# Trends in dForensics, Jan/2013

*proneer*

*proneer@gmail.com*

*http://forensic-proof.com*

*Security is a people problem…*

## Domestic Stuff (cont'd)

- **FORENSIC-PROOF**

1. 디지털포렌식 관련 종사자 인터뷰 (dForensic Practitioner Interview)
2. 디지털포렌식 관련 직업 (What jobs are available in the dForensics)
3. 디지털 포렌식 개요 (An Introduction to Digital Forensics) (slides)
4. 창과 방패, 안티포렌식과 안티안티포렌식 (Anti-Forensics vs. Anti-Anti Forensics)
5. 무작정 포맷하지 말자 (Don't blindly format your hard drive)
6. [인터뷰#1] 사이버테러대응센터 이병길 수사관
7. 덮어쓴 데이터 복구의 진실 (The Truth about Recovering Overwritten Data)

- **malwareL4B**
  - Java Applet JMX 0day Remote Code Execution 취약점(CVE-2013-0422) 분석보고서

## Domestic Stuff (cont'd)

- **Red Alert, NSHC**
  - 국내 인터넷 뱅킹 악성코드 분석 보고서

- **보안인닷컴**
  - e-매거진 19호

- **보안프로젝트**
  - 스택기반 오버플로우 (with KISEC)
  - 쉘코드로 점프하는 방법 (with KISEC)
  - 구조적 예외 핸들러 (with KISEC)
  - Metasploit Forensic

## Domestic Stuff

- **Kyaru's Blog**
  - 악성코드 분석에 도움이 될만한 사이트 정리
- **CIO Korea**
  - 기고 | 데이터 유출 사고 대응법
- **… …**

## Open Security Research (blog.opensecurityresearch.com)

- Windows DLL Injection Basics
- Getting Started With Lock Picking
- Deobfuscating Potentially Malicious URLs - Part 1
- Deobfuscating Potentially Malicious URLs - Part 1 Solution
- Attributing Potentially Malicious URLs - Part 2
- ~~Attributing Potentially Malicious URLs - Part 2 (Solution?)~~

## Journey Into Incident Response (journeyintoir.blogspot.kr/) (cont'd)

- **Re-Introducing $UsnJrnl (NTFS Change Journal)**
  - **저널 데이터**: %SystemDrive%₩$Extend₩$UsnJrnl:$J
  - **저널 데이터 관리 정보**: %SystemDrive%₩$Extend₩$UsnJrnl:$Max
  - 파일과 디렉터리의 변경 정보가 기록
  - $LogFile은 트랙잭션 단위의 변경 기록 관리, $UsnJrnl은 변경 내역만 기록
  - 안티포렌식 기법의 활용이 잦아지면서 $UsnJrnl과 $LogFile의 활용도가 높아짐

## Journey Into Incident Response (journeyintoir.blogspot.kr/) (cont'd)

- **Re-Introducing $UsnJrnl ➔ $UsnJrnl – Journal Entry**

| 위치(Offset) | 크기 (Byte) | 설명 |
|---|---|---|
| 0x00 | 4 | 저널 엔트리의 크기 |
| 0x04 | 2 | 상위 버전 |
| 0x06 | 2 | 하위 버전 |
| 0x08 | 8 | 파일 참조 주소 (File Reference Address) |
| 0x10 | 8 | 부모의 파일 참조 주소 |
| 0x18 | 8 | 저널 데이터($J)에서 해당 저널 엔트리의 위치(USN) |
| 0x20 | 8 | 타임 스탬프 |
| 0x28 | 4 | 사유(reason) 플래그 |
| 0x2B | 4 | 소스 정보 |
| 0x30 | 4 | 보안 ID(SID) |
| 0x34 | 4 | 파일 속성 |
| 0x38 | 2 | 파일 이름 크기 |
| 0x3A | 2 | 파일 이름 위치 |
| 0x3C | 가변 | 파일 이름 |
| 맨 뒤쪽 | 가변 | 8바이트 정렬을 위한 패딩 |

참고: 임베디드 개발자를 위한 파일시스템의 원리와 실습

## Journey Into Incident Response (journeyintoir.blogspot.kr/) (cont'd)

- **Re-Introducing $UsnJrnl ➔ $UsnJrnl – Journal Entry ➔ Reason Flags**

| 위치(Offset) | 설명 |
|---|---|
| 0x00000001 | 기본 $DATA 속성의 내용이 덮어써졌다. |
| 0x00000002 | 기본 $DATA 속성의 내용이 추가되었다. |
| 0x00000004 | 기본 $DATA 속성의 내용이 줄어들었다. |
| 0x00000010 | 이름이 있는 $DATA 속성의 내용이 덮어써졌다. |
| 0x00000020 | 이름이 있는 $DATA 속성의 내용이 추가되었다. |
| 0x00000040 | 이름이 있는 $DATA 속성의 내용이 줄어들었다. |
| 0x00000100 | 파일 또는 디렉터리가 생성되었다. |
| 0x00000200 | 파일 또는 디렉터리가 삭제되었다. |
| 0x00000400 | 파일의 확장 속성이 변경되었다. |
| 0x00000800 | 보안 설명자(Security Descriptor)가 변경되었다. |
| 0x00001000 | 이름이 변경되었다. 저널 엔트리가 이전 이름을 가지고 있다. |
| 0x00002000 | 이름이 변경되었다. 저널 엔트리가 새로운 이름을 가지고 있다. |
| 0x00004000 | 인덱스 상태가 변경되었다. |
| 0x00008000 | 파일 또는 디렉터리의 상태가 변경되었다. |
| 0x00010000 | 하드 링크가 생성되거나 삭제되었다. |
| 0x00020000 | 압축 상태가 변경되었다. |
| 0x00040000 | 암호화 상태가 변경되었다. |
| 0x00080000 | Object ID가 변경되었다. |
| 0x00100000 | Reparse Point 값이 변경되었다. |
| 0x00200000 | 이름있는 $DATA 속성이 생성, 삭제, 변경되었다. |
| 0x80000000 | 파일 또는 디렉터리가 닫혔다. |

## Journey Into Incident Response (journeyintoir.blogspot.kr/) (cont'd)

- **Re-Introducing $UsnJrnl ➔ Data Hiding in Obscure Location**
  - ZeroAccess 변종의 경우 휴지통 경로를 이용
  - IDS ZeroAccess 탐지: 2012-12-14 15:38 UTC
  - 해당 시스템의 $UsnJrnl:$J 파일 조사

| 1 | date | time | MFT entry | seq num | parent | filename | type change |
|---|---|---|---|---|---|---|---|
| 144105 | 12/14/2012 | 15:38:23.364 | 0x00000000a472 | 0x0007 | 0x000000000b17 | TMP000000082CD5F3CA1158680B | file_added; file_created |
| 144106 | 12/14/2012 | 15:38:24.425 | 0x00000000a472 | 0x0007 | 0x000000000b17 | TMP000000082CD5F3CA1158680B | file_added; file_created; file_deleted; file_closed |
| 144107 | 12/14/2012 | 15:38:24.440 | 0x00000000a472 | 0x0008 | 0x000000000165 | Detections.log | file_created |
| 144108 | 12/14/2012 | 15:38:24.440 | 0x00000000a472 | 0x0008 | 0x000000000165 | Detections.log | file_added; file_created |
| 144109 | 12/14/2012 | 15:38:26.250 | 0x00000000a238 | 0x0001 | 0x000000000b0d | Microsoft-Windows-Windows Defender%4Operational.evtx | data_overwritten |
| 144110 | 12/14/2012 | 15:38:30.259 | 0x00000000a477 | 0x0002 | 0x000000002a16 | $5da39e9580074308c6cfbcce61795d0d | file_created |
| 144111 | 12/14/2012 | 15:38:30.275 | 0x00000000a478 | 0x0002 | 0x00000000a477 | L | file_created |
| 144112 | 12/14/2012 | 15:38:30.275 | 0x00000000a478 | 0x0002 | 0x00000000a477 | L | file_created; file_closed |
| 144113 | 12/14/2012 | 15:38:30.275 | 0x00000000a479 | 0x0002 | 0x00000000a477 | U | file_created; attrib_changed |
| 144114 | 12/14/2012 | 15:38:30.275 | 0x00000000a479 | 0x0002 | 0x00000000a477 | U | file_created; attrib_changed; file_closed |
| 144115 | 12/14/2012 | 15:38:30.290 | 0x00000000a47a | 0x0002 | 0x00000000a477 | @ | file_created |
| 144116 | 12/14/2012 | 15:38:30.290 | 0x00000000a47a | 0x0002 | 0x00000000a477 | @ | file_added; file_created |
| 144117 | 12/14/2012 | 15:38:30.290 | 0x00000000a47a | 0x0002 | 0x00000000a477 | @ | file_added; file_created; file_closed |
| 144118 | 12/14/2012 | 15:38:30.290 | 0x00000000a47b | 0x0002 | 0x00000000a477 | n | file_created |
| 144119 | 12/14/2012 | 15:38:30.290 | 0x00000000a47b | 0x0002 | 0x00000000a477 | n | file_added; file_created |
| 144120 | 12/14/2012 | 15:38:30.290 | 0x00000000a47b | 0x0002 | 0x00000000a477 | n | file_added; file_created; file_closed |
| 144121 | 12/14/2012 | 15:38:30.290 | 0x00000000a477 | 0x0002 | 0x000000002a16 | $5da39e9580074308c6cfbcce61795d0d | file_created; file_closed |
| 144122 | 12/14/2012 | 15:38:32.599 | 0x00000000a47c | 0x0002 | 0x00000000c461 | C | file_created |
| 144123 | 12/14/2012 | 15:38:32.630 | 0x00000000a47c | 0x0002 | 0x00000000c461 | C | file_created; file_closed |

