

# Anti-Forensics:

## Leveraging OS and File System Artifacts

*"What one man can invent, another can discover."*

– **Sherlock Holmes**

19-Feb-2016

**Ali Hadi**

***ali@ashemery.com***





# Objective

- Talk on Anti-Forensics focusing on operating system and file system artifacts that can be used to confirm/refute if anti-forensics was used on a hard drive.
- Talk covers Anti-Forensics from a criminal perspective not privacy perspective

# Anti-Forensics?

---

*Tools and techniques that frustrate forensic tools, investigations, and investigators ...*

*- Dr. Simson Garfinkel*

# Anti Forensics

- Locating anti-forensic tools leads to suspicion
  - Crumbs could be found even if removed!
- **Simple:** clearing caches, offline files, app artifacts, deleting catalogs and thumbnail files, Jump Lists, Prefetch files, etc
- **Complex:** Full Disk Encryption, Injected DLLs (meterpreter), Anti-X

# GOALS ?

- Avoid detection
- Disrupting Information Collection
- Increase examination time
- Cast doubt on forensic reports or testimony
- Subverting the tool





# Categories

- Hiding:
  - Data Hiding
  - Trail Obfuscation
- Destruction:
  - Artifact Wiping
  - Attacking Forensic Tools

# Q: What are we looking for?

*"Data! Data! Data!"*

*"I can't make bricks without clay."*

*- Sherlock Holmes*

- Before we check where and how is **Data** "evidence" stored, we must first understand what type of evidence from a forensic perspective are we looking for:
  - **Time**: a duration in this universe
  - **Keywords**: any specific text related to a crime
  - **Action/Operation**: open file, run program, shutdown system, etc
  - **Object**: disk, partition, file, malware, etc

# Operating System Artifacts

---

*"Don't be conned by misleading menu structures!"*



# Techniques

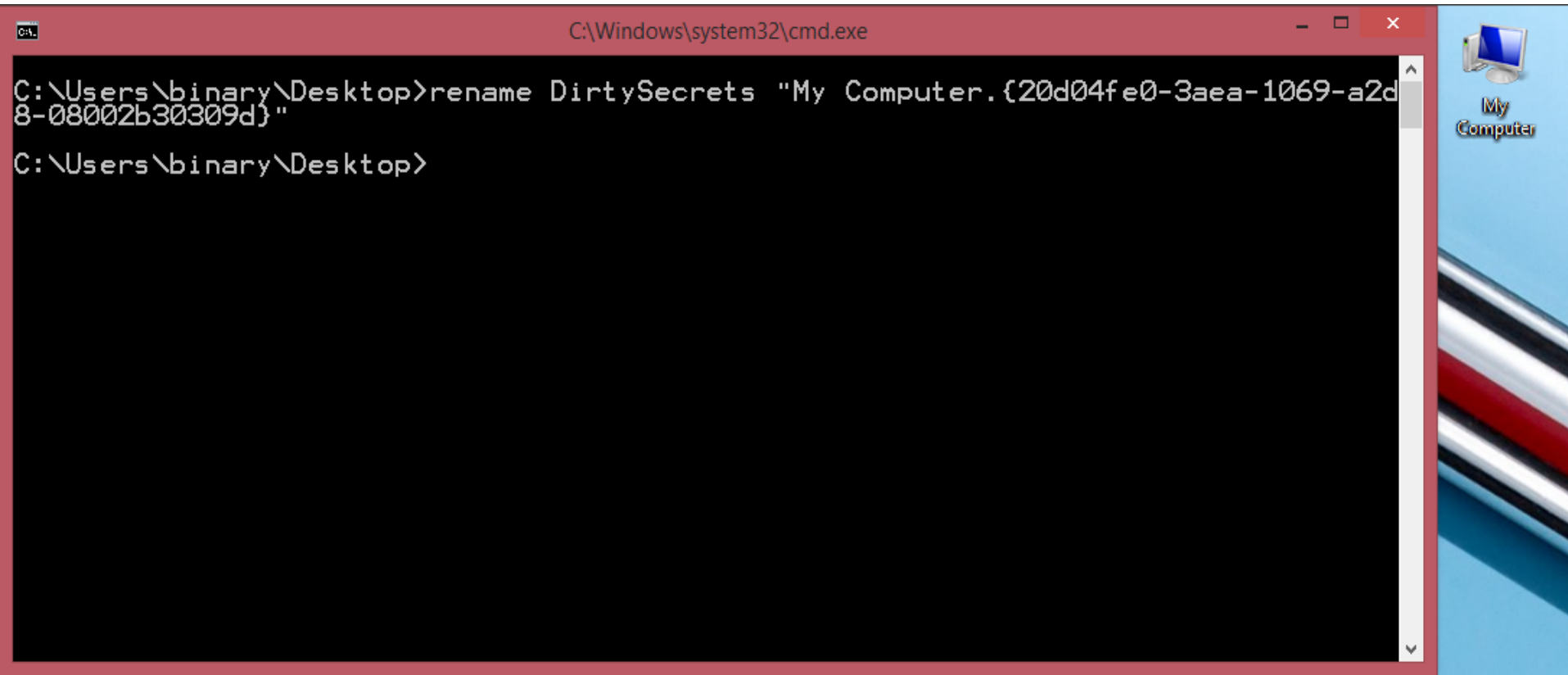
- Shift+del
- Hiding files within system directories
- Changing the file extension
  - .doc → .xls
  - .pdf → .doc
- Merge Streams (Doc into XLS and vice versa)
- Changing one byte in a file
  - Known to Unknown Hashes Bypass
- Split and Scatter (splitting files and then scattering them)
- Changing file headers
  - Transmogrify

# Techniques – Cont.

- Log Injection (misleading events)
- Deleted Files and Removed Programs
  - Restore Points
  - Registry Entries
    - HKCU\Software\Microsoft\Windows\CurrentVersion\Run
- Online Storage: Dropbox, Gdrive, etc
- DLL Injection (Meterpreter)

# How: Simple Techniques – Cont.

- CLSID List (Windows Class Identifiers),  
<https://autohotkey.com/docs/misc/CLSID-List.htm>  
rename FOLDER "My Computer.{20d04fe0-3aea-1069-a2d8-08002b30309d}"



# SysInternals: Autoruns

Autoruns [CYBERSTORM\Administrator] - Sysinternals: www.sysinternals.com

File Entry Options User Help

Applnit KnownDLLs Winlogon Winsock Providers Print Monitors LSA Providers Network Providers

Everything Logon Explorer Internet Explorer Scheduled Tasks Services Drivers Boot Execute Image Hijacks

Autorun Entry	Description	Publisher	Image Path
<b>HKCU\Software\Microsoft\Windows\CurrentVersion\Run</b>			
<input checked="" type="checkbox"/> Google Update	Google Installer	(Verified) Google Inc	c:\documents and settings\administrator\local settings\
<input type="checkbox"/> Google Update	Google Installer	(Verified) Google Inc	c:\documents and settings\administrator\local settings\
<input checked="" type="checkbox"/> SandboxieControl	Sandboxie Control	(Verified) SANDBOXIE L.T.D	c:\program files\sandboxie\sbiectrl.exe
<input checked="" type="checkbox"/> SRS Audio Sandbox	SRS Audio Sandbox control panel	(Verified) SRS Labs, Inc	c:\program files\srs labs\audio sandbox\srsssc.exe
<input checked="" type="checkbox"/> Web Video Downloader	Sothink Web Video Downloader	(Verified) SourceTec Softw...	c:\program files\sourcetec\sothink web video downloa
<b>HKLM\SOFTWARE\Classes\Protocols\Handler</b>			
<input checked="" type="checkbox"/> skype4com	Skype for COM API	(Verified) Skype Technologi...	c:\windows\system32\skype4com.dll
<b>HKLM\SOFTWARE\Microsoft\Active Setup\Installed Components</b>			
<input checked="" type="checkbox"/> n/a			c:\windows\system32\lcpysys.exe
<input checked="" type="checkbox"/> n/a			c:\windows\system32\lcpool.exe
<b>HKLM\Software\Classes\*\ShellEx\ContextMenuHandlers</b>			
<input checked="" type="checkbox"/> 7-Zip	7-Zip Shell Extension	(Not verified) Igor Pavlov	c:\program files\7-zip\7-zip.dll
<input checked="" type="checkbox"/> Notepad++	ShellHandler for Notepad++ (64 bit)		c:\program files\notepad++\nppshell_04.dll
<input checked="" type="checkbox"/> PowerISO	PowerISOShell DLL	(Not verified) PowerISO Co...	c:\program files\poweriso\pwrish.dll
<input checked="" type="checkbox"/> SnagitMainShellExt	Snagit Shell Extension DLL	(Verified) TechSmith Corpor...	c:\program files\techsmith\snagit 10\snagitshellext.dll

Ready.

