PLASO – 슈퍼 타임라인 분석 도구 활용 방안

proneer

proneer(at)gmail.com

forensic-proof.com

개요

1. 타임라인 분석 개요

2. log2timeline

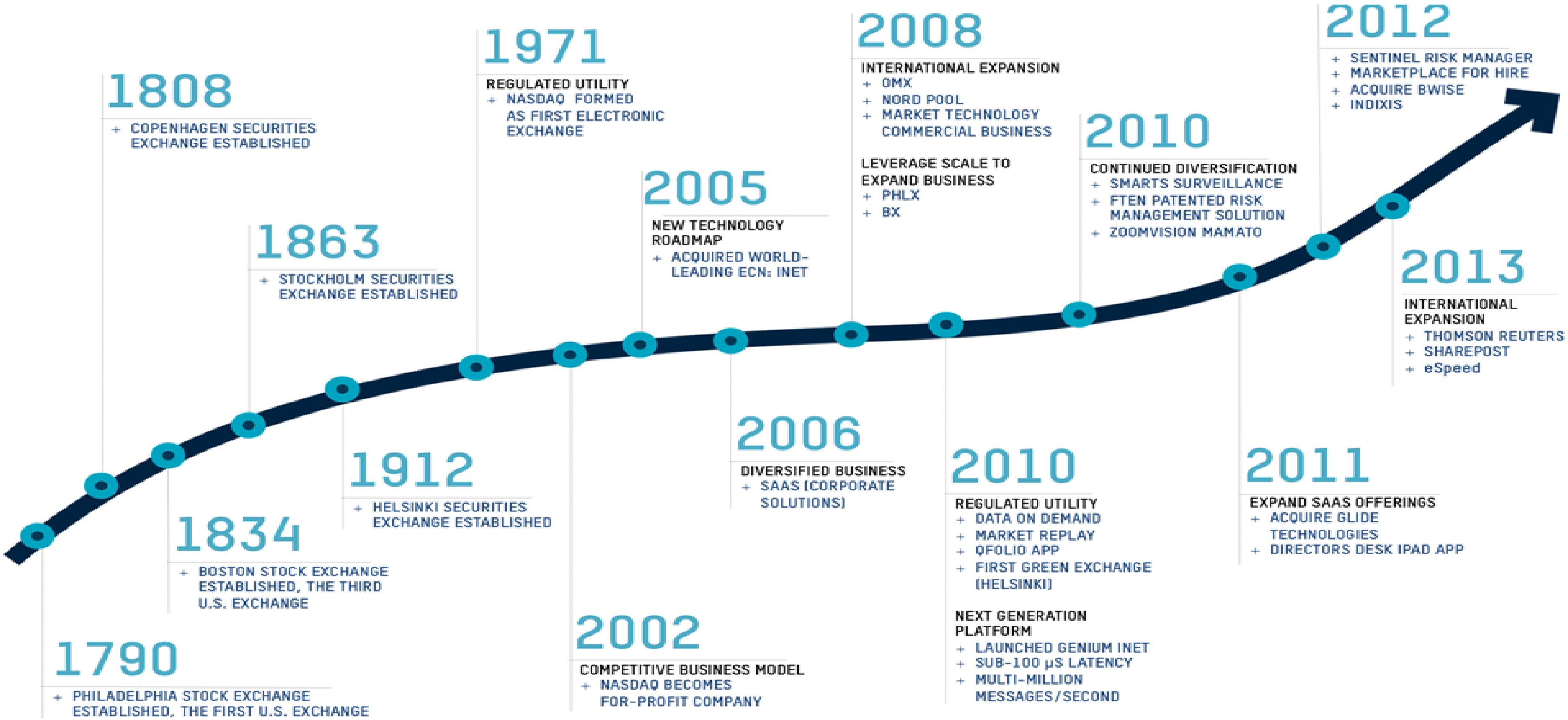
3. Plaso

타임라인 분석 개요

타임라인 분석 개요

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
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

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

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 개요

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 개요

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 개요

타임라인 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
- PE 파일의 컴파일 시간
- JPEG EXIF의 사진 촬영 시간
- … …

타임라인 분석 개요

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

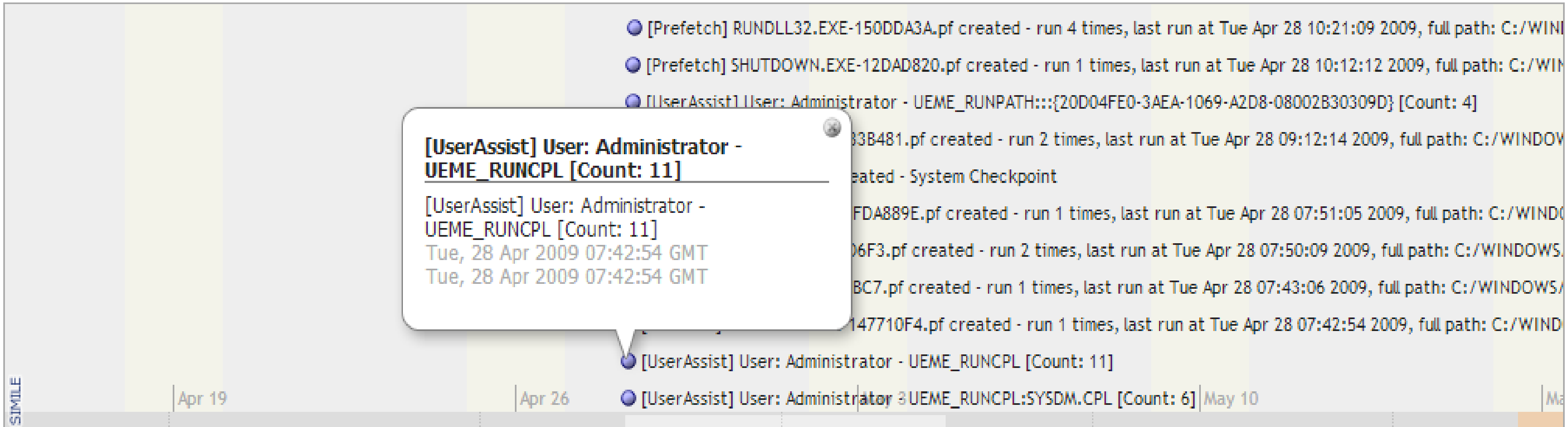
- **통합 타임라인 분석 도구**
  - **log2timeline** – http://log2timeline.net/
  - **Plaso** – http://plaso.kiddaland.net/

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 : Forensic4Cast 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:/WINI
[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]
3B481.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
6F3.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

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)

