

Trends in dForensics, Mar/2013

JK Kim

proneer

proneer@gmail.com

<http://forensic-proof.com>

Security is a people problem...





FORENSIC-PROOF (forensic-proof.com/)

- 파일시스템 터널링을 주의하자 (Pay Attention to the File System Tunneling)
- 포렌식 이미징 도구 비교 (FTK vs Tableau vs EnCase Imager)
- 부트 프리패치 파일 최대한 활용하기 (How to Make the Best Use of NTOSBOOT Prefetch file)
- 배드 섹터와 포렌식 이미징 (Bad Sectors vs Forensic Imaging)
- [인터뷰#2] 한국저작권위원회 감정포렌식팀 방효근 과장
- 구글 드라이브 아티팩트 (Google Drive Artifacts)
- 3.20 사이버테러 저장매체 복구 관점에서 (3.20 Cyber-Terror from recovery perspectives)
- 3.20 사이버테러 저장매체 복구 방법 (3.20 Cyber Terror's Damaged Partition Recovery)
- 3.20 사이버테러 저장매체 상세 복구 방법 (3.20 Cyber Terror's Damaged Partition Recovery)



viaForensics (viaforensics.com)

- **Mobile Encryption: The Good, the Bad and the Broken (slide)**
- **Getting sys_call_table on Android**
- **Dude, Where's My Droid?! – RootedCON 2013 Presentation (slide)**
- **Troopers 13 Presentation – Corporate Espionage via Mobile Compromise (slide)**
- **Security vulnerabilities in Any.DO mobile app for Android (slide)**
- **HTCIA – Android Forensics Training Presentation – March 22, 2013 (slide)**



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

▪ UAC Impact on Malware

• DLL Search Order

✓ SafeDllSearchMode 활성화

1. 어플리케이션이 로드된 디렉터리
2. 시스템 디렉터리
3. 16비트 시스템 디렉터리
4. 윈도우 디렉터리
5. **현재 디렉터리**
6. 환경 변수에 등록된 디렉터리

✓ SafeDllSearchMode 비활성화

1. 어플리케이션이 로드된 디렉터리
2. **현재 디렉터리**
3. 시스템 디렉터리
4. 16비트 시스템 디렉터리
5. 윈도우 디렉터리
6. 환경 변수에 등록된 디렉터리

✓ DLL 검색 순서는 사용하는 함수에 따라서도 차이

✓ LoadLibrary() vs. LoadLibraryEx() vs. SetDllDirectory()



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

▪ UAC Impact on Malware

• DLL Search Order Vulnerability

✓ ZeroAccess Method to Bypass UAC

✓ 감염된 웹 사이트 접속

- 악성 *InstallFlashPlayer.exe* 다운 (%UserProfile%\AppData\Local\Temp)
- 악성 *msimg32.dll*도 함께 다운 (%UserProfile%\AppData\Local\Temp)
- *InstallFlashPlayer.exe* 실행

✓ DLL 로드 순서

LdrLoadDll

("*C:\Users\lab\AppData\Local\Temp;C:\Windows\system32;C:\Windows\system;C:\Windows;C:\Windows\system32;C:\Windows;C:\Windows\System32\Wbem;C:\Windows\System32\WindowsPowerShell\v1.0*", 0x0028fa78, 0x0028fa64, 0x0028fa7c)

✓ 메타스플로잇을 이용해 검증



Evidence Technology Magazine (evidencemagazine.com/) (cont'd)

▪ Online data explosion brings new forensic collection techniques

- 소셜미디어와 웹 메일의 급격한 성장으로 온라인 데이터의 폭발적 증가

→ 이디스커버리와 디지털 포렌식 절차에 영향

- 소셜미디어 통계

- ✓ 5분 중 1분은 온라인 소셜 네트워크에 사용
- ✓ 한 달에 6.6 시간을 페이스북에 소비
- ✓ 매달 3백만 개의 블로그가 새로 생성
- ✓ 매일 4억 개의 트윗 생성
- ✓ 매 분마다 플리커에 450만개의 사진 업로드
- ✓ 매 분마다 유튜브에 72시간 분량의 비디오가 업로드





Evidence Technology Magazine (evidencemagazine.com/) (cont'd)

▪ Online data explosion brings new forensic collection techniques

- **3,100,000,000** – 31억 개의 웹메일 계정
- **901,000,000** – 9억 백만 개의 페이스북 적극 사용자
- **54,000,000** – 5천 4백만 개의 워드프레스 사이트
- **160,000,000** – 1억 6천만 개의 링크드인 사용자
- **64,000,000** – 6천 4백만 개의 Tumblr 블로그
- **140,000,000** – 1억 4천만 개의 트위터 적극 사용자
- **2,400,000,000** – 24억 개의 소셜 네트워크 계정

- 이에 따라 최근 소송이나 조사에서 **온라인 정보는 필수!!! ➔ 효과적인 수집 방법**



Evidence Technology Magazine (evidencemagazine.com/) (cont'd)

- Online data explosion brings new forensic collection techniques
 - The Evolution of eDiscovery
 - ✓ 다양한 미디어와 여러 파일 형식을 다루기 위한 표준과 최선을 개발하며 발전
 - ✓ 소셜 네트워크 사이트(SNS)와 웹메일 플랫폼의 데이터는 상대적으로 **NEW!!**
 - ✓ 각 SNS, 웹 메일은 고유한 형식을 사용 → **Challenge!!**
 - ✓ 초기 문맥과 의미를 유지한 상태로 디지털 증거를 수집 및 보존하는 것이 필요



Evidence Technology Magazine (evidencemagazine.com/) (cont'd)

▪ Online data explosion brings new forensic collection techniques

• Webmail Collection

- ✓ 웹메일 형식이 모두 제각각, 출력 형식도 제각각 → 효과적으로 추려내기가 힘들
- ✓ 실제 케이스
 - 80개의 계정, 500,000 이메일 메시지 수집 및 처리
 - EML, Lotus Notes, Exchange, IMAP/POP3, Gmail, Live Mail, Yahoo, Apple Me.com,
 - 신속 정확히 다양한 전자메일 형식을 수집할 수 있는 도구가 X!!
 - 수집 후 중복 처리도 큰 문제 → 이디스커버리를 위해 데이터 양을 줄여야 함
- ✓ 결국, 독자적으로 수집 및 처리 프로그램을 개발하여 작업 수행



Evidence Technology Magazine (evidencemagazine.com/) (cont'd)

- Online data explosion brings new forensic collection techniques

- Social Networking Sites: Facebook, Twitter, LinkedIn, Google

✓ 페이스북 : 전체 사용자 데이터를 쉽게 다운로드

facebook Search for people, places and things

General Account Settings

Name	Jinkook Kim
Username	http://www.facebook.com/proneer
Email	Primary: proneer@gmail.com
Password	Password last changed over a year ago.
Networks	No networks.
Language	English (US)

[Download a copy](#) of your Facebook data.



