윈도우 10 포렌식 분석

플레인비트 대표

김진국



jinkook.kim@plainbit.co.kr

개요



1. 포렌식 아티팩트 비교

2. NEW 아티팩트



운영체제 비교

Windows 8.1 Windows 10

Windows 8.1 VS Windows 10

Windows 10



메모리 수집 및 분석

- 기존 도구로 수집 가능!!
 - **FDPro** BY HBGary
 - Memorize BY MANDIANT
 - FTK Imager BY AccessData
 -
- 메모리 분석
 - **Volatility** BY The Volatility Foundation?
 - Redline BY MANDIANT ?



기본 프로세스 (Processes)

윈도우 8.1

- + System
 - interrupts
 - smss.exe
- csrss.exe
- csrss.exe
- + wininit.exe
 - + services.exe
 - sychost.exe
 - ...
 - svchost.exe
 - spoolsv.exe
 - MsMpEng.exe
 - SearchIndexer.exe
 - Isass.exe
- winlogon.exe
 - dwm.exe
- explorer.exe
 - iexplore.exe

윈도우 10

+ System

- interrupts
- smss.exe
- csrss.exe
- csrss.exe
- + wininit.exe
 - + services.exe
 - svchost.exe
 - RuntimeBroker.exe
 - MicrosoftEdgeCP.exe
 - MicrosoftEdgeCP.exe
 - MicrosoftEdge.exe
 - browser broker.exe
 - ...
 - svchost.exe
 - spoolsv.exe
 - MsMpEng.exe
 - SearchIndexer.exe
 - Isass.exe
- + winlogon.exe
 - dwm.exe
- explorer.exe
 - iexplore.exe
- OneDrive.exe



기본 프로세스의 주요 변화

- 추가 내용
 - MS Edge 브라우저 관련 프로세스 → svchost.exe 하위에 존재
 - ✓ RuntimeBroker.exe
 - ✓ MicrosoftEdgeCP.exe
 - ✓ MicrosoftEdge.exe
 - ✓ brower_broker.exe
 - OneDrive 관련 프로세스 추가
 - ✓ OneDrive를 이용한 클라우드 서비스 지원 → 탐색기에서 바로 접근 가능



파일시스템 (Filesystem)

- 파일시스템
 - NTFS 그대로 사용
- 볼륨 할당
 - 부트 볼륨 크기 변화
 - √ 100MB → 500MB

Partitioning style: MBR			
Name	Ext.	Size Attr.	1st sector 🔷
🚣 Partition 1	NTFS	500 MB	2048
🚣 Partition 2	NTFS	59.5 GB	1026048
Start sectors		1.0 MB	0
Unpartitionable space		1.0 MB	125827072



파일시스템 로그 (Filesystem Logs)

- **로그 경로 →** 변화 없음!!
 - ₩\$LogFile
 - ₩\$Extend₩\$UsnJrnl:\$J
- 분석 도구 → 분석 잘됨!!
 - NTFS LogTracker (△)
 - X-Ways Forensics (O)
 - EnCase Forensic (O)



프리패치 (Prefetch)

- 프리패치 경로 → 변화 없음!!
 - %SystemRoot%₩Prefetch
- 데이터 구조 → 변경됨!!
 - 압축 사용
 - ✓ 압축 해제 : RtlDecompressBufferEx()
 - ✓ 압축 알고리즘: COMPRESSION_FORMAT_XPRESS_HUFF (XPRESS HUFFMAN)
 - ✓ 윈도우 8.1 슈퍼패치에서 사용 (MEMO/MEMo → MAM)
 - 압축 확장
 - ✓ 슈퍼패치만 압축 → 프리패치+ 슈퍼패치 모두 압축
 - http://blog.digital-forensics.it/2015/06/a-first-look-at-windows-10-prefetch.html (w10pfdecomp.py)
 - https://github.com/libyal/libagdb/blob/master/documentation/Windows%20SuperFetch%20%28DB%29%20format.asciidoc