## Journey Into Incident Response (journeyintoir.blogspot.kr/) (cont'd)

- **Re-Introducing $UsnJrnl ➔ Data Hiding in Obscure Location**
  - $MFT로 전체 경로 획득
  - BlueAngel의 **NTFS Log Tracker** (http://code.google.com/p/ntfs-log-tracker/)

| 1 | Record Number | Record type | Filename #1 | Std Info Creation date |
|---|---|---|---|---|
| 42105 | 42103 | Folder | /$Recycle.Bin/S-1-5-21-2793522790-2301028668-542554750-1000/$5da39e9580074308c6cfbcce61795d0d | 12/14/12 15:38 |
| 42106 | 42104 | Folder | /$Recycle.Bin/S-1-5-21-2793522790-2301028668-542554750-1000/$5da39e9580074308c6cfbcce61795d0d/L | 12/14/12 15:38 |
| 42107 | 42105 | Folder | /$Recycle.Bin/S-1-5-21-2793522790-2301028668-542554750-1000/$5da39e9580074308c6cfbcce61795d0d/U | 12/14/12 15:38 |
| 42108 | 42106 | File | /$Recycle.Bin/S-1-5-21-2793522790-2301028668-542554750-1000/$5da39e9580074308c6cfbcce61795d0d/@ | 12/14/12 15:38 |
| 42109 | 42107 | File | /$Recycle.Bin/S-1-5-21-2793522790-2301028668-542554750-1000/$5da39e9580074308c6cfbcce61795d0d/n | 12/14/12 15:38 |

## Journey Into Incident Response (journeyintoir.blogspot.kr/) (cont'd)

- **Re-Introducing $UsnJrnl ➔ Data Destruction**
  - **Self Deleting Droppers/Downloaders**

| 1 | date | time | MFT entry | filename | type change |
|---|---|---|---|---|---|
| 144182 | 12/14/2012 | 15:38:36.905 | 0x00000000a48d | 9862.exe | file_created |
| 144183 | 12/14/2012 | 15:38:36.905 | 0x00000000a48d | 9862.exe | file_added; file_created |
| 144184 | 12/14/2012 | 15:38:36.905 | 0x00000000a48d | 9862.exe | file_added; file_created; file_closed |
| 144185 | 12/14/2012 | 15:38:36.905 | 0x00000000a470 | 9862.exe | file_deleted; file_closed |
| 144186 | 12/14/2012 | 15:38:36.920 | 0x000000002977 | CMD.EXE-89305D47.pf | file_truncated |
| 144187 | 12/14/2012 | 15:38:36.920 | 0x000000002977 | CMD.EXE-89305D47.pf | file_added; file_truncated |
| 144188 | 12/14/2012 | 15:38:36.920 | 0x000000002977 | CMD.EXE-89305D47.pf | file_added; file_truncated; file_closed |

## Journey Into Incident Response (journeyintoir.blogspot.kr/) (cont'd)

- **Re-Introducing $UsnJrnl ➔ Data Destruction**
  - **Overwriting File System Metadata**
  - **/Users/lab/AppData/Local/{5da39e95-8007-4308-c6cf-bcce61795d0d}/n**
    - ✓ Standard Information Attribute
      Creation: 7/13/2009 23:11:59 UTC
      Access: 7/13/2009 23:11:59 UTC
      Modification: 7/14/2009 1:17:52 UTC
    - ✓ Filename Attribute
      Creation: 12/6/2012 22:18:00 UTC
      Access: 12/6/2012 22:18:00 UTC
      Modification: 12/6/2012 22:18:00 UTC

| | A | B | C | F | G |
|---|---|---|---|---|---|
| 1 | date | time | MFT entry | filename | type change |
| 44312 | 12/6/2012 | 22:17:59.950 | 0x00000000a6f9 | {5da39e95-8007-4308-c6cf-bcce61795d0d} | file_created |
| 44313 | 12/6/2012 | 22:17:59.950 | 0x00000000a6fa | U | file_created; attrib_changed |
| 44314 | 12/6/2012 | 22:17:59.950 | 0x00000000a6fa | U | file_created; attrib_changed; attrib_context_indexed_changed; attrib_changed |
| 44315 | 12/6/2012 | 22:17:59.950 | 0x00000000a6fa | U | file_created; attrib_changed; attrib_context_indexed_changed; attrib_changed; file_closed |
| 44316 | 12/6/2012 | 22:17:59.950 | 0x00000000a6fb | @ | file_created |
| 44317 | 12/6/2012 | 22:17:59.966 | 0x00000000a6fb | @ | file_added; file_created |
| 44318 | 12/6/2012 | 22:17:59.966 | 0x00000000a6fb | @ | file_added; file_created; attrib_context_indexed_changed; attrib_changed |
| 44319 | 12/6/2012 | 22:18:00.075 | 0x00000000a6fb | @ | file_added; file_created; attrib_context_indexed_changed; attrib_changed; file_closed |
| 44320 | 12/6/2012 | 22:18:00.107 | 0x00000000a6fc | L | file_created |
| 44321 | 12/6/2012 | 22:18:00.107 | 0x00000000a6fc | L | file_created; attrib_context_indexed_changed; attrib_changed |
| 44322 | 12/6/2012 | 22:18:00.107 | 0x00000000a6fc | L | file_created; attrib_context_indexed_changed; attrib_changed; file_closed |
| 44323 | 12/6/2012 | 22:18:00.138 | 0x00000000a6fd | n | file_created |
| 44324 | 12/6/2012 | 22:18:00.138 | 0x00000000a6fd | n | file_added; file_created |
| 44325 | 12/6/2012 | 22:18:00.153 | 0x00000000a6fd | n | file_added; file_created; attrib_context_indexed_changed; attrib_changed |
| 44326 | 12/6/2012 | 22:18:00.169 | 0x00000000a6fd | n | file_added; file_created; attrib_context_indexed_changed; attrib_changed; file_closed |

## Journey Into Incident Response (journeyintoir.blogspot.kr/) (cont'd)

- **Re-Introducing $UsnJrnl ➔ Data Destruction**
  - **File System Tunneling**

| date | time | MFT entry | filename | type change |
|---|---|---|---|---|
| 12/6/2012 | 22:18:05.138 | 0x000000004b0b | services.exe | access_changed |
| 12/6/2012 | 22:18:05.138 | 0x000000004b0b | services.exe | access_changed; file_closed |
| 12/6/2012 | 22:18:05.138 | 0x000000004b0b | services.exe | access_changed |
| 12/6/2012 | 22:18:05.138 | 0x000000004b0b | services.exe | access_changed; file_closed |
| 12/6/2012 | 22:18:05.857 | 0x000000004b0b | services.exe | file_renamed |
| 12/6/2012 | 22:18:05.857 | 0x000000004b0b | | file_renamed |
| 12/6/2012 | 22:18:05.872 | 0x00000000a704 | services.exe | file_created; attrib_changed |
| 12/6/2012 | 22:18:05.872 | 0x00000000a704 | services.exe | file_added; file_created; attrib_changed |
| 12/6/2012 | 22:18:05.872 | 0x00000000a704 | services.exe | file_added; file_created; attrib_changed; attrib_changed |
| 12/6/2012 | 22:18:05.872 | 0x00000000a704 | services.exe | file_added; file_created; attrib_changed; attrib_changed; file_closed |
| 12/6/2012 | 22:18:05.872 | 0x000000004b0b | | file_renamed; file_closed |

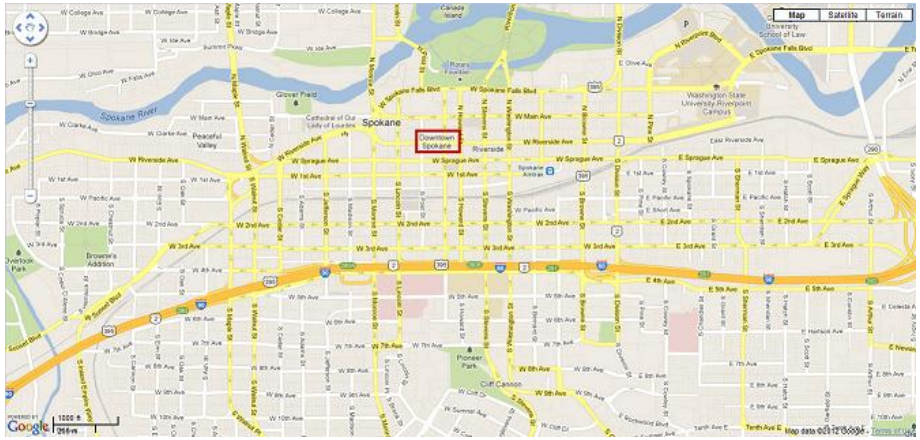
  - **%SystemDrive%₩Windows₩System32₩services.exe**
    - ✓ Standard Information Attribute
      Creation: 7/13/2009 23:11:26 UTC
      Access: 7/13/2009 23:11:26 UTC
      Modification: 7/14/2009 1:14:36 UTC
    - ✓ Filename Attribute
      Creation: 7/13/2009 23:11:26 UTC
      Access: 12/6/2012 22:18:06 UTC
      Modification: 12/6/2012 22:18:06 UTC

