

침해 유입 아티팩트



JK Kim

@pr0neer

forensic-proof.com

proneer@gmail.com

1. 웹 아티팩트
2. 외부저장장치 아티팩트
3. 이메일 아티팩트
4. 방화벽 로그
5. 이벤트 로그

웹 아티팩트

- 웹 브라우저
- 액티브 X
- 자바 애플릿

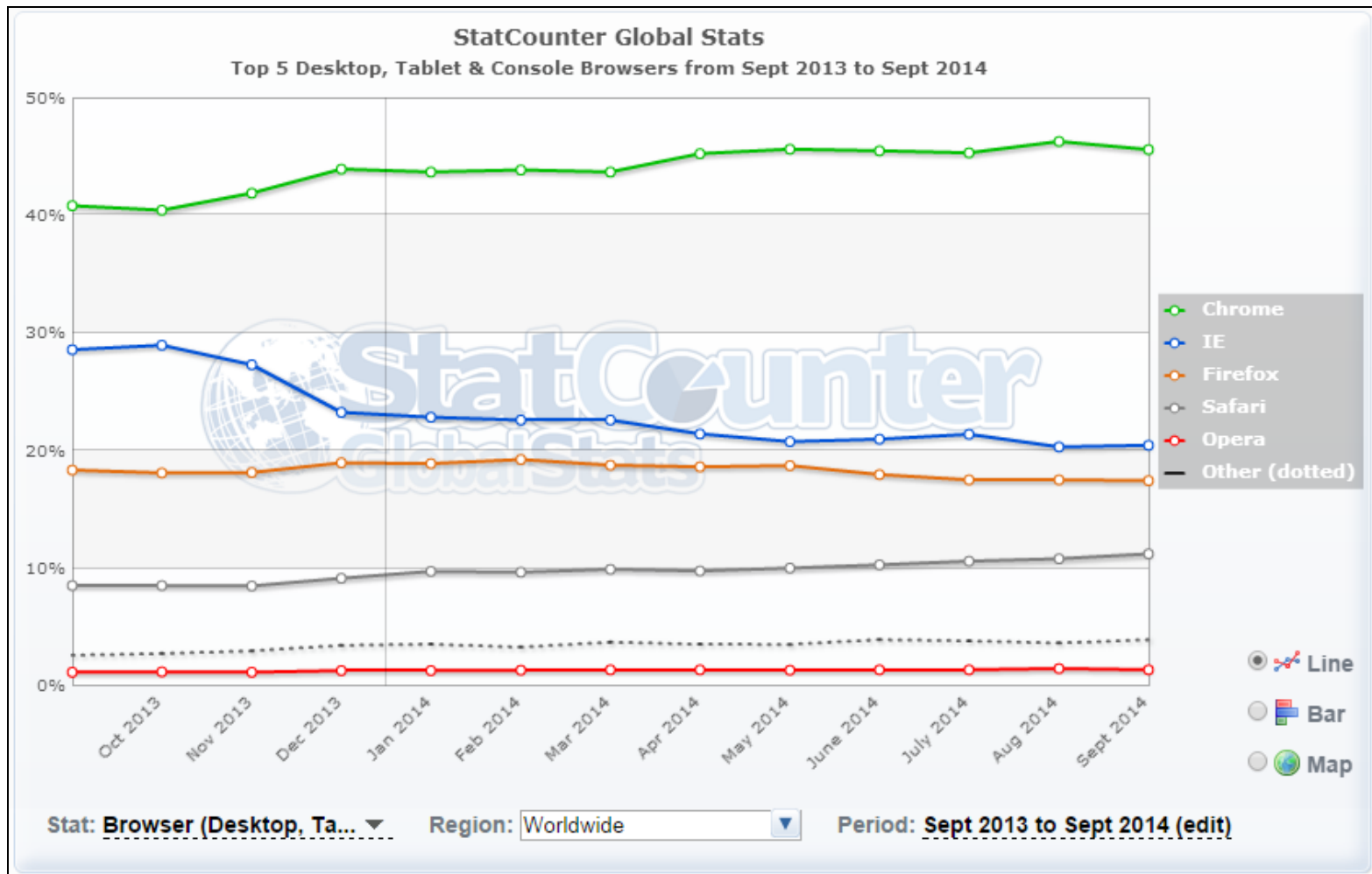
웹 아티팩트

■ 웹 브라우저

- 대부분의 웹 아티팩트는 웹 브라우저 사용 흔적
- 웹 애플리케이션(서버)과 웹 브라우저(클라이언트)가 통신하면서 생성되는 흔적



- 웹 브라우저 점유율
 - StatCounter, 2013.09 ~ 2014.09 까지 통계



■ 웹 브라우저 포렌식

- 웹 브라우저 사용 흔적을 디지털 포렌식 분석에 활용하는 기법

• 필요성

- ✓ 현대인의 생활에서 웹 브라우저는 뗄래야 뗄 수 없는 필수 프로그램 → PC, 스마트폰 등
- ✓ 웹과 관련된 사건이라면 웹 브라우저 흔적이 분석에 매우 중요
- ✓ 사안에 따라 사건의 동기, 목적, 수단, 방법, 사후 처리 등 많은 정보 획득 가능

• 주로 직접 증거보다는 정황증거로 활용

- ✓ 증거재판주의 – “사실의 인정은 증거에 의한다”
- ✓ 직접 증거 – 증명의 대상이 되는 사실의 증명에 직접 이용되는 증거
- ✓ 정황 또는 간접 증거 – 간접 사실을 증명하는 증거

- 웹 브라우저 아티팩트

- 웹 브라우저 캐시
- 웹 브라우저 히스토리
- 웹 브라우저 쿠키
- 웹 브라우저 다운로드 목록
- 웹 브라우저 북마크 정보
- 웹 브라우저 시작 페이지/화면 구성
- 웹 브라우저 세션(탭) 저장 정보
- 웹 브라우저 자동완성(폼 데이터, ID, 비밀번호) 정보
- 웹 브라우저 파비콘 정보
- 그 밖에 다양한 아티팩트

웹 아티팩트

■ 웹 브라우저 아티팩트

• 웹 브라우저 캐시

✓ 웹 사이트 방문 시, 사이트로부터 자동으로 다운받은 콘텐츠

✓ 콘텐츠 캐시를 통해 재 방문 시 로딩 속도 향상

✓ 캐시 데이터 (다운받은 데이터)

- 이미지 파일, 텍스트 파일, 아이콘, HTML 파일, XML 파일, 스크립트 등

✓ 캐시 인덱스 정보

- 캐시 데이터 위치, 다운로드 URL, 다운로드 시간, 다운로드 데이터 크기 등

이름	인터넷 주소	유형	크기	만료 날짜	마지막으로 액세스한 날짜	마지막으로 수정한 날짜
loading-large_V192238965_.gif	http://g-ecx.images-amazon.com/ima...	GIF 이미지	7KB	2033-03-03 오후 12:06	2013-07-19 오후 7:08	2010-06-03 오전 10:06
sprite-site-wide-3_V375430972_.png	http://g-ecx.images-amazon.com/ima...	PNG 이미지	17KB	2033-03-04 오전 4:57	2013-07-19 오후 5:10	2013-02-07 오전 6:25
517akZvN1QL_SL500_Pisitb-sticker-arrow-...	http://ecx.images-amazon.com/image...	JPEG 이미지	5KB	2033-03-04 오전 5:28	2013-07-19 오후 5:10	2013-01-19 오전 5:29
sprite-cbox_V388671922_.png	http://g-ecx.images-amazon.com/ima...	PNG 이미지	3KB	2033-03-04 오전 6:25	2013-07-19 오후 5:10	2012-09-19 오전 8:01
viewcartcheckoutmedium_V195191215_.gif	http://g-ecx.images-amazon.com/ima...	GIF 이미지	3KB	2033-03-04 오전 11:20	2013-07-19 오후 5:10	2010-11-03 오전 12:58
nav-pop-v-v2_V137157005_.png	http://g-ecx.images-amazon.com/ima...	PNG 이미지	2KB	2033-03-04 오후 7:27	2013-07-19 오후 7:08	2012-03-13 오전 8:57
61b-kle1AsL_SL135_.png	http://ecx.images-amazon.com/image...	JPEG 이미지	9KB	2033-03-04 오후 11:01	2013-07-19 오후 7:08	2012-07-25 오후 1:47
navAmazonLogoFooter_V169459313_.gif	http://g-ecx.images-amazon.com/ima...	GIF 이미지	2KB	2033-03-05 오전 1:03	2013-07-19 오후 7:08	2011-03-01 오전 3:36
amznlike_sprite_02_V196113939_.gif	http://g-ecx.images-amazon.com/ima...	GIF 이미지	3KB	2033-03-05 오전 1:49	2013-07-19 오후 5:10	2010-10-23 오전 8:53
51-9l4%2BsVL_SL500_Pisitb-sticker-arrow...	http://ecx.images-amazon.com/image...	JPEG 이미지	5KB	2033-03-05 오전 8:56	2013-07-19 오후 5:10	2012-08-11 오후 9:03
41AcZPYZ68L_SL135_.jpg	http://ecx.images-amazon.com/image...	JPEG 이미지	4KB	2033-03-07 오전 2:43	2013-07-19 오후 7:08	2013-03-08 오후 11:13

웹 아티팩트

■ 웹 브라우저 아티팩트

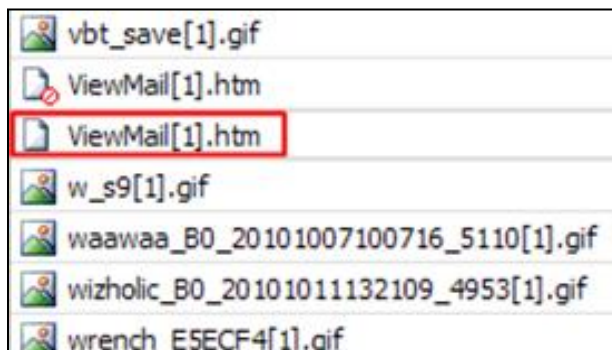
• 웹 브라우저 캐시 ➔ 분석 방법

✓ 다운로드 URL + 다운로드 시간 ➔ 특정 시간에 해당 사이트 이력

✓ 다운로드 URL + 키워드 검색 ➔ 중요 사이트 방문 이력 확인

 mail_view_write.js?t=20130626104800 http://mail3.nate.com/js/mail_view_write.js?t=20130626104800

