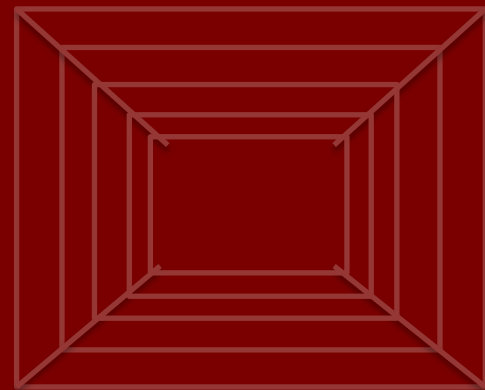




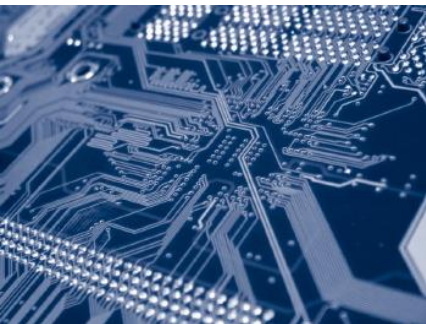
리눅스 시스템 침해사고 분석과 대응

Plainbit Co., Ltd.

CEO & Founder, JK Kim



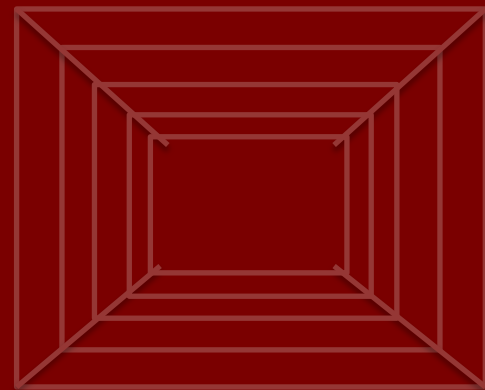
보안 | 신뢰



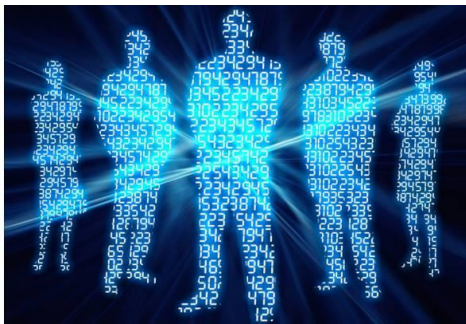
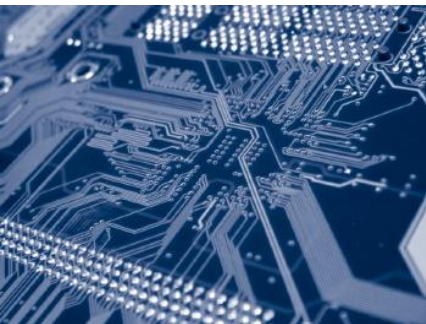
1. 리눅스 포렌식 개요
2. 리눅스 라이브 분석
3. 리눅스 데이터 수집
4. 리눅스 데이터 분석



1. 리눅스 포렌식 개요



보안 | 신뢰



• 리눅스 포렌식의 강점

- 무료로 사용할 수 있는 다양한 도구가 존재
- 강력한 다수의 도구가 오픈소스 형태로 발전
 - ❖ 사용자의 목적에 맞게 수정 및 개선 가능
 - ❖ 코드 분석을 통해 깊이 있는 이해 및 분석 시간 단축
- 명령어 조합만으로 엄청난 작업이 가능!!

• 리눅스 포렌식의 단점

- 너무 많은 도구로 직접 경험해보기 전에는 적합한 도구를 찾기 어려움
- 다양한 배포판으로 인해 표준화된 절차를 마련하기 어려움
- 오픈소스로 인해 도구 및 법적 안정성 보장의 어려움
- 명령어를 사용하기 위해서는 상당한 수준의 경험이 필요!!

- 리눅스 배포판

- 주요 배포판 – http://en.wikipedia.org/wiki/List_of_Linux_distributions

- ❖ 데비안 기반

- Knoppix
- Ubuntu

- ❖ 레드햇 기반

- Red Hat Enterprise
- Fedora
- CentOS

- ❖ 수세 리눅스

- ❖ 젠투 리눅스

- ❖ 슬랙웨어

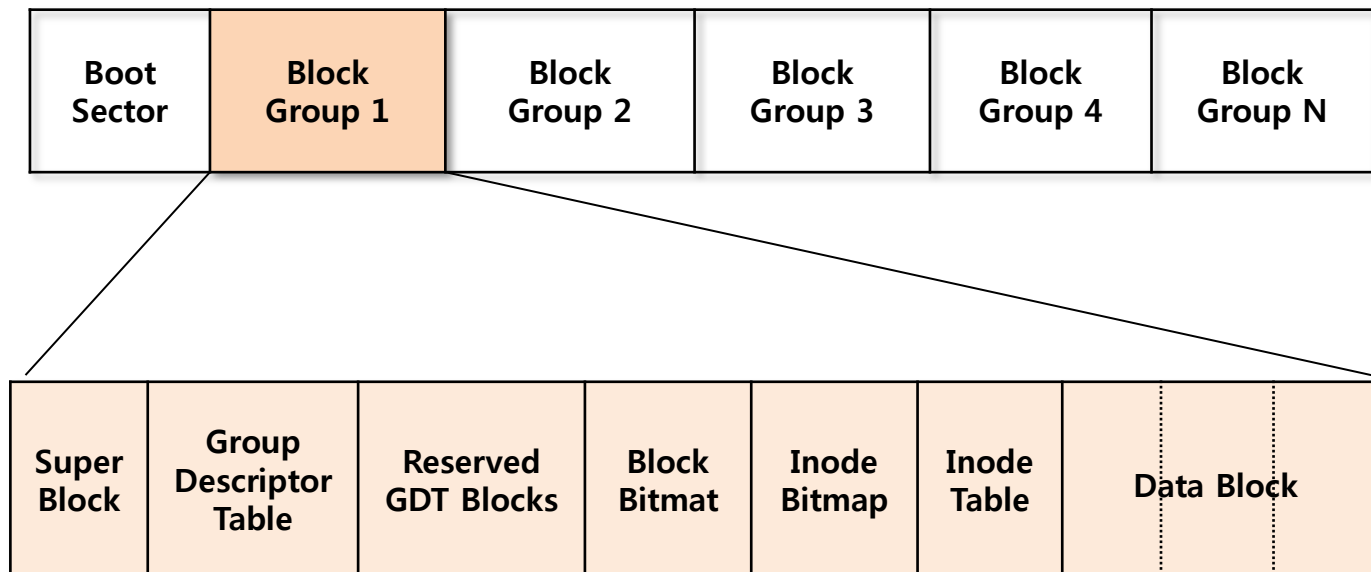
- 리눅스 주요 디렉터리

- **/bin** : 기본 명령어
- **/boot** : 커널을 포함, 부팅 시 필요한 파일이 저장
- **/etc** : 시스템 환경 설정 파일
- **/home** : 시스템 계정 사용자들의 홈 디렉터리
- **/lib** : 각종 프로그램 라이브러리가 저장되는 공간으로 대부분은 공유 라이브러리
- **/mnt** : 외부 장치인 시디롬, 삼바 등을 마운트하기 위한 용도
- **/proc** : 프로세서, 프로그램 정보, 하드웨어 관련 정보가 저장
- **/root** : 시스템 관리자의 홈 디렉터리
- **/sbin** : 관리자가 사용하는 명령어
- **/tmp** : 임시 파일을 위한 디렉터리
- **/usr** : 프로그램 설치 공간으로 프로그램 관련 명령어, 라이브러리가 위치
- **/var** : 각종 로그 파일, 보안 기록, 메일 임시 저장

• 리눅스 파일시스템

▪ EXT 파일시스템

- ❖ 오픈소스로 현재 가장 널리 사용되는 리눅스 파일시스템
- ❖ 리눅스 커널 2.6에 기본 파일시스템
- ❖ 파일 단편화 현상이 많음
- ❖ EXT 2/3/4의 기본 레이아웃은 동일



- 리눅스 파일시스템

- 파일 복구를 위한 요소

- ❖ 아이노드 테이블

- 삭제된 엔트리의 블록 맵핑 정보 혹은 익스텐트 정보
 - 삭제된 엔트리의 크기 정보

- ❖ 디렉터리 엔트리

- 삭제된 엔트리의 아이노드 정보
 - 삭제된 엔트리의 파일명
 - 디렉터리 엔트리 정보가 삭제되어도 데이터 복구는 가능

- 리눅스 파일시스템

- EXT2 파일 복구

- ❖ 아이노드, 데이터 블록 모두 비트맵 값만 0으로 변경
 - ❖ 파일을 완벽하게 복구 가능

- EXT3 파일 복구

- ❖ 디스크 블록을 가리키는 아이노드 값 초기화
 - ❖ 완벽한 파일 복구는 어려움

- EXT4 파일 복구

- ❖ 아이노드 값 초기화
 - ❖ 익스텐션 헤더 초기화
 - ❖ 파일 복구의 어려움

- **vs. 윈도우 시스템**
 - **파일시스템**
 - ❖ 파일 삭제 시 주요 메타데이터가 와이핑 (ext4)
 - ❖ 파일의 생성 시간이 존재하지 않음
 - ❖ 주로 RAID, LVM 등의 논리적인 볼륨을 구성
 - **레지스트리가 존재하지 않음**
 - ❖ 운영체제/애플리케이션의 실시간 정보 관리를 위한 특별한 구조가 존재하지 않음
 - **대부분 텍스트 기반의 파일 데이터**
 - ❖ 명령어를 조합한 문자열 검색/필터링만으로 많은 작업 가능