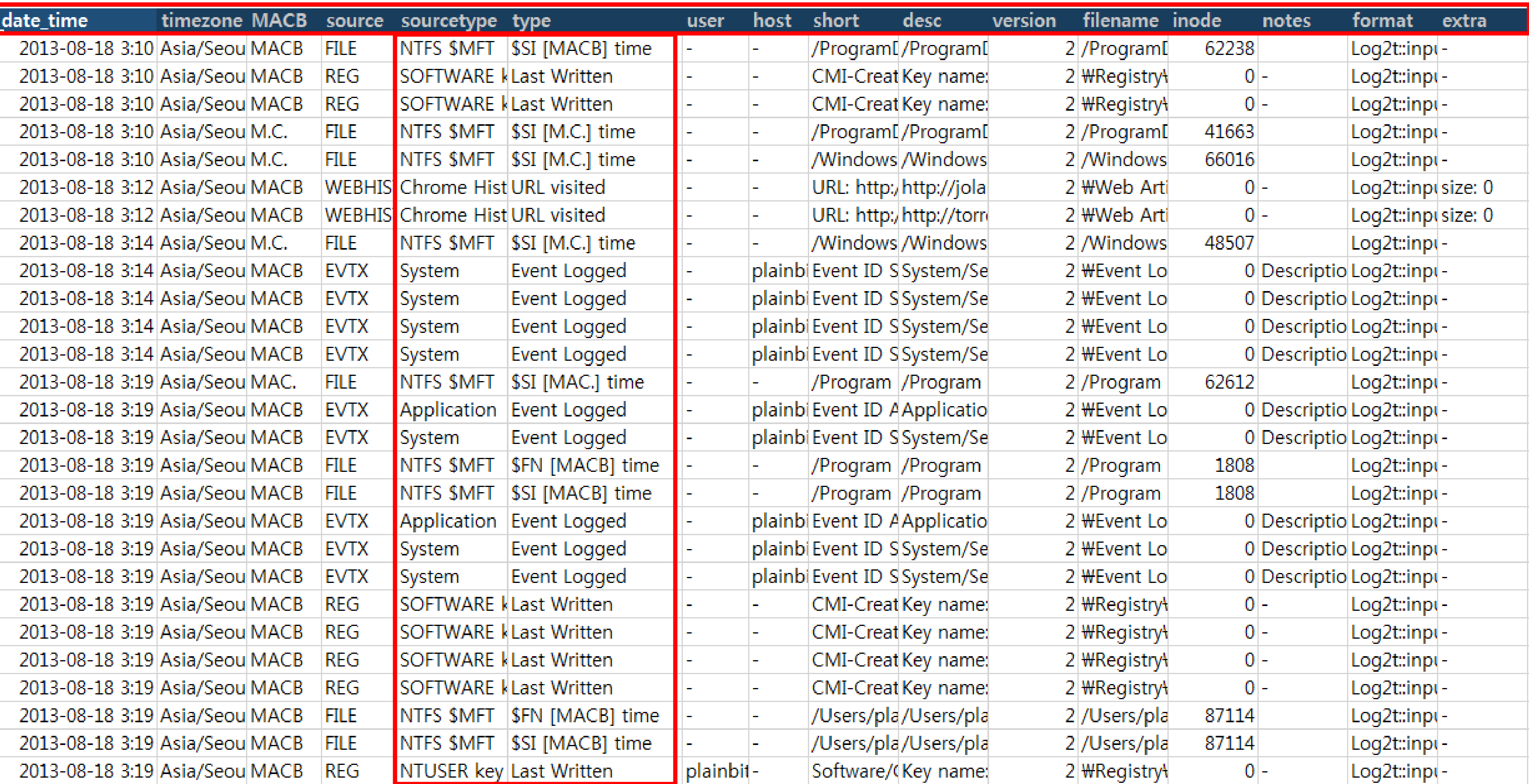
로그 형식 통합

- **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?

log2timeline

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	-
2013-08-18 3:19	Asia/Seou	MACB	REG	NTUSER key	Last Written	plainbit	-	Software/(	Key name:	2	₩Registry	0	-	Log2t::inpu	-