# Detection Techniques

- Different detection techniques (image path, memory, etc)
- Fuzzy Hashes
- Content Analysis
- Scheduled Tasks
- Thumbcache
- Log detection
  - Correlation and Timeline Analysis
  - Memory dump of erased events or wipers
  - Centralized Log Management System
- Meterpreter
  - Memory dump
  - `stdapi_sys_process_getpid`



# Volume Shadow Copies / Restore Points

```
C:\> Administrator: Command Prompt

Q:\>vssadmin list shadows
vssadmin 1.1 - Volume Shadow Copy Service administrative command-line tool
(C) Copyright 2001-2005 Microsoft Corp.

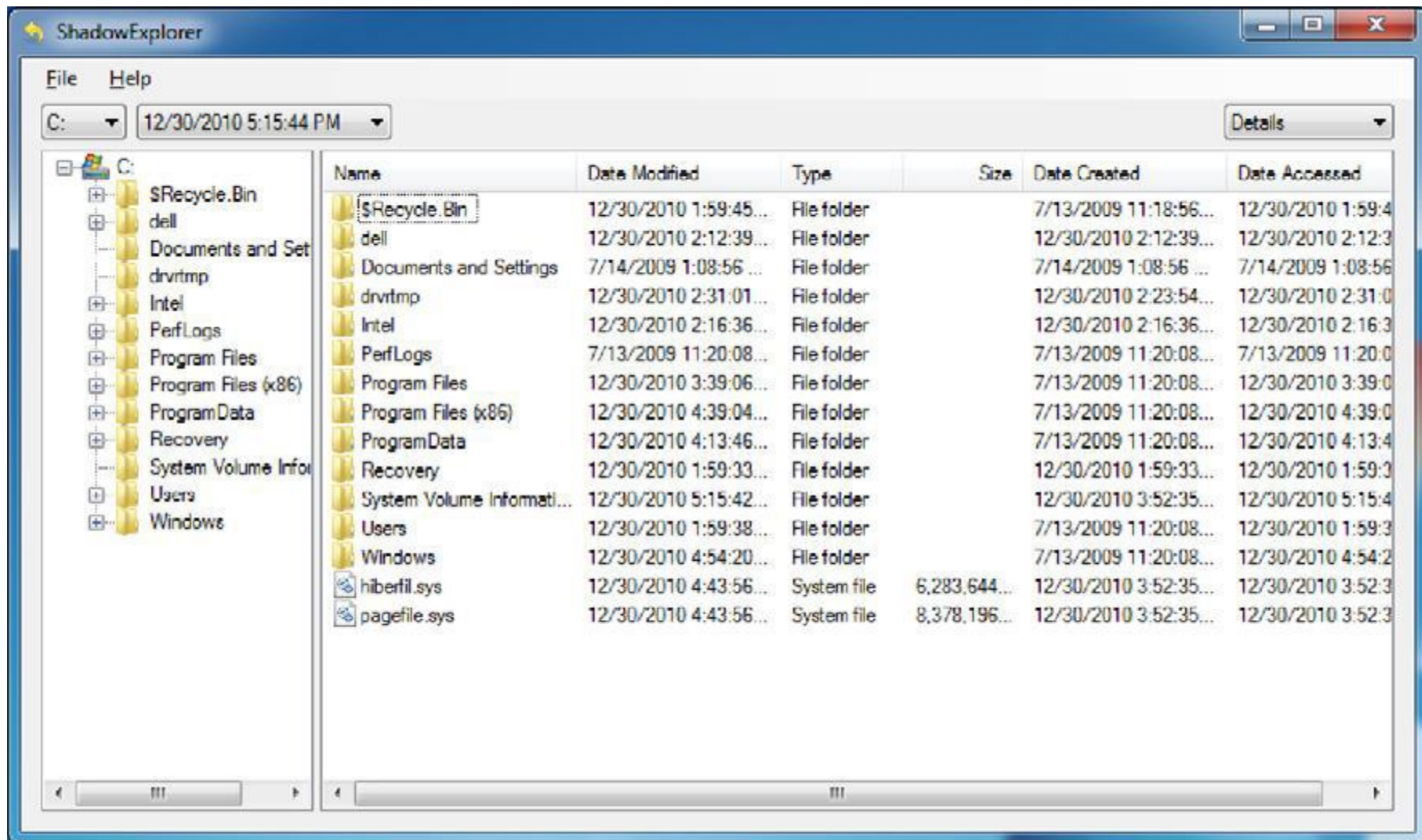
Contents of shadow copy set ID: {a24b3ac0-8a88-4301-ab7b-0a5f966cf426}
  Contained 1 shadow copies at creation time: 10/18/2014 12:00:06 AM
    Shadow Copy ID: {99603c67-3a54-444d-964b-05a9b39acd94}
      Original Volume: (C:)\>\\?\Volume{d37795a5-95aa-11e1-97b0-806e6f6e6963}\
      Shadow Copy Volume: \\?\GLOBALROOT\Device\HarddiskVolumeShadowCopy1
      Originating Machine: unilab
      Service Machine: unilab
      Provider: 'Microsoft Software Shadow Copy provider 1.0'
      Type: ClientAccessibleWriters
      Attributes: Persistent, Client-accessible, No auto release, Differential
1. Auto recovered

Contents of shadow copy set ID: {5bd99410-8b1b-4618-a69d-50704773b58e}
  Contained 1 shadow copies at creation time: 10/26/2014 12:00:06 AM
    Shadow Copy ID: {d1b9988e-11c5-4b95-a37e-72287f41210b}
      Original Volume: (C:)\>\\?\Volume{d37795a5-95aa-11e1-97b0-806e6f6e6963}\
      Shadow Copy Volume: \\?\GLOBALROOT\Device\HarddiskVolumeShadowCopy2
      Originating Machine: unilab
      Service Machine: unilab
      Provider: 'Microsoft Software Shadow Copy provider 1.0'
      Type: ClientAccessibleWriters
      Attributes: Persistent, Client-accessible, No auto release, Differential
1. Auto recovered

Q:\>
```

- Beware of accessing VSCs on Live Systems (why?)

# Shadow Explorer – VSC Browser



# Windows Registry

Registry Explorer v0.0.4.7

File Tools Options Bookmarks (1/0) View Help

Registry hives (18) Available bookmarks (41/0)

Key name	# values	Last write timestamp
C:\Temp\UsrClass account rename.dat		9/11/2014 9:50:48 PM ...
S-1-5-21-1141529136-2431258765-826847743-1000_Cla...	1	3/19/2014 3:23:15 PM ...
C:\Temp\UsrClass CDburn UNC fat filesystem.dat		7/6/2014 9:16:42 PM +...
S-1-5-21-1876483248-2010845669-2174274418-1000_Cl...	1	3/1/2014 3:22:33 PM +...
C:\Temp\UsrClass zip file network stuff.dat		4/4/2012 8:00:11 PM +...
S-1-5-21-2036804247-3058324640-2116585241-1114_Cl...	0	12/6/2009 7:28:29 AM ...
C:\Temp\UsrClass unicode and network.dat		8/26/2013 9:23:46 PM ...
S-1-5-21-3640650475-3814930019-1523317725-1003_Cl...	1	8/23/2013 6:10:04 PM ...
C:\Temp\usrclass.dat		9/11/2014 9:50:48 PM ...
S-1-5-21-1141529136-2431258765-826847743-1000_Cla...	1	3/19/2014 3:23:15 PM ...
C:\Temp\UsrClass FTP.dat		5/20/2014 2:19:35 PM ...
S-1-5-21-2417227394-2575385136-2411922467-1105_Cl...	0	11/22/2014 9:27:06 A...
Unassociated deleted records	0	
C:\Temp\usrclass2.dat		4/4/2012 8:00:11 PM +...
S-1-5-21-2036804247-3058324640-2116585241-1114_Cl...	0	12/6/2009 7:28:29 AM ...
C:\Temp\UsrClass program assoc Bitlocker.dat		8/1/2014 10:33:25 PM ...
S-1-5-21-1760429251-2387087200-3224058304-1001_Cl...	0	9/20/2014 4:36:53 AM ...
Associated deleted records	0	
Unassociated deleted records	0	
C:\Temp\SAM_hasBigEndianDWord		8/22/2013 1:25:44 PM ...
CsiTool-CreateHive-{00000000-0000-0000-0000-00000000...}	0	8/22/2013 2:45:10 PM ...
C:\Temp\UsrClass MTP.dat		4/24/2014 3:02:54 PM ...
S-1-5-21-2208335738-3127931778-3832183526-1002_Cl...	2	8/23/2014 3:20:25 AM ...
Associated deleted records	0	
C:\Temp\NTUSER_Loveall.DAT		1/30/2008 2:51:20 PM ...
\$\$\$PROTO.HIV	0	1/30/2008 2:47:27 PM ...

Key: S-1-5-21-2208335738-3127931778-3832183526-1002\_Classes

Last write: 8/23/2014 3:20:25 AM +00:00 2 of 2 values shown (100.00 %) Load complete

Hidden keys: 0 345

Values

Drag a column header here to group by that column

Value name	Value type	Data	Value slack
date	RegSz	2014/04/30	6A-E4-EA-03-00-00
publisher	RegSz	512	C0-05-00-00

