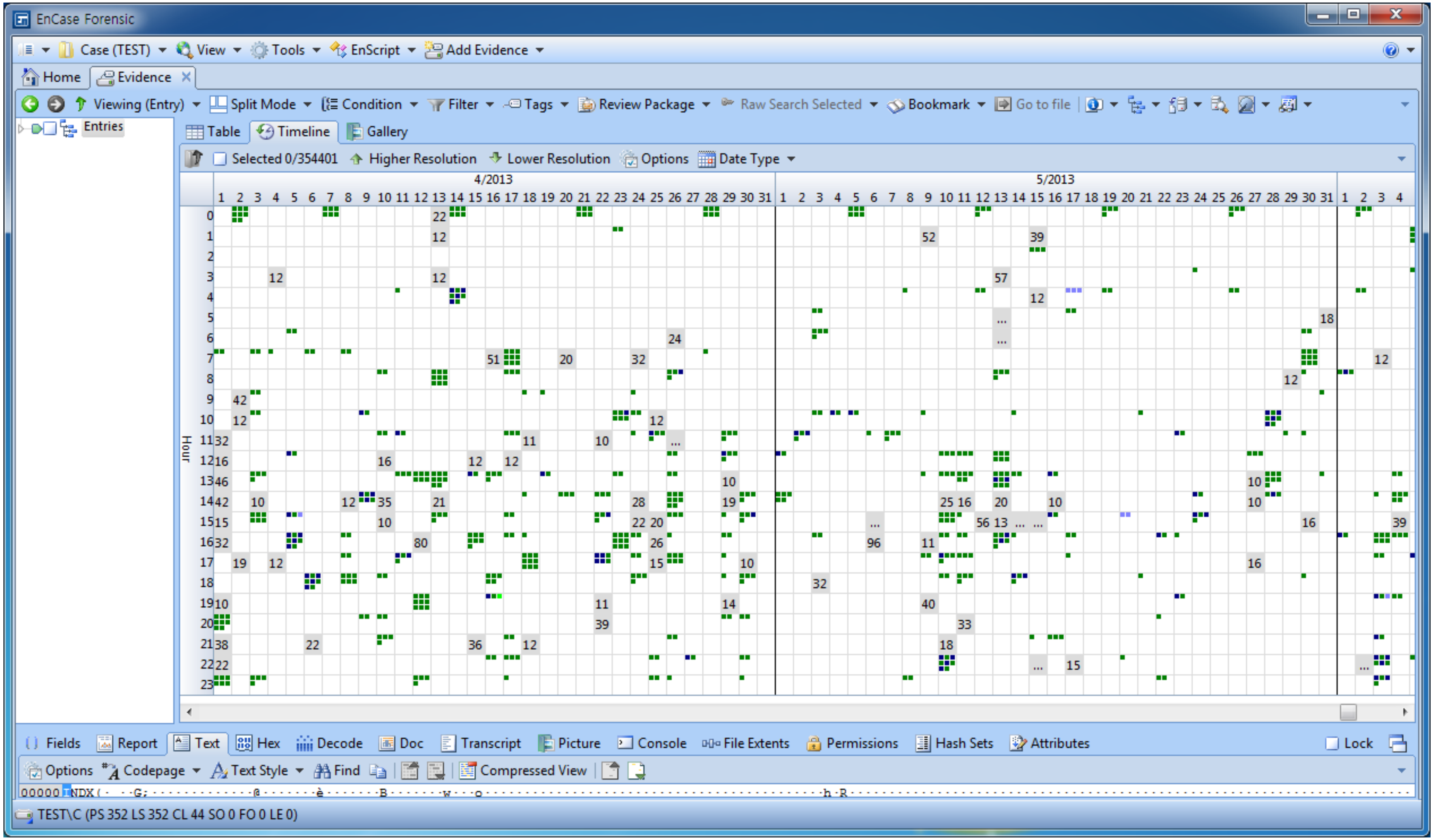
- **시간 정보를 포함하는 아티팩트**
  - 파일시스템 메타데이터 (FAT=3, NTFS=8)
  - 프리패치 파일 생성 시간, 내부 최종 실행 시간
  - 레지스트리 키의 마지막 기록 시간
  - 이벤트 로그의 이벤트 생성/작성 시간
  - 바로가기 파일의 생성/수정/접근 시간과 바로가기 대상의 생성/수정/접근 시간
  - IIS, FTP, MS-SQL Error, AV 로그 등의 시간 정보
  - 웹 브라우저 사용 흔적의 방문/수정/접근/만료/다운로드 시간
  - 시스템 복원 지점과 볼륨 섀도 복사본의 파일시스템 시간 정보
  - PE 파일의 컴파일 시간
  - 휴지통의 삭제된 시간
  - JPEG EXIF의 사진 촬영 시간
  - … …

타임라인 분석 소개

- **타임라인 분석 도구**
  - **파일시스템 타임라인 분석 도구**
    - ✓ EnCase, FTK, X-Ways Forensics, X-Ways WinHex, Autopsy 등
  - **메모리 타임라인 분석 도구**
    - ✓ Redline – http://www.mandiant.com/resources/download/redline
    - ✓ Volatility Plugin "timeliner" – https://code.google.com/p/volatility/wiki/CommandReference23#timeliner
  - **통합 타임라인 분석 도구**
    - ✓ **log2timeline** – http://log2timeline.net/
    - ✓ Splunk – http://www.splunk.com (???)

타임라인 분석 소개

- 타임라인 분석 도구
  - EnCase Forensic


EnCase Forensic
Case (TEST) · View · Tools · EnScript · Add Evidence
Home · Evidence
Viewing (Entry) · Split Mode · Condition · Filter · Tags · Review Package · Raw Search Selected · Bookmark · Go to file
Entries
Table · Timeline · Gallery
Selected 0/354401 · Higher Resolution · Lower Resolution · Options · Date Type
4/2013
5/2013
Hour
Fields · Report · Text · Hex · Decode · Doc · Transcript · Picture · Console · File Extents · Permissions · Hash Sets · Attributes · Lock
Options · Codepage · Text Style · Find · Compressed View
TEST\C (PS 352 LS 352 CL 44 SO 0 FO 0 LE 0)

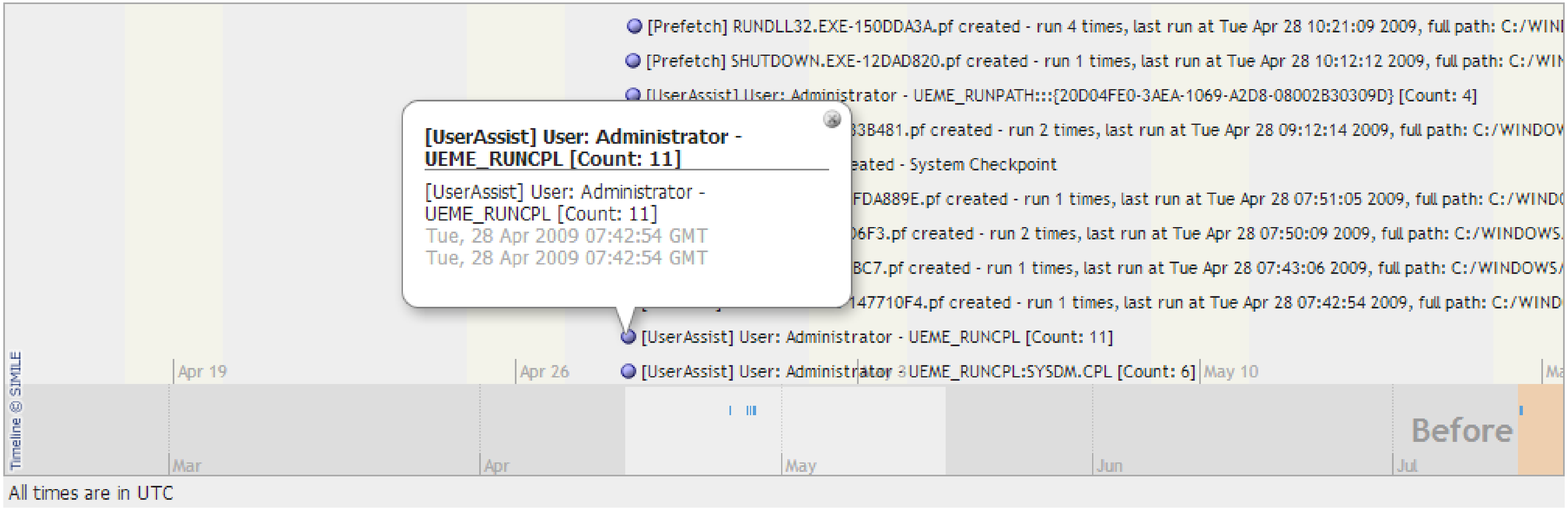
타임라인 분석 소개

➔ 실습

- WinHex를 이용해 파일시스템 타임라인 분석하기!!

타임라인 분석 소개

- **log2timeline**
  - **log2timeline 개발 과정**
    - ✓ 2009-07-31 : 첫 베타 버전 v0.12b
    - ✓ 2009-11-25 : 타임 존 기능 추가 등의 요구사항을 반영한 v4.0
    - ✓ 2010-06-30 : 구조 변경과 추가 기능이 늘어난 v5.0
    - ✓ 2010-08-25 : SANS Gold Paper 선정, Mastering the Super Timeline With log2timeline
    - ✓ 2011-05-04 : Forensc4Cast Award의 "best computer forensic software" 수상
    - ✓ 2012-09-19 : utmp, selinux 모듈이 추가된 v.0.65



```
[Prefetch] RUNDLL32.EXE-150DDA3A.pf created - run 4 times, last run at Tue Apr 28 10:21:09 2009, full path: C:/WIN
[Prefetch] SHUTDOWN.EXE-12DAD820.pf created - run 1 times, last run at Tue Apr 28 10:12:12 2009, full path: C:/WIN
[UserAssist] User: Administrator - UEME_RUNPATH:::{20D04FE0-3AEA-1069-A2D8-08002B30309D} [Count: 4]
33B481.pf created - run 2 times, last run at Tue Apr 28 09:12:14 2009, full path: C:/WINDOW
eated - System Checkpoint
FDA889E.pf created - run 1 times, last run at Tue Apr 28 07:51:05 2009, full path: C:/WIND
06F3.pf created - run 2 times, last run at Tue Apr 28 07:50:09 2009, full path: C:/WINDOWS.
BC7.pf created - run 1 times, last run at Tue Apr 28 07:43:06 2009, full path: C:/WINDOWS/
147710F4.pf created - run 1 times, last run at Tue Apr 28 07:42:54 2009, full path: C:/WIND
[UserAssist] User: Administrator - UEME_RUNCPL [Count: 11]
[UserAssist] User: Administrator - UEME_RUNCPL:SYSDM.CPL [Count: 6]
```

[UserAssist] User: Administrator - UEME_RUNCPL [Count: 11]

[UserAssist] User: Administrator - UEME_RUNCPL [Count: 11]
Tue, 28 Apr 2009 07:42:54 GMT
Tue, 28 Apr 2009 07:42:54 GMT

