DFRWS USA 2016

Recovery method of deleted records and tables from ESE Database

2016. 8. 9.

Kim Jeonghyeon

Contents

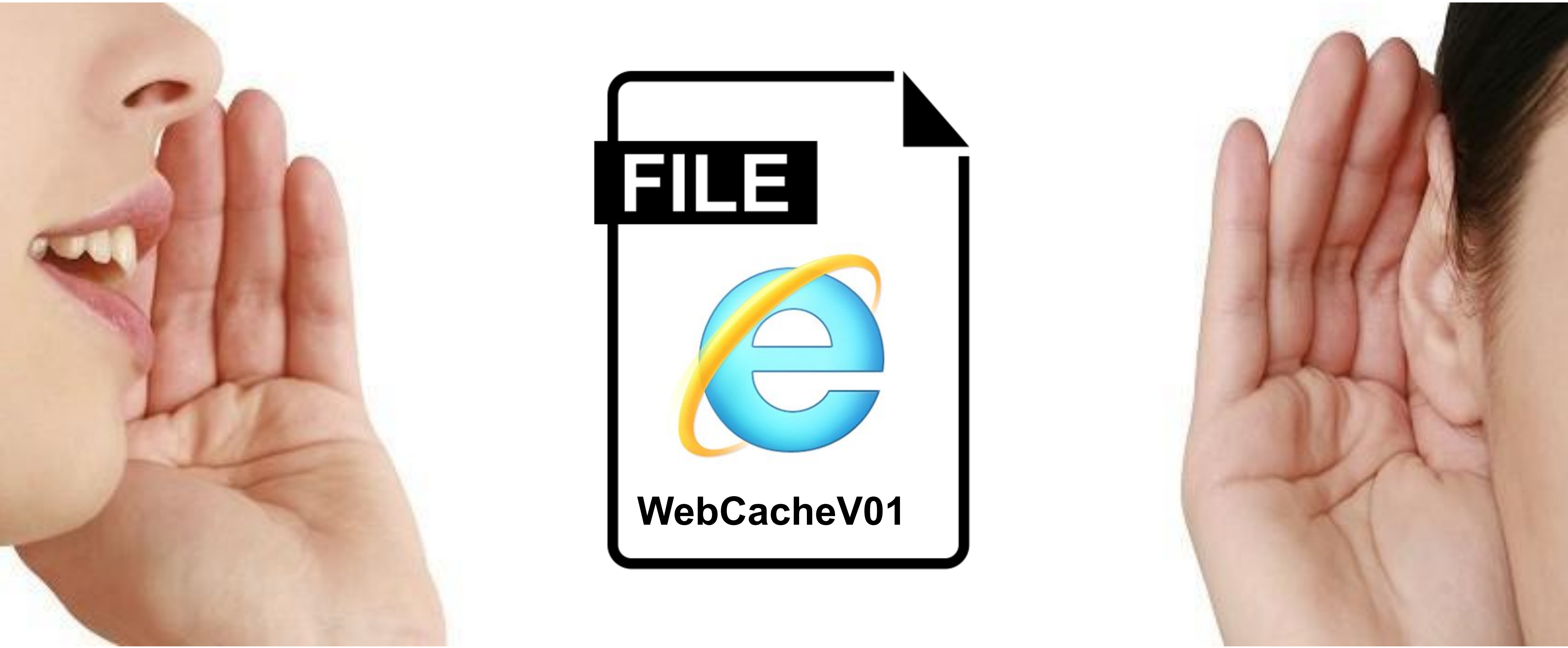
- Introduction
- Background knowledge
- Relate works
- ESE database format analysis
- Verifying changes after deleting records
- Record recovery technique
- Implementation and performance
- Conclusion

Introduction

TWO YEARS AGO

Friend

Me



Introduction

- **What is ESE database?**
  - Data storage technology developed by Microsoft
  - Has been used mainly in web browsers and window systems
  - Save and manage the main records of systems and users in the Window OS.

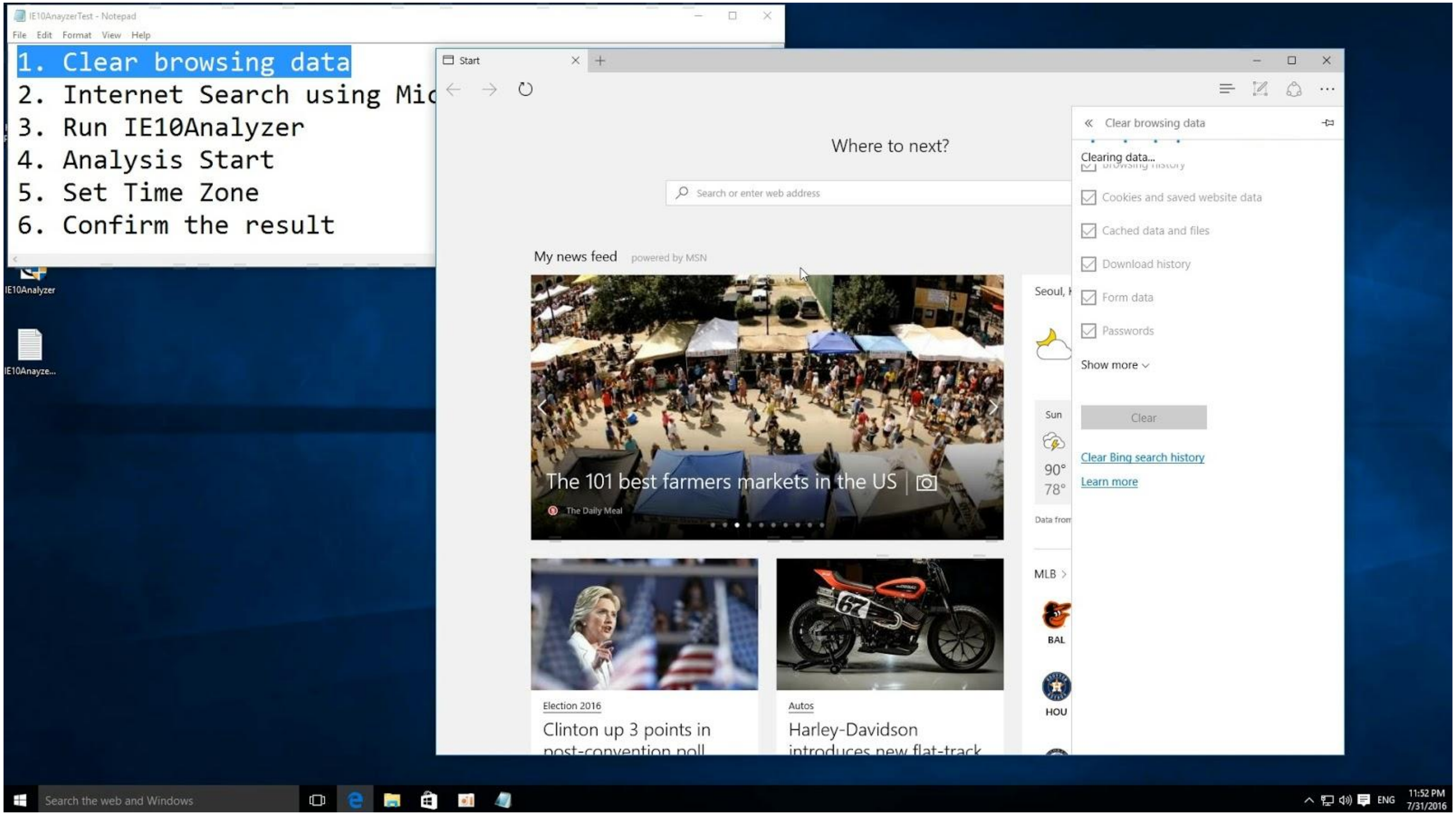
[Table] Programs using ESE database

Program	Path	File Name
Edge Browser	%LOCALAPPDATA%\Microsoft\Windows\WebCache	WebCacheV01.dat
Internet Explorer 10	%LOCALAPPDATA%\Microsoft\Windows\WebCache	WebCacheV01.dat
System Resource Usage Monitor	%WINDIR%\system32\SRU	SRUDB.dat
Windows Update	%WINDIR%\SoftwareDistribution\DataStore	DataStore.edb
Windows Live	%LOCALAPPDATA%\Microsoft\Windows\SettingSync\metastore	contacts.edb
Windows Mail	%USERPROFILE%\AppData\Local\Microsoft\Windows Mail	WindowsMail.MSMessageStore
Active Directory	%WINDIR%\System32	ntds.dit
Windows Search	%PROGRAMDATA%\Microsoft\Search\Data\Applications\Windows	Windows.edb

Introduction

- **If I recovery deleted records from ESE database, What can I see?**

1) Clear browsing data to be exact.



```
1. Clear browsing data
2. Internet Search using Mic
3. Run IE10Analyzer
4. Analysis Start
5. Set Time Zone
6. Confirm the result
```

Clear browsing data

Clearing data...

☑ Browsing history

☑ Cookies and saved website data

☑ Cached data and files

☑ Download history

☑ Form data

☑ Passwords

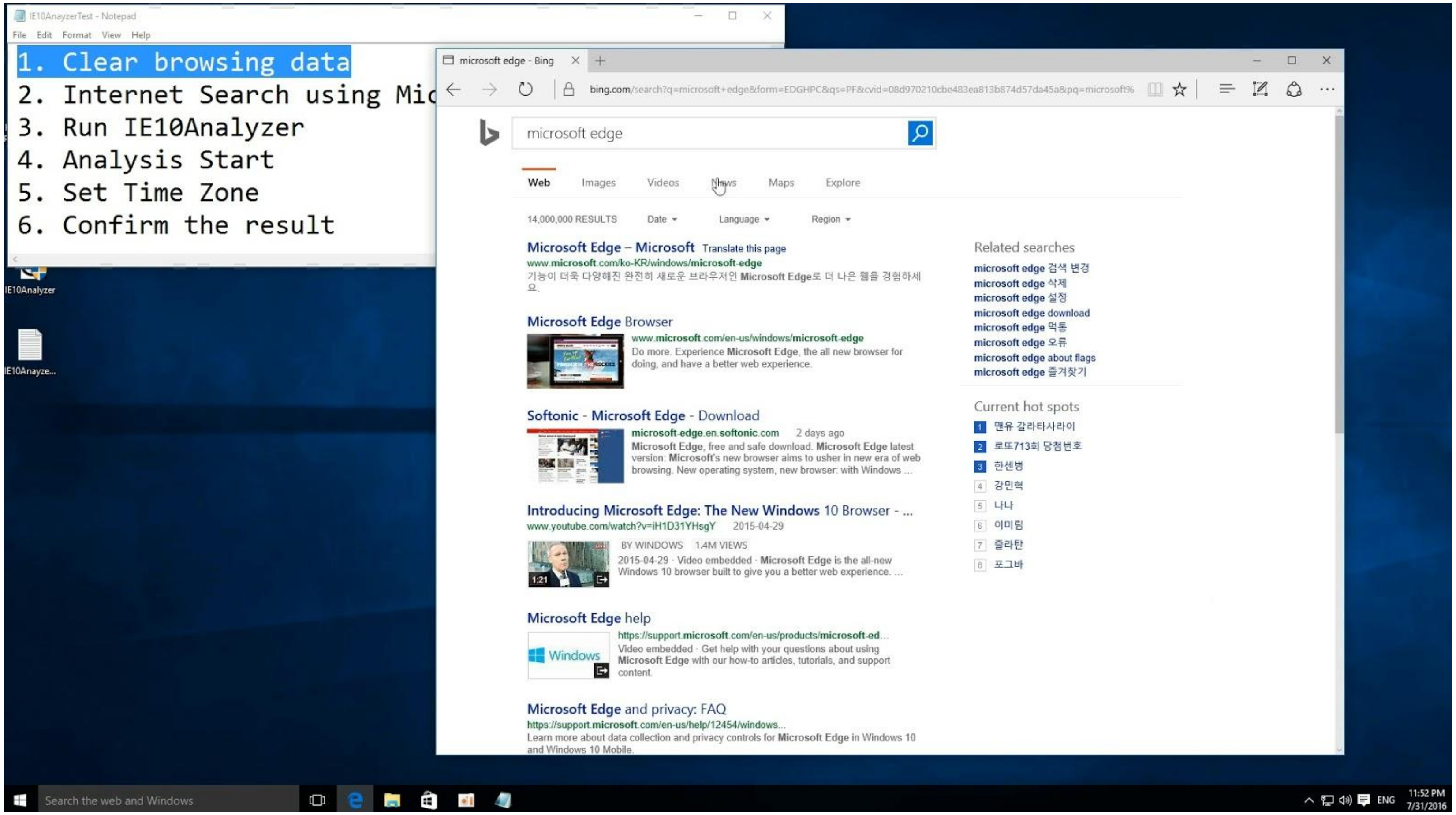
IE10AnayzerTest - Notepad
File Edit Format View Help
IE10Analyzer
IE10Anayze...
Start
Where to next?
Search or enter web address
My news feed powered by MSN
The 101 best farmers markets in the US
The Daily Meal
Election 2016
Clinton up 3 points in post-convention poll
Autos
Harley-Davidson introduces new flat-track
Seoul, K
Sun
90°
78°
Data from
MLB
BAL
HOU
Show more
Clear
Clear Bing search history
Learn more
Search the web and Windows
ENG
11:52 PM
7/31/2016

- youtube title : "Internet Explorer 10, Microsoft Edge Forensic on Windows 10 "

Introduction

- **If I recovery deleted records from ESE database, What can I see?**

2) Search for 'Microsoft Edge' and 'notepad' on Google.



IE10AnayzerTest - Notepad
File Edit Format View Help
microsoft edge - Bing
IE10Analyzer
IE10Anayze...
Web Images Videos News Maps Explore
Search the web and Windows
ENG
11:52 PM
7/31/2016

```
1. Clear browsing data
2. Internet Search using Mic
3. Run IE10Analyzer
4. Analysis Start
5. Set Time Zone
6. Confirm the result
```

bing.com/search?q=microsoft+edge&form=EDGHPC&qs=PF&cvid=08d970210cbe483ea813b874d57da45a&pq=microsoft%

microsoft edge

14,000,000 RESULTS Date Language Region

Microsoft Edge – Microsoft Translate this page
www.microsoft.com/ko-KR/windows/microsoft-edge
기능이 더욱 다양해진 완전히 새로운 브라우저인 Microsoft Edge로 더 나은 웹을 경험하세요.

Microsoft Edge Browser
www.microsoft.com/en-us/windows/microsoft-edge
Do more. Experience Microsoft Edge, the all new browser for doing, and have a better web experience.

Softonic - Microsoft Edge - Download
microsoft-edge.en.softonic.com 2 days ago
Microsoft Edge, free and safe download. Microsoft Edge latest version: Microsoft's new browser aims to usher in new era of web browsing. New operating system, new browser: with Windows ...

Introducing Microsoft Edge: The New Windows 10 Browser - ...
www.youtube.com/watch?v=iH1D31YHsgY 2015-04-29
BY WINDOWS 1.4M VIEWS
2015-04-29 · Video embedded · Microsoft Edge is the all-new Windows 10 browser built to give you a better web experience. ...

Microsoft Edge help
https://support.microsoft.com/en-us/products/microsoft-ed...
Video embedded · Get help with your questions about using Microsoft Edge with our how-to articles, tutorials, and support content.

Microsoft Edge and privacy: FAQ
https://support.microsoft.com/en-us/help/12454/windows...
Learn more about data collection and privacy controls for Microsoft Edge in Windows 10 and Windows 10 Mobile.

Related searches
microsoft edge 검색 변경
microsoft edge 삭제
microsoft edge 설정
microsoft edge download
microsoft edge 먹통
microsoft edge 오류
microsoft edge about flags
microsoft edge 즐겨찾기

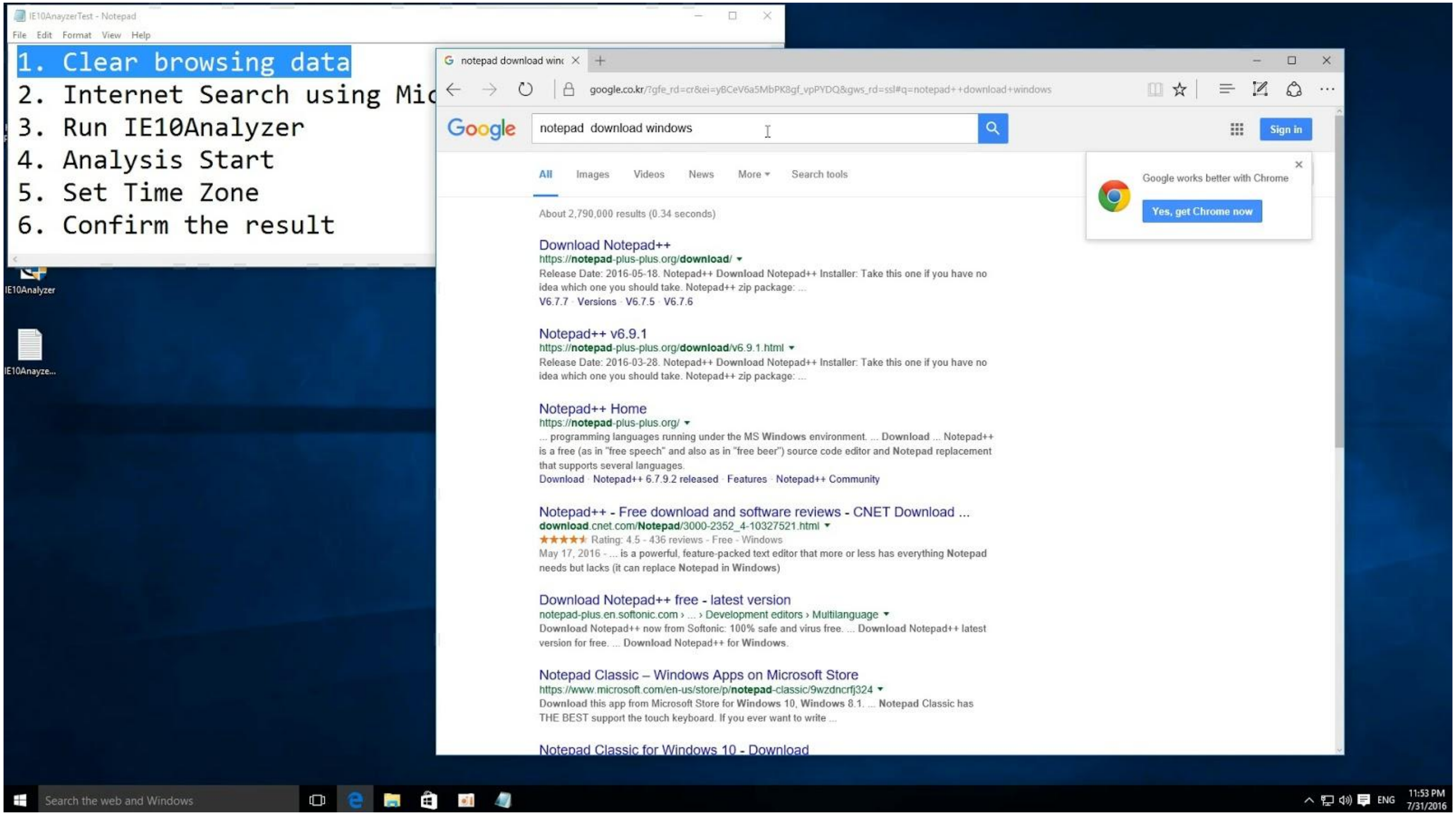
Current hot spots
1 맨유 갈라타사라이
2 로또713회 당첨번호
3 한센병
4 강민혁
5 나나
6 이미림
7 즐라탄
8 포그바

- youtube title : "Internet Explorer 10, Microsoft Edge Forensic on Windows 10 "

Introduction

- **If I recovery deleted records from ESE database, What can I see?**

2) Search for 'Microsoft Edge' and 'notepad' in Google.



```
1. Clear browsing data
2. Internet Search using Mic
3. Run IE10Analyzer
4. Analysis Start
5. Set Time Zone
6. Confirm the result
```

google.co.kr/?gfe_rd=cr&ei=yBCeV6a5MbPK8gf_vpPYDQ&gws_rd=ssl#q=notepad++download+windows

notepad download windows

About 2,790,000 results (0.34 seconds)

Download Notepad++
https://notepad-plus-plus.org/download/ ▾
Release Date: 2016-05-18. Notepad++ Download Notepad++ Installer: Take this one if you have no idea which one you should take. Notepad++ zip package: ...
V6.7.7 · Versions · V6.7.5 · V6.7.6

Notepad++ v6.9.1
https://notepad-plus-plus.org/download/v6.9.1.html ▾
Release Date: 2016-03-28. Notepad++ Download Notepad++ Installer: Take this one if you have no idea which one you should take. Notepad++ zip package: ...

Notepad++ Home
https://notepad-plus-plus.org/ ▾
... programming languages running under the MS Windows environment. ... Download ... Notepad++ is a free (as in "free speech" and also as in "free beer") source code editor and Notepad replacement that supports several languages.
Download · Notepad++ 6.7.9.2 released · Features · Notepad++ Community

Notepad++ - Free download and software reviews - CNET Download ...
download.cnet.com/Notepad/3000-2352_4-10327521.html ▾
★★★★★ Rating: 4.5 - 436 reviews - Free - Windows
May 17, 2016 - ... is a powerful, feature-packed text editor that more or less has everything Notepad needs but lacks (it can replace Notepad in Windows)

Download Notepad++ free - latest version
notepad-plus.en.softonic.com › ... › Development editors › Multilanguage ▾
Download Notepad++ now from Softonic: 100% safe and virus free. ... Download Notepad++ latest version for free. ... Download Notepad++ for Windows.

Notepad Classic – Windows Apps on Microsoft Store
https://www.microsoft.com/en-us/store/p/notepad-classic/9wzdncrfj324 ▾
Download this app from Microsoft Store for Windows 10, Windows 8.1. ... Notepad Classic has THE BEST support the touch keyboard. If you ever want to write ...