Type viewer Slack viewer

Value name date

Value type RegSz

Slack 6A-E4-EA-03-00-00

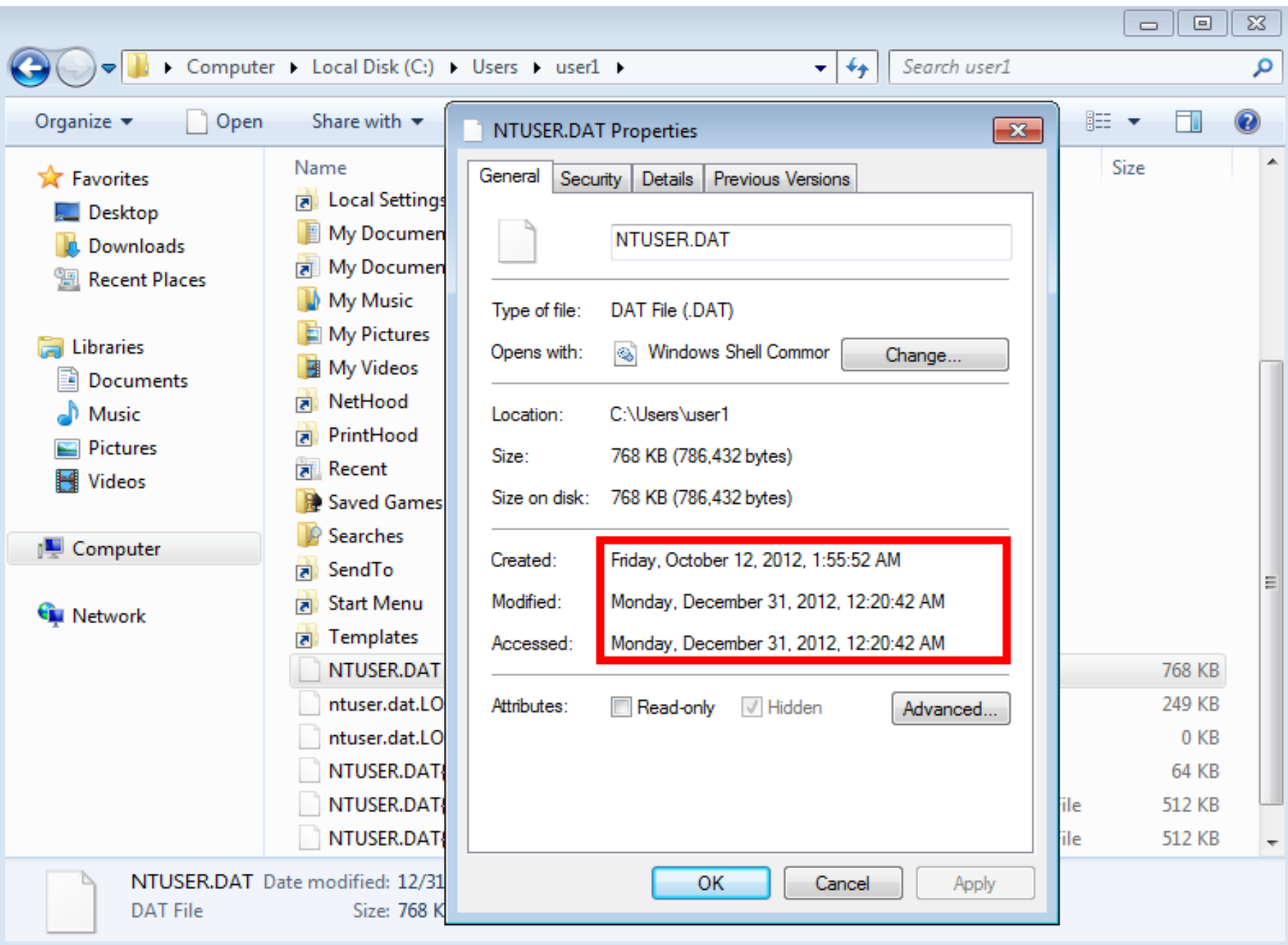
Value 2014/04/30

Value: date Collapse all hives



# User Registry File

- NTUser.Dat file
  - Personal preferences and computer settings for user
  - If just look at file meta data – file attributes
    - Find out a lot of information
    - First time user logged on
      - Creation date of file
    - Last time user logged on
      - Last modified date of file



# Recycle.Bin

- [Volume]:\ \$Recycle.Bin
- \$Recycle.Bin (hidden by default)
- Subfolder per user named with account SID
- When a file is moved to the Recycle Bin, it becomes two files \$I and \$R.
  - \$I -> original name and path, and deleted date
  - \$R -> original file data stream and other attributes

# Recycle Bin

```
C:\ Command Prompt

Directory of C:\RECYCLER

12/05/2007  09:54 PM    <DIR>        .
12/05/2007  09:54 PM    <DIR>        ..
05/24/2008  09:12 PM    <DIR>        S-1-5-21-1085031214-492894223-682003330-1005
005
           0 File(s)                0 bytes
           3 Dir(s)  32,632,496,128 bytes free

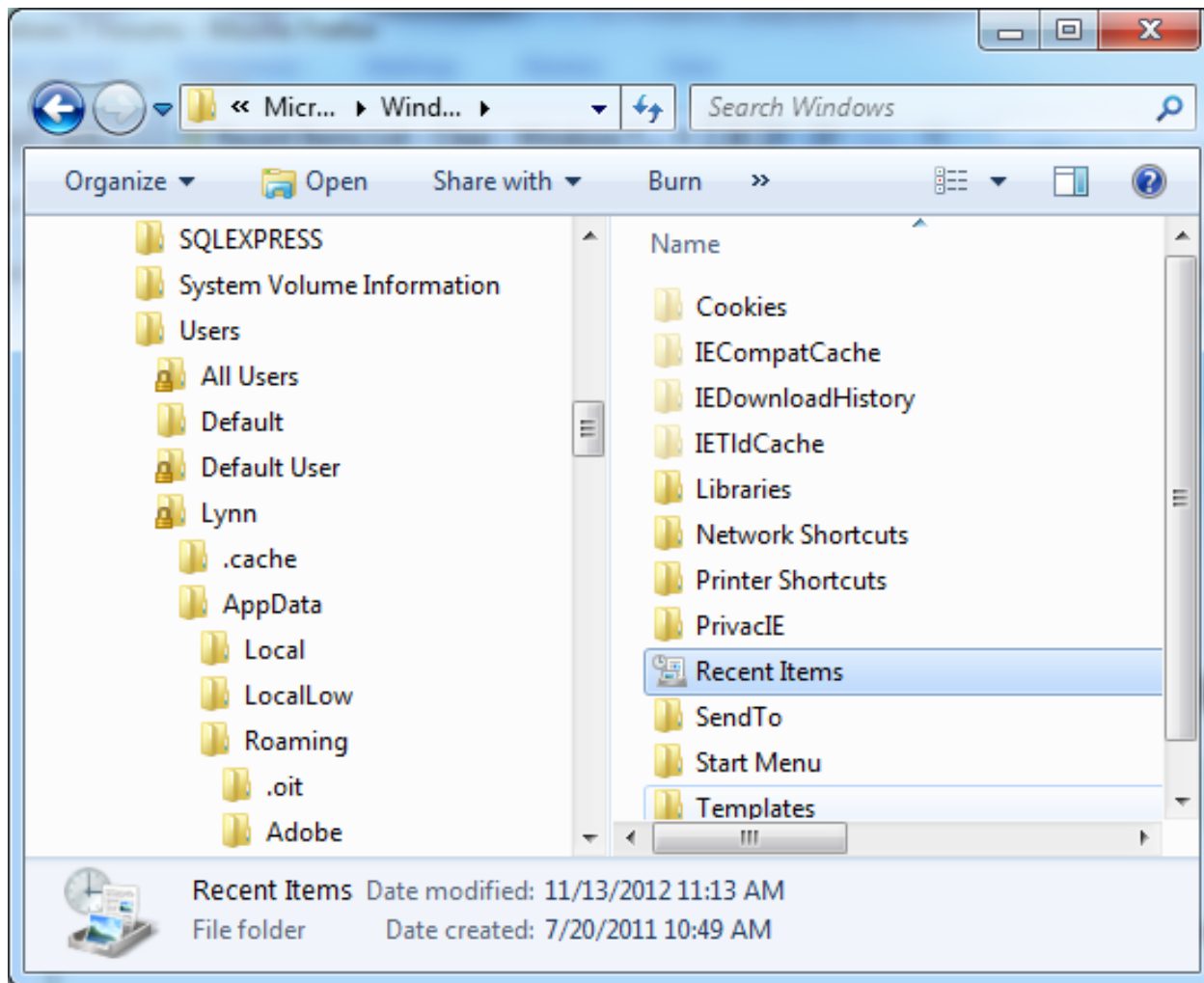
C:\RECYCLER>dir /a S-1-5-21-1085031214-492894223-682003330-1005
Volume in drive C has no label.
Volume Serial Number is 00B5-B536

Directory of C:\RECYCLER\S-1-5-21-1085031214-492894223-682003330-1005

05/24/2008  09:12 PM    <DIR>        .
05/24/2008  09:12 PM    <DIR>        ..
04/13/2008  09:06 PM    <DIR>        Dc1
05/08/2008  08:53 PM                966 Dc2.log
05/22/2008  10:46 AM            100,864 Dc3.ppt
05/22/2008  08:22 AM        10,064,384 Dc4.ppt
05/22/2008  10:23 AM    <DIR>        Dc5
05/22/2008  10:36 AM    <DIR>        Dc6
05/24/2008  08:10 PM        421,099 Dc7.csv
05/02/2008  03:20 PM             65 desktop.ini
05/24/2008  09:12 PM         5,620 INFO2
           6 File(s)        10,592,998 bytes
           5 Dir(s)  32,632,496,128 bytes free

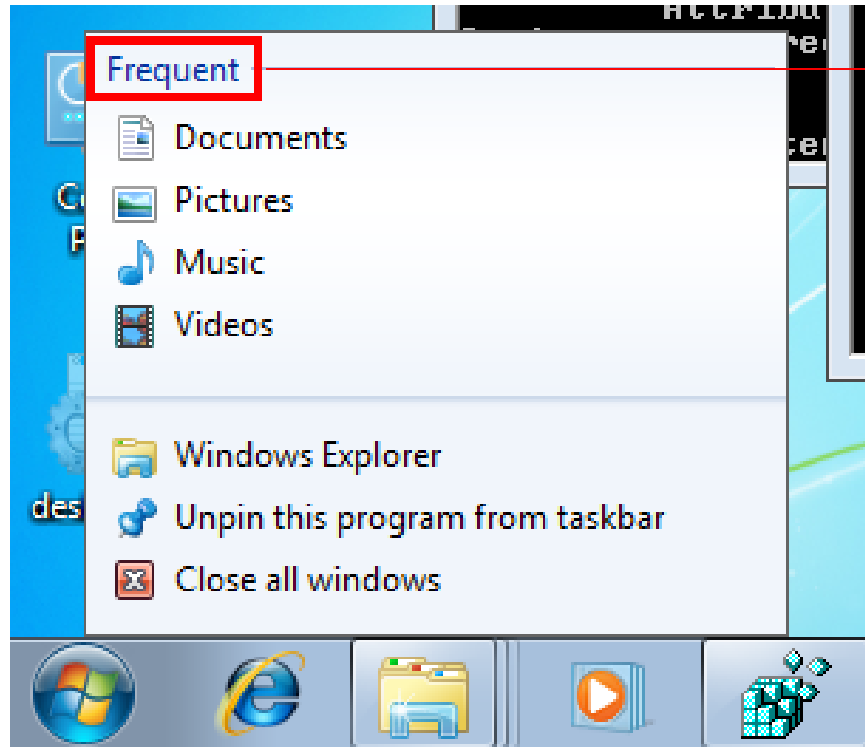
C:\RECYCLER>
```