log2timeline

입력 방식

- 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  -w  timeline.txt “d:₩artifacts₩”
```

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
- **CSV**. Dump the timeline in a comma separated value file (CSV).
- **Mactime**. The format supported for use by TSK's mactime
- **SIMILE**. An XML file that can be read by a SIMILE timeline widget
- **SQLite**. Dump the timeline into a SQLite database.
- **TLN**. Tab Delimited File
- **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

log2timeline 문제점

- 한글 인코딩 처리 문제
- 시간 형식 (월/일/년)
- 일부 파싱 모듈 오류
- 리눅스 환경에서 동작

log2timeline

log2timeline_mod

1. 타임라인 생성

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

2. 시간 순 정렬

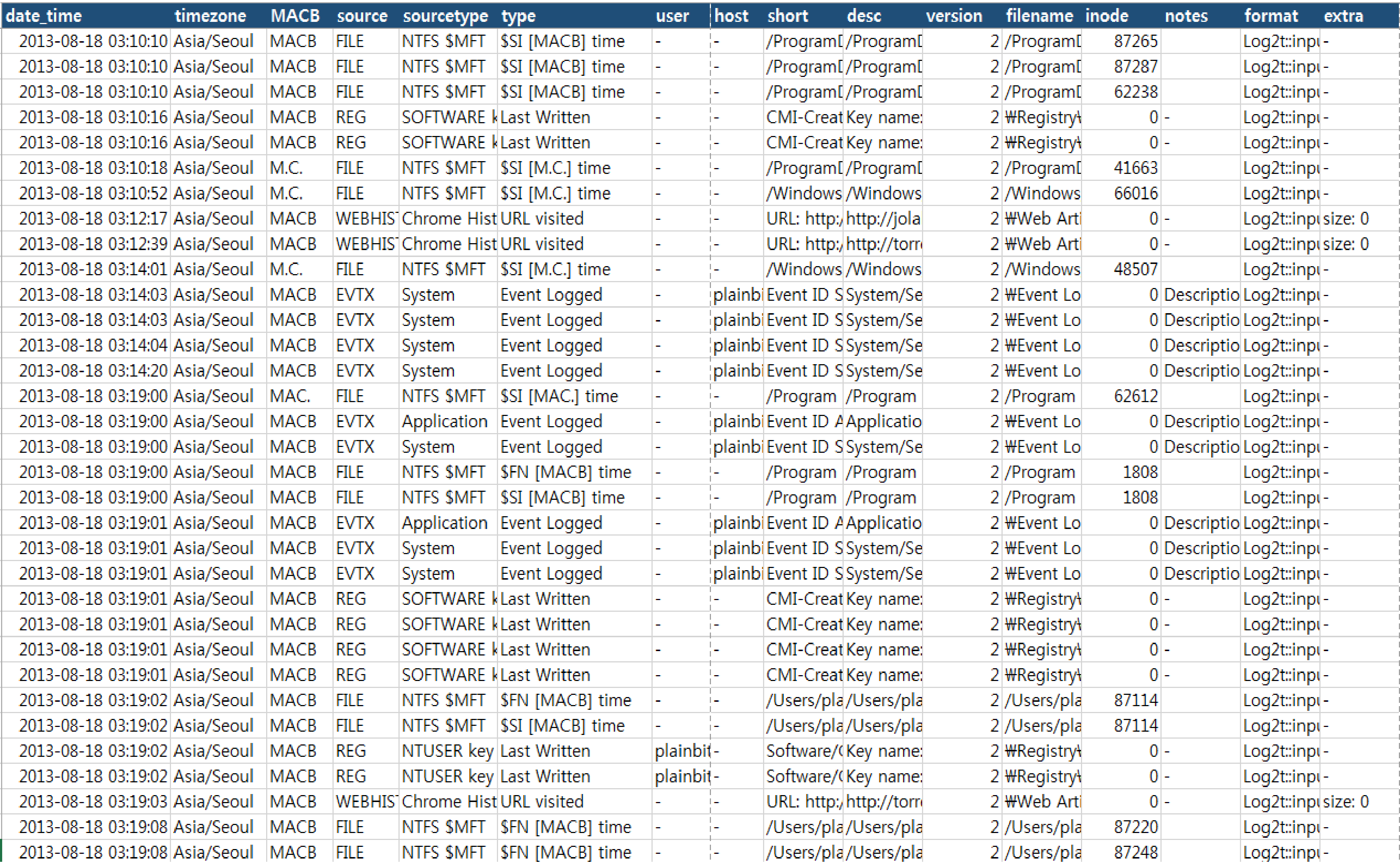
```
$> python log2_sort.py -i <input file> -o <output file> -n <line number>
```

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

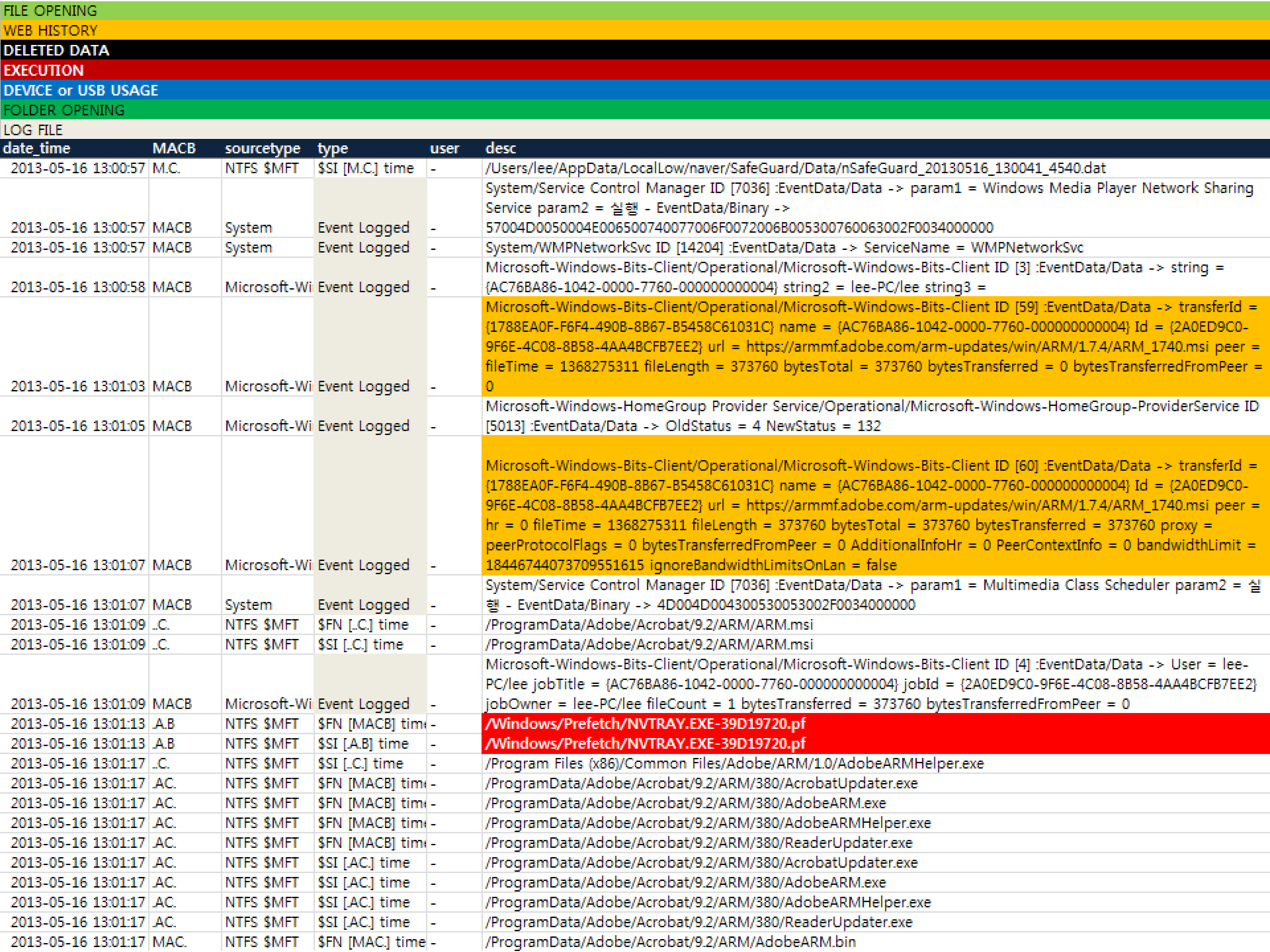
3. TIMELINE_COLOR_TEMPLATE 이용

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

log2timeline