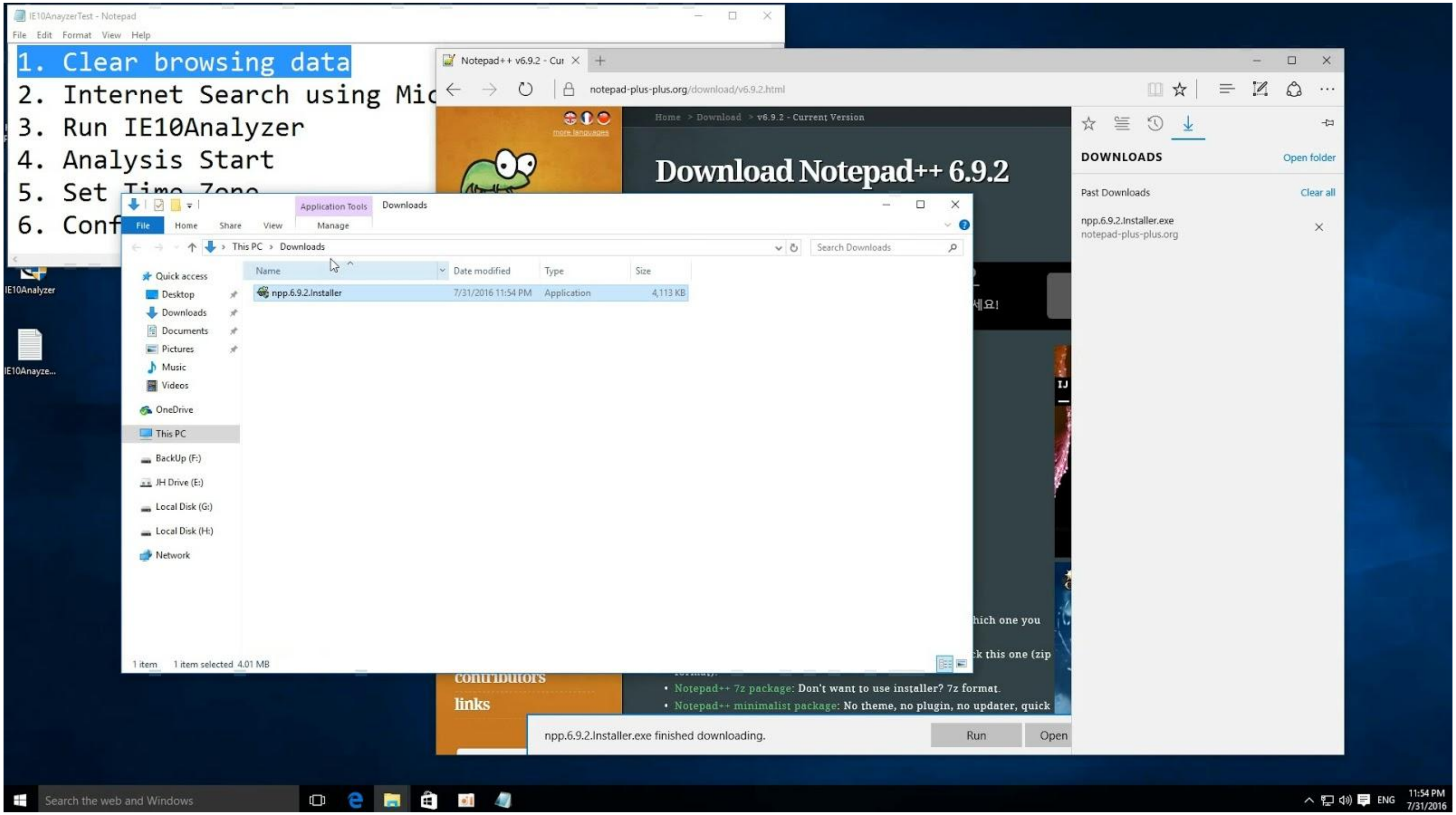
Notepad Classic for Windows 10 - Download

- youtube title : "Internet Explorer 10, Microsoft Edge Forensic on Windows 10 "

Introduction

- **If I recovery deleted records from ESE database, What can I see?**

3) Download notepad++.exe



IE10AnayzerTest - Notepad

1. Clear browsing data
2. Internet Search using Mic
3. Run IE10Analyzer
4. Analysis Start
5. Set Time Zone
6. Conf

Notepad++ v6.9.2 - Cur

notepad-plus-plus.org/download/v6.9.2.html

Home > Download > v6.9.2 - Current Version

Download Notepad++ 6.9.2

- Notepad++ 7z package: Don't want to use installer? 7z format.
- Notepad++ minimalist package: No theme, no plugin, no updater, quick

DOWNLOADS — Open folder

Past Downloads — Clear all

npp.6.9.2.Installer.exe
notepad-plus-plus.org

npp.6.9.2.Installer.exe finished downloading. — Run — Open

This PC > Downloads

Name	Date modified	Type	Size
npp.6.9.2.Installer	7/31/2016 11:54 PM	Application	4,113 KB

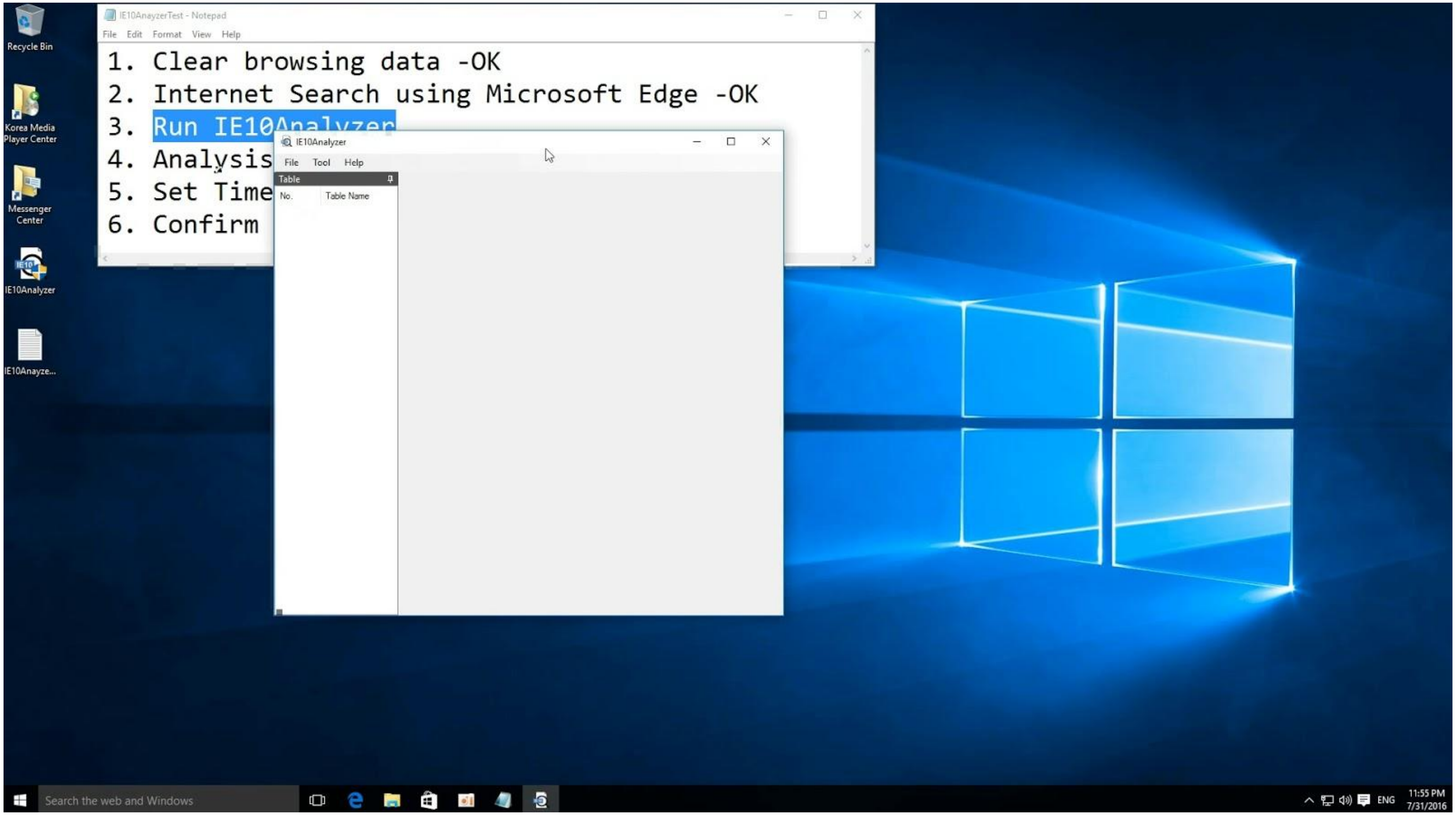
1 item 1 item selected 4.01 MB

- youtube title : "Internet Explorer 10, Microsoft Edge Forensic on Windows 10 "

Introduction

- **If I recovery deleted records from ESE database, What can I see?**

4) Run Program



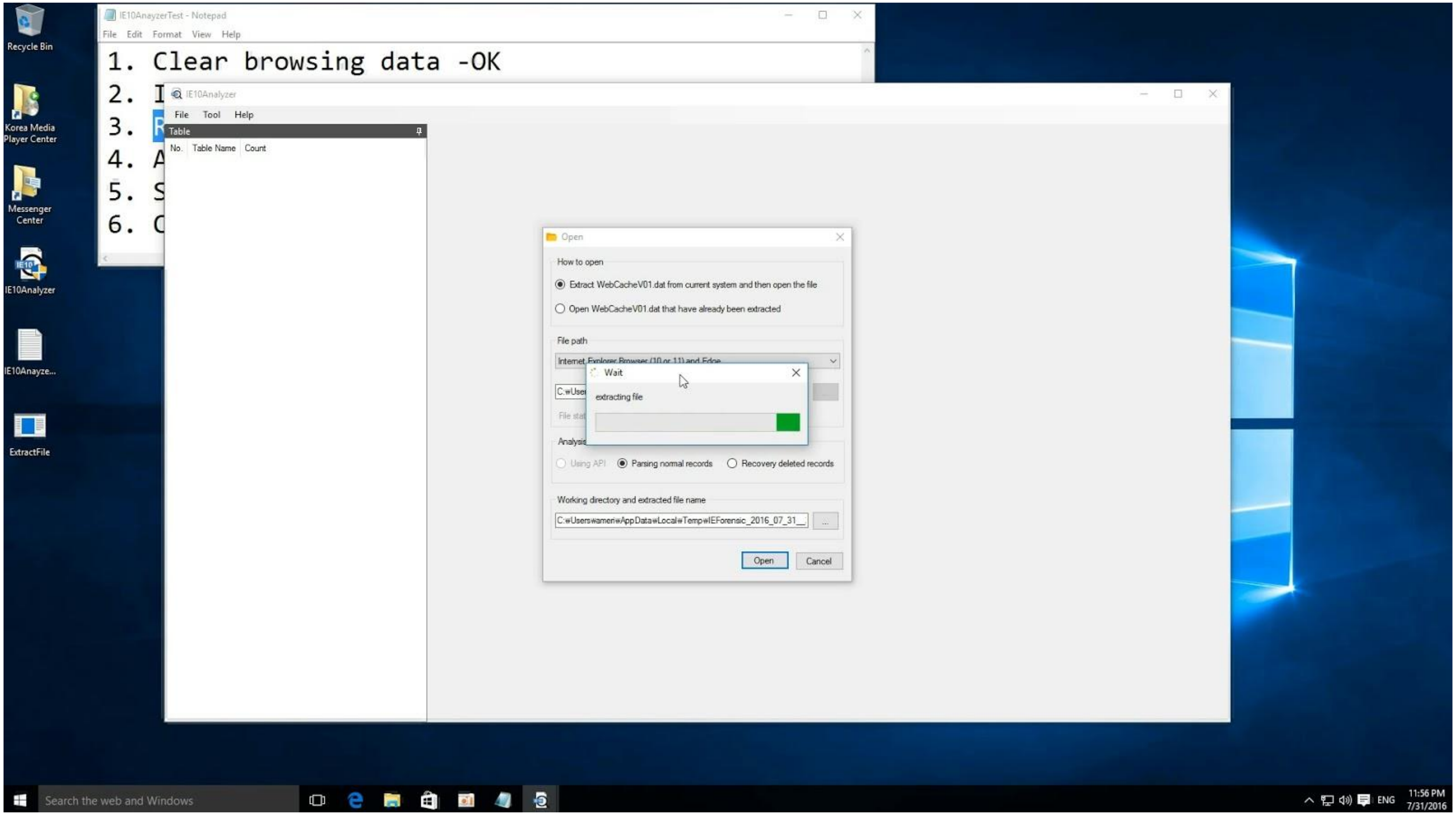
```
1. Clear browsing data -OK
2. Internet Search using Microsoft Edge -OK
3. Run IE10Analyzer
4. Analysis
5. Set Time
6. Confirm
```

- youtube title : "Internet Explorer 10, Microsoft Edge Forensic on Windows 10 "

Introduction

- **If I recovery deleted records from ESE database, What can I see?**

5) Start the analysis



```
1. Clear browsing data -OK
2. I
3. R
4. A
5. S
6. C
```

How to open

- ● Extract WebCacheV01.dat from current system and then open the file
- ○ Open WebCacheV01.dat that have already been extracted

File path

Internet Explorer Browser (10 or 11) and Edge

C:₩User

File stat

extracting file

Analysis

○ Using API ● Parsing normal records ○ Recovery deleted records

Working directory and extracted file name

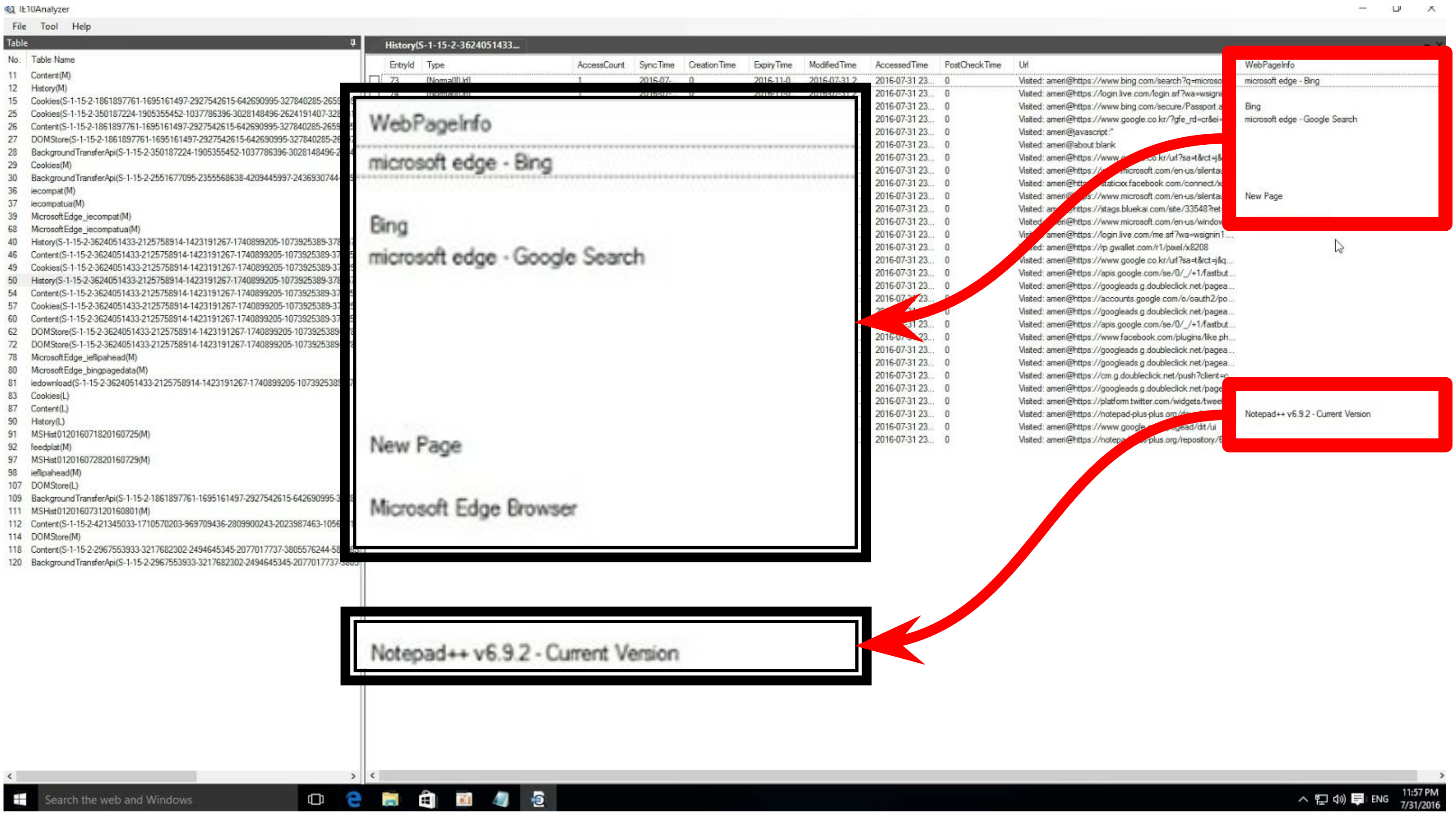
C:₩Users₩ameri₩AppData₩Local₩Temp₩IEForensic_2016_07_31_

- youtube title : "Internet Explorer 10, Microsoft Edge Forensic on Windows 10 "

Introduction

- **If I recovery deleted records from ESE database, What can I see?**

6) Confirm the result - web page title (remains!)



Table

No.	Table Name
11	Content(M)
12	History(M)
15	Cookies(S-1-15-2-1861897761-1695161497-2927542615-642690995-327840285-2659
25	Cookies(S-1-15-2-350187224-1905355452-1037786396-3028148496-2624191407-328
26	Content(S-1-15-2-1861897761-1695161497-2927542615-642690995-327840285-2659
27	DOMStore(S-1-15-2-1861897761-1695161497-2927542615-642690995-327840285-26
28	BackgroundTransferApi(S-1-15-2-350187224-1905355452-1037786396-3028148496-2
29	Cookies(M)
30	BackgroundTransferApi(S-1-15-2-2551677095-2355568638-4209445997-2436930744-
36	iecompat(M)
37	iecompatua(M)
39	MicrosoftEdge_iecompat(M)
68	MicrosoftEdge_iecompatua(M)
40	History(S-1-15-2-3624051433-2125758914-1423191267-1740899205-1073925389-378
46	Content(S-1-15-2-3624051433-2125758914-1423191267-1740899205-1073925389-37
49	Cookies(S-1-15-2-3624051433-2125758914-1423191267-1740899205-1073925389-37
50	History(S-1-15-2-3624051433-2125758914-1423191267-1740899205-1073925389-378
54	Content(S-1-15-2-3624051433-2125758914-1423191267-1740899205-1073925389-37
57	Cookies(S-1-15-2-3624051433-2125758914-1423191267-1740899205-1073925389-37
60	Content(S-1-15-2-3624051433-2125758914-1423191267-1740899205-1073925389-37
62	DOMStore(S-1-15-2-3624051433-2125758914-1423191267-1740899205-1073925389
72	DOMStore(S-1-15-2-3624051433-2125758914-1423191267-1740899205-1073925389
78	MicrosoftEdge_ieflipahead(M)
80	MicrosoftEdge_bingpagedata(M)
81	iedownload(S-1-15-2-3624051433-2125758914-1423191267-1740899205-1073925389
83	Cookies(L)
87	Content(L)
90	History(L)
91	MSHist012016071820160725(M)
92	feedplat(M)
97	MSHist012016072820160729(M)
98	ieflipahead(M)
107	DOMStore(L)
109	BackgroundTransferApi(S-1-15-2-1861897761-1695161497-2927542615-642690995-3
111	MSHist012016073120160801(M)
112	Content(S-1-15-2-421345033-1710570203-969709436-2809900243-2023987463-1056
114	DOMStore(M)
118	Content(S-1-15-2-2967553933-3217682302-2494645345-2077017737-3805576244-58
120	BackgroundTransferApi(S-1-15-2-2967553933-3217682302-2494645345-2077017737-3805

History(S-1-15-2-3624051433...

EntryId	Type	AccessCount	SyncTime	CreationTime	ExpiryTime	ModifiedTime	AccessedTime	PostCheckTime	Url	WebPageInfo
73	[Normal][Url]	1	2016-07-	0	2016-11-0	2016-07-31 2	2016-07-31 23...	0	Visited: ameri@https://www.bing.com/search?q=microso	microsoft edge - Bing
74	[Normal][Url]	1	2016-07-	0	2016-11-0	2016-07-31 2	2016-07-31 23...	0	Visited: ameri@https://login.live.com/login.srf?wa=wsigni	
							2016-07-31 23...	0	Visited: ameri@https://www.bing.com/secure/Passport.a	Bing
							2016-07-31 23...	0	Visited: ameri@https://www.google.co.kr/?gfe_rd=cr&ei=	microsoft edge - Google Search
							2016-07-31 23...	0	Visited: ameri@javascript:"	
							2016-07-31 23...	0	Visited: ameri@about:blank	
							2016-07-31 23...	0	Visited: ameri@https://www.[illegible]co.kr/url?sa=t&rct=j&	
							2016-07-31 23...	0	Visited: ameri@https://[illegible]microsoft.com/en-us/silentau	
							2016-07-31 23...	0	Visited: ameri@htt[illegible]staticxx.facebook.com/connect/x	
							2016-07-31 23...	0	Visited: ameri@[illegible]://www.microsoft.com/en-us/silentau	New Page
							2016-07-31 23...	0	Visited: am[illegible]https://stags.bluekai.com/site/33548?ret	
							2016-07-31 23...	0	Visited[illegible]eri@https://www.microsoft.com/en-us/window	
							2016-07-31 23...	0	Visi[illegible] ameri@https://login.live.com/me.srf?wa=wsignin1....	
							2016-07-31 23...	0	[illegible]ted: ameri@https://rp.gwallet.com/r1/pixel/x8208	
							2016-07-31 23...	0	Visited: ameri@https://www.google.co.kr/url?sa=t&rct=j&q...	
							2016-07-31 23...	0	Visited: ameri@https://apis.google.com/se/0/_/+1/fastbut...	
							2016-07-31 23...	0	Visited: ameri@https://googleads.g.doubleclick.net/pagea...	
							2016-07-[illegible]23...	0	Visited: ameri@https://accounts.google.com/o/oauth2/po...	
							[illegible]	0	Visited: ameri@https://googleads.g.doubleclick.net/pagea...	
							[illegible]31 23...	0	Visited: ameri@https://apis.google.com/se/0/_/+1/fastbut...	
							2016-0[illegible]23...	0	Visited: ameri@https://www.facebook.com/plugins/like.ph...	
							2016-07-31 23...	0	Visited: ameri@https://googleads.g.doubleclick.net/pagea...	
							2016-07-31 23...	0	Visited: ameri@https://googleads.g.doubleclick.net/pagea...	
							2016-07-31 23...	0	Visited: ameri@https://cm.g.doubleclick.net/push?client=c	
							2016-07-31 23...	0	Visited: ameri@https://googleads.g.doubleclick.net/page	
							2016-07-31 23...	0	Visited: ameri@https://platform.twitter.com/widgets/twee	
							2016-07-31 23...	0	Visited: ameri@https://notepad-plus-plus.org/d[illegible]	Notepad++ v6.9.2 - Current Version
							2016-07-31 23...	0	Visited: ameri@https://www.google[illegible]pagead/drt/ui	
							2016-07-31 23...	0	Visited: ameri@https://notepa[illegible]plus.org/repository/6	

WebPageInfo

microsoft edge - Bing

Bing

microsoft edge - Google Search

New Page

Microsoft Edge Browser

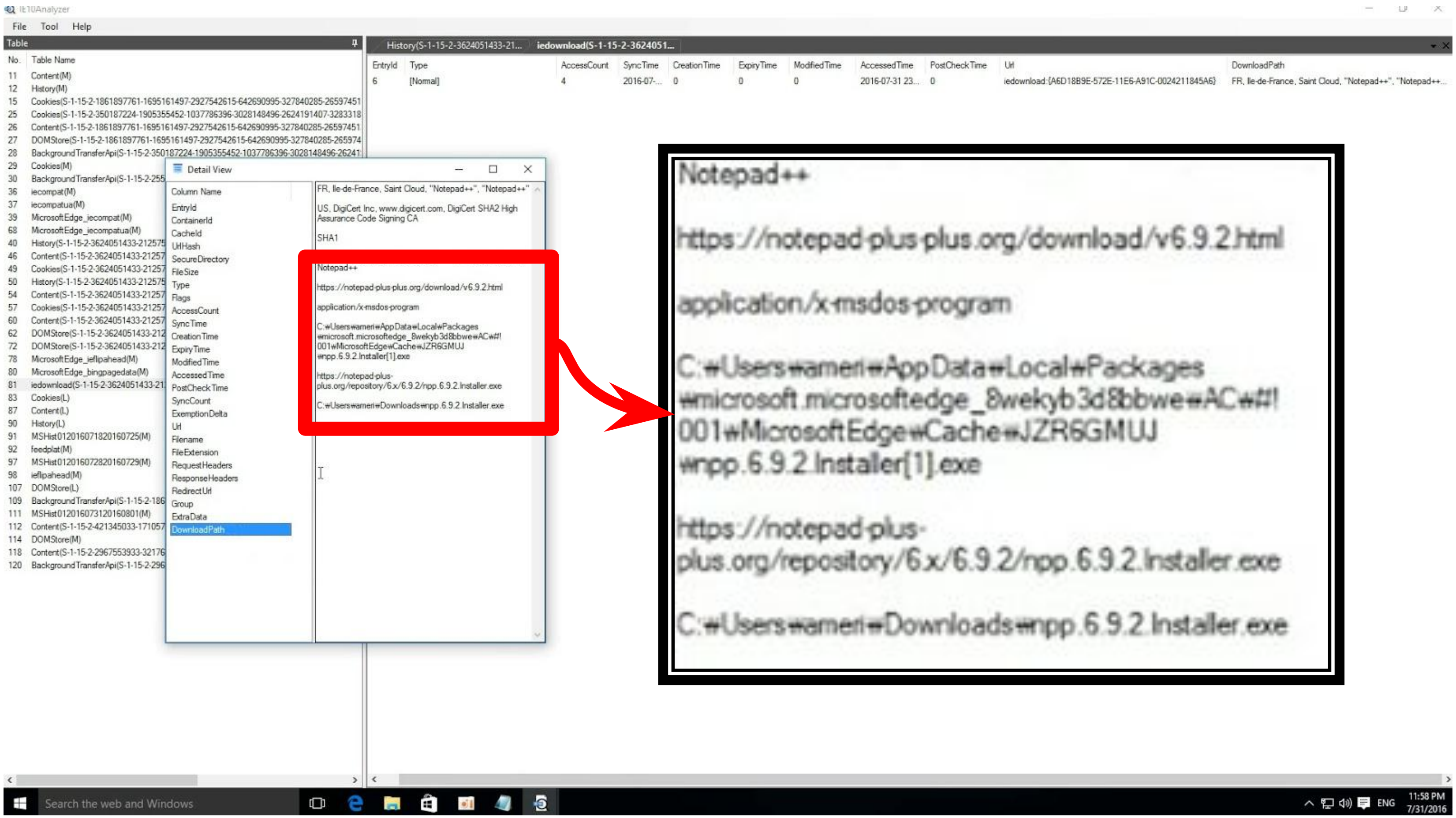
Notepad++ v6.9.2 - Current Version

- youtube title : "Internet Explorer 10, Microsoft Edge Forensic on Windows 10 "

Introduction

- **If I recovery deleted records from ESE database, What can I see?**

6) Confirm the result - download information (remains!)


