

윈도우 8은 포렌식도 다르다?

Windows 8 Forensics

ASEC / A-FIRST

김진국

- 01 새로운 보안 기능
- 02 포렌식 아티팩트 변화
- 03 새로운 포렌식 아티팩트
- 04 실전 악성코드 포렌식

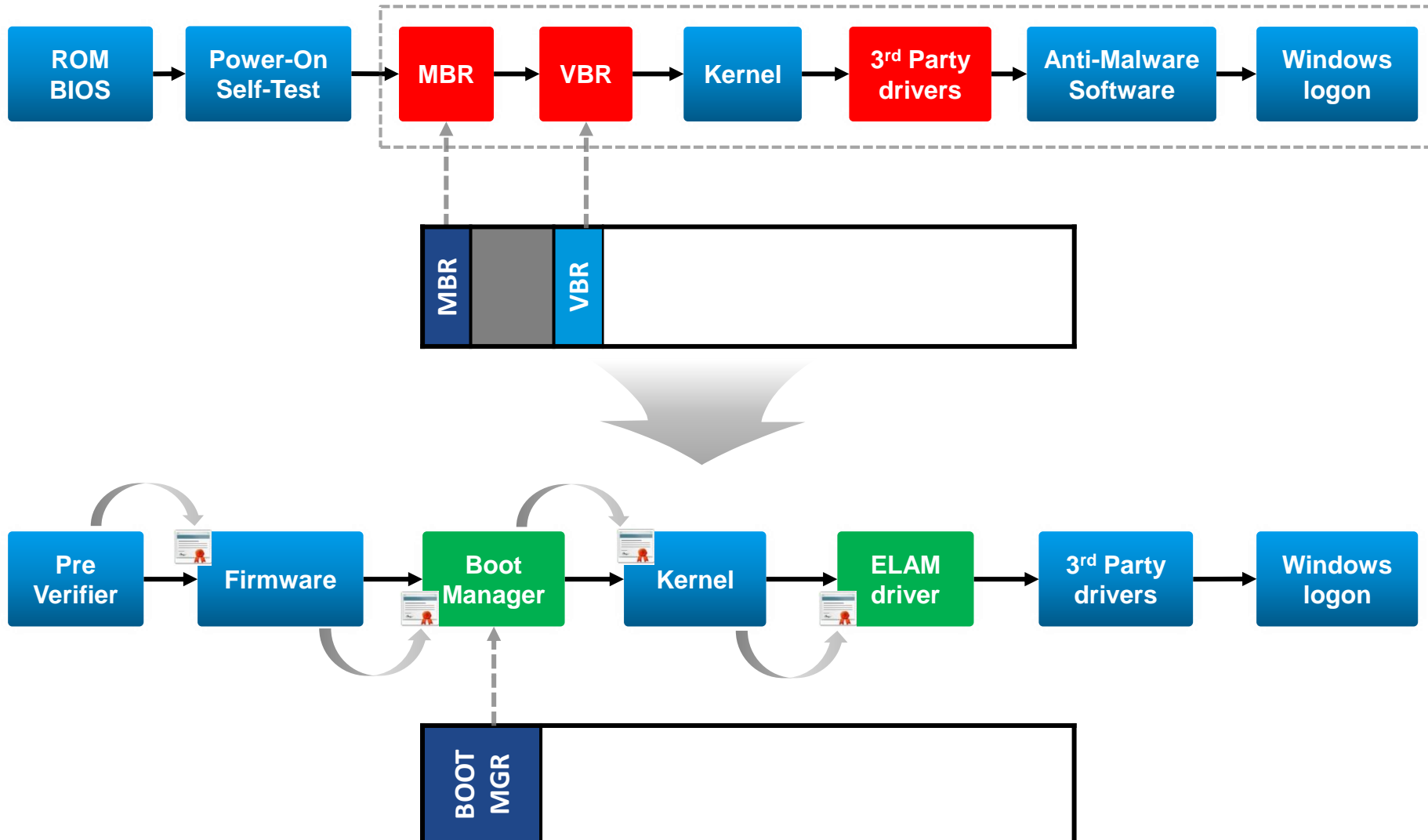
01

새로운 보안 기능

1. 안전한 부팅
2. 신중한 부팅
3. 새로운 로그인 인증 방식
4. 윈도우 디펜더
5. 스마트스크린 필터
6. 익스플로잇 방지 기법

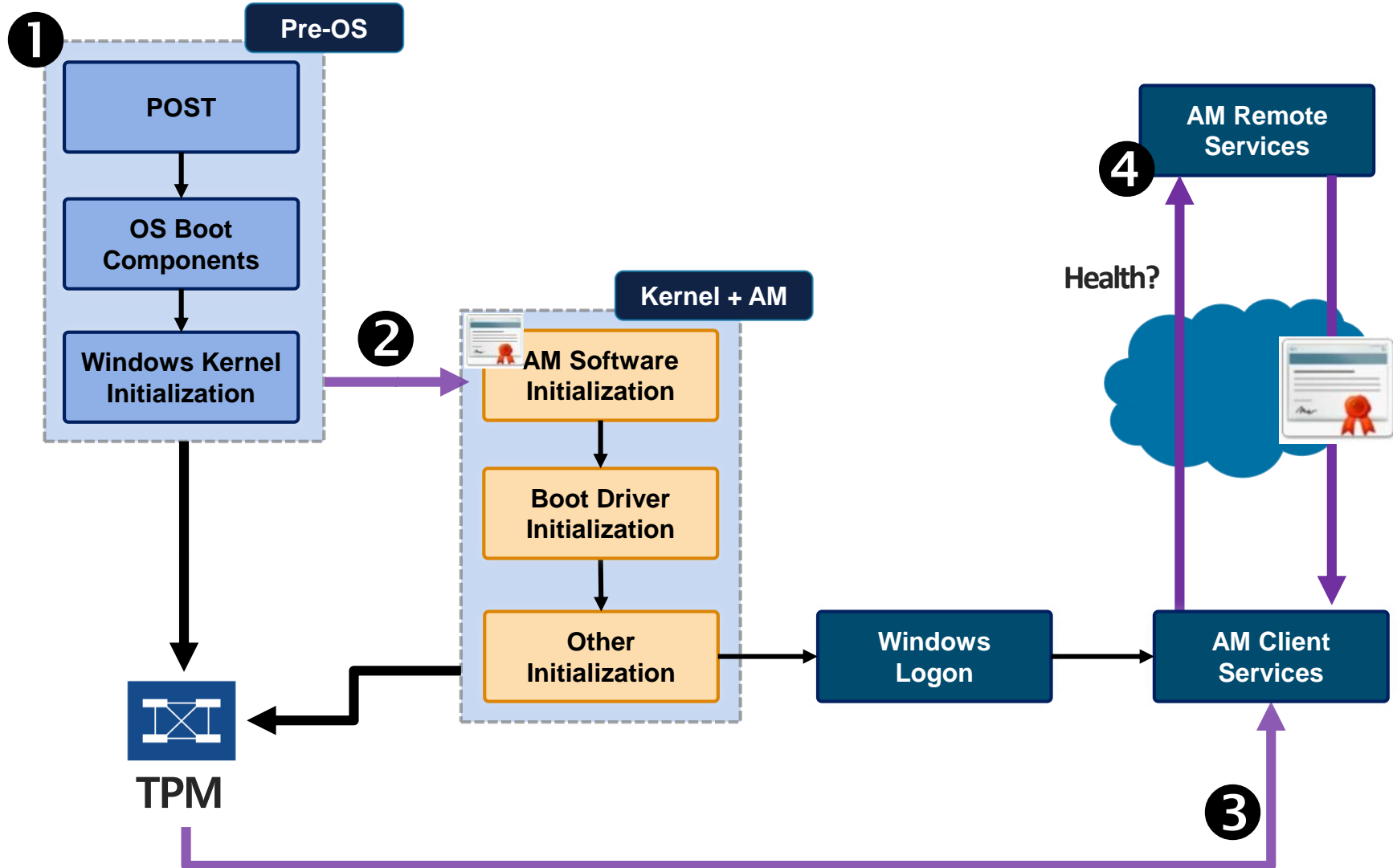
1. 안전한 부팅

- ELAM(Early Launch Anti-Malware)을 사용한 안전한 부팅(Secured Boot)



2. 신중한 부팅

- 원격 증명(Remote Attestation)을 이용한 신중한 부팅(Measured Boot)



3. 새로운 도

- 사진 암호

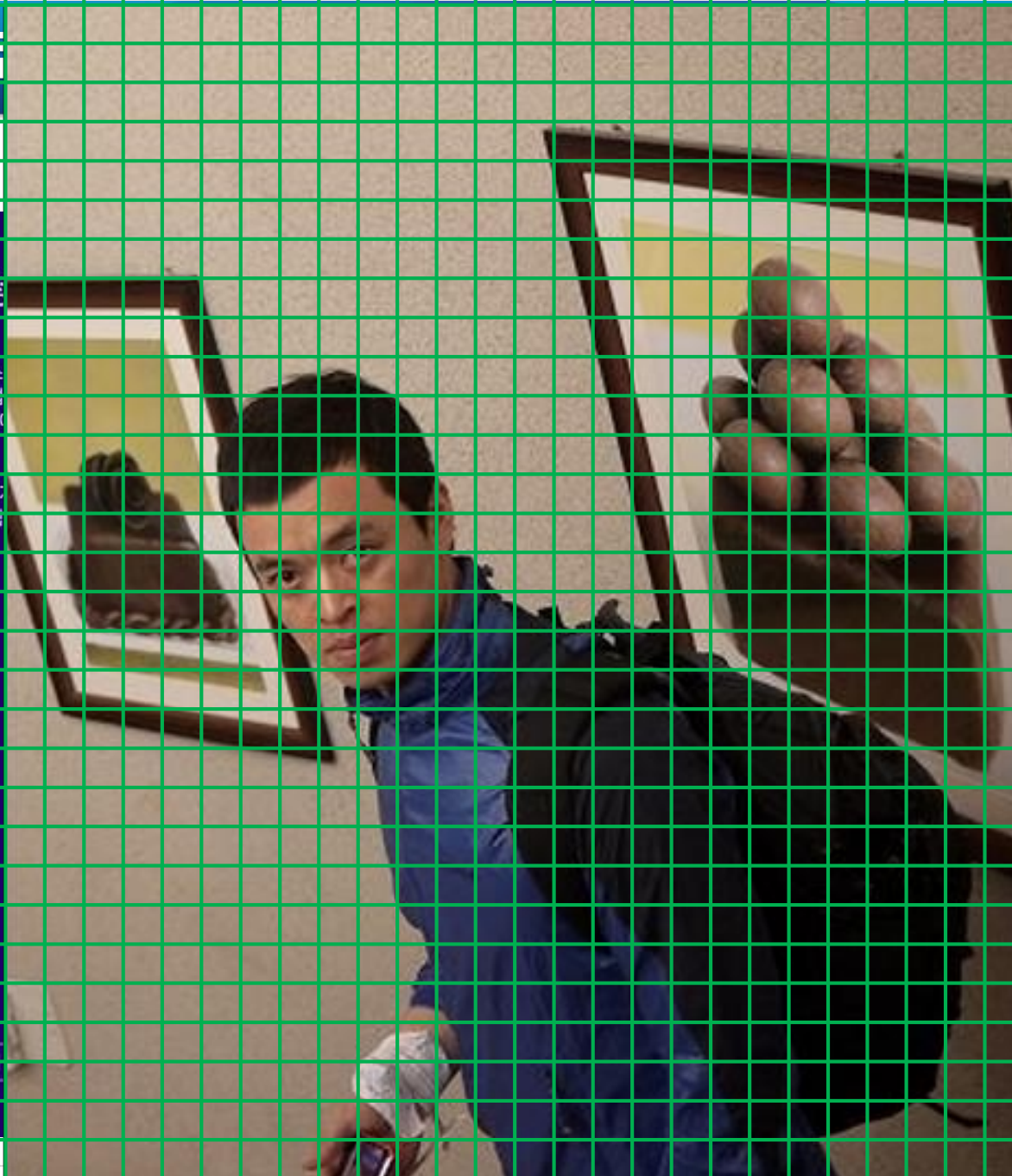
제스처 설정

사진에 세 개의 제스처의 특정 부분을 탭 선택 그리기를 조합합니다.