CMD,E	XE-4	IA81	B36	4. pf	X												
	0	1	2	3	4	5	6	7	8	9	A	В	Ç	D	E	F	0123456789ABCDEF
0000h:	4D	41	4D	04	CC	20	00	00	94	Α7	95	AΒ	A8	A8	9B	0B	MAM
0010h:	A9	08	BA	00	99	A8	ВВ	0B	Α9	В7	В9	ВВ	99	08	9A	A8	
0020h:	99	A7	ΒA	AA	99	A8	AB	0B	88	87	88	9A	89	87	88	89	
0030h:	9A	87	98	98	89	07	08	ВВ	9A	07	В9	В9	AA	08	ВВ	BB	
0040h:	99	08	0B	В9	AA	В7	BA	BB	99	08	BB	ВВ	Α9	08	0B	BB	
0050h:	В9	В7	0B	A0	В8	В7	0B	A0	В8	В8	0B	ΑO	В8	07	0B	A0	
0060h:	B8	В8	ВВ	A0	A8	07	0A	A0	В9	08	0A	во	В8	07	09	BB	
0070h:	B8	08	0A	A0	09	A8	09	во	В9	80	0B	ВВ	09	08	0A	B0	
0080h:	B8	08	0A	B0	A8	B8	08	8A	0B	00	00	00	00	00	00	00	
0090h:	00	00	00	00	00	00	00	во	78	00	0B	00	00	00	00	00	x
00A0h:	97	06	B2	0B	00	00	0B	во	96	00	07	00	00	00	0B	BB	
00B0h:	87	0B	0B	00	00	00	08	A0	87	ВА	BA	ВВ	00	00	во	90	
00C0h:	88	99	8B	0B	Α9	B0	90	80	87	0A	89	0B	ВВ	00	во	70	p
00D0h:	87	A8	В9	00	00	00	90	80	A8	AΒ	97	0B	00	00	AΒ	80	
00E0h:	A7	0B	A0	00	00	00	A0	00	90	00	0A	0A	00	0A	ΑO	00	



레지스트리 하이브 (Hives)

• 하이브 파일 경로, 구조 → 변화 없음!!

유형	윈도우 10 경로
User Account	%UserProfile\NTUSER.DAT %UserProfile\AppData\Local\Microsoft\Windows\UsrClass.dat
SYSTEM Account	%SystemRoot%\System32\config\systemprofile\NTUSER.DAT
LocalService Account	%SystemRoot%\ServiceProfile\LocalService\NTUSER.DAT
NetworkService Account	%SystemRoot%\ServiceProfile\NetworkService\NTUSER.DAT
BBI, BCD-Template COMPONENT, DEFAULT DRIVERS, ELAM, FP SAM, SECURITY SOFTWARE, SYSTEM	%SystemRoot%\System32\config\####
RegBack	%SystemRoot%\System32\config\RegBack\####
AmCache	%SystemRoot%\appcompat\Programs\Amcache.hve
Package(App) Setting	%UserProfile%\AppData\Local\Packages\(AppName)\Settings\settings.dat
Package(App) Config	%UserProfile%\AppData\Local\Packages\(AppName)\ActivationStore\ActivationStore.dat



링크 파일 (LNK)

• 링크 파일 경로, 구조 → 변화 없음!!