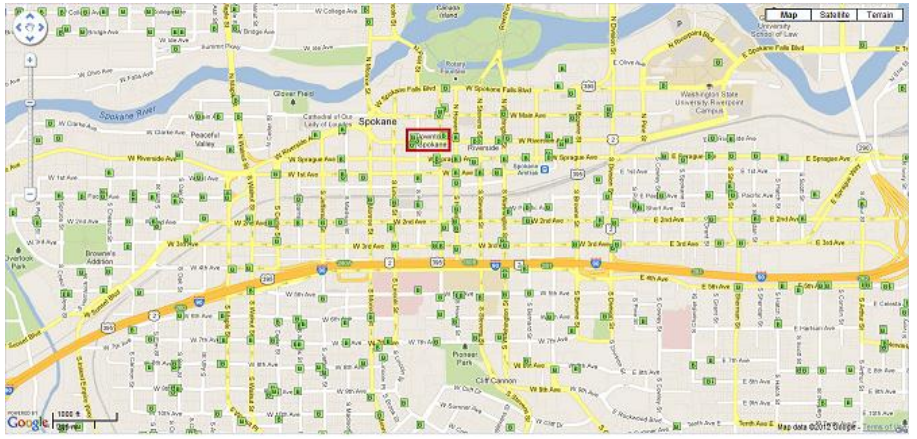
## Journey Into Incident Response (journeyintoir.blogspot.kr/) (cont'd)

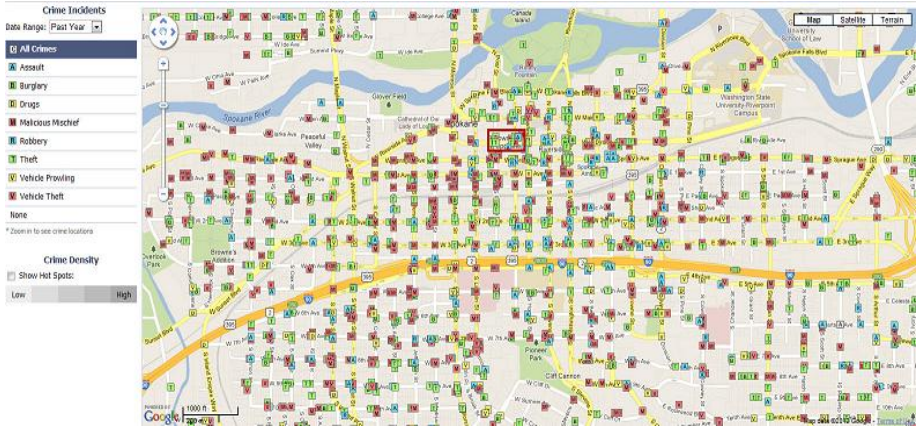
- **Layering Data**
  - 서로 다른 정보를 보여주는 레이어를 결합하면 좀 더 큰 그림을 볼 수 있음
  - DFIR에서 레이어의 결합은 더욱 중요
    - ✓ 시스템 사용 패턴 분석
    - ✓ 침해사고 분석

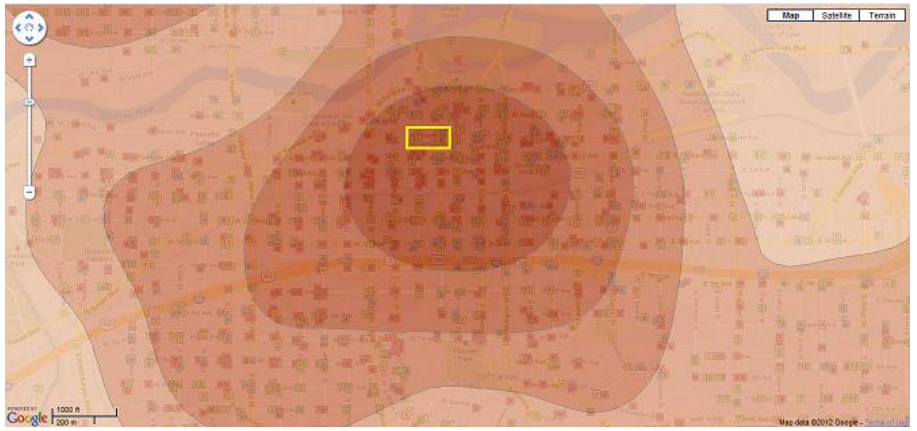
## Journey Into Incident Response (journeyintoir.blogspot.kr/) (cont'd)

- **Layering Data ➔ Layering Data in Action**
  - Crime Map, City of Spokane, Washington (http://www.spokanegis.org/crimemap2/)



## Journey Into Incident Response (journeyintoir.blogspot.kr/) (cont'd)

- **Layering Data ➔ Layering Data in Timelines**

1. Examine the programs ran on the system
2. Examine the auto-start locations
3. Examine the host-based logs
4. Examine file system artifacts

| | A | B | D | F | G | J | K |
|---|---|---|---|---|---|---|---|
| 1 | date | time | MACB | sourcetype | type | short | desc |
| 219414 | 12/6/2012 | 22:18:05 | ...B | NTFS $MFT | $SI [...B] time | /Windows/Installer/{5da39e95-8007-4308-c6cf-bcce61795d0d}/n | desc |
| 219420 | 12/6/2012 | 22:18:06 | .A.. | NTFS $MFT | $SI [.A..] time | /Windows/System32/services.exe | desc |
| 219421 | 12/6/2012 | 22:18:06 | M... | NTFS $MFT | $SI [M...] time | /Windows/System32/services.exe | desc |
| 219422 | 12/6/2012 | 22:18:06 | ..C. | NTFS $MFT | $SI [..C.] time | /Windows/System32/services.exe | desc |

| 1 | date | time | MACB | sourcetype | type | short | desc |
|---|---|---|---|---|---|---|---|
| 219398 | 12/6/2012 | 22:18:05 | ...B | NTFS $MFT | $SI [...B] time | /Windows/Installer/{5da39e95-8007-4308-c6cf-bcce61795d0d}/L | desc |
| 219399 | 12/6/2012 | 22:18:05 | | NTFS $LOGFILE | File Rename Event | File Renamed | Renamed: servic -> - Parent: 1802 |
| 219400 | 12/6/2012 | 22:18:05 | | NTFS $LOGFILE | File Creation Event | FILE Created | Created FILE: services.exe - Parent: 1802 |
| 219411 | 12/6/2012 | 22:18:05 | .A.. | NTFS $MFT | $SI [.A..] time | /Windows/Installer/{5da39e95-8007-4308-c6cf-bcce61795d0d}/n | desc |
| 219412 | 12/6/2012 | 22:18:05 | M... | NTFS $MFT | $SI [M...] time | /Windows/Installer/{5da39e95-8007-4308-c6cf-bcce61795d0d}/n | desc |
| 219413 | 12/6/2012 | 22:18:05 | ..C. | NTFS $MFT | $SI [..C.] time | /Windows/Installer/{5da39e95-8007-4308-c6cf-bcce61795d0d}/n | desc |
| 219414 | 12/6/2012 | 22:18:05 | ...B | NTFS $MFT | $SI [...B] time | /Windows/Installer/{5da39e95-8007-4308-c6cf-bcce61795d0d}/n | desc |
| 219420 | 12/6/2012 | 22:18:06 | .A.. | NTFS $MFT | $SI [.A..] time | /Windows/System32/services.exe | desc |
| 219421 | 12/6/2012 | 22:18:06 | M... | NTFS $MFT | $SI [M...] time | /Windows/System32/services.exe | desc |
| 219422 | 12/6/2012 | 22:18:06 | ..C. | NTFS $MFT | $SI [..C.] time | /Windows/System32/services.exe | desc |