• 윈도우 주요 아티팩트

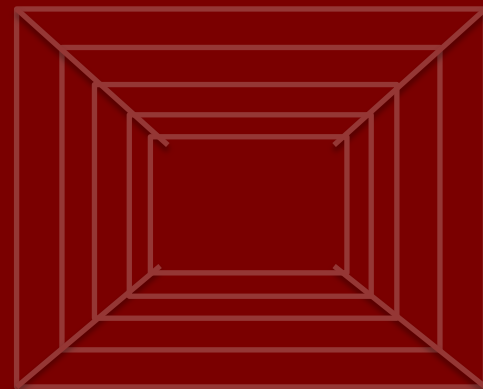
구분	형식	아티팩트
시스템 정보	REG 바이너리	HKEY_LOCAL_MACHINE\SYSTEM\ControlSet001\Control\TimeZoneInformation
	REG 바이너리	HKLM\SOFTWARE\Microsoft\Windows NT\CurrentVersion
	REG 바이너리	HKLM\SYSTEM\ControlSet00X\Services\Tcpip\Parameter\Interfaces\{GUID}
작업 스케줄러	REG 바이너리	HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows NT\CurrentVersion\Schedule\TaskCache\Tasks
네트워크 공유	REG 바이너리	HKU\{USER}\SOFTWARE\Microsoft\Windows\CurrentVersion\Explorer\Map Network Drive MRU
	REG 바이너리	HKU\{USER}\SOFTWARE\Microsoft\Windows\CurrentVersion\Explorer\MountPoints2\{GUID}
	REG 바이너리	HKLM\SYSTEM\ControlSet00X\Services\LanmanServer\Shares
사용자 히스토리	REG 바이너리	HKU\{USER}\SOFTWARE\Microsoft\Windows\CurrentVersion\Explorer\RunMRU
최근 접근 문서	REG 바이너리	HKU\{USER}\SOFTWARE\Microsoft\Windows\CurrentVersion\Explorer\RecentDocs
사용자 계정	REG 바이너리	HKLM\SAM\SAM\Domains\Account\Users\{RID}
	REG 바이너리	HKLM\SOFTWARE\Microsoft\Windows NT\CurrentVersion\ProfileList\{SID}
로그	REG 바이너리	%SystemRoot%\System32\config*.evt
	REG 바이너리	%SystemRoot%\System32\winevt\Logs*.evtx
웹 브라우저	DAT 파일	%UserProfile%\AppData\Local\Microsoft\Windows\Temporary Internet Files\Content.IE5\index.dat
	DAT 파일	%UserProfile%\AppData\Local\Microsoft\Windows\History\History.IE5\index.dat
	DAT 파일	%UserProfile%\AppData\Roaming\Microsoft\Windows\Cookies\index.dat
	DAT 파일	%UserProfile%\AppData\Roaming\Microsoft\Windows\IEDownloadHistory\index.dat
시작 환경 설정	REG 바이너리	HKLM\SYSTEM\ControlSet00X\Services\{sub folder}

• 리눅스 주요 아티팩트

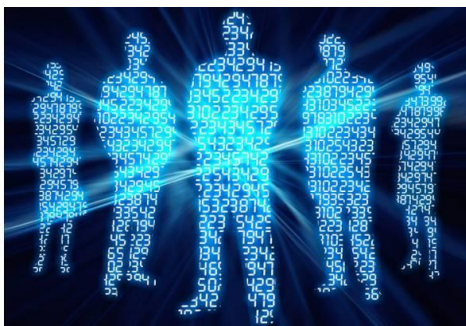
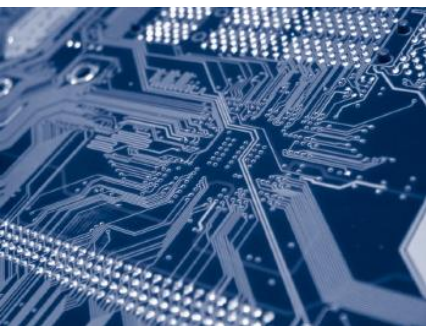
구분	형식	아티팩트
시스템 정보	바이너리	/etc/localtime
	텍스트	/etc/issue, /etc/inittab, /etc/mtab, /etc/fstab
작업 스케줄러	텍스트	/etc/crontab
	디렉터리	/etc/cron.d, /etc/cron.daily, /etc/cron.hourly, /etc/cron.monthly, /etc/cron.weekly
네트워크 공유	텍스트	/etc/samba/lmhosts, /etc/samba/smb.conf, /etc/smbusers, /etc/mtab
사용자 히스토리	텍스트	\$HOME/.bash_history, \$HOME/.history, \$HOME/.sh_history
최근 접근 문서	XML	\$HOME/.recently-used-xbel
	디렉터리	\$HOME/.thumbnails
사용자 계정	텍스트	/etc/passwd, /etc/shadow, /etc/group, /etc/profile
	디렉터리	/etc/skel/, \$HOME
로그	텍스트	/var/log/*
	바이너리	/var/log/lastlog, /var/log/wtmp, /var/log/utmp
웹 브라우저	디렉터리	\$HOME/.mozilla/firefox/*.default/Cache, \$HOME/.mozilla/firefox/*.default/thumbnails/
	SQLite	\$HOME/.mozilla/firefox/*.default/cookies.*, \$HOME/.mozilla/firefox/*.default/downloads.splite
	JS	\$HOME/.mozilla/firefox/*.default/sessionstore.js
	JSON	\$HOME/.mozilla/firefox/*.default/search.json
시작 환경 설정	텍스트	/etc/inittab
	디렉터리	/etc/rc.d, /etc/rc#.d, /etc/init.d



2. 리눅스 라이브 분석



보안 | 신뢰



- 리눅스 라이브 데이터
 - 활성데이터
 - ❖ 프로세스
 - ❖ 네트워크
 - ❖ 시스템 정보
 - ❖ 활성 사용자 정보
 - ❖
 - 비활성데이터
 - ❖ 설정 파일
 - ❖ 로그 파일
 - 메모리 덤프
 - 스왑 파티션

- **활성 데이터 수집**
 - **시스템 정보**
 - ❖ **uname -a**
 - ❖ **date, uptime, runlevel**
 - ❖ **/etc/localtime**
 - ❖ **/var/spool/lpd/lp/***
 - **네트워크 정보**
 - ❖ **ifconfig -a**
 - ❖ **netstat -atunp**
 - ❖ **arp -a**
 - ❖ **lsof -i -P -n**
 - ❖ **cat /etc/hosts**
 - ❖ **/etc/sysconfig/network**

- 활성 데이터 수집
 - 프로세스 정보
 - ❖ `ps tree`
 - ❖ `ps -elf`
 - ❖ `chkconfig --list`
 - ❖ `vmstat`
 - ❖ `lsmod`
 - 설치 패키지 정보
 - ❖ `yum list installed`
 - ❖ `rpm -qa`

- **활성 데이터 수집**
 - **저장장치 정보**
 - ❖ `fdisk -l`
 - ❖ `df -h`
 - ❖ `blkid`
 - ❖ `cat /etc/fstab`
 - ❖ `cat /etc/hosts`
 - **활성 사용자 정보**
 - ❖ `w -l`
 - ❖ `who`
 - ❖ `who -a | -b | -d | -l`
 - ❖ `last`
 - ❖ `lastlog`

- **활성 데이터 수집**
 - **/proc 폴더 정보**
 - ❖ /proc/cmdline
 - ❖ /proc/cpuinfo
 - ❖ /proc/devices
 - ❖ /proc/diskstats
 - ❖ /proc/ide
 - ❖ /proc/meminfo
 - ❖ /proc/scsi/scsi
 - ❖ /proc/partitions
 - ❖ /proc/version
 - ❖ /proc/vmstat
 - ❖ /proc/zoneinfo
 - ❖

- **비활성 데이터 수집**
 - **리눅스 배포판 이름/버전**
 - ❖ /etc/*-release, /etc/issue 확인
 - **설치 시각**
 - ❖ /root/install.log, /etc/ssh/ssh_host_*_key 시간 정보 확인
 - **컴퓨터 이름**
 - ❖ /etc/sysconfig/network
 - **IP 주소**
 - ❖ /etc/hosts (정적), /var/lib/dhclient/* (동적)
 - **타임존 설정**
 - ❖ /etc/localtime (/usr/share/zoneinfo와 일치하는지 확인)
 - **계정 정보**
 - ❖ /etc/passwd, /etc/shadow, /etc/group 확인 (관리자 UID=0)

- 비활성 데이터 수집

- 자동 실행 항목

- ❖ /etc/cron*, /var/spool/cron/*
 - ❖ /etc/inittab, /etc/init.d/*, /etc/rc.d/*
 - ❖ /etc/init.conf, /etc/init
 - ❖ /etc/profile, /etc/bash.bashrc
 - ❖ /etc/vimrc, /etc/virc
 - ❖ /etc/csh.cshrc, /etc/csh.login
 - ❖ \$HOME/.bashrc, \$HOME/.bash_profile, \$HOME/.bash_logout
 - ❖ \$HOME/.vimrc, \$HOME/.xinitrc

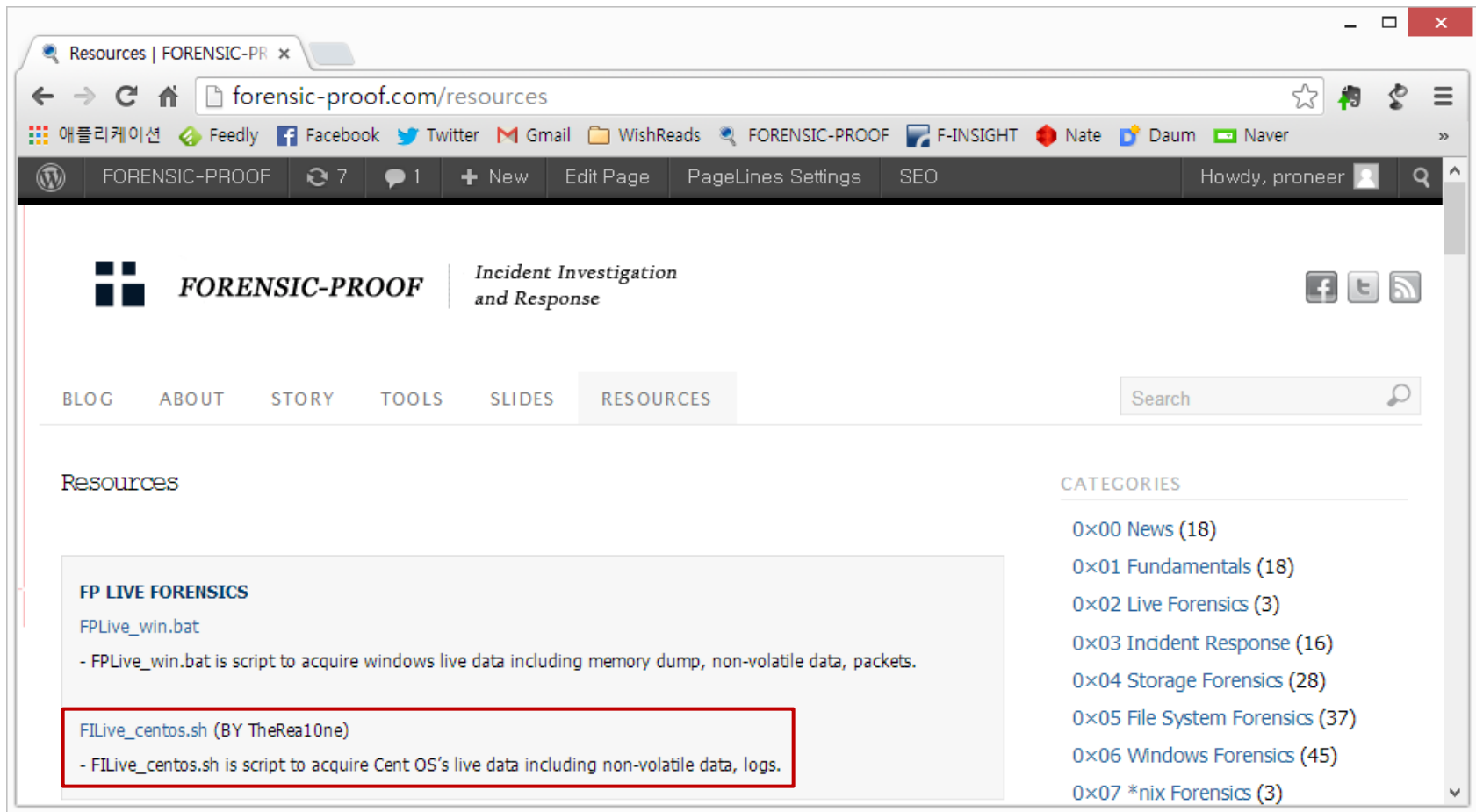
- 비활성 데이터 수집
 - 사용자 계정 폴더 숨긴 파일
 - ❖ \$HOME/.bashrc
 - ❖ \$HOME/.bash_profile
 - ❖ \$HOME/.bash_logout
 - ❖ \$HOME/.bash_history
 - ❖ \$HOME/.vimrc
 - ❖ \$HOME/.mozilla/*
 - ❖ \$HOME/.ssh
 - ❖ \$HOME/.cache/google-chrome/*
 - ❖ \$HOME/.config/google-chrome/Default
 - ❖ (홈 디렉터리 모든 숨긴 파일)