IE10Analyzer
File
Tool
Help
Table
History(S-1-15-2-3624051433-21...
iedownload(S-1-15-2-3624051...
Detail View
Search the web and Windows
ENG
11:58 PM
7/31/2016

No.	Table Name
11	Content(M)
12	History(M)
15	Cookies(S-1-15-2-1861897761-1695161497-2927542615-642690995-327840285-26597451
25	Cookies(S-1-15-2-350187224-1905355452-1037786396-3028148496-2624191407-3283318
26	Content(S-1-15-2-1861897761-1695161497-2927542615-642690995-327840285-26597451
27	DOMStore(S-1-15-2-1861897761-1695161497-2927542615-642690995-327840285-265974
28	BackgroundTransferApi(S-1-15-2-350187224-1905355452-1037786396-3028148496-26241
29	Cookies(M)
30	BackgroundTransferApi(S-1-15-2-255
36	iecompat(M)
37	iecompatua(M)
39	MicrosoftEdge_iecompat(M)
68	MicrosoftEdge_iecompatua(M)
40	History(S-1-15-2-3624051433-212575
46	Content(S-1-15-2-3624051433-21257
49	Cookies(S-1-15-2-3624051433-21257
50	History(S-1-15-2-3624051433-212575
54	Content(S-1-15-2-3624051433-21257
57	Cookies(S-1-15-2-3624051433-21257
60	Content(S-1-15-2-3624051433-21257
62	DOMStore(S-1-15-2-3624051433-212
72	DOMStore(S-1-15-2-3624051433-212
78	MicrosoftEdge_ieflipahead(M)
80	MicrosoftEdge_bingpagedata(M)
81	iedownload(S-1-15-2-3624051433-21
83	Cookies(L)
87	Content(L)
90	History(L)
91	MSHist012016071820160725(M)
92	feedplat(M)
97	MSHist012016072820160729(M)
98	ieflipahead(M)
107	DOMStore(L)
109	BackgroundTransferApi(S-1-15-2-186
111	MSHist012016073120160801(M)
112	Content(S-1-15-2-421345033-171057
114	DOMStore(M)
118	Content(S-1-15-2-2967553933-32176
120	BackgroundTransferApi(S-1-15-2-296

EntryId	Type	AccessCount	SyncTime	CreationTime	ExpiryTime	ModifiedTime	AccessedTime	PostCheckTime	Url	DownloadPath
6	[Normal]	4	2016-07-...	0	0	0	2016-07-31 23...	0	iedownload:{A6D18B9E-572E-11E6-A91C-0024211845A6}	FR, Ile-de-France, Saint Cloud, "Notepad++", "Notepad++...

Column Name
EntryId
ContainerId
CacheId
UrlHash
SecureDirectory
FileSize
Type
Flags
AccessCount
SyncTime
CreationTime
ExpiryTime
ModifiedTime
AccessedTime
PostCheckTime
SyncCount
ExemptionDelta
Url
Filename
FileExtension
RequestHeaders
ResponseHeaders
RedirectUrl
Group
ExtraData
DownloadPath

FR, Ile-de-France, Saint Cloud, "Notepad++", "Notepad++"

US, DigiCert Inc, www.digicert.com, DigiCert SHA2 High Assurance Code Signing CA

SHA1

Notepad++

https://notepad-plus-plus.org/download/v6.9.2.html

application/x-msdos-program

C:₩Users₩ameri₩AppData₩Local₩Packages₩microsoft.microsoftedge_8wekyb3d8bbwe₩AC₩#!001₩MicrosoftEdge₩Cache₩JZR6GMUJ₩npp.6.9.2.Installer[1].exe

https://notepad-plus-plus.org/repository/6.x/6.9.2/npp.6.9.2.Installer.exe

C:₩Users₩ameri₩Downloads₩npp.6.9.2.Installer.exe

Notepad++

https://notepad-plus-plus.org/download/v6.9.2.html

application/x-msdos-program

C:₩Users₩ameri₩AppData₩Local₩Packages₩microsoft.microsoftedge_8wekyb3d8bbwe₩AC₩#!001₩MicrosoftEdge₩Cache₩JZR6GMUJ₩npp.6.9.2.Installer[1].exe

https://notepad-plus-plus.org/repository/6.x/6.9.2/npp.6.9.2.Installer.exe

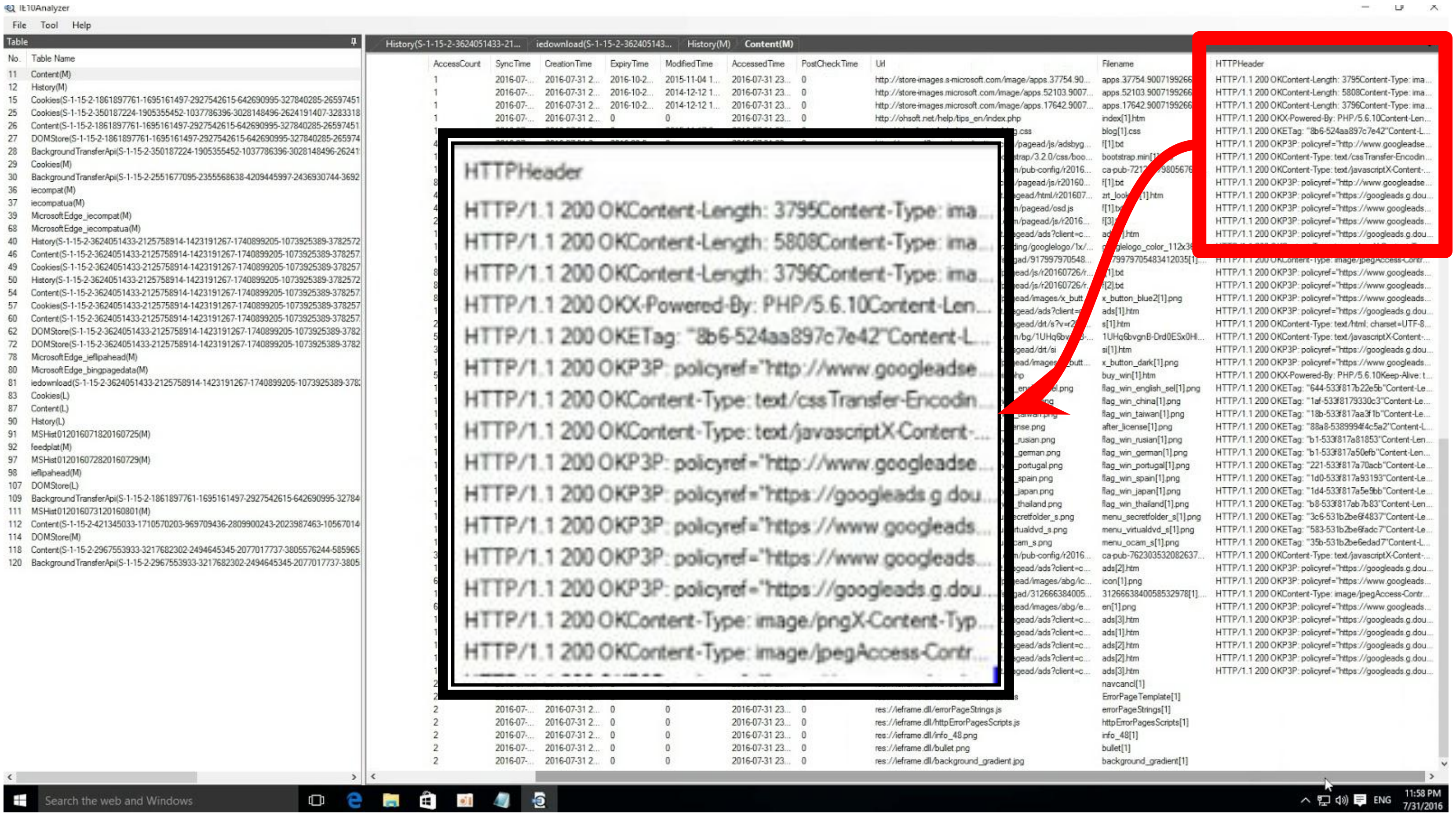
C:₩Users₩ameri₩Downloads₩npp.6.9.2.Installer.exe

- youtube title : "Internet Explorer 10, Microsoft Edge Forensic on Windows 10 "

Introduction

- **If I recovery deleted records from ESE database, What can I see?**

6) Confirm the result   - HTTP response header (remains!)


IE10Analyzer
File
Tool
Help
Table
History(S-1-15-2-3624051433-21...
iedownload(S-1-15-2-362405143...
History(M)
Content(M)
Search the web and Windows
ENG
11:58 PM
7/31/2016

No.	Table Name
11	Content(M)
12	History(M)
15	Cookies(S-1-15-2-1861897761-1695161497-2927542615-642690995-327840285-26597451
25	Cookies(S-1-15-2-350187224-1905355452-1037786396-3028148496-2624191407-3283318
26	Content(S-1-15-2-1861897761-1695161497-2927542615-642690995-327840285-26597451
27	DOMStore(S-1-15-2-1861897761-1695161497-2927542615-642690995-327840285-265974
28	BackgroundTransferApi(S-1-15-2-350187224-1905355452-1037786396-3028148496-26241
29	Cookies(M)
30	BackgroundTransferApi(S-1-15-2-2551677095-2355568638-4209445997-2436930744-3692
36	iecompat(M)
37	iecompatua(M)
39	MicrosoftEdge_iecompat(M)
68	MicrosoftEdge_iecompatua(M)
40	History(S-1-15-2-3624051433-2125758914-1423191267-1740899205-1073925389-3782572
46	Content(S-1-15-2-3624051433-2125758914-1423191267-1740899205-1073925389-378257
49	Cookies(S-1-15-2-3624051433-2125758914-1423191267-1740899205-1073925389-378257
50	History(S-1-15-2-3624051433-2125758914-1423191267-1740899205-1073925389-3782572
54	Content(S-1-15-2-3624051433-2125758914-1423191267-1740899205-1073925389-378257
57	Cookies(S-1-15-2-3624051433-2125758914-1423191267-1740899205-1073925389-378257
60	Content(S-1-15-2-3624051433-2125758914-1423191267-1740899205-1073925389-378257
62	DOMStore(S-1-15-2-3624051433-2125758914-1423191267-1740899205-1073925389-3782
72	DOMStore(S-1-15-2-3624051433-2125758914-1423191267-1740899205-1073925389-3782
78	MicrosoftEdge_ieflipahead(M)
80	MicrosoftEdge_bingpagedata(M)
81	iedownload(S-1-15-2-3624051433-2125758914-1423191267-1740899205-1073925389-378
83	Cookies(L)
87	Content(L)
90	History(L)
91	MSHist012016071820160725(M)
92	feedplat(M)
97	MSHist012016072820160729(M)
98	ieflipahead(M)
107	DOMStore(L)
109	BackgroundTransferApi(S-1-15-2-1861897761-1695161497-2927542615-642690995-32784
111	MSHist012016073120160801(M)
112	Content(S-1-15-2-421345033-1710570203-969709436-2809900243-2023987463-10567014
114	DOMStore(M)
118	Content(S-1-15-2-2967553933-3217682302-2494645345-2077017737-3805576244-585965
120	BackgroundTransferApi(S-1-15-2-2967553933-3217682302-2494645345-2077017737-3805

AccessCount	SyncTime	CreationTime	ExpiryTime	ModifiedTime	AccessedTime	PostCheckTime	Url	Filename	HTTPHeader
1	2016-07-...	2016-07-31 2...	2016-10-2...	2015-11-04 1...	2016-07-31 23...	0	http://store-images.s-microsoft.com/image/apps.37754.90...	apps.37754.9007199266	HTTP/1.1 200 OKContent-Length: 3795Content-Type: ima...
1	2016-07-...	2016-07-31 2...	2016-10-2...	2014-12-12 1...	2016-07-31 23...	0	http://store-images.microsoft.com/image/apps.52103.9007...	apps.52103.9007199266	HTTP/1.1 200 OKContent-Length: 5808Content-Type: ima...
1	2016-07-...	2016-07-31 2...	2016-10-2...	2014-12-12 1...	2016-07-31 23...	0	http://store-images.microsoft.com/image/apps.17642.9007...	apps.17642.9007199266	HTTP/1.1 200 OKContent-Length: 3796Content-Type: ima...
1	2016-07-...	2016-07-31 2...	0	0	2016-07-31 23...	0	http://ohsoft.net/help/tips_en/index.php	index[1].htm	HTTP/1.1 200 OKX-Powered-By: PHP/5.6.10Content-Len...
							g.css	blog[1].css	HTTP/1.1 200 OKETag: "8b6-524aa897c7e42"Content-L...
							/pagead/js/adsbyg...	f[1].txt	HTTP/1.1 200 OKP3P: policyref="http://www.googleadse...
							strap/3.2.0/css/boo...	bootstrap.min[1]	HTTP/1.1 200 OKContent-Type: text/cssTransfer-Encodin...
							m/pub-config/r2016...	ca-pub-721 9805676	HTTP/1.1 200 OKContent-Type: text/javascriptX-Content-...
							/pagead/js/r20160...	f[1].txt	HTTP/1.1 200 OKP3P: policyref="http://www.googleadse...
							gead/html/r201607...	zrt_look [1].htm	HTTP/1.1 200 OKP3P: policyref="https://googleads.g.dou...
							m/pagead/osd.js	f[1].txt	HTTP/1.1 200 OKP3P: policyref="https://www.googleads...
							m/pagead/js/r2016...	f[3]	HTTP/1.1 200 OKP3P: policyref="https://www.googleads...
							gead/ads?client=c...	ad].htm	HTTP/1.1 200 OKP3P: policyref="https://googleads.g.dou...
							ding/googlelogo/1x/...	glelogo_color_112x36	
							gad/917997970548...	7997970548341 2035[1]...	HTTP/1.1 200 OKContent-Type: image/jpegAccess-Contr...
							ead/js/r20160726/r...	[1].txt	HTTP/1.1 200 OKP3P: policyref="https://www.googleads...
							ead/js/r20160726/r...	f[2].txt	HTTP/1.1 200 OKP3P: policyref="https://www.googleads...
							ead/images/x_butt...	x_button_blue2[1].png	HTTP/1.1 200 OKP3P: policyref="https://www.googleads...
							gead/ads?client=	ads[1].htm	HTTP/1.1 200 OKP3P: policyref="https://googleads.g.dou...
							gead/drt/s?v=r2	s[1].htm	HTTP/1.1 200 OKContent-Type: text/html; charset=UTF-8...
							m/bg/1UHq6bv	1UHq6bvgnB-Drd0ESx0HI...	HTTP/1.1 200 OKContent-Type: text/javascriptX-Content-...
							gead/drt/si	si[1].htm	HTTP/1.1 200 OKP3P: policyref="https://googleads.g.dou...
							ead/images butt...	x_button_dark[1].png	HTTP/1.1 200 OKP3P: policyref="https://www.googleads...
							hp	buy_win[1].htm	HTTP/1.1 200 OKX-Powered-By: PHP/5.6.10Keep-Alive: t...
							_en el.png	flag_win_english_sel[1].png	HTTP/1.1 200 OKETag: "644-533f817b22e5b"Content-Le...
							ng	flag_win_china[1].png	HTTP/1.1 200 OKETag: "1af-533f8179330c3"Content-Le...
							_taiwan.png	flag_win_taiwan[1].png	HTTP/1.1 200 OKETag: "18b-533f817aa3f1b"Content-Le...
							ense.png	after_license[1].png	HTTP/1.1 200 OKETag: "88a8-5389994f4c5a2"Content-L...
							_rusian.png	flag_win_rusian[1].png	HTTP/1.1 200 OKETag: "b1-533f817a81853"Content-Len...
							_german.png	flag_win_german[1].png	HTTP/1.1 200 OKETag: "b1-533f817a50efb"Content-Len...
							_portugal.png	flag_win_portugal[1].png	HTTP/1.1 200 OKETag: "221-533f817a70acb"Content-Le...
							_spain.png	flag_win_spain[1].png	HTTP/1.1 200 OKETag: "1d0-533f817a93193"Content-Le...
							_japan.png	flag_win_japan[1].png	HTTP/1.1 200 OKETag: "1d4-533f817a5e9bb"Content-Le...
							_thailand.png	flag_win_thailand[1].png	HTTP/1.1 200 OKETag: "b8-533f817ab7b83"Content-Len...
							ecretfolder_s.png	menu_secretfolder_s[1].png	HTTP/1.1 200 OKETag: "3c6-531b2be6f4837"Content-Le...
							rtualdvd_s.png	menu_virtualdvd_s[1].png	HTTP/1.1 200 OKETag: "583-531b2be6fadc7"Content-Le...
							cam_s.png	menu_ocam_s[1].png	HTTP/1.1 200 OKETag: "35b-531b2be6edad7"Content-L...
							m/pub-config/r2016...	ca-pub-762303532082637...	HTTP/1.1 200 OKContent-Type: text/javascriptX-Content-...
							gead/ads?client=c...	ads[2].htm	HTTP/1.1 200 OKP3P: policyref="https://googleads.g.dou...
							ead/images/abg/ic...	icon[1].png	HTTP/1.1 200 OKP3P: policyref="https://www.googleads...
							gad/312666384005...	312666384005853 2978[1]....	HTTP/1.1 200 OKContent-Type: image/jpegAccess-Contr...
							ead/images/abg/e...	en[1].png	HTTP/1.1 200 OKP3P: policyref="https://www.googleads...
							gead/ads?client=c...	ads[3].htm	HTTP/1.1 200 OKP3P: policyref="https://googleads.g.dou...
							gead/ads?client=c...	ads[1].htm	HTTP/1.1 200 OKP3P: policyref="https://googleads.g.dou...
							gead/ads?client=c...	ads[2].htm	HTTP/1.1 200 OKP3P: policyref="https://googleads.g.dou...
							gead/ads?client=c...	ads[2].htm	HTTP/1.1 200 OKP3P: policyref="https://googleads.g.dou...
							gead/ads?client=c...	ads[3].htm	HTTP/1.1 200 OKP3P: policyref="https://googleads.g.dou...
2								navcancl[1]	
2							s	ErrorPageTemplate[1]	
2	2016-07-...	2016-07-31 2...	0	0	2016-07-31 23...	0	res://ieframe.dll/errorPageStrings.js	errorPageStrings[1]	
2	2016-07-...	2016-07-31 2...	0	0	2016-07-31 23...	0	res://ieframe.dll/httpErrorPagesScripts.js	httpErrorPagesScripts[1]	
2	2016-07-...	2016-07-31 2...	0	0	2016-07-31 23...	0	res://ieframe.dll/info_48.png	info_48[1]	
2	2016-07-...	2016-07-31 2...	0	0	2016-07-31 23...	0	res://ieframe.dll/bullet.png	bullet[1]	
2	2016-07-...	2016-07-31 2...	0	0	2016-07-31 23...	0	res://ieframe.dll/background_gradient.jpg	background_gradient[1]	

