Trends in dForensics, May/2013

JK Kim

proneer

proneer@gmail.com

http://forensic-proof.com

Security is a people problem…

FORENSIC-PROOF (forensic-proof.com)

- 화이트 해커를 양성해야 하는가?
- NTFS 1시간, FAT 1일 법칙 (The law of NTFS's 1 hour and FAT's 1 day)
- APT 공격 방어 전략 (APT Countermeasures)

n0fate's Forensic Space (forensic.n0fate.com)

- Keychain Forensics: Part I
- Keychain Forensics: Part II

CYLANCE TECHNICAL BLOG (cylance.com/labs.shtml)

- When Advanced Persistent Threats Aren't
- Google's Building Hackable
- How to Prevent/Detect Security Breaches with the Help of Regulators
- C2 Malware Targets Battle.Net Accounts
- WordPress Under Attack
- Uncommon Handle Analysis in Incident Response and Forensics
- Uncommon Event Log Analysis for Incident Response and Forensic Investigations

DFINews - Articles (dfinews.com/articles)

- The Case for Teaching Network Protocols to Computer Forensics Examiners: Part 1
- Forensic Insight into Solid State Drives
- Training is Not Enough: A Case for Education Over Training
- Catching the Ghost: How to Discover Ephemeral Evidence through Live RAM Analysis
- Starting A Career in Digital Forensics: Part 2
- The Rise (and Risk) of Modern Media
- Today's Facility Design for Tomorrow's Cyber Crime
- Ethical Practices in Digital Forensics: Part 2
- Reporting Examination Results

DFINews - Articles (dfinews.com/articles)

- **The Case for Teaching Network Protocols to Computer Forensics Examiners: Part 1**
  - 포렌식 조사관은 하드웨어, 운영체제, 소프트웨어에 능통 ➔ 이 분야에 교육 집중
  - 최근 컴퓨터 통신 및 네트워크 프로토콜에 대한 네트워크 포렌식 기술이 급부상
  - **네트워크 포렌식의 역할**
    - ✓ 컴퓨터 종료 ➔ 하드 드라이브 내용은 정적으로 유지
    - ✓ 네트워크는 항상 끊임없이 변화 ➔ 스냅샷 분석에 치중 ➔ 복제 불가능
    - ✓ 네트워크 기반 정보는 다양한 영역에 활용
      - 네트워크 관리, 정보 보증, 민.형사 사건 조사
    - ✓ 법적 제약
      - Sarbanes-Oxley [SOX], Health Insurance Portability and Accountability Act [HIPAA]
      - 수색 영장의 범위

DFINews - Articles (dfinews.com/articles)

- **The Case for Teaching Network Protocols to Computer Forensics Examiners: Part 1**
  - 침입 탐지, 네트워크 보안 모니터링, 포렌식 분석을 위한 데이터 수집 ➔ 질문으로 구분
    - ✓ 정보 수집의 목적이 무엇인가?
    - ✓ 어떤 정보를 수집하는가?
    - ✓ 언제 정보를 수집하는가? 사전/사후?
    - ✓ 정보는 어떻게/어디에 저장되는가?
    - ✓ 정보는 어떻게/언제/누가 검색하는가?

DFINews - Articles (dfinews.com/articles)

- **The Case for Teaching Network Protocols to Computer Forensics Examiners: Part 1**
  - **포렌식 조사관에 의해 수집되는 네트워크 정보의 4자리 분류**
    1. **전체 데이터 (Full content data)**
       - 네트워크 상의 모든 비트 정보
    2. **세션 데이터 (Session data)**
       - 특정 조사와 관련된 정보 (특정 날짜 및 시간에 특정 고객과 관련된 정보)
    3. **경보 데이터 (Alert data)**
       - 흥미로운 특정 데이터만 수집, IDS 동작과 유사
    4. **통계 데이터 (Statistical data)**
       - 개별적으로는 의미가 없지만 전체 네트워크에서 볼 때 의미가 있는 데이터
       - 운영 모델, 평균 및 표준 편차 모델, 다변량 모델, 시계열 모델, 마르코프 과정 모델