- 비활성 데이터 수집
 - 주요 사용 브라우저
 - ❖ 파이어폭스는 기본 브라우저
 - ❖ 추가적으로 크롬 브라우저를 많이 사용
 - 브라우저 아티팩트 경로
 - ❖ 파이어폭스
 - \$HOME/.mozilla/firefox/*.default
 - ❖ 크롬
 - \$HOME/.cache/google-chrome/Default
 - \$HOME/.config/google-chrome/Default
 - 브라우저 아티팩트
 - ❖ 아티팩트의 파일 형식은 윈도우와 동일(SQLite)

- 비활성 데이터 수집
 - 숨긴 파일
 - ❖ 파일명이 "."으로 시작하는 파일
 - ❖ 애플리케이션 세부 설정 정보
 - ❖ 로그인 시 실행되는 정보
 - ❖ 백도어나 지속 매킨즘의 가능성
 - .bash_history
 - ❖ 사용자 명령어 실행 이력 확인
 - ❖ 시간 정보는 포함하지 않음
 - ❖ 사용자에게 의해 임의로 수정 가능

- 비활성 데이터 수집
 - 썸네일
 - ❖ \$HOME/.thumbnails
 - 실행 프로세스의 바이너리
 - /var 하위의 로그 파일

- 라이브 데이터 - 수집 스크립트
 - <http://forensic-proof.com/resources>



- 라이브 데이터 - 수집 스크립트
 - <http://forensic-proof.com/resources>



The screenshot shows a terminal window titled 'root@localhost:/home/proneer/Downloads/FILive_centos'. The window contains the following text:

```
Forensic Insight Live Script for CentOS
                                by Forensic Insight TheReal10ne

1. Please enter case name : TESTCASE
Case Name : TESTCASE

2. Please enter examiner name : PRONEER
Examiner Name : PRONEER

CASE_NAME : TESTCASE
EXAMINER_NAME : PRONEER
Please check case name & exam name [Y/N] █
```

- 메모리 덤프
 - 시스템 메모리
 - ❖ `/dev/mem` → 전체 물리메모리에 접근할 수 없음
 - 커널 메모리
 - ❖ `/dev/kmem`

- 메모리 덤프 - 수집 도구

- **fmem** (<http://hysteria.sk/~niekt0/foriana>)

- ❖ 리눅스 커널 모듈(LKM, Linux Kernel Module)을 이용해 전체 메모리 접근
 - ❖ /dev/mem과 유사하게 물리메모리에 직접 접근
 - ❖ 가상 생성된 /dev/fmem은 dd(disk dumper) 형태의 도구로 접근 가능

- **LiME** (<http://code.google.com/p/lime-forensics/>)

- ❖ 리눅스 커널 모듈(LKM, Linux Kernel Module)을 이용해 전체 메모리 접근
 - ❖ 안드로이드와 네트워크 획득 기능 지원

- **Second Look®: The Linux Memory Forensic Acquisition**

(<http://secondlookforensics.com/>)

- ❖ 크래시 드라이브 + 스크립트로 이뤄진 상용 솔루션

- 메모리 덤프 - 수집 도구

- LiME (<http://code.google.com/p/lime-forensics/>)

1. **svn checkout** <http://lime-forensics.googlecode.com/svn/trunk/> lime-forensics-read-only
2. **make** (→ compile)
3. **insmod** lime.ko "path=<target dir>/lime_dump.dd format=lime" (→ load LKM)
4. **rmmod** lime

```
[root@ubuntu:/var/tmp]# ls
lime.ko
root@ubuntu:/var/tmp# insmod lime.ko "path=/var/tmp/lime_dump.dd format=lime"
root@ubuntu:/var/tmp# ll
total 1046256
-r--r--r--. 1 root root 4294441088 Mar  7 00:59 lime_dump.dd
root@ubuntu:/var/tmp# lsmod | grep lime
lime 12686 0
root@ubuntu:/var/tmp# rmmod lime
```

- 메모리 덤프 - 분석 도구

- **Volatility** (<https://github.com/volatilityfoundation>)

- ❖ 오픈소스 메모리 분석 도구
 - ❖ 윈도우, 리눅스, 맥 메모리 분석 지원

- **Foriana** (<http://hysteria.sk/~niekt0/foriana>)

- ❖ fmem 개발자가 함께 개발
 - ❖ 프로세스, 모듈, 파일 등 출력 지원

- **Volatilitux** (<http://code.google.com/p/volatilitux/>)

- ❖ 파이썬 기반의 메모리 분석 도구
 - ❖ ARM, x86, x86(PAE) 지원
 - ❖ 프로세스, 메모리맵, 파일 목록 등 지원
 - ❖ 안드로이드를 비롯해 다양한 리눅스 배포판 지원

- 메모리 덤프 – 볼라틸리티 준비

- 필수 패키지 설치

- ❖ `# yum install kernel-devel kernel-headers elfutils elfutils-devel gcc-c++`

- dwarfdump 설치

- ❖ DEBIAN*

- `# apt-get install dwarfdump`

- ❖ REDHAT*

- `# wget http://pkgs.fedoraproject.org/repo/pkgs/libdwarf/libdwarf-20130729.tar.gz/4cc5e48693f7b93b7aa0261e63c0e21d/libdwarf-20130729.tar.gz`

- `# ./configure`

- `# make`

- `# cd dwarfdump`

- ❖ `# cp ./dwarfdump /usr/local/bin`

- ❖ Source

- ➔ <http://reality.sgiweb.org/davea/dwarf.html>

- 메모리 덤프 – 볼라틸리티 준비
 - Module.dwarf 파일 생성
 - ❖ # **cd** /usr/local/src/volatility-read-only/tools/linux
 - ❖ # **make**
 - ❖ # **head** module.dwarf
 - System.map, module.dwarf 파일 압축
 - ❖ # **zip** /usr/local/src/volatility-read-only/volatility/plugins/overlays/linux/CentOS_64.zip
module.dwarf /boot/System.map-2.6.32-358.el6.i686

- 메모리 덤프 – 볼라틸리티 리눅스 프로파일
 - <https://github.com/volatilityfoundation/profiles/tree/master/Linux>
 - /usr/local/src/volatility-read-only/volatility/plugins/overlays/linux/ 하위로 복사

branch: master profiles / Linux / +

adding linux profiles

imHlv2 authored 20 days ago latest commit 756eb69245

CentOS	adding linux profiles	20 days ago
Debian	adding linux profiles	20 days ago
Fedora	adding linux profiles	20 days ago
OpenSUSE	adding linux profiles	20 days ago
RedHat	adding linux profiles	20 days ago
Ubuntu	adding linux profiles	20 days ago

- 메모리 덤프 – 볼라틸리티 리눅스 프로파일
 - 로드된 프로파일 확인

```
[root@localhost ~]# vol.py --info | grep Linux
```

```
Volatility Foundation Volatility Framework 2.4
```

```
LinuxCentOS64x86 - A Profile for Linux CentOS64 x86
```

```
linux_banner - Prints the Linux banner information
```

```
linux_yarascan - A shell in the Linux memory image
```

- 메모리 덤프 – 볼라틸리티 활용
 - 다양한 플러그인을 이용한 분석

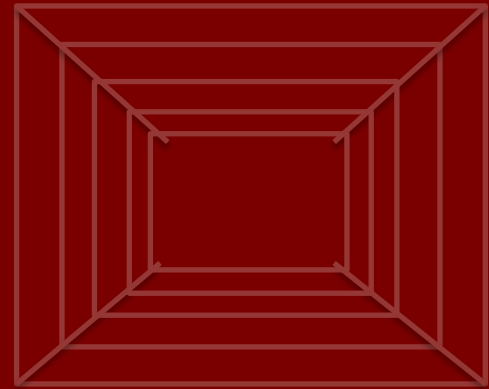
```
[root@localhost ~]# vol.py -f memory.dd --profile=LinuxCentOS64x86 linux_bash | more
```

Volatility Foundation Volatility Framework 2.4

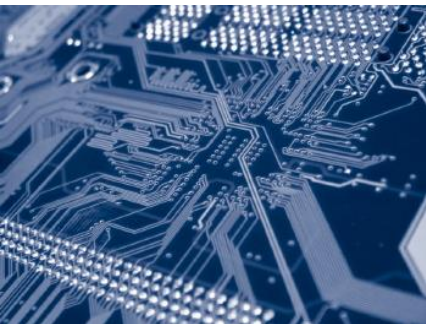
Pid	Name	Command Time	Command
2659	bash	2014-08-25 16:01:33 UTC+0000	vi host.conf
2659	bash	2014-08-25 16:01:33 UTC+0000	zdump
2659	bash	2014-08-25 16:01:33 UTC+0000	zdump localtime
2659	bash	2014-08-25 16:01:33 UTC+0000	ls -c
2659	bash	2014-08-25 16:01:33 UTC+0000	ll
2659	bash	2014-08-25 16:01:33 UTC+0000	ls
2659	bash	2014-08-25 16:01:33 UTC+0000	cat /etc/fstab
2659	bash	2014-08-25 16:01:33 UTC+0000	cat /etc/mtab
2659	bash	2014-08-25 16:01:33 UTC+0000	cd .cache