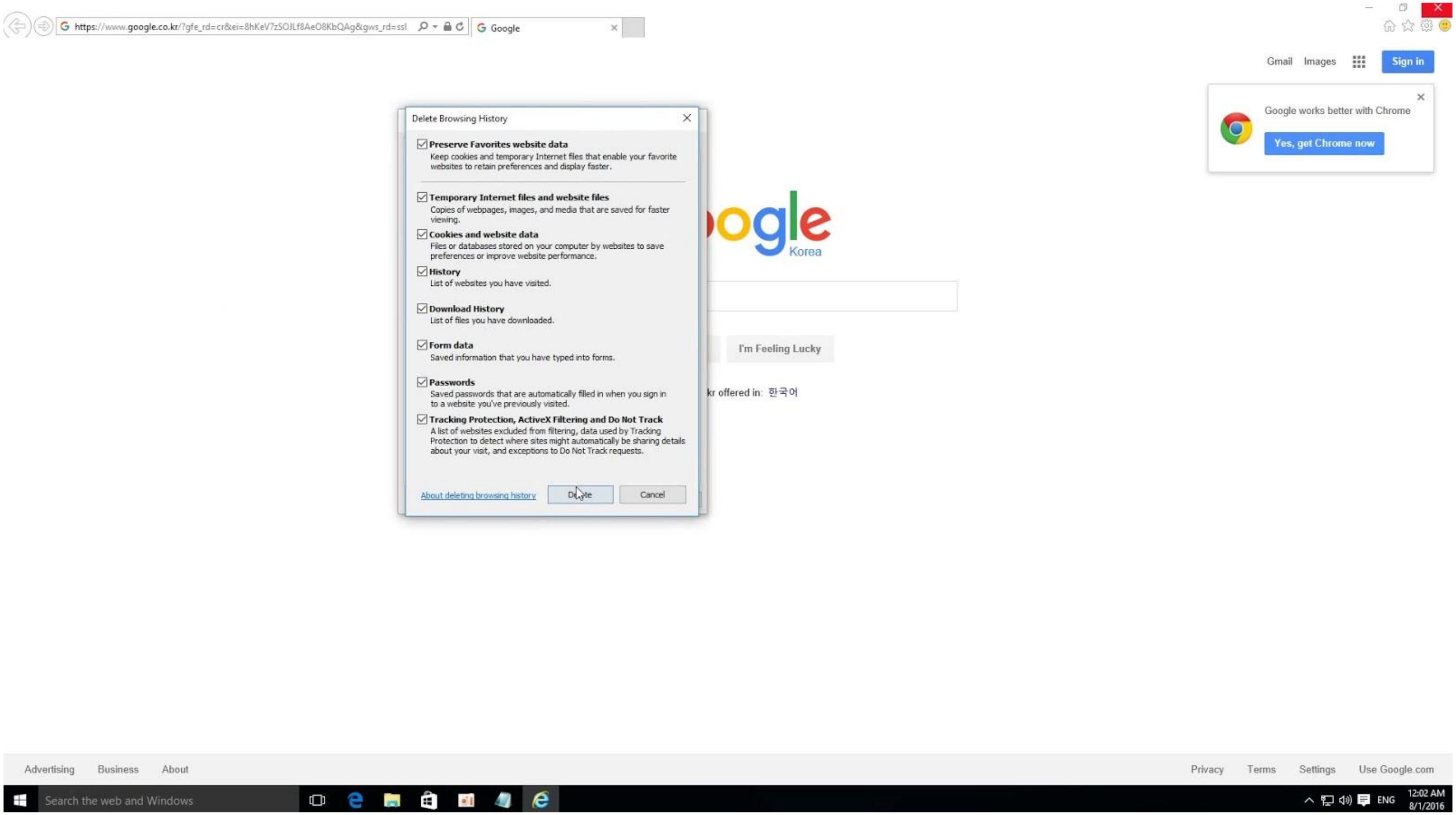
HTTPHeader
HTTP/1.1 200 OKContent-Length: 3795Content-Type: ima...
HTTP/1.1 200 OKContent-Length: 5808Content-Type: ima...
HTTP/1.1 200 OKContent-Length: 3796Content-Type: ima...
HTTP/1.1 200 OKX-Powered-By: PHP/5.6.10Content-Len...
HTTP/1.1 200 OKETag: "8b6-524aa897c7e42"Content-L...
HTTP/1.1 200 OKP3P: policyref="http://www.googleadse...
HTTP/1.1 200 OKContent-Type: text/cssTransfer-Encodin...
HTTP/1.1 200 OKContent-Type: text/javascriptX-Content-...
HTTP/1.1 200 OKP3P: policyref="http://www.googleadse...
HTTP/1.1 200 OKP3P: policyref="https://googleads.g.dou...
HTTP/1.1 200 OKP3P: policyref="https://www.googleads...
HTTP/1.1 200 OKP3P: policyref="https://www.googleads...
HTTP/1.1 200 OKP3P: policyref="https://googleads.g.dou...
HTTP/1.1 200 OKContent-Type: image/pngX-Content-Typ...
HTTP/1.1 200 OKContent-Type: image/jpegAccess-Contr...

- youtube title : "Internet Explorer 10, Microsoft Edge Forensic on Windows 10 "

Introduction

- **If I recovery deleted records from ESE database, What can I see?**

7) Clear browsing data on Internet Explorer



Delete Browsing History

☑ **Preserve Favorites website data**
Keep cookies and temporary Internet files that enable your favorite websites to retain preferences and display faster.

☑ **Temporary Internet files and website files**
Copies of webpages, images, and media that are saved for faster viewing.

☑ **Cookies and website data**
Files or databases stored on your computer by websites to save preferences or improve website performance.

☑ **History**
List of websites you have visited.

☑ **Download History**
List of files you have downloaded.

☑ **Form data**
Saved information that you have typed into forms.

☑ **Passwords**
Saved passwords that are automatically filled in when you sign in to a website you've previously visited.

☑ **Tracking Protection, ActiveX Filtering and Do Not Track**
A list of websites excluded from filtering, data used by Tracking Protection to detect where sites might automatically be sharing details about your visit, and exceptions to Do Not Track requests.

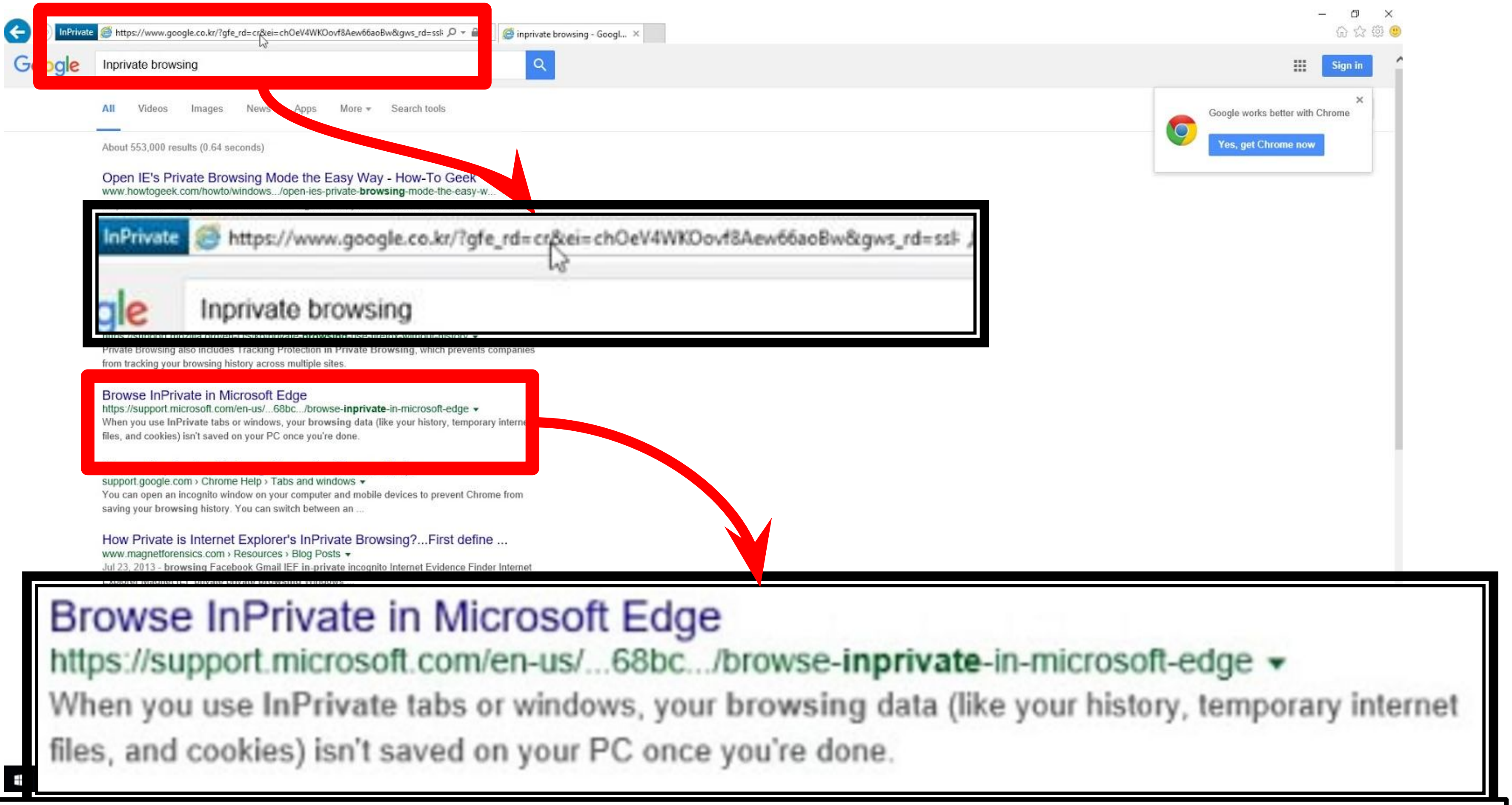
About deleting browsing history

- youtube title : "Internet Explorer 10, Microsoft Edge Forensic on Windows 10 "

Introduction

- **If I recovery deleted records from ESE database, What can I see?**

8) Start InPrivate Browsing



InPrivate https://www.google.co.kr/?gfe_rd=cr&ei=chOeV4WKOovf8Aew66aoBw&gws_rd=ssl

inprivate browsing - Googl...

Google Inprivate browsing

About 553,000 results (0.64 seconds)

Open IE's Private Browsing Mode the Easy Way - How-To Geek
www.howtogeek.com/howto/windows.../open-ies-private-**browsing**-mode-the-easy-w...

InPrivate https://www.google.co.kr/?gfe_rd=cr&ei=chOeV4WKOovf8Aew66aoBw&gws_rd=ssl
gle Inprivate browsing

Private Browsing also includes Tracking Protection in Private Browsing, which prevents companies from tracking your browsing history across multiple sites.

Browse InPrivate in Microsoft Edge
https://support.microsoft.com/en-us/...68bc.../browse-**inprivate**-in-microsoft-edge ▾
When you use **InPrivate** tabs or windows, your **browsing** data (like your history, temporary interne files, and cookies) isn't saved on your PC once you're done.

support.google.com › Chrome Help › Tabs and windows ▾
You can open an incognito window on your computer and mobile devices to prevent Chrome from saving your **browsing** history. You can switch between an ...

How Private is Internet Explorer's InPrivate Browsing?...First define ...
www.magnetforensics.com › Resources › Blog Posts ▾
Jul 23, 2013 - **browsing** Facebook Gmail IEF **in-private** incognito Internet Evidence Finder Internet

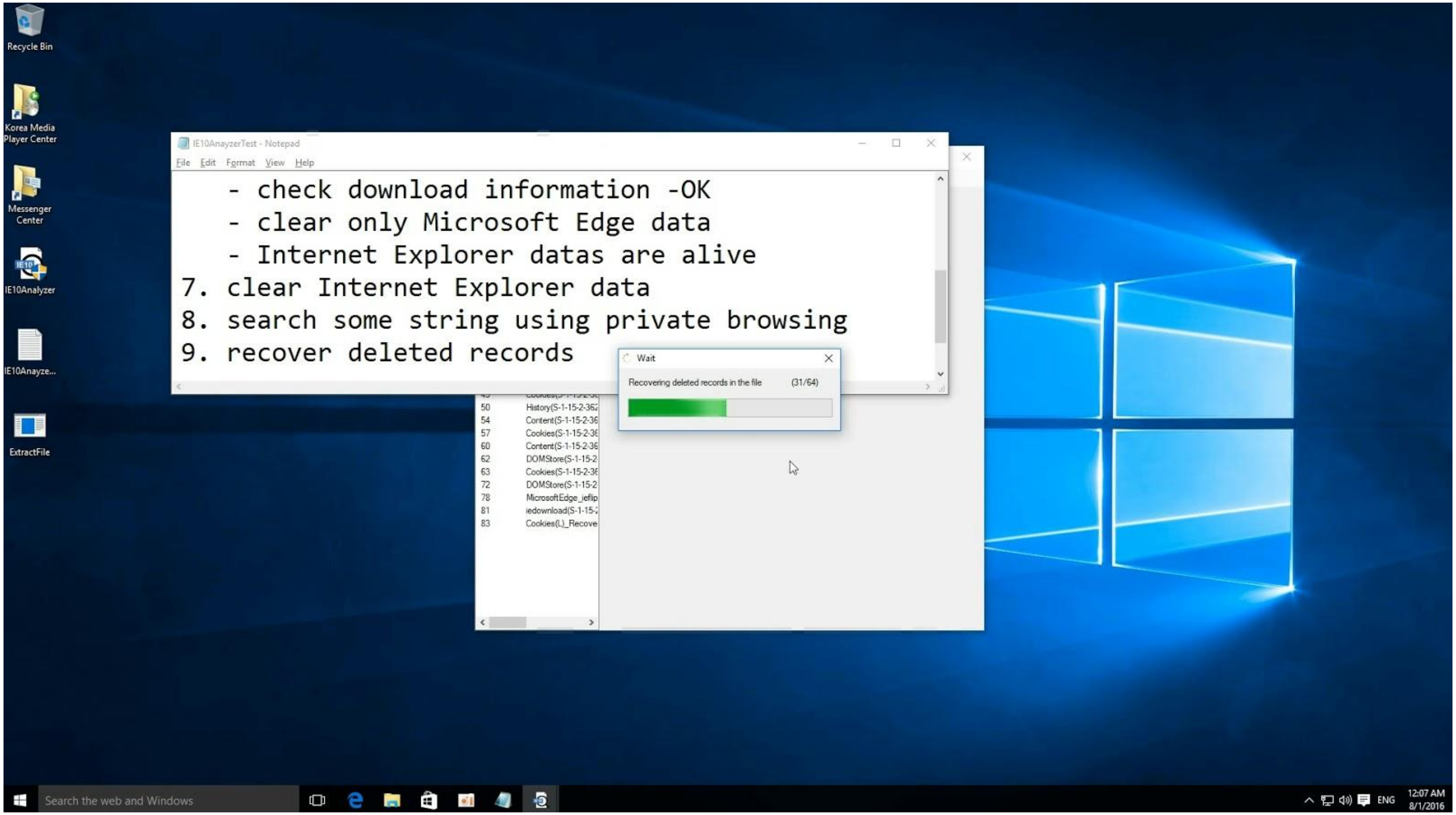
Browse InPrivate in Microsoft Edge
https://support.microsoft.com/en-us/...68bc.../browse-**inprivate**-in-microsoft-edge ▾
When you use **InPrivate** tabs or windows, your **browsing** data (like your history, temporary internet files, and cookies) isn't saved on your PC once you're done.

- youtube title : "Internet Explorer 10, Microsoft Edge Forensic on Windows 10 "

Introduction

- **If I recovery deleted records from ESE database, What can I see?**

9) Confirm the result about recovered data


Recycle Bin
Korea Media Player Center
Messenger Center
IE10Analyzer
IE10Anayze...
ExtractFile
IE10AnayzerTest - Notepad
File Edit Format View Help
Wait
Search the web and Windows
ENG
12:07 AM
8/1/2016

```
    - check download information -OK
    - clear only Microsoft Edge data
    - Internet Explorer datas are alive
7. clear Internet Explorer data
8. search some string using private browsing
9. recover deleted records
```

Recovering deleted records in the file (31/64)

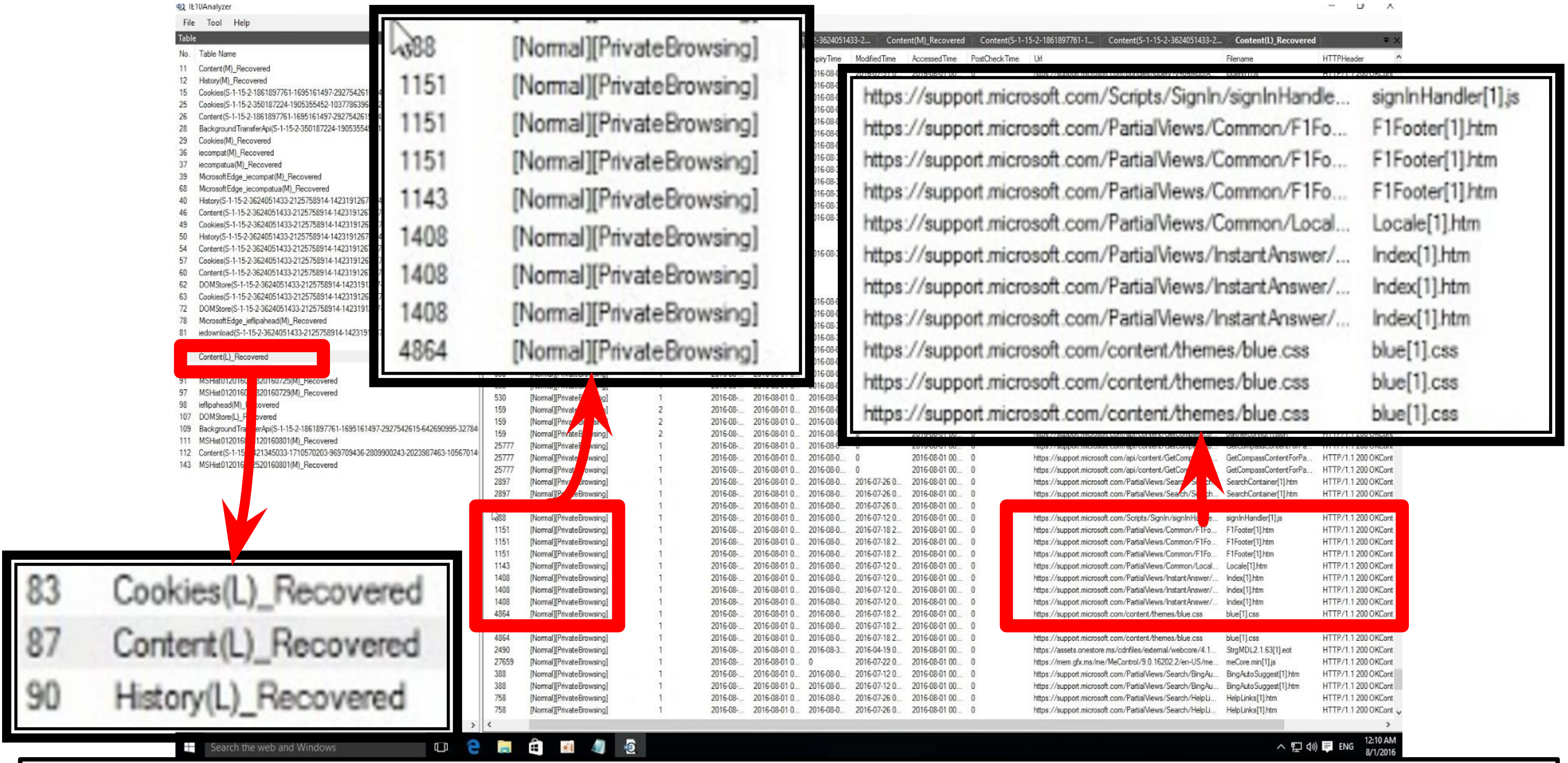
```
50    History(S-1-15-2-362
54    Content(S-1-15-2-36
57    Cookies(S-1-15-2-36
60    Content(S-1-15-2-36
62    DOMStore(S-1-15-2
63    Cookies(S-1-15-2-36
72    DOMStore(S-1-15-2
78    MicrosoftEdge_ieflip
81    iedownload(S-1-15-2
83    Cookies(L)_Recove
```

- youtube title : "Internet Explorer 10, Microsoft Edge Forensic on Windows 10 "

Introduction

- **If I recovery deleted records from ESE database, What can I see?**

10) Confirm the result about private browsing



No.	Table Name
11	Content(M)_Recovered
12	History(M)_Recovered
15	Cookies(S-1-15-2-1861897761-1695161497-292754261
25	Cookies(S-1-15-2-350187224-1905355452-1037786396
26	Content(S-1-15-2-1861897761-1695161497-292754261
28	BackgroundTransferApi(S-1-15-2-350187224-19053554
29	Cookies(M)_Recovered
36	iecompat(M)_Recovered
37	iecompatua(M)_Recovered
39	MicrosoftEdge_iecompat(M)_Recovered
68	MicrosoftEdge_iecompatua(M)_Recovered
40	History(S-1-15-2-3624051433-2125758914-1423191267
46	Content(S-1-15-2-3624051433-2125758914-142319126
49	Cookies(S-1-15-2-3624051433-2125758914-142319126
50	History(S-1-15-2-3624051433-2125758914-1423191267
54	Content(S-1-15-2-3624051433-2125758914-142319126
57	Cookies(S-1-15-2-3624051433-2125758914-142319126
60	Content(S-1-15-2-3624051433-2125758914-142319126
62	DOMStore(S-1-15-2-3624051433-2125758914-1423191
63	Cookies(S-1-15-2-3624051433-2125758914-142319126
72	DOMStore(S-1-15-2-3624051433-2125758914-1423191
78	MicrosoftEdge_ieflipahead(M)_Recovered
81	iedownload(S-1-15-2-3624051433-2125758914-142319
	Content(L)_Recovered
91	MSHist0120160 320160725(M)_Recovered
97	MSHist0120160 320160729(M)_Recovered
98	ieflipahead(M)_ covered
107	DOMStore(L)_F overed
109	BackgroundTra erApi(S-1-15-2-1861897761-1695161497-2927542615-642690995-32784
111	MSHist012016 120160801(M)_Recovered
112	Content(S-1-15 21345033-1710570203-969709436-2809900243-2023987463-10567014
143	MSHist012016 2520160801(M)_Recovered

83	Cookies(L)_Recovered
87	Content(L)_Recovered
90	History(L)_Recovered

388	[Normal][PrivateBrowsing]
1151	[Normal][PrivateBrowsing]
1151	[Normal][PrivateBrowsing]
1151	[Normal][PrivateBrowsing]
1143	[Normal][PrivateBrowsing]
1408	[Normal][PrivateBrowsing]
1408	[Normal][PrivateBrowsing]
1408	[Normal][PrivateBrowsing]
4864	[Normal][PrivateBrowsing]

https://support.microsoft.com/Scripts/SignIn/signInHandle...	signInHandler[1].js
https://support.microsoft.com/PartialViews/Common/F1Fo...	F1Footer[1].htm
https://support.microsoft.com/PartialViews/Common/F1Fo...	F1Footer[1].htm
https://support.microsoft.com/PartialViews/Common/F1Fo...	F1Footer[1].htm
https://support.microsoft.com/PartialViews/Common/Local...	Locale[1].htm
https://support.microsoft.com/PartialViews/InstantAnswer/...	Index[1].htm
https://support.microsoft.com/PartialViews/InstantAnswer/...	Index[1].htm
https://support.microsoft.com/PartialViews/InstantAnswer/...	Index[1].htm
https://support.microsoft.com/content/themes/blue.css	blue[1].css
https://support.microsoft.com/content/themes/blue.css	blue[1].css
https://support.microsoft.com/content/themes/blue.css	blue[1].css

- youtube title : "Internet Explorer 10, Microsoft Edge Forensic on Windows 10 "

Introduction

- **Anyone can delete records in ESE database**
  - Use Microsoft.Isam.Esent.Interop.Api

