

Trends in dForensics, Apr/2013

JK Kim

forensic-proof.com

proneer@gmail.com

Security is a people problem...





FORENSIC-PROOF (forensic-proof.com/)

- IconCache를 최대한 활용하자
- [인터뷰#3] 한국인터넷진흥원-1 코드분석팀 김기종 선임
- [인터뷰#4] 한국인터넷진흥원-2 해킹대응팀 김정호 주임



FORENSIC FOCUS (forensicfocus.com/)

▪ Interpretation of NTFS Timestamps (cont'd)

- 타임스탬프는 분석가가 공통적으로 다루는 데이터 ➔ 타임스탬프 변환은 정확해야 함
- 타임스탬프 형식
 - ✓ DOS Date/Time (날짜: 2바이트, 시간: 2바이트)
 - 시작 시간 : 1980년 01월 01년 00:00:00 (00 : 21 : 00 : 00)
 - 종료 시간 : 2107년 12월 31일 23:59:58 (FF : 9F : BF : 7D)
 - ✓ Unix Data/Time (4바이트), 초 단위 카운트
 - 시작 시간 : 1970년 01월 01일 00:00:00 (UTC)
 - 종료 시간 : 2038년 01월 19일 03:14:07 (UTC)
 - ✓ Windows 64-Bit Time Stamp (8바이트), 100나노초 단위 카운트
 - 시작 시간 : 1601년 01월 01일 00:00:00.00000000 (00000000 : 00000000)
 - 종료 시간 : 30828년 09월 14일 02:48:05.4775807 (7FFFFFFF : FFFFFFFF)



FORENSIC FOCUS (forensicfocus.com/)

▪ Interpretation of NTFS Timestamps (cont'd)

- 윈도우 타임스탬프

- ✓ FILETIME 구조의 64비트 타임스탬프
- ✓ 1601년 1월 1일(UTC)을 기준으로 100 나노초마다 카운트
- ✓ 0x0000000000000000, 0xFFFFFFFFFFFFFFFF 값은 예약
- ✓ `FileTimeToSystemTime()` 함수로 시간 변환
 - **`FILETIME ≤ 0x7FFFFFFFFFFFFFFF`**
- ✓ 파일의 시간정보 얻어오기 (생성, 수정, 접근 시간)
 - `GetFileInformationByHandle`
- ✓ 파일의 시간정보 설정하기 (생성, 수정, 접근, 변경 시간)
 - `SetFileInformationByHandle`



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

▪ Interpretation of NTFS Timestamps

- 테스트 요구사항

1. 테스트는 사람이 수행해야 하며 테스트 포인트는 최대 100개 정도가 적당
2. 알려진 시간 범위(0x0 ~ 0x7FFFFFFFFFFFFFFF)를 해석할 수 있어야 하며, 해석할 수 없을 경우 분석가가 오해하지 않도록 이유를 명확히 알려줘야 함
3. 주어진 범위 내에서 타임스탬프 해석은 정확해야 하며, 초 단위보다 더 정확한 정밀도를 지원하지 않는 경우 허용 오차는 0.5초(반올림), 최대 1초(버림)



FORENSIC FOCUS (forensicfocus.com/)

▪ Interpretation of NTFS Timestamps (cont'd)

- 테스트 설계 고려 사항

1. 범위 (Coverage), 1601-01-01 up to 30828-09-14

2. 윤년 (Leap Years)

3. 반올림 (Rounding)

4. 정렬 (Sorting), 반올림이 정렬에 미치는 영향

5. 특별 테스트

- | | |
|----------------------|-----------------------|
| • 0x0000000000000000 | • 0x8000000000000000 |
| • 0x00FFFFFFFFFFFFFF | • 0xFFFFFFFFE0000000 |
| • 0X01FFFFFFFFFFFFFF | • 0xFFFFFFFFF0000000 |
| • 0X03FFFFFFFFFFFFFF | • 0xFFFFFFFFFFFFFFFFE |
| • ... | • 0xFFFFFFFFFFFFFFFF |
| • 0X0FFFFFFFFFFFFFFF | |

6. 다른 고려 사항, TZ & DST, 윤초, 요일 번역 → 고려하지 않음



FORENSIC FOCUS (forensicfocus.com/)

▪ Interpretation of NTFS Timestamps (cont'd)

- 테스트 결과 – **Autopsy 3.0.4 (1/2)**

- ✓ 타임스탬프 범위

- 1970-01-01 00:00:01 – 2106-02-07 06:28:00

- ✓ 1970-01-01 00:00:00.00000000 변환

- '0000-00-00 00:00:00' 변환됨

- ✓ 범위를 벗어난(1673,1809,1945,2149,2285 등) 타임스탬프 변환

- 2013으로 변환됨



FORENSIC FOCUS (forensicrofocus.com/)

■ Interpretation of NTFS Timestamps (cont'd)

- 테스트 결과 – Autopsy 3.0.4 (2/2)

✓ 1965-1969년 사이의 타임스탬프는 2032-2036으로 변환

NTFSTEST001 - Autopsy 3.0.4

File Edit View Tools Window Help

Close Case Add Image Generate Report Keyword Lists Search...

Directory Listing

/img_NTFSTEST001.001/NTFSTEST001 - TIMESTAMPS/A - YEAR COVERAGE/03 - YEARS/1900 102 Results

Name	Created Time	Access Time	Mod. Time	Change Time	Size
1965	2032-08-09 13:29:46	2032-08-09 13:29:46	2033-08-09 13:29:46	2033-08-09 13:29:46	0
1966	2033-08-09 13:29:46	2033-08-09 13:29:46	2034-08-09 13:29:46	2034-08-09 13:29:46	0
1967	2034-08-09 13:29:46	2034-08-09 13:29:46	2035-08-09 13:29:46	2035-08-09 13:29:46	0
1968	2035-08-09 13:29:46	2035-08-09 13:29:46	2036-08-09 13:29:46	2036-08-09 13:29:46	0
1969	2036-08-09 13:29:46	2036-08-09 13:29:46	2037-08-09 13:29:46	2037-08-09 13:29:46	0
1970	0000-00-00 00:00:00	0000-00-00 00:00:00	1970-12-31 23:59:59	1970-12-31 23:59:59	0
1971	1971-01-01 00:00:00	1971-01-01 00:00:00	1971-12-31 23:59:59	1971-12-31 23:59:59	0
1972	1972-01-01 00:00:00	1972-01-01 00:00:00	1972-12-31 23:59:59	1972-12-31 23:59:59	0
1973	1973-01-01 00:00:00	1973-01-01 00:00:00	1973-12-31 23:59:59	1973-12-31 23:59:59	0
1974	1974-01-01 00:00:00	1974-01-01 00:00:00	1974-12-31 23:59:59	1974-12-31 23:59:59	0
1975	1975-01-01 00:00:00	1975-01-01 00:00:00	1975-12-31 23:59:59	1975-12-31 23:59:59	0
1976	1976-01-01 00:00:00	1976-01-01 00:00:00	1976-12-31 23:59:59	1976-12-31 23:59:59	0