리눅스 시스템 침해사고 분석과 대응

3. 리눅스 데이터 수집



보안 | 신뢰



- 아티팩트 수집
 - 다양한 비활성 아티팩트 수집
 - 명령어 + 셸 스크립트
 - ❖ cp (copy) 명령을 이용한 자동화된 수집 스크립트 작성

- 저장장치 이미징

- 고려 사항

- ❖ 주로 라이브 환경에서 수집
 - ❖ RAID, LVM 환경 고려
 - ❖ 정확한 수집 데이터 저장위치 파악
 - ❖ 가능한 네트워크 인터페이스 활용
 - 외부 포트 → 추가 스토리지 장착 → 네트워크 인터페이스 (여분의 포트, 대역폭 제한)

- 소프트웨어 vs. 하드웨어

- ❖ 주로 소프트웨어 방식 사용
 - 별도 도구를 사용하기 보다는 "(dcfl)dd + nc" 를 주로 사용
 - ❖ 저장장치 분리가 가능한 경우 하드웨어 방식 사용

- 저장장치 이미징 – 소프트웨어

- 저장용 디스크 포맷

```
[root@localhost ~]# dcfldd if=/dev/zero of=/dev/sdb bs=4k conv=noerror,sync  
[root@localhost ~]# fdisk /dev/sdb  
[root@localhost ~]# shutdown -r now  
[root@localhost ~]# mkfs -t ext3 /dev/sdb1
```

- 저장용 디스크 폴더 구조

```
[root@localhost ~]# mount /dev/sdb1 /mnt/sdb1  
[root@localhost ~]# mkdir /mnt/sdb1/[case_##]  
[root@localhost ~]# mkdir /mnt/sdb1/[case_##]/[evidence_name]
```

- 저장장치 이미징 – 소프트웨어
 - 대상 시스템 정보 – 텍스트 파일 저장
 - ❖ 조사자 이름, 조직
 - ❖ 케이스 이름, 식별자, 증거 번호
 - ❖ 수집한 날짜, 시간
 - ❖ 시스템 제조사, 모델, 시리얼 번호
 - ❖ 저장장치 제조사, 모델, 시리얼 번호
 - ❖ IP 주소, 호스트명
 - ❖ 기타 특이 사항

- 저장장치 이미징 – 소프트웨어
 - 저장장치 마운트명 확인 (로컬 저장장치 vs. 저장용 저장장치)

```
[root@localhost ~]# fdisk -l
```

```
Disk /dev/sda: 21.5 GB, 21474836480 bytes
```

```
255 heads, 63 sectors/track, 2610 cylinders
```

```
Units = cylinders of 16065 * 512 = 8225280 bytes
```

```
Sector size (logical/physical): 512 bytes / 512 bytes
```

```
I/O size (minimum/optimal): 512 bytes / 512 bytes
```

```
Disk identifier: 0x000627db
```

Device	Boot	Start	End	Blocks	Id	System
/dev/sda1	*	1	39	307200	83	Linux
Partition 1 does not end on cylinder boundary.						
/dev/sda2		39	2354	18598912	83	Linux
/dev/sda3		2354	2611	2064384	82	Linux swap / Solaris

- 저장장치 이미징 – 소프트웨어

- 저장장치 정보 수집

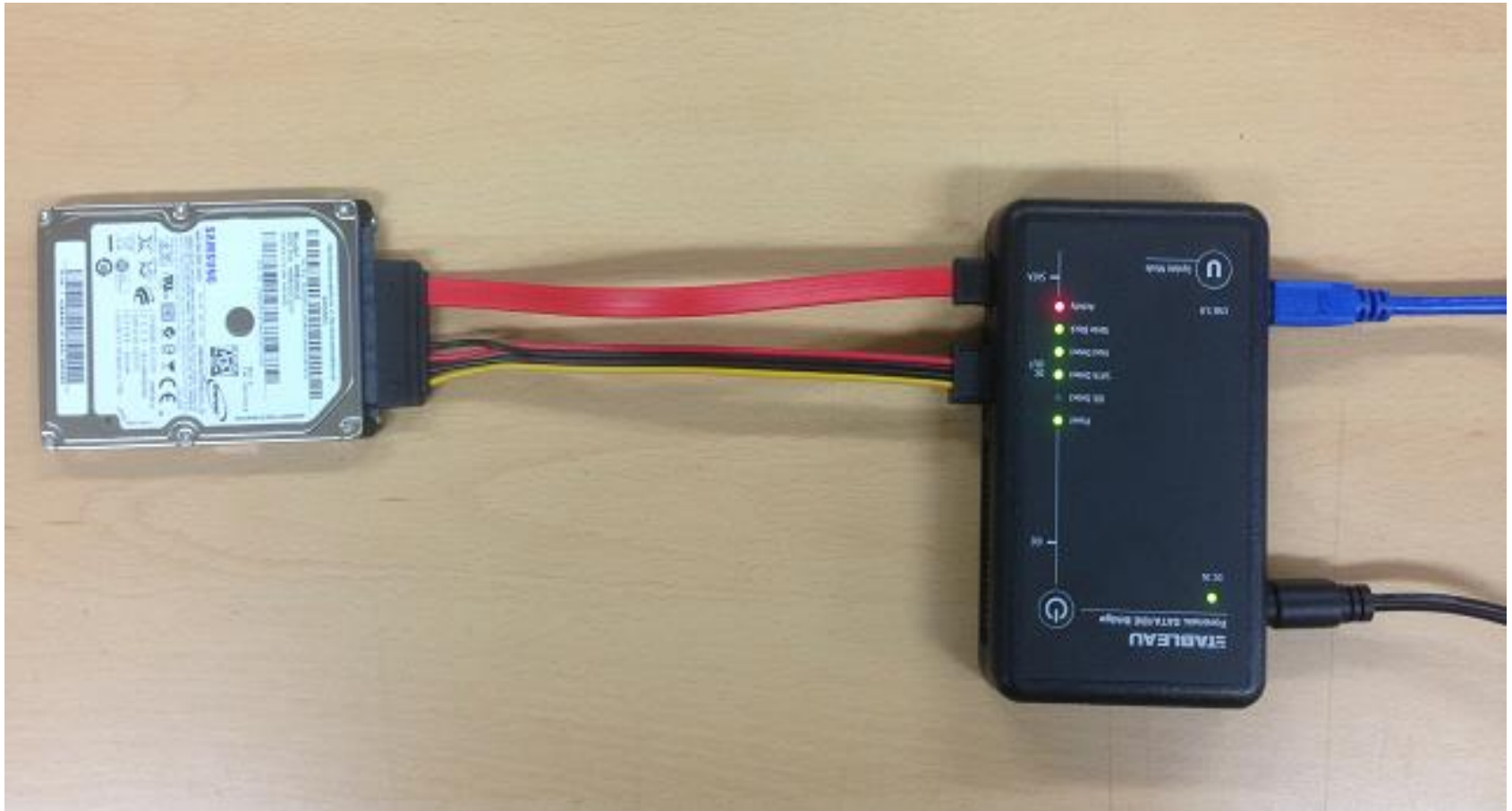
```
[root@localhost ~]# hdparm -gi /dev/sda2 | tee  
/dev/sdb1/[case_##]/[evidence_name]_hdram.txt
```

- 저장장치 이미징

```
[root@localhost ~]# dcfldd if=/dev/sda1 of=/mnt/sdb1/[evidence_name].dd  
conv=noerror, sync hashwindow=0 hashlog=dd.log
```

```
[root@localhost ~]# dcfldd if=/dev/sda1 of=/mnt/sdb1/[evidence_name].dd  
conv=noerror, sync hashwindow=0 hashlog=dd.log  
| 192.168.0.100 9999
```

- 저장장치 이미징 – 하드웨어
 - 쓰기 방지 장치

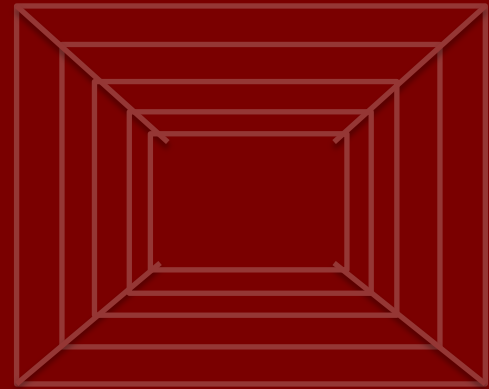


- 저장장치 이미징 – 하드웨어
 - 이미징/복제 장치

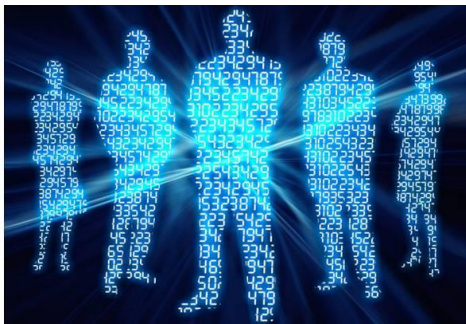
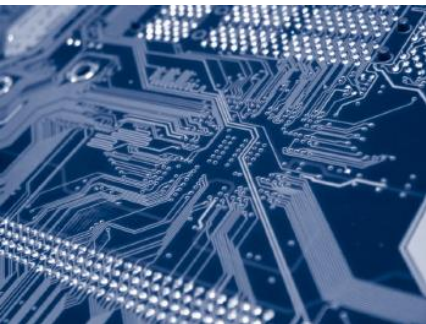


리눅스 시스템 침해사고 분석과 대응

4. 리눅스 데이터 분석



보안 | 신뢰



- 루트킷 점검

- Chkrootkit – <http://www.chkrootkit.org/download.htm>
- Rkhunter – http://www.rootkit.nl/projects/rootkit_hunter.html

- 알려진 악성코드 검사

- ClamAV 검사 – <http://www.clamav.net/>

- 비정상 계정 조사

- /etc/passwd, /etc/shadow, /etc/group, \$HOME
- 공격자가 생성한 계정 조사
- UID 0을 가지는 추가 계정 조사
- 패스워드를 가지고 있는 응용프로그램 계정 조사
> # **tail** – 5 /etc/passwd

- 비정상 데몬 조사

- /etc/inetd.d, /etc/xinetd.d
- 비정상적으로 설정이 변경된 데몬 조사
 - > # **grep** -v "^#" /etc/xinetd.d/*
 - > # **grep** -v "^#" /etc/httpd/conf/httpd.conf