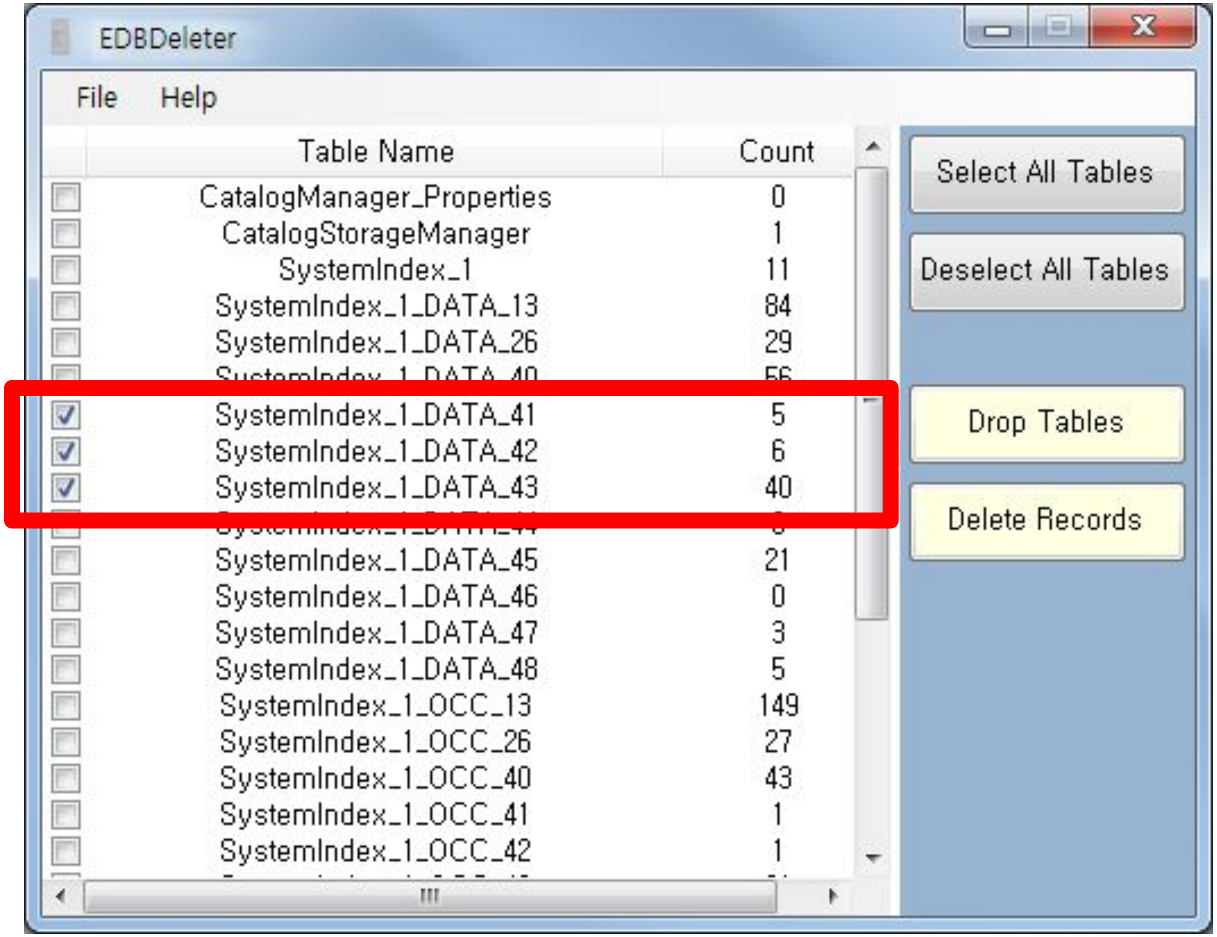


	Table Name	Count
□	CatalogManager_Properties	0
□	CatalogStorageManager	1
□	SystemIndex_1	11
□	SystemIndex_1_DATA_13	84
□	SystemIndex_1_DATA_26	29
□	SystemIndex_1_DATA_40	56
☑	SystemIndex_1_DATA_41	5
☑	SystemIndex_1_DATA_42	6
☑	SystemIndex_1_DATA_43	40
□	SystemIndex_1_DATA_44	[illegible]
□	SystemIndex_1_DATA_45	21
□	SystemIndex_1_DATA_46	0
□	SystemIndex_1_DATA_47	3
□	SystemIndex_1_DATA_48	5
□	SystemIndex_1_OCC_13	149
□	SystemIndex_1_OCC_26	27
□	SystemIndex_1_OCC_40	43
□	SystemIndex_1_OCC_41	1
□	SystemIndex_1_OCC_42	1

Introduction

- **Anyone can delete records in ESE database**
  - Use Microsoft.Isam.Esent.Interop.Api

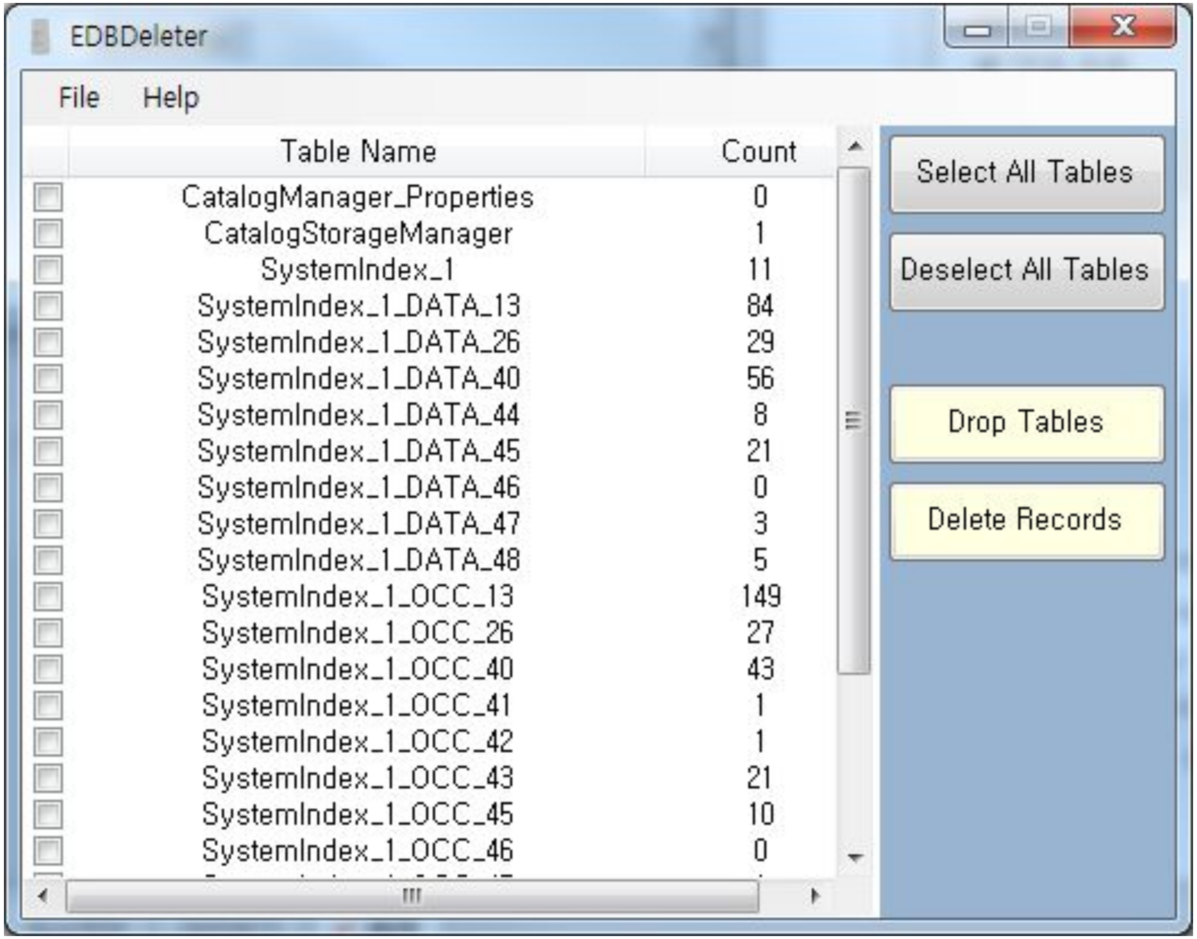


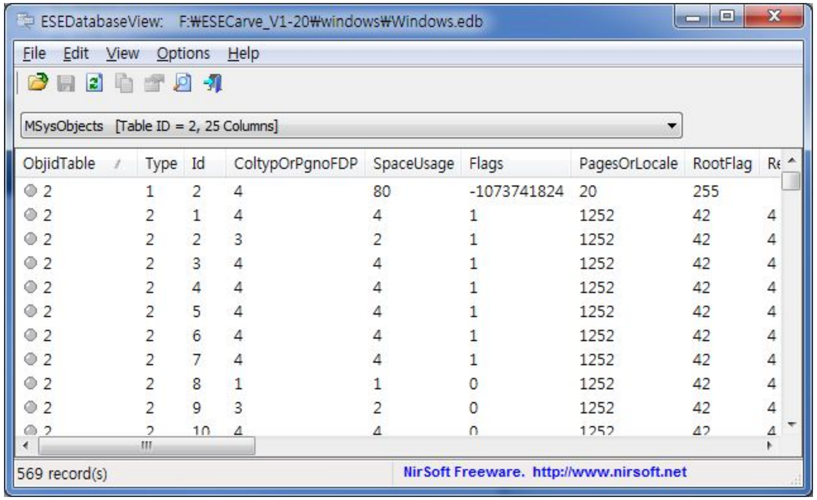
	Table Name	Count
□	CatalogManager_Properties	0
□	CatalogStorageManager	1
□	SystemIndex_1	11
□	SystemIndex_1_DATA_13	84
□	SystemIndex_1_DATA_26	29
□	SystemIndex_1_DATA_40	56
□	SystemIndex_1_DATA_44	8
□	SystemIndex_1_DATA_45	21
□	SystemIndex_1_DATA_46	0
□	SystemIndex_1_DATA_47	3
□	SystemIndex_1_DATA_48	5
□	SystemIndex_1_OCC_13	149
□	SystemIndex_1_OCC_26	27
□	SystemIndex_1_OCC_40	43
□	SystemIndex_1_OCC_41	1
□	SystemIndex_1_OCC_42	1
□	SystemIndex_1_OCC_43	21
□	SystemIndex_1_OCC_45	10
□	SystemIndex_1_OCC_46	0

Relate works

- **Problem with existing viewer**
  - ESEDatabaseView
    - Output a wrong value
    - Output empty screen

      (if a table has a complex data structure)
  - EseDbViewer
    - Can read normally-terminated files alone

      (Can not read dirty-status files)


ESEDatabaseView: F:₩ESECarve_V1-20₩windows₩Windows.edb
File Edit View Options Help

MSysObjects [Table ID = 2, 25 Columns]

ObjidTable	Type	Id	ColtypOrPgnoFDP	SpaceUsage	Flags	PagesOrLocale	RootFlag	Re
2	1	2	4	80	-1073741824	20	255	
2	2	1	4	4	1	1252	42	4
2	2	2	3	2	1	1252	42	4
2	2	3	4	4	1	1252	42	4
2	2	4	4	4	1	1252	42	4
2	2	5	4	4	1	1252	42	4
2	2	6	4	4	1	1252	42	4
2	2	7	4	4	1	1252	42	4
2	2	8	1	1	0	1252	42	4
2	2	9	3	2	0	1252	42	4
2	2	10	4	4	0	1252	42	4

569 record(s)

NirSoft Freeware. http://www.nirsoft.net

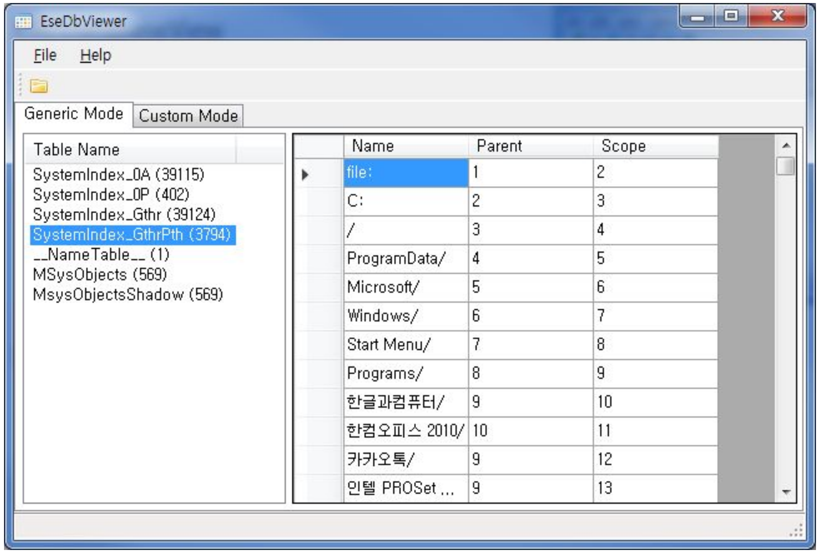
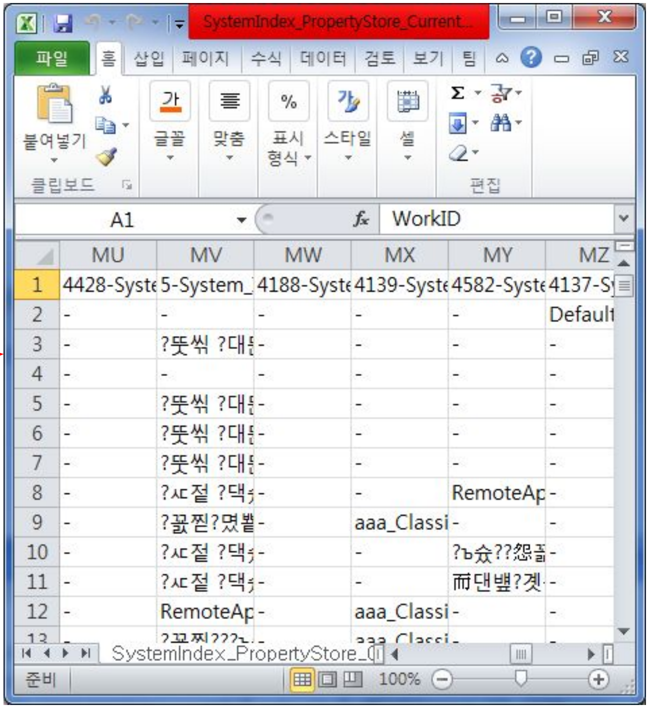


Table Name
SystemIndex_0A (39115)
SystemIndex_0P (402)
SystemIndex_Gthr (39124)
SystemIndex_GthrPth (3794)
__NameTable__ (1)
MSysObjects (569)
MsysObjectsShadow (569)

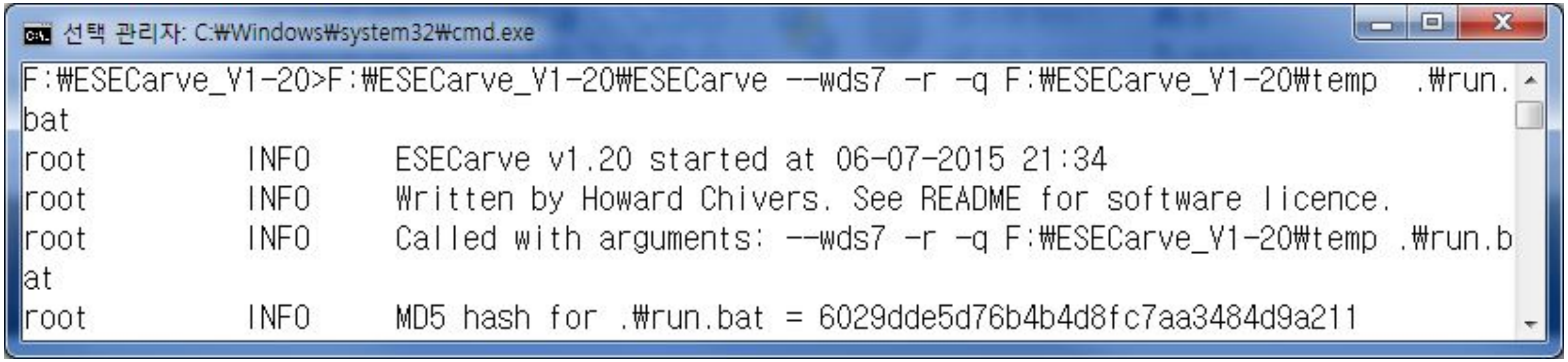
Name	Parent	Scope
file:	1	2
C:	2	3
/	3	4
ProgramData/	4	5
Microsoft/	5	6
Windows/	6	7
Start Menu/	7	8
Programs/	8	9
한글과컴퓨터/	9	10
한컴오피스 2010/	10	11
카카오톡/	9	12
인텔 PROSet ...	9	13

Relate works

- **Problem with existing recovery program**
  - ESECarve
    - Applies only to some tables
      - Windows.edb, WebCacheV01.dat
    - Can not use dirty-state files
    - Output incomprehensible words



	MU	MV	MW	MX	MY	MZ
1	4428-Syste	5-System_	4188-Syste	4139-Syste	4582-Syste	4137-Sy
2	-	-	-	-	-	Default
3	-	?뚯씪 ?대ё	-	-	-	-
4	-	-	-	-	-	-
5	-	?뚯씪 ?대ё	-	-	-	-
6	-	?뚯씪 ?대ё	-	-	-	-
7	-	?뚯씪 ?대ё	-	-	-	-
8	-	?ㅻ절 ?댁;	-	-	RemoteAp	-
9	-	?꾧찐?몄뷭	-	aaa_Classi	-	-
10	-	?ㅻ절 ?댁;	-	-	?ㅎ숏??怨곸	-
11	-	?ㅻ절 ?댁;	-	-	而댄뱄?겟	-
12	-	RemoteAp	-	aaa_Classi	-	-

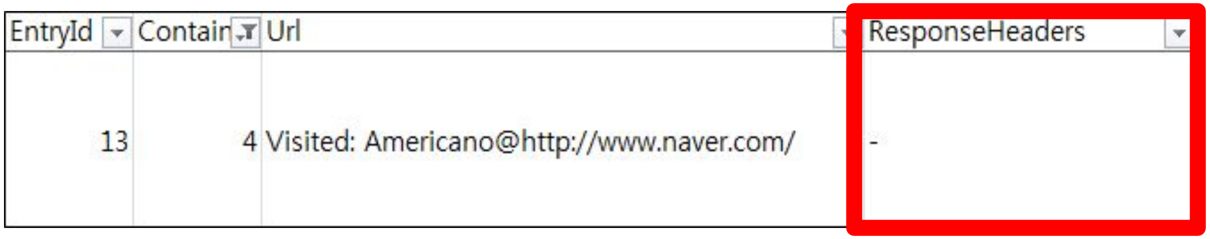


```
F:₩ESECarve_V1-20>F:₩ESECarve_V1-20₩ESECarve --wds7 -r -q F:₩ESECarve_V1-20₩temp  .₩run.
bat
root          INFO     ESECarve v1.20 started at 06-07-2015 21:34
root          INFO     Written by Howard Chivers. See README for software licence.
root          INFO     Called with arguments: --wds7 -r -q F:₩ESECarve_V1-20₩temp .₩run.b
at
root          INFO     MD5 hash for .₩run.bat = 6029dde5d76b4b4d8fc7aa3484d9a211
```

Relate works

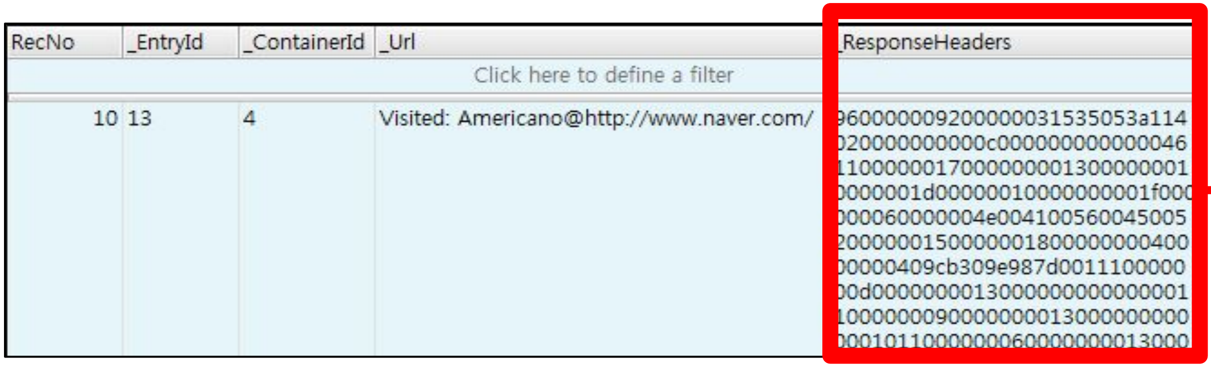
- **Problem with existing recovery program**
  - ESECarve
    - Could not recover the final field items of all the records
    - Could not recover the items saved in the LV table

[Figure] Results recovered by using ESE carve



EntryId	Contain	Url	ResponseHeaders
13	4	Visited: Americano@http://www.naver.com/	-

[Figure] Results recovered by using our recovery method

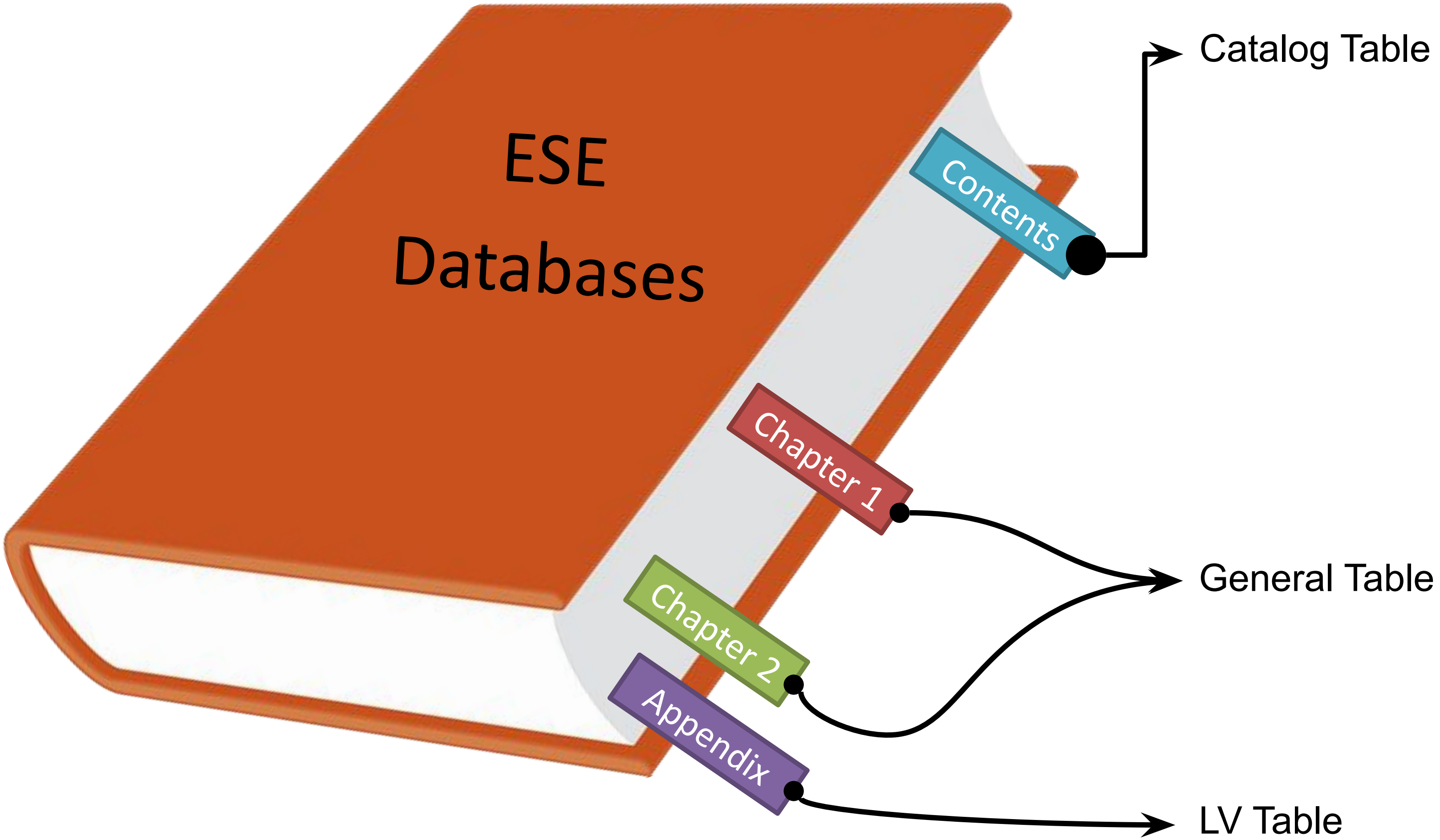


RecNo	_EntryId	_ContainerId	_Url	_ResponseHeaders
		Click here to define a filter		
10	13	4	Visited: Americano@http://www.naver.com/	9600000092000000031535053a114 020000000000c000000000000046 1100000017000000001300000001 000001d0000001000000001f000 00006000004e00410056004500 5 2000000150000001800000000400 00000409cb309e987d0011100000 00d000000001300000000000001 1000000090000000013000000000 0001011000000060000000013000