Hex View String View Result View Text View Media View



FORENSIC FOCUS (forensicfocus.com/)

▪ Interpretation of NTFS Timestamps (cont'd)

- 테스트 결과 – **EnCase Forensic 6.19.6 (1/2)**
 - ✓ 타임스탬프 범위
 - 1970-01-01 13:00 — 2038-01-19 03:14:06
 - ✓ 1970-01-01 00:00 — 12:00 변환
 - (empty)
 - ✓ 범위를 벗어난 타임스탬프 변환
 - (empty)



FORENSIC FOCUS (forensicrofocus.com/)

■ Interpretation of NTFS Timestamps (cont'd)

• 테스트 결과 – EnCase Forensic 6.19.6 (2/2)

The screenshot displays the EnCase Forensic 6.19.6 interface. On the left, a file tree shows the structure of the disk image, including folders for '2200', '2300', '04 - CUT-OFF DATES', and 'B - LEAP YEARS'. The main window shows a table of NTFS timestamps. A red box highlights rows 25 through 37. The bottom status bar indicates the current file is 'Empty File' and provides the path: 'Case Blue\Disk Image\NTFSTEST001 - TIMESTAMPS\A - YEAR COVERAGE\04 - CUT-OFF DATES\1970...00 - HH-24 (PS 169912 LS 169912 CL 21239 SO 400 FO 0 LE 1)'.

Name	Last Accessed	File Created	Last Written	Entry Modified
25 24 - HH+0				
26 25 - HH+1				
27 26 - HH+2				
28 27 - HH+3				
29 28 - HH+4				
30 29 - HH+5				
31 30 - HH+6				
32 31 - HH+7				
33 32 - HH+8				
34 33 - HH+9				
35 34 - HH+10				
36 35 - HH+11				
37 36 - HH+12			1970-01-01 12:59:59	1970-01-01 12:59:59
38 37 - HH+13	1970-01-01 13:00:00	1970-01-01 13:00:00	1970-01-01 13:59:59	1970-01-01 13:59:59
39 38 - HH+14	1970-01-01 14:00:00	1970-01-01 14:00:00	1970-01-01 14:59:59	1970-01-01 14:59:59
40 39 - HH+15	1970-01-01 15:00:00	1970-01-01 15:00:00	1970-01-01 15:59:59	1970-01-01 15:59:59



FORENSIC FOCUS (forensicfocus.com/)

▪ Interpretation of NTFS Timestamps (cont'd)

- 테스트 결과 – **ProDiscover Basic 6.5.0.0 (1/2)**

- ✓ 타임스탬프 범위

- 1970-01-02 — 2038, 2107 — 2174, 2242 — 2310, 2378 — 2399

- ✓ 1970-01-02 이전과 일부 3000년 이후의 시간 범위

- 1970-01-01 00:00

- ✓ 범위를 벗어난 2038년 이후의 타임스탬프

- (unknown)

- ✓ 분 단위 이하의 범위는 표시하지 않음



FORENSIC FOCUS (forensicrofocus.com/)

▪ Interpretation of NTFS Timestamps (cont'd)

- 테스트 결과 – ProDiscover Basic 6.5.0.0 (2/2)

The screenshot shows the ProDiscover Basic interface for NTFSTESTS001. The left pane displays a file tree structure under 'Images' and 'C:\CASES\Blue256\EVIDENCE\NTFS'. The right pane shows a table of NTFS timestamps for various files.

Select	File Name	File Extension	Created Date	Accessed Date	Modified Date	Size
<input type="checkbox"/>	1600		01/01/1970 00:00	01/01/1970 00:00	01/01/1970 00:00	
<input type="checkbox"/>	1700		01/01/1970 00:00	01/01/1970 00:00	01/01/1970 00:00	
<input type="checkbox"/>	1800		01/01/1970 00:00	01/01/1970 00:00	01/01/1970 00:00	
<input type="checkbox"/>	1900		01/01/1970 00:00	01/01/1970 00:00	12/31/1999 23:59	
<input type="checkbox"/>	2000		01/01/2000 00:00	01/01/2000 00:00	{unknown}	
<input type="checkbox"/>	2100		{unknown}	{unknown}	{unknown}	
<input type="checkbox"/>	2200		{unknown}	{unknown}	12/31/2299 23:59	
<input type="checkbox"/>	2300		01/01/2300 00:00	01/01/2300 00:00	12/31/2399 23:59	

8 Object(s) (8 Folder(s), 0 File(s))



FORENSIC FOCUS (forensicfocus.com/)

▪ Interpretation of NTFS Timestamps (cont'd)

- 테스트 결과 – **WinHex 16.6 SR-4 (1/2)**

- ✓ 타임스탬프 범위

- 1601-01-01 00:00:01 — 2286-01-09 23:30:11.

- ✓ 1601-01-01 00:00:00.0000000|.0000001, 30828-09-14 02:48:05

- (blank)

- ✓ 2286-01-09 23:30:11 이후의 타임스탬프, 지정된 범위의 시간도 일부

- ?



FORENSIC FOCUS (forensicrofocus.com/)

▪ Interpretation of NTFS Timestamps (cont'd)

- 테스트 결과 – WinHex 16.6 SR-4 (2/2)

WinHex - [NTFSTEST.001] 16.6 SR-4

File Edit Search Navigation View Tools Specialist Options Window Help

Case Data

File Edit

NTFSTEST

\NTFSTEST001 - TIMESTAMPS\A - Y... \01 - MILLENNIA 30 files, 0 dir.