All times are in UTC

타임라인 분석 소개

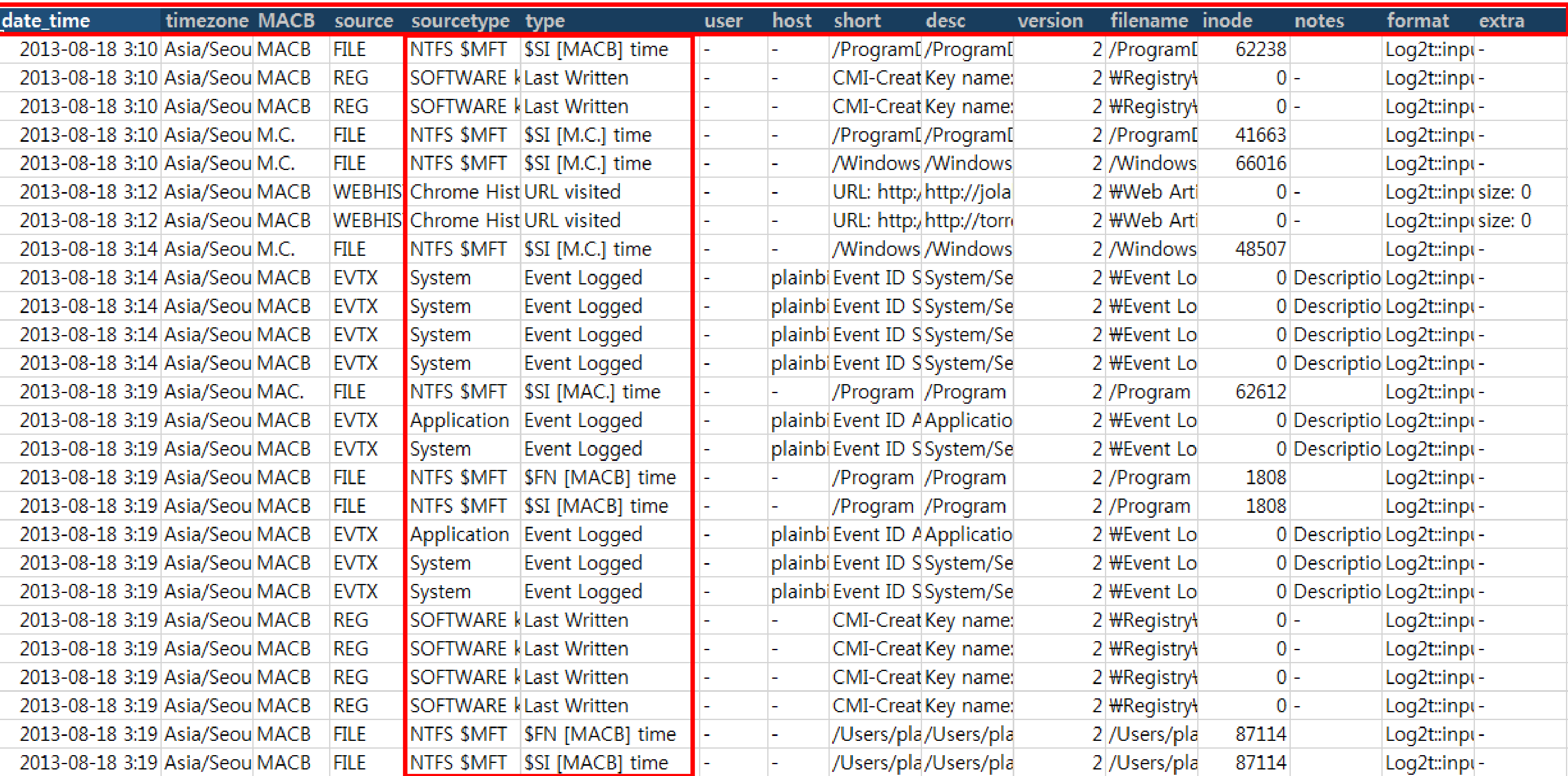
- **log2timeline**
  - **입력 모듈**
    - ✓ Apache2 Access logs
    - ✓ Apache2 Error logs
    - ✓ Google Chrome history
    - ✓ Encase dirlisting
    - ✓ Windows Event Log files (EVT)
    - ✓ Windows Event Log files (EVTX)
    - ✓ EXIF
    - ✓ Firefox bookmarks
    - ✓ Firefox 2 history
    - ✓ Firefox 3 history
    - ✓ FTK Imager Dirlisting CSV file
    - ✓ Generic Linux log file
    - ✓ Internet Explorer history files
    - ✓ Windows IIS W3C log files
    - ✓ ISA server text export.
    - ✓ Mactime body files
    - ✓ McAfee AntiVirus Log files
    - ✓ MS-SQL Error log
    - ✓ Opera Global and Direct browser history
    - ✓ OpenXML metadata
    - ✓ PCAP files
    - ✓ PDF. Parse the basic PDF metadata
    - ✓ Windows Prefetch directory
    - ✓ Windows Recycle Bin (INFO2 or I$)
    - ✓ Windows Restore Points
    - ✓ Safari Browser history files
    - ✓ Windows XP SetupAPI.log file
    - ✓ Adobe Local Shared Object files (SOL/LSO),
    - ✓ Squid Access Logs (httpd_emulate off)
    - ✓ TLN (timeline) body files
    - ✓ UserAssist key of the Windows registry
    - ✓ Volatility. The output from psscan/psscan2
    - ✓ Windows Shortcut files (LNK)
    - ✓ Windows WMIProv log file
    - ✓ Windows XP Firewall Log files (W3C format)

타임라인 분석 소개

- **log2timeline**
  - **다양한 로그 형식**
    - ✓ **Apache2 Access logs (TEXT)**
      - [Remote Host IP] [Remote Logname] [User ID] [Date] [Client Request] [Status Code] [Size]
    - ✓ **MS-SQL Error Log (TEXT)**
      - [Date] [Source] [Message]
    - ✓ **NTFS MFT (BINARY)**
      - 유용한 정보 추출 (8개의 시간 정보, 파일 이름, 속성, 데이터 등)
    - ✓ **Internet Explorer History Files (BINARY)**
      - 유용한 정보 추출 (접속 URL, 접속 시간, 방문 횟수, 웹 페이지 제목, 로컬 파일 열람 정보 등)
    - ✓ **EXIF (BINARY)**
      - 유용한 정보 추출 (촬영 시간 포함) ➔ 뭘 뽑아낼 것인가?

타임라인 분석 소개

- **log2timeline**
  - **다양한 로그 형식 ➔ 정형화!!**
    - ✓ [date_time] [timezone] [MACB] [source] [sourcetype] [type] [user] [host] [short] [desc] [version] [filename] [inode] [notes] [format] [extra]



date_time	timezone	MACB	source	sourcetype	type	user	host	short	desc	version	filename	inode	notes	format	extra
2013-08-18 3:10	Asia/Seou	MACB	FILE	NTFS $MFT	$SI [MACB] time	-	-	/ProgramD	/ProgramD	2	/ProgramD	62238		Log2t::inpu	-
2013-08-18 3:10	Asia/Seou	MACB	REG	SOFTWARE k	Last Written	-	-	CMI-Creat	Key name:	2	₩Registry₩	0	-	Log2t::inpu	-
2013-08-18 3:10	Asia/Seou	MACB	REG	SOFTWARE k	Last Written	-	-	CMI-Creat	Key name:	2	₩Registry₩	0	-	Log2t::inpu	-
2013-08-18 3:10	Asia/Seou	M.C.	FILE	NTFS $MFT	$SI [M.C.] time	-	-	/ProgramD	/ProgramD	2	/ProgramD	41663		Log2t::inpu	-
2013-08-18 3:10	Asia/Seou	M.C.	FILE	NTFS $MFT	$SI [M.C.] time	-	-	/Windows	/Windows	2	/Windows	66016		Log2t::inpu	-
2013-08-18 3:12	Asia/Seou	MACB	WEBHIS	Chrome Hist	URL visited	-	-	URL: http:/	http://jola	2	₩Web Arti	0	-	Log2t::inpu	size: 0
2013-08-18 3:12	Asia/Seou	MACB	WEBHIS	Chrome Hist	URL visited	-	-	URL: http:/	http://torr	2	₩Web Arti	0	-	Log2t::inpu	size: 0
2013-08-18 3:14	Asia/Seou	M.C.	FILE	NTFS $MFT	$SI [M.C.] time	-	-	/Windows	/Windows	2	/Windows	48507		Log2t::inpu	-
2013-08-18 3:14	Asia/Seou	MACB	EVTX	System	Event Logged	-	plainbi	Event ID S	System/Se	2	₩Event Lo	0	Descriptio	Log2t::inpu	-
2013-08-18 3:14	Asia/Seou	MACB	EVTX	System	Event Logged	-	plainbi	Event ID S	System/Se	2	₩Event Lo	0	Descriptio	Log2t::inpu	-
2013-08-18 3:14	Asia/Seou	MACB	EVTX	System	Event Logged	-	plainbi	Event ID S	System/Se	2	₩Event Lo	0	Descriptio	Log2t::inpu	-
2013-08-18 3:14	Asia/Seou	MACB	EVTX	System	Event Logged	-	plainbi	Event ID S	System/Se	2	₩Event Lo	0	Descriptio	Log2t::inpu	-
2013-08-18 3:19	Asia/Seou	MAC.	FILE	NTFS $MFT	$SI [MAC.] time	-	-	/Program	/Program	2	/Program	62612		Log2t::inpu	-
2013-08-18 3:19	Asia/Seou	MACB	EVTX	Application	Event Logged	-	plainbi	Event ID A	Applicatio	2	₩Event Lo	0	Descriptio	Log2t::inpu	-
2013-08-18 3:19	Asia/Seou	MACB	EVTX	System	Event Logged	-	plainbi	Event ID S	System/Se	2	₩Event Lo	0	Descriptio	Log2t::inpu	-
2013-08-18 3:19	Asia/Seou	MACB	FILE	NTFS $MFT	$FN [MACB] time	-	-	/Program	/Program	2	/Program	1808		Log2t::inpu	-
2013-08-18 3:19	Asia/Seou	MACB	FILE	NTFS $MFT	$SI [MACB] time	-	-	/Program	/Program	2	/Program	1808		Log2t::inpu	-
2013-08-18 3:19	Asia/Seou	MACB	EVTX	Application	Event Logged	-	plainbi	Event ID A	Applicatio	2	₩Event Lo	0	Descriptio	Log2t::inpu	-
2013-08-18 3:19	Asia/Seou	MACB	EVTX	System	Event Logged	-	plainbi	Event ID S	System/Se	2	₩Event Lo	0	Descriptio	Log2t::inpu	-
2013-08-18 3:19	Asia/Seou	MACB	EVTX	System	Event Logged	-	plainbi	Event ID S	System/Se	2	₩Event Lo	0	Descriptio	Log2t::inpu	-
2013-08-18 3:19	Asia/Seou	MACB	REG	SOFTWARE k	Last Written	-	-	CMI-Creat	Key name:	2	₩Registry₩	0	-	Log2t::inpu	-
2013-08-18 3:19	Asia/Seou	MACB	REG	SOFTWARE k	Last Written	-	-	CMI-Creat	Key name:	2	₩Registry₩	0	-	Log2t::inpu	-
2013-08-18 3:19	Asia/Seou	MACB	REG	SOFTWARE k	Last Written	-	-	CMI-Creat	Key name:	2	₩Registry₩	0	-	Log2t::inpu	-
2013-08-18 3:19	Asia/Seou	MACB	REG	SOFTWARE k	Last Written	-	-	CMI-Creat	Key name:	2	₩Registry₩	0	-	Log2t::inpu	-
2013-08-18 3:19	Asia/Seou	MACB	FILE	NTFS $MFT	$FN [MACB] time	-	-	/Users/pla	/Users/pla	2	/Users/pla	87114		Log2t::inpu	-
2013-08-18 3:19	Asia/Seou	MACB	FILE	NTFS $MFT	$SI [MACB] time	-	-	/Users/pla	/Users/pla	2	/Users/pla	87114		Log2t::inpu	-