DFINews - Articles (dfinews.com/articles)

- **The Case for Teaching Network Protocols to Computer Forensics Examiners: Part 1**
  - **네트워크 데이터의 출처와 유형**
    - ✓ IDS와 방화벽 로그
    - ✓ HTTP, FTP, 이메일, 그 밖에 서버 로그
    - ✓ 네트워크 애플리케이션 로그
    - ✓ 네트워크 패킷 역추적, TCP 연결 정보
    - ✓ HDD 상의 네트워크 트래픽 아티팩트
    - ✓ 패킷 스니퍼나 네트워크 포렌식 도구에 의해 수집된 라이브 트래픽
    - ✓ 라우팅 및 ARP 테이블 정보, 포트 스캔 정보, SNMP 메시지

DFINews - Articles (dfinews.com/articles)

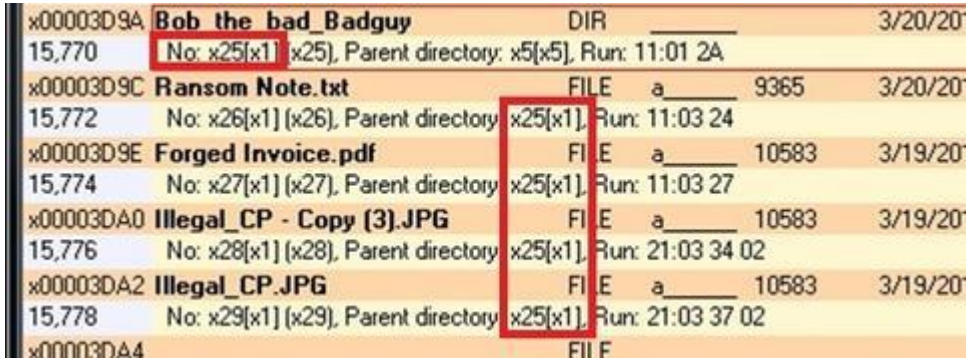
- **The Case for Teaching Network Protocols to Computer Forensics Examiners: Part 1**
  - **네트워크 데이터의 출처와 유형**
    - ✓ 잠재적인 약점
      - 다양한 원인에 의해 수집 데이터가 영향을 받음
      - TCP 릴레이, 프록시 서버, 복잡한 패킷 라우팅, IP 주소 및 이메일 스푸핑, 감염된 다른 시스템, 세션 하이재킹, DNS 포이즈닝 등
      - 패킷 스니퍼가 항상 잘 동작하는가? ➔ 패킷 손실 발생
  - **프로토콜 분석 역할**
    - ✓ 채팅 로그, 이미지, 전자 메일 등 다양한 프로토콜의 연구 필요

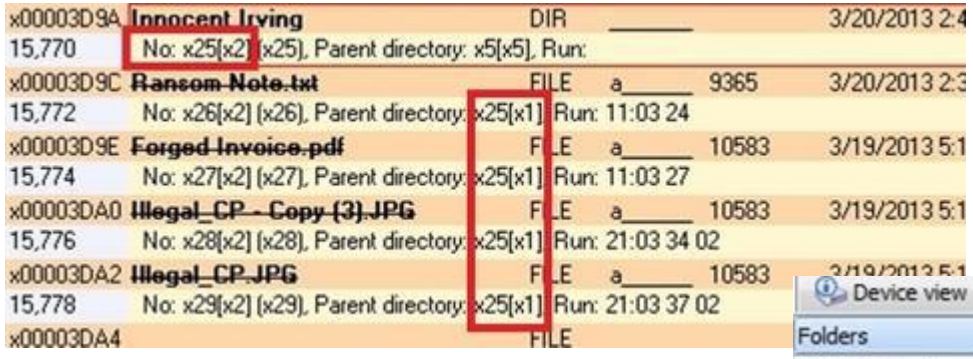
DFINews - Articles (dfinews.com/articles)