- Web page title
- HTTP Response Header
- Download information

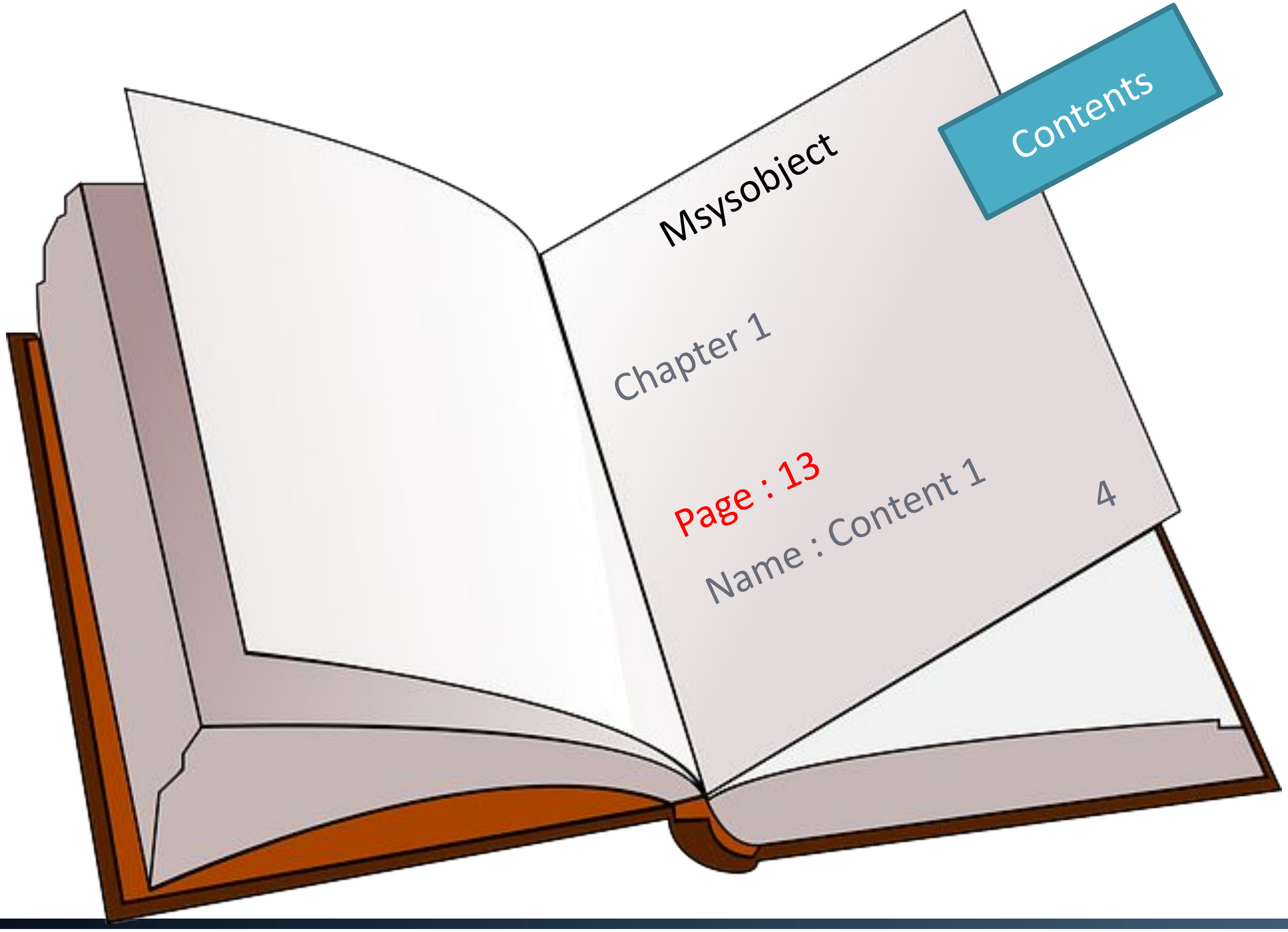
Background knowledge

- **ESE Database**



Background knowledge

- **Catalog table**
  - MSysObject table
  - Explains about all the tables including itself



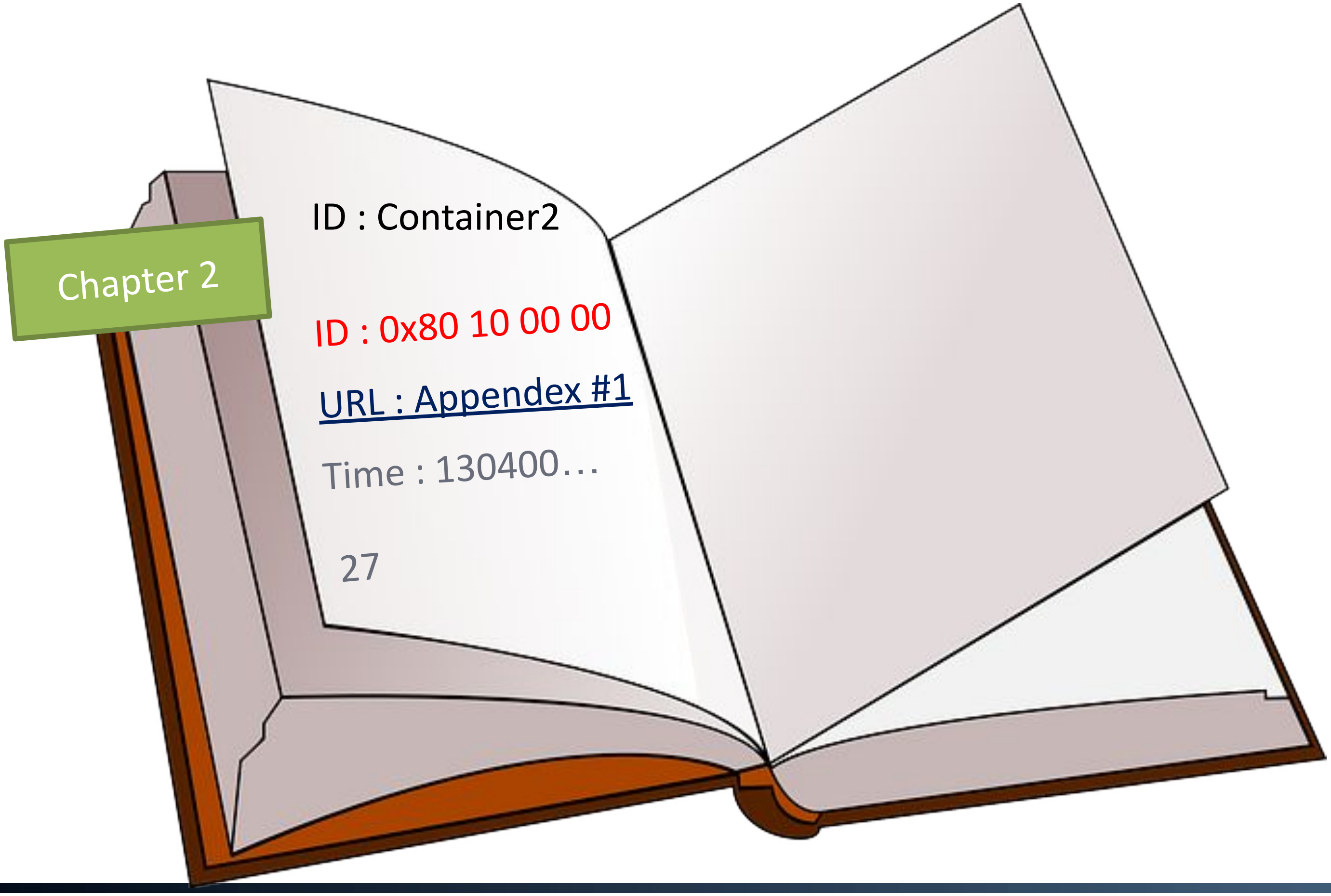
Background knowledge

- **Table**
  - Be comprised of multiple pages
  - Manage pages in B-Tree structure

ID : Container1
Chapter 1
ID : 0x80 10 00 00
URL: http://naver.com
Time : 130400…
13

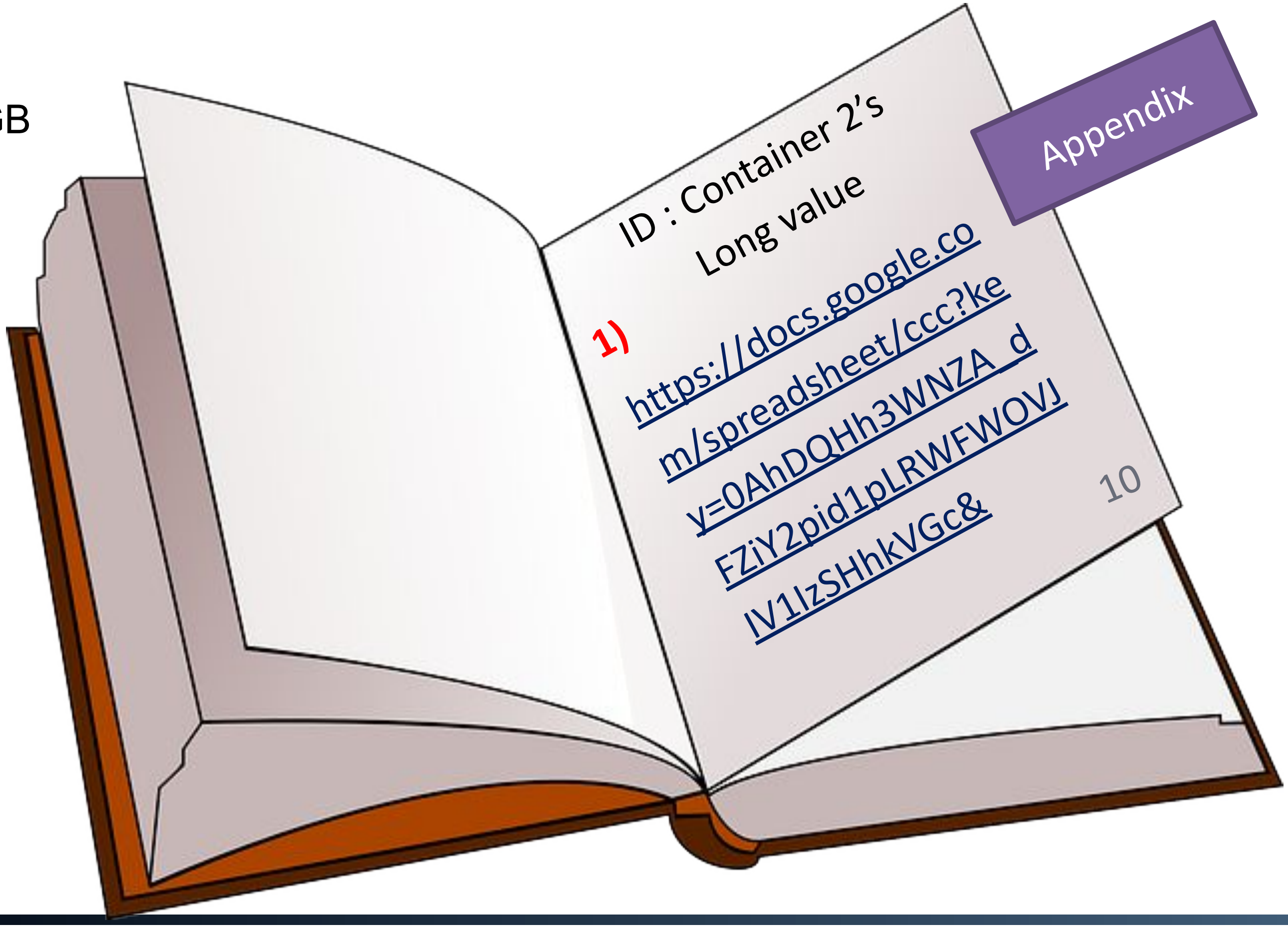
Background knowledge

- **Table** (method of saving)
  - Only one page are utilized to save data
  - Save sub-tables called LV without saving big data directly in records.



Background knowledge

- **Save long value**
  - Long value page
  - Save a data by using multiple records
  - Use Long value page
  - Maximum data size : 2GB



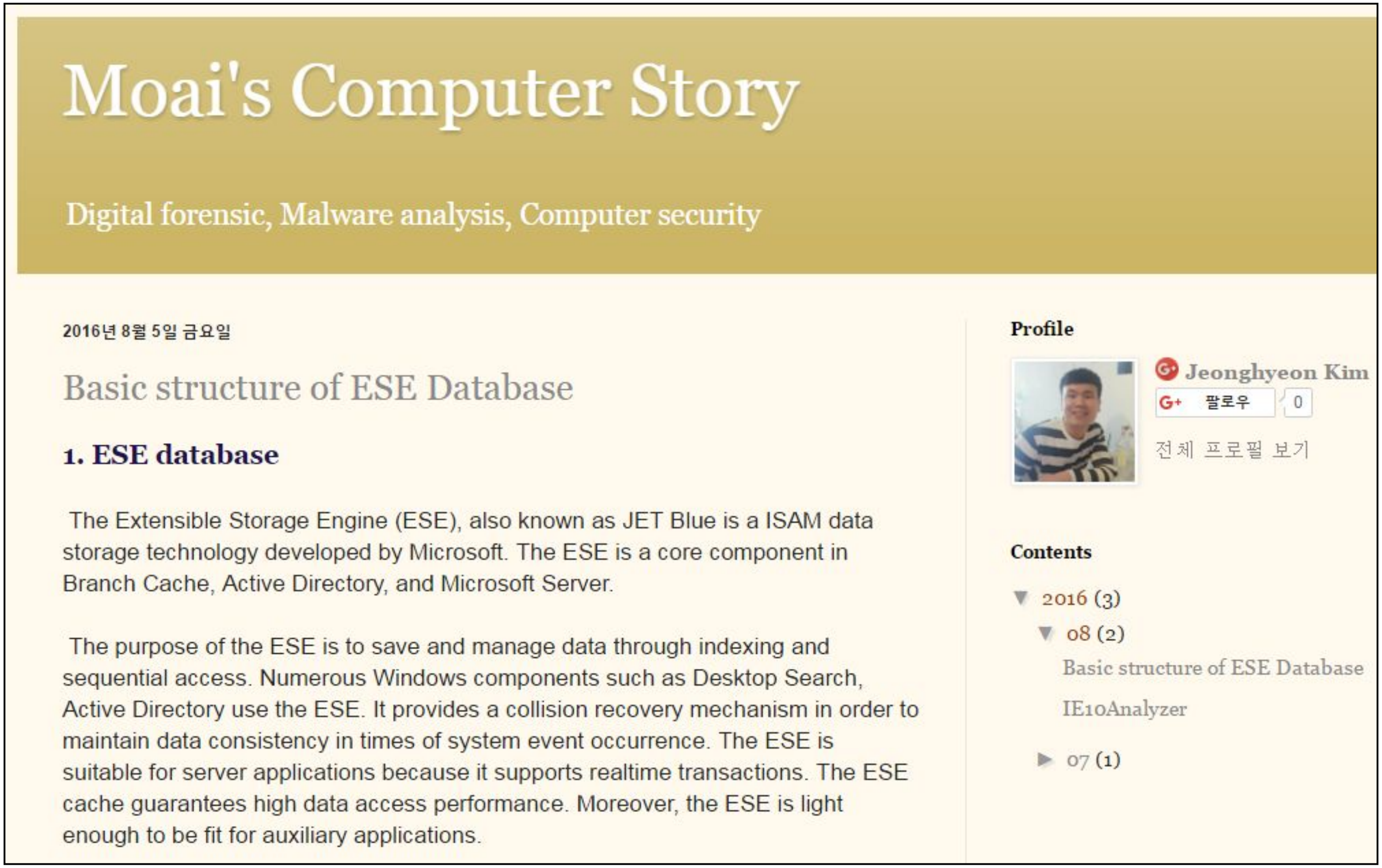
ID : Container 2's

Long value

1) https://docs.google.com/spreadsheet/ccc?key=0AhDQHh3WNZA_dFZiY2pid1pLRWFWOVJIV1IzSHhkVGc&

Background knowledge

- **Refer my blog**
  - http://moaistory.blogspot.kr/



Moai's Computer Story

Digital forensic, Malware analysis, Computer security

2016년 8월 5일 금요일

Basic structure of ESE Database

1. ESE database

The Extensible Storage Engine (ESE), also known as JET Blue is a ISAM data storage technology developed by Microsoft. The ESE is a core component in Branch Cache, Active Directory, and Microsoft Server.

The purpose of the ESE is to save and manage data through indexing and sequential access. Numerous Windows components such as Desktop Search, Active Directory use the ESE. It provides a collision recovery mechanism in order to maintain data consistency in times of system event occurrence. The ESE is suitable for server applications because it supports realtime transactions. The ESE cache guarantees high data access performance. Moreover, the ESE is light enough to be fit for auxiliary applications.

Profile

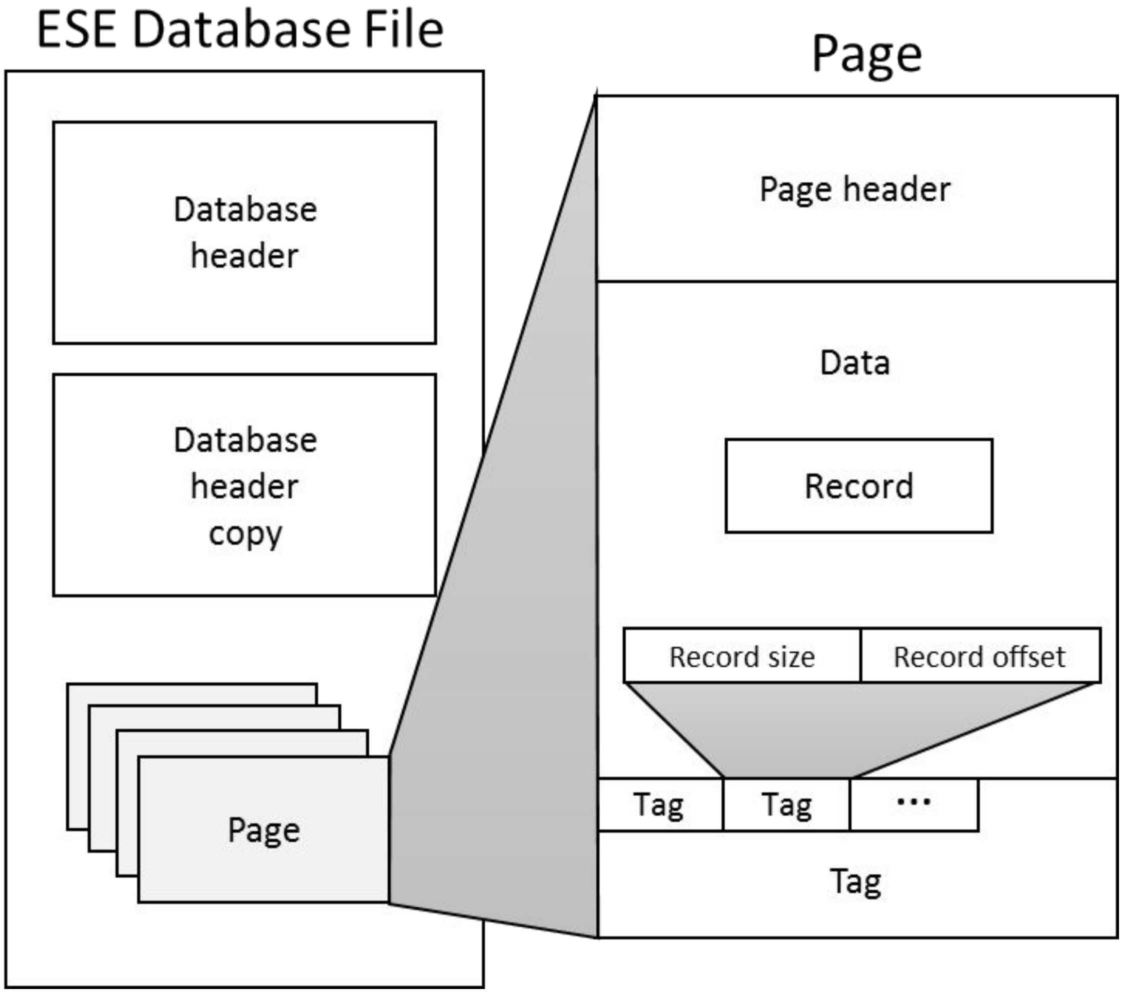
Jeonghyeon Kim

Contents

▼ 2016 (3)
▼ 08 (2)
Basic structure of ESE Database
IE10Analyzer
► 07 (1)

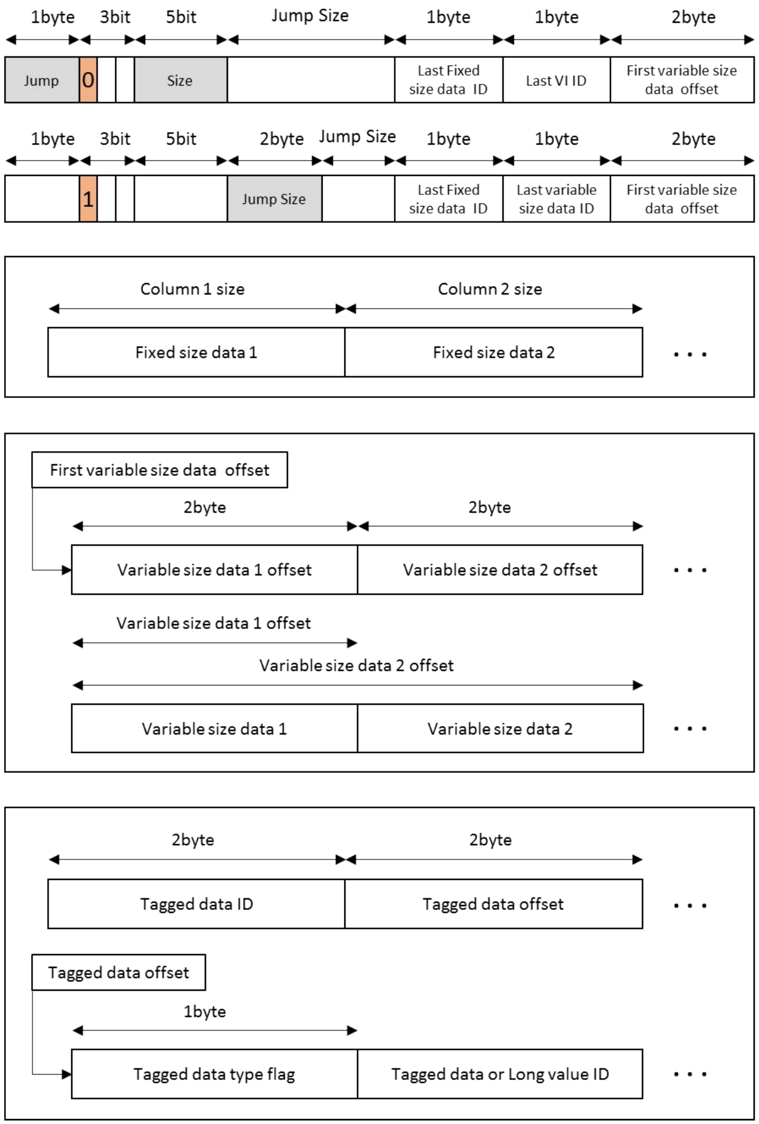
ESE database format analysis

- **Internal structure of the ESE database**



ESE database format analysis

- **Analysis of record structure**
  - Record structure differs depending on the kind of pages
    - Record analysis of data page
      - General data of a table is recorded
      - Record storage method is field-type dependent
        - Fixed size
        - Variable size(< 256)
        - Variable size(> 256)



1byte 3bit 5bit Jump Size 1byte 1byte 2byte

Jump | 0 | Size | Last Fixed size data ID | Last VI ID | First variable size data offset

1byte 3bit 5bit 2byte Jump Size 1byte 1byte 2byte

1 | Jump Size | Last Fixed size data ID | Last variable size data ID | First variable size data offset

Column 1 size

Column 2 size

Fixed size data 1 | Fixed size data 2 | . . .