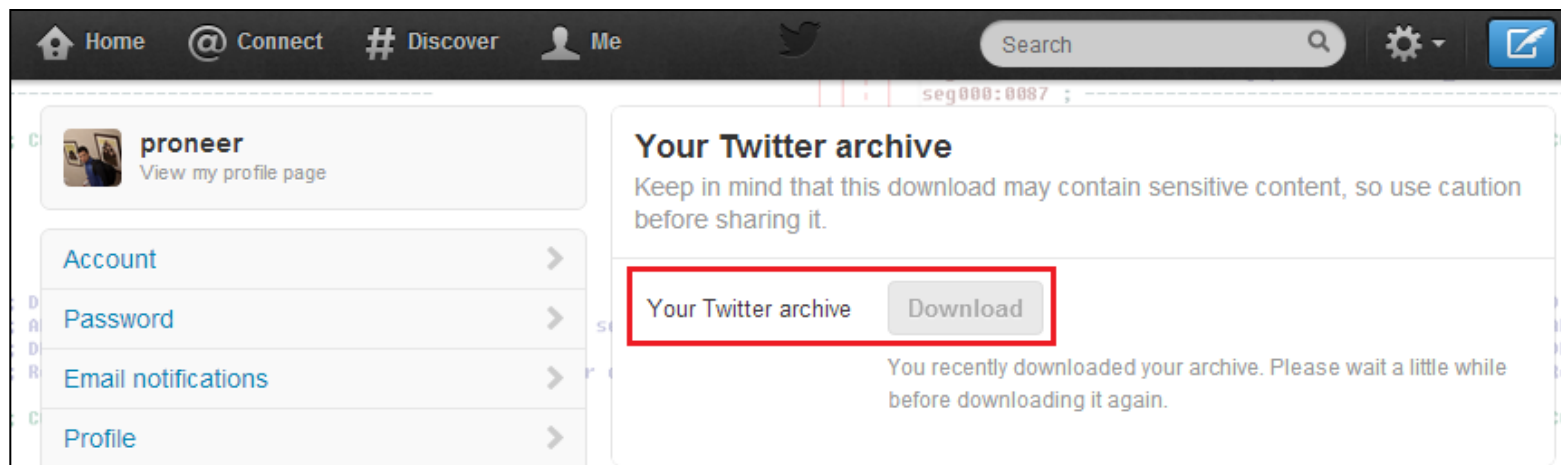
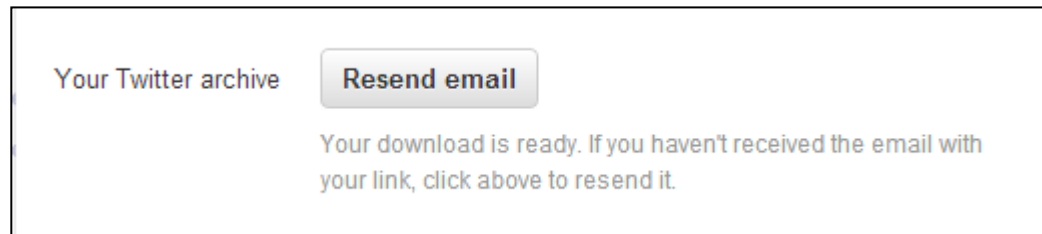
Evidence Technology Magazine (evidencemagazine.com/) (cont'd)

▪ Online data explosion brings new forensic collection techniques

• Social Networking Sites: Facebook, Twitter, LinkedIn, Google

✓ 트위터 : 전체 트윗을 쉽게 다운로드

- Settings → Your Twitter archive





Evidence Technology Magazine (evidencemagazine.com/) (cont'd)

▪ Online data explosion brings new forensic collection techniques

- Social Networking Sites: Facebook, Twitter, LinkedIn, Google

✓ 트위터 : 전체 트윗을 쉽게 다운로드

The screenshot shows the Twitter profile of @pr0neer. The header includes the profile picture, name, and a search bar labeled "Search all Tweets". Below the header, there is a section for "Apr 2013" with 23 tweets. Three tweets are visible, all linking to "securelist.com/en/downloads/v...". The first tweet is from @pr0neer (5 hrs), the second is from @MinhTrietPT (6 hrs) and retweeted by @pr0neer, and the third is from @pr0neer (3 days). To the right of the tweets is a "Tweets Archive" section showing a bar chart for each year from 2010 to 2013. The chart shows the number of tweets per month, with 2013 having the most tweets. Below the chart, it says "This is an offline archive of your Tweets from Twitter. Use the months above to navigate the archive."



Evidence Technology Magazine (evidencemagazine.com/) (cont'd)

▪ Online data explosion brings new forensic collection techniques

- Social Networking Sites: Facebook, Twitter, LinkedIn, Google

✓ 링크드인

- 써드파티 도구를 이용하거나 직접 API를 이용해 코드를 작성 ☹

Privacy Controls

Turn on/off your activity broadcasts

Select who can see your activity feed

Select what others see when you've viewed their profile

Select who can see your connections

Change your profile photo & visibility »

Show/hide "Viewers of this profile also viewed" box

Privacy Controls

Turn on/off data sharing with 3rd party applications

Manage settings for LinkedIn plugins on third-party sites



Evidence Technology Magazine (evidencemagazine.com/) (cont'd)

▪ Online data explosion brings new forensic collection techniques

• Social Networking Sites: Facebook, Twitter, LinkedIn, Google

✓ 구글 : 다양한 데이터를 쉽게 다운로드

- 전용 이디스커버리 도구나 Google Apps Vault 이용

▼ Account

Google lets you save a backup

Account Activity

Download your data

Me on the Web

Download your data

Google Apps 관리자 문서함 소개

Google Apps 관리자 문서함은 Google Apps의 추가 기능이며, 디지털 증거 검색 및 규정 준수를 위해 조직의 이메일을 보관, 저장, 검색하고 내보낼 수 있습니다. 관리자 문서함은 100% 웹 기반이므로 소프트웨어를 설치하거나 관리할 필요가 없습니다.