- 바이너리 파일 변경 여부

- /bin, /sbin 폴더의 시스템 바이너리 변경 여부 조사
- 파일의 시간 정보나 아이노드 순서를 통해 점검
- 해시값 비교를 통해 변경 여부 검사
 - > # **ls** -lt /bin
 - > # **ls** -lt /sbin

- 비정상적인 경로에 생성된 파일
 - /dev 디렉터리에 생성된 정상 파일
 - > # **find** /dev/ -type f -exec ls -l {} \;
- 파일 속성 조사
 - "."으로 시작하는 숨긴 파일 조사
 - > # **find** ~ -name "." -print
- 권한, 소유자, 크기 확인
 - 파일의 권한이 너무 낮거나 높은 파일
 - 파일 소유자가 비정상적인 파일
 - 파일 크기가 큰 파일
 - > # **find** ~ -size +1024k -exec ls -lh {} \;

- **setuid, setgid가 설정된 파일 조사**
 - 시스템 상에 존재하는 모든 setuid, setgid
 - > # **find** / -user root -perm -4000 -print
- **백도어 점검**
 - 비정상 포트나 외부 연결 확인
 - > # **netstat** -nlp / > # **netstat** -an | grep LISTEN
 - > # **find** / -name .rhosts -print
 - > # **lsof** -I
- **웹셸 점검**
 - 웹 루트에서 웹셸 시그니처 검사
 - asp(x), asa, cer, cdx, php, jsp, htm(l), jpg, gif, bmp, png 등

- **지속 매커니즘 확인**

- /etc/inittab, /etc/init.d, /etc.rc.d
- /etc/init.conf, /etc/init
- /etc/profile, /etc/bash.bashrc
- /etc/vimrc, /etc/virc
- /etc/csh.cshrc, /etc/csh.login
- /etc/cron*
- /var/spool/cron/*
- \$HOME/.bashrc, \$HOME/.bash_profile, \$HOME/.bash_logout
- \$HOME/.vimrc, \$HOME/.xinitrc

• 리눅스 각종 로그

로그 이름	형식	설명
dmesg, boot	텍스트	부팅될 때 출력되거나 로깅되는 정보
secure	텍스트	사용자 인증 관련 정보
btmp, failedlogin	텍스트	로그인 실패 정보
maillog	텍스트	메일 데몬과 관련된 정보
messages	텍스트	화면에 출력되는 메시지 정보
xferlog	텍스트	FTP 데몬을 통해 송수신되는 정보
access_log	텍스트	웹 서버의 접근 로그
error_log	텍스트	웹 서버의 에러 로그
utmp, utmpx	바이너리	현재 로그인한 사용자의 상태 정보
wtmp, wtmpx	바이너리	사용자의 로그인, 로그아웃 정보
lastlog	바이너리	사용자의 최근 로그인 정보
pacct	바이너리	각 사용자별 프로세스, 명령어 정보

• 로그 분석

▪ utmp, utmpx

- ❖ /var/run/utmp (바이너리)
- ❖ 시스템에 현재 로그인한 사용자들의 상태 정보
- ❖ 사용자 이름, 터미널 장치 이름, 원격 호스트 이름, 로그인 시간, 로그인 기간 등
- ❖ "w", "who", "users", "finger" 등의 명령을 통해 내용 확인 가능

```
proneer@localhost:/var/log
File Edit View Search Terminal Help
[proneer@localhost log]$ w
00:47:16 up 2:14, 3 users, load average: 0.00, 0.00, 0.00
USER      TTY      FROM          LOGIN@   IDLE   JCPU   PCPU WHAT
proneer   tty1     :0             22:36    2:14m 34.87s 0.14s pam: gdm-password
proneer   pts/0    :0.0           22:36    0.00s 0.77s 0.60s w
proneer   pts/1    :0.0           23:18    57:46 0.02s 0.02s bash
[proneer@localhost log]$
```

- 접속된 사용자가 모두 정상 사용자인가?
- 접속 IP의 위치가 비정상적인가?
- 사용자 행위가 정상적인가?

- 로그 분석

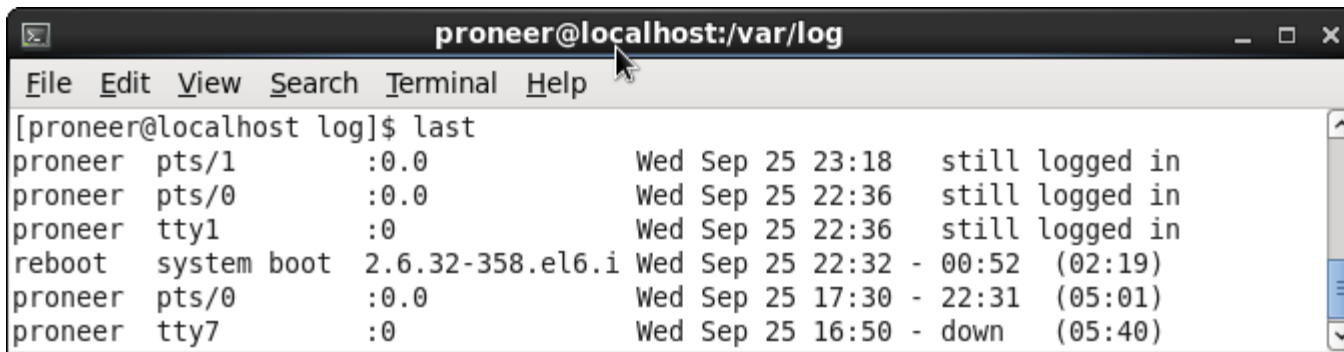
- wtmp, wtmpx

- ❖ /var/log/wtmp (바이너리)

- ❖ 각 사용자별 로그인/로그아웃 정보, 시스템 종료 정보, 부팅 관련 히스토리 등

- ❖ "last" 명령을 통해 내용 확인 가능

- ❖ 로그가 꽉 차면 "wtmp.1"로 백업



A terminal window titled 'proneer@localhost:/var/log' showing the output of the 'last' command. The output lists login and system events for the previous session.

Username	Terminal	IP Address	Date and Time	Session Info
proneer	pts/1	:0.0	Wed Sep 25 23:18	still logged in
proneer	pts/0	:0.0	Wed Sep 25 22:36	still logged in
proneer	tty1	:0	Wed Sep 25 22:36	still logged in
reboot	system boot	2.6.32-358.el6.i	Wed Sep 25 22:32 - 00:52	(02:19)
proneer	pts/0	:0.0	Wed Sep 25 17:30 - 22:31	(05:01)
proneer	tty7	:0	Wed Sep 25 16:50 - down	(05:40)

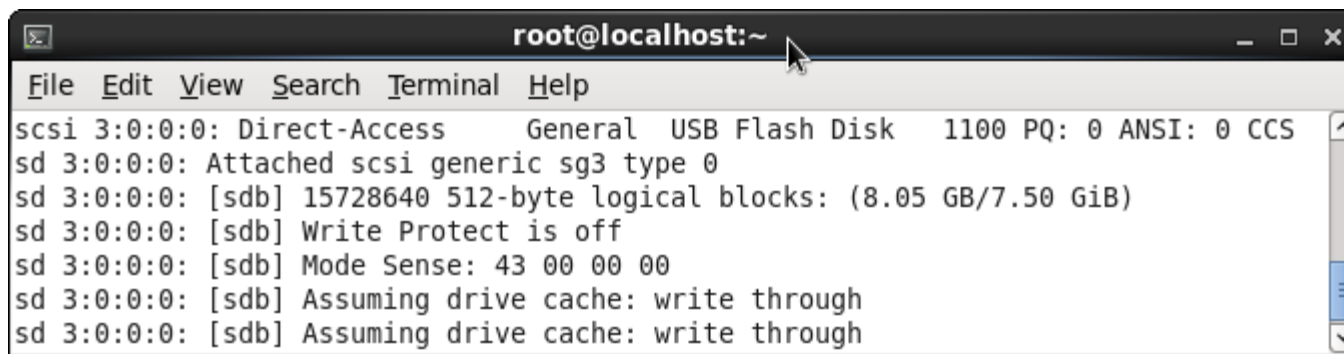
- ❖ 분석 관점

- 접속 시간이 업무 시간대인가?
 - 접속 IP의 위치가 비정상적인가?

- 로그 분석

- dmesg, boot

- ❖ /var/log/dmesg, /var/log/boot.log (텍스트)
 - ❖ 부팅 시 출력되는 메시지 저장
 - ❖ 부팅 과정에 발생하는 메시지를 살펴볼 필요가 있을 경우 활용
 - ❖ "dmesg" 명령으로 /var/log/dmesg 내용 확인 가능



```
root@localhost:~  
File Edit View Search Terminal Help  
scsi 3:0:0:0: Direct-Access      General  USB Flash Disk  1100 PQ: 0 ANSI: 0 CCS  
sd 3:0:0:0: Attached scsi generic sg3 type 0  
sd 3:0:0:0: [sdb] 15728640 512-byte logical blocks: (8.05 GB/7.50 GiB)  
sd 3:0:0:0: [sdb] Write Protect is off  
sd 3:0:0:0: [sdb] Mode Sense: 43 00 00 00  
sd 3:0:0:0: [sdb] Assuming drive cache: write through  
sd 3:0:0:0: [sdb] Assuming drive cache: write through
```

- ❖ 분석 관점

- 부팅 과정에서 발생한 오류는 없는가?
 - 부팅 과정에서 발생한 비정상적인 행위는 없는가?