✓ HTML 캐시 파일 - 웹 메일 내용 확인



웹 아티팩트

■ 웹 브라우저 아티팩트

• 웹 브라우저 캐시 → 분석 방법

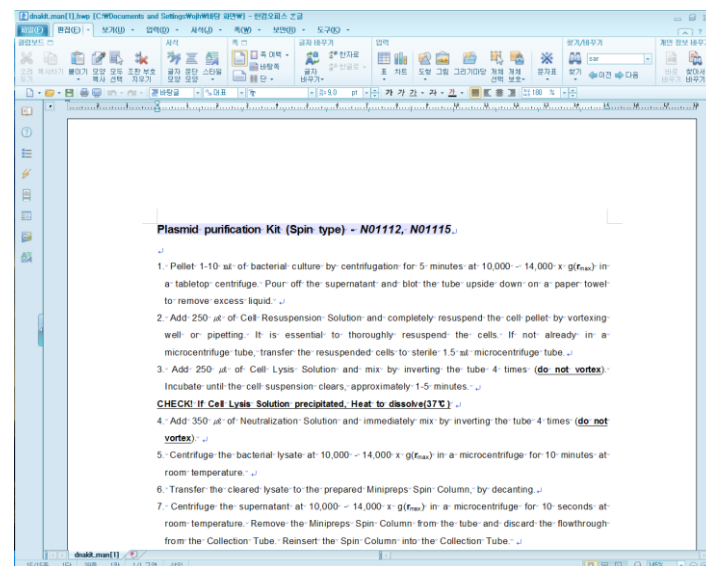
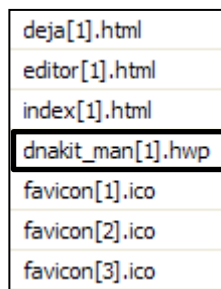
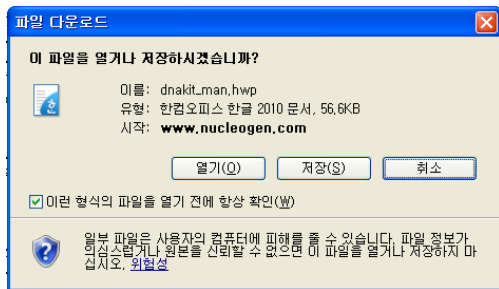
✓ 웹 브라우저에서 문서 열람 시 열람 파일 그대로 저장 – PDF, HWP 등

[HWP] [Plasmid purification Kit \(Spin type\) - N01112, N01115](#)

파일 형식: HWP/Hancom Hanword - [HTML 버전](#)

Plasmid purification Kit (Spin type) - N01112, N01115. 1. Pellet 1-10 ml of bacterial culture by centrifugation for 5 minutes at 10000 - 14000 x g(rmax) in ...

www.nucleogen.com/misc/dnakit_man.hwp



웹 아티팩트

■ 웹 브라우저 아티팩트

• 웹 브라우저 히스토리

✓ 사용자가 방문한 웹 사이트 접속 정보 저장

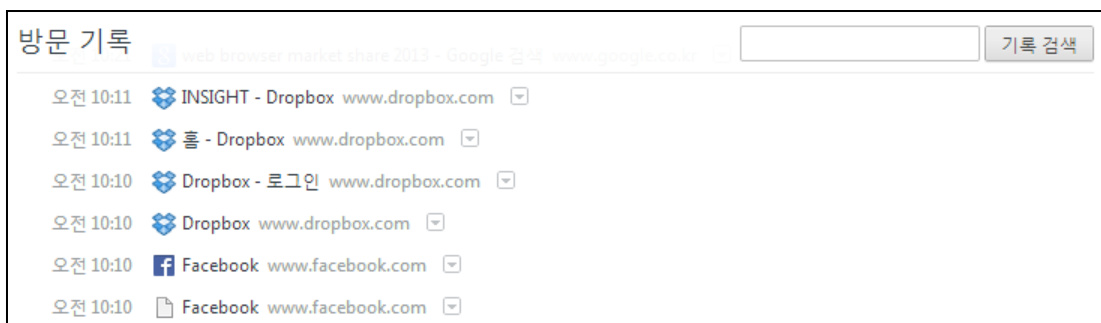
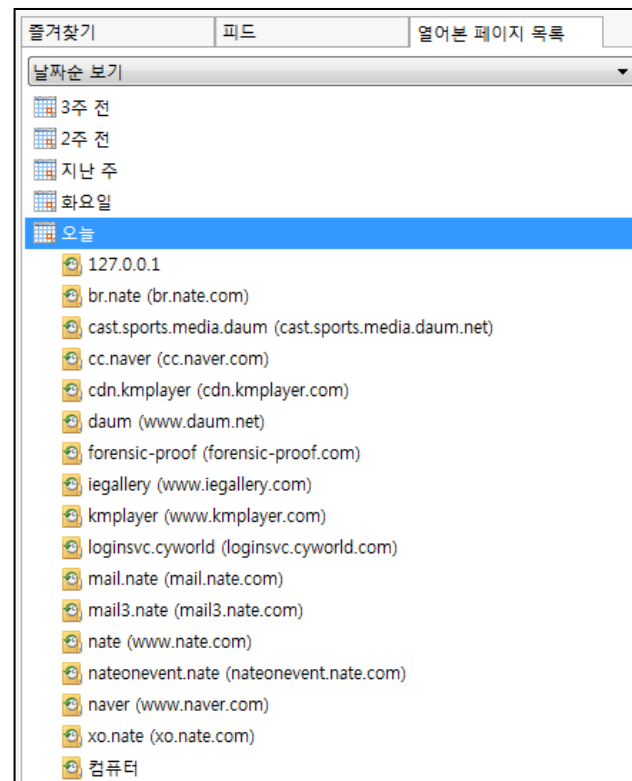
✓ 월별, 일별 방문 기록을 분류해서 저장

✓ 히스토리 정보

- 방문 사이트 URL, 방문 시간, 방문 횟수, 사이트 제목 등

✓ 저장 형식

- 직접 접근 – URL 입력창에 직접 주소 입력
- 간접 접근 – URL 링크를 통해서 접근



■ 웹 브라우저 아티팩트

• 웹 브라우저 히스토리 ➔ 분석 방법

- ✓ 방문 사이트 URL + 방문 시간 ➔ 해당 사이트 방문 이력
- ✓ 방문 사이트 URL + 방문 횟수 + 키워드 검색 ➔ 사용자 행위 분석

✓ GET 방식으로 전달된 인자 값 분석

- 검색어 추출 `https://www.google.co.kr/search?q=forensic-proof`
- 아이디, 패스워드 추출

✓ 검색어 URL 인코딩

- "포렌식" 검색 (UTF-8) ➔ 구글, 다음, 네이버, 네이트, 야후, 페이스북, ZUM, BING, BAIDU, ...
http://search.daum.net/search?w=tot&DA=YZRR&t_nil_searchbox=btn&sug=&sq=&o=&q=%ED%8F%AC%EB%A0%8C%EC%8B%9D
- "포렌식" 검색 (EUC-KR) ➔ 쥬니어네이버, ...
http://jrsearch.naver.com/jrsearch.naver?ie=&sm=tab_hy&where=nexearch&query=%C6%F7%B7%BB%BD%C4

■ 웹 브라우저 아티팩트

• 웹 브라우저 쿠키







✓ 웹 사이트 방문 시 자동으로 사용자 저장장치에 저장되는 텍스트 데이터

✓ 사용자 기반 서비스 제공

- 자동 로그인 기능
- 쇼핑몰 열람한 물건, 장바구니 물건
- 웹 하드 찜 해놓은 자료, 다운받은 자료

✓ 쿠키 정보

- 호스트 사이트, 경로, 수정 시간, 만료 시간, 이름, 값 등

이름	인터넷 주소	유형	크기	만료 날짜
 cookie:forensic32@plus.google.com/	Cookie:forensic32@plus.google.com/	텍스트 문서	1KB	2013-07-14 오후 2:23
 cookie:forensic32@pubmatic.com/	Cookie:forensic32@pubmatic.com/	텍스트 문서	1KB	2015-07-19 오후 5:10
 cookie:forensic32@q828.tistory.com/	Cookie:forensic32@q828.tistory.com/	텍스트 문서	1KB	2015-03-20 오후 7:58
 cookie:forensic32@realmedia.co.kr/	Cookie:forensic32@realmedia.co.kr/	텍스트 문서	1KB	2021-01-01 오전 9:00
 cookie:forensic32@rubiconproject.com/	Cookie:forensic32@rubiconproject.com/	텍스트 문서	1KB	2021-07-17 오후 5:10
 cookie:forensic32@sanddroid.xjtu.edu....	Cookie:forensic32@sanddroid.xjtu.edu.cn/	텍스트 문서	1KB	2015-07-04 오후 5:27

■ 웹 브라우저 아티팩트

• 웹 브라우저 쿠키 → 분석 방법

- ✓ 호스트, 경로 → 접속한 사이트, 사용한 서비스
- ✓ 수정 시간 → 마지막 접속 시간
- ✓ 이름, 값 → 로그인 아이디 저장 옵션 활성화 시, 로그인 아이디 획득 가능
- ✓ 구글 애널리틱스 정보

- <http://www.dfinews.com/articles/2012/02/google-analytics-cookies-and-forensic-implications>
- http://az4n6.blogspot.kr/2012/11/google-analytics-cookie-parser_23.html



■ 웹 브라우저 아티팩트

• 웹 브라우저 다운로드 목록

- ✓ 사용자가 선택하여 내려 받은 파일 정보 → 사용자 편의를 위해 저장
- ✓ 사용자 의도와 관련 없이 다운로드되는 캐시 데이터와는 구분

✓ 다운로드 목록 정보

- 다운로드 파일 저장 경로, 소스 URL, 파일 크기, 다운로드 시간, 다운로드 성공 여부

다운로드		
오늘 2013. 8. 14.		불후의 명곡 - 전설을 노래하다.E112.여름가요의 절대감자%21 클 특집.130803.HDTV.H264.720p-HANrel.avi.torrent http://www.torrentby.com/bbs/download.php?bo_table=torrent_variety&wr_id=32961&no=1 폴더 열기 목록에서 삭제
2013. 8. 10.		BETA_ANJP_CLI_AUGUST (1).exe 삭제됨 https://doc-08-5s-docs.googleusercontent.com/docs/securesc/ha0ro937gcuc717deffksulhg5... 목록에서 삭제
		BETA_ANJP_CLI_AUGUST.exe 삭제됨 https://doc-08-5s-docs.googleusercontent.com/docs/securesc/ha0ro937gcuc717deffksulhg5... 목록에서 삭제
		adroit_pf_31d_install_dm.exe http://digital-assembly.com/products/adroit-photo-forensics/downloads/get_apf/26b16614... 폴더 열기 목록에서 삭제
2013. 8. 9.		id32.v.0.58.win.zip https://tzworks.net/prototypes/index_dat/id32.v.0.58.win.zip 폴더 열기 목록에서 삭제

- 웹 브라우저 아티팩트

- 웹 브라우저 다운로드 목록 ➔ 분석 방법

- ✓ 다운로드 URL ➔ 접속 사이트
- ✓ 다운로드 시간 ➔ 해당 파일의 다운로드 시간
- ✓ 다운로드 파일의 경로 ➔ 파일 내용 확인
- ✓ 다운로드 받은 파일이 없을 경우, 저장된 URL을 이용해 다운로드 재시도

■ 웹 브라우저 아티팩트 경로

• 인터넷 익스플로러 (IE, Internet Explorer)

구분	경로
Cache	%UserProfile%\AppData\Local\Microsoft\Windows\Temporary Internet Files\Content.IE5\index.dat %UserProfile%\AppData\Local\Microsoft\Windows\Temporary Internet Files\Content.IE5\<Random>\<All Files>
History	%UserProfile%\AppData\Local\Microsoft\Windows\History\History.IE5\index.dat %UserProfile%\AppData\Local\Microsoft\Windows\History\History.IE5\<period>\index.dat
Cookie	%UserProfile%\AppData\Roaming\Microsoft\Windows\Cookies\index.dat %UserProfile%\AppData\Roaming\Microsoft\Windows\Cookies\<All Files>
Download	%UserProfile%\AppData\Roaming\Microsoft\Windows\IEDownloadHistory\index.dat (IE9 ~)
IE v10	%UserProfile%\AppData\Local\Microsoft\Windows\WebCache\WebCacheV(01 24).dat