타임라인 분석 소개

- **log2timeline**
  - **출력 모듈**
    - ✓ **BeeDocs**. A visualization tool designed for the Mac OS X.
    - ✓ **CEF**. Common Event Format as described by ArcSight
    - ✓ **CFTL**. A XML file that can be read by CyberForensics TimeLab (for timeline visualization)
    - ✓ **CSV**. Dump the timeline in a comma separated value file (CSV).
    - ✓ **Mactime**. Both older and newer version of the format supported for use by TSK's mactime
    - ✓ **SIMILE**. An XML file that can be read by a SIMILE timeline widget for timeline visualization
    - ✓ **SQLite**. Dump the timeline into a SQLite database.
    - ✓ **TLN**. Tab Delimited File (same as the CSV, but with tabs instead of commas to separate)
    - ✓ **TLN**. Timeline format that is used by some of H. Carvey tools, ASCII output
    - ✓ **TLNX**. Timeline format that is used by some of H. Carvey tools, XML document

타임라인 실전

타임라인 분석 실전

log2timeline

- 디스크 이미지

```
$> perl  log2timeline  -z  Asia/Seoul  -r  -p  -w  timeline.txt  -I  disk.dd
```

```
$> perl  log2timeline  -z  Asia/Seoul  -r  -p  -w  timeline.txt  -p  0  -I  partition.dd
```

- 라이브 볼륨

```
$> perl  log2timeline  -z  Asia/Seoul  -r  -p  -w  timeline.txt  “C:₩”
```

- 아티팩트 폴더

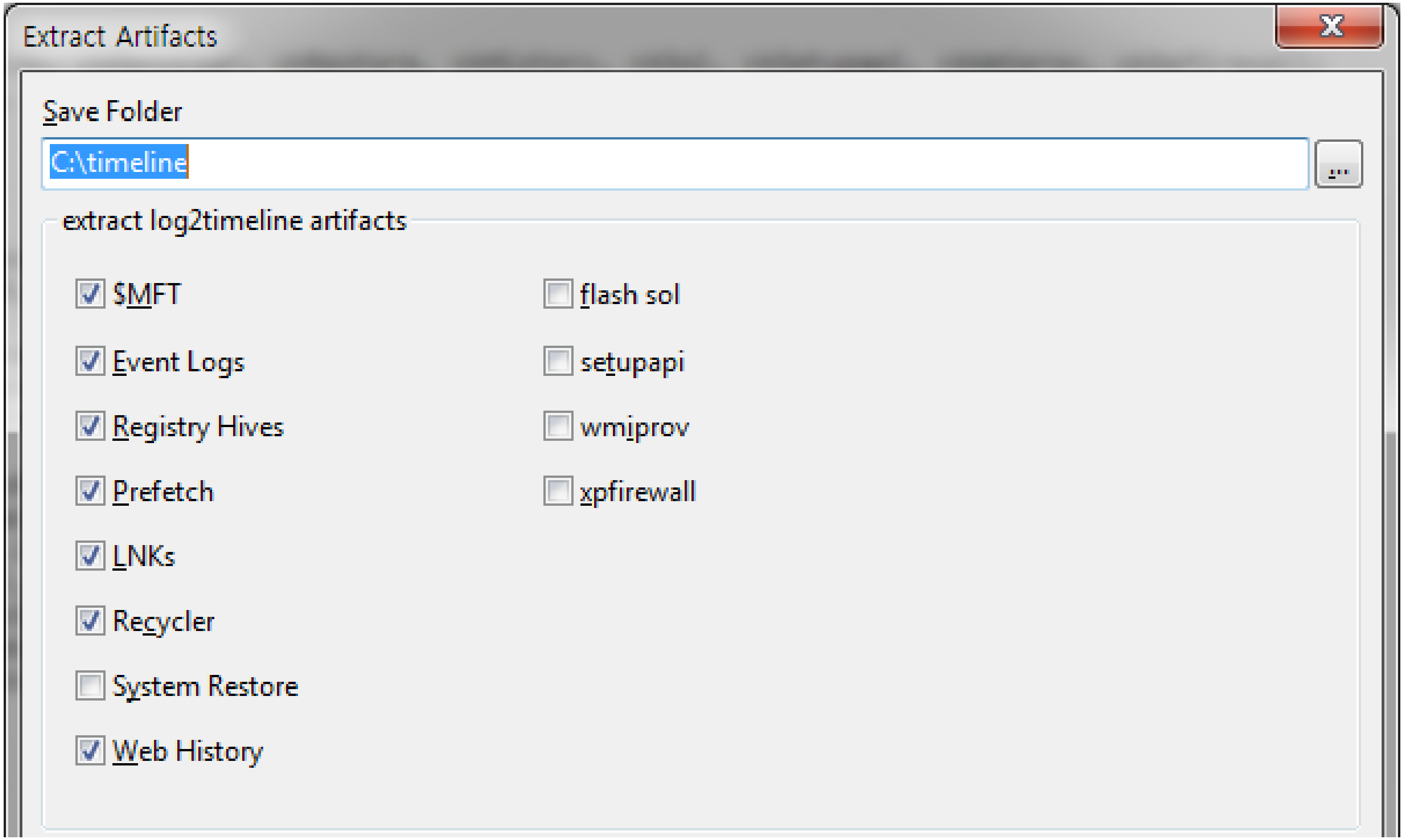
```
$> perl  log2timeline  -z  Asia/Seoul  -r  -p  -w  timeline.txt “d:₩artifacts₩”
```

타임라인 분석 실전

- **log2timeline_mod**
  - **수정 사항**
    - ✓ 한글 인코딩 처리 문제 해결
    - ✓ 시간 형식 변경 (월/일/년 ➔ 년-월-일)
    - ✓ 일부 파싱 모듈 수정
    - ✓ 윈도우 환경에서 동작 가능
  - **입력 대상**
    - ✓ 디스크 **이미지**
    - ✓ 라이브 **볼륨**
    - ✓ 아티팩트 **폴더**

타임라인 분석 실전

- log2timeline_mod
  - 아티팩트 수집
    - ✓ EnScript 사용



Extract Artifacts

Save Folder

C:\timeline

extract log2timeline artifacts

☑ $MFT
☑ Event Logs
☑ Registry Hives
☑ Prefetch
☑ LNKs
☑ Recycler
□ System Restore
☑ Web History

□ flash sol
□ setupapi
□ wmiprov
□ xpfirewall

타임라인 분석 실전

- **log2timeline_mod**
  - **아티팩트 수집**
    - ✓ **FORECOPY** 사용 (https://code.google.com/p/proneer/downloads/list)

$MFT	forecopy_handy –m <save folder>
REGISTRY	forecopy_handy –g <save folder>
PREFETCH	forecopy_handy –p <save folder>
EVENT LOGs	forecopy_handy –e <save folder>
Shortcuts (LNK)	forecopy_handy –r "%AppData%₩Microsoft₩Windows₩Recent" %1
IE Artifacts	forecopy_handy –i <save folder>
FIREFOX Artifacts	forecopy_handy –f <save folder>
CHROME Artifacts	forecopy_handy –x <save folder>
$RECYCLE.BIN	forecopy_handy –r "C:₩Recycle.Bin" %1
SETUPAPI Log	forecopy_handy -f "%SystemRoot%₩inf₩setupapi.dev.log" %1
WMIPROV Log	forecopy_handy -f "%SystemRoot%₩system32₩wbem₩logs₩wmiprov.log" %1

타임라인 분석 실전

➔ 실습

- FORECOPY를 이용해 라이브에서 아티팩트 수집하기!!
- Arsenal Imager Mounter로 이미지 마운트 후 아티팩트 수집하기!!

타임라인 분석 실전

➔ 실습

- WinHex를 이용해 수동으로 포렌식 아티팩트 추출하기!!

Artifacts	Path
$MFT	%SystemDrive%₩$MFT
$LogFile	%SystemDrive%₩$LogFile
$UsnJrnl	%SystemDrive%₩$Extend₩$UsnJrnl:$J
PREFETCH	%SystemRoot%₩Prefetch₩*
EVENT LOG	%SystemRoot%₩System32₩winevt₩Logs₩* %SystemRoot%₩SysWOW64₩winevt₩Logs₩*
Shortcuts (LNK)	%UserProfile%₩AppData₩Roaming₩Microsoft₩Windows₩Recent₩*.lnk %UserProfile%₩AppData₩Roaming₩Microsoft₩Office₩Recent₩*.lnk %UserProfile%₩AppData₩Roaming₩HNC₩Office₩Recent₩*.lnk
JUMPLIST	%UserProfile%₩AppData₩Roaming₩Microsoft₩Windows₩Recent₩AutomaticDestinations₩* %UserProfile%₩AppData₩Roaming₩Microsoft₩Windows₩Recent₩CustomDestinations₩*
$RECYCLE.BIN	%Drive%₩$Recycle.Bin₩*
systemprofile	%SystemRoot%₩System32₩config₩systemprofile₩* %SystemRoot%₩SysWOW64₩config₩systemprofile₩*

타임라인 분석 실전

➔ 실습

- WinHex를 이용해 수동으로 포렌식 아티팩트 추출하기!!

Artifacts	Path
Registry	%UserProfile%₩NTUSER.DAT %UserProfile%₩AppData₩Local₩Microsoft₩Windows₩UsrClass.dat %SystemRoot%₩ServiceProfiles₩LocalService₩NTUSER.DAT %SystemRoot%₩ServiceProfiles₩NetworkService₩NTUSER.DAT %SystemRoot%₩System32₩config₩DEFAULT %SystemRoot%₩System32₩config₩SAM %SystemRoot%₩System32₩config₩SECURITY %SystemRoot%₩System32₩config₩SOFTWARE %SystemRoot%₩System32₩config₩SYSTEM %SystemRoot%₩System32₩config₩systemprofile₩ntuser.dat
SetupAPI Log	%SystemRoot%₩inf₩setupapi.dev.log
IconCache	%UserProfile%₩AppData₩Local₩IconCache.유
Thumbnail Cache	%UserProfile%₩AppData₩Local₩Microsoft₩Windows₩Explorer₩thumbcache_32.db %UserProfile%₩AppData₩Local₩Microsoft₩Windows₩Explorer₩thumbcache_96.db %UserProfile%₩AppData₩Local₩Microsoft₩Windows₩Explorer₩thumbcache_256.유 %UserProfile%₩AppData₩Local₩Microsoft₩Windows₩Explorer₩thumbcache_1024.db

타임라인 분석 실전

➔ 실습

- WinHex를 이용해 수동으로 포렌식 아티팩트 추출하기!!