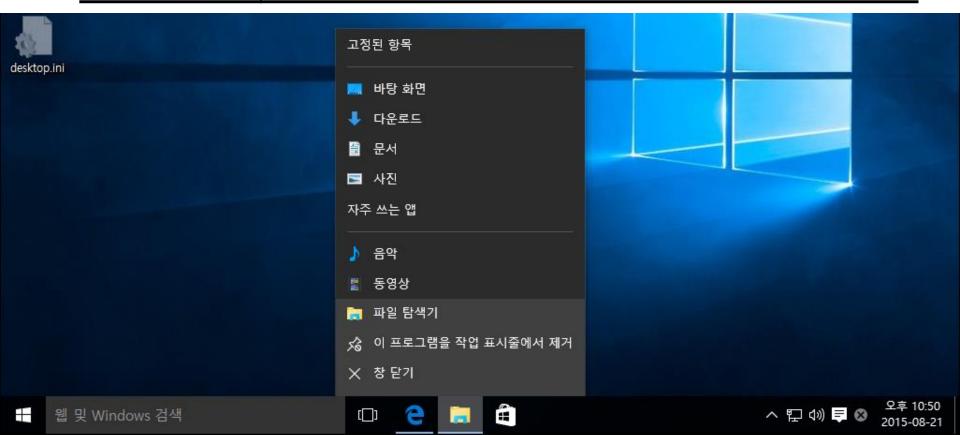
유형	윈도우 10 경로
Start Menu Places	\ProgramData\Microsoft\Windows\Start Menu Places*.lnk
Start Menu	\ProgramData\Microsoft\Windows\Start Menu\Programs**.Ink \Users\Default\AppData\Roaming\Microsoft\Windows\Start Menu\Programs**.Ink %UserProfile%\AppData\Roaming\Microsoft\Windows\Start Menu\Programs**.Ink %ServiceProfile%\AppData\Roaming\Microsoft\Windows\Start Menu\Programs**.Ink
WinX Group	\Users\Default\AppData\Local\Microsoft\Windows\WinX\Group#*.lnk %UserProfile%\AppData\Local\Microsoft\Windows\WinX\Group#*.lnk %ServiceProfile%\AppData\Local\Microsoft\Windows\WinX\Group#*.lnk
Quick Launch	\Users\Default\AppData\Local\Microsoft\Internet Explorer\Quick Launch*.Ink %UserProfile%\AppData\Local\Microsoft\Internet Explorer\Quick Launch*.Ink %ServiceProfile%\AppData\Local\Microsoft\Internet Explorer\Quick Launch*.Ink
Send To	\Users\Default\AppData\Roaming\Microsoft\Windows\SendTo*.lnk %UserProfile%\AppData\Roaming\Microsoft\Windows\SendTo*.lnk %ServiceProfile%\AppData\Roaming\Microsoft\Windows\SendTo*.lnk
Application(App) Shortcuts	%UserProfile%\AppData\Local\Microsoft\Windows\Application Shortcuts*.lnk
Recent	%UserProfile\AppData\Roaming\Microsoft\Windows\Recent*.lnk
Links	%UserProfile%\Links*.lnk



점프 목록 (Jump List)

■ **점프 목록 경로, 구조 →** 변화 없음!!

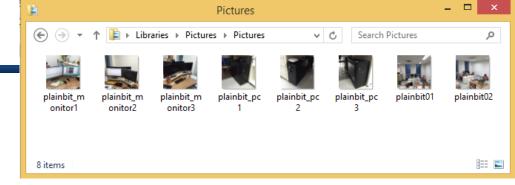
유형	윈도우 10 경로
Automatic	%UserProfile%\AppData\Roaming\Microsoft\Windows\Recent\AutomaticDestinations
Custom	%UserProfile%\AppData\Roaming\Microsoft\Windows\Recent\CustomDestinations



썸네일 캐시 (ThumbCache)

- **썸네일 캐시 경로 →** 변화 없음!!
 - %UserProfile%₩AppData₩Local₩Microsoft₩Windows₩Explorer
- ► 썸네일 캐시 파일 → 구조 약간 변화, 기존 도구 사용에 지장 없음!!

윈도우 8.1	윈도우 10
thumbcache_16.db	thumbcache_16.db
thumbcache_32.db	thumbcache_32.db
thumbcache_48.db	thumbcache_48.db
thumbcache_96.db	thumbcache_96.db
thumbcache_256.db	thumbcache_256.db
thumbcache_1024.db	thumbcache_768.db
thumbcache_1600.db	thumbcache_1280.db
thumbcache_idx.db	thumbcache_1920.db
thumbcache_sr.db	thumbcache_2560.db
thumbcache_exif.db	thumbcache_idx.db
thumbcache_wide.db	thumbcache_sr.db
thumbcache_wide_alternate.db	thumbcache_exif.db
	thumbcache_wide.db
	thumbcache_wide_alternate.db
	thumbcache_custom_stream.db