Google Apps 관리자 문서함으로 수행할 수 있는 작업

- 도메인의 이메일 데이터 검색
- 사용자 계정 및 관련 데이터에 대해 [소송자료 보호](#) 조치를 설정해 이메일 데이터 보존
- 소송자료 보호에 대해 사용자에게 알리고 사용자 동의 기록을 관리
- [법적 사안](#)이라는 단일 보관함에서 관련 검색 자료 및 법적 자료 보존 관리
- 승인된 사용자 간 [법적 사안 공유](#)
- 표준 파일 형식으로 [검색결과 내보내기](#)
- [검색어 저장](#)
- 도메인에 대한 [이메일 보관 정책 설정](#)



Evidence Technology Magazine (evidencemagazine.com/)

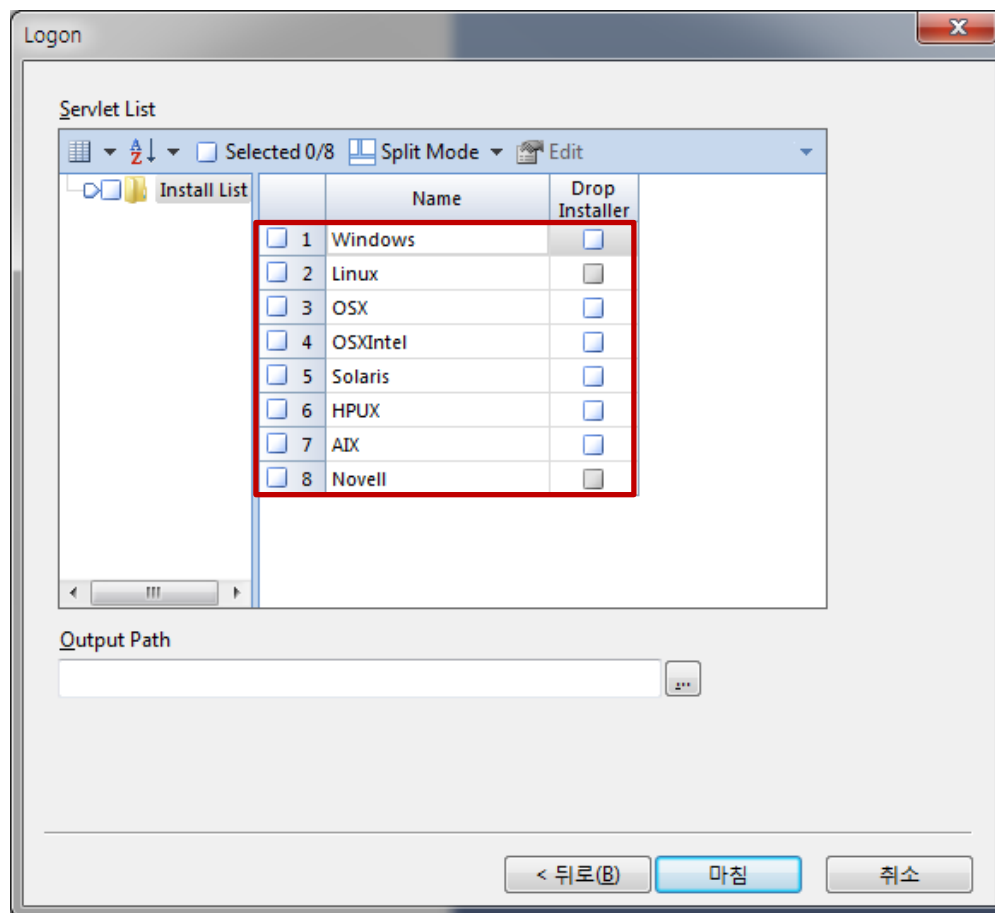
▪ Online data explosion brings new forensic collection techniques

- SNS, 웹 메일의 데이터 수집 방법은 다양하지만 신중을 기해야 함
- 서비스 공급자로부터 적절한 권한을 가져야 하고 위반 사항에 대한 신중한 검토
- 향후 SNS, 웹메일은 모두 페이스북, 트위터, 구글과 같은 형식을 지원할 것으로 예상
- 단, SNS, 웹메일을 수집하기 전
- 절차, 프로토콜, 품질 관리 기준에 대한 심도 있는 심사가 필요



Guidance Software (guidancesoftware.com/) (cont'd)