# Clear “Recent Items” Windows 7

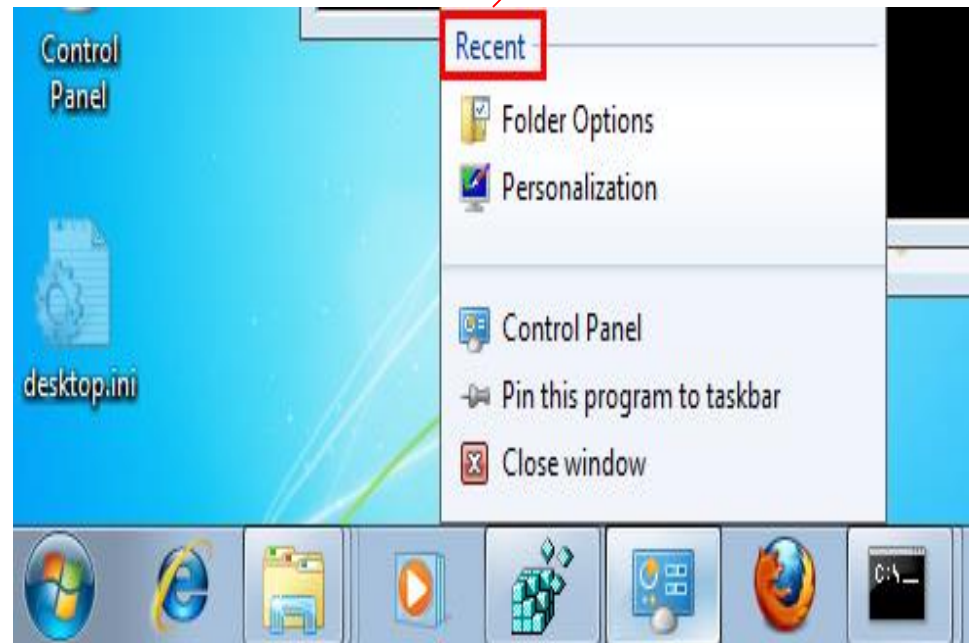


To clear “Recent Item List”  
Right click on Recent Items  
and select clear

# Jump Lists – Cont.

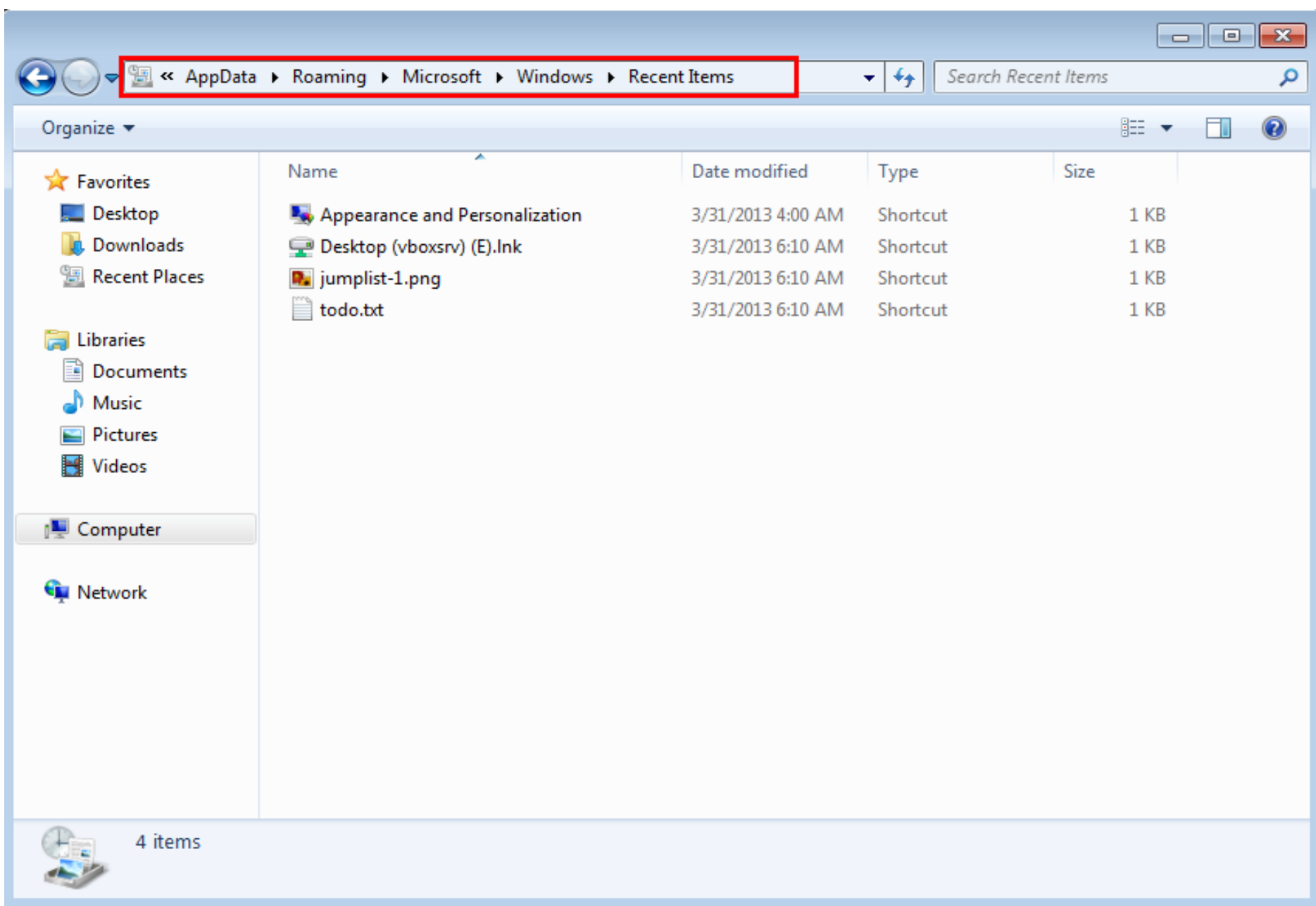


Frequent files used



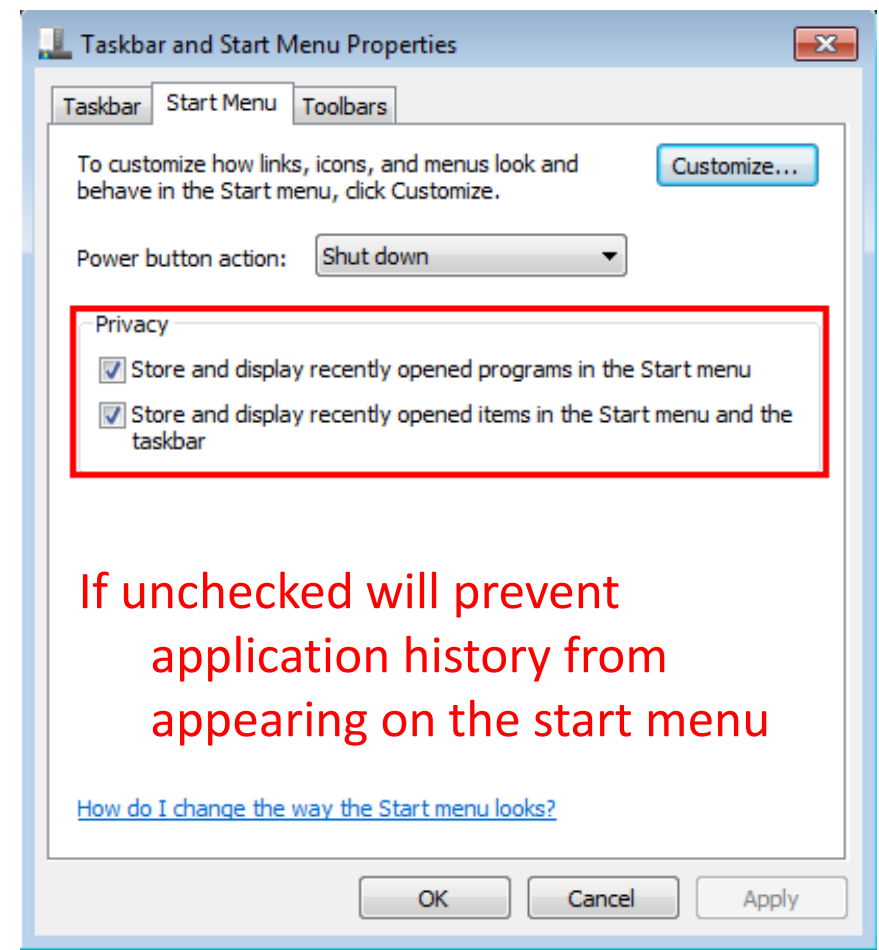
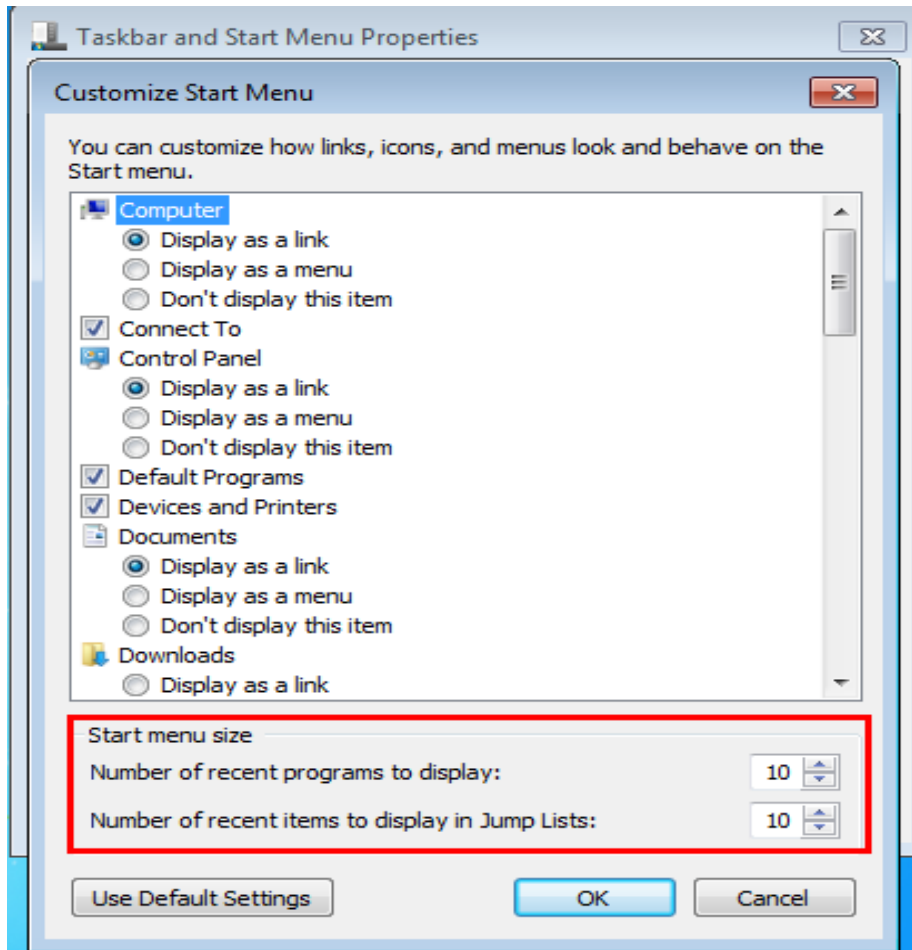
Recent files used





C:\Users\<username>\AppData\Roaming\Microsoft\Windows\Recent Items

# Jump Lists – Settings

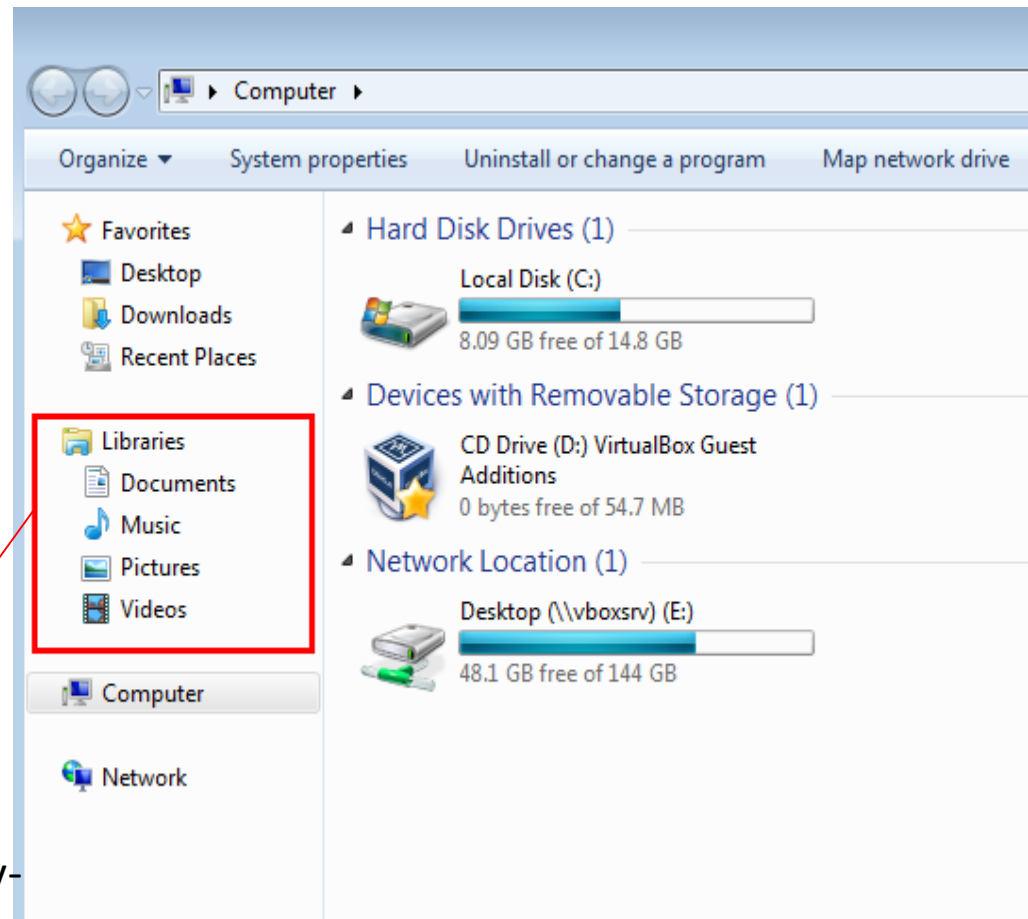


Used to adjust the number of items to display in the Jump Lists



# Libraries

- A list of Monitored folders
- Used to assist users to find and organize their media
  - Documents
  - Music
  - Pictures
  - Videos



View them using a Forensic tool:  
XML based files named with the library-  
ms extension!

They look like any other folder!!!

# Link Explorer (LECmd)

```
λ LECmd.exe -f d:\Code\Lnk\Lnk.Test\TestFiles\Misc\native.seven.01.test
LECmd version 0.5.0.0
```

```
Author: Eric Zimmerman (saericzimmerman@gmail.com)
https://github.com/EricZimmerman/LECmd
```

```
Command line: -f d:\Code\Lnk\Lnk.Test\TestFiles\Misc\native.seven.01.test
Processing 'd:\Code\Lnk\Lnk.Test\TestFiles\Misc\native.seven.01.test'
```

```
Source file: d:\Code\Lnk\Lnk.Test\TestFiles\Misc\native.seven.01.test
```

```
Source created: 2/9/2016 2:32:13 AM +00:00
```

```
Source modified: 9/9/2013 2:02:44 PM +00:00
```

```
Source accessed: 2/9/2016 2:32:13 AM +00:00
```

```
--- Header ---
```

```
Target created: 3/26/2010 10:07:11 AM +00:00
```

```
Target modified: 9/4/2005 8:18:26 PM +00:00
```

```
Target accessed: 3/26/2010 10:07:11 AM +00:00
```

```
File size: 1,019,392
```

```
Flags: HasTargetIdList, HasLinkInfo, HasRelativePath, HasWorkingDir, IsUnicode
```

```
File attributes: FileAttributeArchive