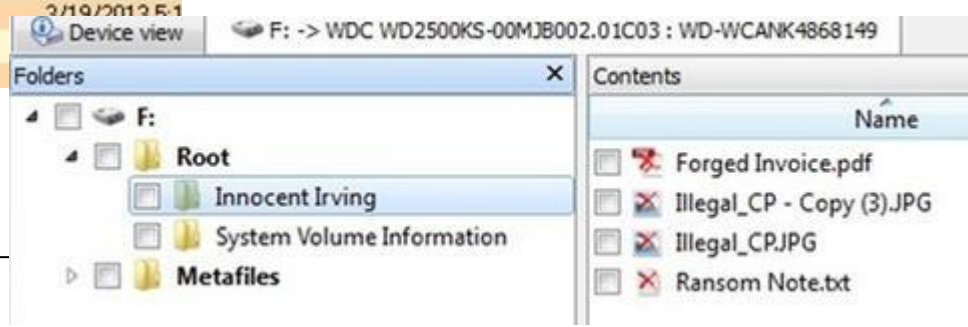
- **Training is Not Enough: A Case for Education Over Training (cont'd)**
  - 단순한 교육 만으로도 반복적인 작업 수행 가능
  - 파일시스템에 대한 깊은 지식 없이도 유용한 결과 도출 가능
  - 하지만, 도구 검증이나 맥락(전후 사정) 분석에는 한계

DFINews - Articles (dfinews.com/articles)

- **Training is Not Enough: A Case for Education Over Training (cont'd)**
  - 도구 검증 예







DFINews - Articles (dfinews.com/articles)

- **Training is Not Enough: A Case for Education Over Training**
  - **맥락 분석**
    - ✓ 디지털포렌식은 단순히 누군가의 유죄를 증명할만한 파일을 복구하는 작업이 아님
      - 사건과 관련하여 죄를 씌우거나 무죄를 증명할 수 있는 종류의 증거 포인트는 보통 수백, 수천에서 수백만까지 있을 수 있음 ➔ 디지털포렌식 조사관의 안목이 필요
    - ✓ 도구를 이용해 수 천장의 이미지 복구 ➔ 더 기술적인 지식을 갖추면 더 많은 데이터 복구 가능
    - ✓ 맥락 분석은 도구에서 제공해주지 않음 ➔ 조사관의 보다 큰 인식 필요
    - ✓ 능숙한 디지털포렌식 조사관
      - 데이터 복구를 넘어 ➔ 복구된 데이터의 신뢰성 검증과 전체 맥락에서 적절한 판단이 가능

SANS Computer Forensics Blog (computer-forensics.sans.org/blog)

- **Tools for Examining XOR Obfuscation for Malware Analysis**
  - **XOR 기반의 난독화 분석 도구**
    - ✓ XORSearch
    - ✓ XORStrings
    - ✓ xorBruteForcer
    - ✓ Brutexor
    - ✓ NoMoreXOR

- **Automating Static Malware Analysis with MASTIFF**
  - 악성코드 정적 분석을 자동화하기 위한 오픈소스 프레임워크

Sketchymoose's Blog (sketchmoose.blogspot.kr)

- **PDF Dissected in 4 ways**
  - **PDF 구조 상세 분석 도구**
    - ✓ pdf-parser
    - ✓ pdf-walker
    - ✓ peepdf
    - ✓ PDF Stream Dumper