그려진 제스처의 크기가 사진 암호가 됩니다.

1 2

새로 만들기



3. 새로운 로그인 인증 방식

- PIN 암호

PIN 만들기

4자리 숫자로 된 PIN을 사용하면 PC에 빠르고 간편하게 로그인할 수 있습니다.

PIN 입력

PIN 확인

마침

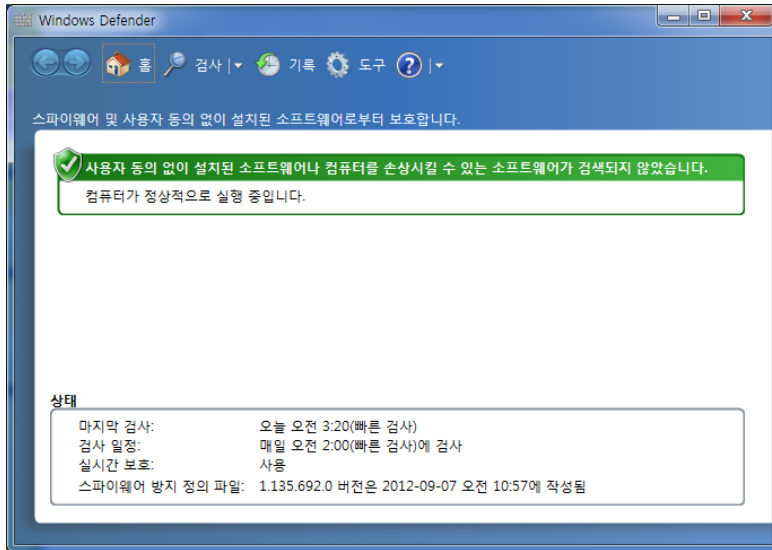
취소



4. 윈도우 디펜더

- 안티스파이웨어로 알려진 마이크로소프트 보호 솔루션

윈도우 7



- 스파이웨어 실행 방지
- 동의 없이 설치된 소프트웨어 실행 방지

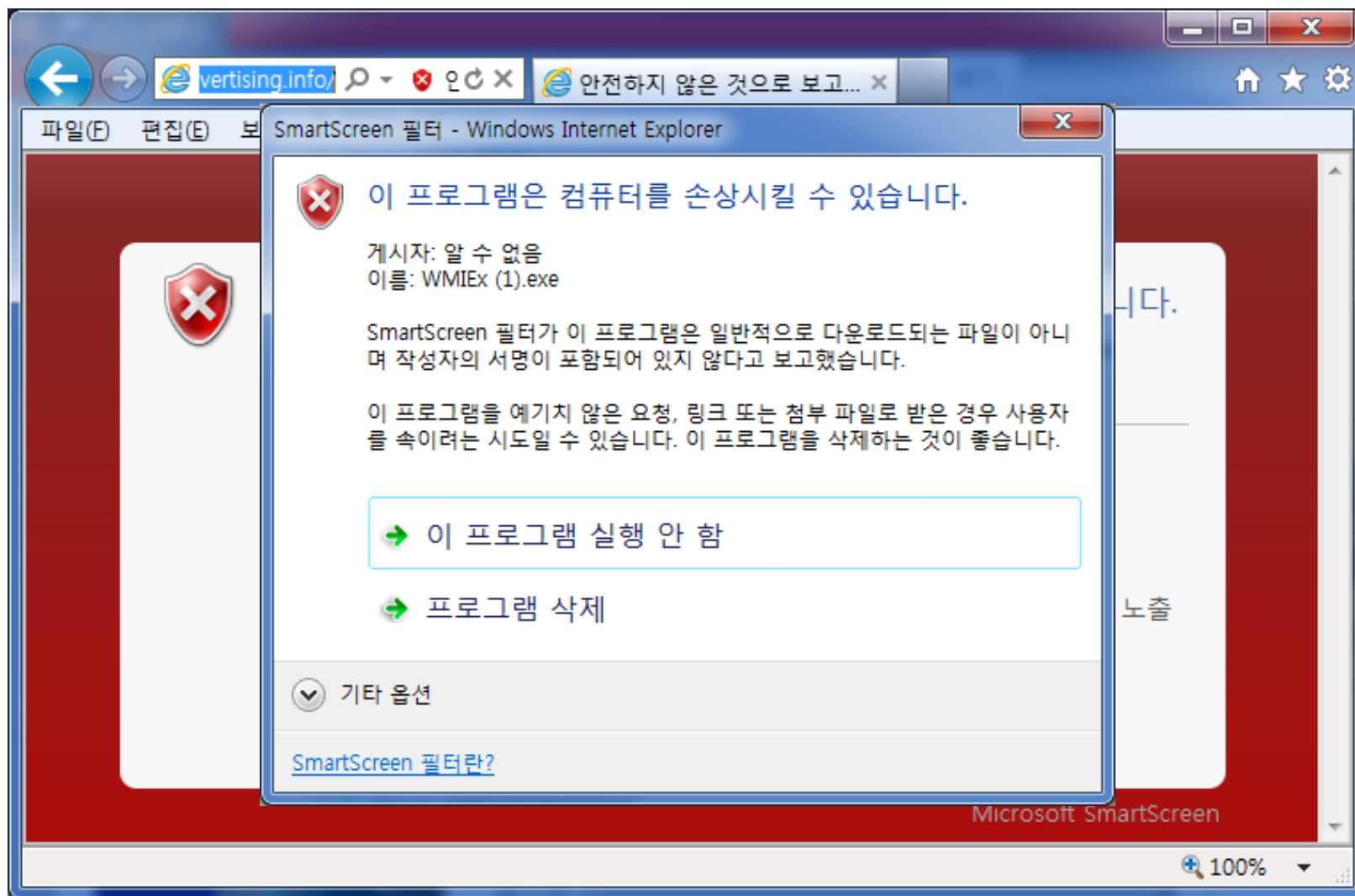
윈도우 8



- 스파이웨어 실행 방지
- 바이러스 탐지
- 행위기반 탐지
- 네트워크 침입 탐지

5. 스마트스크린 필터

- 기존 윈도우의 IE 스마트스크린 필터 (IE 8.0부터 지원)

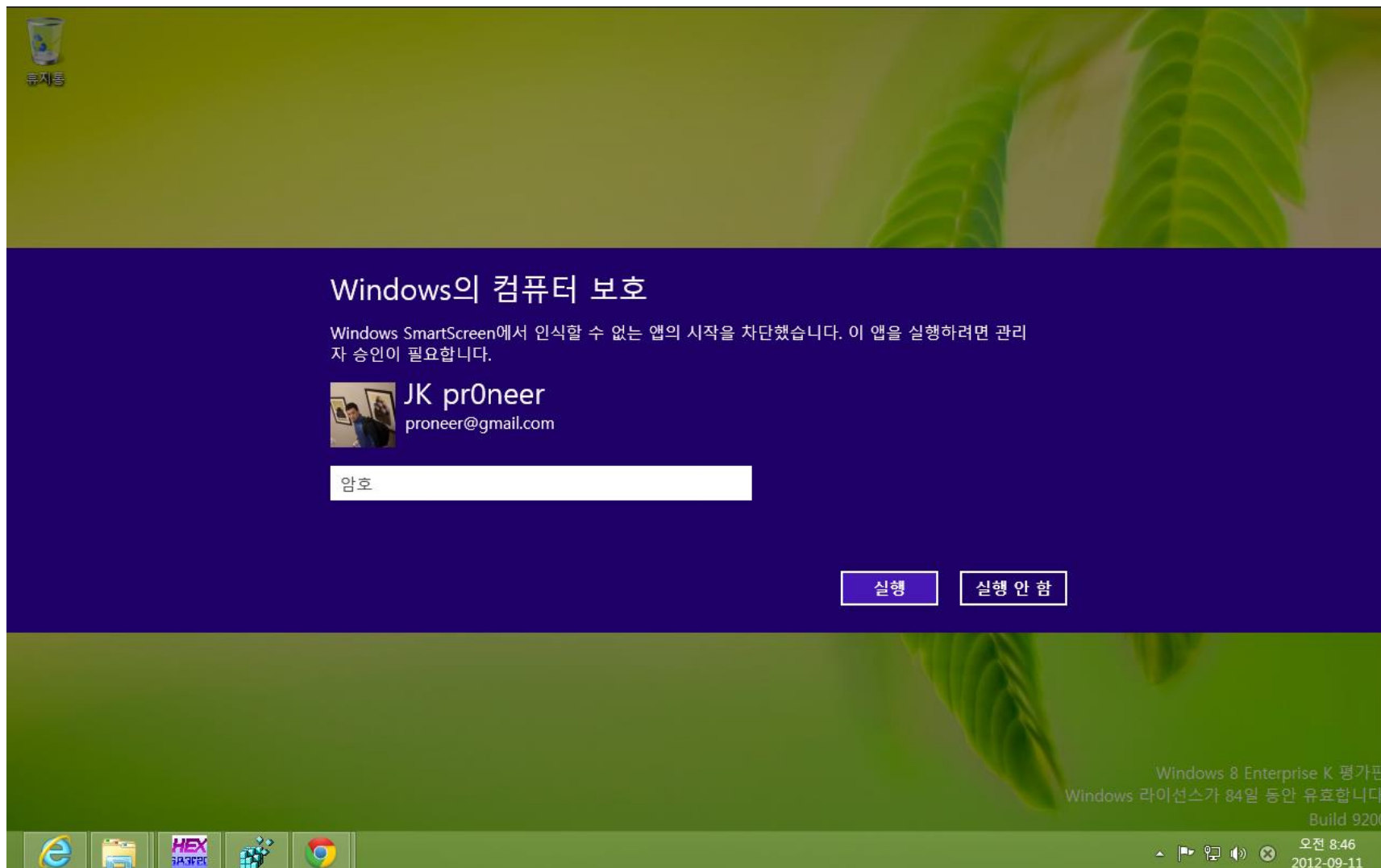


인터넷에서 다운받은
파일을 식별하는
방법은?