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	WEBHIST	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	WEBHIST	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/C	Key name:	2	₩Registry	0	-	Log2t::inpu	-
2013-08-18 03:19:02	Asia/Seoul	MACB	REG	NTUSER key	Last Written	plainbit	-	Software/C	Key name:	2	₩Registry	0	-	Log2t::inpu	-
2013-08-18 03:19:03	Asia/Seoul	MACB	WEBHIST	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	-



FILE OPENING

WEB HISTORY

DELETED DATA

EXECUTION

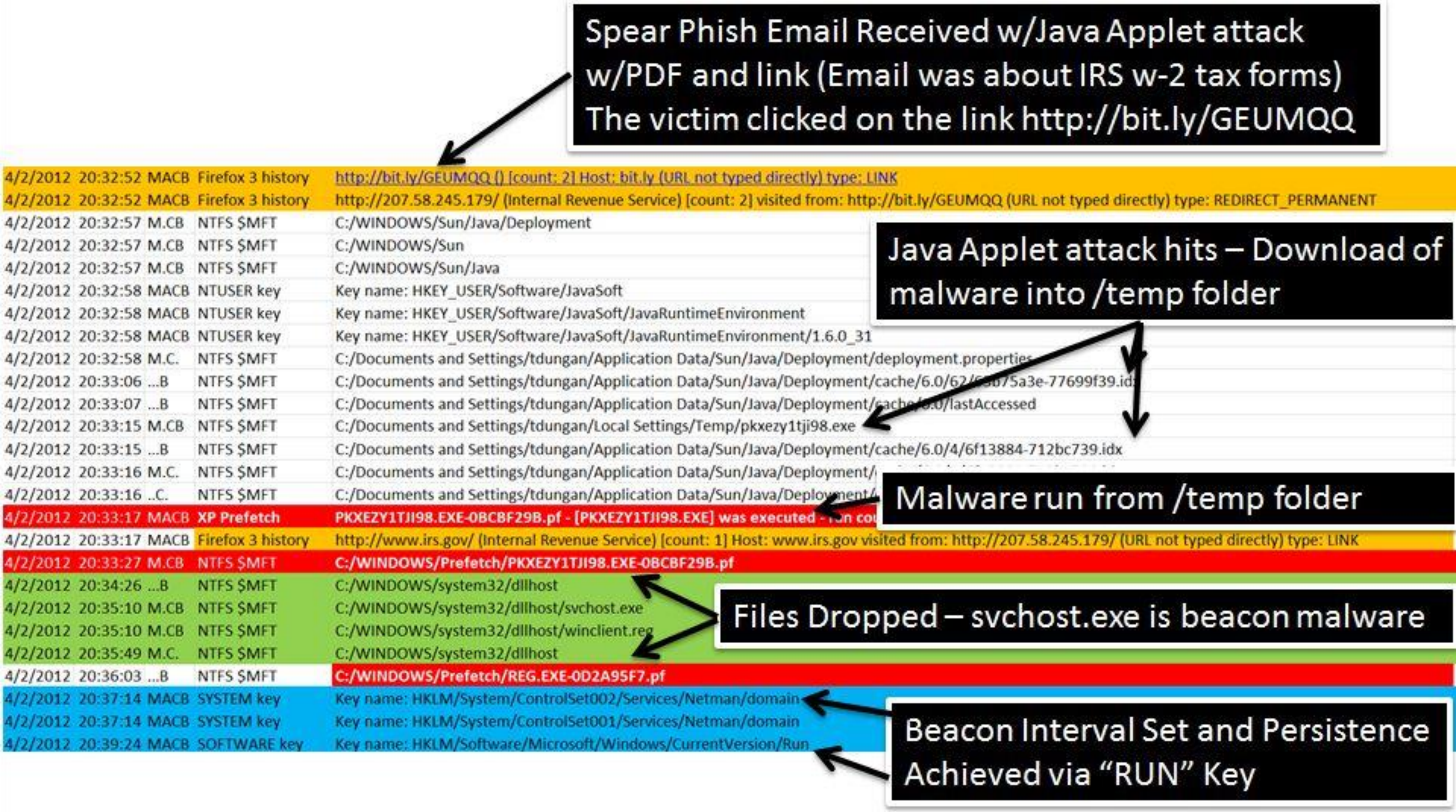
DEVICE or USB USAGE

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

Spearphishing Attack SuperTimeline



Spear Phish Email Received w/Java Applet attack w/PDF and link (Email was about IRS w-2 tax forms)
The victim clicked on the link http://bit.ly/GEUMQQ

Java Applet attack hits – Download of malware into /temp folder

Malware run from /temp folder

Files Dropped – svchost.exe is beacon malware

Beacon Interval Set and Persistence Achieved via “RUN” Key