```

```
Icon index: 0
```

```
Show window: SwNormal (Activates and displays the window. The window is restore
```

```
Relative Path: ..\..\..\Program Files\ConTEXT\ConTEXT.exe
```

```
Working Directory: C:\Program Files\ConTEXT
```

# Prefetch Files

- Prefetch files indicates to the examiner the following:
  - Existence: application named was run
  - Creation date: when the application was first run
  - Modification date: when the application was last run

```
ddUserCase$ python prefetch.py NET1.EXE-849DA590.pf
##### NET1.EXE-849DA590.pf #####
magic      = SCCA
version    = 23
OS         = Win7
filesize   = 11626
crc        = 849DA590
appName    = NET1.EXE
appPath    = \DEVICE\HARDDISKVOLUME2\WINDOWS\SYSTEM32\NET1.EXE
dwRun      = 6
lastRun    = 2015-01-07 14:40:02

ddUserCase$ python prefetch.py NET.EXE-DF44F913.pf
##### NET.EXE-DF44F913.pf #####
magic      = SCCA
version    = 23
OS         = Win7
filesize   = 7296
crc        = DF44F913
appName    = NET.EXE
appPath    = \DEVICE\HARDDISKVOLUME2\WINDOWS\SYSTEM32\NET.EXE
dwRun      = 6
lastRun    = 2015-01-07 14:40:02
```

# User Activity with ShellBags

ShellBags Explorer - UsrClass.dat.copy0

File Tools Help

Desktop

- User Libraries
- ShellBagsExplorer-New
- Computers and Devices
- addUserCase
- My Computer
- Control Panel
  - All Control Panel Items
    - User Accounts** ←
    - Manage Accounts
    - Create New Account
  - Administrative Tools
- System and Security
- Network and Internet
  - Network Connections
  - Network and Sharing Center
- LocaleMetaData
- Shared Documents Folder (Users Files)

Drag a column header here to group by that column.

Value	Icon	Type	Bag pa	Type I	Slot	MRU	Creat	Modifi	Acces	First E	Last Explored
Manage...		Variable: Users...	BagM...	00	0	0					1/7/2015 2:40:2...