힌트) NTFS

5. 스마트스크린 필터

- 윈도우 8의 스마트스크린 필터 (타 웹 브라우저 지원, ADS Zone Identifier로 경고)



6. 익스플로잇 방지 기법

- 기존 윈도우의 익스플로잇 방지 기법

DEP

데이터 실행 방지(Data Execution Prevention), 윈도우 XP SP2에서 도입

ASLR

주소 공간 레이아웃 랜덤화(Address Space Layout Randomization), 윈도우 비스타부터

- 윈도우 8의 향상된 익스플로잇 방지 기법

ASLR

랜덤화 블록의 크기를 작게 하고, 랜덤 지수를 높임

Kernel

구조 변경, 무결성 체크, NX(Non-Executable) non-paged pool 등

Heap

구조 변경, 인코딩, 검증, 랜덤성 강화 등

IE 10

향상된 보호 모드(Enhanced Protected Mode) 지원

02

포렌식 아티팩트 변화

-
1. 포렌식 아티팩트 비교
 2. 물리/가상메모리
 3. 레지스트리
 4. 웹 브라우저 사용흔적
 5. 익스플로러 캐시

1. 포렌식 아티팩트 비교

윈도우 7

1	물리/가상 메모리
2	파일시스템
3	레지스트리
4	프리/슈퍼패치
5	웹 브라우저 사용흔적
6	이벤트 로그
7	링크 파일
8	휴지통 흔적
9	볼륨 새도우 복사본
10	익스플로러 캐시



윈도우 8

물리/가상 메모리
파일시스템
레지스트리
프리/슈퍼패치
웹 브라우저 사용흔적
이벤트 로그
링크 파일
휴지통 흔적
볼륨 새도우 복사본
익스플로러 캐시

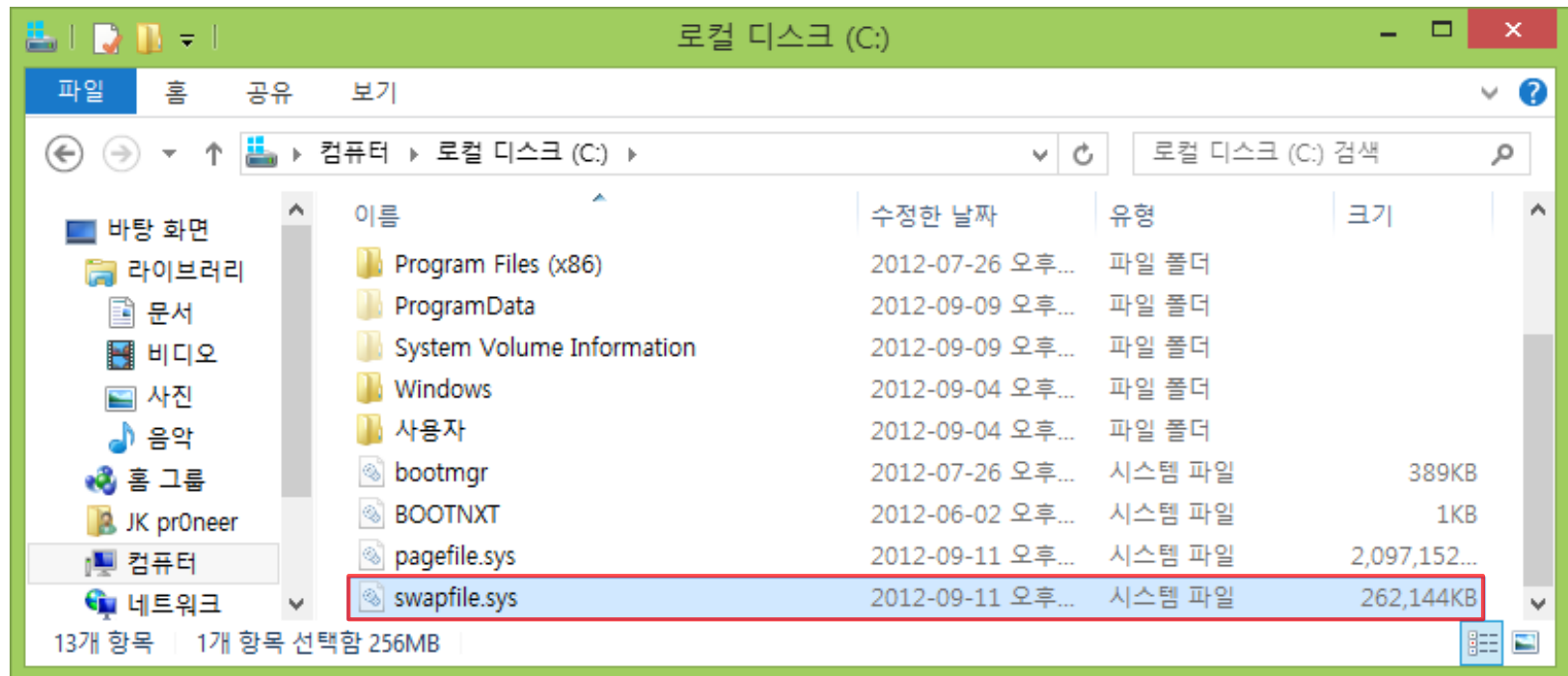
2. 물리/가상 메모리

- 물리메모리

- ✓ 메모리 구조 변경 → 기존 메모리 분석 도구로 분석 불가능

- 가상메모리

- ✓ pagefile.sys 이외에 **swapfile.sys(256 MB)** 추가



2. 물리/가상 메모리

- **swapfile.sys ?**

```
C:\Temp> strings swapfile.sys
```

```
... ..
```

```
PUBLIC=C:\Users\Public
```

```
SystemDrive=C:
```

```
SystemRoot=C:\Windows
```

```
TEMP=C:\Users\JK\AppData\Local\Packages\microsoft.windowscomm_8wekyb3d8bbwe\AC\Temp
```

```
TMP=C:\Users\JK\AppData\Local\Packages\microsoft.windowscomm_8wekyb3d8bbwe\AC\Temp
```

```
USERDOMAIN=FORENSICER
```

```
USERDOMAIN_ROAMINGPROFILE=FORENSICER
```

```
USERNAME=JK
```

```
USERPROFILE=C:\Users\JK
```

```
windir=C:\Windows
```

```
C:\Program
```

```
Files\WindowsApps\microsoft.windowscomm_16.4.4206.722_x64_8wekyb3d8bbwe\LiveComm.exe
```

```
"C:\Program
```

```
Files\WindowsApps\microsoft.windowscomm_16.4.4206.722_x64_8wekyb3d8bbwe\LiveComm.exe" -
```

```
ServerName:Microsoft.WindowsLive.Platform.Server
```

```
"C:\Program
```

```
Files\WindowsApps\microsoft.windowscomm_16.4.4206.722_x64_8wekyb3d8bbwe\LiveComm.exe"
```

```
`We
```

```
C:\Windows\SYSTEM32\ntdll.dll
```

```
C:\Windows\system32
```

```
... ..
```


3. 레지스트리

- 윈도우의 다양한 설정 정보를 담고 있는 하이브 구조의 데이터베이스

%SystemRoot%\system32\config, %UserProfile%

BCD-Template

부팅 환경 설정 데이터 (Boot Configuration Data)

COMPONENTS

설치된 컴포넌트 관리 정보

DEFAULT

제어판, 환경변수, 키보드 레이아웃, 프린터 등의 정보

SAM

로컬 계정과 그룹 정보

SECURITY

시스템 보안 정책과 권한 할당 정보

SOFTWARE

시스템 부팅과 관련 없는 시스템 전역 설정 정보

SYSTEM

시스템 부팅에 필요한 시스템 전역 설정 정보

NTUSER.DAT
UsrClass.dat

사용자 별 시스템 설정 정보

3. 레지스트리

- 새로운 레지스트리 하이브 파일

BBI

메트로 앱 이벤트, 백그라운드 작업

DRIVERS

드라이버 ID, 파일, INF 파일, 패키지 정보 (HKLM\SYSTEM\DriverDatabase)

ELAM

윈도우 디펜더 신중한(Measured) 부팅 관련 정보

Windows\System32\config								2 min. ago
Name ^	Ext. ^	Size	Created	Modified	Accessed	Attr.	1st sector	
BBI		0.5 MB	2012-07-26 14:26:37	2012-09-11 18:50:59	2012-09-11 18:50:59	SHA...	3360480	
BCD-Template		256 KB	2012-07-26 17:13:07	2012-09-04 21:03:50	2012-09-04 21:03:50	HA	104012...	
COMPONENTS		22.8 MB	2012-07-26 14:26:37	2012-09-11 08:55:49	2012-09-11 08:55:49	HA	3597432	
DEFAULT		0.5 MB	2012-07-26 14:26:37	2012-09-11 18:50:59	2012-09-11 18:50:59	HA (...)	1838032	
DRIVERS		4.5 MB	2012-07-26 17:08:10	2012-09-11 21:23:31	2012-09-11 21:23:31	HA	2027968	
ELAM		8.0 KB	2012-07-26 14:26:37	2012-07-26 16:22:17	2012-07-26 16:22:17	SHAX	104031...	

Settings.dat

메트로 앱 로컬과 로밍 상태

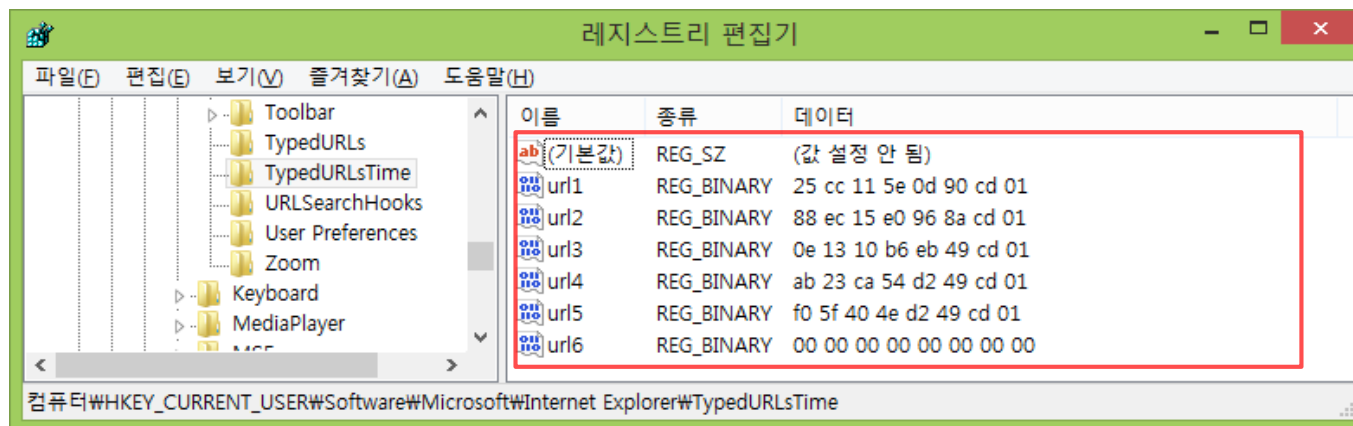
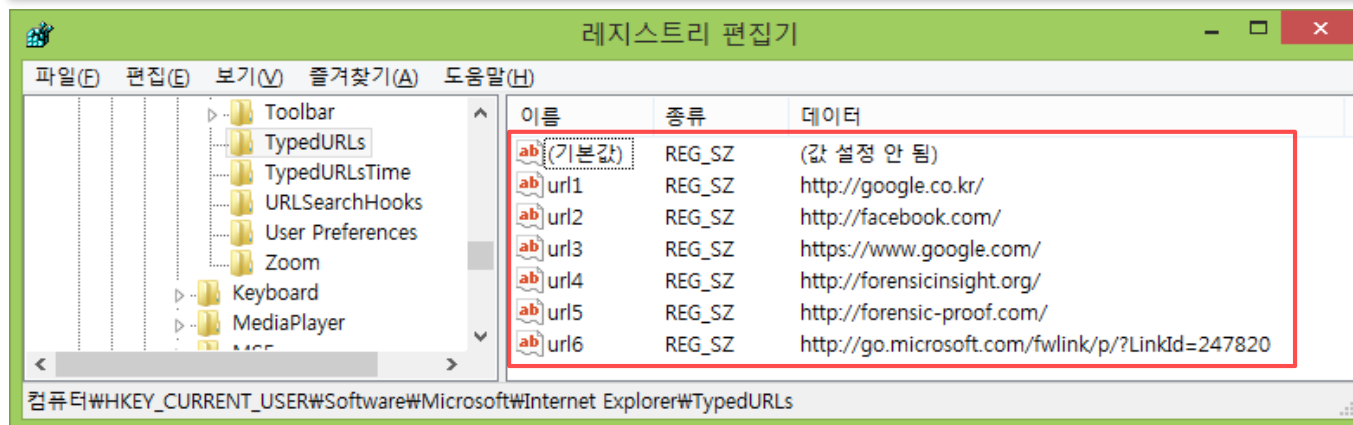
Users\prOneer\AppData\Local\Packages\Microsoft.Reader_8wekyb3d8bbwe\Settings								1 min. ago
Name ^	Ext.	Size	Created	Modified	Accessed	Attr.	1st sector	
..								
roaming.lock	lock	0 B	2012-09-04 23:37:49	2012-09-04 23:37:49	2012-09-04 23:37:49	A		
settings.dat	dat	8.0 KB	2012-09-04 23:37:49	2012-09-04 23:37:59	2012-09-10 23:17:30	A	2402856	
settings.dat.LOG1	LOG1	8.0 KB	2012-09-04 23:37:59	2012-09-04 23:37:59	2012-09-04 23:37:59	SHA	127056...	
settings.dat.LOG2	LOG2	0 B	2012-09-04 23:37:59	2012-09-04 23:37:59	2012-09-04 23:37:59	SHA		