First variable size data offset

2byte 2byte

Variable size data 1 offset | Variable size data 2 offset | . . .

Variable size data 1 offset

Variable size data 2 offset

Variable size data 1 | Variable size data 2 | . . .

2byte 2byte

Tagged data ID | Tagged data offset | . . .

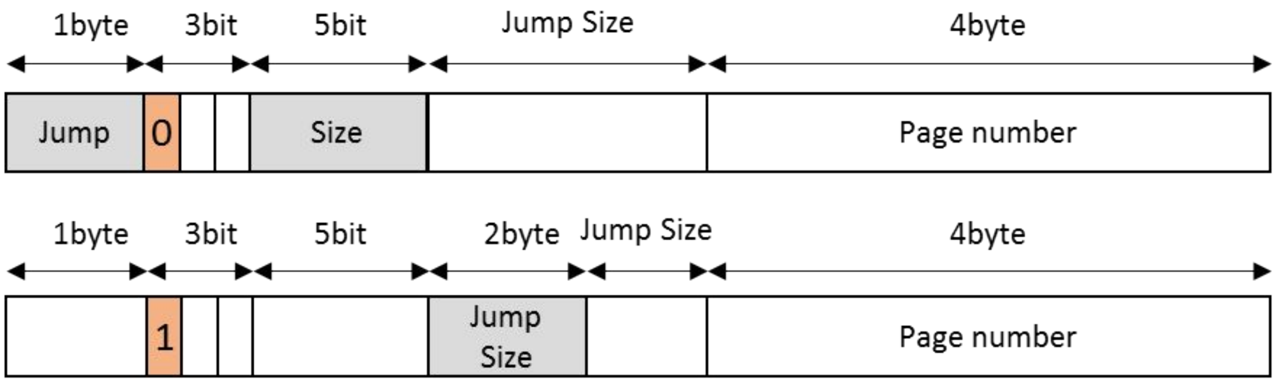
Tagged data offset

1byte

Tagged data type flag | Tagged data or Long value ID | . . .

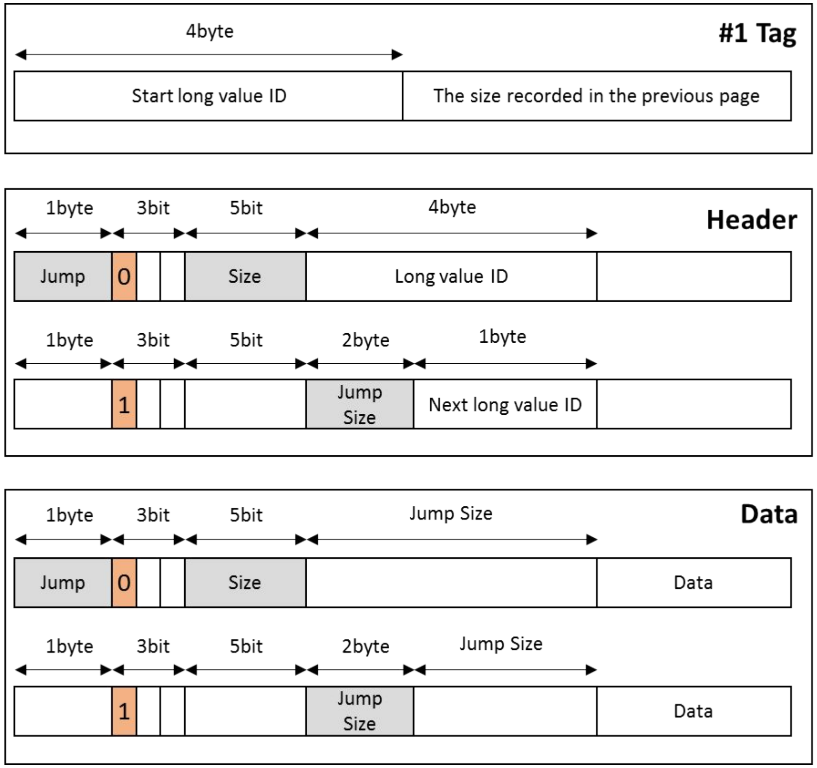
ESE database format analysis

- **Analysis of record structure**
  - Record structure differs depending on the kind of pages
    - Record analysis of branch page
      - Page number is recorded



ESE database format analysis

- **Analysis of record structure**
  - Record structure differs depending on the kind of pages
    - Record analysis of long value page
      - Save a single instance refer to multiple records and multiple pages



#1 Tag

4byte

Start long value ID | The size recorded in the previous page

Header

1byte | 3bit | 5bit | 4byte

Jump | 0 | | Size | Long value ID

1byte | 3bit | 5bit | 2byte | 1byte

| 1 | | | Jump Size | Next long value ID

Data

1byte | 3bit | 5bit | Jump Size

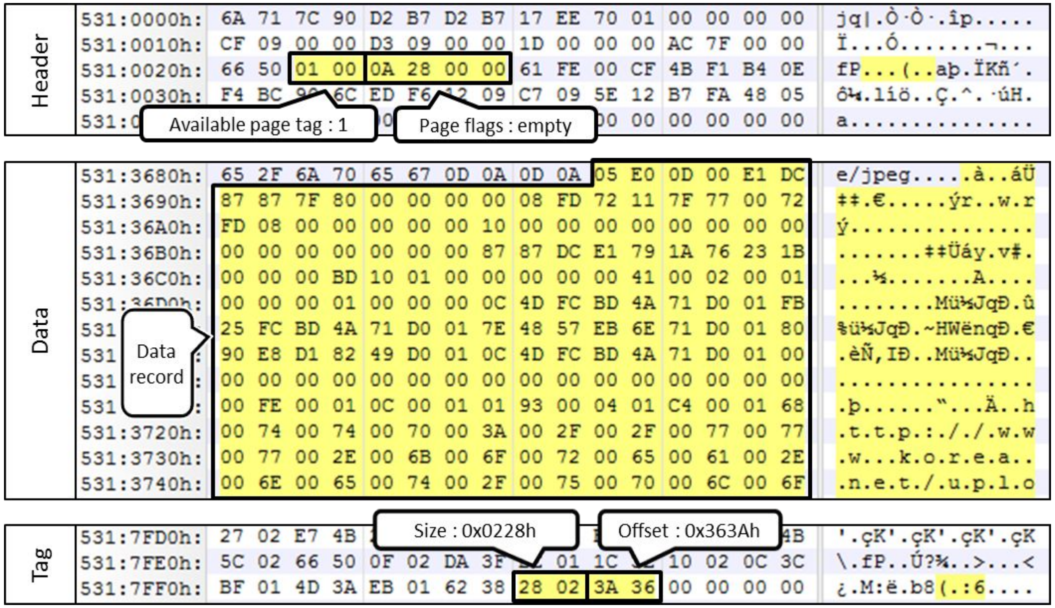
Jump | 0 | | Size | | Data

1byte | 3bit | 5bit | 2byte | Jump Size

| 1 | | | Jump Size | | Data

Verifying changes after deleting records

- **Change information after deleting records**
  - File size : No change
  - Changed parts in page
    - Header : page flag and record count are changed
    - Data area : Remain
    - Tag area : Remain or be overwritten

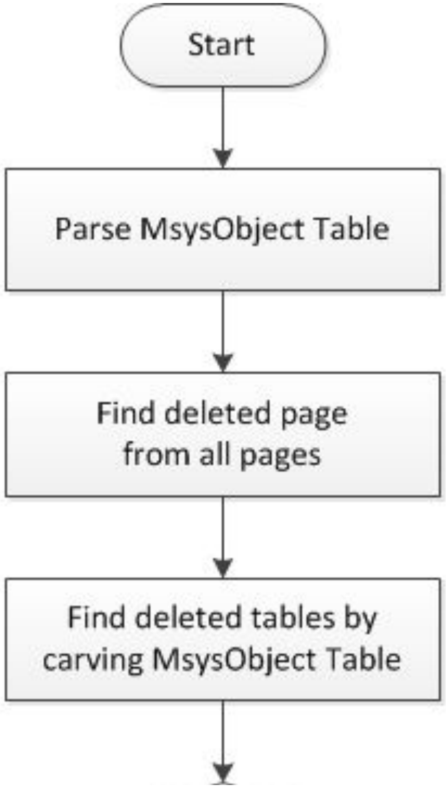


```
531:0000h: 6A 71 7C 90 D2 B7 D2 B7 17 EE 70 01 00 00 00 00  jq|.Ò·Ò·.îp.....
531:0010h: CF 09 00 00 D3 09 00 00 1D 00 00 00 AC 7F 00 00  Ï...Ó.......¬...
531:0020h: 66 50 01 00 0A 28 00 00 61 FE 00 CF 4B F1 B4 0E  fP...(..aþ.ÏKñ´.
531:0030h: F4 BC 90 6C ED F6 12 09 C7 09 5E 12 B7 FA 48 05  ô¼.líö..Ç.^.·úH.
531:0                                 00 00 00 00 00 00  a...............

531:3680h: 65 2F 6A 70 65 67 0D 0A 0D 0A 05 E0 0D 00 E1 DC  e/jpeg......à..áÜ
531:3690h: 87 87 7F 80 00 00 00 00 08 FD 72 11 7F 77 00 72  ‡‡.€.....ýr..w.r
531:36A0h: FD 08 00 00 00 00 00 10 00 00 00 00 00 00 00 00  ý...............
531:36B0h: 00 00 00 00 00 00 00 87 87 DC E1 79 1A 76 23 1B  .......‡‡Üáy.v#.
531:36C0h: 00 00 00 BD 10 01 00 00 00 00 00 41 00 02 00 01  ...½.......A....
531:36D0h: 00 00 00 01 00 00 00 0C 4D FC BD 4A 71 D0 01 FB  ........Mü½JqÐ.û
531        25 FC BD 4A 71 D0 01 7E 48 57 EB 6E 71 D0 01 80  %ü½JqÐ.~HWënqÐ.€
531        90 E8 D1 82 49 D0 01 0C 4D FC BD 4A 71 D0 01 00  .èÑ‚IÐ..Mü½JqÐ..
531        00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00  ................
531        00 FE 00 01 0C 00 01 01 93 00 04 01 C4 00 01 68  .þ......“...Ä..h
531:3720h: 00 74 00 74 00 70 00 3A 00 2F 00 2F 00 77 00 77  .t.t.p.:././.w.w
531:3730h: 00 77 00 2E 00 6B 00 6F 00 72 00 65 00 61 00 2E  .w...k.o.r.e.a..
531:3740h: 00 6E 00 65 00 74 00 2F 00 75 00 70 00 6C 00 6F  .n.e.t./.u.p.l.o

531:7FD0h: 27 02 E7 4B                                  4B  '.çK'.çK'.çK'.çK
531:7FE0h: 5C 02 66 50 0F 02 DA 3F    01 1C    10 02 0C 3C  \.fP..Ú?¾..>...<
531:7FF0h: BF 01 4D 3A EB 01 62 38 28 02 3A 36 00 00 00 00  ¿.M:ë.b8(.:6....
```

Record recovery technique

- **Recovery Procedures**

1. Parse MSysObject table
    - Get normal Table schema
2. Investigate all pages
    - Find deleted pages
    - Add parsing list if a table number remains in page header
3. Carve MsysObject table
    - Find deleted table

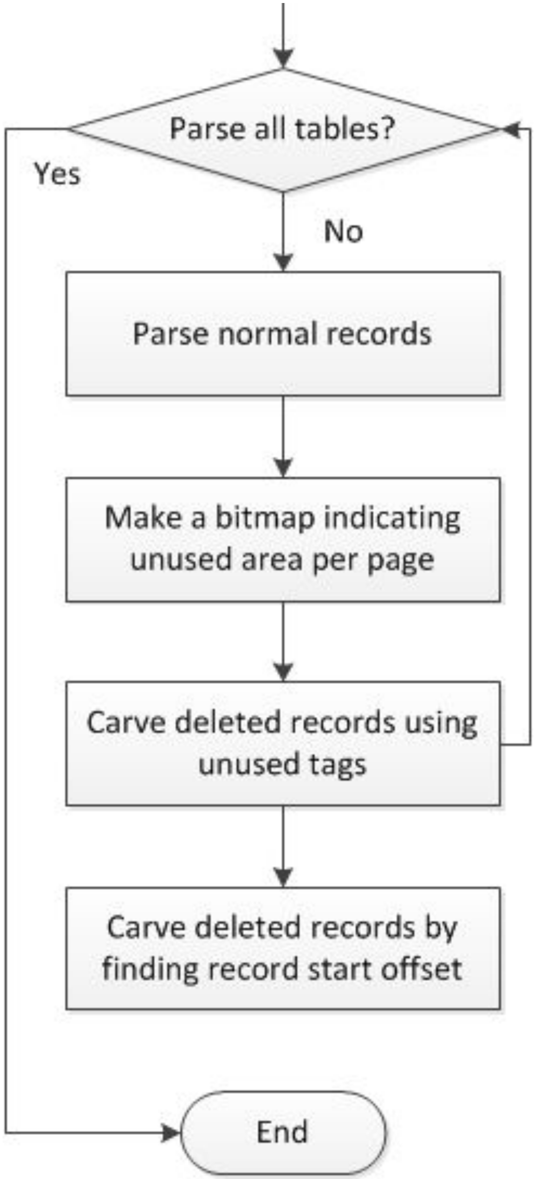

Start
Parse MsysObject Table
Find deleted page from all pages
Find deleted tables by carving MsysObject Table

Record recovery technique

- **Recovery Procedures**

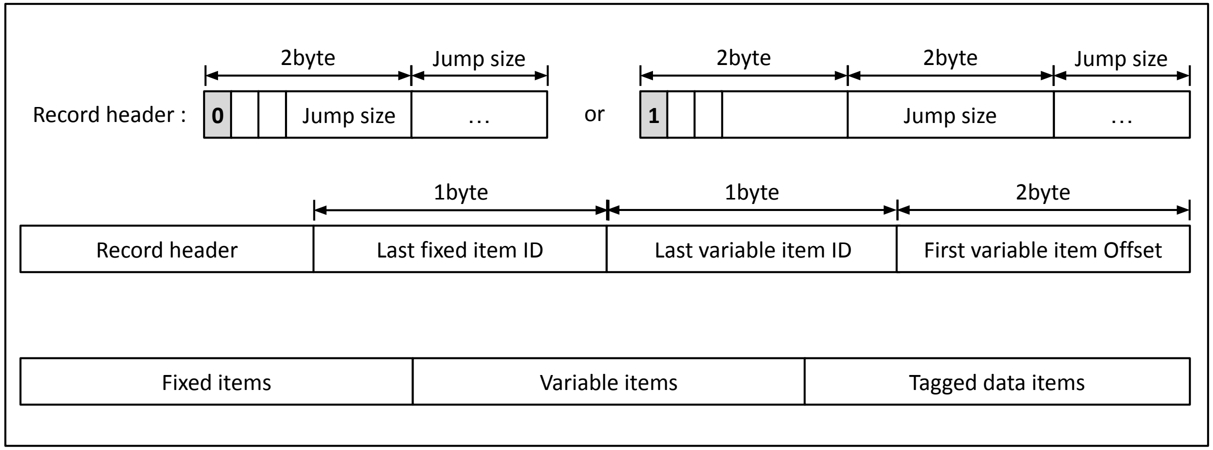
4. Parsing table

   - Create page tree
   - Parse normal records
   - Check unused page area
   - Recover deleted records using unused tag
   - Recover deleted records by finding start offset


Parse all tables?
Yes
No
Parse normal records
Make a bitmap indicating unused area per page
Carve deleted records using unused tags
Carve deleted records by finding record start offset
End

Record recovery technique

- **Method for finding start point of deleted records**

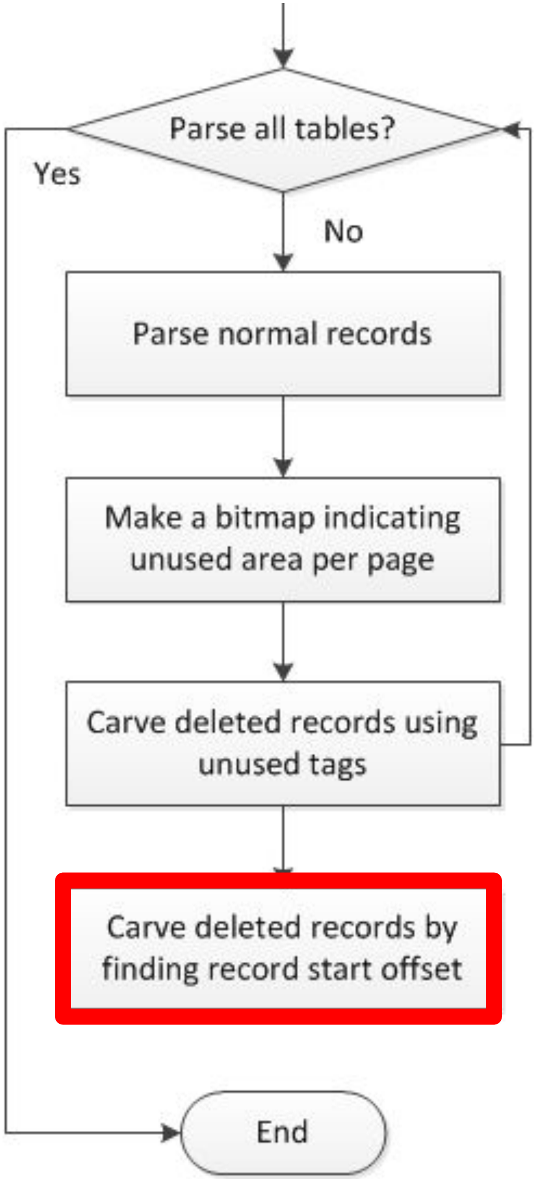


Record header : 0 | | | Jump size | … (2byte, Jump size) or 1 | | | | Jump size | … (2byte, 2byte, Jump size)

Record header | Last fixed item ID (1byte) | Last variable item ID (1byte) | First variable item Offset (2byte)

Fixed items | Variable items | Tagged data items

Conditional statements		
First byte	!=	0
Record size, offset	<	Page size
Jump size	<	The rest of the slack area, 100
Last fixed item ID	In	Fixed item column
Last variable item ID	In	Variable size data columns ID, 127
Last variable item Offset	<	The rest of the slack area
Last variable item Offset	<	Fixed size data's area



Parse all tables?