- 로그 분석

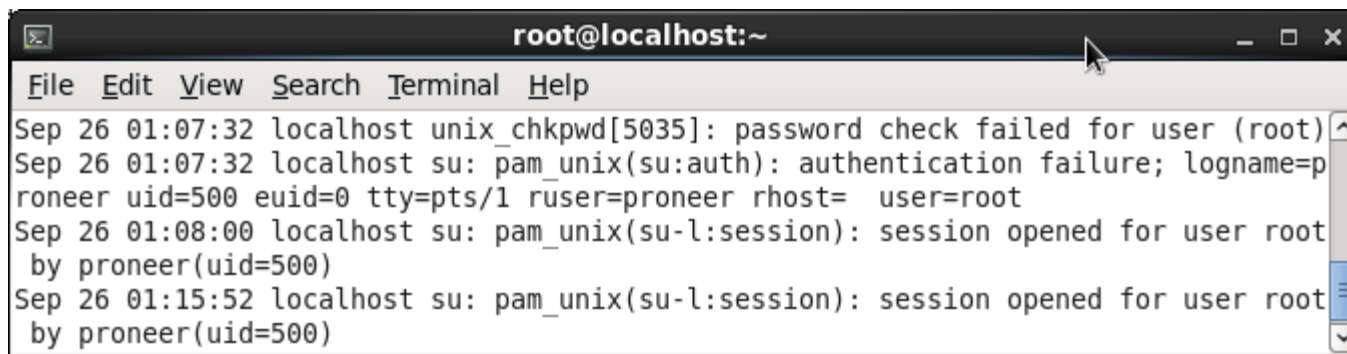
- secure

- ❖ /var/log/secure (텍스트)

- ❖ 사용자 인증과 관련된 로그, 커널/데몬에 의해 생성되는 로그

- ❖ rsh, rlogin, ftp, telnet, pop3 등의 접속 성공/실패 기록 등 보안과 밀접한 관련

- ❖ 보안 문제가 발생할 경우 가장 먼저 백업 후 분석해야 할 로그



A terminal window titled 'root@localhost:~' showing log entries from /var/log/secure. The window has a menu bar with File, Edit, View, Search, Terminal, and Help. The log entries are as follows:

```
Sep 26 01:07:32 localhost unix_chkpwd[5035]: password check failed for user (root)
Sep 26 01:07:32 localhost su: pam_unix(su:auth): authentication failure; logname=p
roneer uid=500 euid=0 tty=pts/1 ruser=proneer rhost= user=root
Sep 26 01:08:00 localhost su: pam_unix(su-l:session): session opened for user root
by proneer(uid=500)
Sep 26 01:15:52 localhost su: pam_unix(su-l:session): session opened for user root
by proneer(uid=500)
```

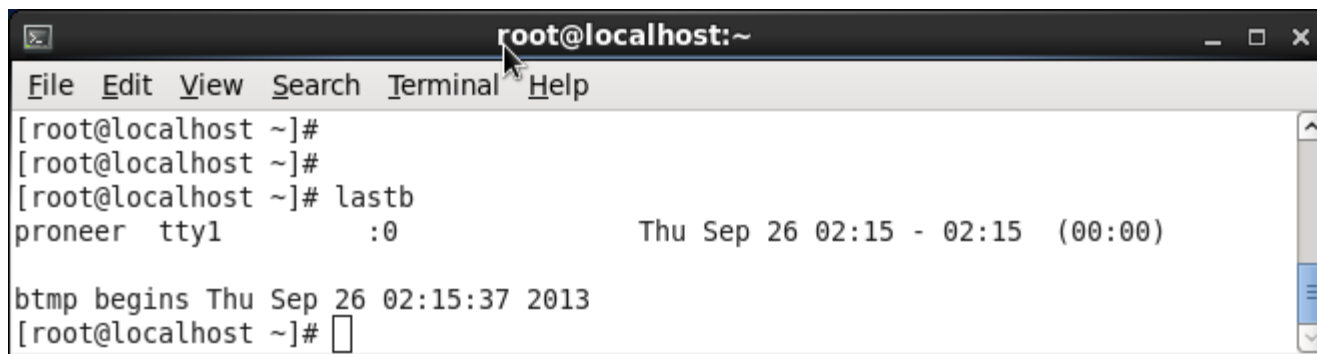
- ❖ 분석 관점

- 정상적으로 이뤄진 인증인가?
 - 무차별 인증 시도가 있는가?

- 로그 분석

- btmp

- ❖ /var/log/btmp (텍스트)
 - ❖ 로그인 실패 기록으로 사용자 ID, 터미널 이름, 시간 정보 등이 저장
 - ❖ "messages" 로그와 연관 분석
 - ❖ "lastb" 명령으로 내용 확인 가능



```
root@localhost:~  
File Edit View Search Terminal Help  
[root@localhost ~]#  
[root@localhost ~]#  
[root@localhost ~]# lastb  
proneer tty1 :0 Thu Sep 26 02:15 - 02:15 (00:00)  
  
btmp begins Thu Sep 26 02:15:37 2013  
[root@localhost ~]#
```

- ❖ 분석 관점

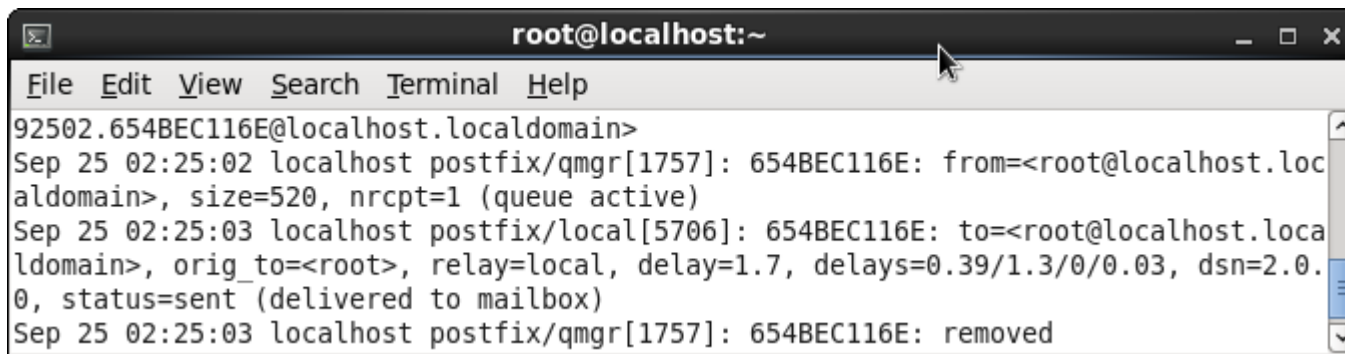
- 특정 IP 혹은 특정 계정에 대해 다수의 접속 실패가 있었는가?
 - 짧은 시간 안에 혹은 주기적으로 접속 실패가 있었는가?

- 로그 분석

- maillog

- ❖ /var/log/maillog (텍스트)

- ❖ 메일 데몬과 관련된 로그

A terminal window titled 'root@localhost:~' with a menu bar (File, Edit, View, Search, Terminal, Help). The terminal output shows three lines of maillog data: a header line for a message from root@localhost.localdomain, a line from postfix/qmgr[1757] showing the message was received, and a line from postfix/local[5706] showing the message was delivered to the mailbox. The last line shows the message was removed from the queue.

```
root@localhost:~  
File Edit View Search Terminal Help  
92502.654BEC116E@localhost.localdomain>  
Sep 25 02:25:02 localhost postfix/qmgr[1757]: 654BEC116E: from=<root@localhost.localdomain>, size=520, nrcpt=1 (queue active)  
Sep 25 02:25:03 localhost postfix/local[5706]: 654BEC116E: to=<root@localhost.localdomain>, orig_to=<root>, relay=local, delay=1.7, delays=0.39/1.3/0/0.03, dsn=2.0.0, status=sent (delivered to mailbox)  
Sep 25 02:25:03 localhost postfix/qmgr[1757]: 654BEC116E: removed
```

- ❖ 분석 관점

- 의도하지 않은 메일이 전송된 적이 있는가?
 - 스팸 메일이 발송된 적이 있는가?

• 로그 분석

▪ lastlog

- ❖ /var/log/lastlog (바이너리)
- ❖ 각 사용자의 가장 최근 로그인 시간, IP 등의 정보 저장
- ❖ "wtmp(x)", "utmp(x)" 로그와 연관 분석
- ❖ "lastlog" 명령으로 내용 확인 가능

```

root@localhost:~
File Edit View Search Terminal Help
Username      Port      From      Latest
root          *Never   logged in**
bin           *Never   logged in**
daemon        *Never   logged in**
adm           *Never   logged in**
lp            *Never   logged in**
sync          *Never   logged in**
  
```

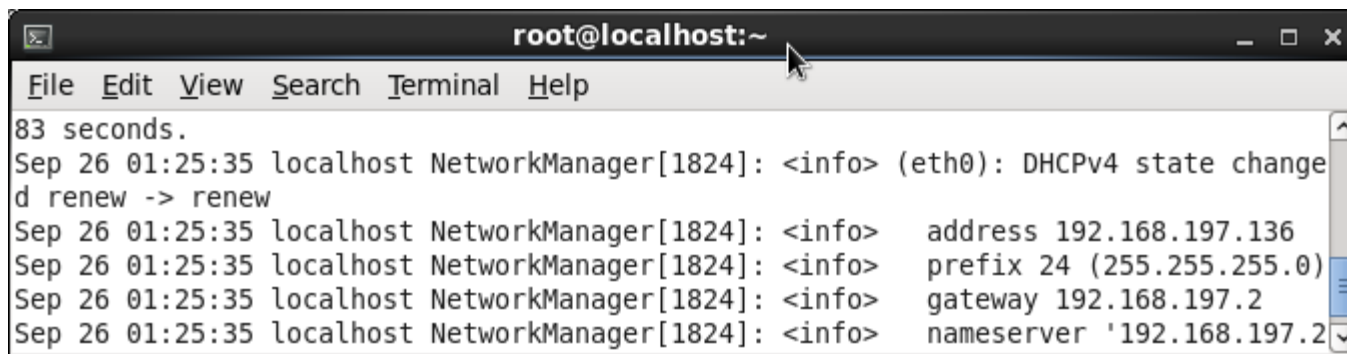
❖ 분석 관점

- 로그인하지 않는 유휴 계정이 존재하는가?
- 접속 IP의 위치가 비정상적인가?

- 로그 분석

- messages

- ❖ /var/log/messages (텍스트)
 - ❖ 시스템 로그 파일로 시간 정보, 호스트명, 프로그램명, 메시지 정보 저장
 - ❖ su 실패에 대한 로그, 데몬 상태 변경 로그, 부팅 에러 등 다양한 정보 저장
 - ❖ 보안 사고 발생 시 가장 먼저 분석해야 하는 로그 중 하나



A screenshot of a terminal window titled 'root@localhost:~'. The terminal displays the output of the 'cat /var/log/messages' command. The output shows a series of log messages from the NetworkManager service. The first line is '83 seconds.' followed by a log entry: 'Sep 26 01:25:35 localhost NetworkManager[1824]: <info> (eth0): DHCPv4 state change d renew -> renew'. This is followed by four more log entries, all at the same timestamp, showing configuration details: 'address 192.168.197.136', 'prefix 24 (255.255.255.0)', 'gateway 192.168.197.2', and 'nameserver '192.168.197.2''. The terminal window has a menu bar with 'File', 'Edit', 'View', 'Search', 'Terminal', and 'Help'.

```
root@localhost:~  
File Edit View Search Terminal Help  
83 seconds.  
Sep 26 01:25:35 localhost NetworkManager[1824]: <info> (eth0): DHCPv4 state change  
d renew -> renew  
Sep 26 01:25:35 localhost NetworkManager[1824]: <info> address 192.168.197.136  
Sep 26 01:25:35 localhost NetworkManager[1824]: <info> prefix 24 (255.255.255.0)  
Sep 26 01:25:35 localhost NetworkManager[1824]: <info> gateway 192.168.197.2  
Sep 26 01:25:35 localhost NetworkManager[1824]: <info> nameserver '192.168.197.2'
```

- 비정상 로그는 없는가? (BOF의 경우 보통 비정상 로그가 기록됨)
 - 특정 프로그램의 시스템 로그를 확인해야 하는가?
 - 인가하지 않은 시스템 상태 변경이 있는가?