```
4/2/2012 20:32:52 MACB Firefox 3 history  http://bit.ly/GEUMQQ () [count: 2] Host: bit.ly (URL not typed directly) type: LINK
4/2/2012 20:32:52 MACB Firefox 3 history  http://207.58.245.179/ (Internal Revenue Service) [count: 2] visited from: http://bit.ly/GEUMQQ (URL not typed directly) type: REDIRECT_PERMANENT
4/2/2012 20:32:57 M.CB NTFS $MFT          C:/WINDOWS/Sun/Java/Deployment
4/2/2012 20:32:57 M.CB NTFS $MFT          C:/WINDOWS/Sun
4/2/2012 20:32:57 M.CB NTFS $MFT          C:/WINDOWS/Sun/Java
4/2/2012 20:32:58 MACB NTUSER key         Key name: HKEY_USER/Software/JavaSoft
4/2/2012 20:32:58 MACB NTUSER key         Key name: HKEY_USER/Software/JavaSoft/JavaRuntimeEnvironment
4/2/2012 20:32:58 MACB NTUSER key         Key name: HKEY_USER/Software/JavaSoft/JavaRuntimeEnvironment/1.6.0_31
4/2/2012 20:32:58 M.C. NTFS $MFT          C:/Documents and Settings/tdungan/Application Data/Sun/Java/Deployment/deployment.properties
4/2/2012 20:33:06 ...B NTFS $MFT          C:/Documents and Settings/tdungan/Application Data/Sun/Java/Deployment/cache/6.0/62/[illegible]75a3e-77699f39.id
4/2/2012 20:33:07 ...B NTFS $MFT          C:/Documents and Settings/tdungan/Application Data/Sun/Java/Deployment/cache/6.0/lastAccessed
4/2/2012 20:33:15 M.CB NTFS $MFT          C:/Documents and Settings/tdungan/Local Settings/Temp/pkxezy1tji98.exe
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
4/2/2012 20:33:16 M.C. NTFS $MFT          C:/Documents and Settings/tdungan/Application Data/Sun/Java/Deployment/
4/2/2012 20:33:16 ..C. NTFS $MFT          C:/Documents and Settings/tdungan/Application Data/Sun/Java/Deployment/
4/2/2012 20:33:17 MACB XP Prefetch        PKXEZY1TJI98.EXE-0BCBF29B.pf - [PKXEZY1TJI98.EXE] was executed - run cou
4/2/2012 20:33:17 MACB Firefox 3 history  http://www.irs.gov/ (Internal Revenue Service) [count: 1] Host: www.irs.gov visited from: http://207.58.245.179/ (URL not typed directly) type: LINK
4/2/2012 20:33:27 M.CB NTFS $MFT          C:/WINDOWS/Prefetch/PKXEZY1TJI98.EXE-0BCBF29B.pf
4/2/2012 20:34:26 ...B NTFS $MFT          C:/WINDOWS/system32/dllhost
4/2/2012 20:35:10 M.CB NTFS $MFT          C:/WINDOWS/system32/dllhost/svchost.exe
4/2/2012 20:35:10 M.CB NTFS $MFT          C:/WINDOWS/system32/dllhost/winclient.reg
4/2/2012 20:35:49 M.C. NTFS $MFT          C:/WINDOWS/system32/dllhost
4/2/2012 20:36:03 ...B NTFS $MFT          C:/WINDOWS/Prefetch/REG.EXE-0D2A95F7.pf
4/2/2012 20:37:14 MACB SYSTEM key         Key name: HKLM/System/ControlSet002/Services/Netman/domain
4/2/2012 20:37:14 MACB SYSTEM key         Key name: HKLM/System/ControlSet001/Services/Netman/domain
4/2/2012 20:39:24 MACB SOFTWARE key       Key name: HKLM/Software/Microsoft/Windows/CurrentVersion/Run
```

Plaso

log2timeline 한계

- 펄로 작성
- 단일 쓰레드 사용
- 초 단위의 시간 정밀도 사용
- 텍스트 형식의 출력
- 새로운 기능 추가를 위해 많은 노력 필요
- 필터나 사후 처리 기능 빈약
- 한글 처리의 한계
- 시간 형식의 차이 (년-월-일 <-> 월/일/년)

Plaso

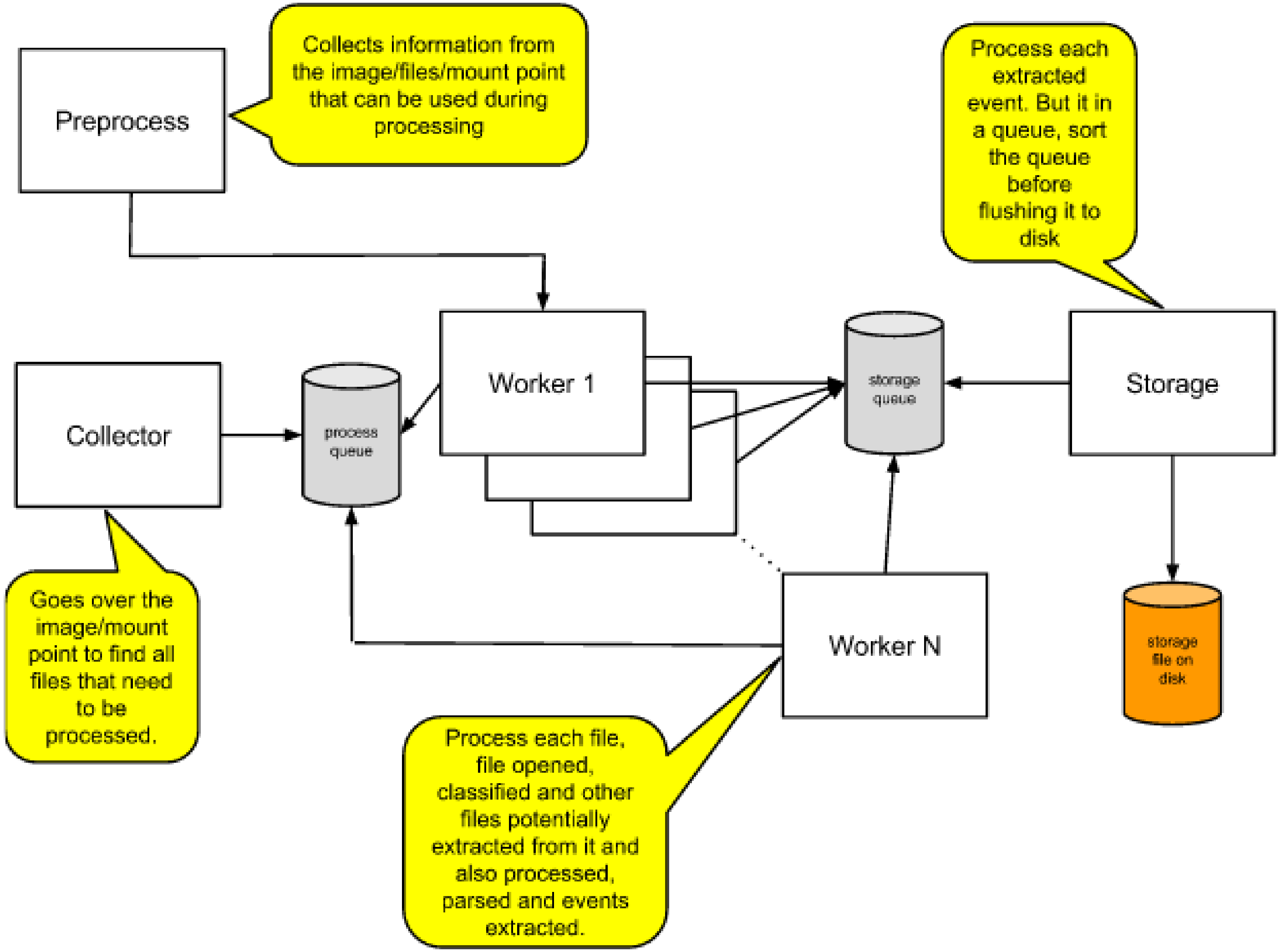
http://plaso.kiddaland.net/

Plaso

특징

- 전반부는 log2timeline 이용
- 실행 및 후반부 기능 강화
  - 멀티 쓰레딩 지원
  - 이미지 파일 파싱
  - VSS 파싱
  - 태그 기능
  - 필터 기능
  - 선별 수집 기능
  - … …

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
Goes over the image/mount point to find all files that need to be processed.
Worker N
storage file on disk
Process each file, file opened, classified and other files potentially extracted from it and also processed, parsed and events extracted.

Plaso

역할

- **Preprocessing**
  - 모든 기능 중 가장 먼저 수행되며 마운트 포인트나 이미지 대상
  - 파싱에 사용할 수 있는 정보를 사전에 미리 획득
  - 타임존, 사용자 경로, 호스트명, 브라우저, 애플리케이션 등
- **Collection**
  - 파일, 마운트 포인트, 이미지를 대상으로 Worker에서 처리할 아티팩트를 식별 ➔ 큐
- **Worker**
  - 큐에 저장된 각 작업을 처리
- **Storage**
  - 처리된 데이터를 구조적으로저장

지원 도구

- **log2timeline**
  - 파일, 마운트 포인트, 이미지를 대상으로 아티팩트를 처리하여 스토리지로 저장
- **pinfo**
  - 저장된 스토리지 정보를 출력
- **pprof (plaso profiler)**
  - 파일에 대한 프로파일링 정보 출력 ➔ 파서를 최적화하거나 개발 시 주로 사용
- **preg**
  - 레지스트리 파일, 이미지에서 레지스트리를 파싱하기 위한 도구
- **pshell**
  - 출력, 디버깅, 테스트를 위해 Plaso 모든 라이브러리에 접근 가능한 iPython 콘솔
- **psort**
  - 스토리지 파일에 대한 필터, 정렬을 담당하는 도구
- **plasm (Plaso Langar Að Safna Minna)**
  - 스토리지 파일 내 이벤트를 그룹화하거나 태깅하기 위한 도구

Plaso

지원 도구

- **log2timeline**

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

- **[STORAGE_FILE] :** 파싱 결과를 출력한 스토리지 파일 지정
- **[SOURCE]** : 파일, 디렉터리, 마운트 포인트, 이미지 지정
- **[FILTER]** : 사전 필터 작업이 필요한 경우 필터링 규칙 추가 (보통은 사후 필터링)

Plaso

지원 도구

- **log2timeline**

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

- **[-z TIMEZONE] :** 타임존 지정, “-z list”로 확인
- **[-p]** : preprocess 작업 여부 (이미지는 기본으로 수행, 마운트 포인트는 사용자 입력 요구)
- **[-i]** : 이미지 지정
- **[-o]** : 이미지 파일 내 볼륨의 위치 지정 (섹터 번호)

Plaso

log2timeline 활용, http://plaso.kiddaland.net/usage/log2timeline

- 이미지 파일 대상