Artifacts	Path
Internet Explorer	%UserProfile%₩AppData₩Local₩Microsoft₩Windows₩History₩* %UserProfile%₩AppData₩Local₩Microsoft₩Windws₩Temporary Internet Files₩* %UserProfile%₩AppData₩Roaming₩Microsoft₩Windows₩Cookies₩* %UserProfile%₩AppData₩Roaming₩Microsoft₩Windows₩IEDownloadHistory₩* %UserProfile%₩AppData₩Local₩Microsoft₩Windws₩WebCache₩WebCacheV01.dat (IE10+)
Chrome	%UserProfile%₩AppData₩Local₩Google₩Chrome₩User Data₩Default₩Cache₩data_0 %UserProfile%₩AppData₩Local₩Google₩Chrome₩User Data₩Default₩Cache₩data_1 %UserProfile%₩AppData₩Local₩Google₩Chrome₩User Data₩Default₩Cache₩data_2 %UserProfile%₩AppData₩Local₩Google₩Chrome₩User Data₩Default₩Cache₩data_3 %UserProfile%₩AppData₩Local₩Google₩Chrome₩User Data₩Default₩Cookies %UserProfile%₩AppData₩Local₩Google₩Chrome₩User Data₩Default₩History

타임라인 분석 실전

- log2timeline_mod

1. 타임라인 생성

```
$> perl  log2timeline_mod  -z  Asia/Seoul  -r  -p  -w  timeline.txt  “d:₩artifacts₩”
```

2. 시간 순 정렬

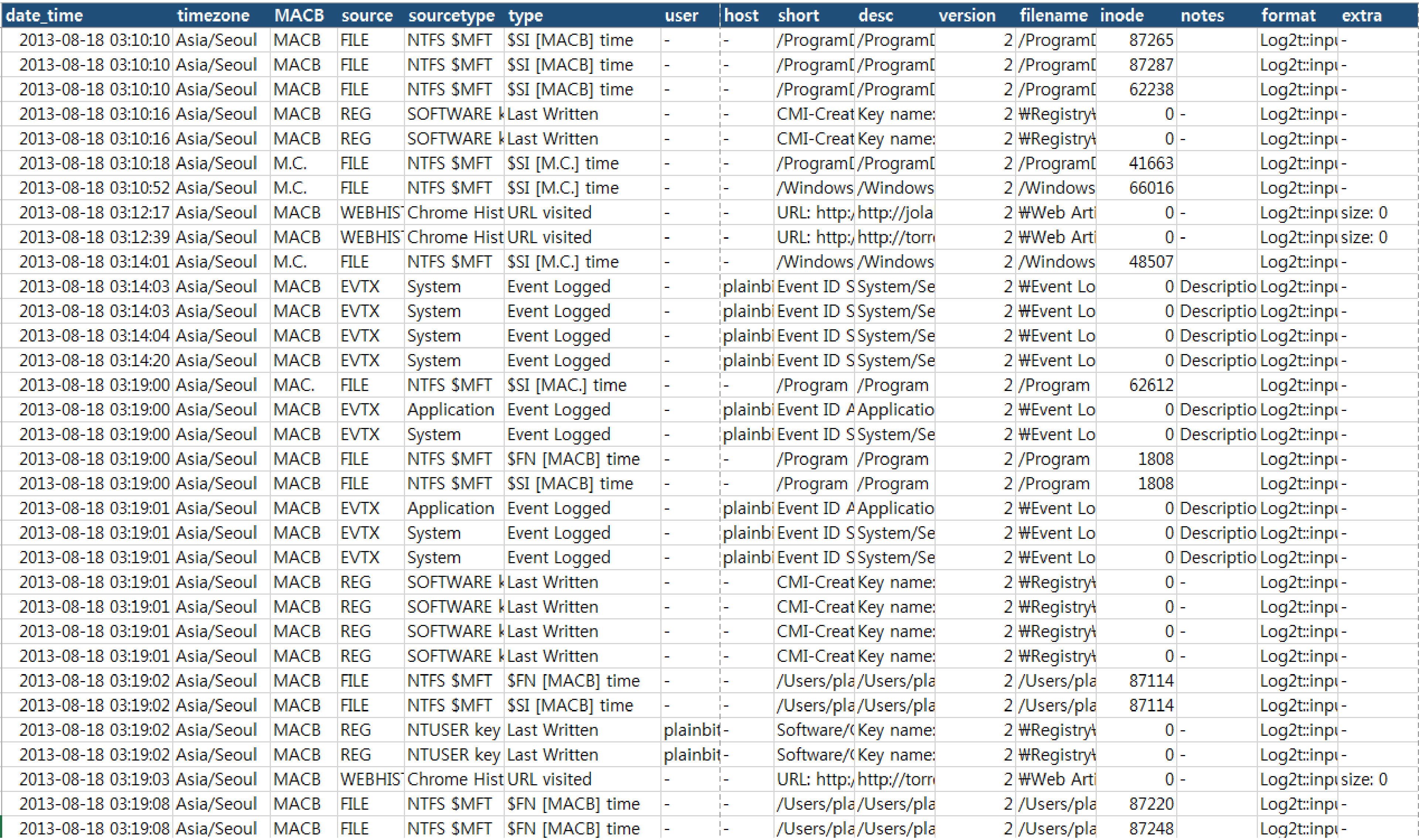
```
$> python  log2_sort.py  -i  <input file>  -o  <output file>  -n  <line number>
```

```
$> python  log2_sort.py  -i  timeline.txt  -o  timeline_sort.csv  -n  200000
```

3. TIMELINE_COLOR_TEMPLATE을 이용해 로드

   ✓ http://computer-forensics.sans.org/blog/2011/12/07/digital-forensic-sifting-super-timeline-analysis-and-creation