3. 레지스트리

- 새로운 레지스트리 아티팩트

- ✓ TypedURLsTime

HKU\{SID}\Software\Microsoft\Internet Explorer\TypeURLsTime

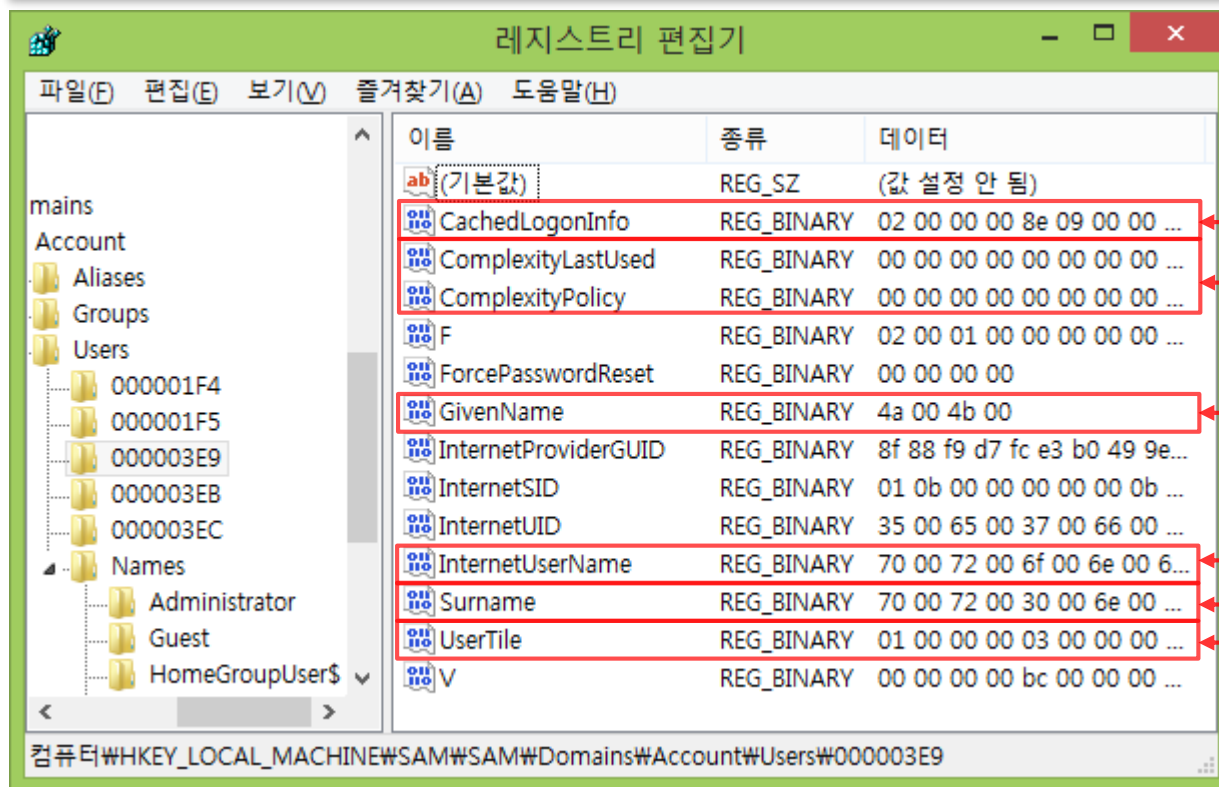


3. 레지스트리

- 새로운 레지스트리 아티팩트

- ✓ 사용자 계정 정보

HKEY_LOCAL_MACHINE\SAM\SAM\Domains\Account\Users\{RID}



암호화 Live 로그인 정보

로그온 방식

JK

proneer@gmail.com

pr0neer

사용자 프로필 사진

4. 웹 브라우저 사용흔적

- 인터넷 익스플로러 버전 9

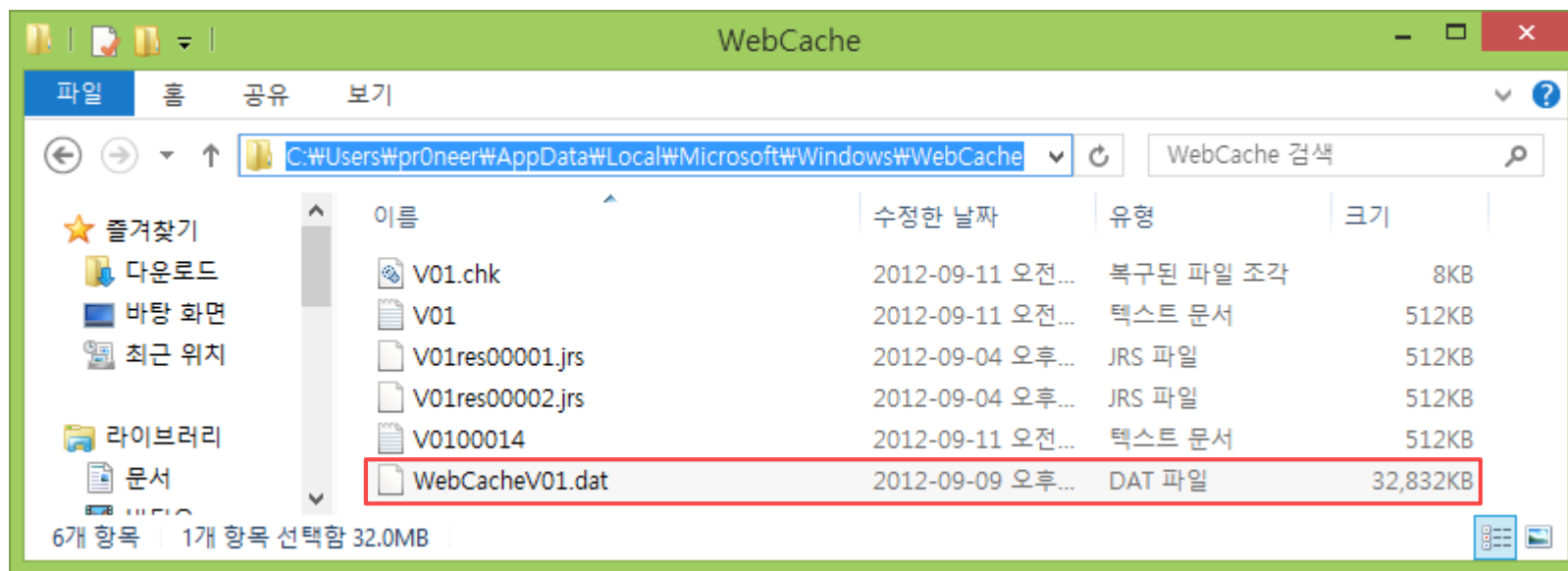
캐시	%LOCALAPPDATA%\Microsoft\Windows\Temporary Internet Files\Content.IE5\index.dat %LOCALAPPDATA%\Microsoft\Windows\Temporary Internet Files\Content.IE5\<Random>\<All Files>
히스토리	%LOCALAPPDATA%\Microsoft\Windows\History\History.IE5\index.dat %LOCALAPPDATA%\Microsoft\Windows\History\History.IE5\<period>\index.dat
쿠키	%APPDATA%\Microsoft\Windows\Cookies\index.dat %APPDATA%\Microsoft\Windows\Cookies\<All Files>
다운로드 목록	%APPDATA%\Microsoft\Windows\IEDownloadHistory\index.dat
아이콘 캐시	%LOCALAPPDATA%\Microsoft\Internet Explorer\iconcache.dat
세션 복원 정보	%LOCALAPPDATA%\Microsoft\Internet Explorer\Recovery\Active\RecoveryStore.{GUID}.dat %LOCALAPPDATA%\Microsoft\Internet Explorer\Recovery\Last Active\RecoveryStore.{GUID}.dat %LOCALAPPDATA%\Microsoft\Internet Explorer\Recovery\High\Active\RecoveryStore.{GUID}.dat %UserProfile%\AppData\Local\Microsoft\Internet Explorer\Recovery\High\Last Active\RecoveryStore.{GUID}.dat
호환성 목록	%LOCALAPPDATA%\Microsoft\Internet Explorer\IECompatData\iecompatdata.xml HKU\Software\Microsoft\Internet Explorer\BrowserEmulation\ClearableListData\UserFilter
DOM 저장소	%LOCALAPPDATA%\Microsoft\Internet Explorer\DOMStore\index.dat