- 로그 분석

- xferlog

- ❖ /var/log/xferlog (텍스트)

- ❖ ftp 데몬으로 송수신되는 모든 데이터 메타 기록

- ❖ 송수신 대상 이름/크기, 시간, 원격 호스트, 사용자 등의 정보

- ❖ 기본으로는 남지 않기 때문에 ftp 데몬 설정 파일을 로깅하도록 변경

- ❖ 분석 관점

- 접속 시간이 정상적인가?

- 접속 IP의 위치가 비정상적인가?

- 송수신한 파일에 기밀 정보나 공격용 도구가 포함되어 있지 않는가?

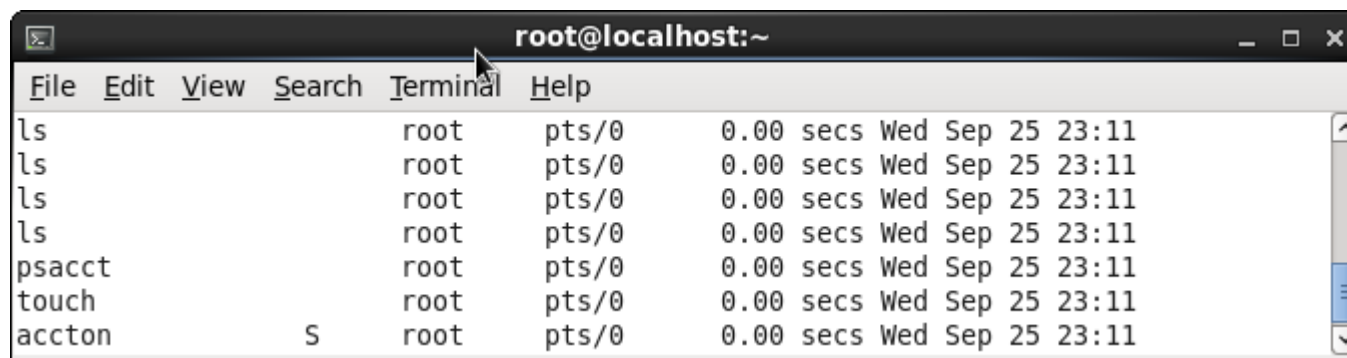
- 로그 분석

- pacct

- ❖ /var/account/pacct (바이너리)

- ❖ 각 사용자와 관련된 프로세스 정보나 명령어 저장

- ❖ "lastcomm" 명령으로 내용 확인



Command	User	Shell	Duration	Date	Time
ls	root	pts/0	0.00 secs	Wed Sep 25	23:11
ls	root	pts/0	0.00 secs	Wed Sep 25	23:11
ls	root	pts/0	0.00 secs	Wed Sep 25	23:11
ls	root	pts/0	0.00 secs	Wed Sep 25	23:11
psacct	root	pts/0	0.00 secs	Wed Sep 25	23:11
touch	root	pts/0	0.00 secs	Wed Sep 25	23:11
accton	root	pts/0	0.00 secs	Wed Sep 25	23:11

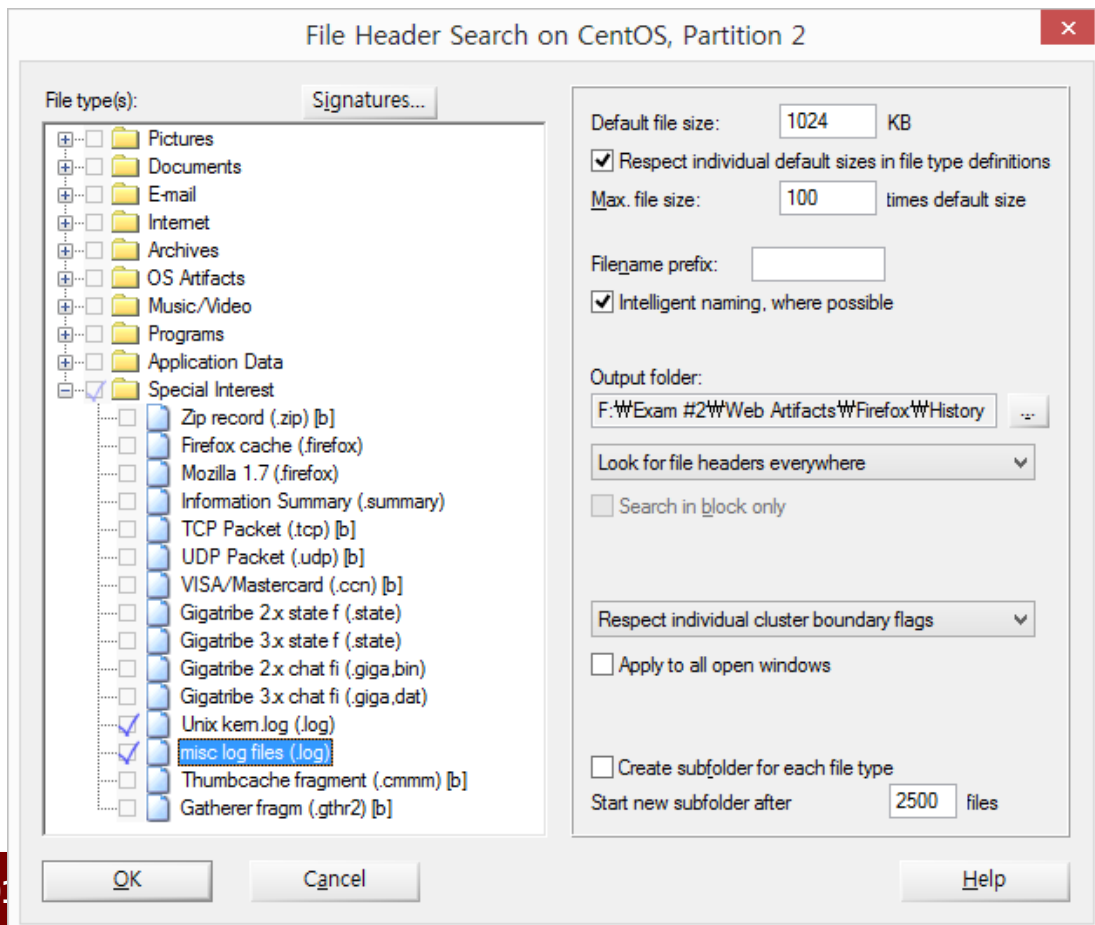
- ❖ 분석 관점

- 의도하지 않은 계정 사용이 있는가?

- 비정상적인 명령 실행이 있는가?

• 로그 파일 복구

- 리눅스는 대부분 고유한 형식의 텍스트 기반의 로그 → 고유 형식으로 카빙
- 카빙된 로그 파일을 다시 타임라인 분석이나 로그 통합/정밀 분석에 이용



- 로그 파일 복구
 - 리눅스 명령 + 정규 표현식

```
[root@localhost forensic]# strings /dev/sda | egrep "[A-Z][a-z]{1,2} ( [0-9]|[0-9]{1,2}) [0-9]+:[0-9]+:[0-9]+  
localhost"
```

```
Jul 31 13:17:15 localhost syslogd 1.4.1: restart.  
Jul 31 13:18:31 localhost dhclient: DHCPREQUEST on eth0 to 192.168.8.254 port 67  
Jul 31 13:18:31 localhost dhclient: DHCPACK from 192.168.8.254  
Jul 31 13:18:31 localhost dhclient: bound to 192.168.8.138 -- renewal in 703 seconds.  
Jul 31 13:19:34 localhost gconfd (root-6017):  
Jul 31 13:19:34 localhost gconfd (root-6017):  
Jul 31 13:19:34 localhost scim-bridge: Panel client has not yet been prepared  
Jul 31 13:19:34 localhost last message repeated 2 times  
Jul 31 13:19:34 localhost pcscd: winscard.c:304:SCardConnect() Reader E-Gate 0 0 Not Found  
Jul 31 13:19:34 localhost gconfd (root-9203):  
Jul 31 13:19:34 localhost gconfd (root-9203):  
Jul 31 13:19:35 localhost scim-bridge: Failed to open the panel socket  
Jul 31 13:19:35 localhost scim-bridge: Panel client has not yet been prepared  
Jul 31 13:19:35 localhost last message repeated 2 times  
Jul 31 13:19:35 localhost scim-bridge: The lockfile is destroyed  
Jul 31 13:19:35 localhost scim-bridge: Cleanup, done. Exiting...  
Jul 31 13:19:36 localhost smartd[3938]: smartd received signal 15: Terminated  
Jul 31 13:19:36 localhost smartd[3938]: smartd is exiting (exit status 0)  
Jul 31 13:19:36 localhost avahi-daemon[3880]: Got SIGTERM, quitting.
```

.....