Details Hex view

Value: User Accounts  
Shell Type: GUID: Control panel


Bag Path: BagMRU\4\2 Slot #: 1 MRU Position: 0  
Absolute Path: Desktop\Control Panel\All Control Panel Items\User Accounts

# Child Bags: 1

Last explored: 1/7/2015 2:40:20 PM +00:00

Last Write Time: 1/7/2015 2:40:20 PM +00:00

Hex Value: 1E-00-71-80-00-00-00-00-00-00-00-00-00-00-54-27-63-60-23-C5-62-4B-8



- I still know what you did !!!



# Index.DAT

- Contains all of the Web sites
- Every URL
- Every Web page
- All email sent or received through Outlook or Outlook Express
- All internet temp files
- All pictures viewed

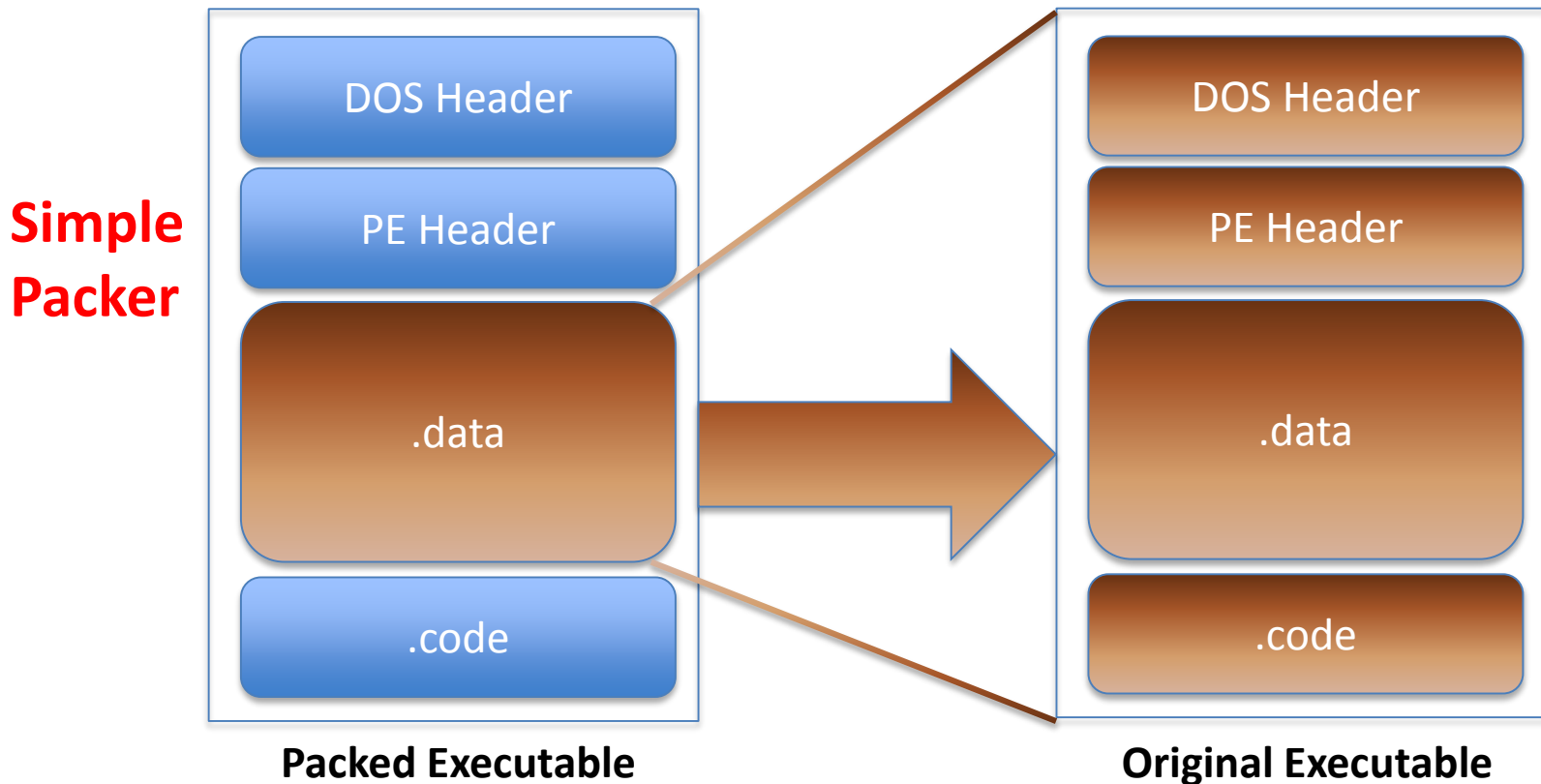


# Thumbs.DB

- Pictures opened in Windows OS
- Filmstrip
- Thumbnails
- Thumbs.DB Viewer

# Binary Obfuscation

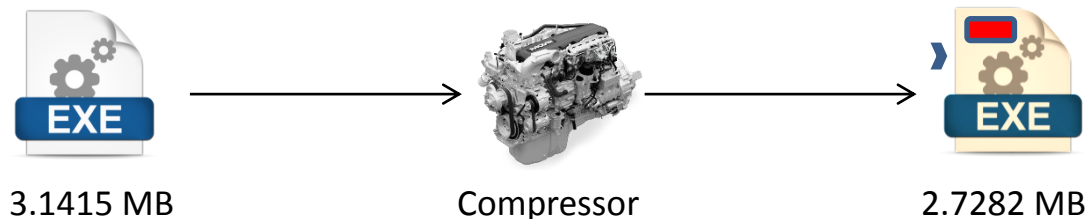
- Packers / Unpackers
  - Reduce size, Hide actual code, Hide IAT, Anti-X



# Binary Obfuscation – Cont.

- Complex packers might overwrite its own memory space
- Unpacking:
  - Statically (complex and time consuming)
  - Dynamically (easy, needs native env.)
  - Hybrid (best of both)
- Types:
  - Common: UPX, FSG, MEW
  - Complex: Armadillo, Obsidium, Sdprotect, ExeCrypt, VMProtect

GetProcAddress  
VirtualProtect  
VirtualAlloc  
VirtualFree  
ExitProcess





# File Systems Artifacts

---

*“Don’t let jumbled Data Structures fool  
you!”*

# Disks

- Without understanding of disks layout, you'll never know what is truly hidden over there!

<b>Disk 0</b> Basic 22.00 GB Online	<b>System Reserved</b> 100 MB NTFS Healthy (System, Active, Primary Partition)	<b>(C:)</b> 21.90 GB NTFS Healthy (Boot, Page File, Crash Dump, Primary Partition)
<b>Disk 1</b> Basic 204 MB Online	<b>test (Q:)</b> 202 MB NTFS Healthy (Primary Partition)	<b>2 MB</b> Unallo

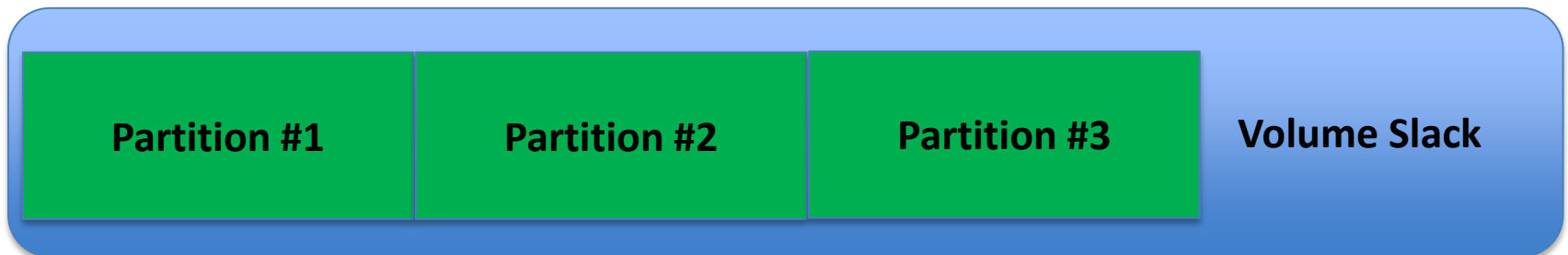
Do you know what's here?

# File Systems

- Can reveal useful artifacts like:
  - Manipulated Timestamps
  - Metadata : deleted or crumbs
  - Logs of actions : Journals