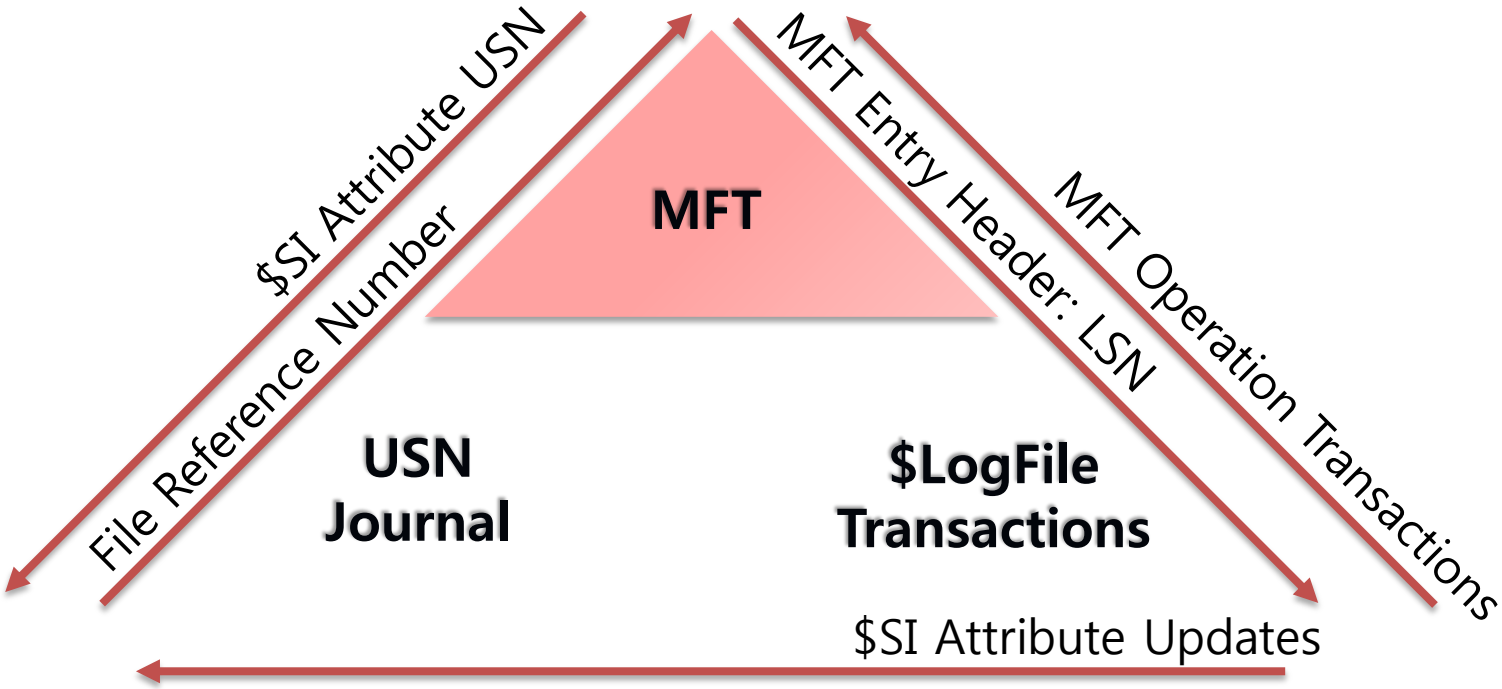
Hacking Exposed CF Blog (hackingexposedcomputerforensicsblog.blogspot.kr)

- **CEIC 2013 and the public beta of the NTFS TriForce (cont'd)**
  - **Tri-Force Overview**
    - ✓ **NTFS System Files**
      - 파일 메타데이터 제공
    - ✓ **USN Journal ($J)**
      - 파일 및 디렉터리 변경 관리
    - ✓ **Transactional Journal ($LogFile)**
      - 파일시스템 변경 관리

Hacking Exposed CF Blog (hackingexposedcomputerforensicsblog.blogspot.kr)

- CEIC 2013 and the public beta of the NTFS TriForce (cont'd)