```
$> log2timeline.exe  –z  Asia/Seoul  /path/to/output.dump   /path/to/image.dd(E01)
```

- 마운트 위치 대상

```
$> log2timeline.exe  –z  Asia/Seoul  -p  /path/to/output.dump   /path/to/mount_point
```

- 파일 또는 디렉터리 대상

```
$> log2timeline.exe  –z  Asia/Seoul  /path/to/output.dump   /path/to/file_or_directory
```

Plaso

log2timeline 활용, http://plaso.kiddaland.net/usage/log2timeline

- 선별 분석

```
$> log2timeline.exe –z Asia/Seoul -f browser_filter.txt history.dump /mnt/browser.E01
```

```
/(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
```

Plaso

pinfo 활용, http://plaso.kiddaland.net/usage/pinfo

- **스토리지 파일 정보 출력**

```
$> pinfo.exe  TESTCASE.dump
```

```
--------------------------------------------------------------------------------
                Plaso Storage Information
--------------------------------------------------------------------------------
Storage file:              TESTCASE.dump
Source processed:          G:₩TEST₩TESTCASE.E01
Time of processing:        2014-09-27T13:44:24+00:00

Collection information:
        parser_selection = win7
        os_detected = N/A
        configured_zone = Asia/Seoul
        preprocess = True
        parsers = [u'esedb', u'winfirewall', u'recycle_bin', u'filestat', u'sqlite', u'lnk', u'symantec_scanlog', u'winevtx', u'plist',
u'opera_global
', u'chrome_cache', u'prefetch', u'winreg', u'msiecf', u'bencode', u'skydrive_log', u'openxml', u'opera_typed_history', u'winjob', u'olecf',
u'java_id
x', u'firefox_cache', u'mcafee_protection', u'skydrive_log_error']
        protobuf_size = 0
        vss parsing = False
        recursive = False
        preferred_encoding = cp949
        workers = 5
        output_file = ./TESTCASE.dump
        image_offset = 105906176
        version = 1.1.0
        cmd_line = C:₩Users₩ADMINI~1₩TOOL₩plaso₩log2timeline.exe -z Asia/Seoul -p ./TESTCASE.dump G:₩TEST₩TESTCASE.E01
```

Plaso

psort 활용, http://plaso.kiddaland.net/usage/psort

- **스토리지 파일 정렬**

```
$> psort.exe   [-o FORMAT]  [-w OUTPUTFILE]  [--slice  DATE]  [STORAGE_FILE]  [FILTER]
```

  - **[-o FORMAT]** : 출력 형식 지정
    - ✓ **L2tcsv**, L2ttln, Dynamic, Rawpy, Raw, **Sql4n6**, Pstorage, Tln
  - **[-w OUTPUTFILE]** : 정렬 후 저장할 파일 지정
  - **[--slice DATE]** : 지정한 날짜만 전, 후 이벤트만 표시
  - **[STORAGE_FILE]** : 정렬할 스토리지 파일
  - **[FILTER]** : 정렬 시 필터링

- **정렬 후 SQLite 출력 예**

```
$> psort.exe   -o  Sql4n6   -w  TESTCASE.db    TESTCASE.dump
```

Plaso

psort 활용, http://plaso.kiddaland.net/usage/psort

- **[--slice DATE]**
  - --slice "2012-04-05 17:01:06" sample_output.dump
  - --slicer sample_output.dump "date > '2012-01-01' AND parser is 'winjob'”
  - --slicer --slice_size 10 sample_output.dump "date > '2012-01-01' AND parser is 'winjob'”
- **[FILTER],** http://plaso.kiddaland.net/usage/filters
  - "date > '2013-01-23 15:23:51' and date < '2013-01-23 21:42:13'”
  - "date > '2012-01-01' AND tag contains 'Application Execution'”
  - "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"

Plaso

plasm 활용, http://plaso.kiddaland.net/usage/plasm

- **태그 파일 생성**

```
TAG  MESSAGE
        CONDITION
        CONDITION
```

  - **TAG MESSAGE** : 자유롭게 정의 가능
  - **CONDITION** : 이벤트 필터 규칙 사용
  - 응용프로그램 실행 관련 태그

```
Application Execution
      data_type is 'windows:prefetch:prefetch'
      data_type is 'windows:lnk:link' and filename contains 'Recent' and (local_path
                   contains '.exe' or network_path contains '.exe' or relative_path contains '.exe')
```

- **스토리지 파일에 태깅하기**

```
$>  plasm.exe   tag   --tagfile="/path/to/tag/file/tagfile.txt"    TESTCASE.dump
```

Plaso

plasm 활용, http://plaso.kiddaland.net/usage/plasm

- 태깅 결과 확인

```
$> pinfo.py  TESTCASE.dump
    …
    Counter information:
    Counter: Total = 210
    Counter: Application Execution = 196
    Counter: Document Opened = 11
    Counter: Startup Application = 3
    Counter: AutoRun = 3
    …
```

- 태깅 이벤트 필터하기

```
$> psort.exe  TESTCASE.dump
              "date > '2013-01-01'  AND  tag contains  'Application Execution '"
```

Plaso

plasm 활용, http://plaso.kiddaland.net/usage/plasm

- **태그 파일 예제 (계속)**

```
Application Execution
  data_type is 'windows:prefetch'
  data_type is 'windows:lnk:link' and filename contains 'Recent' and (local_path contains '.exe' or
                 network_path contains '.exe' or relative_path contains '.exe')
  data_type is 'windows:registry:key_value' AND (plugin contains 'userassist' or plugin contains
                 'mru') AND regvalue.__all__ contains '.exe'
  data_type is 'windows:evtx:record' and strings contains 'user mode service' and strings contains
                 'demand start'
  data_type is 'fs:stat' and filename contains 'Windows/Tasks/At'
  data_type is 'windows:tasks:job'
  data_type is 'windows:evt:record' and source_name is 'Security' and event_identifier is 592
  data_type is 'windows:evtx:record' and source_name is 'Microsoft-Windows-Security-Auditing'
                 and event_identifier is 4688
  data_type is 'windows:registry:appcompatcache'
```

Plaso

plasm 활용, http://plaso.kiddaland.net/usage/plasm

- **태그 파일 예제 (계속)**