## Journey Into Incident Response (journeyintoir.blogspot.kr/)

- Layering Data ➔ Layering Data in Timelines

| 1 | date | time | MACB | sourcetype | type | short | desc |
|---|---|---|---|---|---|---|---|
| 219398 | 12/6/2012 | 22:18:05 | ...B | NTFS $MFT | $SI [...B] time | /Windows/Installer/{5da39e95-8007-4308-c6cf-bcce61795d0d}/L | desc |
| 219399 | 12/6/2012 | 22:18:05 | | NTFS $LOGFILE | File Rename Event | File Renamed | Renamed: servic -> - Parent: 1802 |
| 219400 | 12/6/2012 | 22:18:05 | | NTFS $LOGFILE | File Creation Event | FILE Created | Created FILE: services.exe - Parent: 1802 |
| 219401 | 12/6/2012 | 22:18:05 | ...B | NTFS:$UsnJrnl:J$ | file_created | n | |
| 219402 | 12/6/2012 | 22:18:05 | ...B | NTFS:$UsnJrnl:J$ | file_added | n | |
| 219403 | 12/6/2012 | 22:18:05 | ..C. | NTFS:$UsnJrnl:J$ | attrib_changed | n | |
| 219404 | 12/6/2012 | 22:18:05 | ...B | NTFS:$UsnJrnl:J$ | file_added | n | |
| 219405 | 12/6/2012 | 22:18:05 | ..C. | NTFS:$UsnJrnl:J$ | attrib_changed | n | |
| 219406 | 12/6/2012 | 22:18:05 | ...B | NTFS:$UsnJrnl:J$ | file_added | n | |
| 219407 | 12/6/2012 | 22:18:05 | ..C. | NTFS:$UsnJrnl:J$ | attrib_changed | {5da39e95-8007-4308-c6cf-bcce61795d0d} | |
| 219408 | 12/6/2012 | 22:18:05 | ...B | NTFS:$UsnJrnl:J$ | file_created | {5da39e95-8007-4308-c6cf-bcce61795d0d} | |
| 219409 | 12/6/2012 | 22:18:05 | ..C. | NTFS:$UsnJrnl:J$ | attrib_changed | {5da39e95-8007-4308-c6cf-bcce61795d0d} | |
| 219410 | 12/6/2012 | 22:18:05 | ...B | NTFS:$UsnJrnl:J$ | file_created | {5da39e95-8007-4308-c6cf-bcce61795d0d} | |
| 219411 | 12/6/2012 | 22:18:05 | .A.. | NTFS $MFT | $SI [.A..] time | /Windows/Installer/{5da39e95-8007-4308-c6cf-bcce61795d0d}/n | desc |
| 219412 | 12/6/2012 | 22:18:05 | M... | NTFS $MFT | $SI [M...] time | /Windows/Installer/{5da39e95-8007-4308-c6cf-bcce61795d0d}/n | desc |
| 219413 | 12/6/2012 | 22:18:05 | ..C. | NTFS $MFT | $SI [..C.] time | /Windows/Installer/{5da39e95-8007-4308-c6cf-bcce61795d0d}/n | desc |
| 219414 | 12/6/2012 | 22:18:05 | ...B | NTFS $MFT | $SI [...B] time | /Windows/Installer/{5da39e95-8007-4308-c6cf-bcce61795d0d}/n | desc |
| 219415 | 12/6/2012 | 22:18:05 | ..C. | NTFS:$UsnJrnl:J$ | access_changed | services.exe | |
| 219416 | 12/6/2012 | 22:18:05 | ..C. | NTFS:$UsnJrnl:J$ | access_changed | services.exe | |
| 219417 | 12/6/2012 | 22:18:05 | ..C. | NTFS:$UsnJrnl:J$ | access_changed | services.exe | |
| 219418 | 12/6/2012 | 22:18:05 | ..C. | NTFS:$UsnJrnl:J$ | access_changed | services.exe | |
| 219419 | 12/6/2012 | 22:18:06 | ..C. | NTFS:$UsnJrnl:J$ | file_renamed | services.exe | |
| 219420 | 12/6/2012 | 22:18:06 | .A.. | NTFS $MFT | $SI [.A..] time | /Windows/System32/services.exe | desc |
| 219421 | 12/6/2012 | 22:18:06 | M... | NTFS $MFT | $SI [M...] time | /Windows/System32/services.exe | desc |
| 219422 | 12/6/2012 | 22:18:06 | ..C. | NTFS $MFT | $SI [..C.] time | /Windows/System32/services.exe | desc |
| 219423 | 12/6/2012 | 22:18:06 | ..C. | NTFS:$UsnJrnl:J$ | attrib_changed | services.exe | |
| 219424 | 12/6/2012 | 22:18:06 | ...B | NTFS:$UsnJrnl:J$ | file_created | services.exe | |
| 219425 | 12/6/2012 | 22:18:06 | ..C. | NTFS:$UsnJrnl:J$ | attrib_changed | services.exe | |
| 219426 | 12/6/2012 | 22:18:06 | ...B | NTFS:$UsnJrnl:J$ | file_added | services.exe | |
| 219427 | 12/6/2012 | 22:18:06 | ..C. | NTFS:$UsnJrnl:J$ | attrib_changed | services.exe | |
| 219428 | 12/6/2012 | 22:18:06 | ...B | NTFS:$UsnJrnl:J$ | file_added | services.exe | |

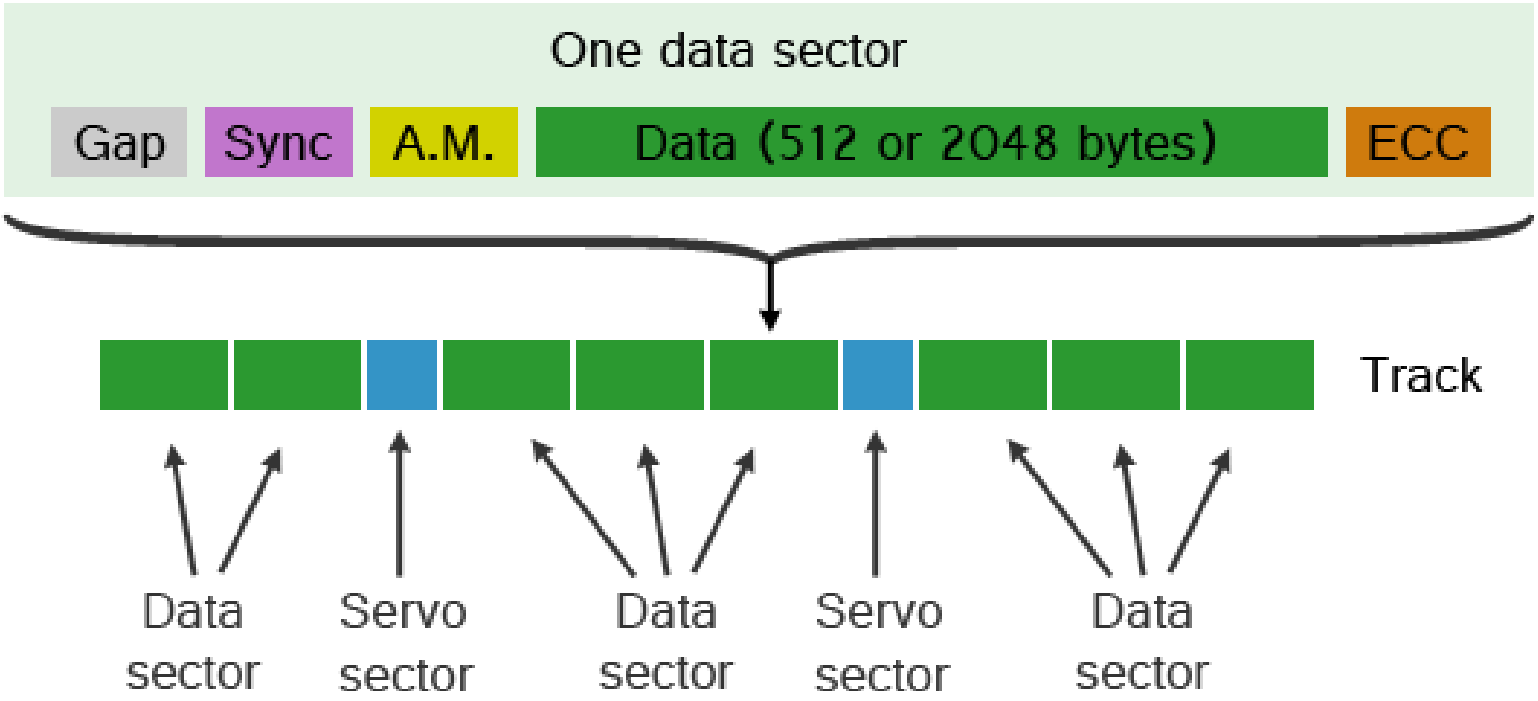
## FORENSIC FOCUS (forensicfocus.com) (cont'd)

- **Bad Sector Recovery**
  - HDD는 신뢰할 수 없는 데이터를 리턴하지 않음 ➔ 오류 매커니즘
  - 요청한 데이터가 100% 정확하지 않다면 오류를 발생시키거나 일부 데이터만 반환

- **General causes of bad sector formation**
  - **Physical Corruption**
    - ✓ 미디어 표면이 물리적인 충격으로 손상
  - **Magnetic Corruption**
    - ✓ 틀린 위치에 데이터를 잘못 기록
    - ✓ 물리적 손상만큼 위험
    - ✓ 인접한 섹터와 서보(servo) 섹터까지도 손상 위험

## FORENSIC FOCUS (forensicfocus.com) (cont'd)

- **Bad Sector Recovery ➔ Data/Servo Sectors**



## FORENSIC FOCUS (forensicfocus.com) (cont'd)

- **Bad Sector Recovery ➔ Possible outcomes**
  - 피해 원인과 관계없이 배드 섹터로 발생할 수 있는 결과
    - ✓ **Address Mark field corruption**
    - ✓ **Data corruption**
    - ✓ **ECC field corruption**
    - ✓ **Servo sector corruption**
    - ✓ **Or any combination of these**
  - 배드 섹터로 발생하는 오류는 운영체제나 일반적인 데이터 복구 도구에서 해결 불가능
  - 위 결과에서 도구로 섹터를 읽을 때

## FORENSIC FOCUS (forensicfocus.com) (cont'd)

- **Bad Sector Recovery ➔ Address Mark Corruption**
  - 디스크 주소 표시(Address Mark)가 손상되면 요청한 섹터를 찾을 수 없음
  - 데이터는 그대로 있을 수 있지만, 어디인지....?
  - 최근 일부 디스크는 섹터 ID나 주소 표시를 사용하지 않고, 정보를 서보 섹터에 인코딩

- **Bad Sector Recovery ➔ Data Corruption**
  - HDD는 항상 ECC 코드를 사용하여 오류 검사와 정정 알고리즘으로 무결성 유지
  - 데이터가 손상되면, ECC 알고리즘으로 복구 시도 ➔ 성공이면 데이터 반환
  - 실패하면, 일부 데이터가 정상이더라도 오류 반환

## FORENSIC FOCUS (forensicfocus.com) (cont'd)

- **Bad Sector Recovery ➔ ECC field corruption**
  - 매우 드문 경우지만,
  - 데이터는 정상이더라도 ECC가 맞지 않으면 오류 반환 ➔ 무결성을 검증할 방법 X

- **Bad Sector Recovery ➔ Servo sector corruption**
  - 한 트랙 당 수백 개의 서보 섹터가 기록
  - 트랙 상에 헤드 위치를 정확히 위치시킬 수 있는 위치 정보, 트랙 ID 포함
  - 서보 섹터는 위성의 GPS 수신기와 마찬가지로 헤드 위치 정보를 얻는 역할을 담당
  - 서보 섹터가 손상되면, 이어서 나오는 데이터 섹터를 찾을 수 없음 ➔ 읽기 작업 중단