4. 웹 브라우저 사용흔적

- 인터넷 익스플로러 버전 10

- ✓ index.dat가 사라짐
- ✓ 모든 브라우저 사용 흔적을 단일 캐시 파일에 기록

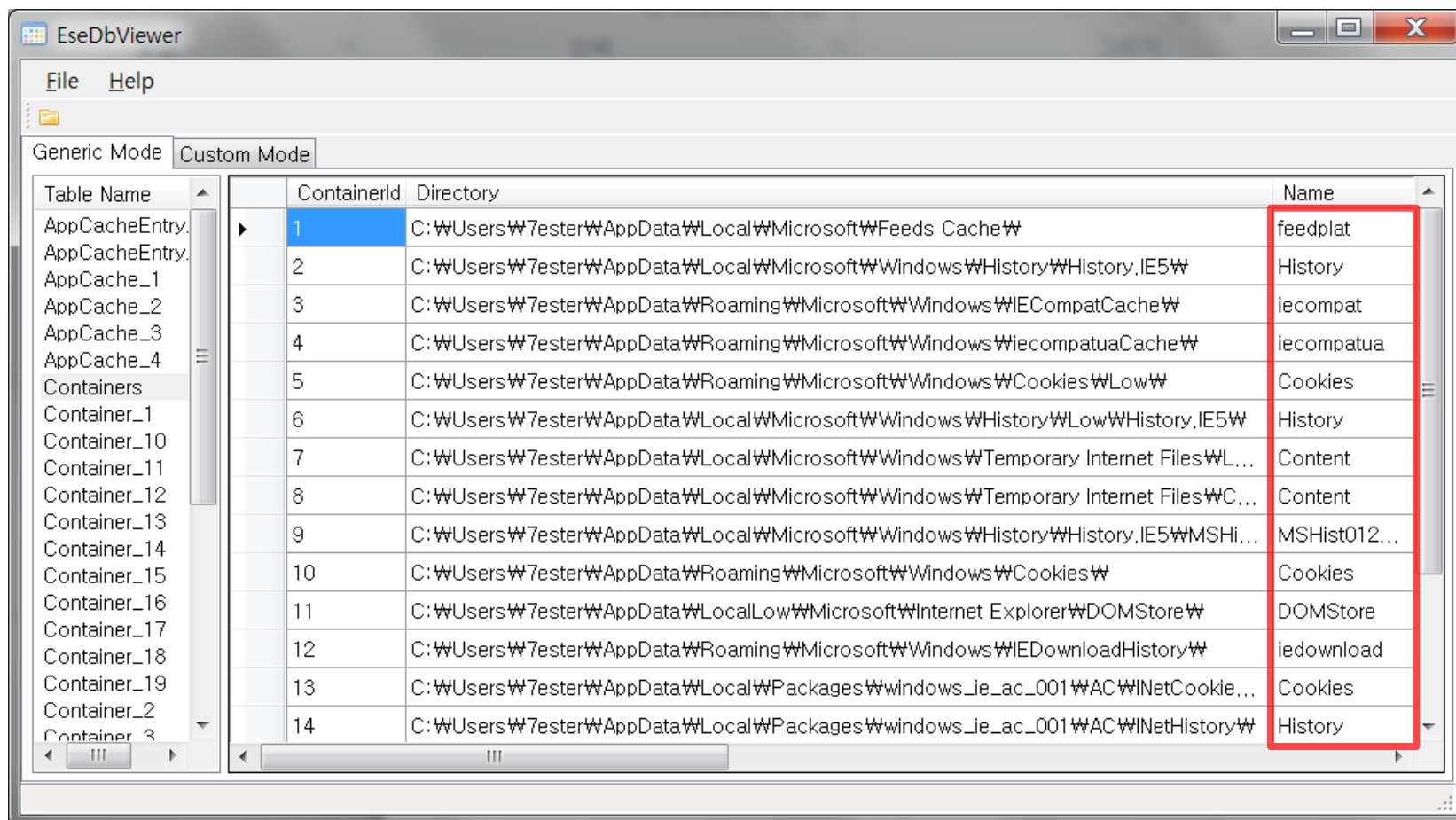
%UserProfile%\AppData\Local\Microsoft\Windows\WebCache\WebCacheV###.dat



4. 웹 브라우저 사용흔적

- WebCacheV##.dat

✓ ESE (Extensible Storage Engine) 데이터베이스 형식 (Exchange Server, AD, Live Messenger, Search)



The screenshot shows the ESEDbViewer application window. The 'Generic Mode' tab is selected. The left pane lists various containers, and the right pane displays a table of these containers. A red box highlights the 'Name' column in the table.

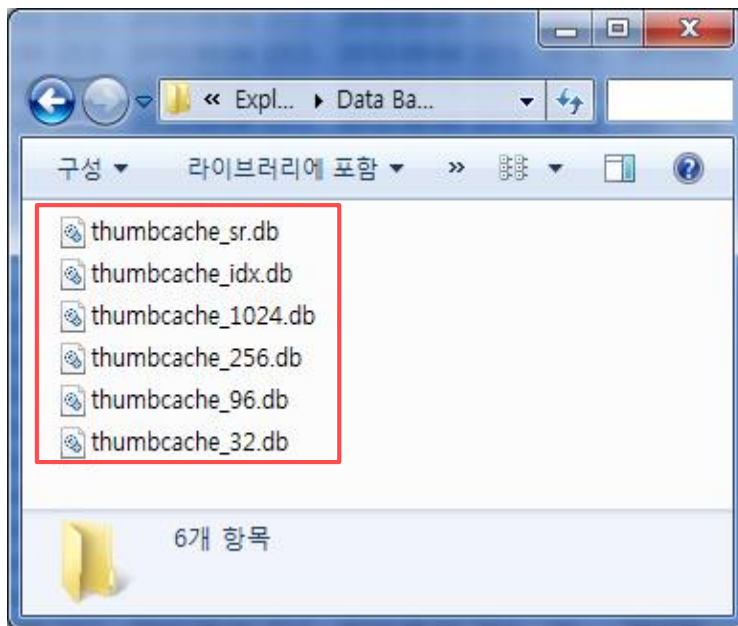
Table Name	ContainerId	Directory	Name
AppCacheEntry...	1	C:\Users\W7ester\AppData\Local\Microsoft\Feeds Cache\	feedplat
AppCacheEntry...	2	C:\Users\W7ester\AppData\Local\Microsoft\Windows\History\History.IE5\	History
AppCache_1	3	C:\Users\W7ester\AppData\Roaming\Microsoft\Windows\IECompatCache\	iecompat
AppCache_2	4	C:\Users\W7ester\AppData\Roaming\Microsoft\Windows\iecompatuaCache\	iecompatua
AppCache_3	5	C:\Users\W7ester\AppData\Roaming\Microsoft\Windows\Cookies\Low\	Cookies
AppCache_4	6	C:\Users\W7ester\AppData\Local\Microsoft\Windows\History\Low\History.IE5\	History
Containers	7	C:\Users\W7ester\AppData\Local\Microsoft\Windows\Temporary Internet Files\WL...	Content
Container_1	8	C:\Users\W7ester\AppData\Local\Microsoft\Windows\Temporary Internet Files\WC...	Content
Container_10	9	C:\Users\W7ester\AppData\Local\Microsoft\Windows\History\History.IE5\MSHI...	MSHist012...
Container_11	10	C:\Users\W7ester\AppData\Roaming\Microsoft\Windows\Cookies\	Cookies
Container_12	11	C:\Users\W7ester\AppData\LocalLow\Microsoft\Internet Explorer\DOMStore\	DOMStore
Container_13	12	C:\Users\W7ester\AppData\Roaming\Microsoft\Windows\IEDownloadHistory\	iedownload
Container_14	13	C:\Users\W7ester\AppData\Local\Packages\windows_ie_ac_001\AC\WinNetCookie...	Cookies
Container_15	14	C:\Users\W7ester\AppData\Local\Packages\windows_ie_ac_001\AC\WinNetHistory\	History
Container_16			
Container_17			
Container_18			
Container_19			
Container_2			
Container_3			

5. 익스플로러 캐시 확장

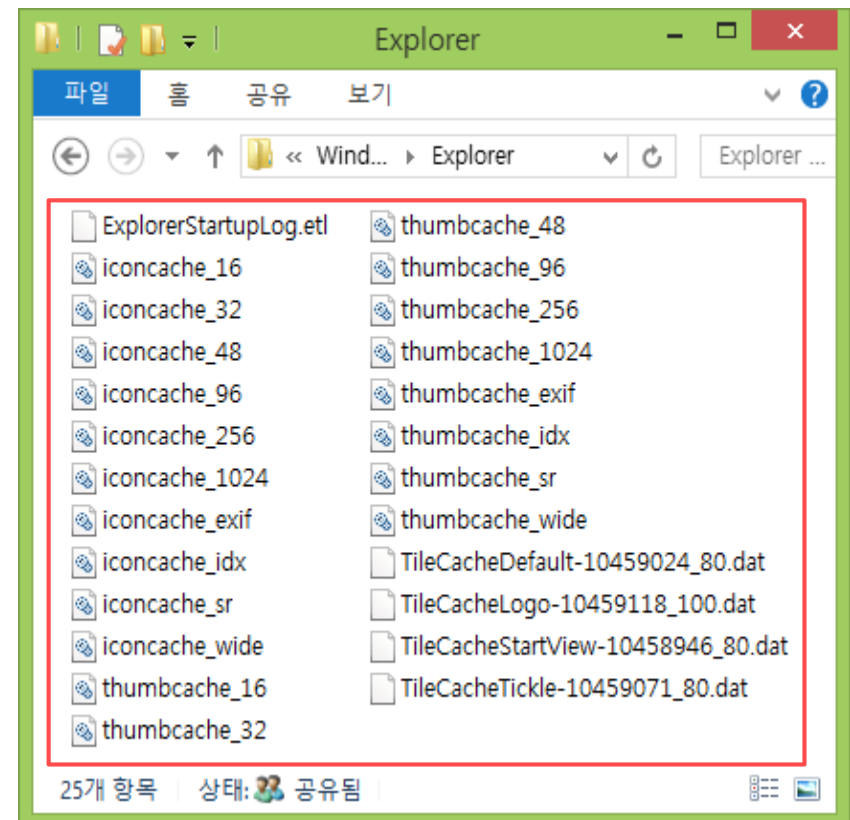
- 익스플로러 캐시 저장 경로

%UserProfile%\AppData\Local\Microsoft\Windows\Explorer

윈도우 7



윈도우 8

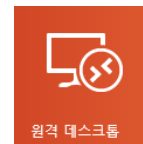
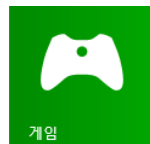
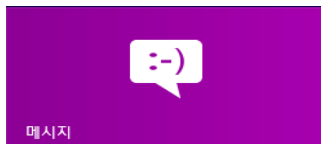
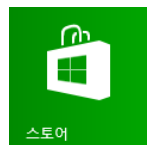
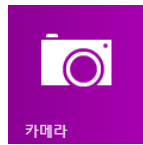
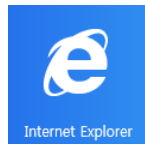