- EnCase Forensic v7.06 Resources
 - Direct Network Preview

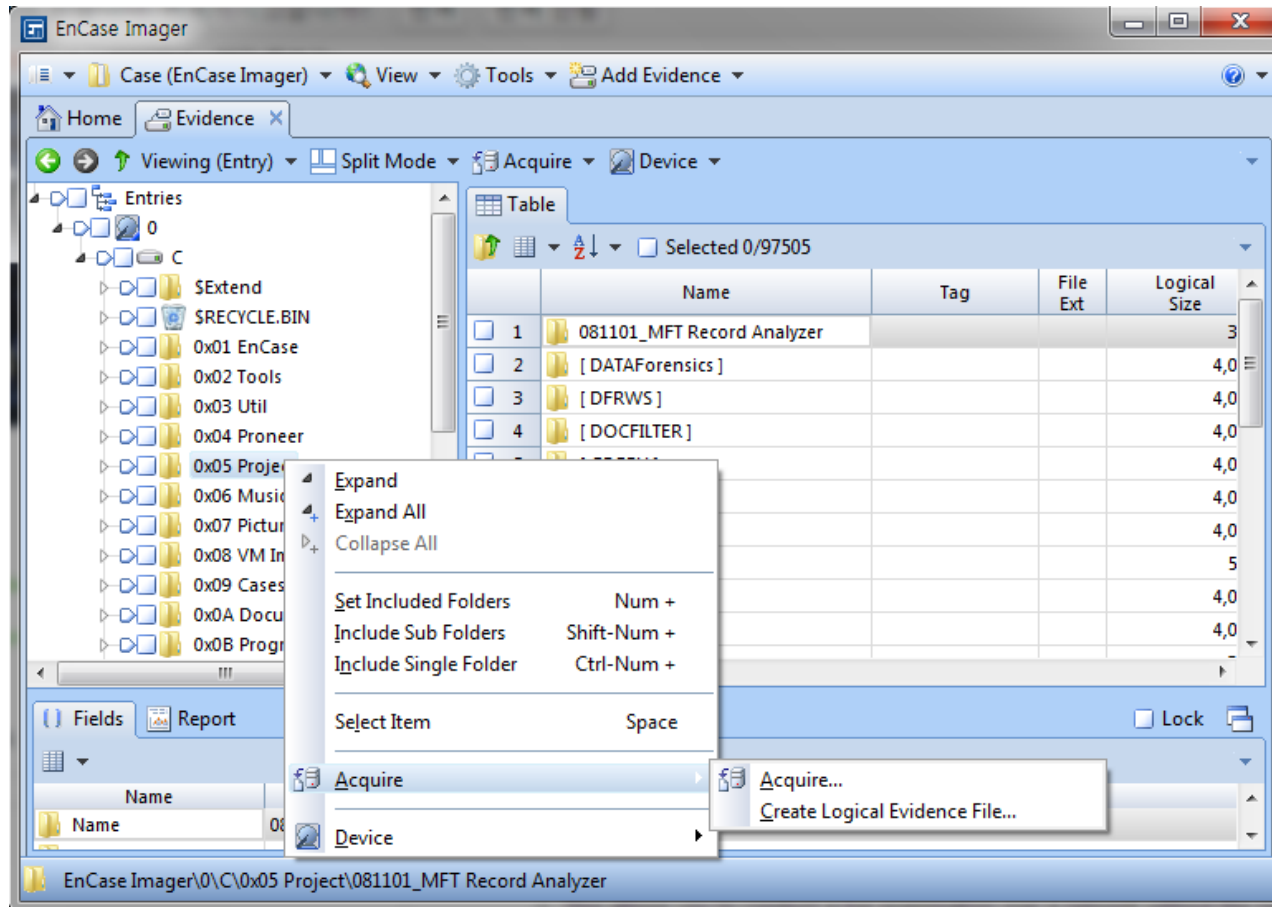




Guidance Software (guidancesoftware.com/) (cont'd)

- EnCase Forensic v7.06 Resources

- EnCase Forensic Imager





Guidance Software (guidancesoftware.com/)

▪ EnCase Forensic v7.06 Resources

• Mac 지원 확장

- ✓ HFS+ 파일시스템 압축/비압축 파일 표시
- ✓ Finder 정보와 확장 파일 속성 지원
- ✓ 보안 ACL 표시
- ✓ OS X Trash 항목 지원 향상
- ✓ 맥 (OS X 10.8) 설치 지원
- ✓ 맥 논리적 볼륨 지원

• 안드로이드 수집 모듈 향상

• 추가적인 암호화 지원

• 윈도우 8, 서버 2012 지원 향상

- ✓ 윈도우 8, 서버 2012 서블릿
- ✓ 윈도우 8 아티팩트 : 레지스트리 파싱, 시스템 정보 파싱
- ✓ 윈도우 8 비트락커
- ✓ 윈도우 7 점프 목록 (Automatic) 파싱
- ✓ 윈도우 7 thumbs.db 파싱

• 태블릿 지원

- ✓ Google Nexus 7, Acer Iconia Tab A500, Samsung Galaxy Tab 2, Kindle Fire HD



Guidance Software (store.encase.com/)

▪ EnCase App Central

[View All Apps](#)

Search Apps:

Search

REFINE YOUR RESULTS

[Start a New Search](#)
Narrow search results for ""

Categories

☐ Artifact (13)

☐ Utility (13)

☐ Windows Artifacts (8)

☐ Mac OSX Artifacts (6)

☐ Reporting (4)

[show more](#)

Rating
No Rating (7)

[Search Again](#)

Viewing 1 to 10 of 45 apps [1](#) [2](#) [3](#) [4](#) [5](#) [Next](#)

Apps per page [10](#) Sort by [Relevance](#)

OfficeRecovery 2013 Ultimate

Repair and examine the contents of corrupted files in collected evidence. Word Excel digital images and dozens of other formats are supported.

Version: 1.0.0
Developer: Recoveronix Software, LLC
Works with: 7.05

[Learn More »](#)
[View Discussion Board](#)

[Add to Cart](#)
\$748.00

OfficeRecovery 2013 Ultimate - Trial Version

Repair and examine the contents of corrupted files in collected evidence. Word Excel digital images and dozens of other formats are supported.

Version: 1.0.0
Developer: Recoveronix Software, LLC
Works with: 7.05

[Learn More »](#)
[View Discussion Board](#)

[Add to Cart](#)
\$0.00

SQLiteQuery

Allows SQL querying of all SQLite databases from within Encase.

Version: 1.0.0
Developer: Doug Collins
Works with: 7.05

[Learn More »](#)
[View Discussion Board](#)

[Add to Cart](#)
\$0.00

forensicsight.org

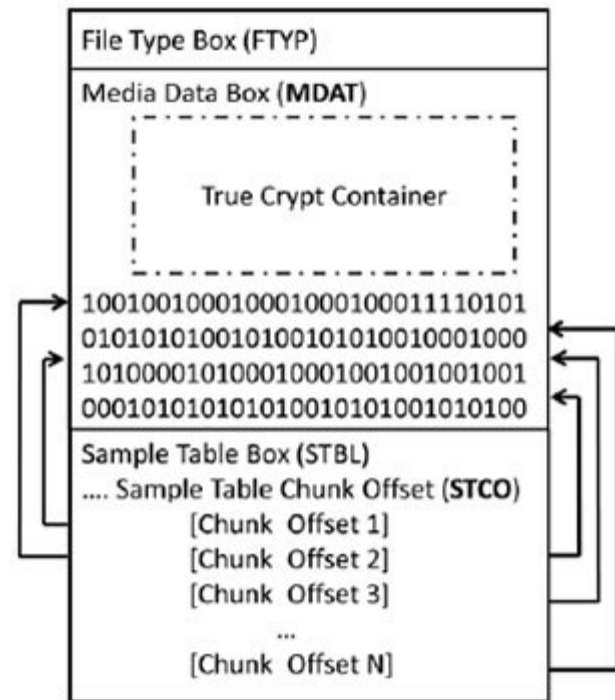
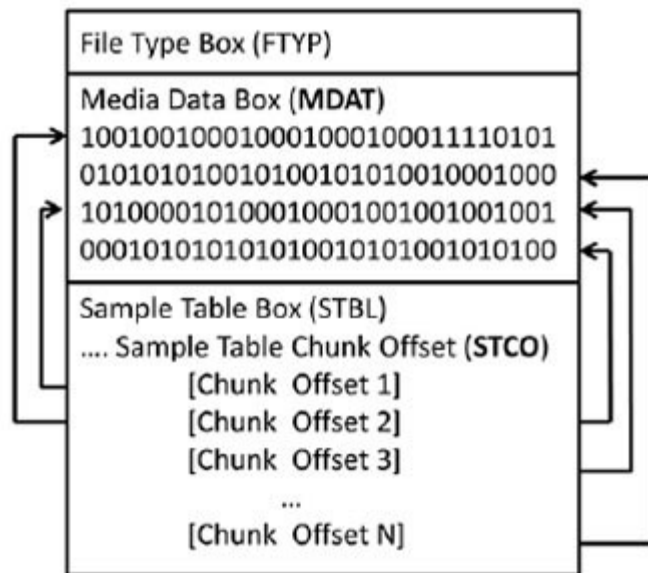
Page 19