• 파이어폭스 (Firefox)

구분	경로
Cache	%UserProfile%\AppData\Local\Mozilla\Firefox\Profiles\<Random>\Cache*.*
History	%UserProfile%\AppData\Roaming\Mozilla\Firefox\Profiles\<Random>.default\places.sqlite
Cookie	%UserProfile%\AppData\Roaming\Mozilla\Firefox\Profiles\<Random>.default\cookies.sqlite
Download	%UserProfile%\AppData\Roaming\Mozilla\Firefox\Profiles\<Random>.default\download.sqlite

■ 웹 브라우저 아티팩트 경로

• 크롬 (Chrome)

구분	경로
Cache	%UserProfile%\AppData\Local\Google\Chrome\User Data\Default\Cache\
History	%UserProfile%\AppData\Local\Google\Chrome\User Data\Default\History %UserProfile%\AppData\Local\Google\Chrome\User Data\Default\History\History Index <year-month>
Cookie	%UserProfile%\AppData\Local\Google\Chrome\User Data\Default\Cookies
Download	%UserProfile%\AppData\Local\Google\Chrome\User Data\Default\History

• 사파리 (Safari)

구분	경로
Cache	%UserProfile%\AppData\Local\Apple Computer\Safari\Cache.db
History	%UserProfile%\AppData\Roaming\Apple Computer\Safari\History.plist
Cookie	%UserProfile%\AppData\Roaming\Apple Computer\Safari\Cookies\Cookies.plist
Download	%UserProfile%\AppData\Roaming\Apple Computer\Safari\Downloads.plist

- 웹 브라우저 아티팩트 경로

- 오페라(Opera)

구분	경로
Cache	%UserProfile%\AppData\Local\Opera\Opera\cache\dcache4.url
History	%UserProfile%\AppData\Roaming\Opera\Opera\global_history.dat
Cookie	%UserProfile%\AppData\Roaming\Opera\Opera\cookies4.dat
Download	%UserProfile%\AppData\Roaming\Opera\Opera\download.dat

- 웹 브라우저 아티팩트 분석

- 시점이 특정되는 경우

- ✓ 시점을 기준으로 캐시, 히스토리, 쿠키, 다운로드 목록에 대한 통합 타임라인 분석

- 시점이 특정되지 않는 경우

- ✓ 웹 브라우저로 다운받은 PE 파일 검색
- ✓ 이상 패턴 검색 (a.jpg, b.gif, 1322.jpg, 2499.jpg 등)
- ✓ 악성 사이트 접속 여부
- ✓ 시스템 프로파일(%SystemRoot%\System32\config\systemprofile\W) 분석
- ✓

- 웹 브라우저 아티팩트 분석

- 악성 URL 목록 및 URL 점검

- ✓ AVG Online Web Page Scanner – <http://www.avg.com.au/resources/web-page-scanner/>
- ✓ BrightCloud URL/IP Lookup – <http://www.brightcloud.com/support/lookup.php>
- ✓ Cisco SenderBase – <http://www.senderbase.org/home>
- ✓ Norton Safe Web – <http://safeweb.norton.com/>
- ✓ PhishTank – <http://www.phishtank.com/>
- ✓ Malware Domain List – <http://www.malwaredomainlist.com/mdl.php>
- ✓ Malware URL – <http://www.malwareurl.com/listing-urls.php>
- ✓ McAfee SiteAdvisor – <http://www.siteadvisor.com/>
- ✓ TrendMicro Site Safety Center – <http://global.sitesafety.trendmicro.com/>
- ✓ URL Blacklist – <http://urlblacklist.com/?sec=search>
- ✓ URL Query – <http://urlquery.net/>
- ✓ URL Void – <http://urlvoid.com/>
- ✓ vURL Online – <http://vurl.mysteryfcm.co.uk/>
- ✓ Wepawet – <http://wepawet.iseclab.org/>
- ✓ Zulu URL Risk Analyzer – <http://zulu.zscaler.com/>

- 웹 브라우저 아티팩트 분석 도구

- **WEFA (IE v10 지원)** – DFRC

- ✓ <http://forensic.korea.ac.kr/tools/wefa.html>

- **Internet Evidence Finder(IEF) (IE v10 지원)** – Magnet Forensics

- ✓ <http://www.magnetforensics.com/software/internet-evidence-finder/ief-standard/>

- **Web Browser Tools** – NirSoft

- ✓ http://nirsoft.net/web_browser_tools.html

- **Web Historian™** – Mandiant

- ✓ <https://www.mandiant.com/resources/download/web-historian>

- **IE v10 아티팩트 분석 도구**

- ✓ **EseDbViewer** – <http://www.woanware.co.uk/forensics/esedbviewer.html>

- ✓ **ESEDatabaseView** – http://www.nirsoft.net/utls/ese_database_view.html

➔ 실습

- 웹 아티팩트 분석하기!!
 - ✓ 정상 웹 아티팩트 추출 후 분석
 - ✓ 삭제된 웹 아티팩트 추출 후 분석

➔ 실습

- 샘플 웹 아티팩트 분석하기!!

- 1) 사용자가 접근한 웹 메일을 모두 선택하세요.
- 2) 사용자가 가장 많이 방문한 사이트는 어디인가요?
- 3) 사용자가 구글독스에서 다운로드한 파일은 무엇인가요?
- 4) 사용자가 웹에서 다운받은 실행파일은 무엇인가요?
- 5) 사용자의 네이버 계정명은 무엇인가요?

웹 아티팩트

■ 액티브 X

- 웹 상에서 콘텐츠를 다운로드하기 위한 프레임워크 (IE 상에서만 실행됨)
- 웹 서비스만으로 부족한 부분을 클라이언트에 프로그램 설치로 보완
- 사용자의 동의를 유도하여 악성 프로그램 설치