03

새로운 포렌식 아티팩트

1. 메트로 환경 아티팩트
2. 파일 히스토리
3. PC 복구와 PC 초기화
4. 익스플로러 캐시 확장

1. 메트로 아티팩트



앱 실행 파일

%SystemDrive%\Program Files\WindowsApps

앱 패키지 목록

%UserProfile%\AppData\Local\Packages

앱 바로가기

%UserProfile%\AppData\Local\Microsoft\Windows\Application Shortcuts

시작화면 고정 목록

%UserProfile%\AppData\Local\Microsoft\Windows\RoamingTiles

시작 화면 타일 배열

%UserProfile%\AppData\Local\Microsoft\Windows\appsFolder.itemdata-ms

앱 인터넷 사용흔적

%UserProfile%\AppData\Packages\[AppName]\AC

앱 저장소

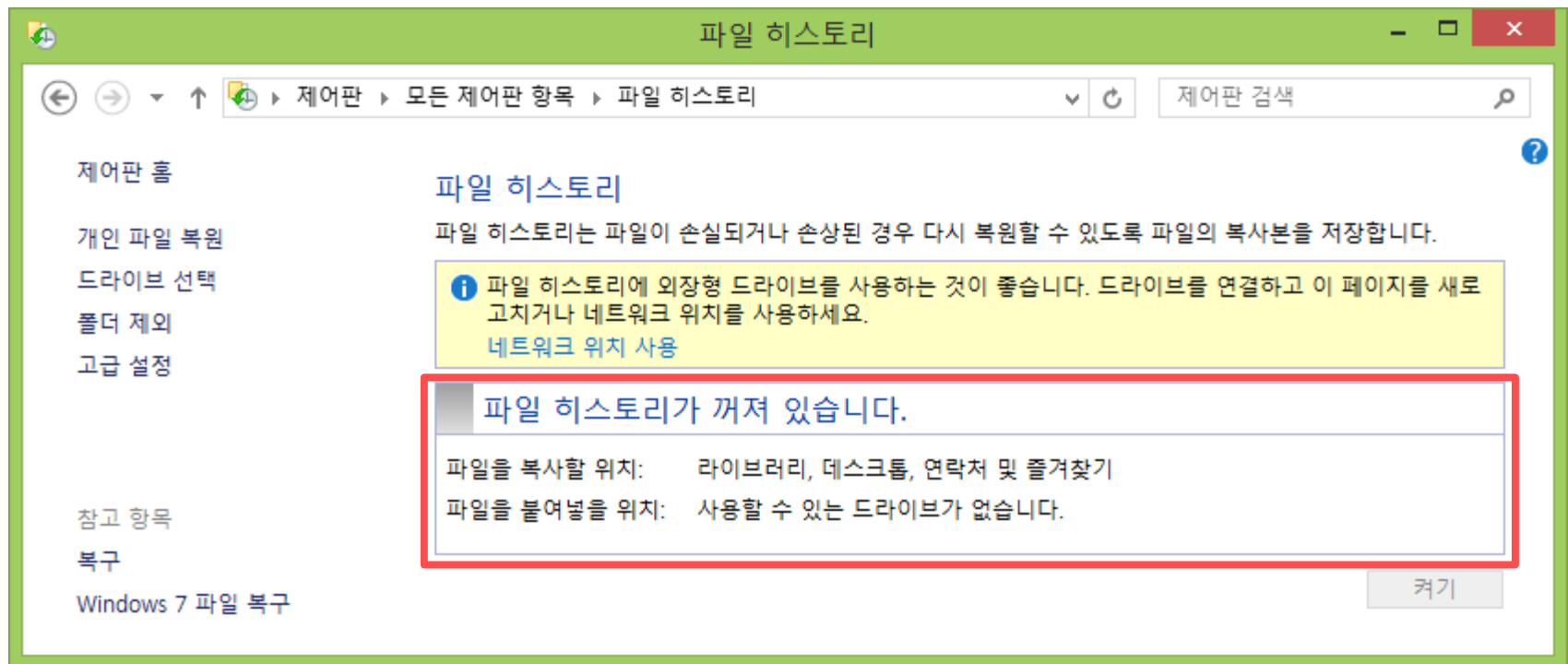
%SystemDrive%\ProgramData\Microsoft\Windows\AppRepository

앱 푸시 알림 설정

HKLM\SOFTWARE\Microsoft\Windows\CurrentVersion\PushNotifications

2. 파일 히스토리

- 새롭게 추가된 파일 백업 기능
 - ✓ 제어판 → 파일 히스토리
 - ✓ 네트워크 위치, 외장형 드라이브에 자동 백업
 - ✓ 라이브러리, 데스크톱, 연락처, 즐겨찾기



- 포맷 없이 간편하게 시스템 복구 가능

언어 기본 설정

PC 설정

사용 가능한 기능

PC 복구

이 작업을 할 경우,

- 파일 및 개인 설정은 변경되지 않습니다.
- PC 설정이 기본값으로 다시 변경됩니다.
- Windows 스토어의 앱은 유지됩니다.
- 디스크 또는 웹 사이트에서 설치한 앱이 제거됩니다.
- 단, 제거된 앱 목록은 데스크톱에 저장됩니다.

다음

취소

접근성

설정 동기화

홈 그룹

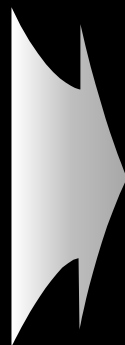
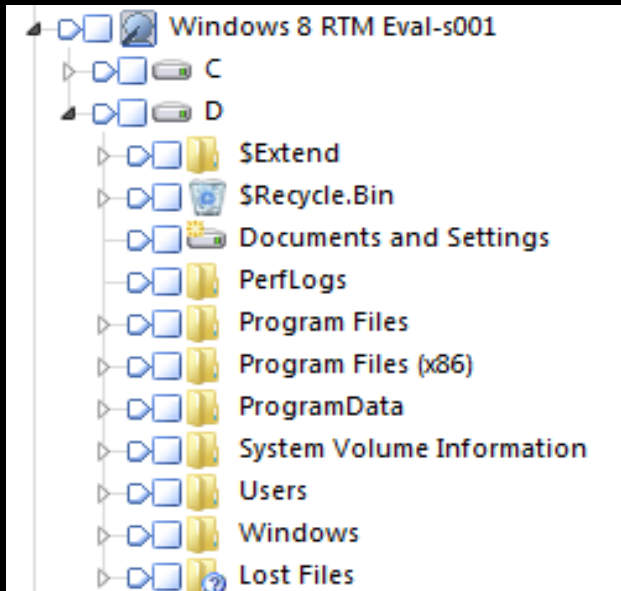
Windows 업데이트

프롬프트 시작 접근

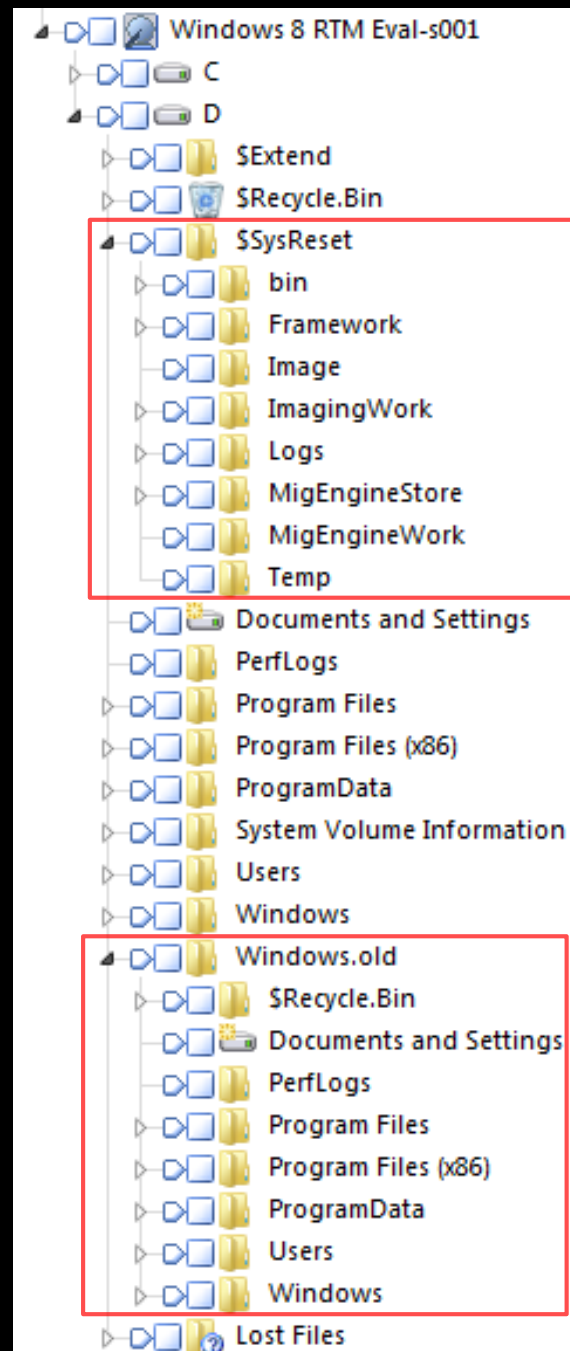
USB 드라이브 또는 DVD 등의 장치 또는 디스크에서 직접 시작하거나, Windows 시작 설정을 변경하거나, 또는 시스템 이미지로 Windows를 복원할 수 있습니다. PC가 다시 시작됩니다. 모든 사용자가 로그아웃되고 저장하지 않은 작업은 손실될 수 있습니다.

다시 시작

PC 복구 전



PC 복구 후



- 포맷 없이 간편하게 시스템 초기화 가능

언어 기본 설정

⬅ 드라이브를 완전히 정리하시겠습니까?

파일을 제거할 경우 파일을 쉽게 복구할 수 없도록 드라이브를 정리할 수 있습니다. 이렇게 하면 더 안전하지만 시간이 훨씬 더 오래 걸립니다.

내 파일만 제거
이 작업은 곧 완료됩니다.

드라이브를 완전히 정리
이 작업은 많은 시간이 걸립니다.

취소

접근성

설정 동기화

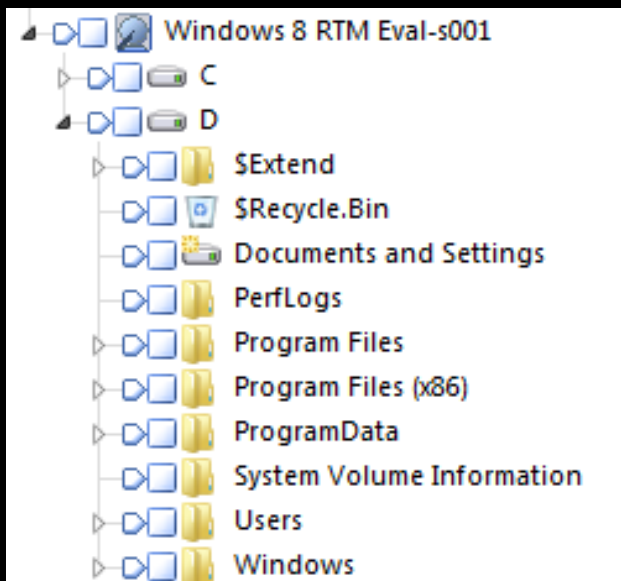
홈 그룹

Windows 업데이트

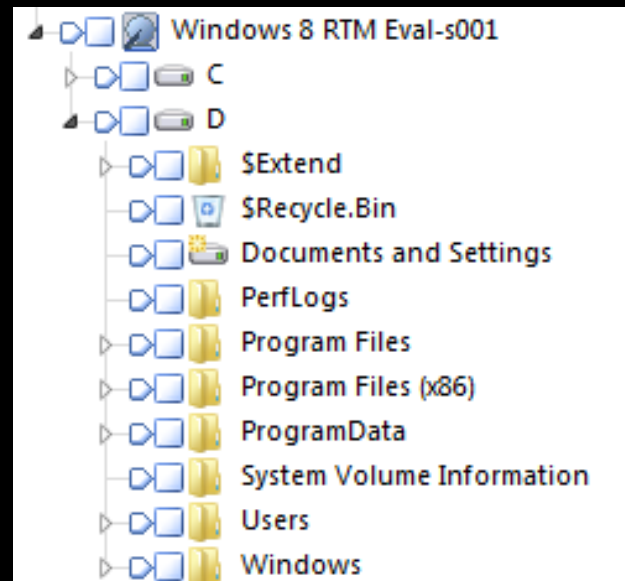
USB 드라이브 또는 DVD 등의 장치 또는 디스크에서 직접 시작하거나, Windows 시작 설정을 변경하거나, 또는 시스템 이미지로 Windows를 복원할 수 있습니다. PC가 다시 시작됩니다. 모든 사용자가 로그아웃되고 저장하지 않은 작업은 손실될 수 있습니다.