DFINews (dfinews.com/)

▪ The Future of Steganography

- MP4, QuickTime 멀티미디어 파일에 TrueCrypt 컨테이너 삽입
- **Steganography** – **tcsteg.py** (<http://keyj.emphy.de/files/tcsteg.py>)
- **Steganalysis** - Python Script to Detect Hidden Data (<http://www.dfinews.com/article/python-script-detect-hidden-data>)





Windows Incident Response (windowsir.blogspot.kr/)

▪ Indicator of Program Execution

- Application Prefetch File
- Shortcut/LNK file, Jump List
- Browser History
- Hibernation File
- Windows Event Logs
- Registry
- MSIs
- RecentDocs
- AppCompatCache
- MUICache
- *Tracing
- *DirectDraw
- SysInternals
- AppCompatFlags
- UserAssist
- RunMRU
- AutoStart Locations
- LANDesk
- Windows Services



The Hacker Factor Blog (hackerfactor.com/) (cont'd)

▪ HIGH WATERMARK

- Basically Watermark

- ✓ 그림 위에 반투명 이미지나 로고를 덮어씀
- ✓ 워터마크 제거를 위해 이미지를 자르거나 더 큰 로고로 덮어씀





The Hacker Factor Blog (hackerfactor.com/) (cont'd)

- HIGH WATERMARK

- Unpaid Image's Watermark

- ✓ 비용을 지불하지 않으면 워터마킹된 이미지/영상 제공



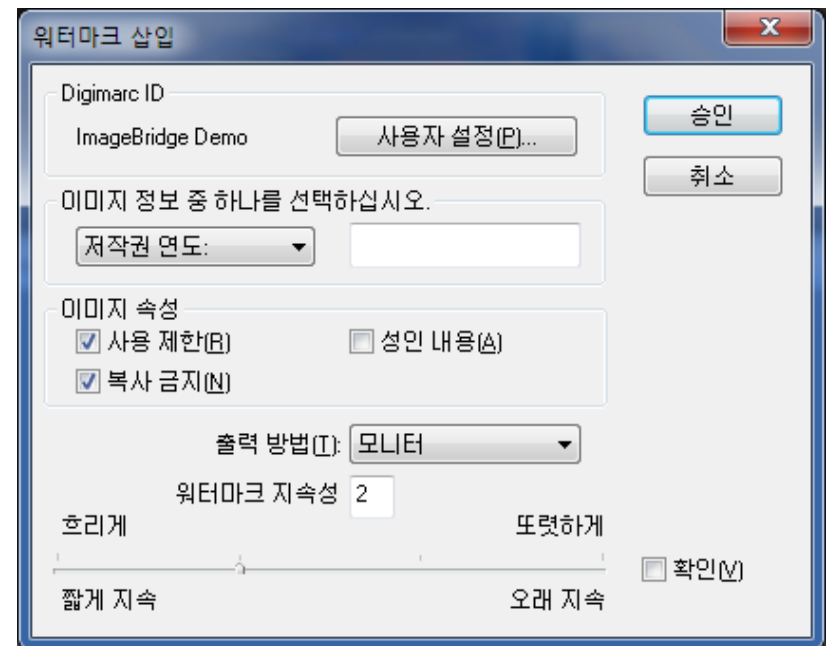
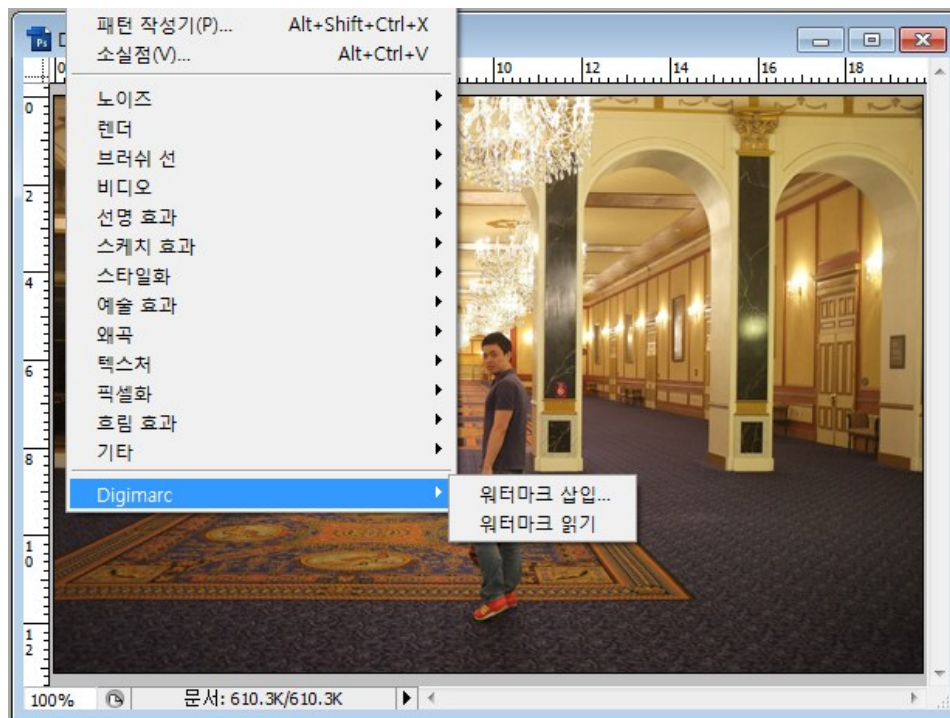