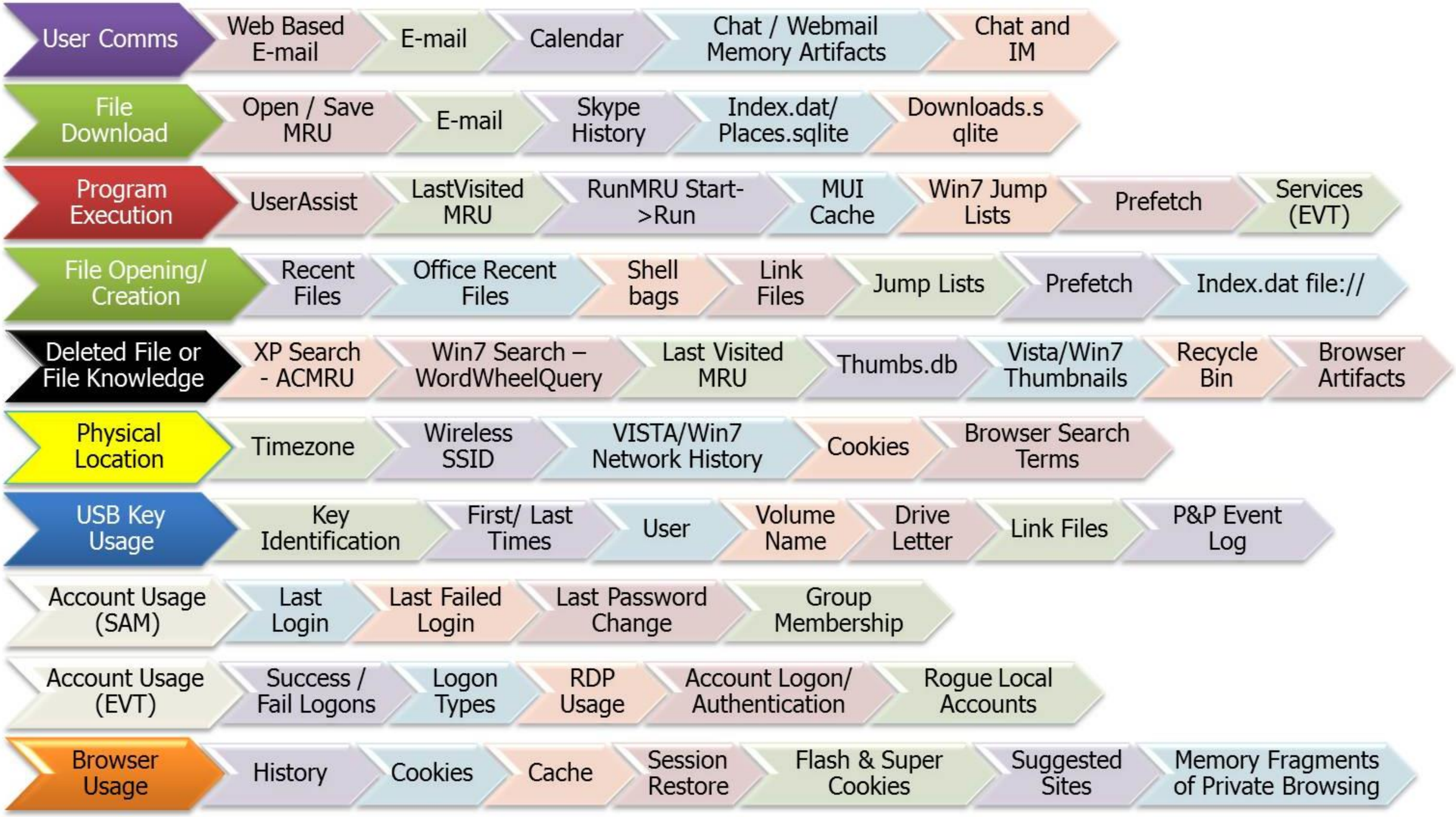
타임라인 분석 실전



date_time	timezone	MACB	source	sourcetype	type	user	host	short	desc	version	filename	inode	notes	format	extra
2013-08-18 03:10:10	Asia/Seoul	MACB	FILE	NTFS $MFT	$SI [MACB] time	-	-	/ProgramD	/ProgramD	2	/ProgramD	87265		Log2t::inpu	-
2013-08-18 03:10:10	Asia/Seoul	MACB	FILE	NTFS $MFT	$SI [MACB] time	-	-	/ProgramD	/ProgramD	2	/ProgramD	87287		Log2t::inpu	-
2013-08-18 03:10:10	Asia/Seoul	MACB	FILE	NTFS $MFT	$SI [MACB] time	-	-	/ProgramD	/ProgramD	2	/ProgramD	62238		Log2t::inpu	-
2013-08-18 03:10:16	Asia/Seoul	MACB	REG	SOFTWARE k	Last Written	-	-	CMI-Creat	Key name:	2	₩Registry₩	0	-	Log2t::inpu	-
2013-08-18 03:10:16	Asia/Seoul	MACB	REG	SOFTWARE k	Last Written	-	-	CMI-Creat	Key name:	2	₩Registry₩	0	-	Log2t::inpu	-
2013-08-18 03:10:18	Asia/Seoul	M.C.	FILE	NTFS $MFT	$SI [M.C.] time	-	-	/ProgramD	/ProgramD	2	/ProgramD	41663		Log2t::inpu	-
2013-08-18 03:10:52	Asia/Seoul	M.C.	FILE	NTFS $MFT	$SI [M.C.] time	-	-	/Windows	/Windows	2	/Windows	66016		Log2t::inpu	-
2013-08-18 03:12:17	Asia/Seoul	MACB	WEBHIS	Chrome Hist	URL visited	-	-	URL: http:/	http://jola	2	₩Web Arti	0	-	Log2t::inpu	size: 0
2013-08-18 03:12:39	Asia/Seoul	MACB	WEBHIS	Chrome Hist	URL visited	-	-	URL: http:/	http://torr	2	₩Web Arti	0	-	Log2t::inpu	size: 0
2013-08-18 03:14:01	Asia/Seoul	M.C.	FILE	NTFS $MFT	$SI [M.C.] time	-	-	/Windows	/Windows	2	/Windows	48507		Log2t::inpu	-
2013-08-18 03:14:03	Asia/Seoul	MACB	EVTX	System	Event Logged	-	plainbi	Event ID S	System/Se	2	₩Event Lo	0	Descriptio	Log2t::inpu	-
2013-08-18 03:14:03	Asia/Seoul	MACB	EVTX	System	Event Logged	-	plainbi	Event ID S	System/Se	2	₩Event Lo	0	Descriptio	Log2t::inpu	-
2013-08-18 03:14:04	Asia/Seoul	MACB	EVTX	System	Event Logged	-	plainbi	Event ID S	System/Se	2	₩Event Lo	0	Descriptio	Log2t::inpu	-
2013-08-18 03:14:20	Asia/Seoul	MACB	EVTX	System	Event Logged	-	plainbi	Event ID S	System/Se	2	₩Event Lo	0	Descriptio	Log2t::inpu	-
2013-08-18 03:19:00	Asia/Seoul	MAC.	FILE	NTFS $MFT	$SI [MAC.] time	-	-	/Program	/Program	2	/Program	62612		Log2t::inpu	-
2013-08-18 03:19:00	Asia/Seoul	MACB	EVTX	Application	Event Logged	-	plainbi	Event ID A	Applicatio	2	₩Event Lo	0	Descriptio	Log2t::inpu	-
2013-08-18 03:19:00	Asia/Seoul	MACB	EVTX	System	Event Logged	-	plainbi	Event ID S	System/Se	2	₩Event Lo	0	Descriptio	Log2t::inpu	-
2013-08-18 03:19:00	Asia/Seoul	MACB	FILE	NTFS $MFT	$FN [MACB] time	-	-	/Program	/Program	2	/Program	1808		Log2t::inpu	-
2013-08-18 03:19:00	Asia/Seoul	MACB	FILE	NTFS $MFT	$SI [MACB] time	-	-	/Program	/Program	2	/Program	1808		Log2t::inpu	-
2013-08-18 03:19:01	Asia/Seoul	MACB	EVTX	Application	Event Logged	-	plainbi	Event ID A	Applicatio	2	₩Event Lo	0	Descriptio	Log2t::inpu	-
2013-08-18 03:19:01	Asia/Seoul	MACB	EVTX	System	Event Logged	-	plainbi	Event ID S	System/Se	2	₩Event Lo	0	Descriptio	Log2t::inpu	-
2013-08-18 03:19:01	Asia/Seoul	MACB	EVTX	System	Event Logged	-	plainbi	Event ID S	System/Se	2	₩Event Lo	0	Descriptio	Log2t::inpu	-
2013-08-18 03:19:01	Asia/Seoul	MACB	REG	SOFTWARE k	Last Written	-	-	CMI-Creat	Key name:	2	₩Registry₩	0	-	Log2t::inpu	-
2013-08-18 03:19:01	Asia/Seoul	MACB	REG	SOFTWARE k	Last Written	-	-	CMI-Creat	Key name:	2	₩Registry₩	0	-	Log2t::inpu	-
2013-08-18 03:19:01	Asia/Seoul	MACB	REG	SOFTWARE k	Last Written	-	-	CMI-Creat	Key name:	2	₩Registry₩	0	-	Log2t::inpu	-
2013-08-18 03:19:01	Asia/Seoul	MACB	REG	SOFTWARE k	Last Written	-	-	CMI-Creat	Key name:	2	₩Registry₩	0	-	Log2t::inpu	-
2013-08-18 03:19:02	Asia/Seoul	MACB	FILE	NTFS $MFT	$FN [MACB] time	-	-	/Users/pla	/Users/pla	2	/Users/pla	87114		Log2t::inpu	-
2013-08-18 03:19:02	Asia/Seoul	MACB	FILE	NTFS $MFT	$SI [MACB] time	-	-	/Users/pla	/Users/pla	2	/Users/pla	87114		Log2t::inpu	-
2013-08-18 03:19:02	Asia/Seoul	MACB	REG	NTUSER key	Last Written	plainbit	-	Software/(	Key name:	2	₩Registry₩	0	-	Log2t::inpu	-
2013-08-18 03:19:02	Asia/Seoul	MACB	REG	NTUSER key	Last Written	plainbit	-	Software/(	Key name:	2	₩Registry₩	0	-	Log2t::inpu	-
2013-08-18 03:19:03	Asia/Seoul	MACB	WEBHIS	Chrome Hist	URL visited	-	-	URL: http:/	http://torr	2	₩Web Arti	0	-	Log2t::inpu	size: 0
2013-08-18 03:19:08	Asia/Seoul	MACB	FILE	NTFS $MFT	$FN [MACB] time	-	-	/Users/pla	/Users/pla	2	/Users/pla	87220		Log2t::inpu	-
2013-08-18 03:19:08	Asia/Seoul	MACB	FILE	NTFS $MFT	$FN [MACB] time	-	-	/Users/pla	/Users/pla	2	/Users/pla	87248		Log2t::inpu	-

타임라인 분석 실전

- **TIMELINE_COLOR_TEMPLATE**



User Comms | Web Based E-mail | E-mail | Calendar | Chat / Webmail Memory Artifacts | Chat and IM

File Download | Open / Save MRU | E-mail | Skype History | Index.dat/ Places.sqlite | Downloads.sqlite

Program Execution | UserAssist | LastVisited MRU | RunMRU Start->Run | MUI Cache | Win7 Jump Lists | Prefetch | Services (EVT)

File Opening/ Creation | Recent Files | Office Recent Files | Shell bags | Link Files | Jump Lists | Prefetch | Index.dat file://

Deleted File or File Knowledge | XP Search - ACMRU | Win7 Search – WordWheelQuery | Last Visited MRU | Thumbs.db | Vista/Win7 Thumbnails | Recycle Bin | Browser Artifacts

Physical Location | Timezone | Wireless SSID | VISTA/Win7 Network History | Cookies | Browser Search Terms

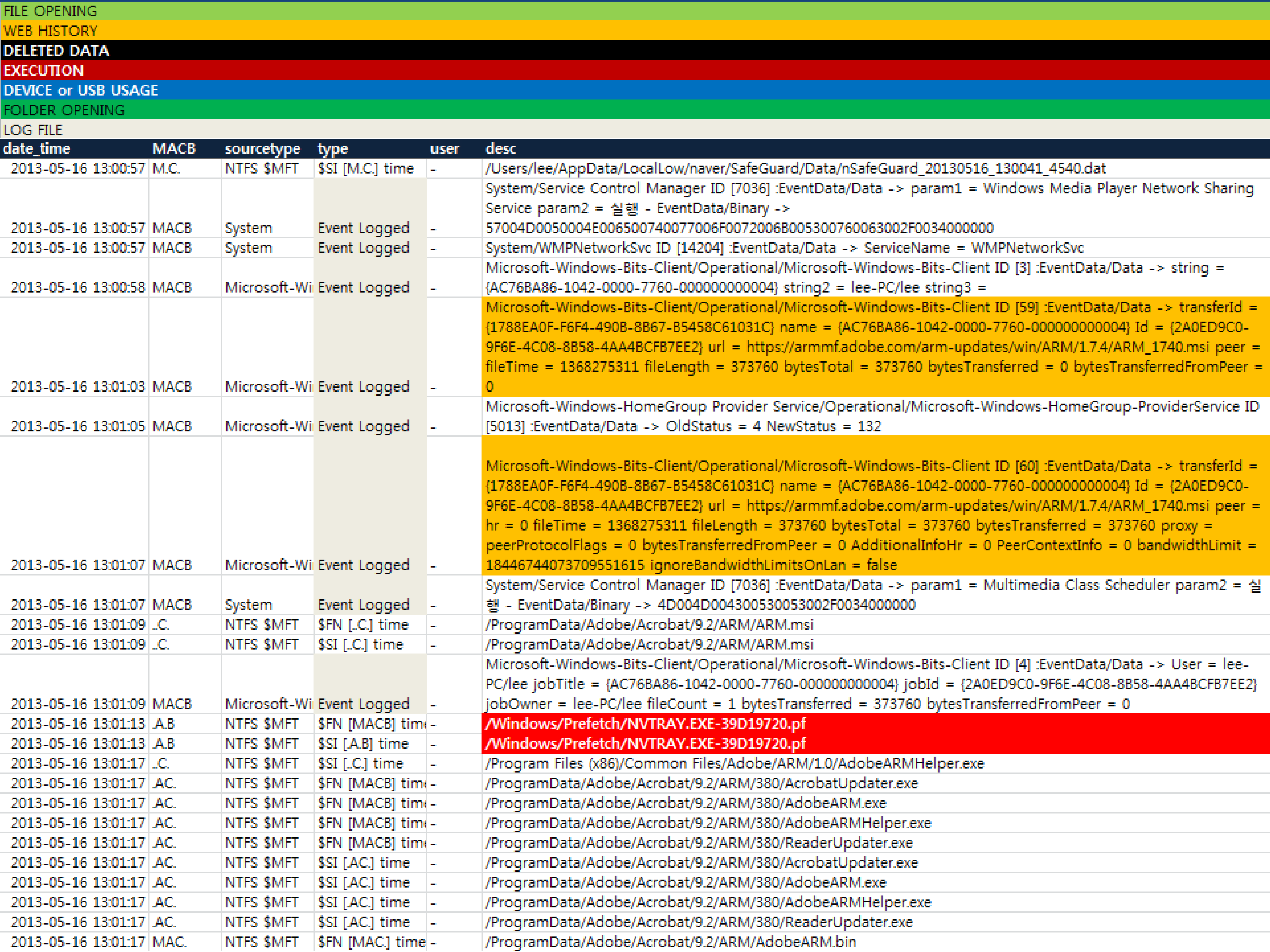
USB Key Usage | Key Identification | First/ Last Times | User | Volume Name | Drive Letter | Link Files | P&P Event Log