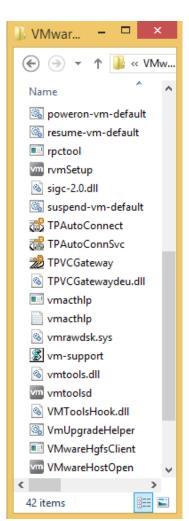




아이콘 캐시 (IConCache)

- 아이콘 캐시 경로 → 변화 없음!!
 - %UserProfile%₩AppData₩Local₩**IconCache.db (기존)**
 - %UserProfile%\pi\AppData\pi\Local\pi\Microsoft\pi\Windows\pi\Explorer\pi\iconcache*
- 아이콘 캐시 파일 → 구조 변화 없음!!

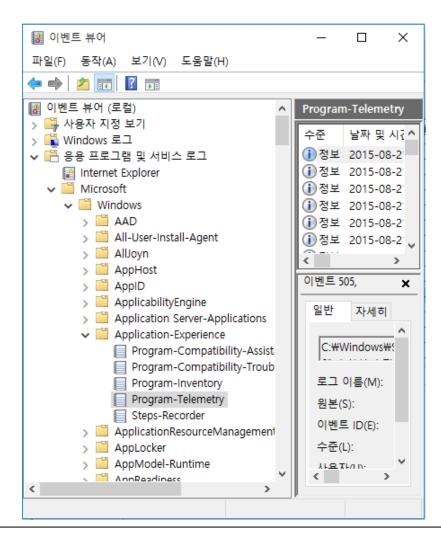
윈도우 8.1	윈도우 10
iconcache_16.db	iconcache_16.db
iconcache_32.db	iconcache_32.db
iconcache_48.db	iconcache_48.db
iconcache_96.db	iconcache_96.db
iconcache_256.db	iconcache_256.db
iconcache_1024.db	iconcache_768.db
iconcache_1600.db	iconcache_1280.db
iconcache_idx.db	iconcache_1920.db
iconcache_sr.db	iconcache_2560.db
iconcache_exif.db	iconcache_idx.db
iconcache_wide.db	iconcache_sr.db
iconcache_wide_alternate.db	iconcache_exif.db
	iconcache_wide.db
	iconcache_wide_alternate.db
	iconcache_custom_stream.db





이벤트 로그 (Event Logs)

- 이벤트 로그 경로 → 변화 없음!!
 - %SystemRoot%₩System32₩winevt₩Logs₩*.evtx
- 주요 이벤트 로그
 - Application.evtx
 - Security.evtx
 - System.evtx
 - Microsoft-Windows-Application-*.evtx
 - Microsoft-Windows-AppXDeployment*.evtx
 - Microsoft-Windows-DateTimeControlPanel*.evtx
 - Microsoft-Windows-DeviceSetup*.evtx
 - Microsoft-Windows-Kernel-Pnp/Device*.evtx
 -
- Sysinternale SysMon (System Monitor)!!





휴지통 (\$Recycle.Bin)

- 휴지통 경로 → 변화 없음!!
 - ₩\$Recycle.Bin₩[SID]
- 휴지통 파일 → 구조 일부 변화!!
 - \$R: 삭제된 파일 데이터
 - \$I: 삭제 정보 → 일부 구조 변경

```
X
 ■ 명령 프롬프트
                                                    132 $IAAC5E2.txt
           오후 09:36
2015-08-15
2015-08-15
           오후 09:36
                                  138 $IEH8TRL.chm
2015-08-15
           오후 09:36
                                  138 $IESMOHY.exe
           오후 09:36
2015-08-15
           오후 09:34
2015-08-15
                                2.009 $RAAC5E2.txt
2015-08-15
           오후 09:34
                               72.154 $REH8TRL.chm
2015-08-15
           오후 09:34
                             2,508,432 $RESMOHY.exe
           오후 09:36
                        <DIR>
2015-08-15
                                      $RMMS4ND
              7개 파일
                               2.583.117 바이트
              1개 디렉터리 53,789,929,472 바이트 남음
c:\$Recycle.Bin\$-1-5-21-1624511600-1441245453-352339348-1001>
```

- ✓ 파일명에 따라 가변 크기를 가짐 (이전에는 544바이트로 고정)
- ✔ Resident 파일...?