■ 액티브 X 다운로드 파일

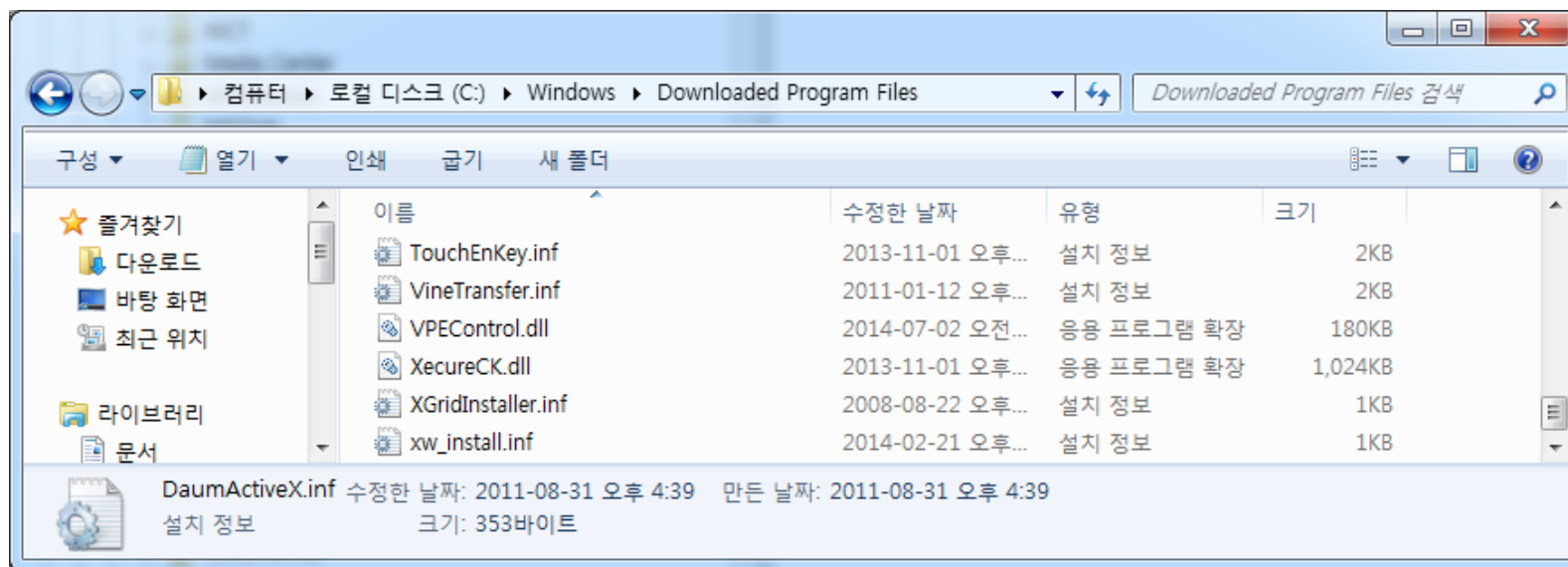
• 다운로드 경로 설정

✓ 키 : HKLM\SOFTWARE\Microsoft\Windows\CurrentVersion\Internet Settings

✓ 값 : ActiveXCache

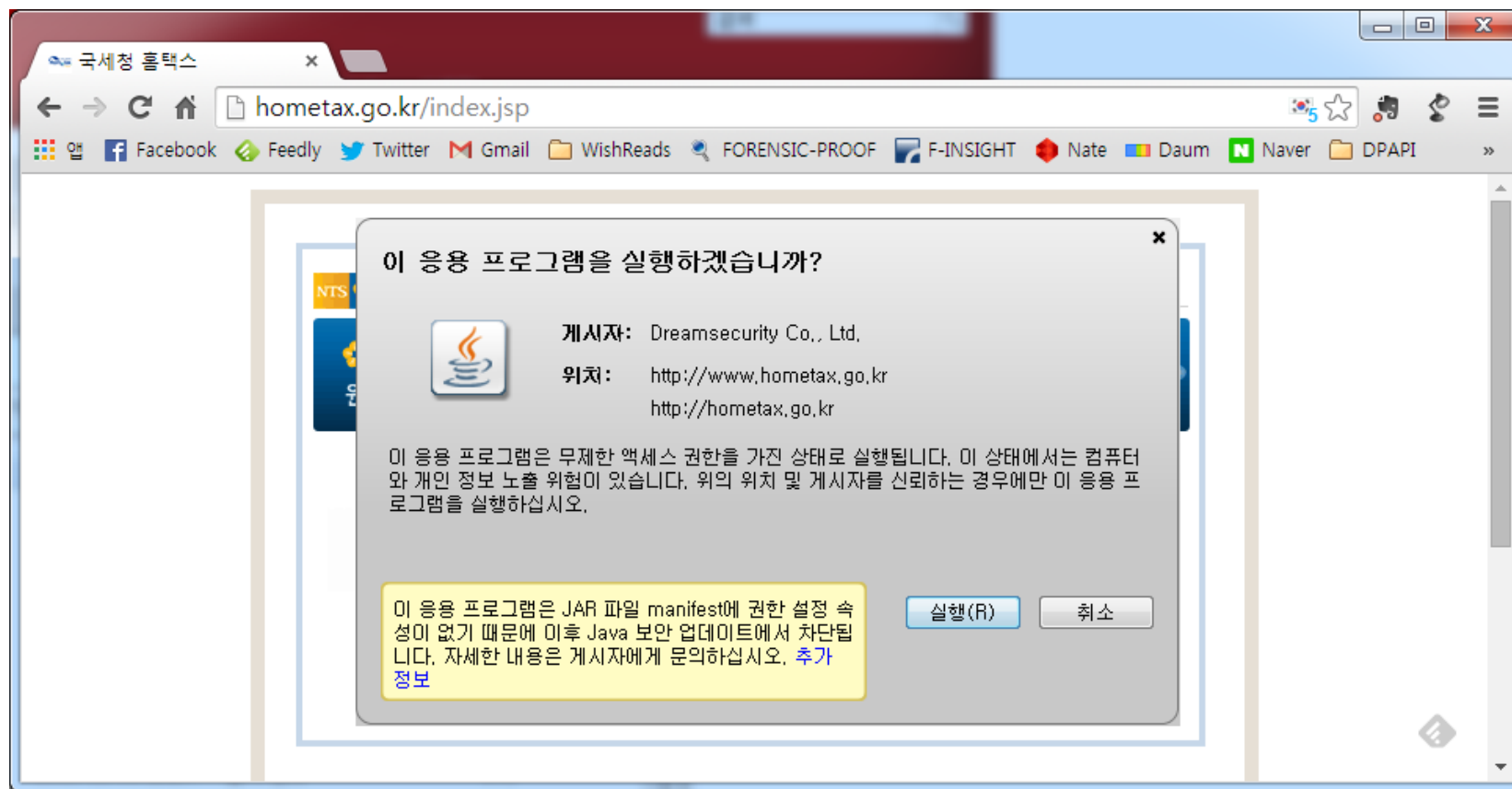
• 기본 다운로드 경로

✓ %SystemRoot%\Downloaded Program Files



■ 자바 애플릿

- 웹 브라우저를 통해 실행되는 자바 기반의 애플리케이션
- 애플릿을 다운받아 클라이언트에서 실행 ➔ 자바 가상머신 설치 필요



■ 자바 애플릿 취약점

- 자바 애플릿(JAR)을 통해 다운로드, 실행 → 악성코드 실행, JRE 취약점 악용
- 자바 애플릿이 실행되면 JAR 파일, IDX 파일이 캐시 폴더에 저장
 - ✓ %UserProfile%\AppData\LocalLow\Sun\Java\Deployment\Cache\##

• 자바 애플릿(JAR) 파일

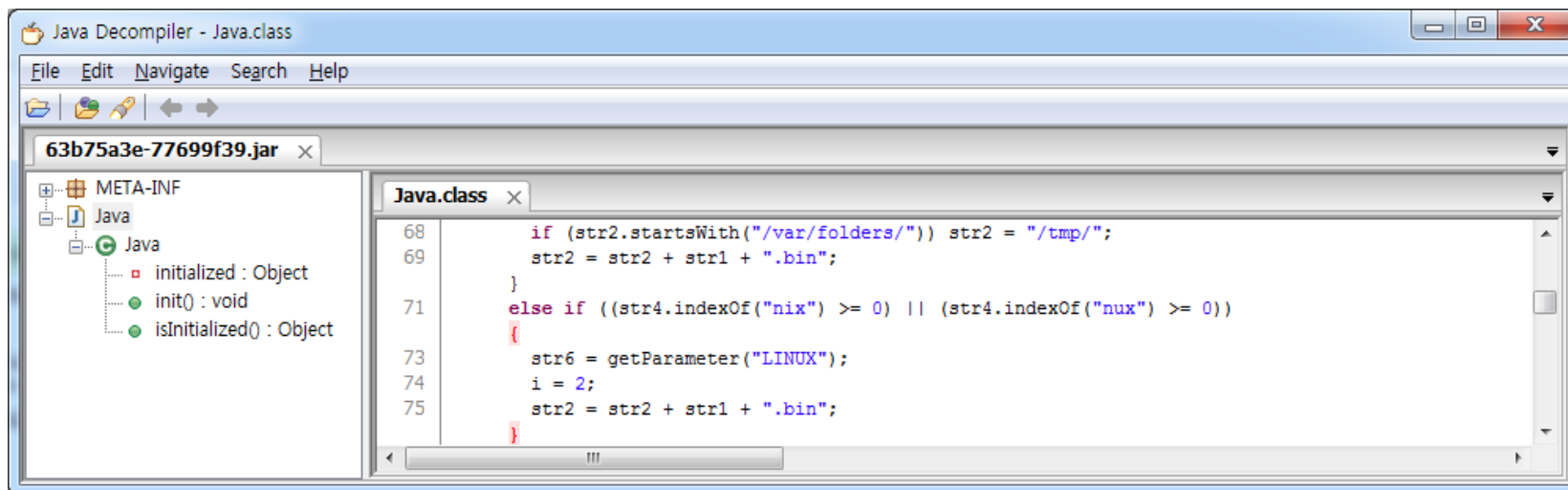
- ✓ 다운로드되면서 랜덤한 이름으로 변환되어 저장
- ✓ JAR 압축 해제 → 디컴파일을 통해 분석 가능

• 자바 IDX 파일

- ✓ 다운받은 JAR 파일과 동일한 경로에 '.idx' 형태로 저장
- ✓ 다운받은 경로(IP 주소 혹은 도메인명), HTTP 헤더, 다운로드 시간 확인 가능

- 자바 애플릿 다운로드 파일

- 자바 애플릿(JAR) 파일



- 자바 IDX 파일

[*] Section 2 (Download History) found:
URL: **http://207.58.245.179:80/tY77np5Yyi**
IP: **207.58.245.179**
<null>: HTTP/1.1 200 OK
content-length: **32768**
last-modified: Tue, 03 Apr 2012 00:25:21 GMT
content-type: text/plain; charset=UTF-8
date: Tue, 03 Apr 2012 00:32:31 GMT
server: **Apache/2.2.17 (Fedora)**

<http://computer-forensics.sans.org/blog/2013/02/16/idx-sample-file-malware>

자바 애플릿 타임라인

Spear Phish Email Received w/Java Applet attack
w/PDF and link (Email was about IRS w-2 tax forms)
The victim clicked on the link <http://bit.ly/GEUMQQ>

4/2/2012	20:32:52	MACB	Firefox 3 history	http://bit.ly/GEUMQQ/ [count: 2] Host: bit.ly (URL not typed directly) type: LINK
4/2/2012	20:32:52	MACB	Firefox 3 history	http://207.58.245.179/ (Internal Revenue Service) [count: 2] visited from: http://bit.ly/GEUMQQ/ (URL not typed directly) type: REDIRECT_PERMANENT
4/2/2012	20:32:57	M.CB	NTFS \$MFT	C:/WINDOWS/Sun/Java/Deployment
4/2/2012	20:32:57	M.CB	NTFS \$MFT	C:/WINDOWS/Sun
4/2/2012	20:32:57	M.CB	NTFS \$MFT	C:/WINDOWS/Sun/Java
4/2/2012	20:32:58	MACB	NTUSER key	Key name: HKEY_USER/Software/JavaSoft
4/2/2012	20:32:58	MACB	NTUSER key	Key name: HKEY_USER/Software/JavaSoft/JavaRuntimeEnvironment
4/2/2012	20:32:58	MACB	NTUSER key	Key name: HKEY_USER/Software/JavaSoft/JavaRuntimeEnvironment/1.6.0_31
4/2/2012	20:32:58	M.C.	NTFS \$MFT	C:/Documents and Settings/tdungan/Application Data/Sun/Java/Deployment/deployment.properties
4/2/2012	20:33:06	...B	NTFS \$MFT	C:/Documents and Settings/tdungan/Application Data/Sun/Java/Deployment/cache/6.0/62/c3b75a3e-77699f39.idx
4/2/2012	20:33:07	...B	NTFS \$MFT	C:/Documents and Settings/tdungan/Application Data/Sun/Java/Deployment/cache/6.0/lastAccessed
4/2/2012	20:33:15	M.CB	NTFS \$MFT	C:/Documents and Settings/tdungan/Local Settings/Temp/pkxezy1tji98.exe
4/2/2012	20:33:15	...B	NTFS \$MFT	C:/Documents and Settings/tdungan/Application Data/Sun/Java/Deployment/cache/6.0/4/6f13884-712bc739.idx
4/2/2012	20:33:16	M.C.	NTFS \$MFT	C:/Documents and Settings/tdungan/Application Data/Sun/Java/Deployment/
4/2/2012	20:33:16	...C.	NTFS \$MFT	C:/Documents and Settings/tdungan/Application Data/Sun/Java/Deployment/
4/2/2012	20:33:17	MACB	XP Prefetch	PKXEZY1TJI98.EXE-0BCBF29B.pf - [PKXEZY1TJI98.EXE] was executed - on col
4/2/2012	20:33:17	MACB	Firefox 3 history	http://www.irs.gov/ (Internal Revenue Service) [count: 1] Host: www.irs.gov visited from: http://207.58.245.179/ (URL not typed directly) type: LINK
4/2/2012	20:33:27	M.CB	NTFS \$MFT	C:/WINDOWS/Prefetch/PKXEZY1TJI98.EXE-0BCBF29B.pf
4/2/2012	20:34:26	...B	NTFS \$MFT	C:/WINDOWS/system32/dllhost
4/2/2012	20:35:10	M.CB	NTFS \$MFT	C:/WINDOWS/system32/dllhost/svchost.exe
4/2/2012	20:35:10	M.CB	NTFS \$MFT	C:/WINDOWS/system32/dllhost/winclient.reg
4/2/2012	20:35:49	M.C.	NTFS \$MFT	C:/WINDOWS/system32/dllhost
4/2/2012	20:36:03	...B	NTFS \$MFT	C:/WINDOWS/Prefetch/REG.EXE-0D2A95F7.pf
4/2/2012	20:37:14	MACB	SYSTEM key	Key name: HKLM/System/ControlSet002/Services/Netman/domain
4/2/2012	20:37:14	MACB	SYSTEM key	Key name: HKLM/System/ControlSet001/Services/Netman/domain
4/2/2012	20:39:24	MACB	SOFTWARE key	Key name: HKLM/Software/Microsoft/Windows/CurrentVersion/Run

