Forensic

08. 5. 19.

지현석(binish@binish.or.kr)

http://binish.or.kr

Index

- Forensic?
  - Forensic Methodologies
  - Forensic Target
- Evidence Searching
- Evidence Analysis
- Anti-Forensics Methods
- Further more and Q&A

Forensic?

- "Gathering and analyzing data in a manner as free from distortion or bias as possible to reconstruct data or what happened in the past on a system [or a network]“ - Dan Farmer / Wietse Venema (1999)

- “증거훼손”
  - 범죄 현장을 다루는데 있어 가장 주의해야 할 사항
  - ‘범죄자와 똑같이 생각하라’

Forensic Methodologies

- Traditional Forensics
  - Analyzing a “dead” system that has had it’s power cord pulled
  - Least chance of modifying data on disk, but “live” data is lost forever
    - This method is great for preserving data on disk, but you lose a lot of volatile data which may be useful

- Live Forensics (Often Incident Response)
  - Methodology which advocates extracting “live” system data before pulling the cord to preserve memory, process, and network information that would be lost with traditional forensic approach
  - Goal is to minimize impacts to the integrity of the system while capturing volatile forensic data

Forensic Target

- Data on Disk
  - “Disk Imaging” 피해 시스템의 저장매체 증거 보존
    - Bit 단위 수행, “dd”
- Volatile Data
  - 저장매체의 전원 공급이 차단되거나 시간이 지남에 따라 사라지는 정보
  - 증거 휘발성의 순서
    - 레지스터와 캐시
    - 라우팅 테이블, ARP cash table, 프로세스 테이블, 커널 통계
    - RAM, Cash, VGA, NIC등의 시스템 onBoard 메모리
    - 임시 파일 시스템, 디스크의 데이터
  - 시스템 상태
    - “Live Data” 시스템이 운영되는 현황을 나타내는 데이터
      - 네트워크 상태(netstat, ipconfig), 프로세스 상태(ps) 등