# Volume Slack

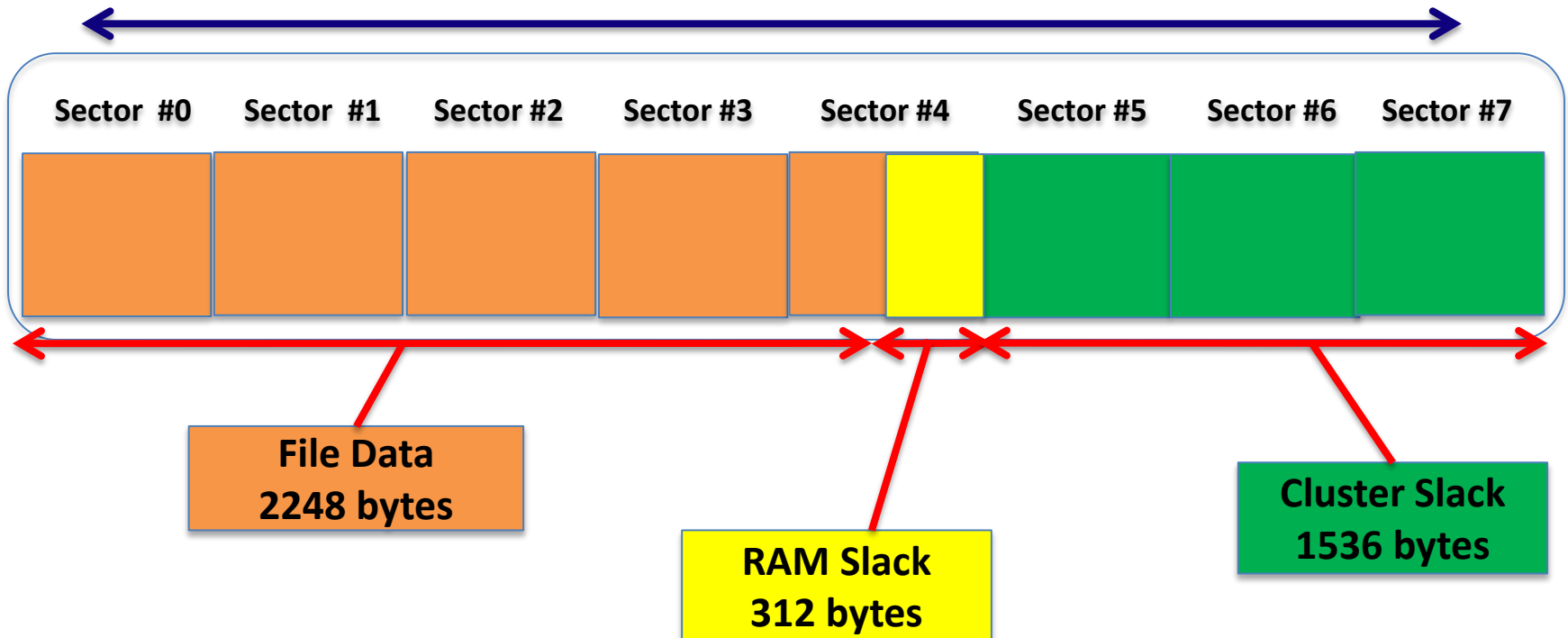
- Unused space between the end of the volume and the end of the partition
- Size of the hidden data in volume slack is only limited by the space on the hard disk available for a partition



# File Slack Space

- Slack space could be used to hide data

## Single Cluster with 8 sectors (4096 bytes)



# File Systems (NTFS)

- Everything written to the disk is considered a **file**
  - Files, directories, metadata, etc
- MFT is the heart of NTFS (array of records 1024 bytes each)
- Records in the MFT are called **metadata**
- First 16 records in the MFT reserved for metadata files
- Entry #1 is **\$MFT**

# PowerForensics

```
PS C:\Windows\system32> $mft = Get-ForensicFileRecord -VolumeName \\.\C:  
PS C:\Windows\system32> $mft[0]
```

```
FullName           : C:\$MFT  
Name               : $MFT  
SequenceNumber     : 1  
RecordNumber       : 0  
ParentSequenceNumber : 5  
ParentRecordNumber  : 5  
Directory          : False  
Deleted            : False  
ModifiedTime       : 8/13/2015 9:35:13 PM  
AccessedTime       : 8/13/2015 9:35:13 PM  
ChangedTime        : 8/13/2015 9:35:13 PM  
BornTime           : 8/13/2015 9:35:13 PM  
FNModifiedTime     : 8/13/2015 9:35:13 PM  
FNAccessedTime     : 8/13/2015 9:35:13 PM  
FNChangedTime      : 8/13/2015 9:35:13 PM  
FNBornTime         : 8/13/2015 9:35:13 PM
```





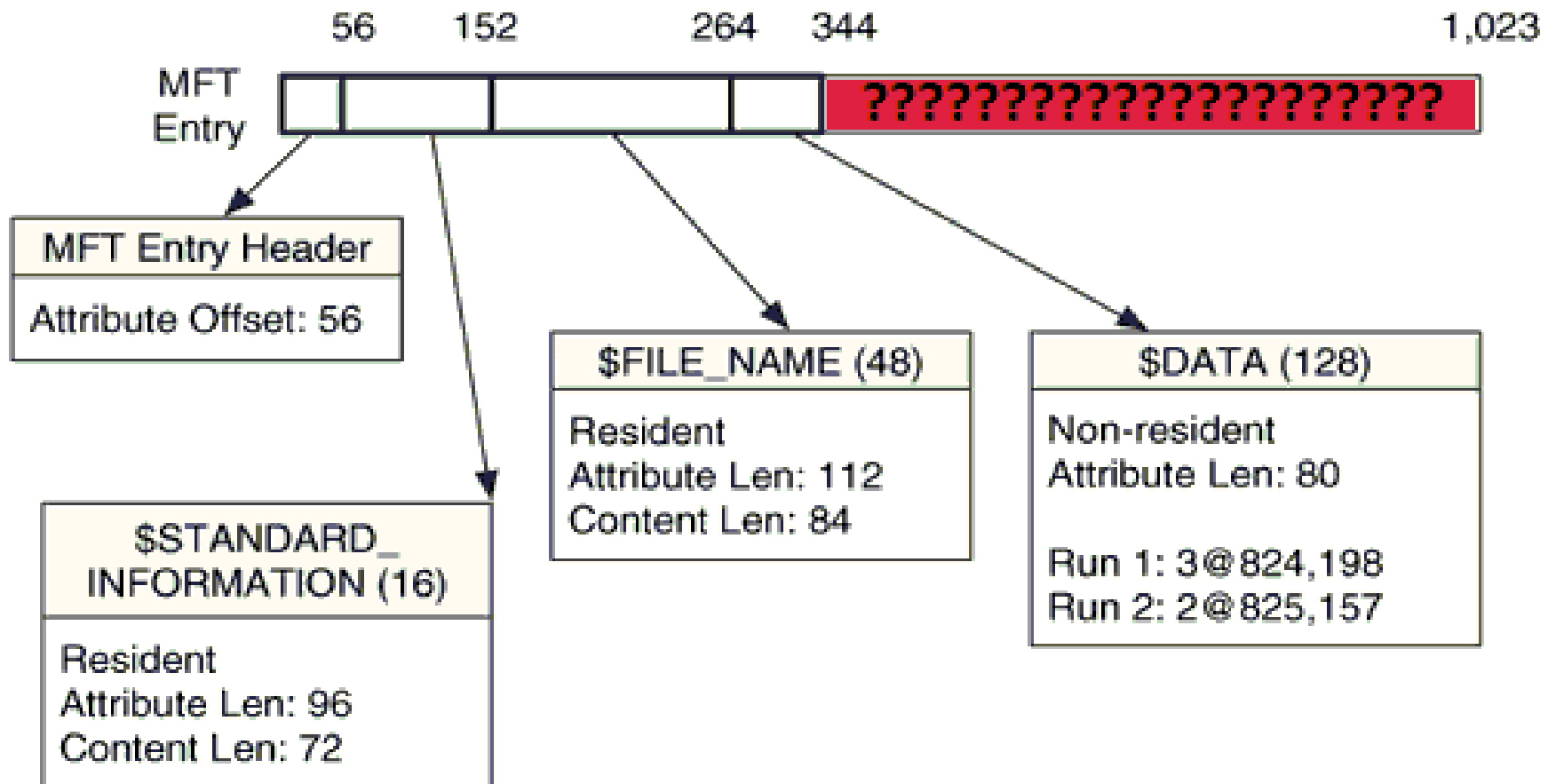
# File Systems (NTFS) – Cont.

- Deleted Files
  - Unallocated space
  - File System Journals, Index Files, and Log files: **\$I30**, **\$LogFile**, **\$UsnJrnl**
- File Wipers
  - Some crumbs left for investigator!
- Hiding within **\$DATA** attribute
- Timestamps and timestomp tools
  - MACE / MACB



# \$MFT Slack Space

- MFT Slack Space



# Bad Blocks (\$BadClus)

- Marked in the metadata file **\$BadClus** (*MFT entry 8*)
- Sparse file with the size set to the size of the entire file system
- Bad clusters are allocated to this file
- Clusters can be allocated to **\$BadClus** and used to store data

# Alternate Data Streams (ADS)

- More than one \$DATA attribute
- Locating streams:
  - Streams, LADS, etc
  - DF tools
  - Manually!

```
echo I am the hidden text > file.txt:Hidden.txt
```

- Can also hide binaries!
  - Images
  - EXEs
  - etc

46 49 4C 45 30 00 03 00	9F 45 10 00 00 00 00 00	FILE0	ÿÈ
01 00 01 00 38 00 01 00	B0 01 00 00 00 04 00 00	8	°
00 00 00 00 00 00 00 00	08 00 00 00 25 00 00 00		§
04 00 00 00 00 00 00 00	10 00 00 00 60 00 00 00		·
00 00 00 00 00 00 00 00	48 00 00 00 18 00 00 00		H
AA 5C 79 8B 77 F1 CF 01	44 E8 01 A6 77 F1 CF 01	*\y<wñĩ	Dè ;wñĩ
44 E8 01 A6 77 F1 CF 01	AA 5C 79 8B 77 F1 CF 01	Dè ;wñĩ	*\y<wñĩ
20 00 00 00 00 00 00 00	00 00 00 00 00 00 00 00		
00 00 00 00 08 01 00 00	00 00 00 00 00 00 00 00		
00 00 00 00 00 00 00 00	30 00 00 00 70 00 00 00	0	p
00 00 00 00 00 00 04 00	52 00 00 00 18 00 01 00	R	
05 00 00 00 00 00 05 00	AA 5C 79 8B 77 F1 CF 01	*\y<wñĩ	
AA 5C 79 8B 77 F1 CF 01	AA 5C 79 8B 77 F1 CF 01	*\y<wñĩ	*\y<wñĩ
AA 5C 79 8B 77 F1 CF 01	00 00 00 00 00 00 00 00	*\y<wñĩ	
00 00 00 00 00 00 00 00	20 00 00 00 00 00 00 00		
	00 74 00 78 00	file.txt	
	00 28 00 00 00	t.TX@	(
00 00 00 00 00 00 05 00	10 00 00 00 18 00 00 00		
45 2B DD 49 C4 5B E4 11	A7 B6 D4 CA 3F E5 0F CA	E+ÝIÄ[ä sqÔÊ?â Ê	
80 00 00 00 30 00 00 00	00 00 18 00 00 00 06 00	€ 0	
16 00 00 00 18 00 00 00	49 20 61 6D 20 74 68 65	I am the	
20 6F 72 69 67 69 6E 61	6C 20 74 65 78 74 00 00	original text	
80 00 00 00 48 00 00 00	00 0A 18 00 00 00 07 00	€ H	
17 00 00 00 30 00 00 00	68 00 69 00 64 00 64 00	0 hidd	
65 00 6E 00 2E 00 74 00	78 00 74 00 2E 00 74 00	en.txt.t	
49 20 61 6D 20 74 68 65	20 68 69 64 64 65 6E 20	I am the hidden	
74 65 78 74 20 0D 0A 00	FF FF FF FF 82 79 47 11	text ÿÿÿÿ,yG	
FF FF FF FF 82 79 47 11	00 00 00 00 00 00 00 00	ÿÿÿÿ,yG	

# Time Manipulation: Timestamp

- Also a form of Data Hiding!