Account Usage (SAM) | Last Login | Last Failed Login | Last Password Change | Group Membership

Account Usage (EVT) | Success / Fail Logons | Logon Types | RDP Usage | Account Logon/ Authentication | Rogue Local Accounts

Browser Usage | History | Cookies | Cache | Session Restore | Flash & Super Cookies | Suggested Sites | Memory Fragments of Private Browsing

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



FILE OPENING

WEB HISTORY

DELETED DATA

EXECUTION

DEVICE or USB USAGE

FOLDER OPENING

LOG FILE

date_time	MACB	sourcetype	type	user	desc
2013-05-16 13:00:57	M.C.	NTFS $MFT	$SI [M.C.] time	-	/Users/lee/AppData/LocalLow/naver/SafeGuard/Data/nSafeGuard_20130516_130041_4540.dat
2013-05-16 13:00:57	MACB	System	Event Logged	-	System/Service Control Manager ID [7036] :EventData/Data -> param1 = Windows Media Player Network Sharing Service param2 = 실행 - EventData/Binary -> 57004D0050004E006500740077006F0072006B005300760063002F0034000000
2013-05-16 13:00:57	MACB	System	Event Logged	-	System/WMPNetworkSvc ID [14204] :EventData/Data -> ServiceName = WMPNetworkSvc
2013-05-16 13:00:58	MACB	Microsoft-Wi	Event Logged	-	Microsoft-Windows-Bits-Client/Operational/Microsoft-Windows-Bits-Client ID [3] :EventData/Data -> string = {AC76BA86-1042-0000-7760-000000000004} string2 = lee-PC/lee string3 =
2013-05-16 13:01:03	MACB	Microsoft-Wi	Event Logged	-	Microsoft-Windows-Bits-Client/Operational/Microsoft-Windows-Bits-Client ID [59] :EventData/Data -> transferId = {1788EA0F-F6F4-490B-8B67-B5458C61031C} name = {AC76BA86-1042-0000-7760-000000000004} Id = {2A0ED9C0-9F6E-4C08-8B58-4AA4BCFB7EE2} url = https://armmf.adobe.com/arm-updates/win/ARM/1.7.4/ARM_1740.msi peer = fileTime = 1368275311 fileLength = 373760 bytesTotal = 373760 bytesTransferred = 0 bytesTransferredFromPeer = 0
2013-05-16 13:01:05	MACB	Microsoft-Wi	Event Logged	-	Microsoft-Windows-HomeGroup Provider Service/Operational/Microsoft-Windows-HomeGroup-ProviderService ID [5013] :EventData/Data -> OldStatus = 4 NewStatus = 132
2013-05-16 13:01:07	MACB	Microsoft-Wi	Event Logged	-	Microsoft-Windows-Bits-Client/Operational/Microsoft-Windows-Bits-Client ID [60] :EventData/Data -> transferId = {1788EA0F-F6F4-490B-8B67-B5458C61031C} name = {AC76BA86-1042-0000-7760-000000000004} Id = {2A0ED9C0-9F6E-4C08-8B58-4AA4BCFB7EE2} url = https://armmf.adobe.com/arm-updates/win/ARM/1.7.4/ARM_1740.msi peer = hr = 0 fileTime = 1368275311 fileLength = 373760 bytesTotal = 373760 bytesTransferred = 373760 proxy = peerProtocolFlags = 0 bytesTransferredFromPeer = 0 AdditionalInfoHr = 0 PeerContextInfo = 0 bandwidthLimit = 18446744073709551615 ignoreBandwidthLimitsOnLan = false
2013-05-16 13:01:07	MACB	System	Event Logged	-	System/Service Control Manager ID [7036] :EventData/Data -> param1 = Multimedia Class Scheduler param2 = 실행 - EventData/Binary -> 4D004D0043005300530053002F0034000000
2013-05-16 13:01:09	..C.	NTFS $MFT	$FN [..C.] time	-	/ProgramData/Adobe/Acrobat/9.2/ARM/ARM.msi
2013-05-16 13:01:09	..C.	NTFS $MFT	$SI [..C.] time	-	/ProgramData/Adobe/Acrobat/9.2/ARM/ARM.msi
2013-05-16 13:01:09	MACB	Microsoft-Wi	Event Logged	-	Microsoft-Windows-Bits-Client/Operational/Microsoft-Windows-Bits-Client ID [4] :EventData/Data -> User = lee-PC/lee jobTitle = {AC76BA86-1042-0000-7760-000000000004} jobId = {2A0ED9C0-9F6E-4C08-8B58-4AA4BCFB7EE2} jobOwner = lee-PC/lee fileCount = 1 bytesTransferred = 373760 bytesTransferredFromPeer = 0
2013-05-16 13:01:13	.A.B	NTFS $MFT	$FN [MACB] tim	-	/Windows/Prefetch/NVTRAY.EXE-39D19720.pf
2013-05-16 13:01:13	.A.B	NTFS $MFT	$SI [.A.B] time	-	/Windows/Prefetch/NVTRAY.EXE-39D19720.pf
2013-05-16 13:01:17	..C.	NTFS $MFT	$SI [..C.] time	-	/Program Files (x86)/Common Files/Adobe/ARM/1.0/AdobeARMHelper.exe
2013-05-16 13:01:17	.AC.	NTFS $MFT	$FN [MACB] tim	-	/ProgramData/Adobe/Acrobat/9.2/ARM/380/AcrobatUpdater.exe
2013-05-16 13:01:17	.AC.	NTFS $MFT	$FN [MACB] tim	-	/ProgramData/Adobe/Acrobat/9.2/ARM/380/AdobeARM.exe
2013-05-16 13:01:17	.AC.	NTFS $MFT	$FN [MACB] tim	-	/ProgramData/Adobe/Acrobat/9.2/ARM/380/AdobeARMHelper.exe
2013-05-16 13:01:17	.AC.	NTFS $MFT	$FN [MACB] tim	-	/ProgramData/Adobe/Acrobat/9.2/ARM/380/ReaderUpdater.exe
2013-05-16 13:01:17	.AC.	NTFS $MFT	$SI [.AC.] time	-	/ProgramData/Adobe/Acrobat/9.2/ARM/380/AcrobatUpdater.exe
2013-05-16 13:01:17	.AC.	NTFS $MFT	$SI [.AC.] time	-	/ProgramData/Adobe/Acrobat/9.2/ARM/380/AdobeARM.exe
2013-05-16 13:01:17	.AC.	NTFS $MFT	$SI [.AC.] time	-	/ProgramData/Adobe/Acrobat/9.2/ARM/380/AdobeARMHelper.exe
2013-05-16 13:01:17	.AC.	NTFS $MFT	$SI [.AC.] time	-	/ProgramData/Adobe/Acrobat/9.2/ARM/380/ReaderUpdater.exe
2013-05-16 13:01:17	MAC.	NTFS $MFT	$FN [MAC.] time	-	/ProgramData/Adobe/Acrobat/9.2/ARM/AdobeARM.bin

타임라인 분석 실전

➔ 실습

- log2timeline을 이용해 수집한 아티팩트로 타임라인 생성하기!!

타임라인 분석 실전

➔ 실습

- log2timeline을 이용해 샘플 아티팩트로 타임라인 생성하기!!

타임라인 분석 실전

- **log2timeline**
  - **특징**
    - ✓ 펄로 작성
    - ✓ 아티팩트별 독립된 모듈
    - ✓ 단일 쓰레드 사용
  - **한계**
    - ✓ 초 단위의 시간 정밀도 사용
    - ✓ 파일 단위로 작업 수행 ➔ 이미지 처리를 위해서는 별도의 전처리 작업 수행
    - ✓ 텍스트 형식의 출력
    - ✓ 새로운 기능 추가를 위해 많은 노력 필요
    - ✓ 필터나 사후 처리 기능이 매우 빈약
    - ✓ 한글 처리의 한계
    - ✓ 시간 형식의 차이 (년-월-일 <-> 월/일/년)

타임라인 분석 실전

- **Plaso** (https://code.google.com/p/plaso/)

타임라인 분석 실전

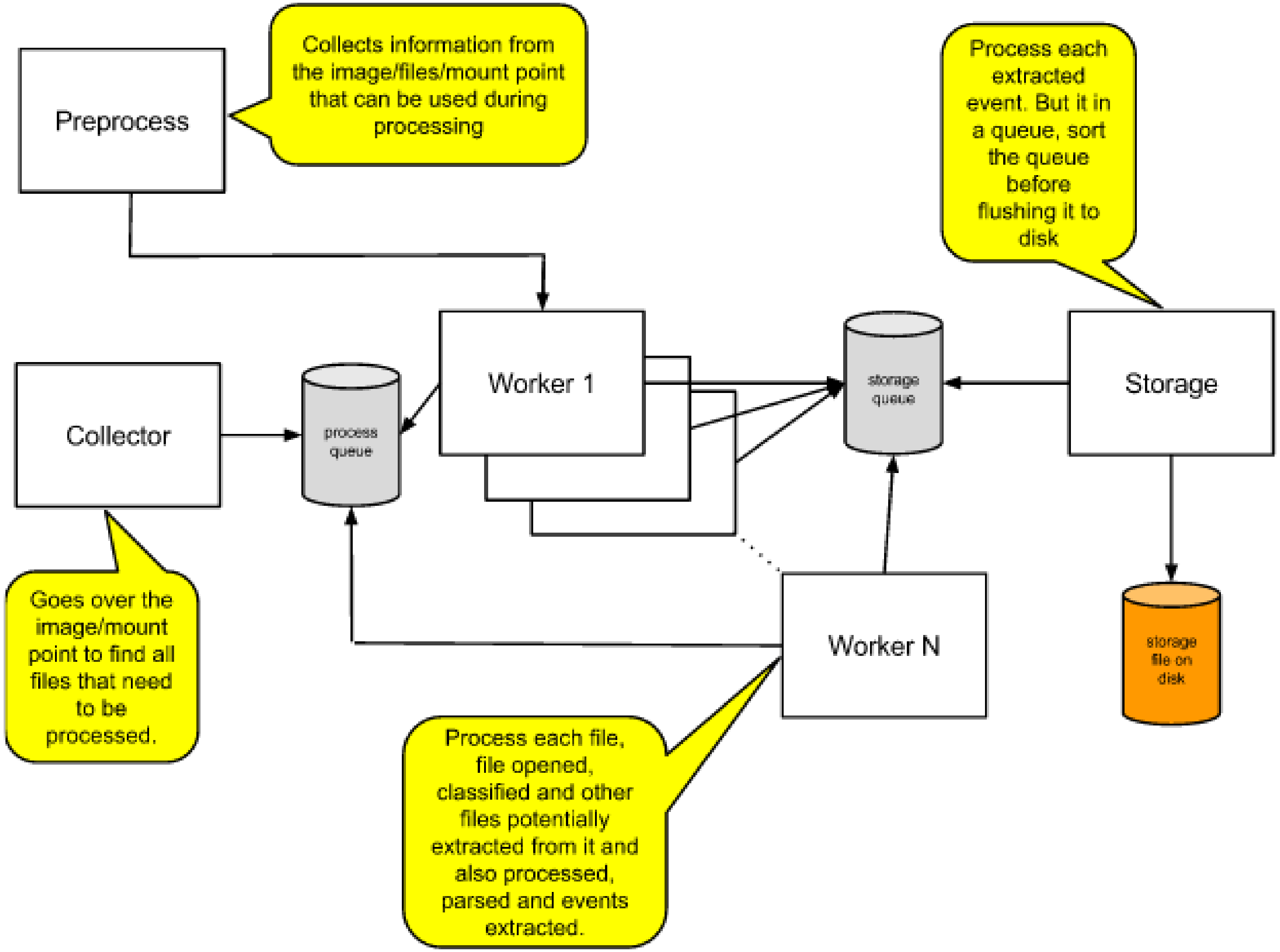
- **Plaso**
  - **구글 소프트웨어 개발자에 의해 log2timeline을 강화**
  - **전반부는 log2timeline 이용**
  - **실행 및 후반부 기능 강화**
    - ✓ 멀티 쓰레딩 추가
    - ✓ 이미지 파일 파싱
    - ✓ VSS 파싱
    - ✓ 태그 기능 추가
    - ✓ 필터 기능 추가
    - ✓ 선별 수집 기능 추가