Disk Imaging

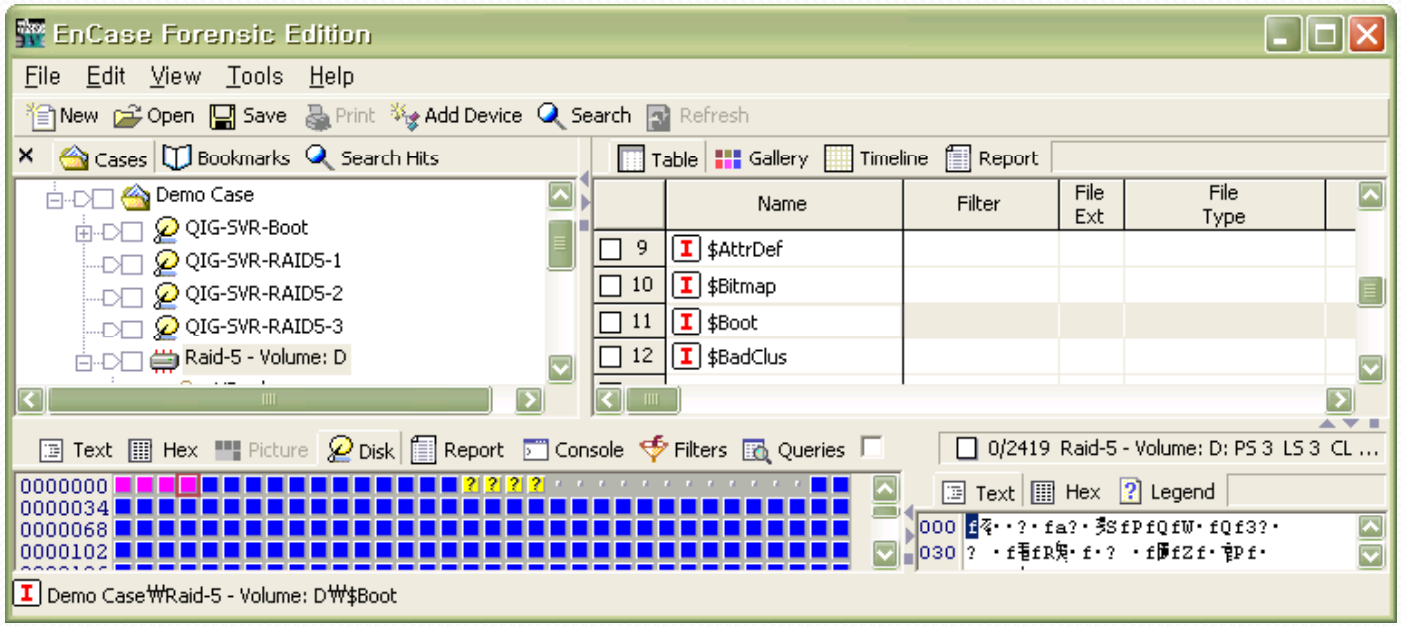
- Disk Imaging

구분	Disk Copy	Disk Image
저장방식	Read & Write	Bit Stream
저장대상	파일과 디렉토리 정보	모든 물리적 섹터
정보손실	Read 과정에서 오류 가능성 존재	거의 없음
파일복구	삭제된 파일은 복사 과정에서제외	섹터상의 파일 모두 복구

- 직접적인 분석은 증거물이 손상의 우려가 있음 → Imaging & mount 이용
  - Disk Image : 디스크와 정확히 같은 사본 파일
  - Image Mount : Image를 디스크로 OS에 인식 시키는 과정

Disk Imaging Tools

- Disk Imaging Tools
  - Encase
    - 그래픽 인터페이스 제공, 이미지 생성 (Bit Stream)
    - 증거 미리 보기, 데이터 검색과 분석
    - 윈도우, Palm OS등의 플랫폼과 RAID 방식 지원
    - 국내외 널리 사용되는 도구
    - 상용 프로그램



Disk Imaging Tools

- Linux/UNIX “dd”
  - 디스크 이미지 파일 생성
    - dd if=장치명 of=파일이름
    - dd if=/dev/fdo of=disk.img
  - 파일을 디스크에 복구
    - dd if=파일이름 of=/dev/fdo
    - dd if=disk.img of=/dev/fdo
  - 이미지 mount
    - mount [image path] [mount path] –r –o loop –t ext2
    - mount /forensic/disk.img /mnt/disk –r –o loop –t ext2

Volatile Data Acquisition

- Volatile Data Acquisition
  - 시스템의 상태를 변경 → Forensic Live CD
    - Ex) F.I.R.E.(Forensic & Incident Response Environment, freeware), fire-0.3.5b.iso
  - 많은 수집 도구를 순차적이고 자동으로 실행 하는 Shell Script 개발
    - Like, Server Penetration Test에서의 취약점 진단 Shell Script → 컨설턴트 기술력
  - 기 설치된 정보 수집 Agent에서 증거를 수집 하는 기술
    - Snap Shot
  - 수집 대상 운영체제의 프로그램이나 라이브러리를 사용하지 않고도 증거를 수집 할 수 있는 기술 개발 필요
    - Why? Rootkit 설치로 인해 변조된 프로그램 및 라이브러리 존재 가능
      - Hidden process, port, files..
    - 동일 OS의 정상적인 바이너리를 복사해서 사용하는 경우도 발생

Volatile Data Acquisition Tools

- Forensic Script
  - 시스템 정보 및 휘발성 데이터 획득을 위해 일련의 명령어를 수행하여 자동으로 정보를 수집하는 BAT, Shell Script 파일
  - Static Library 사용의 실행 파일 필요

```
@echo  = 초기 분석 점검 날짜 =
date /t

@echo  = 초기 분석 점검 시간 =
time /t
••••••••••••••••••
@echo  = 키 스트로크 정보 =
doskey /history

@echo  = 초기 분석 종료 정보 =
time /t
```

Volatile Data Acquisition Tools

- Memory Dump
  - Memory의 전체 내용을 수집하여 각 프로세스의 세부 내용을 분석
    - Linux : dd if=/dev/mem of=Linux.dump
      - tip) gdb –p PID를 이용 process attach 후 dump memory 사용!
    - Windows : Micosoft OEM Support Tools userdump.exe
  - 문서 내용, ID/패스워드, 메신저 대화 내용 등 정보를 확인할 수 있음

```
[root@neoshine-Linux root]# dd if=/dev/mem of=Linux.dump
1048448+0개의 레코드를 입력하였습니다
1048448+0개의 레코드
```