```
Document Opened
  data_type is 'windows:registry:key_value' AND plugin contains 'mru' AND regvalue.__all__ not
                    contains '.exe' AND timestamp > 0
Logon
  data_type is 'windows:evt:record' and source_name is 'Security' and event_identifier is 540
  data_type is 'windows:evtx:record' and source_name is 'Microsoft-Windows-Security-Auditing'
                    and event_identifier is 4624
  data_type is 'windows:evtx:record' and source_name is 'Microsoft-Windows-TerminalServices-
                    LocalSessionManager' and event_identifer is 21
Logoff
  data_type is 'windows:evt:record' and source_name is 'Security' and event_identifier is 538
  data_type is 'windows:evtx:record' and source_name is 'Microsoft-Windows-Security-Auditing'
                    and event_identifier is 4634
  data_type is 'windows:evtx:record' and source_name is 'Microsoft-Windows-TerminalServices-
                    LocalSessionManager' and event_identifer is 21
```

Plaso

plasm 활용, http://plaso.kiddaland.net/usage/plasm

- **태그 파일 예제**

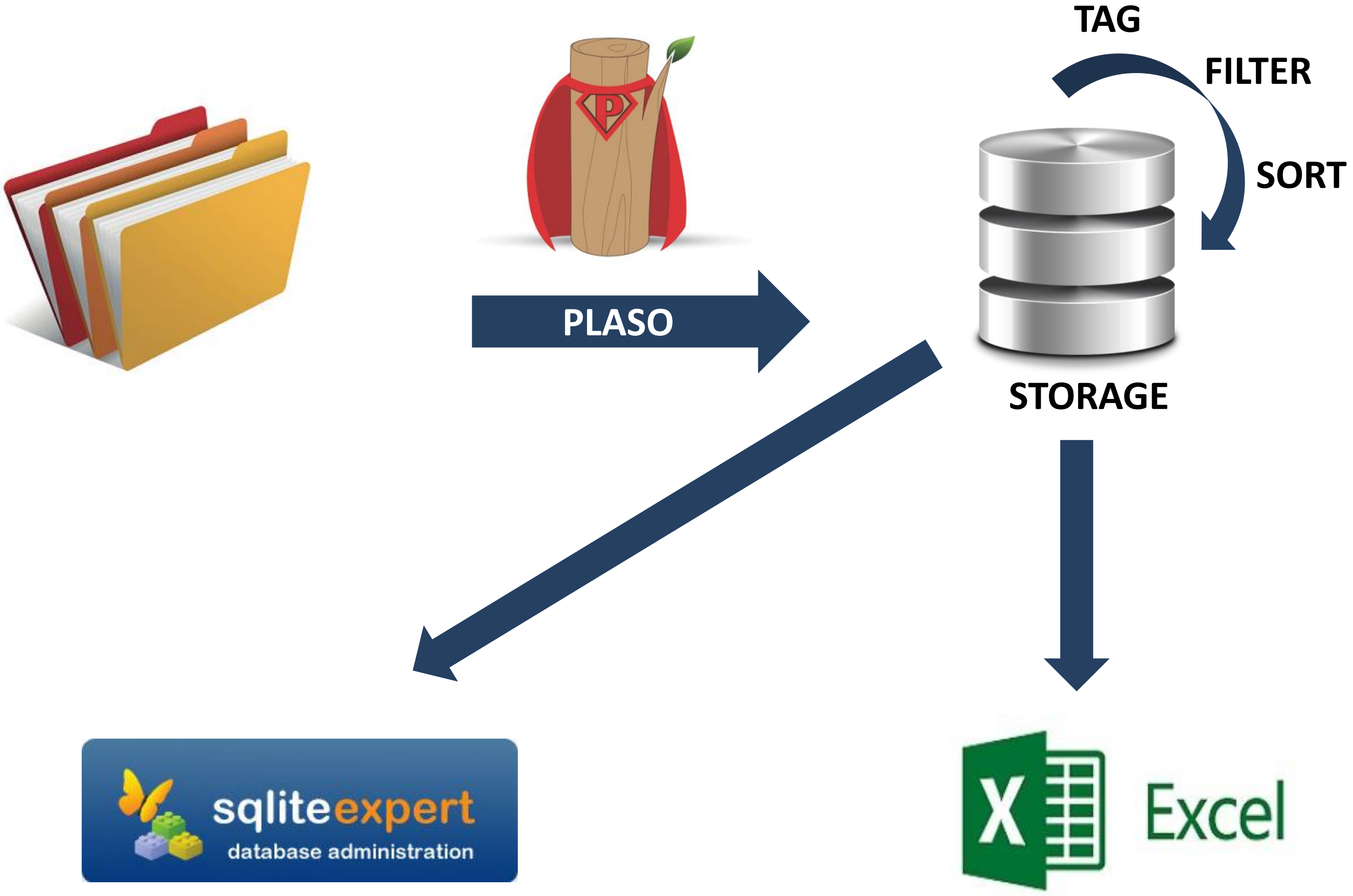
```
Task Scheduled
  data_type is 'windows:evt:record' and source_name is 'Security' and event_identifier is 602
  data_type is 'windows:evtx:record' and source_name is 'Microsoft-Windows-Security-Auditing'
                    and event_identifier is 4698
AutoRun
  data_type is 'windows:registry:key_value' and plugin contains 'Run'
File Downloaded
  data_type is 'chrome:history:file_downloaded'
  timestamp_desc is 'File Downloaded'
Document Printed
  (data_type is 'metadata:hachoir' OR data_type is 'olecf:summary_info') AND timestamp_desc
                    contains 'Printed'
Startup Application
  data_type is 'windows:registry:key_value' AND (plugin contains 'run' or plugin contains 'lfu') AND
                    (regvalue.__all__ contains '.exe' OR regvalue.__all__ contains '.dll')
```

파서 & 플러그인 작성

- **사용자 정의 파서 및 플러그인 작성 지원**
- **파서 (parser)**
  - 파일 단위로 동작하는 모듈
- **플러그인 (plugin)**
  - 파일 확장 형식 (Chrome History SQLite Database)
  - 파일의 부분 데이터 (Application Compatibility cache Windows Registry data)

Plaso

Plaso 분석 방법



TAG

FILTER

SORT

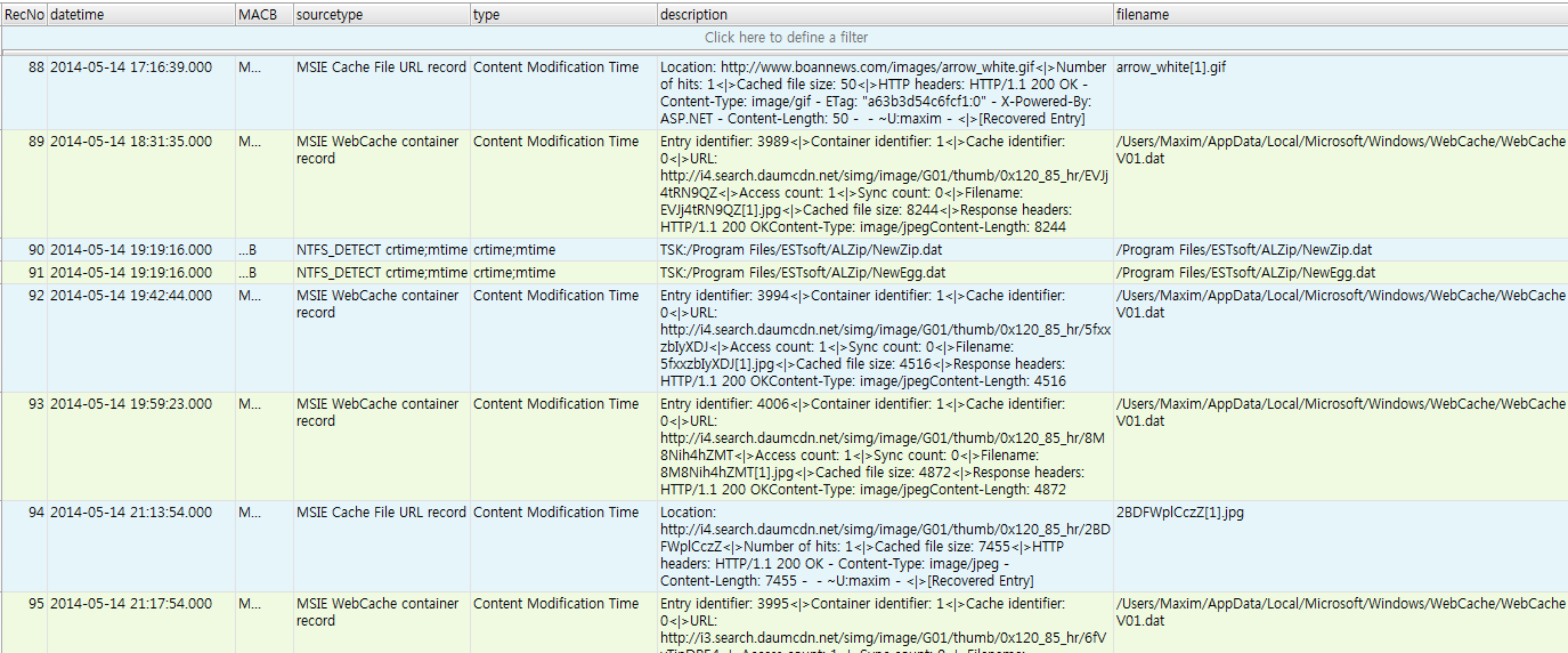
PLASO

STORAGE

Plaso

SQLite 활용