타임라인 분석 실전

- **Plaso, 도구**
  - **log2timeline**
    - ✓ 타임라인 추출
  - **psort (Plaso Sort)**
    - ✓ 사후 처리 (Post Processing)
  - **plasm (Plaso Langar Að Safna Minna)**
    - ✓ 태깅 (Tagging)
  - **pinfo (Plaso Information)**
    - ✓ 스토리지 정보(메타데이터) 확인
  - **preg (Plaso Registry)**
    - ✓ 레지스트리 파싱 도구
  - **pprof (Plaso Profiler)**
    - ✓ 프로파일 파싱 도구

타임라인 분석 실전

- **Plaso, 구조**


Preprocess
Collects information from the image/files/mount point that can be used during processing
Process each extracted event. But it in a queue, sort the queue before flushing it to disk
Worker 1
storage queue
Storage
Collector
process queue
Worker N
storage file on disk
Goes over the image/mount point to find all files that need to be processed.
Process each file, file opened, classified and other files potentially extracted from it and also processed, parsed and events extracted.

타임라인 분석 실전

- **Plaso, 도구**
  - **Preprocessing**
    - ✓ 모든 기능 중 가장 먼저 수행
    - ✓ 타임존, 사용자 경로, 호스트명, 응용프로그램 목록, 레지스트리 설정 등을 확인하는 기능
  - **Collection**
    - ✓ 이미지, 디렉터리, 마운트 위치 등에서 필요한 정보만 수집 (VSS 수집 기능 포함)
  - **Worker**
    - ✓ 메인 작업으로 파싱과 정형화 등을 담당
  - **Storage**
    - ✓ 처리된 데이터를 구조적으로 저장한 파일

타임라인 분석 실전

Plaso, 실행

- 지원 옵션

```
usage: log2timeline.exe [-z TZONE] [-t TEXT] [--parsers PARSER_LIST] [-h]
                        [--logfile FILENAME] [-p] [--buffer_size BUFFER_SIZE]
                        [--workers WORKERS] [-i] [--vss]
                        [--vss_stores VSS_STORES] [--single_thread]
                        [-f FILE_FILTER] [-o IMAGE_OFFSET]
                        [--ob IMAGE_OFFSET_BYTES] [-v] [--info]
                        [--partition_map] [--sector_size BYTES_PER_SECTOR]
                        [--partition PARTITION_NUMBER] [--use_old_preprocess]
                        [--output OUTPUT_MODULE] [-d]
                        [STORAGE_FILE] [FILENAME_OR_MOUNT_POINT] [FILTER]
```

- 이미지 실행

```
$> log2timeline.exe [-z TIMEZONE] [-f filterfile] [--parsers PARSER_LIST] -i [-o OFFSET] [--vss]
/path/to/output.dump /path/to/image.dd ["FILTER"]
```

- 마운트 위치 실행

```
$> log2timeline.exe [-z TIMEZONE] -p /path/to/output.dump /path/to/dir/or/mount_point
```

타임라인 분석 실전

Plaso, 실행

타임라인 생성

```
$> log2timeline.exe  -o  63  /cases/storage.dump  /cases/evil.dd
```

- ✓ **-o :** 볼륨의 시작 섹터
- ✓ **storage.dump :** 스토리지 파일
- ✓ **Evil.dd :** 케이스 이미지

```
$> log2timeline.exe  -p /cases/storage.dump  C:₩
```

- ✓ **-p :** 사전처리(Preprocessing)
- ✓ **C:₩** : 마운트 위치

타임라인 분석 실전

Plaso, 선별 수집

- 선별 수집 예

```
$> log2timeline.exe -i -f browser_filter.txt history.dump /mnt/e01/ewf1
```

```
/(Users|Documents And Settings)/.+/AppData/Local/Google/Chrome/.+/History
/(Users|Documents And Settings)/.+/Local Settings/Application Data/Google/Chrome/.+/History
/Users/.+/AppData/Local/Microsoft/Windows/History/History.IE5/index.dat
/Users/.+/AppData/Local/Microsoft/Windows/History/History.IE5/MSHist.+/index.dat
/Users/.+/AppData/Local/Microsoft/Windows/History/Low/History.IE5/index.dat
/Users/.+/AppData/Local/Microsoft/Windows/History/Low/History.IE5/MSHist.+/index.dat
/Users/.+/AppData/Local/Microsoft/Windows/Temporary Internet Files/Content.IE5/index.dat
/Users/.+/AppData/Local/Microsoft/Windows/Temporary Internet Files/Low/Content.IE5/index.dat
/Users/.+/AppData/Roaming/Microsoft/Windows/Cookies/index.dat
/Users/.+/AppData/Roaming/Microsoft/Windows/Cookies/Low/index.dat
/Documents And Settings/.+/Local Settings/History/History.IE5/index.dat
/Documents And Settings/.+/Local Settings/Temporary Internet Files/Content.IE5/index.dat
/Documents And Settings/.+/Cookies/index.dat
/(Users|Documents And Settings)/.+/AppData/Roaming/Mozilla/Firefox/Profiles/.+/places.sqlite
/(Users|Documents And Settings)/.+/Local Settings/Application Data/Mozilla/Firefox/Profiles/.+/places.sqlite
```

타임라인 분석 실전

Plaso, 필터

- **필터 사용법**

```
$> psort [options] "filter"
```

```
$> log2timeline [options] file/image/mount_point/dir "filter"
```

- **필터 예제**

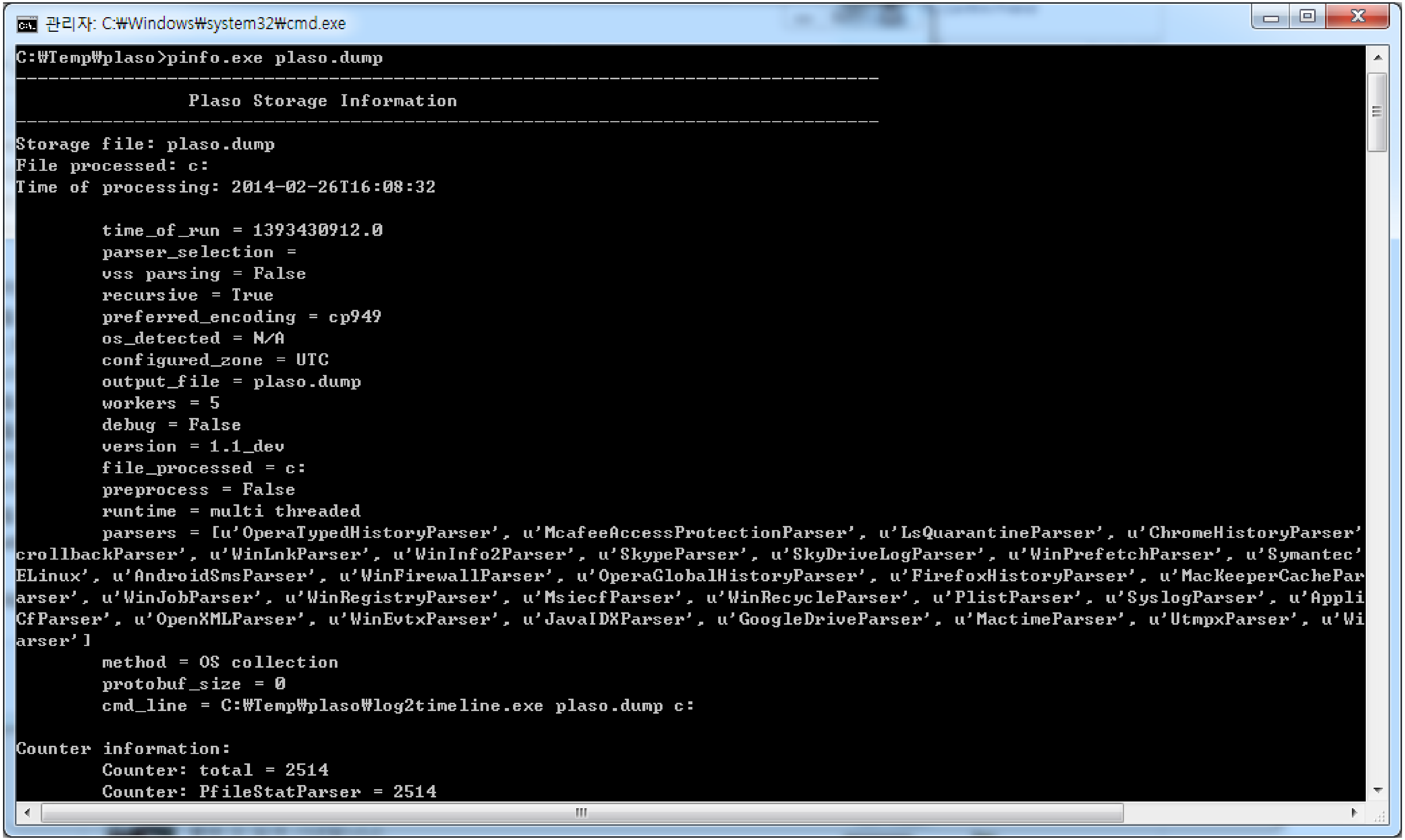
```
"parser is 'SyslogParser' and message contains 'root'"
```

```
"source_short is 'LOG' AND (timestamp_desc CONTAINS 'written' OR timestamp_desc CONTAINS
'visited')"
```

```
"parser contains 'firefox' AND pathspec.vss_store_number > 0"
```