4. 리눅스 데이터 분석

• 로그 타임라인 분석

▪ 도구 다운로드

❖ Plaso – <http://plaso.kiddaland.net/>

❖ log2timeline – <http://log2timeline.net/>

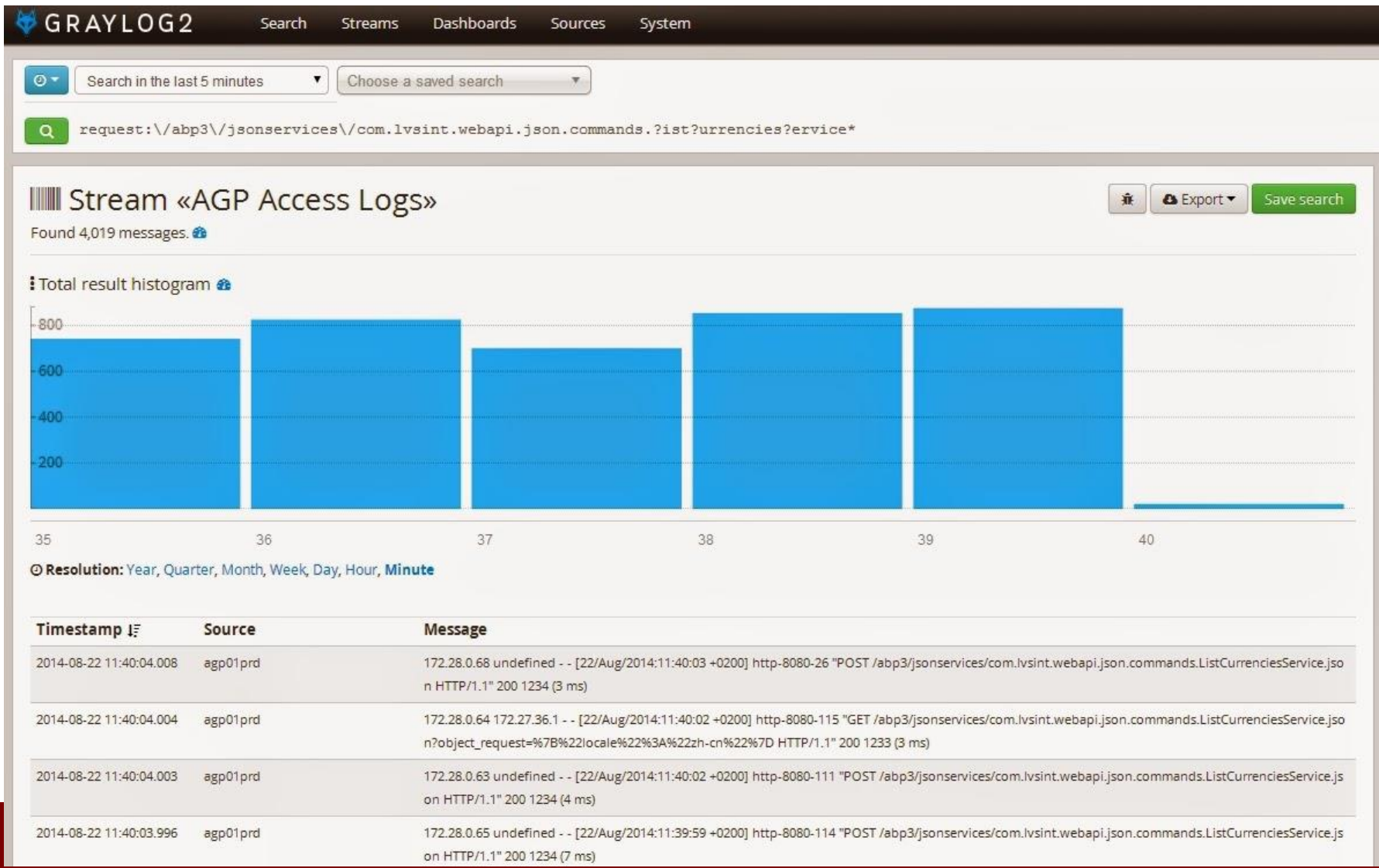
▪ 타임라인 생성

```
# log2timeline.py [-z TIMEZONE] -p /path/to/output.dump /path/mount_point
```

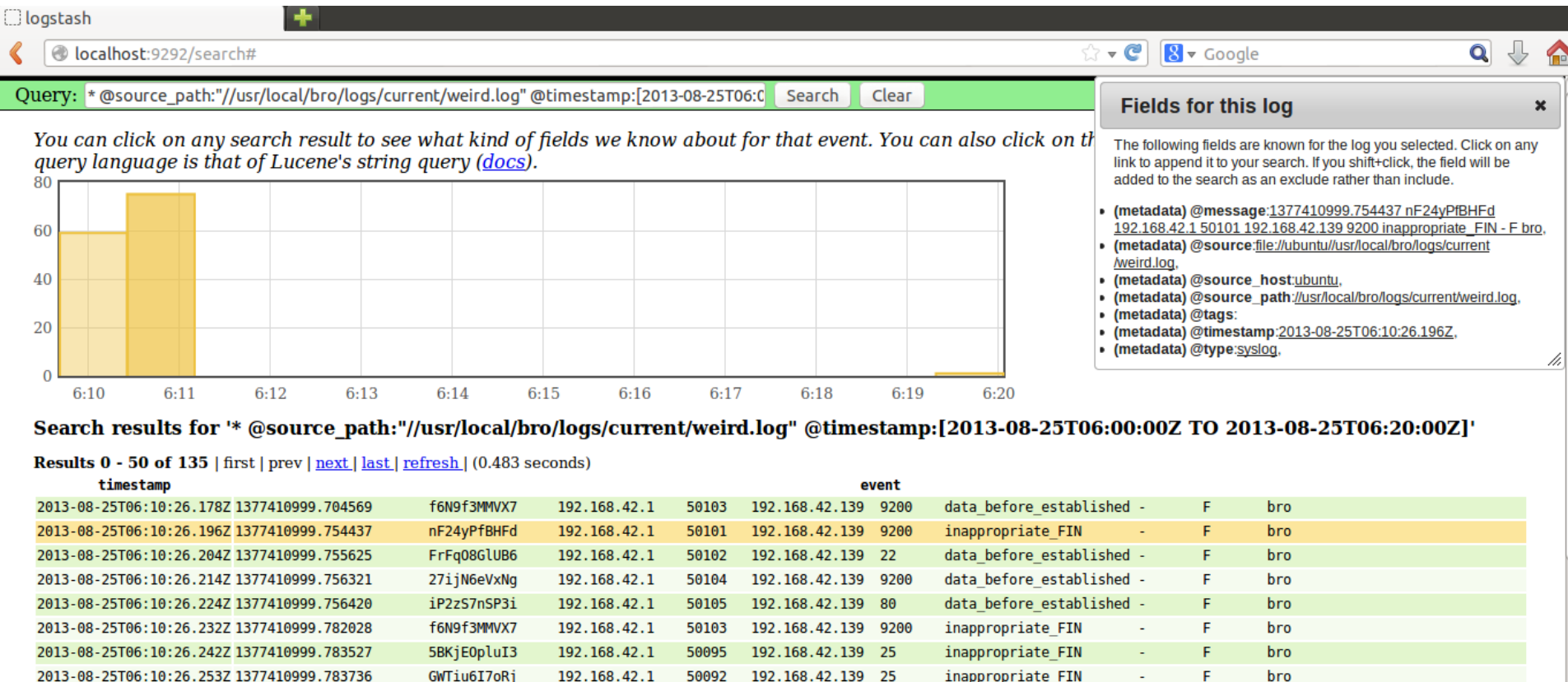
6/18/2009	23:33:57	EST5EDT	MACB	REG	Deleted Registry	Last Written	[DELETED] ???/0000000E/00000000/
6/18/2009	23:33:57	EST5EDT	MACB	REG	Deleted Registry	Last Written	[DELETED] ???/{83da6326-97a6-4088-9453-a1923f573b29}/00000003/00000000/
6/18/2009	23:33:57	EST5EDT	MACB	REG	Deleted Registry	Last Written	[DELETED] ???/00000003/00000000/
6/18/2009	23:33:57	EST5EDT	MACB	REG	Deleted Registry	Last Written	[DELETED] ???/00000008/00000000/
6/18/2009	23:34:09	EST5EDT	MACB	PRE	Vista/Win7 Prefetch	Last run	PKMAILER.EXE-83FAD500.pf: PKMAILER.EXE was executed
6/18/2009	23:34:35	EST5EDT	MACB	REG	NTUSER key	Last Written	Software/Google/GoogleToolbarNotifier/Stats
6/18/2009	23:34:36	EST5EDT	MACB	REG	NTUSER key	Last Written	Software/Google/GoogleToolbarNotifier/Temp
6/18/2009	23:34:50	EST5EDT	MACB	PRE	Vista/Win7 Prefetch	Last run	IPODSERVICE.EXE-FE1A6FF7.pf: IPODSERVICE.EXE was executed
6/18/2009	23:34:59	EST5EDT	MACB	PRE	Vista/Win7 Prefetch	Last run	RUNDLL32.EXE-2E65B341.pf: RUNDLL32.EXE was executed
6/18/2009	23:34:59	EST5EDT	MACB	REG	UserAssist key	Time of Launch	UEME_RUNPATH:C:/Windows/system32/rundll32.exe
6/18/2009	23:35:05	EST5EDT	MACB	LSO	Flash Cookie	LSO created	Flash Cookie: site ui/preferences
6/18/2009	23:35:07	EST5EDT	MACB	REG	NTUSER key	Last Written	Software/Microsoft/InternetExplorer/LowRegistry/Audio/PolicyConfig/PropertyStore/5447cc
6/18/2009	23:35:38	EST5EDT	MACB	REG	UserAssist key	Time of Launch	UEME_RUNPATH:Mozilla Firefox.lnk
6/18/2009	23:35:39	EST5EDT	MACB	REG	UserAssist key	Time of Launch	UEME_RUNPATH:C:/Program Files/Mozilla Firefox/firefox.exe
6/18/2009	23:35:39	EST5EDT	MACB	PRE	Vista/Win7 Prefetch	Last run	FIREFOX.EXE-E60C0AA7.pf: FIREFOX.EXE was executed
6/18/2009	23:41:36	EST5EDT	MACB	REG	Deleted Registry	Last Written	[DELETED] ???/00000003/
6/18/2009	23:41:36	EST5EDT	MACB	REG	Deleted Registry	Last Written	[DELETED] ???/{83da6326-97a6-4088-9453-a1923f573b29}/
6/18/2009	23:41:36	EST5EDT	MACB	REG	Deleted Registry	Last Written	[DELETED] ???/0000000E/
6/18/2009	23:41:36	EST5EDT	MACB	REG	Deleted Registry	Last Written	[DELETED] ???/00000008/

- 리눅스 로그 분석 도구
 - Graylog2, <http://graylog2.org/>
 - Logstash, <http://logstash.net/>
 - Apache Flume, <http://flume.apache.org/>
 - Graphite, <http://graphite.wikidot.com/>
 - Kibana, <http://www.elasticsearch.org/overview/kibana/>
 - Scribe, <https://github.com/facebookarchive/scribe>
 - Chukwa, <https://chukwa.apache.org/>

- 리눅스 로그 분석 도구 – Graylog2, <http://graylog2.org/>



- 리눅스 로그 분석 도구 - Logstash, <http://logstash.net/>



- 리눅스 로그 분석 도구
 - **ELK (ElasticSearch + Logstash + Kibana)**
 - ❖ Logstash – 로그 데이터 수집 관리
 - ❖ Kibana – 프론트 엔진
 - ❖ ElasticSearch – 검색 엔진
 - **EPK (ElasticSearch + Plaso + Kibana)**
 - **ElasticSearch + Kibana vs. Splunk**

- 리눅스 로그 분석 도구
 - ELK (ElasticSearch + Logstash + Kibana)