## FORENSIC FOCUS (forensicfocus.com) (cont'd)

- **Bad Sector Recovery ➔ How Bad Sector Recovery Works**
  - **Read Long Command**
    - ✓ 데이터를 읽는 동안 오류 검사와 정정 알고리즘을 비활성화하는 명령
    - ✓ 데이터 + ECC 영역 반환
    - ✓ ATA-1(1994) ~ ATA-3(1997) ➔ HDD 제조사는 명령 계속 유지
  - **SMART Command Transport (SCT) ➔ Long Sector Access Command**
    - ✓ SMART(Self-Monitoring, Analysis and Reporting Technology)의 확장 프로토콜
    - ✓ 사라졌던 Read Long 명령의 기능이 부활
  - 배드 섹터 발생 시, 버퍼에 남는 일부 데이터를 이용한 복구 ➔ **테스트 결과 가능성이 낮음**

## FORENSIC FOCUS (forensicfocus.com) (cont'd)

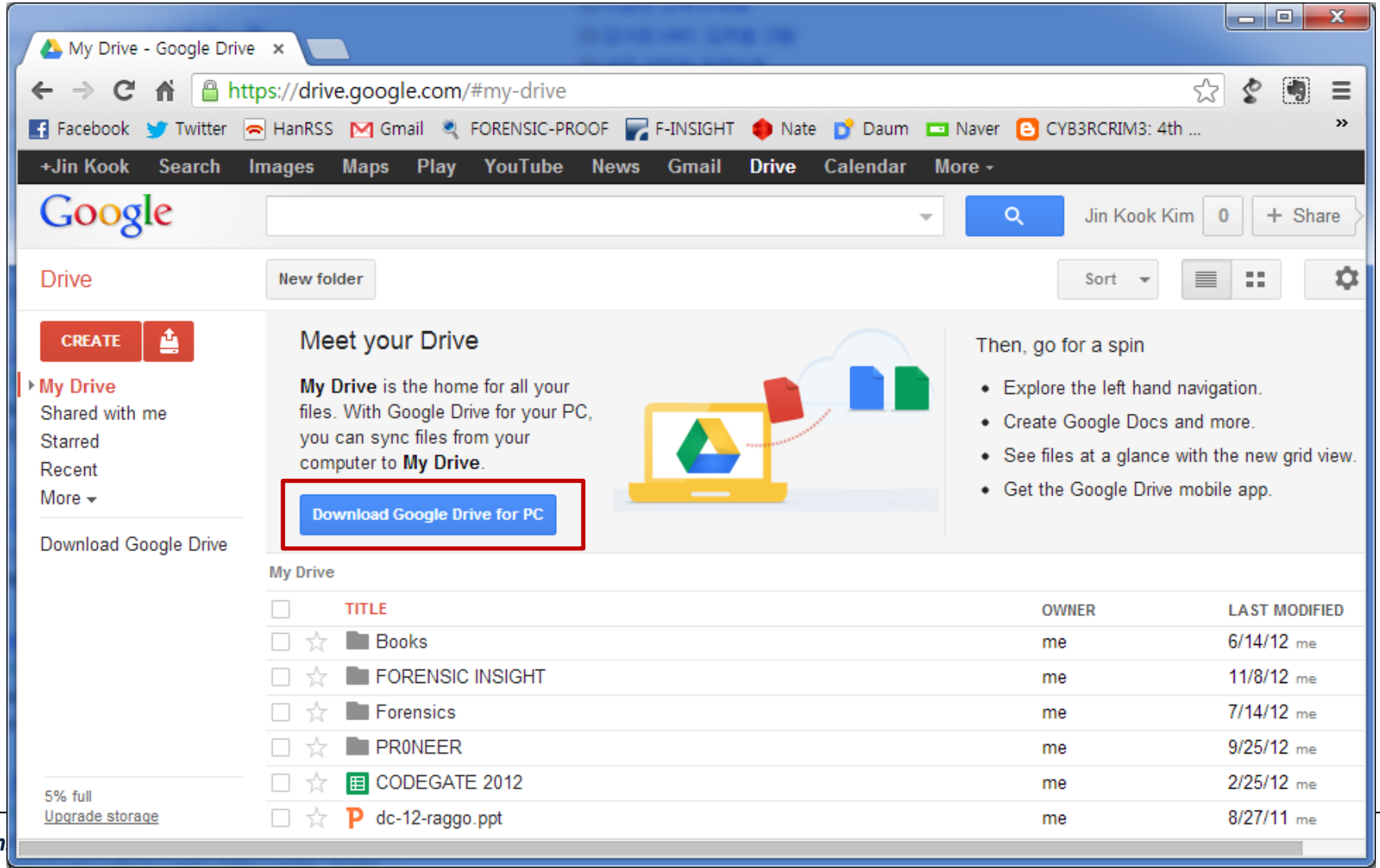
- **Bad Sector Recovery ➔ Debunking Bad Sector Recovery**
  - 최근 더 많은 복구 도구에서 배드 섹터 복구 기능을 지원
  - 오류 검사와 정정 알고리즘의 목적은 무결성
  - Read Long 명령을 통해 얻은 데이터의 무결성은 입증할 수 없음
  - 실제 데이터 복구에서 배드 섹터 복구는 매우 드문 경우
  - **배드 섹터의 원인은 다양**
    - ✓ 복구한 데이터가 실제 데이터의 일부분 vs 그냥 랜덤 데이터

## FORENSIC FOCUS (forensicfocus.com)

- **Bad Sector Recovery ➔ Dangers of Read Long approach**
  - 조사관이 배드 섹터 복구 기능으로 데이터를 복구
  - 복구한 데이터에서 유효한 데이터를 추출 ➔ 사회보장번호 발견 ➔ 조사에 활용
  - 번호를 보장할 수 있는가?
    - ✓ 777-677-766 vs. 776-676-677
  - 손상된 파일시스템을 복구 ➔ MFT 데이터가 조금이라도 변경된다면??
  - **도구:** 통계적인 방법과 반복적인 읽기 작업으로 원본 데이터를 최대한 복구한다고 주장
  - 타당성을 뒷받침할만한 증거가 부족, 배드 섹터의 반복적인 읽기로 추가적인 손상 우려
  - 배드 섹터 복구 기능을 사용할 경우, 한번 더 고려하자
  - 굳이 사용해야 한다면, 꼭 복구한 데이터를 구분시켜 두고 수동으로 무결성 검증을 수행

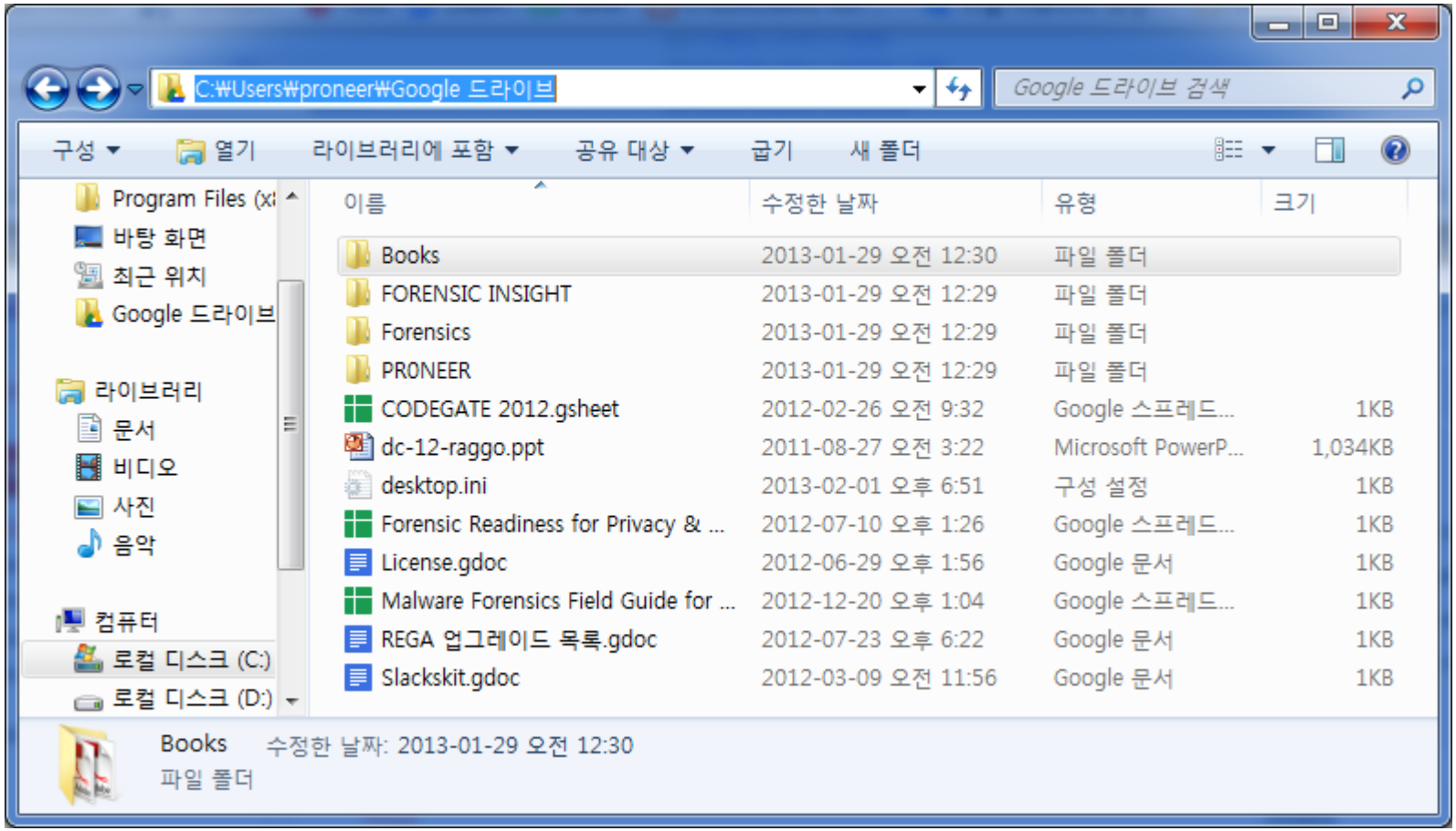
## FORENSIC FOCUS (forensicfocus.com) (cont'd)