타임라인 분석 실전

- **Plaso, 스토리지 정보 ➔ pinfo**



```
C:₩Temp₩plaso>pinfo.exe plaso.dump
--------------------------------------------------------------------------------
                Plaso Storage Information
--------------------------------------------------------------------------------
Storage file: plaso.dump
File processed: c:
Time of processing: 2014-02-26T16:08:32

        time_of_run = 1393430912.0
        parser_selection =
        vss parsing = False
        recursive = True
        preferred_encoding = cp949
        os_detected = N/A
        configured_zone = UTC
        output_file = plaso.dump
        workers = 5
        debug = False
        version = 1.1_dev
        file_processed = c:
        preprocess = False
        runtime = multi threaded
        parsers = [u'OperaTypedHistoryParser', u'McafeeAccessProtectionParser', u'LsQuarantineParser', u'ChromeHistoryParser'
crollbackParser', u'WinLnkParser', u'WinInfo2Parser', u'SkypeParser', u'SkyDriveLogParser', u'WinPrefetchParser', u'Symantec'
ELinux', u'AndroidSmsParser', u'WinFirewallParser', u'OperaGlobalHistoryParser', u'FirefoxHistoryParser', u'MacKeeperCachePar
arser', u'WinJobParser', u'WinRegistryParser', u'MsiecfParser', u'WinRecycleParser', u'PlistParser', u'SyslogParser', u'Appli
CfParser', u'OpenXMLParser', u'WinEvtxParser', u'JavaIDXParser', u'GoogleDriveParser', u'MactimeParser', u'UtmpxParser', u'Wi
arser']
        method = OS collection
        protobuf_size = 0
        cmd_line = C:₩Temp₩plaso₩log2timeline.exe plaso.dump c:

Counter information:
        Counter: total = 2514
        Counter: PfileStatParser = 2514
```

타임라인 분석 실전

Plaso, 스토리지 처리 ➔ psort

```
$> psort  storage.dump
```

```
$> psort  -o  [output module]  storage.dump  -w  “output”
```

- **Output module**
  - ✓ l2tcsv : log2timeline 형태의 csv 출력
  - ✓ dynamic : 각 필드 구분을 동적으로 선택할 수 있도록 출력
  - ✓ rawpy | raw : 모든 EventObject를 그대로 출력
  - ✓ sql4n6 : 4n6time의 SQLite 출력
  - ✓ pstorage : plaso 스토리지 파일 출력

타임라인 분석 실전

- **Plaso, 스토리지 처리 ➔ psort**

```
$> psort  -z  “Asia/Seoul”  –w  “output_sort.txt”  storage.dump  [FILTER]
```

- **FILTER**
  - ✓ psort.py -q sample_output "date > '2013-01-23 15:23:51' and date < '2013-01-23 21:42:13'”
  - ✓ psort.py -q --slice "2013-01-23 15:23:51" sample_output
  - ✓ psort.py -q sample_output.dump "date > '2012-01-01' AND tag contains 'Application Execution'”
  - ✓ psort.py -q --slice "2012-04-05 17:01:06" --slice_size 10 sample_output.dump
  - ✓ psort.py -q --slicer sample_output.dump "date > '2012-01-01' AND parser is 'WinJobParser'"

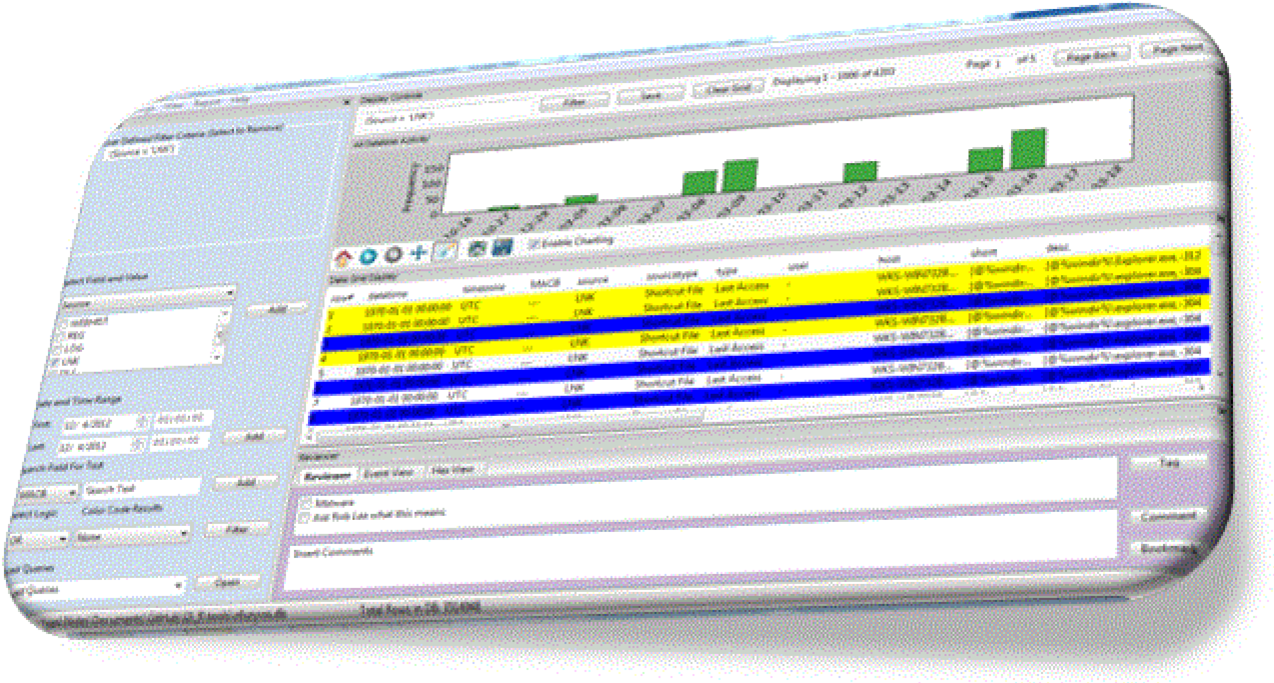
타임라인 분석 실전

- **4n6time** (https://code.google.com/p/plaso/)

Disclaimer: Requires the operation of a mouse

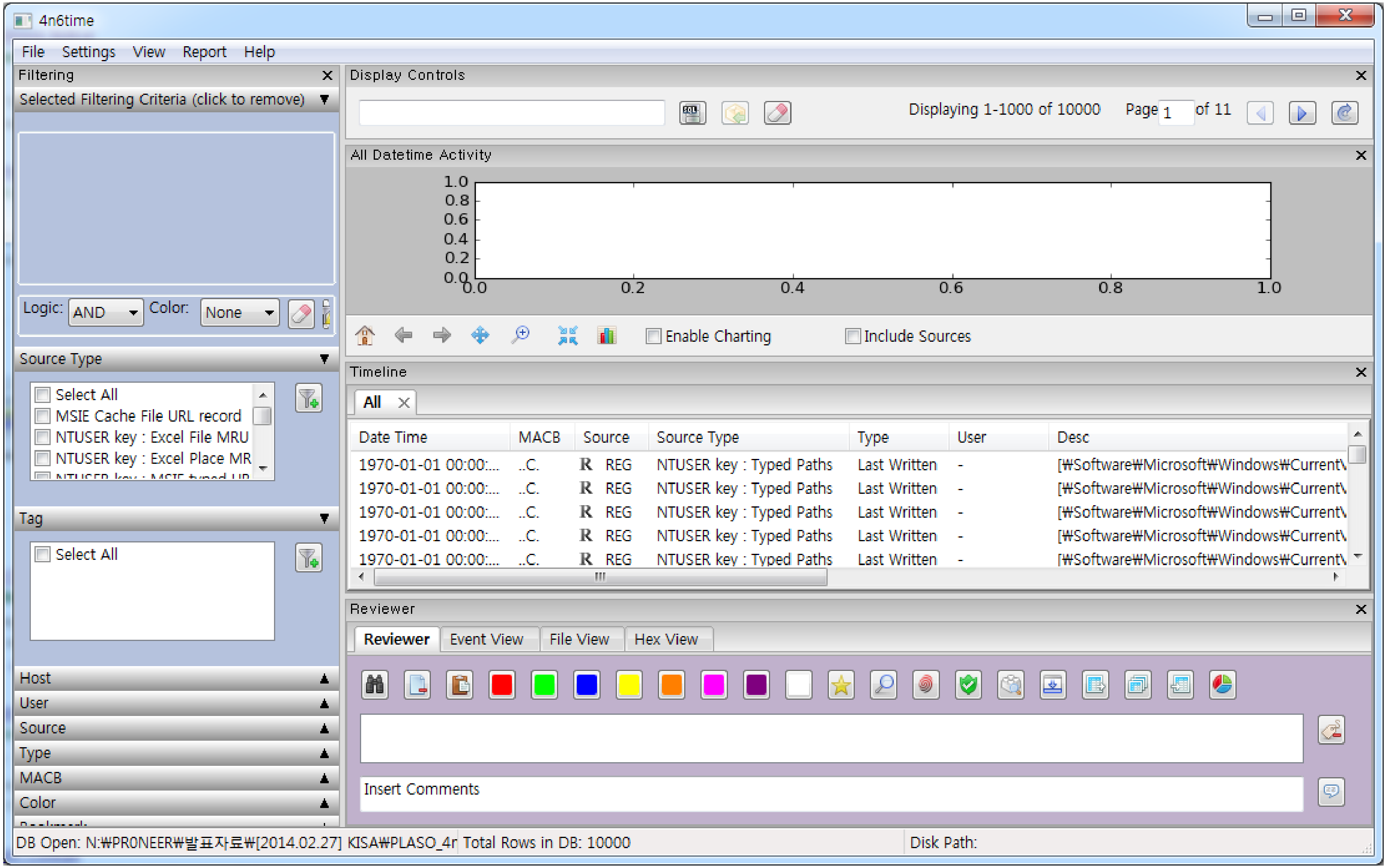
4n6time™

by david nides



타임라인 분석 실전

- **4n6time** (https://code.google.com/p/plaso/)



Displaying 1-1000 of 10000 Page 1 of 11

Logic: AND Color: None

□ Enable Charting □ Include Sources

□ Select All
□ MSIE Cache File URL record
□ NTUSER key : Excel File MRU
□ NTUSER key : Excel Place MR
□ NTUSER key : MSIE typed UR

□ Select All

Date Time	MACB	Source	Source Type	Type	User	Desc
1970-01-01 00:00:...	..C.	R REG	NTUSER key : Typed Paths	Last Written	-	[₩Software₩Microsoft₩Windows₩Current\
1970-01-01 00:00:...	..C.	R REG	NTUSER key : Typed Paths	Last Written	-	[₩Software₩Microsoft₩Windows₩Current\
1970-01-01 00:00:...	..C.	R REG	NTUSER key : Typed Paths	Last Written	-	[₩Software₩Microsoft₩Windows₩Current\
1970-01-01 00:00:...	..C.	R REG	NTUSER key : Typed Paths	Last Written	-	[₩Software₩Microsoft₩Windows₩Current\
1970-01-01 00:00:...	..C.	R REG	NTUSER key : Typed Paths	Last Written	-	[₩Software₩Microsoft₩Windows₩Current\

Insert Comments

DB Open: N:₩PR0NEER₩발표자료₩[2014.02.27] KISA₩PLASO_4r Total Rows in DB: 10000 Disk Path:

질문 및 답변