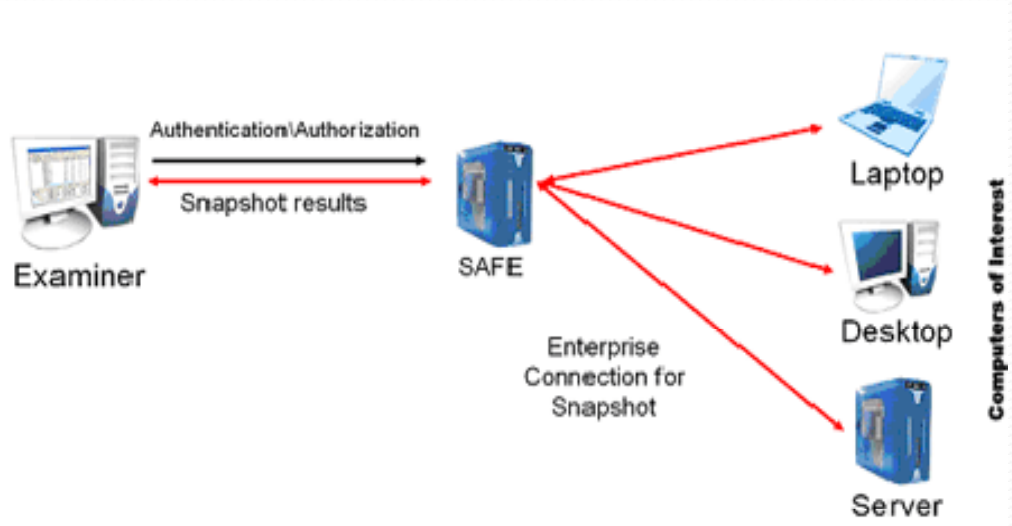
```
C:₩>userdump.exe 1716 Windows.dump
User Mode Process Dumper (Version 3.0)
Copyright (c) 1999 Microsoft Corp. All rights reserved.

Dumping process 1716 (iexplore.exe) to
C:₩Windows.dump...
The process was dumped successfully.
```

- 메모리 정보 수집 및 분석 기술
  - 메모리의 Data 영역뿐 아니라 Kernel 영역의 정보를 수집하는 기술
  - 추출된 Dump 데이터에서 원하는 정보를 검색 및 추출 하는 기술

Volatile Data Acquisition Tools

- Snap Shot
  - EnCase Enterprise 버전에 적용 : 대형 전산망에서 활용
  - 각 Agent를 업무용 PC에 설치하여 내부 직원 정보유출, 전산자원 남용 감시 및 증거 수집용으로도 사용