- **What are 'gdocs'? Google Drive Data**



## FORENSIC FOCUS (forensicfocus.com) (cont'd)

- **What are 'gdocs'? Google Drive Data**
  - **%UserProfile%₩Google Drive ➔ gdoc, gsheet, gslides**



## FORENSIC FOCUS (forensicfocus.com)

- **What are 'gdocs'? Google Drive Data**

  - **License.gdoc**

{"url": "https://docs.google.com/document/d/1H58pLy5tzNbRmkMPjFQNgtGcrjHhCQVGLZPJMrh5ugE/edit", "resource_id": "document:1H58pLy5tzNbRmkMPjFQNgtGcrjHhCQVGLZPJMrh5ugE"}

  - **Forensic Tool.gsheet**

{"url": "https://docs.google.com/spreadsheet/ccc?key=0AvcjdMXf7DDHdEFRM2JMZjlGS3RoTE5GWkhXY0oxaVE", "resource_id": "spreadsheet:0AvcjdMXf7DDHdEFRM2JMZjlGS3RoTE5GWkhXY0oxaVE"}

  - **[INSIGHT] Next Plan.pptx.gslides**

{"url": "https://docs.google.com/presentation/d/1ArxV28ZER0CiFPEgCIs7D-XgJqJTA0TYbodGjrTYo0I/edit", "resource_id": "presentation:1ArxV28ZER0CiFPEgCIs7D-XgJqJTA0TYbodGjrTYo0I"}

## The Hacker Academy (thehackeracademy.com)

- **THA Deep Dive – Analyzing Malware in Memory**

Detailed information about Volatility covered the following areas:

Overview
Per-Process Analysis
API hooking
Misc. Process Data
GUI Subsystem
Registry in Memory
Callbacks
IRP Hooking
Devices
MBR & MFT

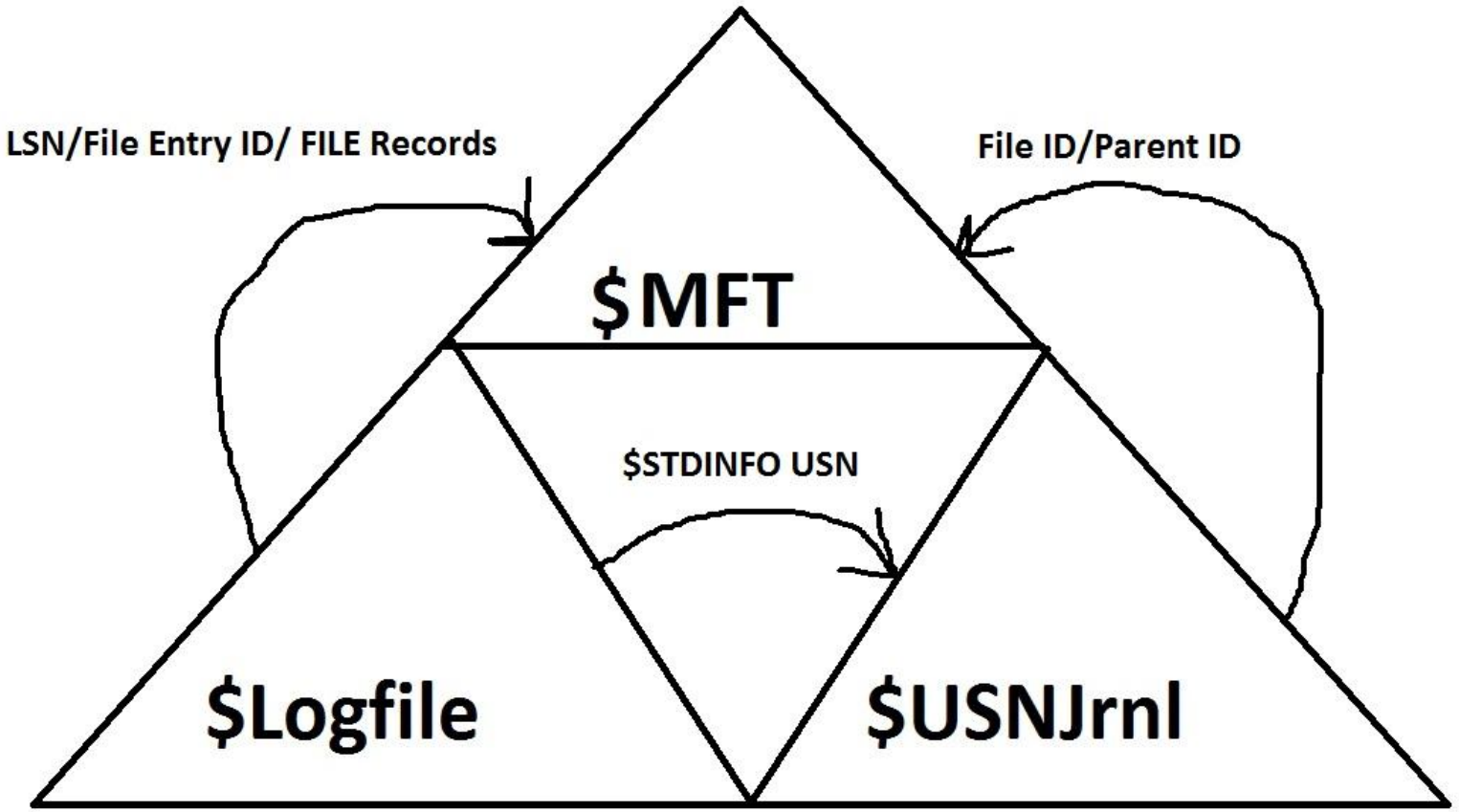
The session wrapped up with suggested resources for further reading, as well as reference links in the slides.

There were some audio issues during the presentation, so as you watch the video, know that it isn't your computer! The slides are available for download here.

Please feel free to contact us if you have any questions!

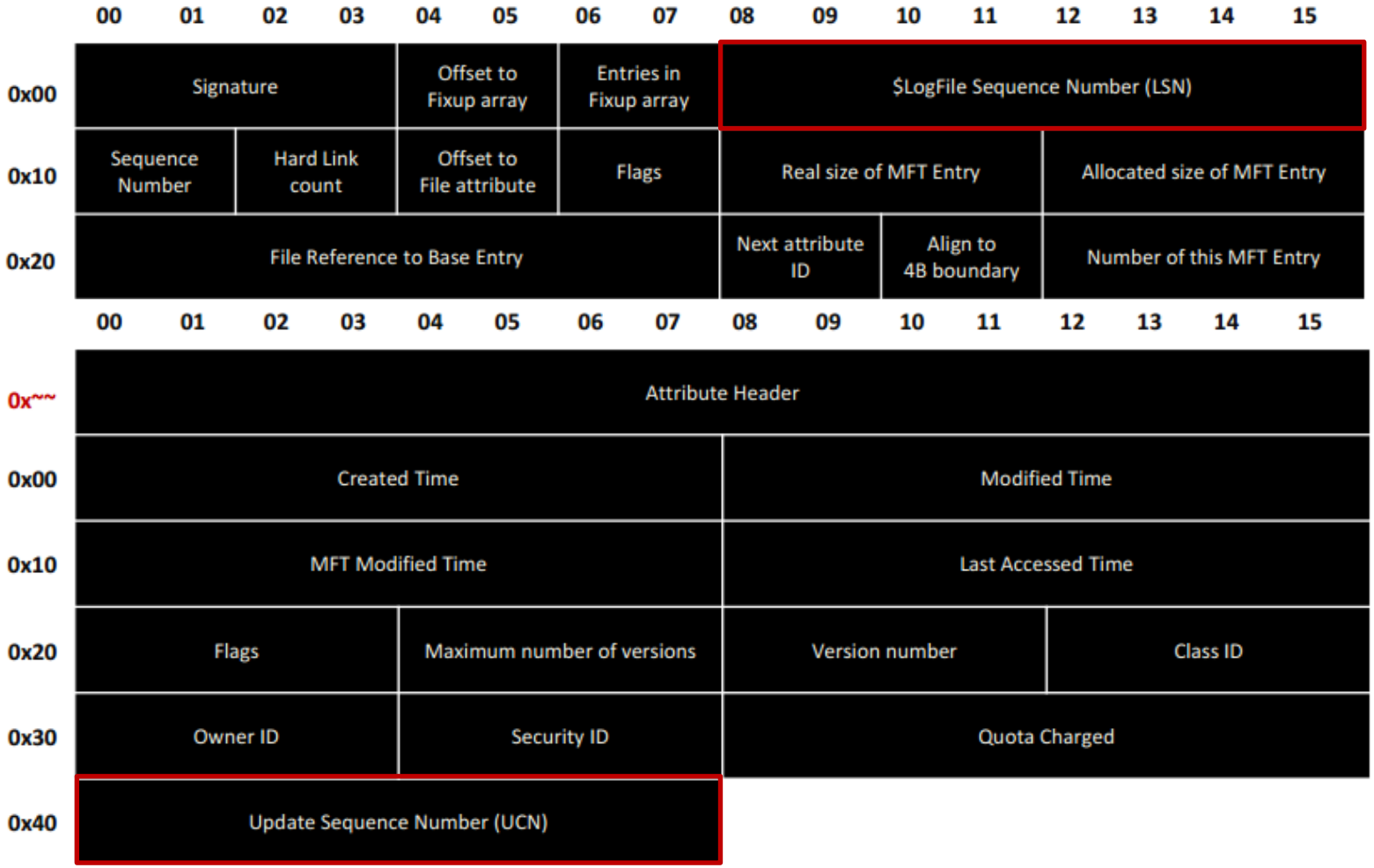
## Hacking Exposed (hackingexposedcomputerforensicsblog.blogspot.kr) (cont'd)