Connecting the Tri-Force



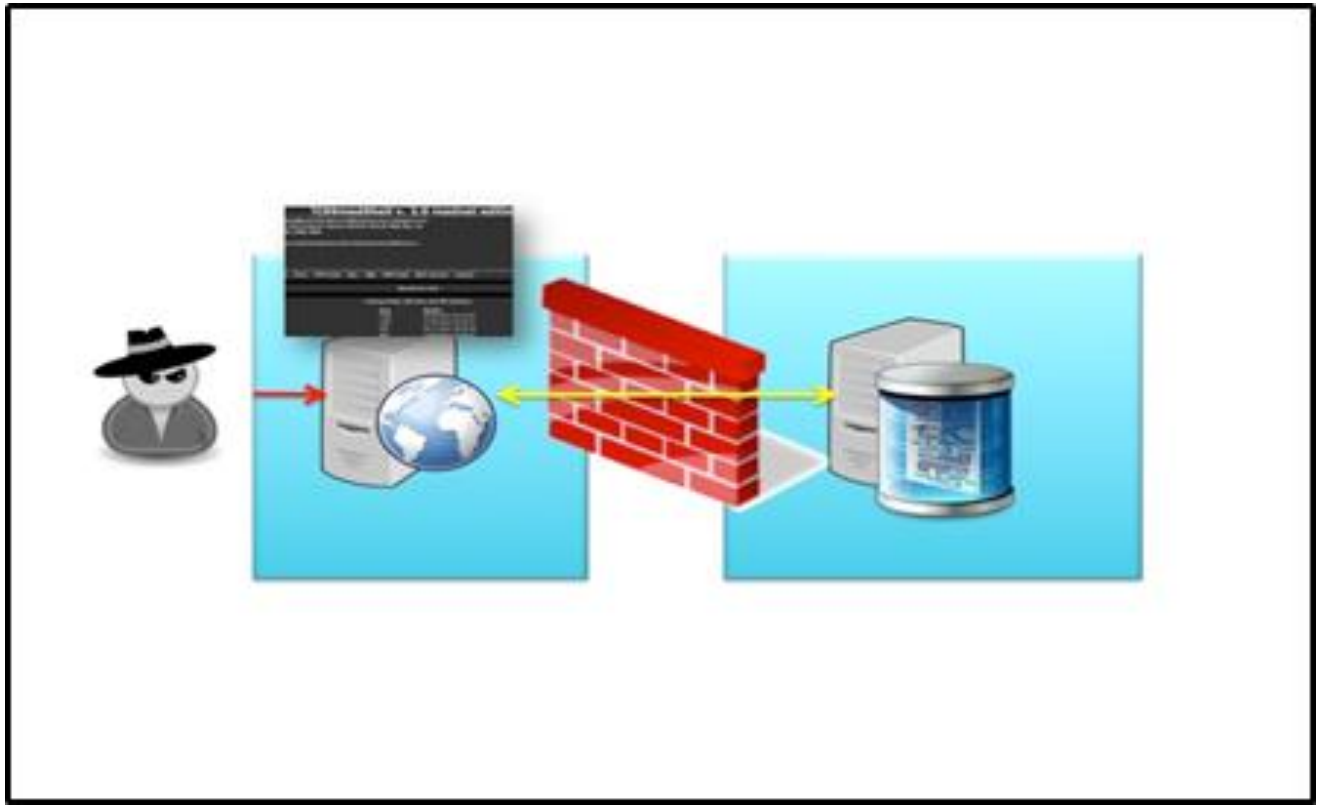
Hacking Exposed CF Blog (hackingexposedcomputerforensicsblog.blogspot.kr)

- **CEIC 2013 and the public beta of the NTFS TriForce**
  - **Labs**
    - ✓ Wiping
    - ✓ CD Burning
    - ✓ Timestamp Changes
    - ✓ Resident Data in XP
  - **Demonstration**
    - ✓ Recovering the Tri-Force in Volume Shadows

Open Security Research (blog.opensecurityresearch.com)

- **Forensics Investigations: Do not forget the database! (cont'd)**

1. 익스플로잇을 사용해 웹 서버 감염
2. 웹 셸로 내부 네트워크(MSSQL) 공격



Open Security Research (blog.opensecurityresearch.com)

- **Forensics Investigations: Do not forget the database! (cont'd)**
  - **휘발성 순서를 기반으로 웹 서버, 데이터베이스 서버에서 다음 순서로 증거 수집**
    1. 메모리 덤프
    2. 페이지 또는 스왑 파일
    3. 실행 중인 프로세스 목록
    4. 응답 포트, 다른 시스템과의 연결 정보와 같은 네트워크 데이터
    5. 시스템 레지스트리
    6. 시스템, 애플리케이션 로그 (IIS 로그, 이벤트 로그 등)
    7. 디스크 포렌식 이미지
    8. 백업 매체
  - **목적 ➔ 타임라인을 통해 공격자의 행위를 재구성**

Open Security Research (blog.opensecurityresearch.com)