Evidence Searching

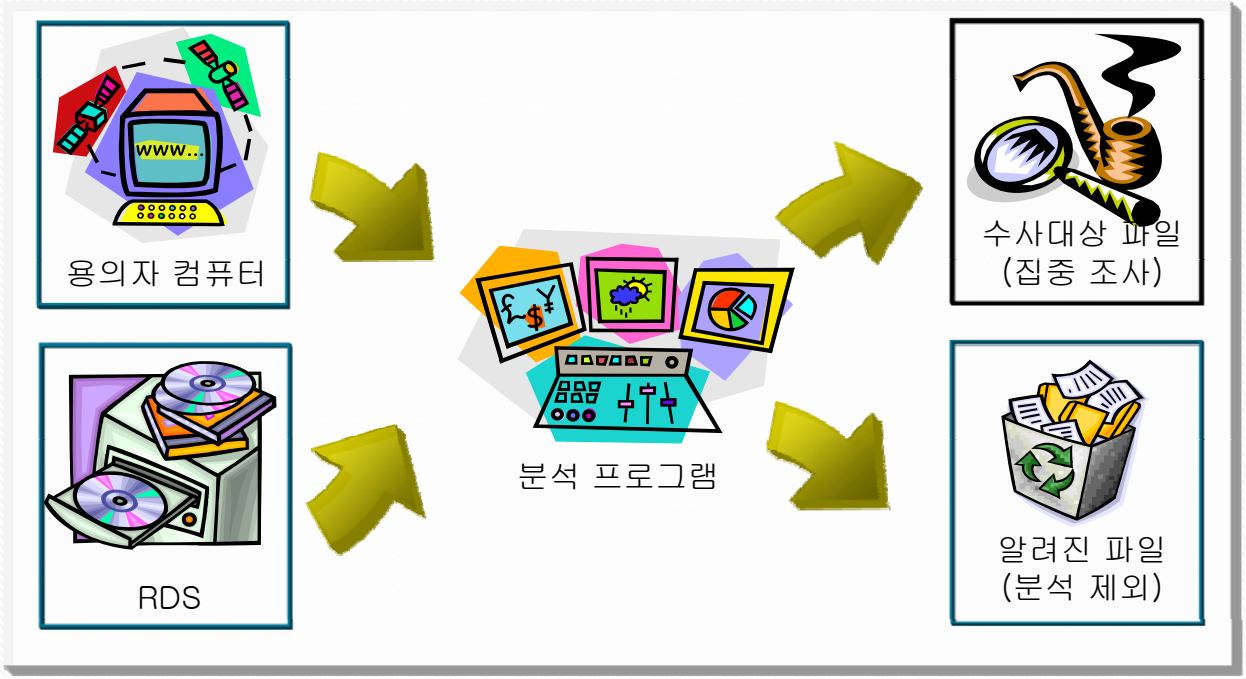
- Searching
  - 잘 알려진 파일은 검색 대상에서 제외하고 주목해서 검색할 대상을 선정하여 검색 범위를 축소하는 것이 중요함
    - "포렌식은 검색의 연속이다"

- National Software Reference Library (NSRL)
  - 美 NIST 산하 CFTT에서 제공하는 국가 표준 참조 데이터
  - NSRL의 목적
    - 범죄에 사용되는 컴퓨터 파일의 식별 자동화
    - 증거에 포함된 파일 조사를 효율적으로 지원
  - NSRL의 세부 내용
    - 다년간 각종 S/W 및 알려진 파일을 수집, 이에 대한 정보와 hash 값을 DB 목록화 (31,743,615 files, 10,533,722 Hash Values)
    - 전세계 7009개 S/W, 35개국 언어 OS의 참조 데이터 셋(RDS:Reference Data Set)

```
"SHA-1",                                  "MD5",                                    "CRC32",   "FileName",       "FileSize","ProductCode"
"00000F6ED90D946C057B55545597C31251DC24E4","F4129AC77F806601BDD44620C17675E7","38CC50B7","004i200r.gif"   ,  1551,228,     "WIN"
"00000FF9D0ED9A6B53BC6A9364C07074DE1565F3","A5D49D6DA9D78FD1E7C32D58BC7A46FB","2D729A1E","cmnres.pdb.dll",76800,2471,     "WIN"
"00000FF9D0ED9A6B53BC6A9364C07074DE1565F3","A5D49D6DA9D78FD1E7C32D58BC7A46FB","2D729A1E","cmnres.pdb.dll",76800,2704,     "WIN"
"00000FF9D0ED9A6B53BC6A9364C07074DE1565F3","A5D49D6DA9D78FD1E7C32D58BC7A46FB","2D729A1E","cmnres.pdb.dll",76800,2741,     "WIN"
"00000FF9D0ED9A6B53BC6A9364C07074DE1565F3","A5D49D6DA9D78FD1E7C32D58BC7A46FB","2D729A1E","cmnres.pdb.dll",76800,2797,     "WIN"
"00000FF9D0ED9A6B53BC6A9364C07074DE1565F3","A5D49D6DA9D78FD1E7C32D58BC7A46FB","2D729A1E","cmnres.pdb.dll",76800,2912,     "WIN"
```