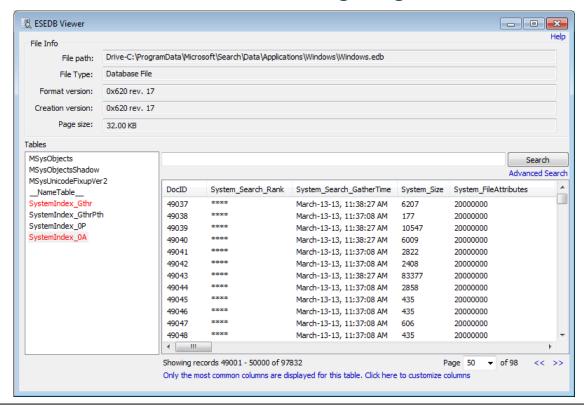
볼륨 섀도 복사본 (VSC; Volume Shadow Copy)

- VSC 경로 → 변화 없음!!
 - ₩System Volume Information
- **VSC 파일** → 구조 변화 없음!!
 - vssadmin 명령 그대로~!!
- 안티포렌식 기법의 일반화@
 - VSC에 대한 정책을 마련하여 관리할 필요가 있음
- · 관리자: 명령 프롬프트 Microsoft Windows [Version 10.0.10240] (c) 2015 Microsoft Corporation. All rights reserved. :\Windows\system32>vssadmin list shadows vssadmin 1.1 - 볼륨 섀도 복사본 서비스 관리 명령줄 도구 (C) Copyright 2001-2013 Microsoft Corp. 섀도 복사본 세트 ID의 콘텐츠: {c57e5931-e197-400f-84ef-d9c5c39156f9} 다음 작성 시간에 1 섀도 복사본 포함: 2015-08-21 오후 11:24:30 섀도 복사본 ID: {c20cafd8-8f83-4643-939b-86491483f506} 원본 볼륨: (C:)\\rangle \rangle \rangle Volume{a81ae2de-0000-0000-0000-501f00000000}\\rangle 컴퓨터: DESKTOP-1047T6C 서비스 컴퓨터: DESKTOP-1047T6C 공급자: 'Microsoft Software Shadow Copy provider 1.0' 형식: ClientAccessibleWriters 특성: Persistent, Client-accessible, No auto release, Differential, 자동 복구됨



윈도우 인덱싱 서비스 (Windows Indexing Service)

- **파일 경로 →** 변화 없음!!
 - ₩ProgramData₩Microsoft₩Search₩Data₩Applications₩Windows₩Windows.edb
- 파일 구조 → ESE(Extensible Storage Engine) DB

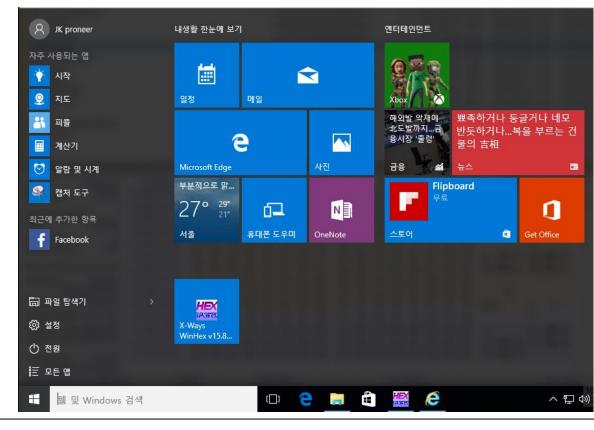




알림 (Notification)

- Modern UI (Metro UI) 앱 알림
 - %UserProfile%₩AppData₩Local₩Microsoft₩Windows₩Notifications₩appdb.dat
 - 캐시 형태로 저장, 아직 구조 역분석 (X) → XML 카빙(byte-level)을 통해 정보 획득