Name	Ext.	Size	Created	Modified	Accessed	Attr.	1st sector
..							
01000		0 B		2000-01-01 00:00:00		A	
02000		0 B	2000-01-01 00:00:00	2086-08-20 00:39:44	2000-01-01 00:00:00	A	
03000		0 B	2086-08-20 00:39:44	2173-04-08 01:19:29	2086-08-20 00:39:44	A	
04000		0 B	2173-04-08 01:19:29	2259-11-27 01:59:14	2173-04-08 01:19:29	A	
05000		0 B	2259-11-27 01:59:14	?	2259-11-27 01:59:14	A	
06000		0 B	?	?	?	A	
07000		0 B		1606-06-10 04:38:13	?	A	
08000		0 B	1606-06-10 04:38:13	1693-01-27 05:17:58	1606-06-10 04:38:13	A	
09000		0 B	1693-01-27 05:17:58	1779-09-16 05:57:43	1693-01-27 05:17:58	A	
10000		0 B	1779-09-16 05:57:43	1866-05-06 06:37:28	1779-09-16 05:57:43	A	
11000		0 B	1866-05-06 06:37:28	1952-12-23 07:17:13	1866-05-06 06:37:28	A	
12000		0 B	1952-12-23 07:17:13	2039-08-12 07:56:57	1952-12-23 07:17:13	A	
13000		0 B	2039-08-12 07:56:57	2126-03-31 08:36:42	2039-08-12 07:56:57	A	
14000		0 B	2126-03-31 08:36:42	2212-11-18 09:16:27	2126-03-31 08:36:42	A	
15000		0 B	2212-11-18 09:16:27	?	2212-11-18 09:16:27	A	
16000		0 B	?	?	?	A	
17000		0 B	?	?	?	A	



FORENSIC FOCUS (forensicfocus.com/)

▪ Interpretation of NTFS Timestamps (cont'd)

- 추가 테스트 – PowerShell (1/2)

- ✓ 타임스탬프 범위

- 1601-01-01 00:00:00 – 9999-12-31 23:59:59

- ✓ 지정된 범위를 넘는 값

- (blank)

- ✓ 항목의 이름, 생성|수정|접근 시간을 얻어온 후 정렬

```
Get-ChildItem path | Select-Object name,creationtime,lastwritetime,lastaccesstime | Sort timefield
```



FORENSIC FOCUS (forensicrofocus.com/)

▪ Interpretation of NTFS Timestamps (cont'd)

- 추가 테스트 – PowerShell (2/2)

✓ LastWriteTime으로 정렬

```
Administrator: C:\WINDOWS\system32\WindowsPowerShell\v1.0\powershell.exe
PS E:\NTFSTEST001 - TIMESTAMPS\D - SORTING\04 - BY NANOSECONDS> Get-Childitem S:\NTFSTEST001 - RECURSIVE - BY LASTWRITETIME
select-Object name,creationtime,lastaccesstime,lastwritetime | sort LastWriteTime
```

Name	CreationTime	LastAccessTime	LastWriteTime
03_C00_A09_W00.M00	2001-01-01 00:00:00	2001-01-01 00:00:00	2001-01-01 00:00:00
01_C02_A07_W01.M66	2001-01-01 00:00:00	2001-01-01 00:00:00	2001-01-01 00:00:00
07_C04_A05_W02.M34	2001-01-01 00:00:00	2001-01-01 00:00:00	2001-01-01 00:00:00
06_C06_A03_W03.M02	2001-01-01 00:00:00	2001-01-01 00:00:00	2001-01-01 00:00:00
04_C08_A01_W04.M68	2001-01-01 00:00:00	2001-01-01 00:00:00	2001-01-01 00:00:00
00_C09_A00_W05.M09	2001-01-01 00:00:00	2001-01-01 00:00:00	2001-01-01 00:00:00
08_C07_A02_W06.M35	2001-01-01 00:00:00	2001-01-01 00:00:00	2001-01-01 00:00:00
05_C05_A04_W07.M67	2001-01-01 00:00:00	2001-01-01 00:00:00	2001-01-01 00:00:00
09_C03_A06_W08.M01	2001-01-01 00:00:00	2001-01-01 00:00:00	2001-01-01 00:00:00
02_C01_A08_W09.M33	2001-01-01 00:00:00	2001-01-01 00:00:00	2001-01-01 00:00:00

```
PS E:\NTFSTEST001 - TIMESTAMPS\D - SORTING\04 - BY NANOSECONDS>
```




FORENSIC FOCUS (forensicfocus.com/)

▪ Interpretation of NTFS Timestamps (cont'd)

- 추가 테스트 – **Windows Explorer GUI (1/2)**

- ✓ 타임스탬프 범위

- 1980-01-01 00:00:00 — 2107-12-31 23:59:57

- ✓ 지정된 범위를 넘는 값, 2010-12-31 23:59:58|59

- (blank)