Evidence Searching

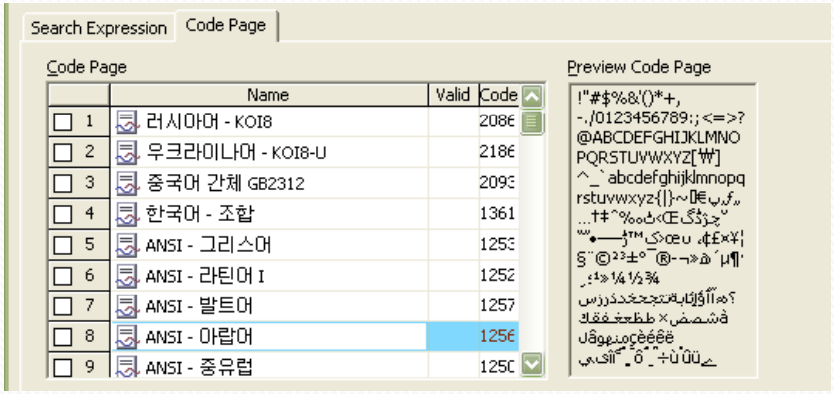
- 한국형 RDS 구축
  - NIST에서 제공하는 National Software Reference Library(NSRL)를 모범으로 한국형 RDS(Reference Data Set) 구축
    - 표준 해쉬셋 : 잘 알려진 응용 프로그램 및 OS 커널 관련 파일
    - 악성 해쉬셋 : 악성 프로그램, 음란 동영상 등 범죄 관련 파일



Evidence Analysis

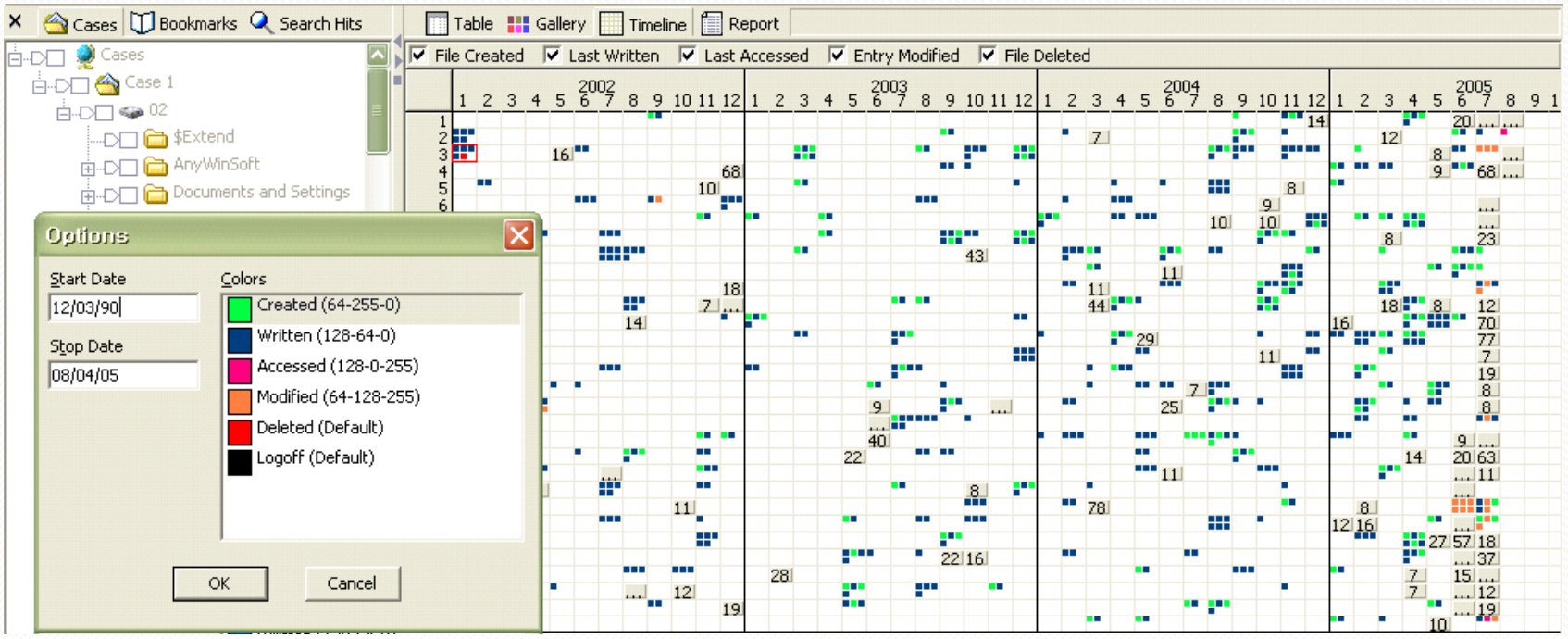
- 각종 파일 포맷 분석 DB 구축
  - Vendor 협력하에 각종 파일 포맷을 자동으로 인식하고 종류에 따라 미리보기, 정보추출, 파일 포맷 복구 등을 지원하는 기술을 개발
    - tip) 국정원 실기평가에서 이와 유사한 문제 출제됨