The Hacker Factor Blog (hackerfactor.com/) (cont'd)

■ HIGH WATERMARK

• Secret Handshakes

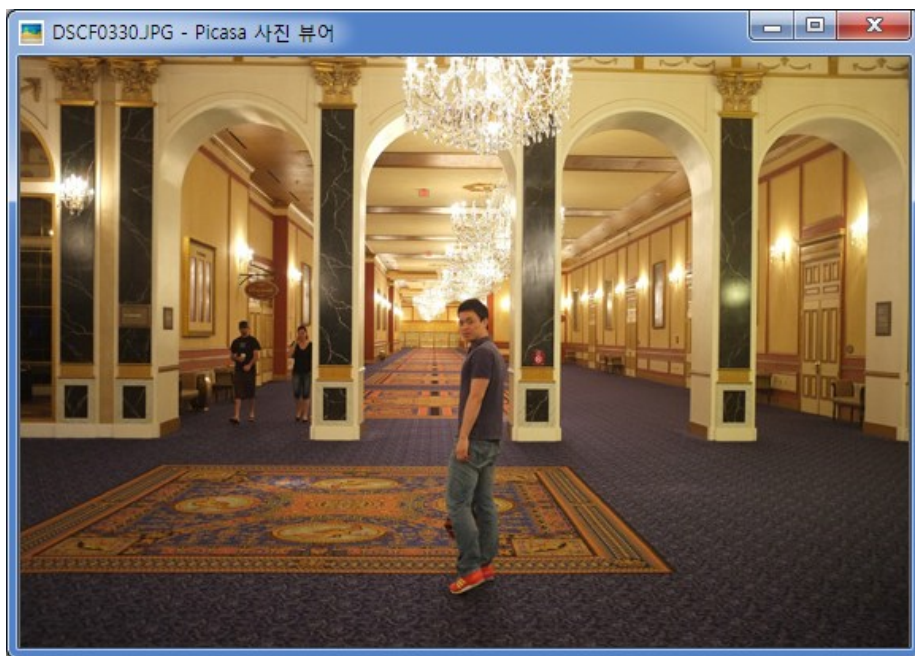
- ✓ 미세한 변경을 통해 인간의 눈은 인식할 수 없도록 만들 → 컴퓨터로 인식 가능
- ✓ Photoshop → Filter → Digimarc



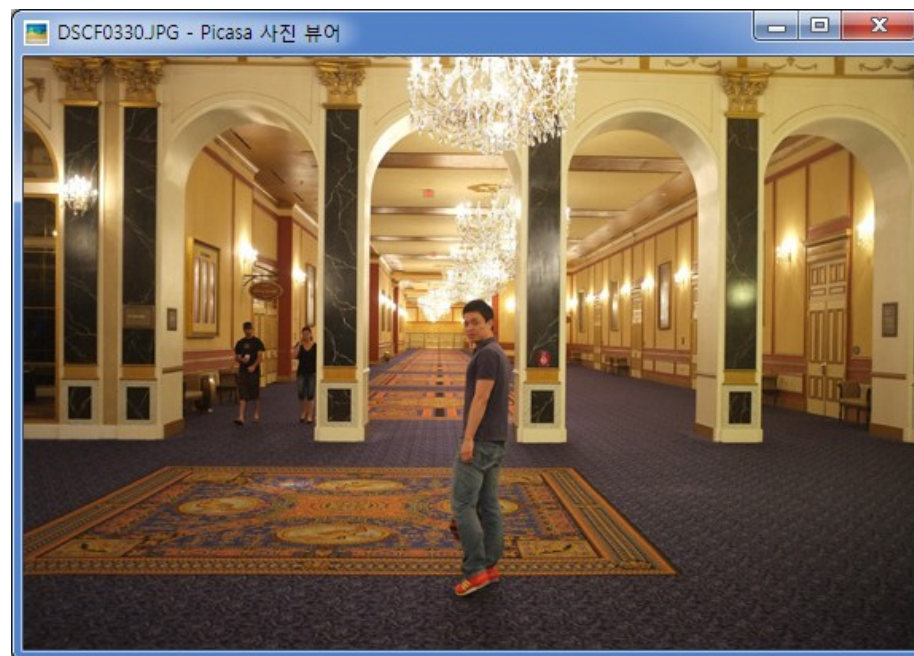


The Hacker Factor Blog (hackerfactor.com/) (cont'd)

- HIGH WATERMARK
 - Secret Handshakes



Before



After



The Hacker Factor Blog (hackerfactor.com/) (cont'd)

▪ HIGH WATERMARK

- Secret Handshakes

- ✓ 워터마크는 종종 추적을 위해 사용

- 월드오브워크래프트(WOW) 스크린샷에도 워터마크 삽입
 - 날짜, 시간, 서버 영역 정보, 사용자의 화면 이름

- ✓ 이런 방법은 수정에 매우 민감 → 크기 조절, 회전, 대비 등

- ✓ 페이스북과 같은 온라인 리소스에 사진을 업로드하면 대부분 워터마크가 제거됨



The Hacker Factor Blog (hackerfactor.com/) (cont'd)