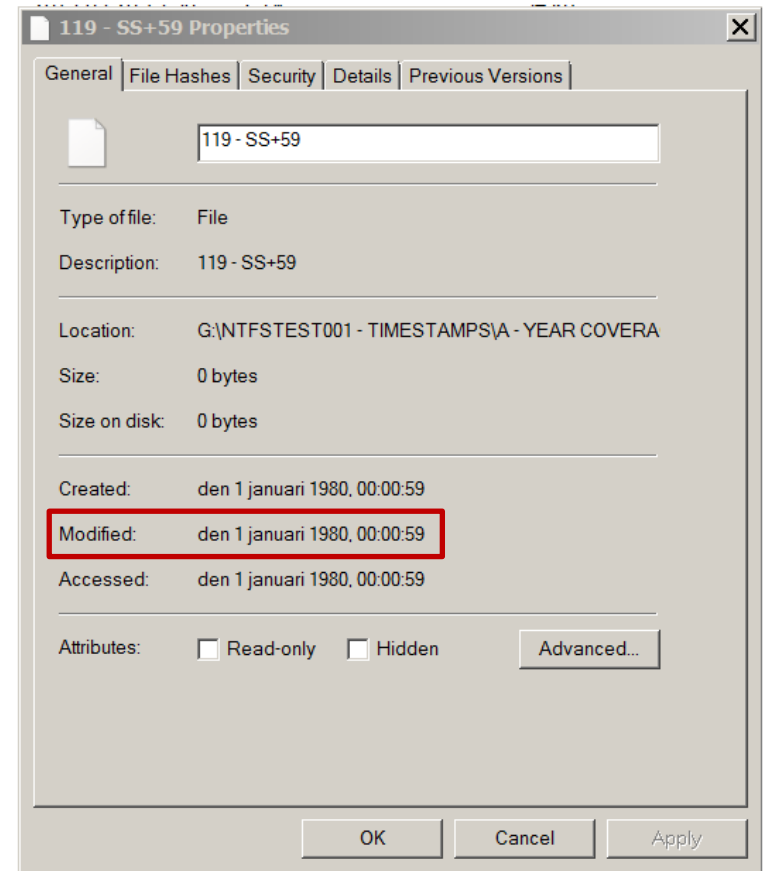
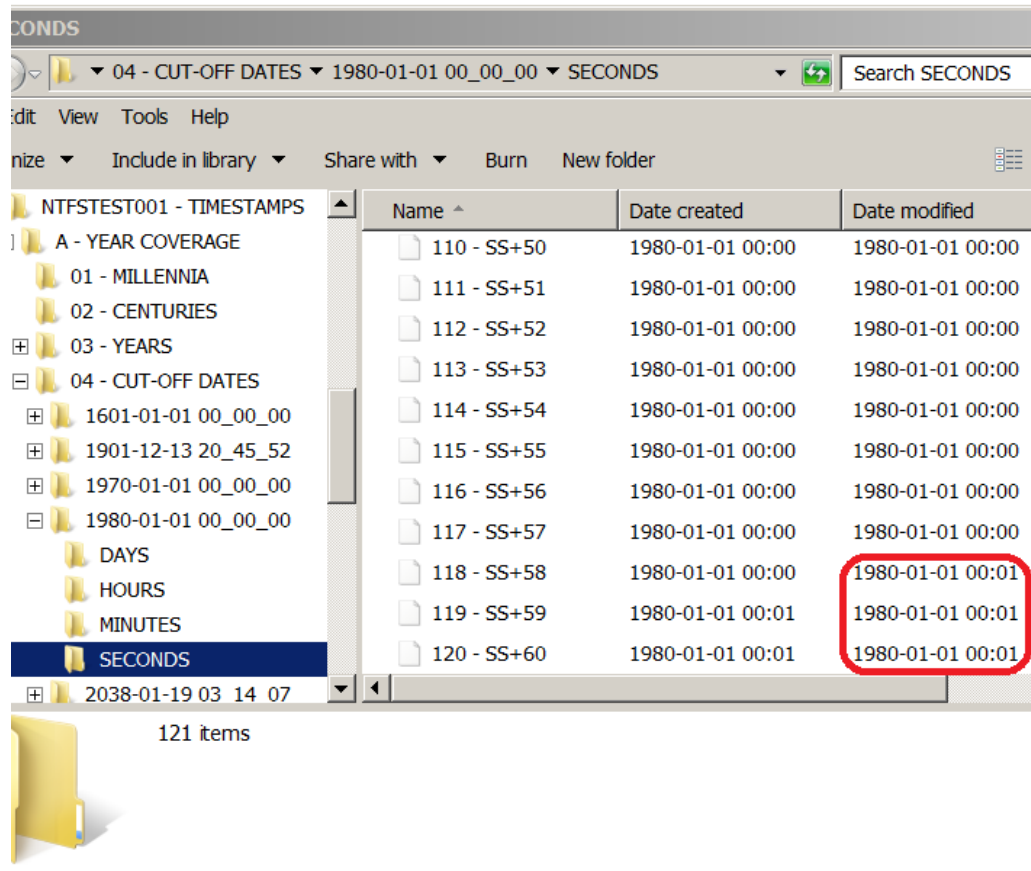
- ✓ 초 단위가 잘못 표현되는 경우도 발생



FORENSIC FOCUS (forensicfocus.com/)

▪ Interpretation of NTFS Timestamps (cont'd)

• 추가 테스트 – Windows Explorer GUI (2/2)





FORENSIC FOCUS (forensicfocus.com/)

▪ Interpretation of NTFS Timestamps (cont'd)

• 결과 해석

✓ 범위 측면에서 테스트된 도구 중 완벽한 도구는 X

✓ 정확히 해석하는 시간 범위

- PowerShell 1.0 (1601–9999) → **Non** Forensics Tool
- Windows Explorer GUI (1980–2107) → **Non** Forensics Tool
- EnCase 6.19 (1970–2038)

✓ 신뢰하기 어려운 도구

- Autopsy 3.0.4
- ProDiscover Basic 6.5.0.0
- WinHex 16.6 SR-4



FORENSIC FOCUS (forensicfocus.com/)

▪ Interpretation of NTFS Timestamps

• 해결 방안

- ✓ 조사 단계를 문서화하는 것이 중요
- ✓ 1970 – 2038년 범위는 대부분의 도구가 정확히 커버
- ✓ 해당 범위를 넘어서는 경우, 이를 판단할 수 있어야 함
- ✓ 항상 두 개 이상의 도구로 상호 검증하는 것이 필요



FORENSIC FOCUS (forensicfocus.com/)

▪ Categorization of embedded system forensic collection methodologies (cont'd)

- 임베디드 시스템

- ✓ 휴대폰, 스마트폰, 태블릿, DVD/BlueRay 플레이어, 디지털시계, TV, 자동차, 엘리베이터, 세탁기, 드라이어 등

- 임베디드 시스템 수집 방법

1. 수동 수집 (Manual Acquisition)
2. 논리 수집 (Logical Acquisition)
3. 의사-물리 수집 (Pseudo-physical Acquisition)
4. 지원-포트 수집 (Support-port Acquisition)
5. 회로 읽기 수집 (Circuit read Acquisition)
6. 게이트 읽기 수집 (Gate read Acquisition)



FORENSIC FOCUS (forensicfocus.com/)