Java Applet attack hits – Download of
malware into /temp folder

Malware run from /temp folder

Files Dropped – svchost.exe is beacon malware

Beacon Interval Set and Persistence
Achieved via “RUN” Key

- 자바 애플릿 분석 도구

- 자바 디컴파일 도구

- ✓ **JD-GUI (Java Decompiler)**

- <http://java.decompiler.free.fr/>

- 자바 IDX 분석 도구

- ✓ **Java_IDX_Parser** – Brian Baskin

- https://github.com/Rurik/Java_IDX_Parser

- ✓ **Javaidx** – Mark Woan

- <https://github.com/woanware/javaidx>

- ✓ **Idxparser** – Harlan Carvey

- <https://code.google.com/p/winforensicaanalysis/downloads/list>

➔ 실습

- **자바 IDX 분석하기!!**

- ✓ 자바 IDX 파일 추출 후 분석
- ✓ JAR 파일 추출 후 분석

- **자바 IDX 감염 샘플 분석하기!!**

- ✓ <http://computer-forensics.sans.org/blog/2013/02/16/idx-sample-file-malware>

외장저장장치 아티팩트

■ 감염 케이스

- 2010년 – 스텍스넷, 지멘스 사의 산업 장비 공격
- 2011년 – 농협 전산망 마비 사고

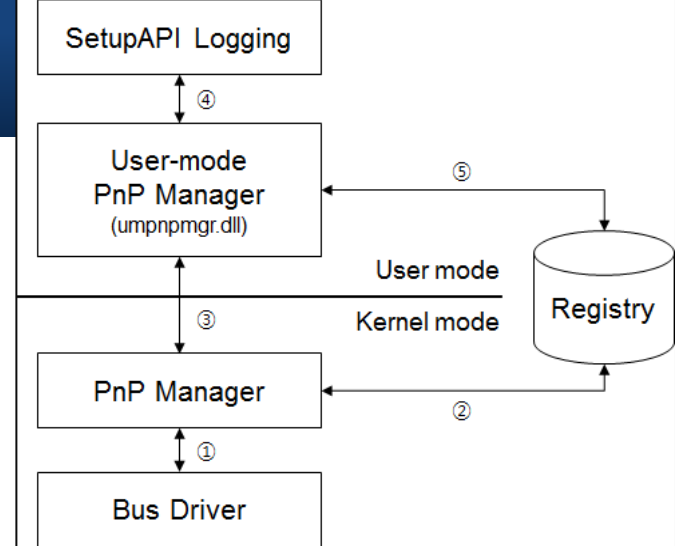
■ 감염 경로

- 우연히 습득한 외장저장장치
- 경품으로 받은 외장저장장치
- 망분리된 내부망 데이터 전달 시 악성코드 전파

■ 외장저장장치 인식 절차

1. 버스 드라이버는 PnP 관리자에게 장치의 고유 식별번호(device descriptor)로 연결 알림

✓ 식별번호 – 제조사, 일련번호, 드라이버 등을 포함



2. PnP 관리자는 받은 정보를 기반으로 Device Class ID를 설정하고 드라이버 검색
3. 드라이버가 없을 경우, PnP 관리자는 장치의 펌웨어로부터 드라이버를 전달받아 설치

✓ 장치 드라이버 설치 과정은 **Setup API 로그**에 기록

4. 드라이버 설치와 함께 **레지스트리**에 장치 관련 키/값 생성

✓ HKLM\SYSTEM\ControlSet00\Enum\USBSTOR\{DID, device class identifier}

✓ HKLM\SYSTEM\ControlSet00\Control\DeviceClasses\{GUID}

5. 장치가 인식되어 연결/해제될 때마다 **이벤트 로그** 기록

외장저장장치 아티팩트

■ 외장저장장치 연결 아티팩트

1. Setup API 로그

- ✓ %SystemRoot%\Winf\Setupapi.dev.log

2. 레지스트리 하이브

- ✓ %SystemRoot%\system32\config\SYSTEM
- ✓ %SystemRoot%\system32\config\SOFTWARE
- ✓ %UserProfile%\NTUSER.DAT

3. 이벤트 로그

- ✓ %SystemRoot%\system32\winevt\Logs\Microsoft-Windows-DriverFrameworks-UserMode%4Operational.evtx

외장저장장치 아티팩트

1. Setup API 로그

- 장치 드라이버, 서비스 팩 등이 설치될 때 남기는 텍스트 로그
- 저장장치 최초 연결 시 장치 드라이버 설치 흔적이 남음 → **최초 연결 시각**
- 윈도우 2K/XP : %SystemRoot%\Setupapi.log
- 윈도우 Vista+ : %SystemRoot%\Winf\Setupapi.dev.log

```
setupapi.dev.log
24773 >>> [Device Install (Hardware initiated) - USBSTOR\Disk&Ven_Seagate&Prod_Backup+_SL&Rev_0409\NA51QN7W&0]
24774 >>> Section start 2013/01/11 14:47:55.884
24775 ump: Creating Install Process: DrvInst.exe 14:47:55.884
24776 ndv: Retrieving device info...
24777 ndv: Setting device parameters...
24778 ndv: Searching Driver Store and Device Path...
24779 dvi: {Build Driver List} 14:47:55.884
24780 dvi: Searching for hardware ID(s):
24781 dvi: usbstor\diskseagate_backup+_sl_____0409
24782 dvi: usbstor\diskseagate_backup+_sl_____
24783 dvi: usbstor\diskseagate_
24784 dvi: usbstor\seagate_backup+_sl_____0
24785 dvi: seagate_backup+_sl_____0
24786 dvi: usbstor\gendisk
24787 dvi: gendisk
24788 dvi: Searching for compatible ID(s):
24789 dvi: usbstor\disk
24790 dvi: usbstor\raw
24791 cpy: Policy is set to make all digital signatures equal.
24792 dvi: Enumerating INFs from path list 'C:\Windows\inf'
```

2. 레지스트리

- 최초 연결 시각

- ✓ HKLM\SOFTWARE\Microsoft\Windows NT\CurrentVersion\EMDMgmt\{Device Entry}
- ✓ HKLM\SOFTWARE\Microsoft\Windows Portable Devices\Devices\{Device Entry}

- 부팅 이후 연결 시각

- ✓ HKLM\SYSTEM\ControlSet00#\Control\DeviceClasses\{53F56307-B6BF-11D0-94F2-00A0C91EFB8B}\{Sub Keys}
- ✓ HKLM\SYSTEM\ControlSet00#\Control\DeviceClasses\{53F5630D-B6BF-11D0-94F2-00A0C91EFB8B}\{Sub Keys}
- ✓ HKLM\SYSTEM\ControlSet00#\Control\DeviceClasses\{6AC27878-A6FA-4155-BA85-F98F491D4F33}\{Sub Keys}
- ✓ HKLM\SYSTEM\ControlSet00#\Control\DeviceClasses\{A5DCBF10-6530-11D2-901F-00C04FB951ED}\{Sub Keys}
- ✓ HKLM\SYSTEM\ControlSet00#\Enum\WpdBusEnumRoot\UMB\{Device Entry}

2. 레지스트리

- <http://forensic-proof.com/archives/3632>

Artifacts	Path
Vendor & Product Name, Version	HKLM\SYSTEM\ControlSet00\Enum\USBSTOR\Disk&Ven_{Vendor Name}&Prod_{Product Name}&Rev_{Version}
Vendor ID, Product ID	HKLM\SYSTEM\ControlSet00\Enum\USB\VID_{Vendor ID}&PID_{Product ID}
Serial Number	HKLM\SYSTEM\ControlSet00\Enum\USB\{Vendor ID & Product ID}\{Serial Number} HKLM\SYSTEM\ControlSet00\Enum\USBSTOR\{Device Class ID}\{Serial Number}&#
Volume Serial Number	HKLM\SOFTWARE\Microsoft\Windows NT\CurrentVersion\EMDMgmt\ _??_USBSTOR#{Device Class ID}#{Unique Instance ID}#{GUID}{Volume Label}_{Volume Serial Number}
Volume Label	HKLM\SOFTWARE\Microsoft\Windows NT\CurrentVersion\EMDMgmt\ _??_USBSTOR#{Device Class ID}#{Unique Instance ID}#{GUID}{Volume Label}_{Volume Serial Number} HKLM\SOFTWARE\Microsoft\Windows Portable Devices\Devices\{Device Entry}\FriendlyName (value) HKLM\System\ControlSet00\Enum\WpdBusEnumRoot\UMB\{Device Entry}\FriendlyName (value)
Drive Letter	HKLM\System\MountedDevices (search for serial number) HKLM\SOFTWARE\Microsoft\Windows Portable Devices\Devices\{Device Entry}\FriendlyName (value) HKLM\System\ControlSet00\Enum\WpdBusEnumRoot\UMB\{Device Entry}\FriendlyName (value)
Volume GUID	HKLM\SYSTEM\MountedDevices\??\Volume{Volume GUID} (search for serial number)
User Name	HKU\{USER}\Software\Microsoft\Windows\CurrentVersion\Explorer\MountPoints2\{Volume GUID}
First Connection Time (Last Written Time in registry key)	%SystemRoot%\inf\Setupapi.dev.log HKLM\SYSTEM\ControlSet00\Control\DeviceClasses\{10497B1B-BA51-44E5-8318-A65C837B6661}\{Sub Keys} HKLM\SOFTWARE\Microsoft\Windows NT\CurrentVersion\EMDMgmt\{Device Entry} HKLM\SOFTWARE\Microsoft\Windows Portable Devices\Devices\{Device Entry}
First Connection Time After Booting (Last Written Time in registry key)	HKLM\SYSTEM\ControlSet00\Control\DeviceClasses\{53F56307-B6BF-11D0-94F2-00A0C91EFB8B}\{Sub Keys} HKLM\SYSTEM\ControlSet00\Control\DeviceClasses\{53F5630D-B6BF-11D0-94F2-00A0C91EFB8B}\{Sub Keys} HKLM\SYSTEM\ControlSet00\Control\DeviceClasses\{6AC27878-A6FA-4155-BA85-F98F491D4F33}\{Sub Keys} HKLM\SYSTEM\ControlSet00\Control\DeviceClasses\{A5DCBF10-6530-11D2-901F-00C04FB951ED}\{Sub Keys} HKLM\SYSTEM\ControlSet00\Enum\WpdBusEnumRoot\UMB\{Device Entry}
Last Connection Time (Last Written Time in registry key)	HKLM\SYSTEM\ControlSet00\Enum\WpdBusEnumRoot\UMB\{Device Entry}\Device Parameters HKU\{USER}\Software\Microsoft\Windows\CurrentVersion\Explorer\MountPoints2\{Volume GUID}

3. 이벤트 로그

- 윈도우 Vista/7에서는 장치 연결/해제 시 드라이버 로드/언로드와 관련된 이벤트 생성
- **윈도우 Vista/7** : %SystemRoot%\System32\winevt\Logs\Microsoft-Windows-DriverFrameworks-UserMode%4Operational.evtx










3. 이벤트 로그

- 장치 연결 시 25개 이벤트 발생

Level	Date and Time	Source	Event ID	Task Category
Information	7/27/2014 1:29:06 AM	DriverFrameworks-UserMo...	2101	Pnp or Power Management operation t...
Information	7/27/2014 1:29:06 AM	DriverFrameworks-UserMo...	2106	Pnp or Power Management operation t...
Information	7/27/2014 1:29:06 AM	DriverFrameworks-UserMo...	2105	Pnp or Power Management operation t...
Information	7/27/2014 1:29:06 AM	DriverFrameworks-UserMo...	2100	Pnp or Power Management operation t...
Information	7/27/2014 1:29:06 AM	DriverFrameworks-UserMo...	2101	Pnp or Power Management operation t...
Information	7/27/2014 1:29:06 AM	DriverFrameworks-UserMo...	2106	Pnp or Power Management operation t...
Information	7/27/2014 1:29:06 AM	DriverFrameworks-UserMo...	2105	Pnp or Power Management operation t...
Information	7/27/2014 1:29:06 AM	DriverFrameworks-UserMo...	2100	Pnp or Power Management operation t...
Information	7/27/2014 1:29:06 AM	DriverFrameworks-UserMo...	2101	Pnp or Power Management operation t...
Information	7/27/2014 1:29:06 AM	DriverFrameworks-UserMo...	2106	Pnp or Power Management operation t...
Information	7/27/2014 1:29:06 AM	DriverFrameworks-UserMo...	2105	Pnp or Power Management operation t...
Information	7/27/2014 1:29:06 AM	DriverFrameworks-UserMo...	2100	Pnp or Power Management operation t...
Verbose	7/27/2014 1:29:06 AM	DriverFrameworks-UserMo...	2006	Loading drivers to control a newly disc...
Verbose	7/27/2014 1:29:06 AM	DriverFrameworks-UserMo...	2005	Loading drivers to control a newly disc...
Verbose	7/27/2014 1:29:06 AM	DriverFrameworks-UserMo...	2005	Loading drivers to control a newly disc...
Verbose	7/27/2014 1:29:06 AM	DriverFrameworks-UserMo...	2005	Loading drivers to control a newly disc...
Verbose	7/27/2014 1:29:06 AM	DriverFrameworks-UserMo...	2005	Loading drivers to control a newly disc...
Verbose	7/27/2014 1:29:05 AM	DriverFrameworks-UserMo...	2005	Loading drivers to control a newly disc...
Verbose	7/27/2014 1:29:05 AM	DriverFrameworks-UserMo...	2004	Loading drivers to control a newly disc...
Information	7/27/2014 1:29:05 AM	DriverFrameworks-UserMo...	2010	Loading drivers to control a newly disc...
Information	7/27/2014 1:29:05 AM	DriverFrameworks-UserMo...	2003	Loading drivers to control a newly disc...
Information	7/27/2014 1:29:05 AM	DriverFrameworks-UserMo...	1004	Creation of a new driver host process.
Information	7/27/2014 1:29:05 AM	DriverFrameworks-UserMo...	2001	Startup of a new driver host process.
Information	7/27/2014 1:29:05 AM	DriverFrameworks-UserMo...	2000	Startup of a new driver host process.
Information	7/27/2014 1:29:05 AM	DriverFrameworks-UserMo...	1003	Creation of a new driver host process.
Information	7/27/2014 1:29:04 AM	DriverFrameworks-UserMo...	1000	Startup of the driver manager service.