■ HIGH WATERMARK

• Snide Comments

- ✓ 파일의 메타데이터를 이용한 워터마크, 몇몇 워터마크는 인코딩을 이용
- ✓ 이베이의 상품 사진



\$T2eC16NHJGAE9nm3oxHpBRARUK0N4w~~0.57.JPG																0123456789ABCDEF													
0000h:	FF	D8	FF	E0	00	10	4A	46	49	46	00	01	01	01	00	48	00	00	00	00	00	00	00	00	00	00	00	00	00
0010h:	00	48	00	00	FF	FE	00	FB	50	72	6F	63	65	73	73	65	00	00	00	00	00	00	00	00	00	00	00	00	00
0020h:	64	20	42	79	20	65	42	61	79	20	77	69	74	68	20	49	00	00	00	00	00	00	00	00	00	00	00	00	00
0030h:	6D	61	67	65	4D	61	67	69	63	6B	2C	20	52	31	2E	31	00	00	00	00	00	00	00	00	00	00	00	00	00
0040h:	2E	31	2E	7C	7C	42	32	7C	7C	54	30	4A	4B	58	30	6C	00	00	00	00	00	00	00	00	00	00	00	00	00
0050h:	45	50	54	52	6D	4E	6A	63	34	4D	6D	51	33	59	54	4D	00	00	00	00	00	00	00	00	00	00	00	00	00
0060h:	30	4E	7A	49	30	4E	6A	41	77	4E	47	59	32	4E	7A	6C	00	00	00	00	00	00	00	00	00	00	00	00	00
0070h:	69	4E	32	45	7A	4D	54	46	6C	4F	54	41	31	4D	54	41	00	00	00	00	00	00	00	00	00	00	00	00	00
0080h:	78	4D	54	55	79	4E	47	51	77	5A	47	55	7A	66	48	78	00	00	00	00	00	00	00	00	00	00	00	00	00
0090h:	54	52	55	78	4D	52	56	4A	66	54	6B	46	4E	52	54	31	00	00	00	00	00	00	00	00	00	00	00	00	00
00A0h:	74	62	33	4E	6C	61	58	4E	73	5A	58	6C	66	59	32	39	00	00	00	00	00	00	00	00	00	00	00	00	00
00B0h:	73	62	47	56	6A	64	47	6C	69	62	47	56	7A	66	48	78	00	00	00	00	00	00	00	00	00	00	00	00	00
00C0h:	50	55	6B	6C	48	53	55	35	42	54	46	39	46	51	6B	46	00	00	00	00	00	00	00	00	00	00	00	00	00
00D0h:	5A	58	31	46	56	51	55	78	4A	56	46	6C	66	55	30	4E	00	00	00	00	00	00	00	00	00	00	00	00	00
00E0h:	50	55	6B	55	39	4E	48	78	38	51	31	4A	46	51	56	52	00	00	00	00	00	00	00	00	00	00	00	00	00
00F0h:	4A	54	30	35	66	52	45	46	55	52	54	30	7A	4C	7A	45	00	00	00	00	00	00	00	00	00	00	00	00	00
0100h:	30	4C	7A	45	7A	49	44	45	79	4F	6A	55	35	49	46	42	00	00	00	00	00	00	00	00	00	00	00	00	00
0110h:	4E	FF	DB	00	43	00	01	01	01	01	01	01	01	01	01	01	00	00	00	00	00	00	00	00	00	00	00	00	00

Template Results - JPG Template, bt			
Name	Value	Start	Size
struct JPGFILE jpgfile		0h	697E3h
enum M_ID SOIMarker	M_SOI (FFD8h)	0h	2h
struct APP0 app0		2h	12h
struct COMMENT comment	Processed By eBay with ImageMagi...	14h	FDh
struct DQT dqt[0]		111h	45h

The Hacker Factor Blog (hackerfactor.com/)

■ HIGH WATERMARK

• Snide Comments

Processed By eBay with ImageMagick, R1.1.1.||B2||
T0JKX0IEPTRmNjc4MmQ3YTM0NzI0NjAwNGY2NzIiN2EzMtFIOTA1MTAxMTUyN
GQwZGUzfHxTRUxMRVJftkFNRT1tb3NlaXNsZXIfY29sbGVjdGlibGVzfHxPUkIHsU5
BTF9FQkFZX1FVQUxJVfIfU0NPUkU9NHx8Q1JFQVRJT05fREFURTozLzE0LzEzIDEy
OjU5IFBN

✓ Decode Base64

- Processed By eBay
- Created with ImageMagick
- **OBJ_ID**=4f6782d7a347246004f679b7a311e9051011524d0de3||

SELLER_NAME=moseisley_collectibles||ORIGINAL_EBAY_QUALITY_SCORE=4||

CREATION_DATE=3/14/13 12:59 PM

#2TeC16NHJGAE9nm3oxHpbRARUk0N4w~~0_57.JPG																																			
	0	1	2	3	4	5	6	7	8	9	A	B	C	D	E	F	0123456789ABCDEF																		
0000h:	FF	00	FF	00	00	10	4A	4E	49	46	00	01	01	00	48		00	4A	JFIF....H																
0010h:	00	48	00	00	FF	00	00	FB	50	72	6F	63	65	73	73	65		00	H...pPProcess																
0020h:	64	20	42	79	20	65	42	61	79	20	77	69	74	68	20	49		00	d By eBay with I																
0030h:	60	61	67	65	40	61	67	69	63	68	20	20	51	2E	31			00	mageMagick, R1.1																
0040h:	2E	31	62	7C	7C	42	32	7C	7C	54	30	40	4B	58	30	6C		00	..1 B2 T0XK00																
0050h:	45	50	54	52	6D	4E	6A	63	34	4D	6D	51	33	59	54			00	EPTRmJc=4Mm3VT																
0060h:	30	4E	74	49	30	4E	6A	41	77	4E	47	59	32	4E	7A	6C		00	OnZiONJwAMNGY2																
0070h:	69	4E	32	45	7A	54	54	46	6C	4F	54	41	31	4D	54	41		00	LN2E2MTFOALTAH																
0080h:	78	4D	54	55	79	4E	47	51	7F	54	47	55	7A	66	68	78		00	ctMtoYGNGwZGZu																
0090h:	54	52	55	58	4D	52	56	4A	66	54	6B	4E	52	54	31			00	TRUxMRVJfTKFNRT																
00A0h:	74	62	33	4E	6C	61	58	4E	73	5A	58	6C	66	59	32	39		00	cb3N1aXnS2X1Ft																
00B0h:	73	62	47	56	64	47	6C	69	62	47	56	7A	66	68	78			00	sbGvJdG1lBgVY29																
00C0h:	50	55	6B	4E	58	55	35	42	54	36	49	36	51	5B	4E			00	FUK1HSUSBT9FQ0K																
00D0h:	5A	58	31	46	56	51	55	78	4A	56	46	6C	66	55	50	4E		00	ZK1FVQJXJVF1J0Q																
00E0h:	50	55	6B	59	4E	48	78	38	31	51	4A	4E	51	56	52			00	FUK9Y9NHX8Q1JFQ																
00F0h:	4A	54	30	35	66	52	45	46	55	52	54	30	7A	4C	7A	45		00	JT05fRETRFQZVVR																
0100h:	30	4C	7A	45	4A	49	44	45	79	4F	6A	55	35	49	4E	42		00	0LzEzIDeYv0U5IFB																
0110h:	4E	FF	D8	00	45	93	01	01	01	01	01	01	01	01	01	01		00	g0G.....																
Template Results - JPGTemplate.bt																																			
Name																	Value																	Start	Size
struct JPGFILE jpgfile																																		0h	697E3h
enum M_ID SOIMarker																	M_SOI (FFD8h)																	0h	2h
struct APP0 app0																																		2h	12h
struct COMMENT comment																	Processed By eBay with ImageMagi...																	14h	FDh
struct DQT dqt[0]																																		111h	45h