- NTFS Triforce



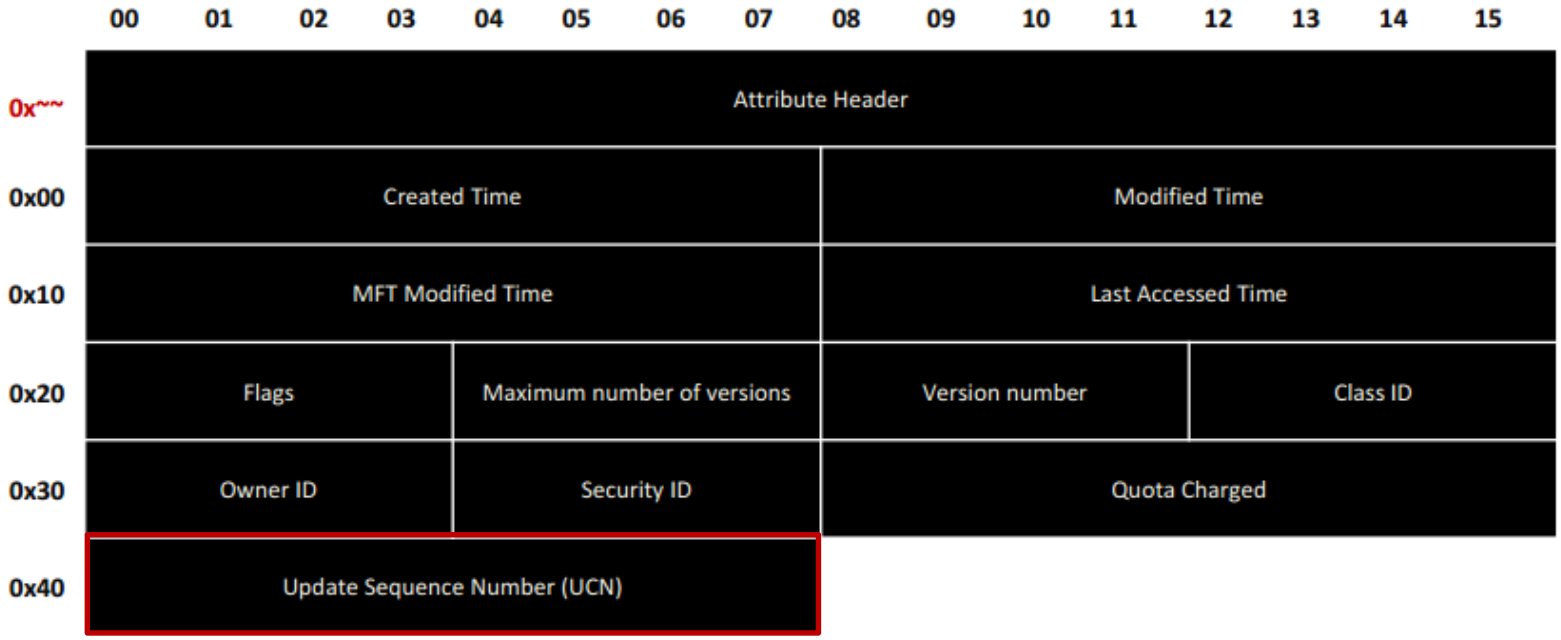
## Hacking Exposed (hackingexposedcomputerforensicsblog.blogspot.kr) (cont'd)

- NTFS Triforce – MFT Entry Header



## Hacking Exposed (hackingexposedcomputerforensicsblog.blogspot.kr) (cont'd)

- NTFS Triforce – $STANDARD_INFORMATION Attribute



## Hacking Exposed (hackingexposedcomputerforensicsblog.blogspot.kr) (cont'd)

- NTFS Triforce – $LogFile

| 0 | 1 | 2 | 3 | 4 | 5 | 6 | 7 | 8 | 9 | A | B | C | D | E | F |
|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|
| This LSN | | | | | | | | Previous LSN | | | | | | | |
| Client Undo LSN | | | | | | | | Client Data Length | | | | Client ID | | | |
| Record Type | | | | Transaction ID | | | | Flags | | Alignment or Reserved | | | | | |
| Redo OP | | Undo OP | | Redo Offset | | Redo Length | | Undo Offset | | Undo Length | | Target Attribute | | LCNs to follows | |
| Record Offset | | Attr Offset | | Alignment or Reserved | | | | Target VCN | | | | Alignment or Reserved | | | |
| Target LCN | | | | Alignment or Reserved | | | | | | | | | | | |

## Hacking Exposed (hackingexposedcomputerforensicsblog.blogspot.kr) (cont'd)

- **NTFS Triforce – $UsnJrnl**

```
typedef struct {
  DWORD          RecordLength;
  WORD           MajorVersion;
  WORD           MinorVersion;
  DWORDLONG      FileReferenceNumber;
  DWORDLONG      ParentFileReferenceNumber;
  USN            Usn;
  LARGE_INTEGER  TimeStamp;
  DWORD          Reason;
  DWORD          SourceInfo;
  DWORD          SecurityId;
  DWORD          FileAttributes;
  WORD           FileNameLength;
  WORD           FileNameOffset;
  WCHAR          FileName[1];
} USN_RECORD_V2, *PUSN_RECORD_V2, USN_RECORD, *PUSN_RECORD;
```

## Hacking Exposed (hackingexposedcomputerforensicsblog.blogspot.kr)

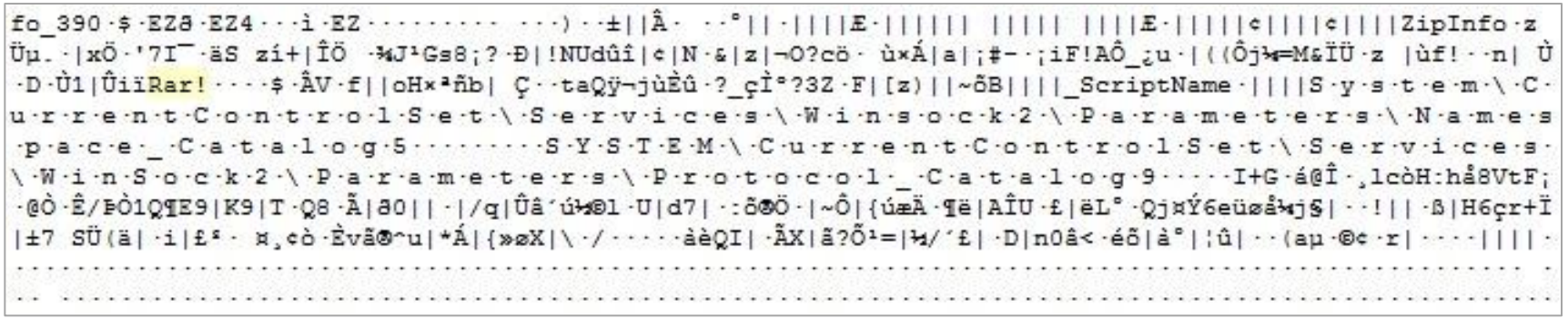
- **NTFS Triforce – Put it all together**
  - **The Power of the NTFS Triforce**
    1. 파일 소유권의 변경 ($LogFile)
    2. 파일 SID의 변경 ($LogFile)
    3. 타임스탬프의 변경 ($LogFile)
    4. 디렉터리 간의 파일 이동 ($LogFile & $UsnJrnl)
    5. 파일 이름 변경 ($LogFile & $UsnJrnl)
    6. 파일에 가한 행위 요약 ($UsnJrnl)
    7. 파일 속성 변경 ($LogFile)

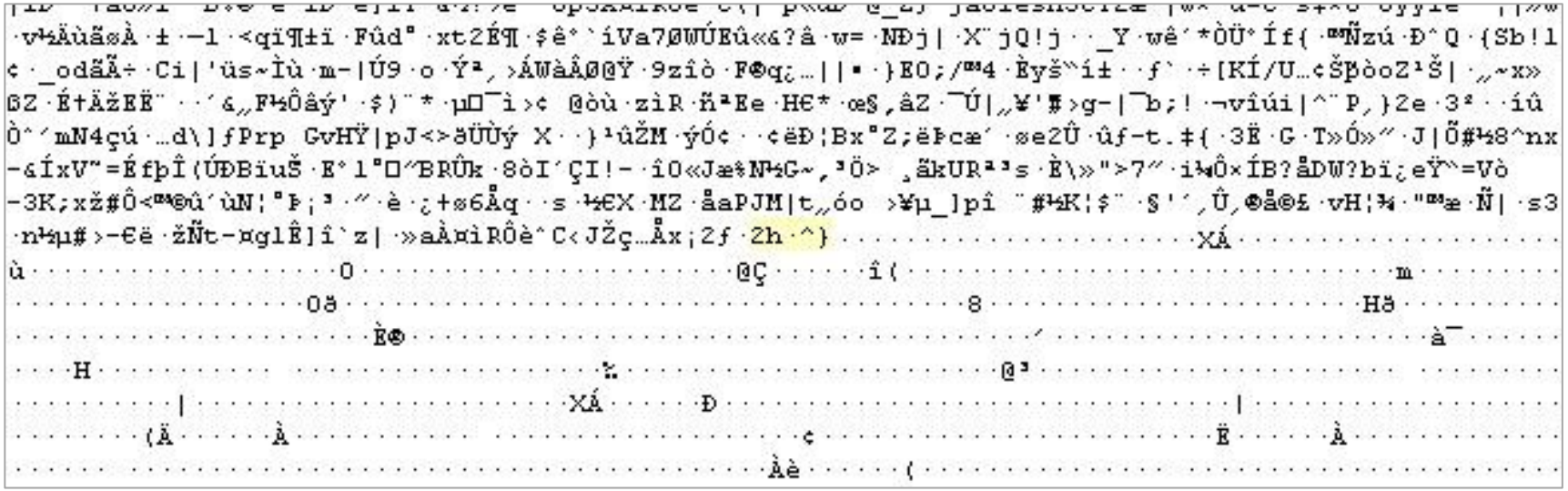
## MANDIANT Blog (mandiant.com/blog) (cont'd)