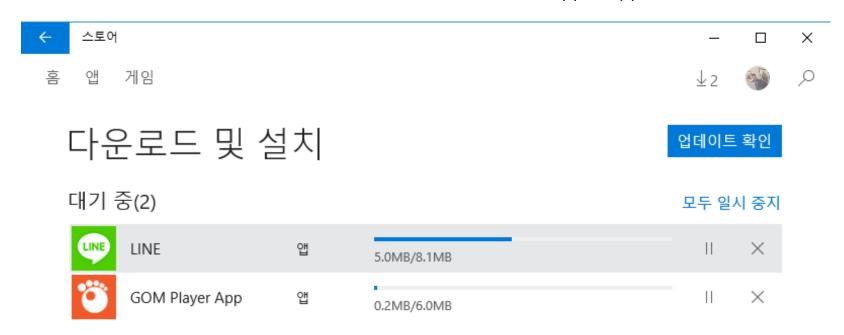




윈도우 스토어 (Windows Store)

- 윈도우 앱 스토어

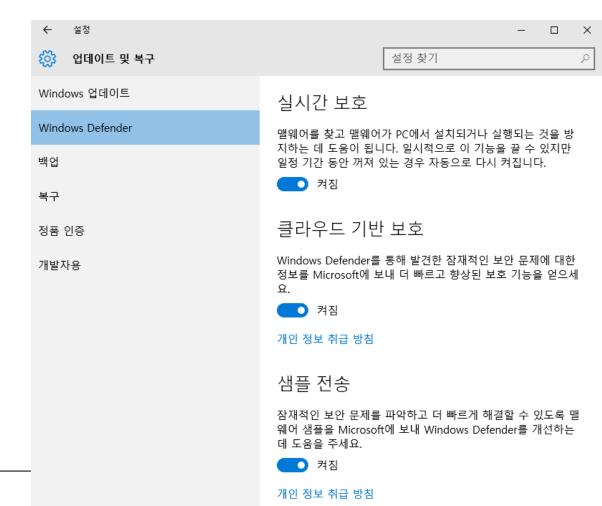
 - HKLM₩SOFTWARE₩Microsoft₩Windows₩CurrentVersion₩Appx₩AppxAllUserStore





윈도우 디펜더 (Windows Defender)

- 윈도우 AV
 - ₩ProgramData₩Microsoft₩Windows Defender
 - 윈도우 10에서 더욱 강화!!
 - ✓ 실시간 보호
 - ✓ 클라우드 기반 보호
 - ✓ 샘플 전송



Microsoft Edge

Edge Browser

- Edge 홈 폴더

 - 브라우저 설정, 캐시 파일, 쿠키 파일 저장

■ Edge 아티팩트

- %UserProfile%\pipData\Local\Microsoft\Windows\WebCache\WebCacheV01.dat
- 히스토리, 쿠키 정보, 다운로드 목록 등

ContainerId	Director
Containerid	Directory /
13	C:\Users\proneer\AppData\Local\Packages\microsoft.microsoftedge_8wekyb3d8bbwe\AC\#!001\MicrosoftEdge\Cache\
◎ 14	C:\Users\proneer\AppData\Local\Packages\nicrosoft.microsoftedge_8wekyb3d8bbwe\AC\#!001\MicrosoftEdge\Cookies\
16	C:\Users\proneer\AppData\Local\packages\microsoft.microsoftedge_8wekyb3d8bbwe\AC\#!001\MicrosoftEdge\History\
24	C:\Users\proneer\AppData\Local\packages\nicrosoft.microsoftedge_8wekyb3d8bbwe\AC\#!001\MicrosoftEdge\User\Default\DOMStore\
15	C:\Users\proneer\AppData\Local\packages\microsoft.microsoftedge_8wekyb3d8bbwe\AC\#!002\MicrosoftEdge\Cache\
17	C:\Users\proneer\AppData\Local\packages\microsoft.microsoftedge_8wekyb3d8bbwe\AC\#!002\MicrosoftEdge\Cookies\
25	C:\Users\proneer\AppData\Local\packages\microsoft.microsoftedge_8wekyb3d8bbwe\AC\#!002\MicrosoftEdge\History\
19	C:\Users\proneer\AppData\Local\packages\nicrosoft.microsoftedge_8wekyb3d8bbwe\AC\#!002\MicrosoftEdge\User\Default\DOMStore\
9	C:\Users\proneer\AppData\Local\packages\microsoft.microsoftedge_8wekyb3d8bbwe\AC\MicrosoftEdge\Cache\
20	C:\Users\proneer\AppData\Local\packages\microsoft.microsoftedge_8wekyb3d8bbwe\AC\MicrosoftEdge\Cookies\
◎ 18	C:\Users\proneer\AppData\Local\packages\microsoft.microsoftedge_8wekyb3d8bbwe\AC\MicrosoftEdge\History\
© 21	C:\Users\proneer\AppData\Local\Packages\microsoft.microsoftedge 8wekyb3d8bbwe\AC\MicrosoftEdge\User\Default\DownloadHistory