Computer Forensics Tool Testing (cftt.nist.gov/)

- **Computer Forensics Tool Catalog** (http://www.cftt.nist.gov/tool_catalog/)

[Home](#) | [Tool Search](#) | [Forensic Tool Taxonomy](#) | [Vendors](#) | [Contacts](#)

Forensic Tool Functionalities

Deleted File Recovery

Disk Imaging

Email Parsing

Forensics Boot Environment

Hardware Write Block

Hash Analysis

Media Sanitization/Drive Re-use

Memory Capture and Analysis

Mobile Device Acquisition and Analysis

P2P Analysis

Remote Capabilities / Remote Forensics

Software Write Block

Steganalysis

String Search

Windows Registry Analysis

Home > Tool Search

Search for forensic tools by functionality

☐ find all Deleted File Recovery tools ☒ refine by search parameters



Forensic Functionality:	Deleted File Recovery		
Technical Parameters:	Tool host OS / runtime environment:	Supported file systems:	Overwritten file identification:
	<div>any</div> <div>Windows</div> <div>Linux</div> <div>Mac</div>	<div>any</div> <div>FAT12</div> <div>FAT16</div> <div>FAT32</div>	<div>any</div> <div>supports identifying overwritten files</div> <div>identifying overwritten files unsupported</div>

Search



WRITE BLOCKED (writeblocked.org/)


- **DFIROnline** (youtube channel)

**Mike Wilkinson**  **Subscribe** 175


175 subscribers 3,442 video views


Browse videos

Uploads **Feed** Comments View ▾


**Mike Wilkinson** uploaded and posted 6 days ago


David Cowen's March DFIROnline is now posted, time to learn about using \$MFT, \$logfile and \$USNJRNL to track all (yes all!) file system activity.

**DFIROnline - NTFS Triforce or anti anti forensics, David Cowen & Matt Seyer**
52 views
It still amazes me that after all this time there is still more to learn about NTFS. Over the past year or so David has been working on a tool to exploit the \$LOGFILE and \$USNJRNL on NTFS. These can

**Mike Wilkinson** uploaded and posted 6 days ago

At long last the recording of Dave Kleiman's presentation on windows log file analysis in depth from February has been posted.

**DFIROnline - Windows Log File Analysis in depth, Dave Kleiman**
41 views
Back by popular demand (and this time not from hospital) Dave took us through the various log files on Microsoft Windows systems (you did know there was more than just the event logs didn't you?)

**Mike Wilkinson**
Recordings of DFIROnline meetups. A monthly online meeting of digital forensic professionals. If you found this useful you can see the schedule of coming events at www.writeblocked.org/dfironline.html

by Mike Wilkinson ▾

Date Joined Oct 15, 2012

Country United States



4:cast (forensic4cast.com/)

▪ 4:mag Issue #1

MORE LEADS. LESS TIME.

Extract, View & Act with Cellebrite UFED Series

Often, it's not so much what your subject knows – it's who they know. With **UFED Link Analysis**, put the data you extract to work:

- **Transform** isolated data into links between subjects and other entities
- **Visualize** the connection strength between individuals and **identify** key witnesses, victims and even suspects
- **Pinpoint** regular and irregular communication and location patterns
- **Drill down** to specific events in a subject's life
- **Plan** operations, interviews and directions for your investigation

UFED Series applications bring you data and timeline analytics at any point in your investigation.

Learn more at www.ufedseries.com

1.888.853.0030
forensicsales@cellebriteusa.com
f www.facebook.com/CellebriteUFED
t @CellebriteUSA

cellebrite
delivering mobile expertise

UFED Series

To see UFED Link Analysis in action, scan the QR code below

4:HOME
contents

- 4 events
- 5 editorial
- 6 a call to action
- 10 device and application data from ios devices
- 13 taking a byte out of apple computers
- 16 win - forensic contest
- 18 starting out and getting ahead
- 23 forensic 4cast awards 2013
- 25 pro-file
- 28 hard drive secrets revealed
- 34 4:ward

Contents Pictures Courtesy of <http://www.flickr.com/photos/kasir512/7495485695/>
<http://www.flickr.com/photos/2014058883/>
Cover Photo Courtesy of <http://www.flickr.com/photos/ianagil/89623315/>

4:mag - issue #1 Q2 2013

3 of 36



Others (cont'd)

▪ Journey Into Incident Response

- Houston We've Had a Problem – Wow64
- Tracking Down Persistence Mechanisms

▪ Digital Forensics Stream

- Windows 8 : Tracking Opened Photos

▪ ForensicKB

- EnScript to parse setupapi.dev.log
- EnCase EnScript to calculate entropy of selected file(s)
- File Entropy explained
- Crafting good keywords in EnCase and using conditions to refine results



Others (cont'd)

- **Yogesh Khatri's forensic blog**
 - Decrypting Apple FileVault Full Volume Encryption

- **Sketchymoose's blog**
 - Crest Con Update- With Slides! ➔ Memory Forensics (slide)

- **jessekornblum**
 - No More TrueCrypt Boot Passphrases

- **Mobile & Technology eDiscovery**
 - (U)SIM Examination (Physical) Pt1



Others (cont'd)

- **DFINews**
 - Memory Analysis and the Ongoing Battle Against Malware
- **LoveMyTool**
 - Open Source Forensics for Windows, MacOS, and Linux (DFF, Digital Forensics Framework)
- **Forensics from the sausage factory**
 - Location Data within JPGs
- **Lab Course: Communication And Communicating Devices**
 - Code Protection in Android
- **ERIC ROMANG BLOG**
 - OSX/Pint-sized Backdoor Additional Details



dForensics Tools

- **Magnet Forensics**

- Dropbox Decryptor

- **Belkasoft**

- Live RAM Capturer

- **Forensic blog**

- ADEL (Android Data Extractor Lite)

- **NirSoft**

- NetworkInterfacesView
- JumpListsView



dForensics Tools

- **KirySoft**

- WSCC (Windows System Control Center), Sysinternals & Nirsoft's Utility Install, Update, Execute

- **fawproject**

- FAW (Forensics Acquisition of Websites)

- **CERT.AT**

- ProcDOT, Visualization Tools using Procmon log and PCAP log (windump, tcpdump)