3. 이벤트 로그

- 장치 해제 시 8개 이벤트 발생

Level	Date and Time	Source	Event ID	Task Category
 Information	7/27/2014 1:43:22 AM	DriverFrameworks-UserMo...	1008	Shutdown of a driver host process.
 Information	7/27/2014 1:43:22 AM	DriverFrameworks-UserMo...	2901	Shutdown of a driver host process.
 Information	7/27/2014 1:43:22 AM	DriverFrameworks-UserMo...	2900	Shutdown of a driver host process.
 Information	7/27/2014 1:43:22 AM	DriverFrameworks-UserMo...	1006	Shutdown of a driver host process.
 Information	7/27/2014 1:43:22 AM	DriverFrameworks-UserMo...	2102	Pnp or Power Management operation t...
 Information	7/27/2014 1:43:22 AM	DriverFrameworks-UserMo...	2100	Pnp or Power Management operation t...
 Information	7/27/2014 1:43:22 AM	DriverFrameworks-UserMo...	2102	Pnp or Power Management operation t...
 Information	7/27/2014 1:43:22 AM	DriverFrameworks-UserMo...	2100	Pnp or Power Management operation t...
 Information	7/27/2014 1:29:06 AM	DriverFrameworks-UserMo...	2101	Pnp or Power Management operation t...

▪ 연결 흔적 분석 도구

• SetupAPI 로그 & 레지스트리 ➔ 분석 도구

✓ **REGA** – DFRC

- <http://forensic.korea.ac.kr/tools/rega.html>

✓ **USBDeviceForensics** – Mark Woan

- <http://www.woanware.co.uk/forensics/usbdeviceforensics.html>

✓ **RegRipper** – Harlan Carvey

- <https://code.google.com/p/regripper/>

• 이벤트 로그 ➔ 분석 도구

✓ **USB Device Tracking Batch Script** – Jason Hale

- <http://dfstream.blogspot.kr/2014/02/usb-device-tracking-batch-script.html>

✓ **USB Event Tracing for Windows** – Microsoft

- [http://msdn.microsoft.com/en-us/library/windows/hardware/jj151577\(v=vs.85\).aspx](http://msdn.microsoft.com/en-us/library/windows/hardware/jj151577(v=vs.85).aspx)

➔ 실습

- 라이브 환경에서 외장저장장치 연결 흔적 분석하기!!
 - ✓ Setup API 로그 분석
 - ✓ 레지스트리 분석
 - ✓ 이벤트 로그 분석

➔ 실습

- (레지스트리 + Setup API 로그) 샘플에서 외장저장장치 흔적 분석하기!!

- 1) 시스템에 장착된 로컬스토리지는 몇 개인가요?
- 2) CD-ROM 드라이브가 마운트된 볼륨은 무엇인가요?
- 3) 시스템에 연결되었던 외장저장장치는 모두 몇 개인가요?
- 4) SanDisk Extreme USB Device 중 2개의 외장저장장치는 항목이 1개만 나오는 이유는?
- 5) 시스템에 가장 먼저 연결된 외장저장장치는 무엇인가요?
- 6) 시스템에 가장 마지막에 연결된 외장저장장치는 무엇인가요?
- 7) USB2.0 Flash Disk USB(9BC517001CB07EF8)를 연결한 사용자는 누구인가요?

- (이벤트 로그) 샘플에서 외장저장장치 흔적 분석하기!!

→ 실습

- **CODEGATE 2011 Quals – F300**

we are investigating the military secret's leaking. we found traffic with leaking secrets while monitoring the network. Security team was sent to investigate, immediately. But, there was no one present. It was found by forensics team that all the leaked secrets were completely deleted by wiping tool. And the team has found a leaked trace using portable device. Before long, the suspect was detained. But he denies allegations.

Now, the investigation is focused on portable device. The given files are acquired registry files from system. The estimated time of the incident is Mon, 21 February 2011 15:24:28(KST). Find a trace of portable device used for the incident.

The Key : "Vendor name" + "volume name" + "serial number" (please write in capitals)

- **CODEGATE 2011 YUT Challenge – Level [3-4]**

we are investigating the military secret's leaking. It seems that the suspect used a portable device. Find a signature of mounted E: drive. (please write in capitals)

이메일 아티팩트

■ 이메일이란?

- 포트 25번으로 서버 간 전달되는 텍스트 메시지

• 이메일 파일 구성

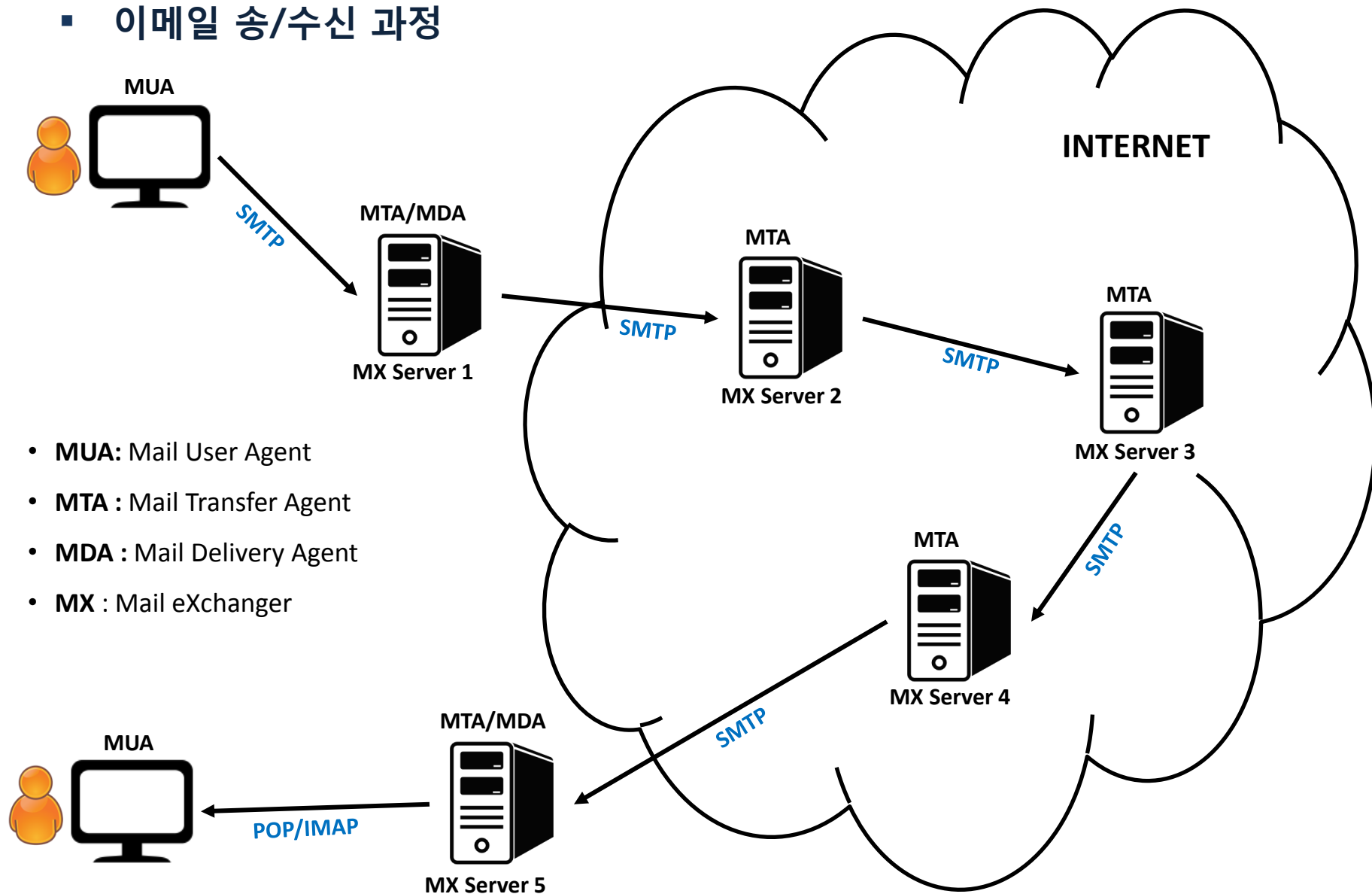
- ✓ 헤더
- ✓ 바디 (메시지)
- ✓ 첨부파일 (텍스트 인코딩)

• 분석 대상

- ✓ 로컬 이메일 클라이언트
- ✓ 웹 메일
- ✓ 스마트폰 동기화 또는 웹 메일 흔적
- ✓ PDA, Tablet PC 등 스마트기기 흔적
- ✓

이메일 아티팩트

이메일 송/수신 과정



- 이메일 아티팩트 분석

- 이메일 헤더

Return-Path: <example_from@dc.edu>

X-SpamCatcher-Score: 1 [X]

Received: from [136.167.40.119] (HELO dc.edu)

by fe3.dc.edu (CommuniGate Pro SMTP 4.1.8)

with ESMTP-TLS id 61258719 for example_to@mail.dc.edu; Mon, 23 Aug 2004 11:40:10 -0400

Message-ID: <4129F3CA.2020509@dc.edu>

Date: Mon, 23 Aug 2005 11:40:36 -0400

From: Taylor Evans <example_from@dc.edu>

User-Agent: Mozilla/5.0 (Windows; U; Windows NT 5.1; en-US; rv:1.0.1) Gecko/20020823 Netscape/7.0

X-Accept-Language: en-us, en

MIME-Version: 1.0

To: Jon Smith <example_to@mail.dc.edu>

Subject: Business Development Meeting

Content-Type: text/plain; charset=us-ascii; format=flowed

Content-Transfer-Encoding: 7bitv

- 이메일 아티팩트 분석

- 이메일 헤더 분석 시 고려 사항 (<https://www.blackhat.com/presentations/bh-usa-03/bh-us-03-akin.pdf>)
 - ✓ Open Relay
 - ✓ False Received From Header
 - ✓ Anonymizer
 - ✓ Open Proxy
 - ✓ SSH Tunnel

■ 이메일 아티팩트란?