```
SELECT
        datetime, MACB, sourcetype, type, description, filename
FROM log2timeline
WHERE description like '%Desktop%’
WHERE datetime BETWEEN '2014-09-01' AND '2014-09-10';
```



Click here to define a filter

<table>
<tr><th>RecNo</th><th>datetime</th><th>MACB</th><th>sourcetype</th><th>type</th><th>description</th><th>filename</th></tr>
<tr><td>88</td><td>2014-05-14 17:16:39.000</td><td>M...</td><td>MSIE Cache File URL record</td><td>Content Modification Time</td><td>Location: http://www.boannews.com/images/arrow_white.gif<|>Number of hits: 1<|>Cached file size: 50<|>HTTP headers: HTTP/1.1 200 OK - Content-Type: image/gif - ETag: "a63b3d54c6fcf1:0" - X-Powered-By: ASP.NET - Content-Length: 50 - - ~U:maxim - <|>[Recovered Entry]</td><td>arrow_white[1].gif</td></tr>
<tr><td>89</td><td>2014-05-14 18:31:35.000</td><td>M...</td><td>MSIE WebCache container record</td><td>Content Modification Time</td><td>Entry identifier: 3989<|>Container identifier: 1<|>Cache identifier: 0<|>URL: http://i4.search.daumcdn.net/simg/image/G01/thumb/0x120_85_hr/EVJj4tRN9QZ<|>Access count: 1<|>Sync count: 0<|>Filename: EVJj4tRN9QZ[1].jpg<|>Cached file size: 8244<|>Response headers: HTTP/1.1 200 OKContent-Type: image/jpegContent-Length: 8244</td><td>/Users/Maxim/AppData/Local/Microsoft/Windows/WebCache/WebCacheV01.dat</td></tr>
<tr><td>90</td><td>2014-05-14 19:19:16.000</td><td>...B</td><td>NTFS_DETECT crtime;mtime</td><td>crtime;mtime</td><td>TSK:/Program Files/ESTsoft/ALZip/NewZip.dat</td><td>/Program Files/ESTsoft/ALZip/NewZip.dat</td></tr>
<tr><td>91</td><td>2014-05-14 19:19:16.000</td><td>...B</td><td>NTFS_DETECT crtime;mtime</td><td>crtime;mtime</td><td>TSK:/Program Files/ESTsoft/ALZip/NewEgg.dat</td><td>/Program Files/ESTsoft/ALZip/NewEgg.dat</td></tr>
<tr><td>92</td><td>2014-05-14 19:42:44.000</td><td>M...</td><td>MSIE WebCache container record</td><td>Content Modification Time</td><td>Entry identifier: 3994<|>Container identifier: 1<|>Cache identifier: 0<|>URL: http://i4.search.daumcdn.net/simg/image/G01/thumb/0x120_85_hr/5fxxzbIyXDJ<|>Access count: 1<|>Sync count: 0<|>Filename: 5fxxzbIyXDJ[1].jpg<|>Cached file size: 4516<|>Response headers: HTTP/1.1 200 OKContent-Type: image/jpegContent-Length: 4516</td><td>/Users/Maxim/AppData/Local/Microsoft/Windows/WebCache/WebCacheV01.dat</td></tr>
<tr><td>93</td><td>2014-05-14 19:59:23.000</td><td>M...</td><td>MSIE WebCache container record</td><td>Content Modification Time</td><td>Entry identifier: 4006<|>Container identifier: 1<|>Cache identifier: 0<|>URL: http://i4.search.daumcdn.net/simg/image/G01/thumb/0x120_85_hr/8M8Nih4hZMT<|>Access count: 1<|>Sync count: 0<|>Filename: 8M8Nih4hZMT[1].jpg<|>Cached file size: 4872<|>Response headers: HTTP/1.1 200 OKContent-Type: image/jpegContent-Length: 4872</td><td>/Users/Maxim/AppData/Local/Microsoft/Windows/WebCache/WebCacheV01.dat</td></tr>
<tr><td>94</td><td>2014-05-14 21:13:54.000</td><td>M...</td><td>MSIE Cache File URL record</td><td>Content Modification Time</td><td>Location: http://i4.search.daumcdn.net/simg/image/G01/thumb/0x120_85_hr/2BDFWplCczZ<|>Number of hits: 1<|>Cached file size: 7455<|>HTTP headers: HTTP/1.1 200 OK - Content-Type: image/jpeg - Content-Length: 7455 - - ~U:maxim - <|>[Recovered Entry]</td><td>2BDFWplCczZ[1].jpg</td></tr>
<tr><td>95</td><td>2014-05-14 21:17:54.000</td><td>M...</td><td>MSIE WebCache container record</td><td>Content Modification Time</td><td>Entry identifier: 3995<|>Container identifier: 1<|>Cache identifier: 0<|>URL: http://i3.search.daumcdn.net/simg/image/G01/thumb/0x120_85_hr/6fV</td><td>/Users/Maxim/AppData/Local/Microsoft/Windows/WebCache/WebCacheV01.dat</td></tr>
</table>

질문과 답변