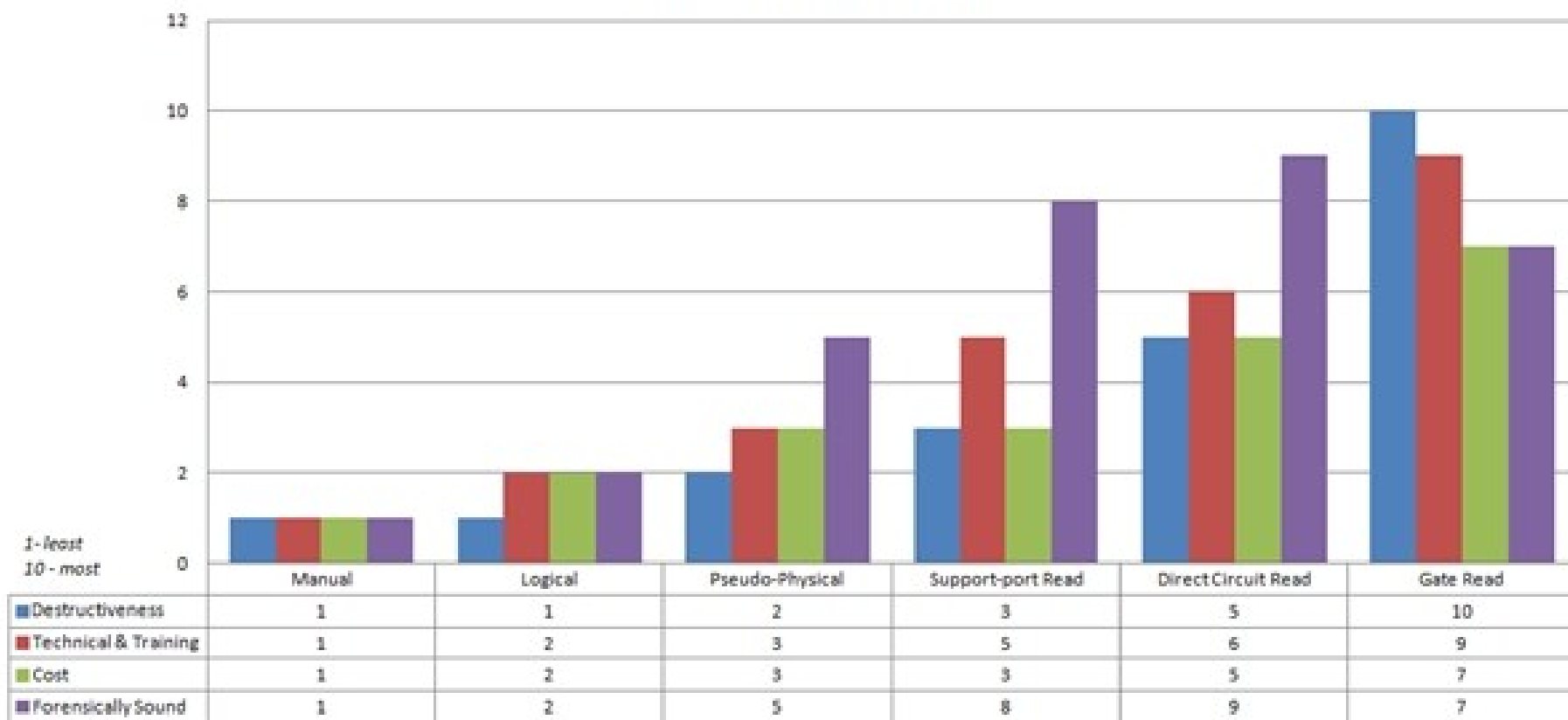
- **Categorization of embedded system forensic collection methodologies (cont'd)**
 - 각 분류를 4가지 영역으로 점수화 (1~10)
 - ✓ 파괴력 (Destructiveness) – 대상 장치에 미치는 영향
 - ✓ 기술과 훈련 (Technical & Training) – 능숙하기 위해 필요한 이해의 폭과 교육
 - ✓ 비용 (Cost) – 필요한 리소스(장비, 도구, 소모품) 비용
 - ✓ 포렌식 건전성 (Forensically Sound) – 고의 또는 과실로 원본을 수정할 가능성



FORENSIC FOCUS (forensicfocus.com/)

- Categorization of embedded system forensic collection methodologies

Methodology Comparison





FORENSIC FOCUS (forensicfocus.com/)

▪ Categorization of embedded system forensic collection methodologies ([cont'd](#))

- 수동 (Manual)

- ✓ 고전적인 방법으로 장치의 모든 변화를 카메라로 기록
- ✓ Paraben Project-A-Phone



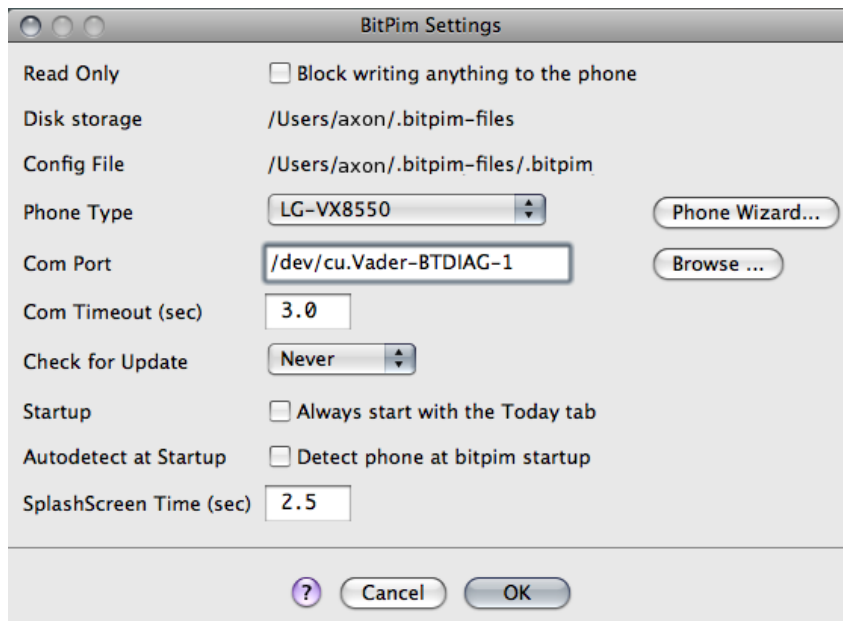


FORENSIC FOCUS (forensicfocus.com/)

▪ Categorization of embedded system forensic collection methodologies (cont'd)

• 논리 (Logical)