- (스피어) 피싱 메일에 첨부된 악성 링크나 악성 파일에 의한 감염
- 타임라인 분석과 연계하여 특정 시점을 기준으로 이메일 아티팩트 분석

• 이메일 아티팩트 분석 범위

- ✓ 웹 메일, 이메일 스토리지 파일 내 아이템 분석
- ✓ 삭제된 웹 메일 아티팩트, 이메일 스토리지 복구
- ✓ 이메일 스토리지 내 삭제된 아이템 복구
- ✓ 이메일 파일 변조 흔적
- ✓ 이메일 발신/수신 내역 조작 분석

■ 이메일 아티팩트 획득

- MS Outlook (.PST, .DBX, .OST, .WAB)
- MS Exchange Server (.EDB, .STM)
- Lotus Notes (.NSF, .NTF)
- Thunderbird (.DB, .RDF, .SQLITE, .DAT, ...)
- Webmail
- EML, MSG, ...

- 이메일 아티팩트 분석

- MS Outlook

- ✓ .PST, .OST 파일 ➔ MS Office Outlook 또는 3rd party 도구 사용
- ✓ .DBX 파일 ➔ MS Outlook Express 또는 3rd party 도구 사용

- MS Exchange Server

- ✓ MS SQL Server로 이메일 관리
- ✓ SQL 데이터 분석 & SQL 서버 아티팩트 분석
- ✓ SQL Server 관리자 인터페이스 또는 3rd party 도구 사용

■ 이메일 아티팩트 분석

• Lotus Notes

- ✓ 서버 관리 프로그램을 이용해 분석
- ✓ .NSF 파일 → PST로 변환 3rd party 도구 사용

• Thunderbird

- ✓ 서버 메일 디렉터리에 개별 메시지 분석 → 텍스트 편집기, 정규 표현식 등
- ✓ 클라이언트는 mbox 형식으로 메일 저장

• Webmail

- ✓ 웹 브라우저 히스토리를 이용해 웹 메일, 사내 메일 사용 흔적 분석
- ✓ 웹 브라우저 캐시를 이용해 캐시된 메일 흔적 분석
- ✓ 자동 완성된 웹 메일 계정/패스워드 획득

- 이메일 아티팩트 분석 도구

- **E-mail Examiner** – Paraben

- ✓ <http://www.paraben.com/email-examiner.html>

- **Mailxaminer** – SysTools

- ✓ <http://www.mailxaminer.com/product/>

- 이메일 스토리지 파일 내 메시지 복구 도구

- **Phoenix® Outlook PST Repair** – Stellar Information Systems

- ✓ <http://www.stellarinfo.com/outlook-pst-file-recovery.htm>

- **Recover My Email** – GetData

- ✓ <http://www.recovermyemail.com/>

➔ 실습

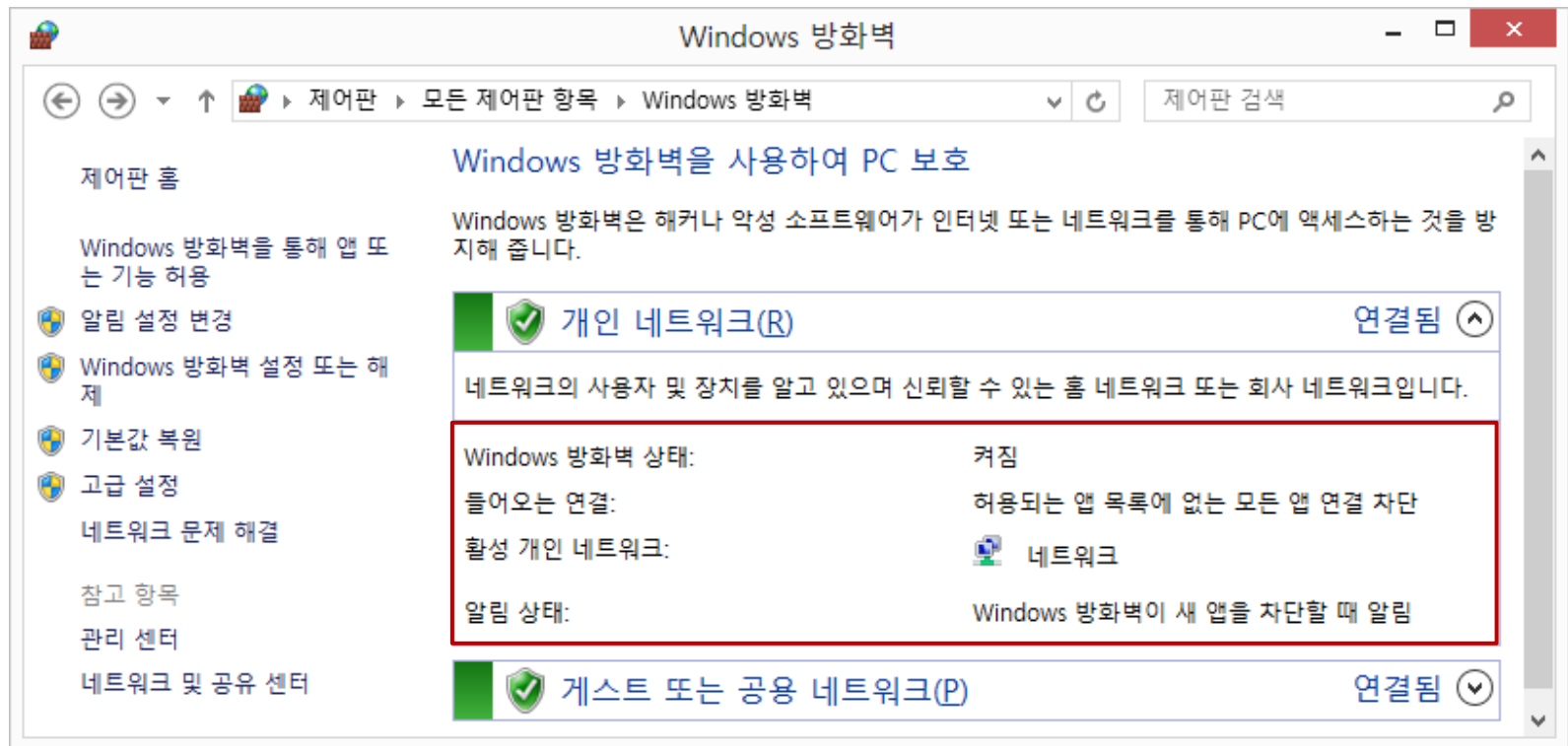
- 이메일 아티팩트 분석하기!!
 - ✓ 웹메일 테스트 데이터 생성
 - ✓ 웹 아티팩트로 웹메일 흔적 분석

방화벽 로그

■ 윈도우 방화벽 설정

• [제어판] → [Windows 방화벽]

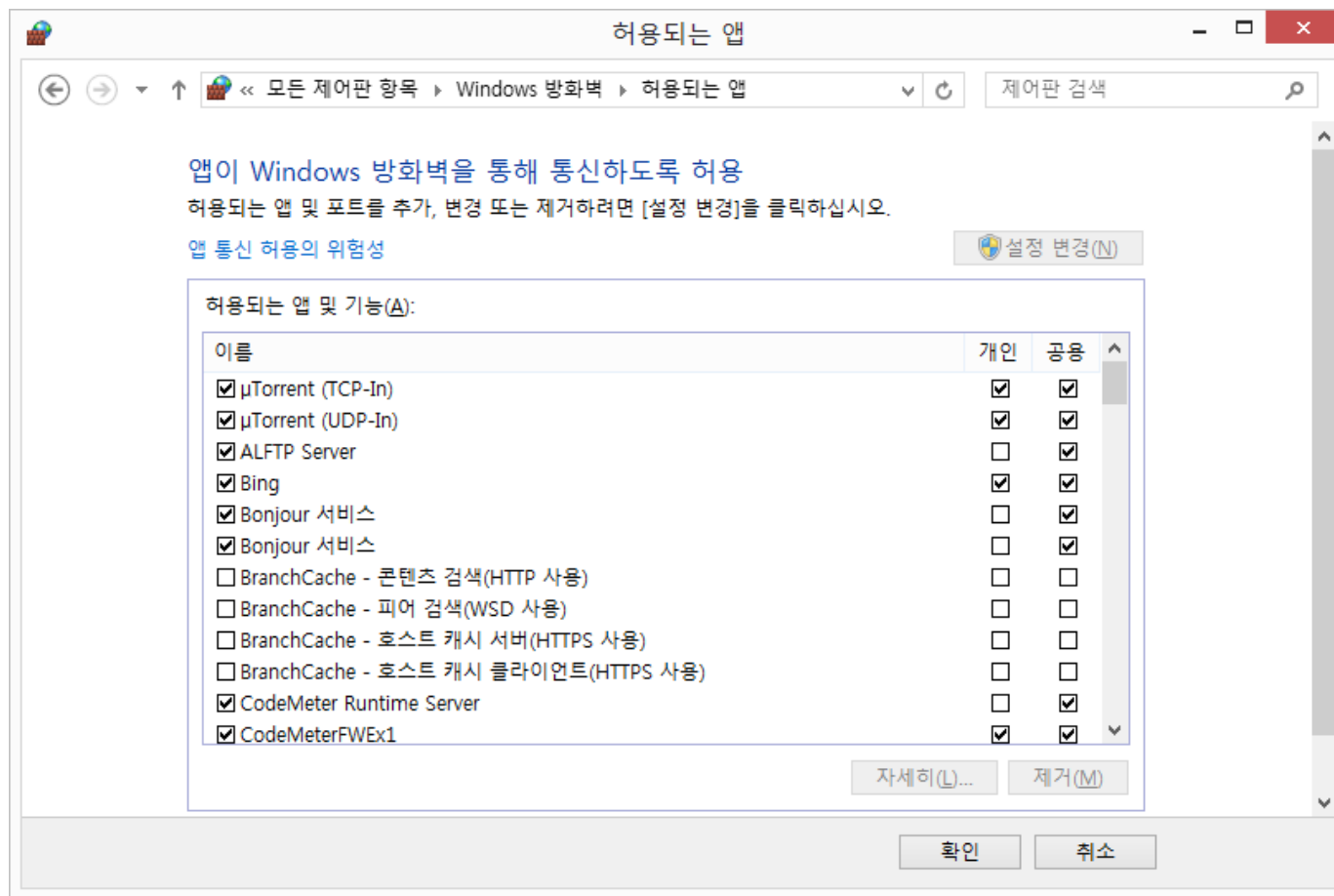
✓ 윈도우 Vista 이후부터, 방화벽 성능이 크게 강화



■ 윈도우 방화벽 설정

- [제어판] → [Windows 방화벽] → [Windows 방화벽을 통해 앱 또는 기능 허용]