- **Carving Station – RAR Files**
  - **공격자가 "RAR.EXE"를 실행한 흔적 발견**
    - ✓ RAR.EXE-12F2DC4F.pf
  - **RAR 카빙**
    - ✓ **헤더**: "52 61 72 21", "52 45 7E 5E"
    - ✓ **푸터**: 없음(?)
  - 비할당 영역에서 카빙 수행

## MANDIANT Blog (mandiant.com/blog) (cont'd)

- **Carving Station – RAR Files**



## MANDIANT Blog (mandiant.com/blog) (cont'd)

- **Carving Station – RAR Files ➔ Password Prompt**


- **Mandiant Redline**

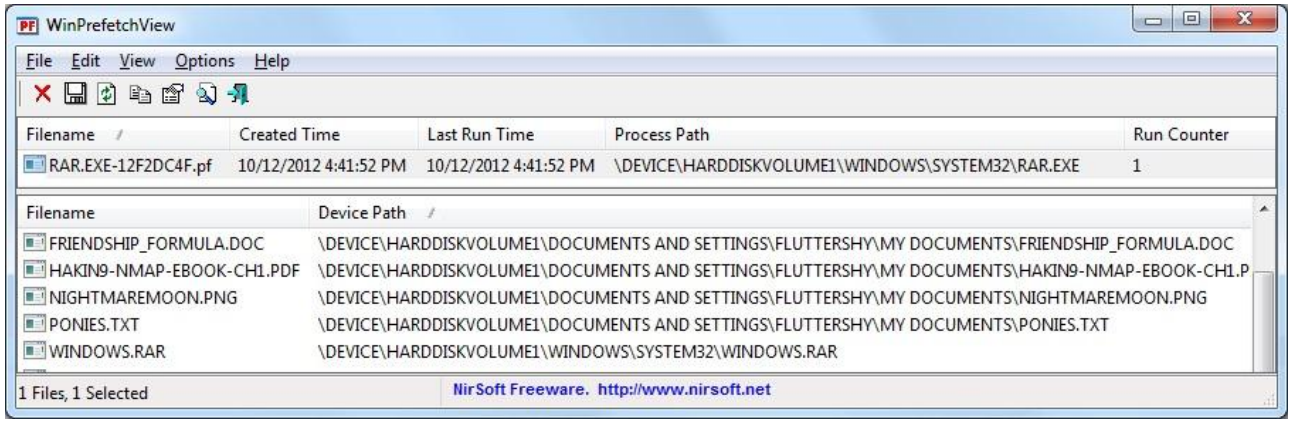
```
·D·AlEB|(F· øÿÿP|¦  øÿÿ0|Ã·|úÿÿ                                    11/0  9/2012  04:2
9 PM    <DIR>          ..                                    10/09/2012  11:29 AM
          18,944 friendship_formula.doc                  10/12/2012  12:43 PM
     411,169 hakin9-nmap-ebook-ch1.pdf                10/1  2/2012  05:04 PM
8,687,967 MLP-FIM                                  10/12/2012  12:40 PM          193
,637 nightmaremoon.png                          11/09/2012  04:29 PM         262,144
ntuser.dat                                  10/1  2/2012  03:15 PM              43 pon
ies.txt                                            6 File(s)      9,573,904 bytes
                                                 2 Dir(s)  23,556,866,048 bytes free

                          C:\Documents and Settings\fluttershy\My Documents>c:\Windows
\system32\rar a -hpevilpony c:\Windows\system32\windows *
                                                  È·····························D·R·CIcr·
Ý9þþ·····························································
```

## MANDIANT Blog (mandiant.com/blog)

- **Carving Station – RAR Files ➔ RAR file content indicators**

1. **Prefetch File**




2. **WinRAR Directory**
   - ✓ **Windows XP:** "%APPDATA%₩WinRAR"
   - ✓ **Windows 7:** "%APPDATA%₩Roaming₩WinRAR"
3. **Shellbags**
4. **Internet History**

## GOV Info Security (govinfosecurity.com)

- **5 Must-Have Skills for Fraud Examiners**

1. **Understand the Business**
   - ✓ IT의 비즈니스 측면에 대한 이해가 바탕이 되야 함
2. **Leverage Technology**
   - ✓ 도구의 자유로운 사용과 포렌식 분석을 통해 사건과 관련된 흔적을 빠르게 찾을 수 있어야 함
3. **Have a Versatile Work Experience**
   - ✓ 조사 경험 뿐만 아니라 사건에 대한 통찰력을 가질 수 있는 다양한 경험을 요구
4. **Understand Where the information Resides**
   - ✓ 신속하게 정보의 위치를 찾으려면 기업 환경, 회사와 조직의 내부 인프라에 대한 충분한 이해
5. **Possess International Capabilities**
   - ✓ 다른 나라의 프라이버시 법률, 보안 표준, 프레임워크를 이해할 수 있는 국제적 역량 필요

## Transparency Report

- **Google Transparency Report (http://www.google.com/transparencyreport/)**
  - 전 세계 Google 서비스의 실시간 및 이전 트래픽
  - 저작권 소유자 또는 정부로부터 받은 삭제 요청 건수
  - 정부 기관 및 법원으로부터 받은 사용자 데이터 요청 건수

- **Twitter's Transparency Report (https://transparency.twitter.com/overview)**
  - 분기별 정보 요청 건수 (국가별)
  - 분기별 삭제 요청 건수 (국가별)
  - 저작권 관련 신고 건수 (월별)

## Others

- **Forensic Artifact: Malware Analysis in Windows 8**
  - 윈도우 8 환경에서 악성코드 분석 시 고려해야 할 점을 살펴본다.
- **BinMode: Parsing Java *.idx files**
  - 자바 위협과 관련해 idx 파일의 활용 방안에 대해 소개한다.
- **Cracking Android Passwords: The Need for Speed (hashcat)**
  - Hashcat을 이용해 안드로이드 패스워드를 크래킹하는 내용을 다룬다.
- **Volume Shadow Copy to Logical Evidence File (LEF)**
  - 볼륨 섀도우 복사본을 LEF로 생성하는 법을 소개한다.
- **Red October – Indicators of compromise (IOC)**
  - 국가 주요 정보 수집용 악성코드인 붉은 10월의 IOC가 공개되었다.

## Others

- **2012 eDiscovery Year in Review: eDiscovery Case Law, Part 1, 2, 3, 4**
  - 2012 이디스커버리 관련 주요 사례를 리뷰한다.
- **Pulsing the HeartBeat APT**
  - 트렌드마이크로에서 발표한 국내를 목표로한  APT 공격에 대한 간단한 분석 내용이다.
- **FCC Smartphone Security Checker**
  - 간단히 안드로이드, 아이폰, 블랙베리, 위놉우 폰의 보안 설정을 점검할 수 있는 서비스이다.
- **Creative Option for Better Authentication of Mobile Phone Users**
  - 모바일 폰에서 사용할 수 있는 대안 인증 방안을 소개한다.
- **Exploiting printer via Jetdirect vunerabilities**
  - Jetdirect 취약점을 이용한 프린터 공격을 소개한다.

## Others

- **HowTo: Extract "Hidden" API-Hooking BHO DLLs**
  - 볼라틸리티를 이용해 API 후킹된 BHO DLL을 추출하는 법을 다룬다.
- **How to add GPS position to images (picasa)**
  - 이미지 파일에 GPS 데이터를 간단히 추가하는 법을 소개한다.
- **Android Messaging: Is Android Getting Religious?**
  - 안드로이드 데이터 복구와 관련하여 SQLite Vacuum에 대해 소개한다.
- **Internet Evidence Finder (IEF) Review**
  - 웹 브라우저 흔적 분석 도구인 IEF에 대한 리뷰이다.

## dForensics Tools

- **NTFS Log Tracker**
  - $LogFile, $UsnJrnl 파일을 분석해주는 도구
- **SyncTools for Sysinternals**
  - 시스인터널 도구의 최신 버전을 자동으로 갱신해주는 도구
- **AnalyzePE**
  - 파이썬 기반의 PE 파일 상세 분석 도구
- **ESEDatabaseView**
  - NirSoft에서 공개한 새로운 ESE DB 뷰어
- **NetAnalysis v1.56 / HstEx v3.10**
  - 웹 흔적 분석 도구인 NetAnalysis와 관련 아티팩트 복구 도구인 HstEx 업데이트

# Question and Answer