- ✓ 장치의 운영체제의 모든 권한을 이용하여 데이터를 획득하는 방법
- ✓ 장치를 워크스테이션에 연결하고 다양한 소프트웨어를 이용해 운영체제와 통신
- ✓ 전용 케이블을 사용하여 USB 포트에 연결한 후 시리얼 통신을 이용해 획득





FORENSIC FOCUS (forensicfocus.com/)

▪ Categorization of embedded system forensic collection methodologies (cont'd)

• 의사-물리 (Pseudo-physical)

- ✓ 대부분의 데이터 영역에 접근할 수 있는 방법
- ✓ 대상 장치에 프로그램 코드를 강제로 주입
- ✓ 프로그램 코드를 이용할 수 있는 다양한 소프트웨어 패키지를 이용해 장치 연결
- ✓ 대상 장치를 손상시키게 됨 → forensically sound
- ✓ Device Firmware Update(DFU)로 부팅하면 주입한 프로그램 코드를 실행
- ✓ 안드로이드 수집 방법
 - 부트로더 잠금 해제(언락)
 - 복구 모드 커널 플래싱(패치) 후 복구 모드(Recovery Mode)로 부팅
 - 램 디스크(hardless)를 이용해 이미징



FORENSIC FOCUS (forensicfocus.com/)

▪ Categorization of embedded system forensic collection methodologies (cont'd)

• 지원-포트 (Support-port)

- ✓ 대량 생산 기기는 테스트, 펌웨어 업데이트를 위해 고유한 포트 지원
- ✓ 보통 포트는 USB, RS232, 핀, 소켓 통신을 지원하도록 구현
- ✓ 포트 접근은 대부분 제조사의 보증 범위를 넘어서는 분해가 필요

✓ 접근 방법

- **Boundary Scan**
- **JTAG**, Joint Test Action Group
- **I2C**, InterIntegrated Circuit
- **SPI**, Serial Peripheral Interface
- **ESSI**, Enhanced Synchronous Serial Interface
- **CAN**, Controller Area Network
- **LIN**, Local Interconnect Network,
- **BDM**, Background Debug Mode



FORENSIC FOCUS (forensicfocus.com/)

▪ Categorization of embedded system forensic collection methodologies (cont'd)

- 회로 읽기 (Circuit read)

- ✓ PCA(Printed Circuit Assembly) 기판에서 칩을 분리(chip-off) ➔ 칩 소켓을 이용

- ✓ 칩 분리 중 영구적인 손상이 발생할 가능성도 존재

- ✓ 회로 읽기 단계

- 1. 장치 분해 후 IC 칩 위치 확인

- 2. 핀 아웃 정보, 세부 통신 방법을 조사

- 3. 칩 예열 후 칩 분리 ➔ 분리된 칩을 임시 소켓에 연결

- 4. TTL(Transistor-Transistor Logic)과 같이 적절한 통신 프로토콜을 사용하는 장치와 연결



FORENSIC FOCUS (forensicfocus.com/)

▪ Categorization of embedded system forensic collection methodologies (cont'd)

• 게이트 읽기 (Gate read)

- ✓ 보통 포렌식 랩에서 찾을 수 없는 장비와 화학 물질이 필요
- ✓ 여러 겹으로 된 칩의 레이어를 분리 후 촬영
- ✓ 사진을 이용해 역공학
- ✓ 게이트 읽기 단계
 1. 장치 분해 후 IC 칩 위치 확인
 2. 핀 아웃 정보 조사
 3. 칩 예열 후 IC 칩 분리 → 화학 물질로 세척 → 실리콘 다이의 조각만 남음
 4. 랩핑하여 실리콘 다이의 각 레이어를 제거, 촬영?
 5. 레이어의 모양, 색상 밀도, 레이어의 상호 연결을 이용해 역공학
(N-타입, P-타입 실리콘, 게이트, 파워, 그라운드 등의 식별이 필요)



FORENSIC FOCUS (forensicfocus.com/)

- **Categorization of embedded system forensic collection methodologies**

	Manual	Logical	Pseudo -physical	Support -port	Circuit Read	Gate Read
Destructiveness	1	1	2	3	5	10
Technical & Training	1	2	3	5	6	9
Cost	1	2	3	3	5	7
Forensically Sound	1	2	5	8	9	7



FORENSIC FOCUS (forensicfocus.com/)

- **KS – an open source bash script for indexing data**
 - /diskspace
 - ✓ disk
 - ✓ deleted
 - ✓ carved
 - ✓ slack
 - **KS** – Keyword Searching Tool
 - ✓ *The Sleuthkit (last release)*
 - ✓ *Photorec*
 - ✓ *MD5Deep*
 - ✓ *RECOLL* – A text search tool for *nix



ForensicKB (forensickb.com)

▪ EnScript to send data directly to SPLUNK for IR, Investigations & Timelines (cont'd)

- 엔케이스 출력을 직접 스플렁크로 보낼 수 있는 엔스크립트
- 기본 설치 위치에 파일 생성

✓ props.conf

```
[source::EnCase]
MAX_DAYS_AGO = 10000
TZ = America/Los_Angeles
REPORT-EnCase = EnCase_Format
TIME_PREFIX = Timestamp..
```














✓ transform.conf

```
[EnCase_Format]
DELIMS="|"
FIELDS="Timestamp","Type","CaseName","Filename","Path","Extension",
"LogicalSize","INode","MD5","ExamHostname","Examiner", "Notes"
```




ForensicKB (forensickb.com)

- EnScript to send data directly to SPLUNK for IR, Investigations & Timelines (cont'd)
 - 보내고자 하는 파일 태그

	Name	Tag
<input checked="" type="checkbox"/> 1	 Install ICQ	SendToSplunk
<input checked="" type="checkbox"/> 2	 Palm	SendToSplunk
<input checked="" type="checkbox"/> 3	 My Music	SendToSplunk
<input checked="" type="checkbox"/> 4	 X Drive	SendToSplunk
<input checked="" type="checkbox"/> 5	 Sabrina Dewercs	SendToSplunk
<input checked="" type="checkbox"/> 6	 desktop.ini	SendToSplunk
<input checked="" type="checkbox"/> 7	 tourstart.exe	SendToSplunk
<input checked="" type="checkbox"/> 8	 Thumbs.db	SendToSplunk
<input checked="" type="checkbox"/> 9	 Sample Pictures.lnk	SendToSplunk
<input checked="" type="checkbox"/> 10	 Sample Music.lnk	SendToSplunk
<input checked="" type="checkbox"/> 11	 INFO2	SendToSplunk
<input checked="" type="checkbox"/> 12	 xdrive_plus_30_build104.exe	SendToSplunk
<input checked="" type="checkbox"/> 13	 X Drive.txt	SendToSplunk



ForensicKB (forensickb.com)

▪ EnScript to send data directly to SPLUNK for IR, Investigations & Timelines (cont'd)

- 엔스크립트 실행

Send files tagged with "SendToSplunk" to ...