- **Forensics Investigations: Do not forget the database! (cont'd)**
  - **셸 (Shell)**
    - ✓ 공격자는 도구 업로드가 가능 (웹 셸 포함) ➔ MSSQL 서버의 SQL 명령 실행 가능
    - ✓ 서버의 사용자 계정 획득

Open Security Research (blog.opensecurityresearch.com)

- **Forensics Investigations: Do not forget the database! (cont'd)**
  - **데이터베이스 포렌식 (Database Forensics)**
    - ✓ **데이터베이스 접속 흔적 발견 ➔ 휘발성 순서에 따라 다음 파일 검색**
      - SQL 서버 세션, 연결 정보, 사용자, 요청
      - 트랜잭션 로그
      - SQL 서버 로그
      - SQL 데이터베이스 파일
      - 시스템 이벤트 로그
      - SQL 서버 Trace 파일
    - ✓ **DB 데이터 파일 및 로그**: ₩₩Microsoft SQL Server₩ MSSQL.1₩MSSQL₩ DATA₩*.MDF | *.LDF
    - ✓ **Trace 파일**: ₩₩Microsoft SQL Server₩MSSQL.1₩MSSQL₩LOG₩LOG_#.TRC
    - ✓ **MS SQL 서버 에러 로그**: ₩₩Microsoft SQLServer₩ MSSQL.1₩ MSSQL₩ LOG₩ERRORLOG

Open Security Research (blog.opensecurityresearch.com)

- **Forensics Investigations: Do not forget the database! (cont'd)**
  - **공격 흔적 확인**
    - ✓ **이벤트 로그**

> **Event ID:** 15281
> **Description:**
> SQL Server blocked access to procedure 'sys.xp_cmdshell' of component 'xp_cmdshell' because this component is turned off as part of the security configuration for this server. A system administrator can enable the use of xp_cmdshell' by using sp_configure. For more information about enabling 'xp_cmdshell', see "Surface Area Configuration" in SQL Server Books Online.

    - ✓ **MSSQL 서버 로그**

> 2013-01-08 14:12:43 spid51 SQL Server blocked access to procedure 'sys.xp_cmdshell' of component 'xp_cmdshell' because this component is turned off as part of the security configuration for this server. A system administrator can enable the use of 'xp_cmdshell' by using sp_configure. For more information about enabling 'xp_cmdshell', see "Surface Area Configuration" in SQL Server Books Online.

Open Security Research (blog.opensecurityresearch.com)

- **Forensics Investigations: Do not forget the database!**
  - **시스템 설정 확인**

```
'select * from sys.configurations where name = 'xp_cmdshell'
```

config_id	name	value	min	max	value_in_use	description
16390	xp_cmdshell	**0**	0	1	0	Enable or disable command shell

  - **설정 변경 테스트**

```
exec sp_configure 'show_advanced_options', 1 reconfigure
exec sp_configure 'xp_cmdshell', 1 reconfigure
```

```
'select * from sys.configurations where name = 'xp_cmdshell'
```

config_id	name	value	min	max	value_in_use	description
16390	xp_cmdshell	**1**	0	1	**1**	Enable or disable command shell

Others

- **Jonathan Zdziarski's Domain**
  - Free Download: iOS Forensic Investigative Methods
- **Linux Sleuthing**
  - SQLite: Hidden Data in Plain Sight
  - iOS6 Photo Streams: "Recover" Deleted Camera Roll Photos
- **4n6k**
  - UserAssist Forensics (timelines, interpretation, testing, & more)
- **BERLA**
  - CEIC 2013 – Vehicle System Forensics
- **Sarah Edwards – CEIC 2013 (SANS DFIR Summit)**
  - When Macs Get Hacked

dForensics Tools

- **ForensicKB –** EnScript to automate Internet Evidence Finder (IEF) for EnCase v6 & v7
- **GetData –** Forensic Explorer
- **NirSoft –** DNSQuerySniffer, WebBrowserPassView
- **Didier Stevens** – VirusTotal: Searching and Submitting
- **Piotribania** – KON-BOOT v2.2
- **Vincent Bénony** – Hopper Multi Platform Disassembler, Decompiler and Debugger

Question and Answer