MFT#	MFTPrnt	CTime	ATime	MTime	RTime	FileName
10978	10456	2014-09-10 15:27:28:207:9439	1999-08-02 00:11:40:000:0000	2014-09-10 15:27:28:207:9439	2014-09-10 15:27:28:207:9439	groucho.art
10979	10456	2014-09-10 15:27:28:248:0015	1999-08-02 00:11:40:000:0000	2014-09-10 15:27:28:248:0015	2014-09-10 15:27:28:248:0015	holly.art
10980	10456	2014-09-10 15:27:28:298:0735	1999-08-02 00:11:40:000:0000	2014-09-10 15:27:28:298:0735	2014-09-10 15:27:28:298:0735	ingrid.art
10981	10456	2014-09-10 15:27:28:348:1455	1999-08-02 00:11:40:000:0000	2014-09-10 15:27:28:348:1455	2014-09-10 15:27:28:348:1455	jessie.art
10982	10456	2014-09-10 15:27:28:398:2175	1999-08-02 00:11:40:000:0000	2014-09-10 15:27:28:398:2175	2014-09-10 15:27:28:398:2175	kathy.art
10983	10456	2014-09-10 15:27:28:448:2895	1999-08-02 00:11:40:000:0000	2014-09-10 15:27:28:448:2895	2014-09-10 15:27:28:448:2895	kelly.art
10984	10456	2014-09-10 15:27:28:488:3471	1999-08-02 00:11:40:000:0000	2014-09-10 15:27:28:488:3471	2014-09-10 15:27:28:488:3471	kennedy.art
10985	10456	2014-09-10 15:27:28:518:3903	1999-08-02 00:11:40:000:0000	2014-09-10 15:27:28:518:3903	2014-09-10 15:27:28:518:3903	kings.art
10986	10456	2014-09-10 15:27:28:568:4623	1999-08-02 00:11:42:000:0000	2014-09-10 15:27:28:568:4623	2014-09-10 15:27:28:568:4623	kirk.art
10987	10456	2014-09-10 15:27:28:608:5199	1999-08-02 00:11:42:000:0000	2014-09-10 15:27:28:608:5199	2014-09-10 15:27:28:608:5199	lincoln.art
10988	10456	2014-09-10 15:27:28:648:5775	1999-08-02 00:11:42:000:0000	2014-09-10 15:27:28:648:5775	2014-09-10 15:27:28:648:5775	lovebox.art
10989	10456	2014-09-10 15:27:28:698:6495	1999-08-02 00:11:42:000:0000	2014-09-10 15:27:28:698:6495	2014-09-10 15:27:28:698:6495	madonna.art
10990	10456	2014-09-10 15:27:28:748:7215	1999-08-02 00:11:42:000:0000	2014-09-10 15:27:28:748:7215	2014-09-10 15:27:28:748:7215	monalisa.art
10991	10456	2014-09-10 15:27:28:788:7791	1999-08-02 00:11:42:000:0000	2014-09-10 15:27:28:788:7791	2014-09-10 15:27:28:788:7791	newyears.art
10992	10456	2014-09-10 15:27:28:868:8943	1999-08-02 00:11:42:000:0000	2014-09-10 15:27:28:868:8943	2014-09-10 15:27:28:868:8943	oliver.art

# Time Manipulation: Detection

- Compare timestamps of SIA with FN attributes
- FN attributes timestamps must be older than SIA timestamps
- Zero milliseconds in timestamps is suspect
- Check creation timestamps earlier than file system format date
- Check Shadow Copies (SVCs) and Restore Points
- Check Journal files
- Creating timelines

# \$UsnJrnl

- Tracking NTFS's history with \$UsnJrnl
  - Creation, deletion, modification, renaming and moving of file and directory
  - It is possible to find trace of deleted file.
  - The event of program execution and opening document can be found through tracking prefetch file and LNK file's history
- \$UsnJrnl record carving from unallocated space
  - There are mass \$UsnJrnl records in unallocated space
  - Tracking old file system history(before several months) through \$UsnJrnl record carving



# NTFS INDX Files (aka: \$i30)

- Each directory index entry contains at least the following metadata for the child:
  - Filename
  - Physical size of file
  - Logical size of file
  - Modified timestamp
  - Accessed timestamp
  - Changed timestamp
  - Created timestamp

# \$LogFile

- A transaction journal of changes to the \$MFT
- Could find file fragments and MFT records
- Could find MFT records in unallocated space
- Could locate file names that no longer exist on the disk

	A	B	C	D	E	F	G	H	I
1	If_Offset	If_MFTRef	If_LSN	If_RedoOperation	If_UndoOperation	If_SI_CTime	If_SI_ATime	If_SI_MTime	If_SI_RTime
2	0x00007040	37	50335240	SetNewAttributeSizes	SetNewAttributeSizes				
3	0x000070C8	37	50335257	UpdateMappingPairs	UpdateMappingPairs				
4	0x00007130	37	50335270	SetNewAttributeSizes	SetNewAttributeSizes				
5	0x000071B8	-1	50335287	ForgetTransaction	CompensationlogRecord				
6	0x00007210	36	50335298	UpdateFileNameRoot	UpdateFileNameRoot	2014-09-05 19:06:26:375:4802	2014-09-05 19:06:33:269:1695	2014-09-05 19:06:33:269:1695	2014-09-05 19:06:26:375:4
7	0x000072D8	-1	50335323	ForgetTransaction	CompensationlogRecord				
8	0x00007330	36	50335334	UpdateFileNameRoot	UpdateFileNameRoot	2014-09-05 19:06:26:375:4802	2014-09-05 19:06:33:269:1695	2014-09-05 19:06:33:269:1695	2014-09-05 19:06:26:375:4
9	0x000073F8	-1	50335359	ForgetTransaction	CompensationlogRecord				
10	0x00007450	37	50335370	SetNewAttributeSizes	SetNewAttributeSizes				
11	0x000074D8	-1	50335387	ForgetTransaction	CompensationlogRecord				
12	0x00007530	36	50335398	UpdateFileNameRoot	UpdateFileNameRoot	2014-09-05 19:06:26:375:4802	2014-09-05 19:06:33:269:1695	2014-09-05 19:06:33:269:1695	2014-09-05 19:06:26:375:4
13	0x000075F8	-1	50335423	ForgetTransaction	CompensationlogRecord				
14	0x00007650	-1	50335434	ClearBitsInNonresidentBitMap	SetBitsInNonresidentBitMap				
15	0x000076B0	37	50335446	UpdateMappingPairs	UpdateMappingPairs				
16	0x00007718	37	50335459	SetNewAttributeSizes	SetNewAttributeSizes				
17	0x000077A0	-1	50335476	ForgetTransaction	CompensationlogRecord				

LogFile

# Finally ...

- To catch a criminal, you need to think like one!
- Without proper understanding of the under-laying technology, its just like you're searching for a needle in the haystack!
- *They can run, but they can't hide for ever 😊*



# References

- <http://blogs.technet.com/b/askcore/archive/2013/03/24/alternate-data-streams-in-ntfs.aspx>
- <http://www.autohotkey.com/docs/misc/CLSID-List.htm>
- <https://www.runtime.org/diskexplorer.htm>
- Anti-Forensics: Techniques, Detection and Countermeasures, Simson Garfinkel
- Metasploit Autopsy – Reconstructing the Crime Scene, <http://www.blackhat.com/presentations/bh-usa-09/SILBERMAN/BHUSA09-Silberman-MetasploitAutopsy-SLIDES.pdf>
- A Windows Registry Quick Reference: For the Everyday Examiner, Derrick J. Farmer and Burlington, Vermont
- [https://en.wikiquote.org/wiki/Sherlock\\_Holmes](https://en.wikiquote.org/wiki/Sherlock_Holmes)
- PowerForensics Get-ForensicUsnJrnl, <http://www.invoke-ir.com/2016/02/forensic-friday-get-forensicusnjrnl.html>

# References – P2

- Advanced \$UsnJrnl Forensics, FORENSIC INSIGHT
- Prefetch Files, <http://www.forensicswiki.org/wiki/Prefetch>
- LECmd, Eric Zimmerman,  
<http://binaryforay.blogspot.com/2016/02/introducing-lecmd.html>
- <http://www.williballenthin.com/forensics/indx/>