다시 시작

PC 초기화 전



PC 초기화 후



비활당영역

204006426907E	3C	39	0E	B9	44	EB	CC	6D	FF	B8	77	EE	BC	56	C2	39	F9	D2	A6	1E	35	24	30	40	64	EB	3F	AE	3F	~<9.¹Dēimŷ. wixVĀ9ùò! .5\$ø@dē?º?
204006427200C	42	DC	0F	09	64	0F	1B	94	C6	84	F8	DE	29	E2	EC	62	99	39	EC	82	66	83	11	B5	B7	44	22	8C	5B	·BÜ. d..”ε,øp)âib™9i,ff·μ·D"ε[
20400642750DB	D5	A3	9C	5C	38	9A	05	23	30	77	A3	0F	93	AB	AE	A9	FD	67	F5	65	33	78	44	23	E3	55	FA	98	53	ÜÖε&ſ. #øwε.“«@ýgøe3xD#äUú”S
2040064278048	90	DF	EC	91	FD	D4	B8	69	3E	6E	1D	15	EC	93	2A	D6	81	F6	13	2D	93	89	B2	CC	87	1D	BB	9C	E2	Kßi’yÖ i>n..i”*Öö.-“ε²i†.»æâ
2040064281058	72	20	A5	40	7F	CC	EF	22	EE	08	D6	A5	7D	FC	8A	A4	86	C3	25	68	4F	BB	08	79	D3	98	F2	4F	CB	Xr *@æii”i.ö*}üſH†Ä%ko».yó>ðoË
20400642840FD	79	9E	98	92	10	FD	E9	80	3E	94	29	5C	DD	B7	06	AE	76	F1	E0	E7	14	CC	92	46	D1	08	F9	0F	22	ýyž”’.ýé€>”) \Ÿ..øvñàç.ì’Fñ.ù.”
204006428702B	EE	9B	60	D9	07	17	A1	27	56	A3	C5	74	66	06	5C	70	26	CA	7B	F9	89	73	7F	99	A9	7E	14	A3	84	+i>`ù..j’vεÄtf.\p&Ë{ùſsø”ø~.ε,,
2040064290073	96	41	E1	76	65	3E	47	70	8D	CD	FD	0E	60	48	42	56	D2	F1	F4	2F	A6	7A	80	42	E1	1E	34	DA	03	s-Aäve>GpIŷ·’HBVðñô/;zεBä.4Ú.
204006429303D	34	0E	D2	77	2A	4A	D9	36	6C	40	85	5C	71	C4	87	CC	10	6F	AF	23	6F	75	2E	92	B0	A4	F8	6B	2E	=4.öw*JÜ6l@_ \qÄ†i.ø”#ou.”ºHøk.
2040064296095	28	EF	08	56	A7	C4	69	3C	42	68	8D	11	48	AE	96	98	17	5F	1E	E1	65	BF	92	AB	78	DE	BD	9D	68	·(i.VſÄi<Bk·Hø-”.._·äeiz’«xb)¼k
204006429903D	AD	6C	81	F0	7B	B8	47	F1	E2	B8	25	D9	64	E3	59	E7	68	1A	B9	2B	C9	0A	2A	50	F3	2A	00	85	64	=-lß{. Gñâ.%ÜdäYçk.¹+É *Pó*._d
204006430209E	46	E3	E5	D1	29	35	6D	2E	1A	46	66	EF	FA	89	CB	80	E9	E3	99	1E	FD	DE	E5	9C	3E	61	8C	91	08	žFââñ)Sm..Ffiúſ&Ëéä”·ýbâæ>aε’.
204006430504E	3A	73	32	E7	D2	5E	D6	B1	50	C2	3F	98	96	30	18	AF	F7	79	F2	1E	5C	69	B2	D9	8A	C2	73	4B	B3	N:s2çð”ö±PÄ?~-ø.”+yð.\i²ÜſÄsK³
2040064308048	FD	64	13	76	45	EE	E6	70	97	3D	7B	92	09	D1	88	D4	80	2D	99	08	1F	AF	78	F7	F9	CF	3D	99	59	Hýd·vEiæp=-{’ Ñ”Öε-”..”x=üi=™y
2040064311035	2D	C5	2A	F9	05	4E	A9	7E	0E	18	C9	DE	66	7C	3F	10	E7	14	41	D8	48	CB	E8	F4	6F	D5	9F	B5	D9	5-Ä*ù·Nø~...Ébfi >·ç·AøHËèðoöÿµÜ
20400643140B5	C8	44	09	7C	A9	E9	D0	A1	7A	68	B0	97	0A	68	E4	45	06	BC	DB	8E	CB	99	9A	AC	2A	E9	D4	F8	DA	µÈD øéð;zhø- kÄε·XÜZË”ſ~·éöøÚ
2040064317001	BA	B9	00	CA	40	05	4C	94	D0	0B	53	8B	DA	9C	33	7F	CA	47	B8	19	1F	09	E2	C6	91	84	4B	D1	44	·ε¹.Ë@·L”D·S<üε3øËG.. äε’.,KNÐ
204006432004E	78	E6	E8	61	3C	C7	D5	8F	F0	A6	5F	2C	10	02	32	A5	72	C9	58	81	36	7C	B3	67	7D	C8	2E	F2	12	Nxæä<çÖö!_,..2*εrÉXö ³g)Ë.ð.
204006432307E	AB	2A	12	EB	E8	D1	C9	7D	D3	D8	58	E9	2D	8E	D1	69	CF	6C	0D	CD	DC	CF	C9	4E	DA	00	D7	46	1B	~«*.ëëNË)øÖxé-ZñiI l ÌÜiÉNU.×F.
20400643260D2	64	DE	37	BA	BB	19	18	1C	01	9E	18	AB	AF	DE	5D	65	7C	4E	09	82	C0	A2	BA	74	70	A7	52	8F	A4	öðb7ε»...·ž.“«pJe NI,ÄçetpSRH
2040064329040	32	89	91	03	1C	8D	76	91	09	67	C8	4A	58	9D	CE	FD	90	14	0A	A7	4E	AA	37	39	CC	EB	76	83	7A	@2ſε..·ŷ’ gÈJXÏŷ . ſN#79iëvfvz
20400643320C4	57	AB	9B	16	0F	89	3B	05	30	6B	79	DA	4E	8D	C9	68	1D	F4	8C	84	49	75	6A	BF	41	C8	85	48	F1	Äw«»..ſ;·økyÚNËH·öε,Iu¿jçÄE-Hñ
20400643350C9	5C	AF	1E	CF	4B	9B	AE	8A	39	A1	79	FC	76	5E	B5	6B	50	C5	87	4E	81	7C	AC	A2	77	EB	69	86	B0	É\`·Ïk.ø59;jüv^µkPÄ†N ~qweigº

04

실전 악성코드 포렌식

1. 악성코드 분석 방법
2. 통합 타임라인 분석
3. 샘플 #1
4. 샘플 #2

01 시점을 알 수 없는 경우

➔ 체계적인 하향식 접근 방법 필요

02 시점을 알거나 의심 시점을 발견한 경우

➔ 해당 시점을 기준으로 통합 타임라인 분석 필요

시간정보가 포함된 **아티팩트**를 시간순으로 **정렬**하거나 **통계**를 내어 **분석**하는 방법

- ✓ 웹 애플리케이션(IIS, 아파치 등) 로그
- ✓ 웹 브라우저(IE, 파폭, 크롬 등) 흔적
- ✓ 이벤트 로그 (EVT, EVTX)
- ✓ 프리패치
- ✓ 복원지점/볼륨 새도우 복사본
- ✓ 링크 파일
- ✓ 레지스트리
- ✓ EXIF 메타데이터
- ✓ 휴지통 정보 (INFO2, \$I)
- ✓ 문서 파일 메타데이터
- ✓ PE 컴파일 정보
- ✓ 데이터베이스 정보
- ✓ 패킷 메타데이터
- ✓ 각종 로그(Setupapi, xpfirewall 등)

2. 통합 타임라인 분석

log2timeline

```
$ mount -o ro, loop, show_sys_files, streams_interface=windows, offset=368050176  
"/mnt/hgfs/image.001" /mnt/windows_mount
```

```
$ log2timeline -p -r -f mft, evtx, restore, recycler,  
win_link, prefetch, sam,  
security, software, ntuser, exif  
-z Asia/Seoul /mnt/windows_mount -w timeline.csv
```

```
$ l2t_process -b image_bodyfile.txt 09-18-2012..09-20-2012 > timeline.csv
```

2. 통합 타임라인 분석

log2timeline

```
sansforensics@SIFT-Workstation: ~  
File Edit View Terminal Help  
sansforensics@SIFT-Workstation:~$ sudo mount -o ro,loop,show_sys_files,streams_interf  
ace=windows,offset=368050176 /mnt/hgfs/vmdk2dd/mal4.001 /mnt/windows mount/  
sansforensics@SIFT-Workstation:~$ log2timeline -p -r -f evtx,exif,prefetch,recycler,r  
estore,win_link,ntuser,software,system,sam,mft -z Asia/Seoul /mnt/windows_mount -w ~/  
Temp/04_timeline.csv  
Start processing file/dir [/mnt/windows_mount] ...  
Starting to parse using input module(s): [evtx,exif,prefetch,recycler,restore,win_li  
nk,ntuser,software,system,sam,mft]  
[PreProcessing] Unable to determine the default browser for user default  
[PreProcessing] Unable to determine the default browser for user pr0neer  
[PreProcessing] Unable to determine the default browser for user jk  
[PreProcessing] Hostname is set to FORENSICER  
[PreProcessing] The timezone according to registry is: (@.,-622) @tzres.dll,-622  
[PreProcessing] The timezone settings are NOT overwritten so the settings might have  
to be adjusted.  
[PreProcessing] The default system browser is: : IEXPLORE.EXE ("C:\Program Files\Inte  
rnet Explorer\iexplore.exe" %1)  
Loading output file: csv  
Unable to open /mnt/windows_mount/$Extend/$ObjId  
Unable to open /mnt/windows_mount/$Extend/$Quota  
Unable to open /mnt/windows_mount/$Extend/$Reparse  
Unable to open /mnt/windows_mount/$Extend/$UsnJrnl  
Unable to open /mnt/windows_mount/$Secure
```

3. 샘플 #1

Win-Trojan/Malpacked3.Gen



```
C:\$Recycle.Bin> x.jpg
```

3. 샘플 #1

Win-Trojan/Malpacked3.Gen

The screenshot shows the Windows Event Viewer window titled "이벤트 뷰어" (Event Viewer). The left pane shows the event log for "Microsoft-Windows-UAC-FileVirtualization%4Operational" with 32 events. The right pane shows the details for event ID 5003, "UAC-FileVirtualization".

Event List:

수준	날짜 및 시간	원본	이벤트...	작업 ...
! 자세한 정보...	2012-09-19 오후 10:47:18	UAC-FileVirtualization	5003	없음
! 자세한 정보...	2012-09-19 오후 10:47:18	UAC-FileVirtualization	5003	없음
! 자세한 정보...	2012-09-19 오후 10:47:18	UAC-FileVirtualization	5003	없음

Event Details: 이벤트 5003, UAC-FileVirtualization

일반 | 자세히

WRP 파일 "#Device#HarddiskVolume2#Windows#SysWOW64#WSHTCPIP.DLL"에서 액세스가 거부되었습니다.