Help

Examiner's name:
Lance Mueller

Your computer hostname (to record as source):
Forensicwork1

Splunk server Hostname or IP:
192.168.186.129

Splunk server TCP Port:
9100

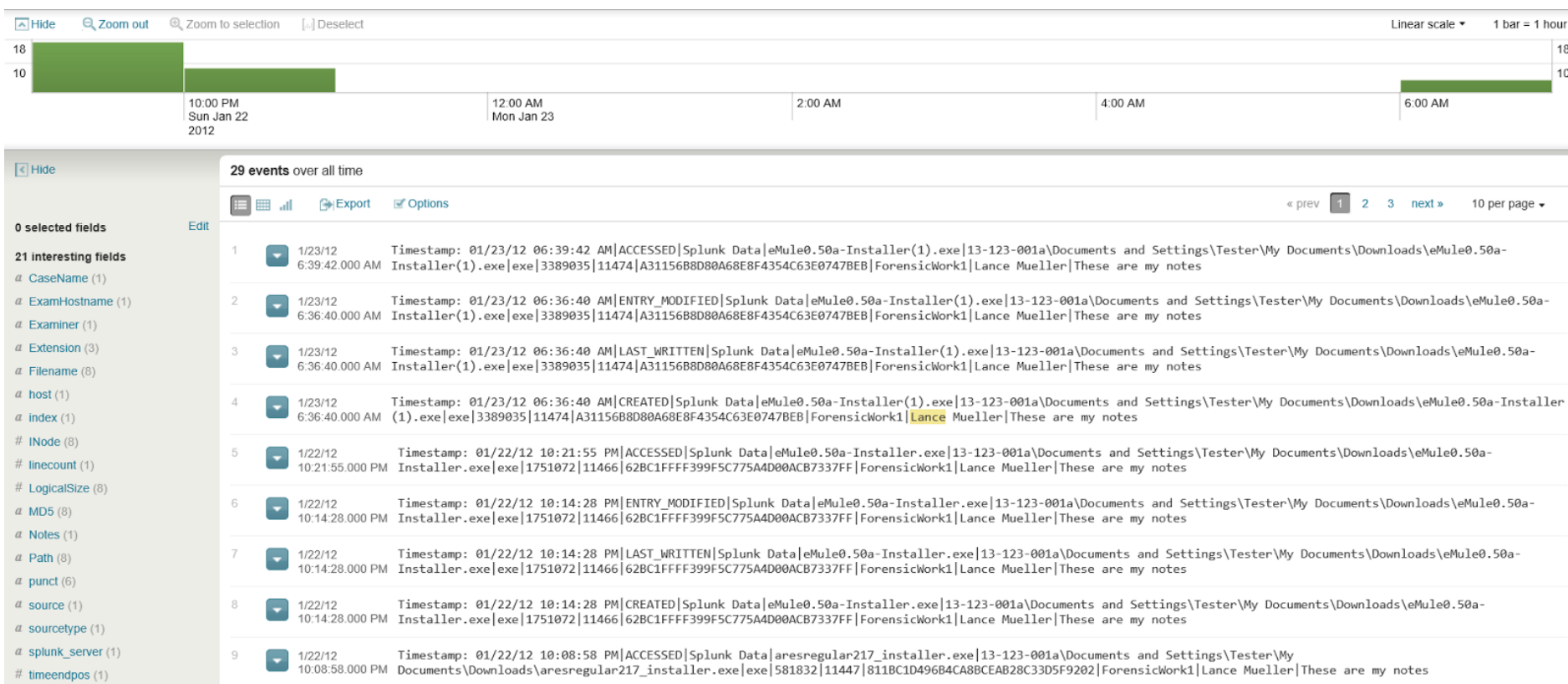
Notes to be included with each event:

OK Cancel



ForensicKB (forensickb.com)