- 각종 Encoding 기법 분석
  - 각종 Encoding(Packing, Unicode, ASCII, Base 64 등)을 한꺼번에 효율적으로 검색하는 기술 필요
  - 국제화 되는 디지털 범죄에 대응하여 외국어를 자동으로 인식하고 검색을 지원할 수 있는 기술 필요



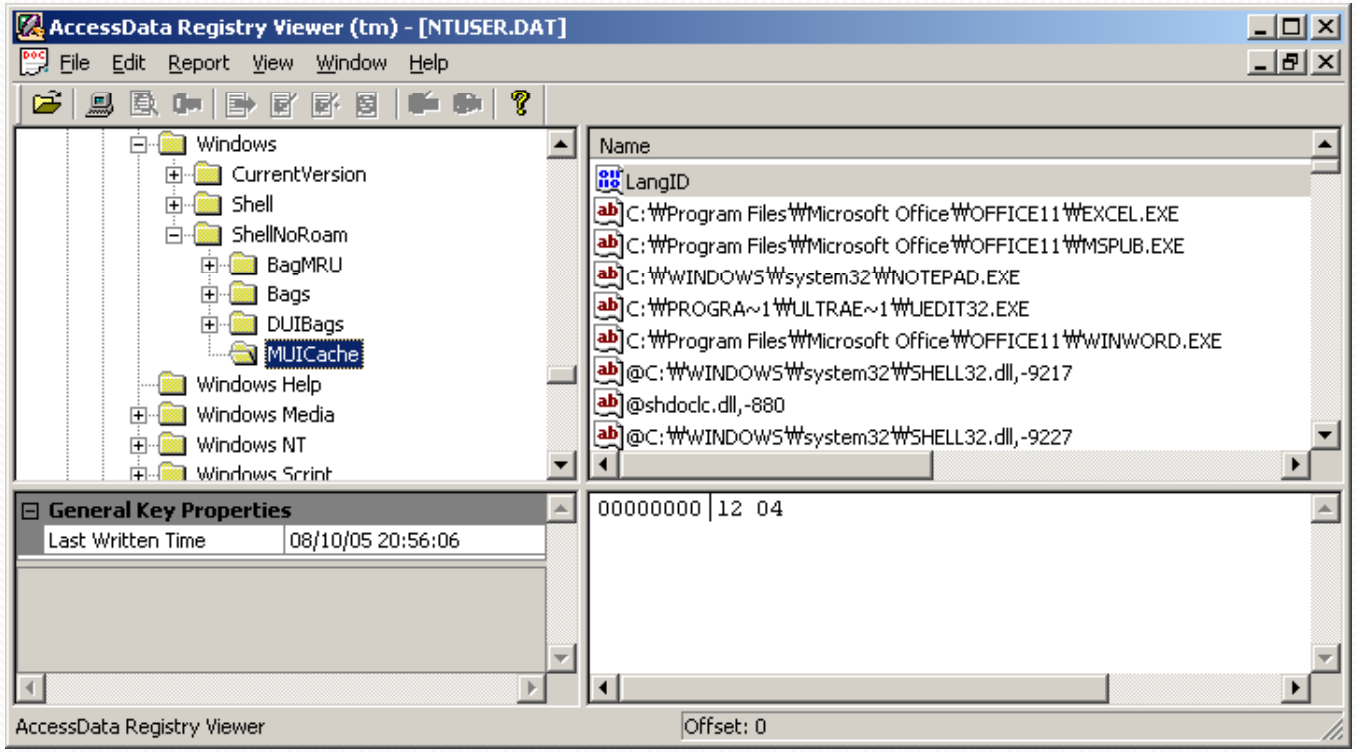
Evidence Analysis

- Timeline 분석
  - create, write, access, modified, deleted time을 GUI 형태로 표시
  - 이미지상의 대상 파일들의 사용 시간대를 한눈에 파악할 수 있는 장점
    - like, find –ctime, ls –aclt (on Linux, timestamp based)