로그 이름(M): Microsoft-Windows-UAC-FileVirtualization/Operational

원본(S): UAC-FileVirtualization **로그된 날짜(D):** 2012-09-19 오후 10:47:18

이벤트 ID(E): 5003 **작업 범주(Y):** 없음

수준(L): 자세한 정보 표시 **키워드(K):**

사용자(U): FORENSICER#JK **컴퓨터(R):** FORENSICER

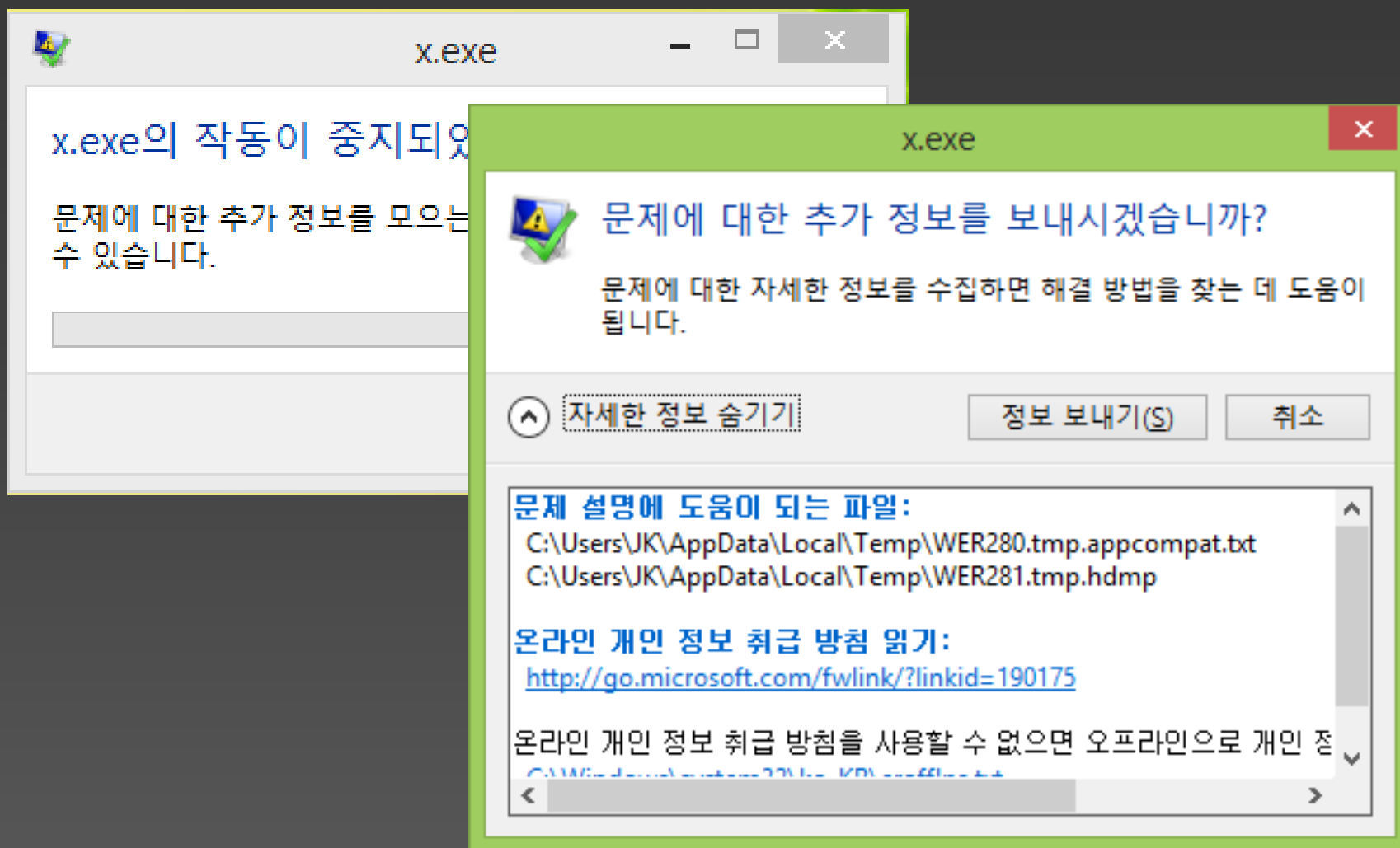
4. 샘플 #2

Win32/Parite

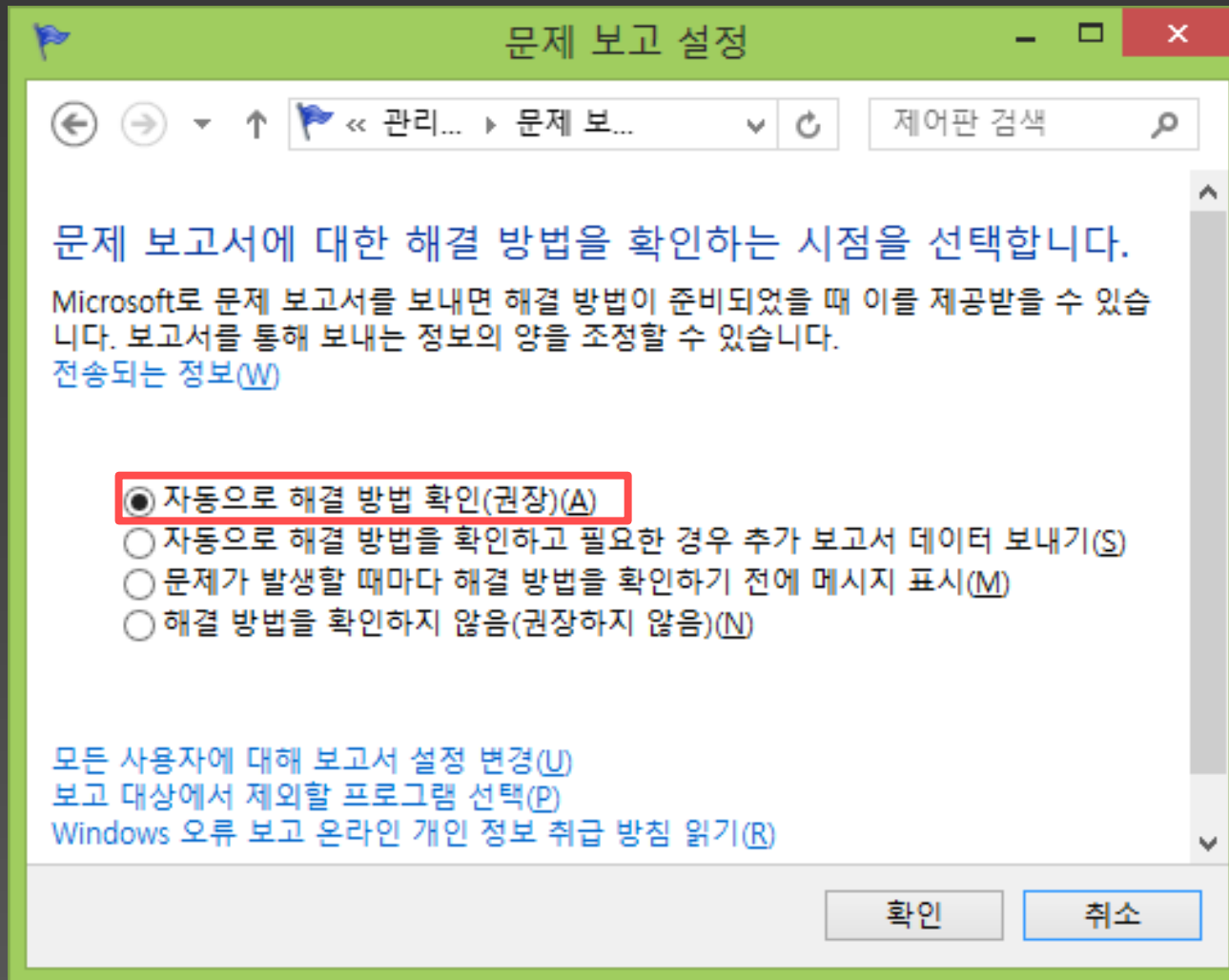


```
C:\$Recycle.Bin> x.exe
```

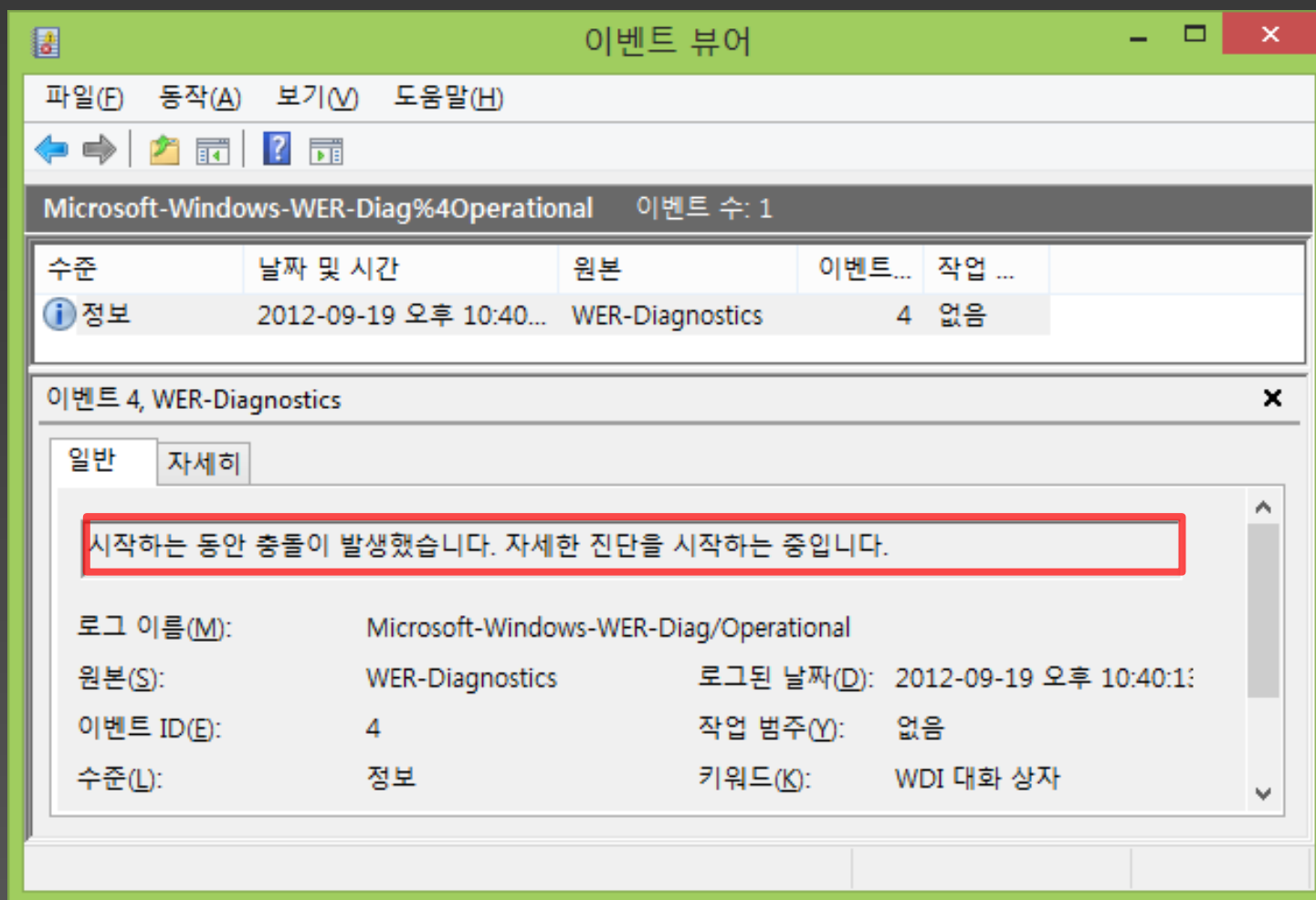
Win32/Parite – 윈도우 문제 보고 (Windows Error Reporting)



Win32/Parite – 윈도우 문제 보고 (Windows Error Reporting)



Win32/Parite – 윈도우 문제 보고 (Windows Error Reporting)



Win32/Parite – 윈도우 문제 보고 (Windows Error Reporting)

```
/ProgramData/Microsoft/Windows/WER/ReportArchive/AppCrash_x.exe_c598da78  
4abfeeaa78a28a697595ebb2f4f7a43_cab_095c6e9a/Report.wer
```

감사합니다

Conference Of Researchers & Engineers