Yes

No

Parse normal records

Make a bitmap indicating unused area per page

Carve deleted records using unused tags

Carve deleted records by finding record start offset

End

Implementation and performance

- **Parse normal records**
  - Compare my program with EseDbViewer (based on API)
    - Record count is the same
    - Data is the same

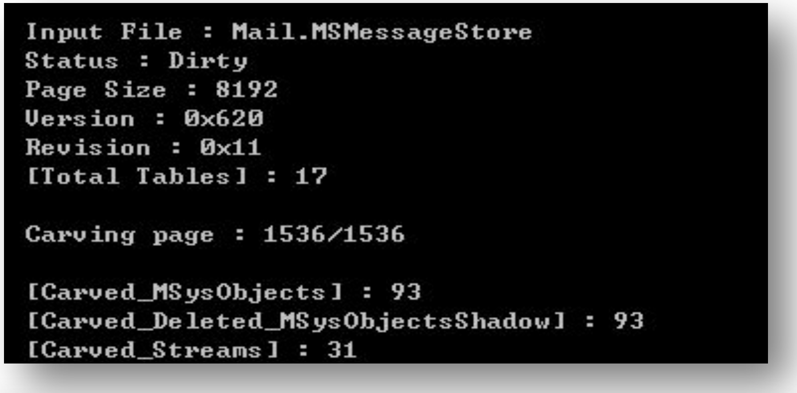
- **Recover deleted records**
  - Compare my program with ESECarve (the only recovery tool)

Our program

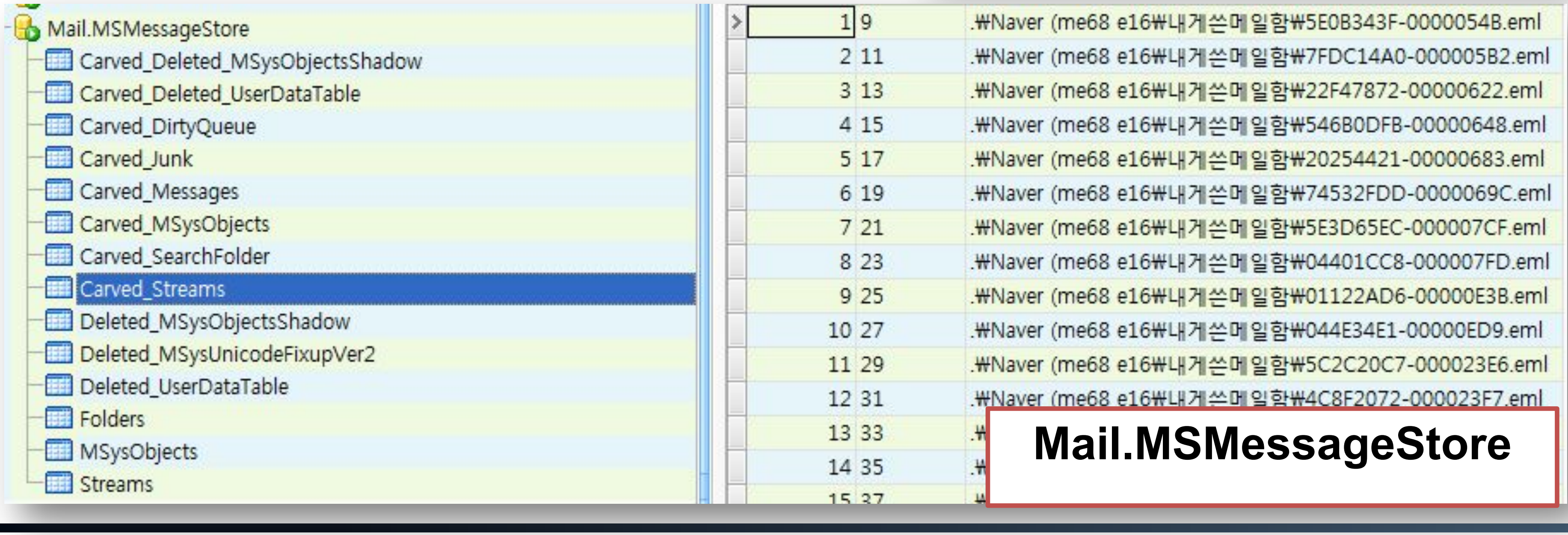
Compare list	ESECarve	ESEDBAnalyzer
Recoverable files	WebCacheV01.dat, Windows.edb	All of ESE database
Record count	= (same)	
Final column of record	Can not recover	Can recover
Dirty status-file	X	O

Implementation and performance

- **My program**
  - EDBForensic.py
    - Python
    - CLI



```
Input File : Mail.MSMessageStore
Status : Dirty
Page Size : 8192
Version : 0x620
Revision : 0x11
[Total Tables] : 17

Carving page : 1536/1536

[Carved_MSysObjects] : 93
[Carved_Deleted_MSysObjectsShadow] : 93
[Carved_Streams] : 31
```



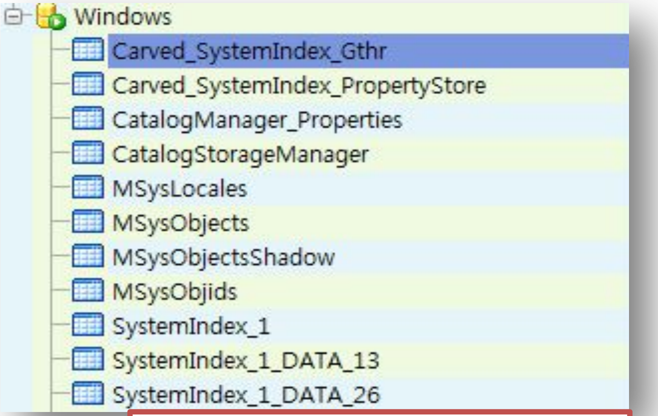
- Mail.MSMessageStore
  - Carved_Deleted_MSysObjectsShadow
  - Carved_Deleted_UserDataTable
  - Carved_DirtyQueue
  - Carved_Junk
  - Carved_Messages
  - Carved_MSysObjects
  - Carved_SearchFolder
  - Carved_Streams
  - Deleted_MSysObjectsShadow
  - Deleted_MSysUnicodeFixupVer2
  - Deleted_UserDataTable
  - Folders
  - MSysObjects
  - Streams

1	9	.₩Naver (me68 e16₩내게쓴메일함₩5E0B343F-0000054B.eml
2	11	.₩Naver (me68 e16₩내게쓴메일함₩7FDC14A0-000005B2.eml
3	13	.₩Naver (me68 e16₩내게쓴메일함₩22F47872-00000622.eml
4	15	.₩Naver (me68 e16₩내게쓴메일함₩546B0DFB-00000648.eml
5	17	.₩Naver (me68 e16₩내게쓴메일함₩20254421-00000683.eml
6	19	.₩Naver (me68 e16₩내게쓴메일함₩74532FDD-0000069C.eml
7	21	.₩Naver (me68 e16₩내게쓴메일함₩5E3D65EC-000007CF.eml
8	23	.₩Naver (me68 e16₩내게쓴메일함₩04401CC8-000007FD.eml
9	25	.₩Naver (me68 e16₩내게쓴메일함₩01122AD6-00000E3B.eml
10	27	.₩Naver (me68 e16₩내게쓴메일함₩044E34E1-00000ED9.eml
11	29	.₩Naver (me68 e16₩내게쓴메일함₩5C2C20C7-000023E6.eml
12	31	.₩Naver (me68 e16₩내게쓴메일함₩4C8F2072-000023F7.eml
13	33	.₩
14	35	.₩
15	37	.₩

Mail.MSMessageStore

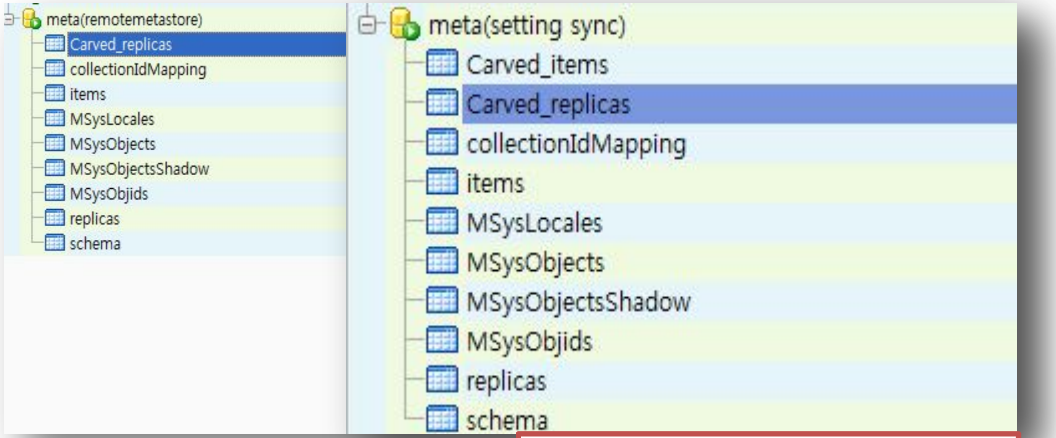
Implementation and performance

- **Screen shot**



Windows
- Carved_SystemIndex_Gthr
- Carved_SystemIndex_PropertyStore
- CatalogManager_Properties
- CatalogStorageManager
- MSysLocales
- MSysObjects
- MSysObjectsShadow
- MSysObjids
- SystemIndex_1
- SystemIndex_1_DATA_13
- SystemIndex_1_DATA_26

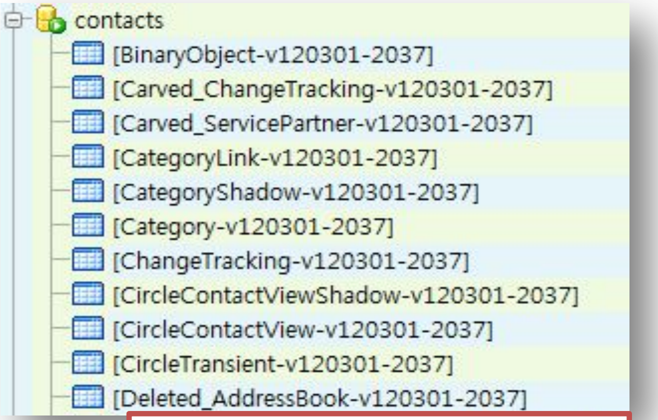
Windows



meta(remotemetastore)
- Carved_replicas
- collectionIdMapping
- items
- MSysLocales
- MSysObjects
- MSysObjectsShadow
- MSysObjids
- replicas
- schema

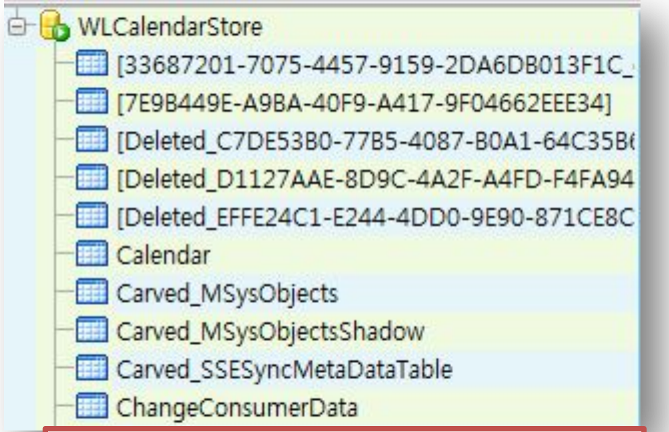
meta(setting sync)
- Carved_items
- Carved_replicas
- collectionIdMapping
- items
- MSysLocales
- MSysObjects
- MSysObjectsShadow
- MSysObjids
- replicas
- schema

meta



contacts
- [BinaryObject-v120301-2037]
- [Carved_ChangeTracking-v120301-2037]
- [Carved_ServicePartner-v120301-2037]
- [CategoryLink-v120301-2037]
- [CategoryShadow-v120301-2037]
- [Category-v120301-2037]
- [ChangeTracking-v120301-2037]
- [CircleContactViewShadow-v120301-2037]
- [CircleContactView-v120301-2037]
- [CircleTransient-v120301-2037]
- [Deleted_AddressBook-v120301-2037]

contacts

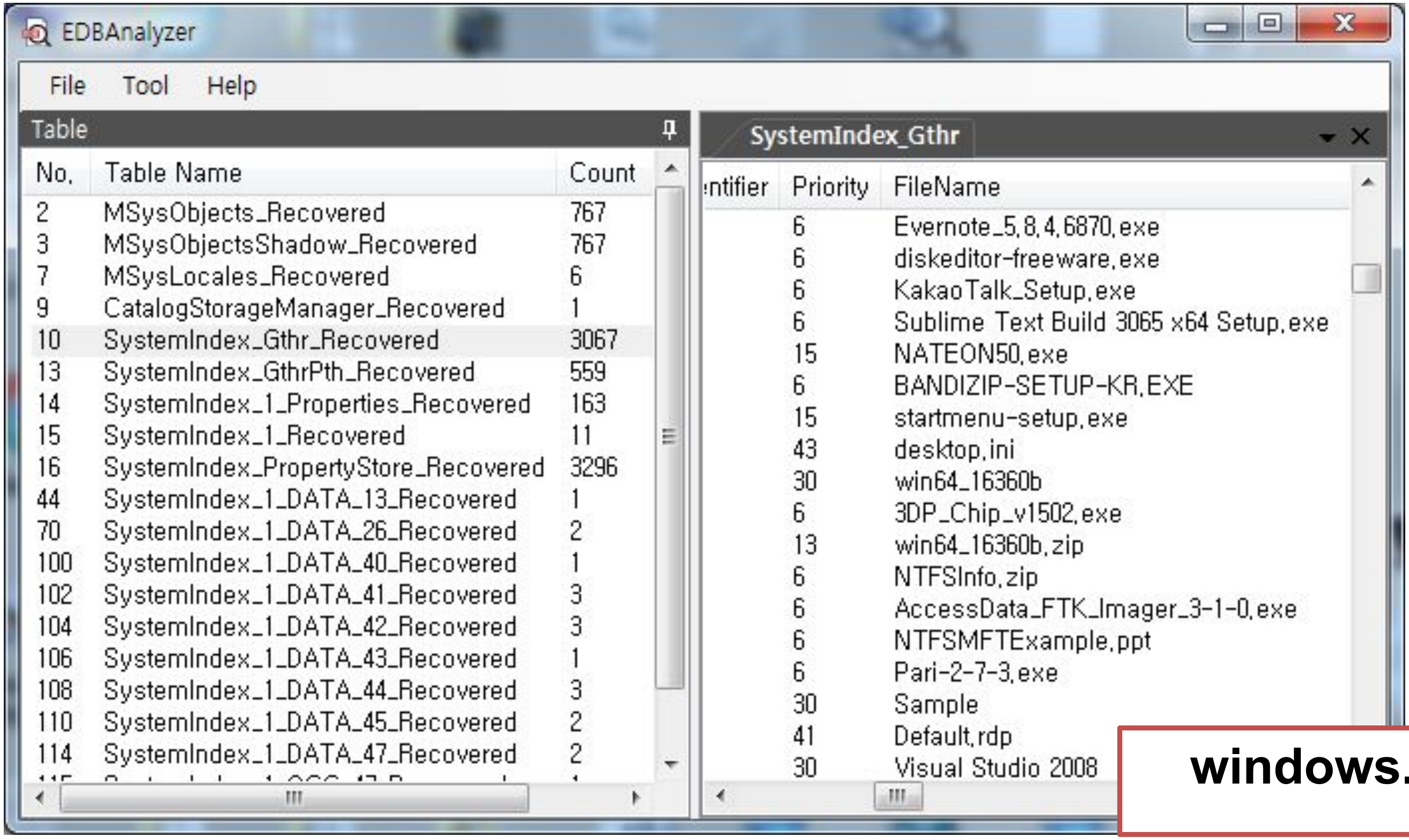


WLCalendarStore
- [33687201-7075-4457-9159-2DA6DB013F1C_
- [7E9B449E-A9BA-40F9-A417-9F04662EEE34]
- [Deleted_C7DE53B0-77B5-4087-B0A1-64C35B
- [Deleted_D1127AAE-8D9C-4A2F-A4FD-F4FA94
- [Deleted_EFFE24C1-E244-4DD0-9E90-871CE8C
- Calendar
- Carved_MSysObjects
- Carved_MSysObjectsShadow
- Carved_SSESyncMetaDataTable
- ChangeConsumerData

WLCalendarStore

Implementation and performance

- **My program(GUI)**
  - Be converting “EDBForensic.py” from CLI to GUI
  - I am going to publish program freely as soon as possible.



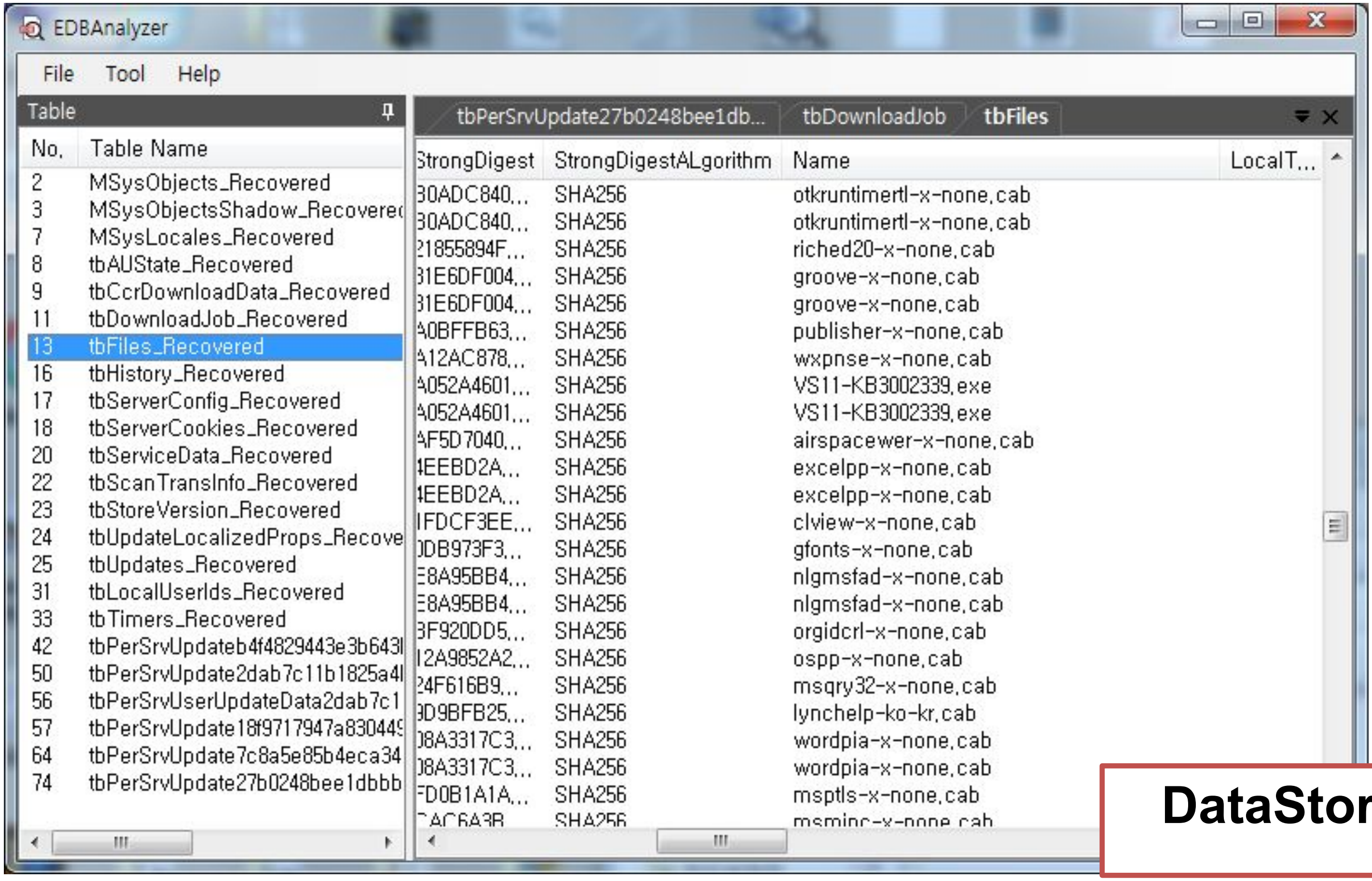
No.	Table Name	Count
2	MSysObjects_Recovered	767
3	MSysObjectsShadow_Recovered	767
7	MSysLocales_Recovered	6
9	CatalogStorageManager_Recovered	1
10	SystemIndex_Gthr_Recovered	3067
13	SystemIndex_GthrPth_Recovered	559
14	SystemIndex_1_Properties_Recovered	163
15	SystemIndex_1_Recovered	11
16	SystemIndex_PropertyStore_Recovered	3296
44	SystemIndex_1_DATA_13_Recovered	1
70	SystemIndex_1_DATA_26_Recovered	2
100	SystemIndex_1_DATA_40_Recovered	1
102	SystemIndex_1_DATA_41_Recovered	3
104	SystemIndex_1_DATA_42_Recovered	3
106	SystemIndex_1_DATA_43_Recovered	1
108	SystemIndex_1_DATA_44_Recovered	3
110	SystemIndex_1_DATA_45_Recovered	2
114	SystemIndex_1_DATA_47_Recovered	2

ntifier	Priority	FileName
	6	Evernote_5.8.4.6870.exe
	6	diskeditor-freeware.exe
	6	KakaoTalk_Setup.exe
	6	Sublime Text Build 3065 x64 Setup.exe
	15	NATEON50.exe
	6	BANDIZIP-SETUP-KR.EXE
	15	startmenu-setup.exe
	43	desktop.ini
	30	win64_16360b
	6	3DP_Chip_v1502.exe
	13	win64_16360b.zip
	6	NTFSInfo.zip
	6	AccessData_FTK_Imager_3-1-0.exe
	6	NTFSMFTExample.ppt
	6	Pari-2-7-3.exe
	30	Sample
	41	Default.rdp
	30	Visual Studio 2008

windows.edb

Implementation and performance

- **My program(GUI)**
  - Be converting “EDBForensic.py” from CLI to GUI
  - I am going to publish program freely as soon as possible.



No.	Table Name
2	MSysObjects_Recovered
3	MSysObjectsShadow_Recoverec
7	MSysLocales_Recovered
8	tbAUState_Recovered
9	tbCcrDownloadData_Recovered
11	tbDownloadJob_Recovered
13	tbFiles_Recovered
16	tbHistory_Recovered
17	tbServerConfig_Recovered
18	tbServerCookies_Recovered
20	tbServiceData_Recovered
22	tbScanTransInfo_Recovered
23	tbStoreVersion_Recovered
24	tbUpdateLocalizedProps_Recove
25	tbUpdates_Recovered
31	tbLocalUserIds_Recovered
33	tbTimers_Recovered
42	tbPerSrvUpdateb4f4829443e3b643l
50	tbPerSrvUpdate2dab7c11b1825a4l
56	tbPerSrvUserUpdateData2dab7c1
57	tbPerSrvUpdate18f9717947a83044!
64	tbPerSrvUpdate7c8a5e85b4eca34
74	tbPerSrvUpdate27b0248bee1dbbb

StrongDigest	StrongDigestALgorithm	Name	LocalT...
30ADC840...	SHA256	otkruntimertl-x-none.cab	
30ADC840...	SHA256	otkruntimertl-x-none.cab	
21855894F...	SHA256	riched20-x-none.cab	
31E6DF004...	SHA256	groove-x-none.cab	
31E6DF004...	SHA256	groove-x-none.cab	
A0BFFB63...	SHA256	publisher-x-none.cab	
A12AC878...	SHA256	wxpnse-x-none.cab	
A052A4601...	SHA256	VS11-KB3002339.exe	
A052A4601...	SHA256	VS11-KB3002339.exe	
AF5D7040...	SHA256	airspacewer-x-none.cab	
4EEBD2A...	SHA256	excelpp-x-none.cab	
4EEBD2A...	SHA256	excelpp-x-none.cab	
IFDCF3EE...	SHA256	clview-x-none.cab	
0DB973F3...	SHA256	gfonts-x-none.cab	
E8A95BB4...	SHA256	nlgmsfad-x-none.cab	
E8A95BB4...	SHA256	nlgmsfad-x-none.cab	
3F920DD5...	SHA256	orgidcrl-x-none.cab	
12A9852A2...	SHA256	ospp-x-none.cab	
24F616B9...	SHA256	msqry32-x-none.cab	
9D9BFB25...	SHA256	lynchelp-ko-kr.cab	
08A3317C3...	SHA256	wordpia-x-none.cab	
08A3317C3...	SHA256	wordpia-x-none.cab	
FD0B1A1A...	SHA256	msptls-x-none.cab	
CAC6A3B	SHA256	msminc-x-none.cab	

DataStore.edb

Conclusion

- **The advantage of this study**
  - Solve the problems of existing tools

Compare list	ESEDatabaseView	EseDbViewer	ESECarve	ESEDBAnalyzer
query	X	X	X	O
Dirty-status file	△	X	X	O
UTF-8 encoding	X	O	X	O
Possible input file	All	All	2	All
Normal parsing	△	O	O	O
recover delete records	X	X	△	O

- **Limitation**
  - Cannot recover deleted data with damaged record header

Q & A

americano@korea.ackr