WebCache

- WebCache 경로
 - %UserProfile%₩AppData₩Local₩Microsoft₩Windows₩WebCache₩WebCacheV01.dat

■ WebCache 기록되는 정보

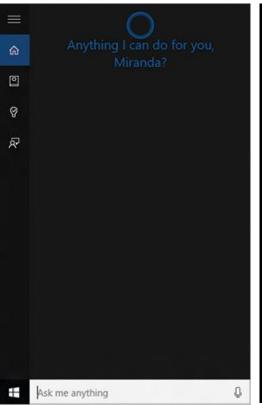
- Internet Explorer (10+)
- Package: microsoft.accountscontrol
- Package: microsoft.microsoftedge
- Package: microsoft.bingnews
- Package: microsoft.office.onenote
- Package: microsoft.windows.authhost
- Package: microsoft.windows.cloudexperiencehost
- Package: microsoft.windows.cortana
- Package: microsoft.windowscommunicationapps
- Package: microsoft.windowsstore



Cortana

- 윈도우 개인 비서 (created by Windows Phone 8.1)

 - 음성 인식, Remind 기능, ...





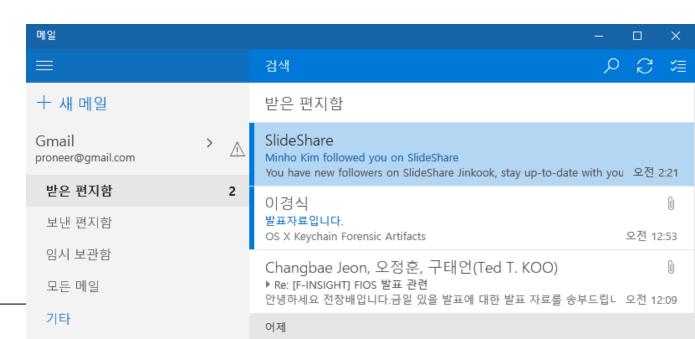


Email (Mail Application)

- 이메일 BODY
 - %UserProfile%₩AppData₩Local₩Comms₩Unistore₩data₩*₩*.dat
 - TXT, HTML 형식으로 저장

이메일 METADATA (ESE DB)

- %UserProfile%₩AppData₩Local₩Comms₩UnistoreDB₩store.vol
- 이메일 헤더
- 주소록, 연락처
- 첨부파일 정보
-



추가 연구 주제

추가 연구 주제



윈도우 10에서 뭘 해보지?

- OneDrive 이벤트 정리
- 윈도우 10 앱(App Packages) 흔적 정리
 - OneDrive, OneNote, Skype, Facebook, Twitter, Windows Live, Maps, Excel, Word, PowerPoint, ...
- 사건 유형 별 행위 아티팩트 분석
 - 프로그램(EXE) 실행
 - 문서 파일 실행
 - 정보유출 아티팩트 분석
 - 침해사고 아티팩트 분석
 -

질문 및 답변





뒷풀이 장소