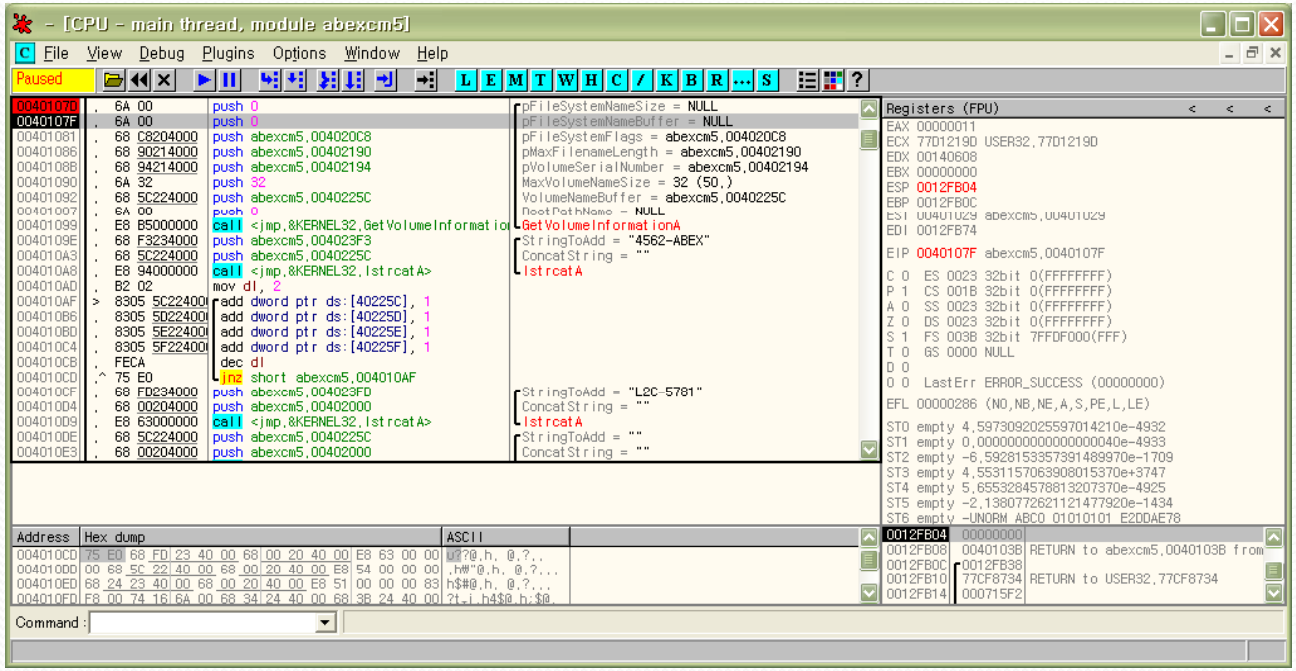
Evidence Analysis

- Registry 분석
  - Regedit는 운영 시스템에서의 정보만을 제공하므로 비가동중인 시스템 및 하드디스크의 레지스트리를 분석할 수 없음
  - Thus, Hive 파일 자체 포멧을 파악하여 포렌식 분석 기능을 제공하는 레지스트리 분석 도구가 필요함