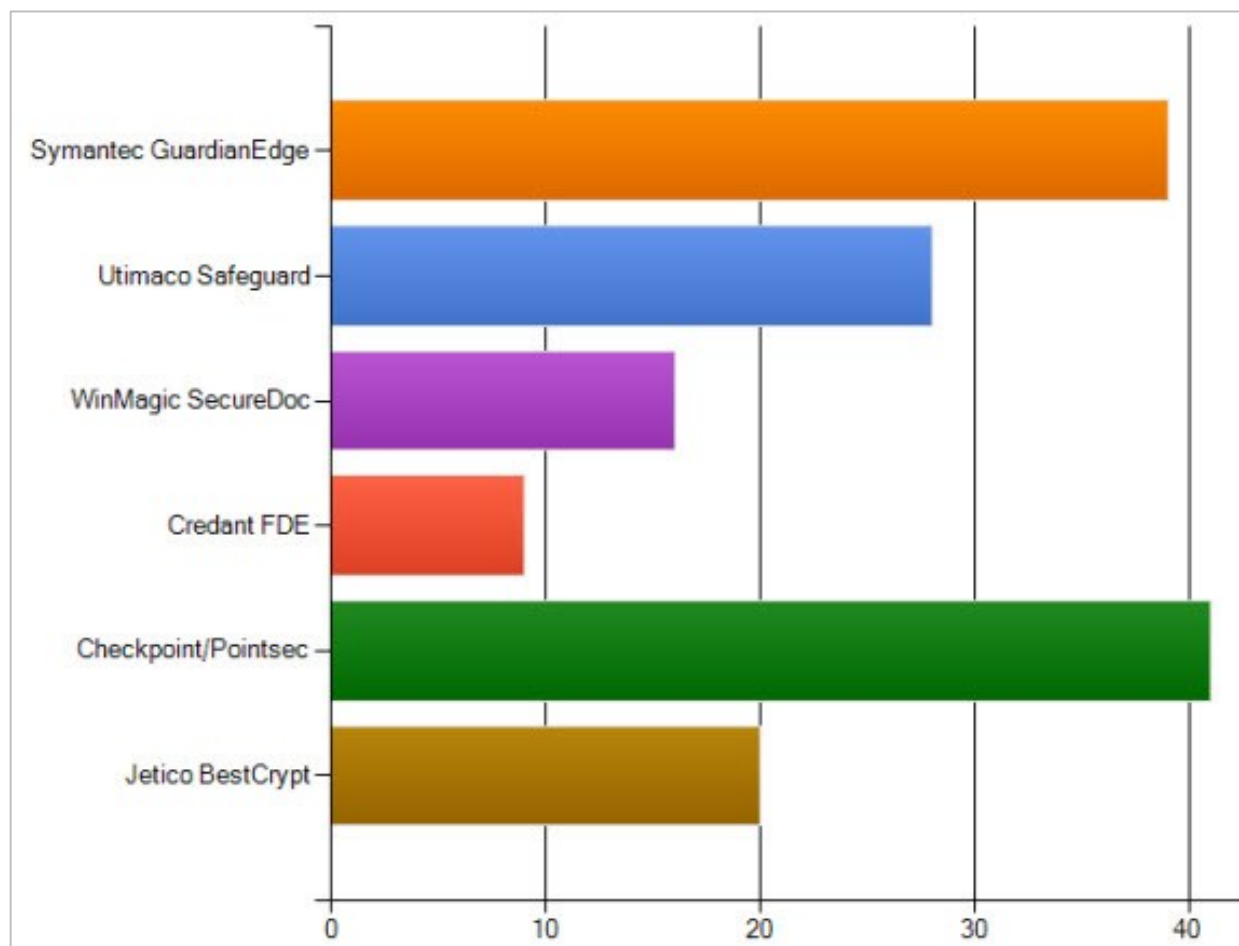
- EnScript to send data directly to SPLUNK for IR, Investigations & Timelines
 - 스플링크로 확인한 데이터





SANS Computer Forensics (computer-forensics.sans.org)

- Encrypted Disk Detector Version 2 (cont'd)





SANS Computer Forensics (computer-forensics.sans.org)

▪ Encrypted Disk Detector Version 2

- 지원하는 FDE

- ✓ TrueCrypt
- ✓ BitLocker
- ✓ PGP
- ✓ SafeBoot
- ✓ Checkpoint
- ✓ GuardianEdge
- ✓ SafeGuard
- ✓ BestCrypt



Others (cont'd)

- **viaForensics** (viaforensics.com) - THOTCON 2013 (slide)
 - THOTCON 2013 – Mobile Security, Forensics, & Malware Analysis with Santoku Linux
 - 시카고 해킹 컨퍼런스에서 viaForensics CEO가 발표한 발표 내용
- **Malware.lu** (malware.lu) - APT1: technical backstage (report)
 - 맨디언트에서 발표한 APT1의 상세 분석 보고서
- **Kaspersky SECURELIST** (securelist.com) - "Winnti" More than just a game (report)
 - 중국에 기반을 둔 해킹 그룹 "Winnti"에 대한 분석 보고서
 - 2011년부터 추적을 시작하여 현재도 진행 중
 - 주 목적은 소스 코드와 디지털 서명서 탈취



Others (cont'd)

- **Security Research and Esoteric PowerShell Knowledge ([exploit-Monday.com](http://exploit-monday.com))** -
Practical Persistence with PowerShell (slide)
 - 파워셸을 이용해 악성코드의 지속성을 유지할 수 있는 방안 소개
- **Kahu Security (kahusecurity.com)** - Dissecting a Malicious Word Document
 - 스피어피싱 캠페인에 사용했던 CVE-2012-0158 취약점을 악용한 RTF 문서의 분석 과정을 설명
- **Sketchymoose's Blog (<http://sketchymoose.blogspot.kr>)** - A Fun Post About Testing it Out...
 - NTFS 1시간의 법칙에 대한 설명



Others (cont'd)

- **Carpe Indicium** (carpeindicium.com/blog/) – Forensic Artifacts of Microsoft Lync 2010
 - 3번에 걸쳐 기업메신저인 MS Lync의 아티팩트를 설명
- **Exploit Monday** (exploit-Monday.com) – Practical Persistence with PowerShell
 - 파워셸의 막강한 능력에 비해 이에 대한 대비 부족
 - 파워셸 악용 가능성 소개 → 파워셸 악용 악성코드 등장
 - 파워셸을 사용하여 윈도우 지속성 매커니즘 구현
- **Delusions of Grandeur Blog** (delogrand.blogspot.fi) – Cyber Defense Exercise 2013:
Extracting cached passphrases in Truecrypt
 - 메모리에서 트루크립트의 캐시된 패스워드 문자열을 추출



Others

- **Document (documentmedia.com)** – The Long-term Preservation of Digital Evidence
 - 이디스커버리의 활성화로 디지털증거의 장기 보존 요구 증가 → 대응
- **Hexacorn (hexacorn.com)** – JumpLists file names and AppID calculator
 - 점프 목록의 AppID 생성 방법 발견 → 스크립트 제공
 - 알려지지 않은 도구의 AppID를 손쉽게 관리 → 안티포렌식 도구 확인 등



dForensics Repository

- **SANS InfoSec Reading Room – Forensics (updated)**
 - **Forensic Analysis on iOS Devices**, JAN 2013
 - **Windows Logon Forensics**, Mar 2013
 - **Indicators of Compromise in Memory Forensics**, Mar 2013
 - **Using IOC(Indicators of Compromise) in Malware Forensics**, Apr 2013
 - **Log2Pcap**, May 2013

- **Invent with Python** – Learn to program by hacking ciphers



dForensics Tools

- **chainbreaker**
- **NirSoft**
 - (New) NetConnectChoose
 - (New) TcpLogView
 - (Updated) RecentFilesView
- **(New) Actaeon** –Hypervisor Hunter
- **(Updated) REMnux** – Linux Distro for Malware Analysis
- **(Updated) AnalyzeMFT**
- **(Updated) EnCase v7.07**