✓ 허용되는 애플리케이션 설정

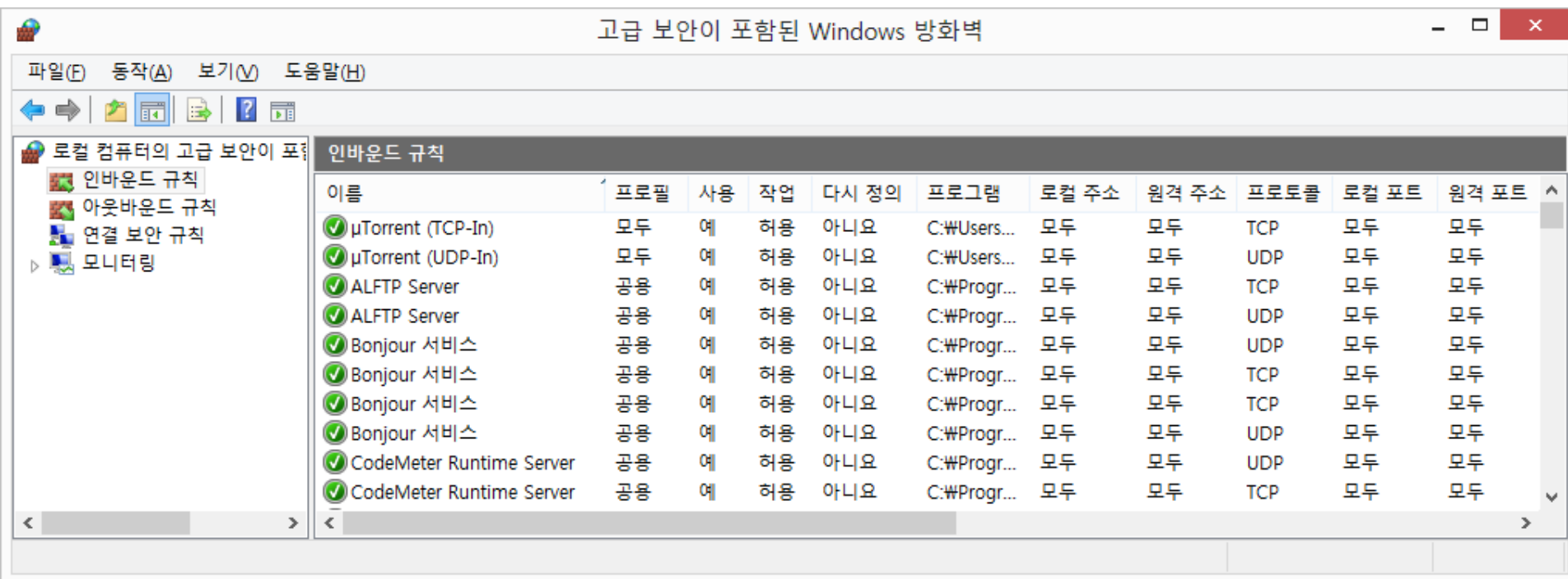


방화벽 로그

■ 윈도우 방화벽 설정

• [제어판] → [Windows 방화벽] → [고급 설정]

✓ 애플리케이션 별 상세한 설정 가능

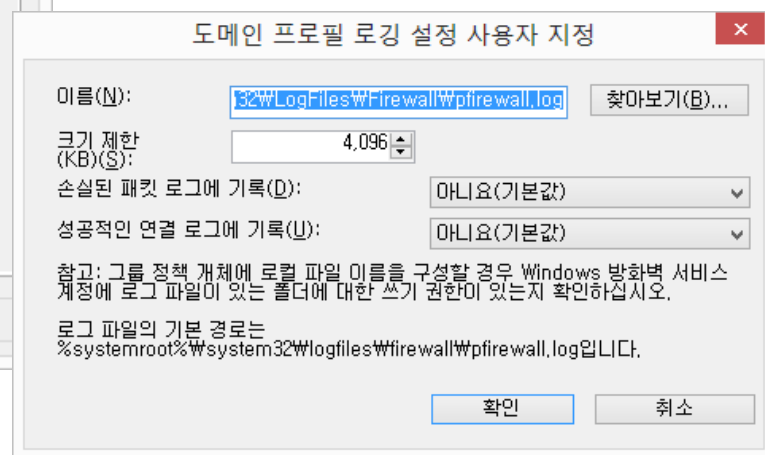
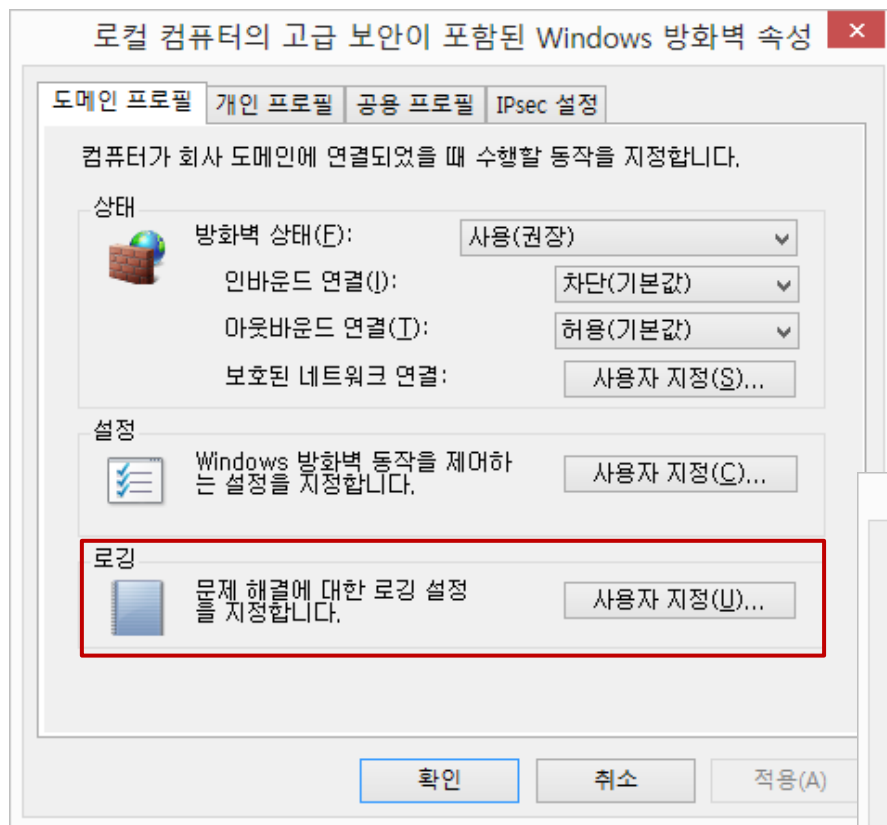


방화벽 로그

■ 윈도우 방화벽 설정

• 방화벽 로깅은 기본 비활성화 ➔ 추가적인 설정 필요

✓ [제어판] ➔ [Windows 방화벽] ➔ [고급 설정] ➔ [동작] ➔ [속성]



방화벽 로그

■ 윈도우 방화벽 설정

• 로그 경로

✓ %SystemRoot%\System32\LogFiles\Firewall\pfirewall.log

pfirewall.log													
1	#Version: 1.5												
2	#Software: Microsoft Windows Firewall												
3	#Time Format: Local												
4	#Fields: date time action protocol src-ip dst-ip src-port dst-port size tcpflags tcpsyn tcpack tcpwin icmptype												
5													
6	2013-07-31	21:07:44	DROP	UDP	163.152.127.20	192.168.0.35	55842	55842	129	-	-	-	RECEIVE
7	2013-07-31	21:07:45	DROP	UDP	163.152.127.20	192.168.0.35	55842	55842	129	-	-	-	RECEIVE
8	2013-07-31	21:07:47	DROP	UDP	163.152.127.20	192.168.0.35	55842	55842	129	-	-	-	RECEIVE
9	2013-07-31	21:08:41	DROP	UDP	220.244.218.222	192.168.0.35	44036	55842	94	-	-	-	RECEIVE
10	2013-07-31	21:08:41	DROP	UDP	94.51.226.18	192.168.0.35	7102	55842	326	-	-	-	RECEIVE
11	2013-07-31	21:11:36	DROP	UDP	121.136.59.250	192.168.0.35	55282	55842	94	-	-	-	RECEIVE
12	2013-07-31	21:11:51	DROP	UDP	79.117.74.227	192.168.0.35	50657	55842	84	-	-	-	RECEIVE
13	2013-07-31	21:11:55	DROP	UDP	172.250.58.235	192.168.0.35	1024	55842	75	-	-	-	RECEIVE
14	2013-07-31	21:12:17	DROP	UDP	101.108.252.165	192.168.0.35	33986	55842	313	-	-	-	RECEIVE
15	2013-08-01	00:07:51	DROP	UDP	163.152.127.20	192.168.0.35	55842	55842	129	-	-	-	RECEIVE
16	2013-08-01	00:07:53	DROP	UDP	163.152.127.20	192.168.0.35	55842	55842	129	-	-	-	RECEIVE
17	2013-08-01	00:07:58	DROP	UDP	163.152.127.20	192.168.0.35	55842	55842	129	-	-	-	RECEIVE
18	2013-08-01	00:09:06	DROP	UDP	74.78.11.185	192.168.0.35	1024	55842	75	-	-	-	RECEIVE
19	2013-08-01	00:09:46	DROP	UDP	94.248.231.44	192.168.0.35	1024	55842	75	-	-	-	RECEIVE
20	2013-08-01	00:09:55	DROP	UDP	24.61.202.233	192.168.0.35	1024	55842	294	-	-	-	RECEIVE
21	2013-08-01	00:11:34	DROP	UDP	112.78.140.98	192.168.0.35	6881	55842	94	-	-	-	RECEIVE
22	2013-08-01	00:14:15	DROP	UDP	86.81.238.252	192.168.0.35	7116	55842	84	-	-	-	RECEIVE
23	2013-08-01	00:14:47	DROP	UDP	24.93.209.179	192.168.0.35	20994	55842	94	-	-	-	RECEIVE
24	2013-08-01	00:15:40	DROP	UDP	93.127.49.195	192.168.0.35	11888	55842	94	-	-	-	RECEIVE
25	2013-08-01	00:17:50	DROP	UDP	178.93.243.184	192.168.0.35	17022	55842	94	-	-	-	RECEIVE
26	2013-08-01	00:18:53	DROP	UDP	201.254.58.190	192.168.0.35	19967	55842	94	-	-	-	RECEIVE
27	2013-08-01	00:21:35	DROP	UDP	163.152.127.20	192.168.0.35	55842	55842	129	-	-	-	RECEIVE

- 윈도우 방화벽 로그 분석 도구

- **WinFirewallLogAnalyser** – ZedLan

- ✓ http://www.zedlan.com/win_firewall_log_analyser.php

- **PowerShell을 이용한 분석** – Microsoft

- ✓ <http://blogs.technet.com/b/heyscriptingguy/archive/2011/08/03/learn-how-to-use-powershell-to-parse-the-firewall-log.aspx>

➔ 실습

- 방화벽 로그 분석하기!!
 - ✓ 방화벽 로깅을 설정하여 로그 저장
 - ✓ 저장된 로그 분석

이벤트 로그

■ 이벤트 로그 분석

- 다른 아티팩트와 다르게 조사 목적을 위해 저장
- 공격 유형별로 시스템에 남는 이벤트 로그 확인 필요
- 외부 접근 이외에 내부 시스템의 접근 로그 확인 필요
- 침해사고와 관련한 이벤트 로그 목록
 - ✓ <http://zeltser.com/log-management/security-incident-log-review-checklist.html>
 - ✓ <http://www.sans.org/reading-room/whitepapers/logging/detecting-security-incidents-windows-workstation-event-logs-34262>
 - ✓ <http://www.sans.org/reading-room/whitepapers/detection/event-monitoring-incident-response-34232>

- 이벤트 로그 분석 도구

- **Log Parser/Log Parser Studio** – Microsoft

- ✓ <http://www.microsoft.com/en-us/download/details.aspx?id=24659>

- ✓ http://blogs.technet.com/b/exchange_ko/archive/2012/04/25/log-parser-studio.aspx

- **Event Log Explorer** – EventLogXP

- ✓ <http://www.eventlogxp.com/>