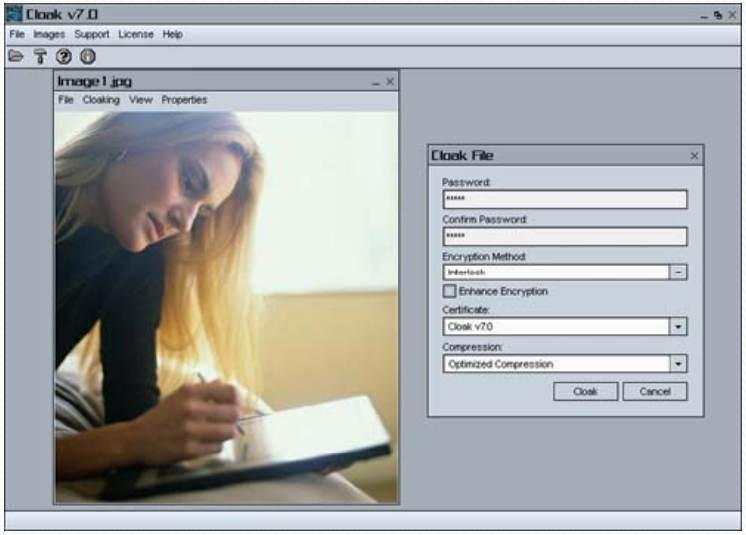
Evidence Analysis

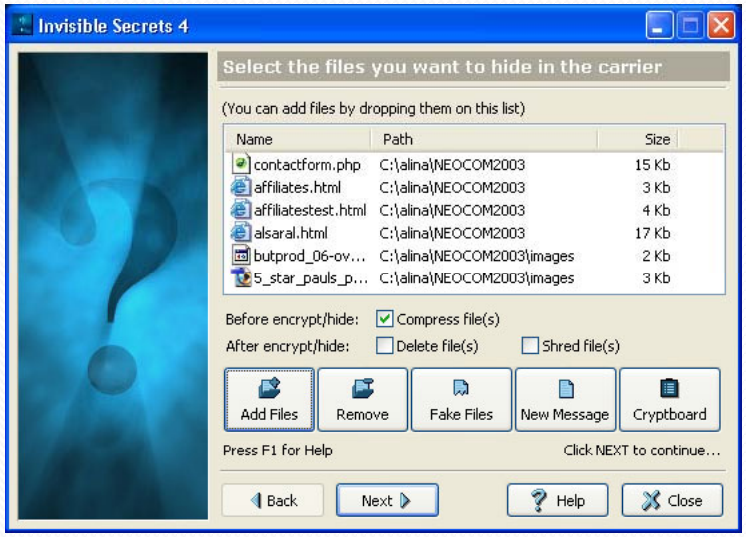
- Binary 분석
  - 설치된 S/W의 정보를 획득하고 실행파일을 분석하는 기술
  - 발견된 악성코드를 분석하여 범죄자에 대한 단서를 추출할 수 있어야 함
    - Unpacking(필요시 MUP), Debugger(ollygdb, IDA pro)
    - Assembly, Important APIs
      - tip) 금결원에서는 Binary 분석 시험에서 ocx, dll, exe등 6문제 출제



Evidence Analysis

- Hidden Data 분석
  - 데이터 은닉은 최신 기법이나 경향은 아니지만 안티 포렌식 기술로 사용됨
    - Cloak v7.0 : Steganography용 S/W
    - Invisible Secrets : 정상파일(JPEG, PNG, BMP, HTML, WAV)에 비밀 데이터를 암호화 하여 은닉 시켜주는 S/W





Evidence Analysis

- Network 분석
  - tcpdump, netstat, lsof -i…
- Rootkit 분석
  - chkrootkit…
    - tip) 국보연에서도 chkrootkit 반드시 수행함
- Memory 분석
  - /proc/kcore, /dev/mem, /proc/PID/mem
  - strings, grep, less등의 적절한 활용 필요
  - file and directory names
    - $ grep -e "\/proc\/" -e "\/bin\/" -e "\/bin\/.*?sh" kcore_strings
    - $ grep -e "ftp" -e "root" kcore_strings
    - $ grep -e "rm -" kcore_strings
    - $ grep -e ".tgz" kcore_strings
  - ip addresses and domain names
    - $ grep -e "[0-9]\+\.[0-9]\+\.[0-9]\+\.[0-9]\+" kcore_strings
    - $ grep -e "\.pl" kcore_strings

Anti–Forensics Methods

- Anti-Forensics Methods
  - Data Contraception
    - Prevent evidence data from existing somewhere that can be analyzed
      - E.g. Memory only malware, memory only exploitation
  - Data Hiding
    - Put the data on disk but put it somewhere the forensic analyst is unlikely to look
      - E.g. Defilers toolkit, runefs
  - Data Destruction
    - Destroy any evidence before someone gets a chance to find it
      - E.g. Disk wiping, wipe, srm, evidence eliminator, necrofile
  - Data Misdirection
    - Provide the forensic analyst false data that is indistinguishable from the real thing