RSA CONFERENCE ASIA PACIFIC 2013

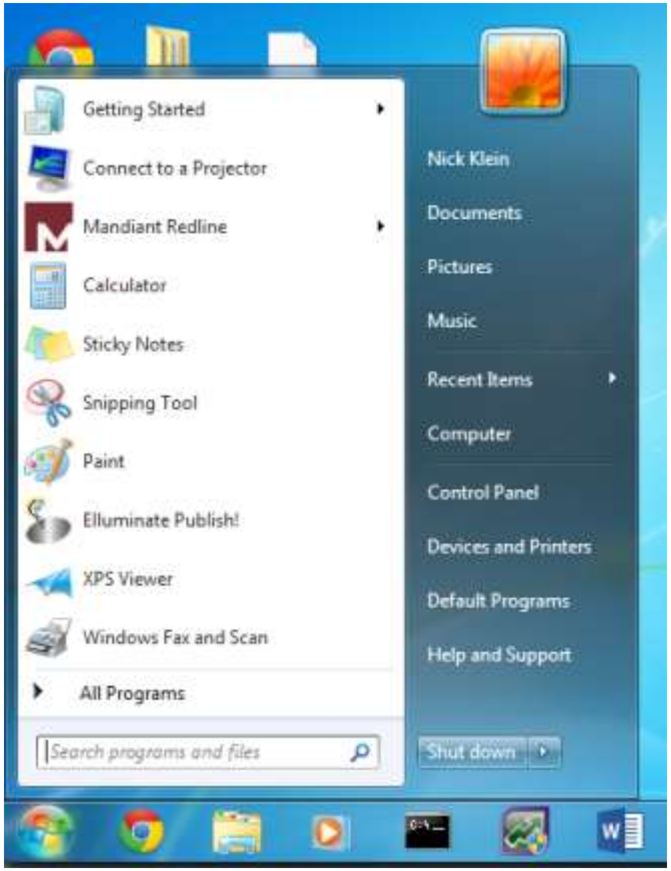
FORENSIC TREASURE HUNT

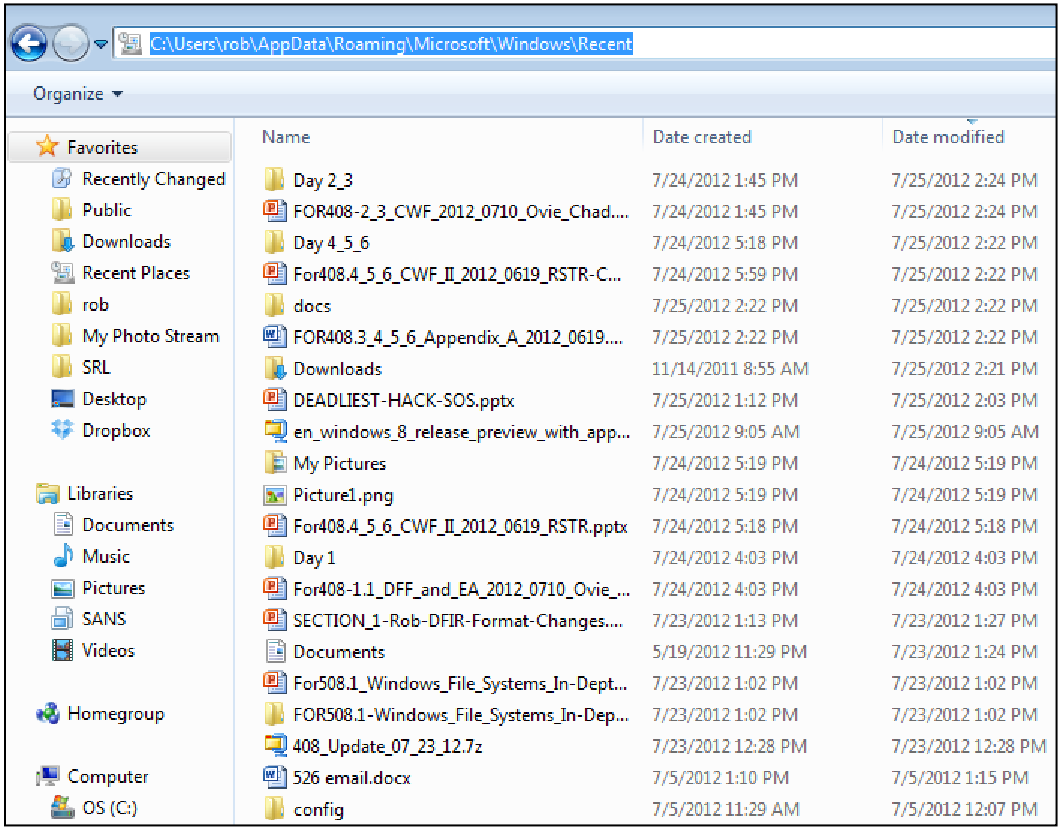
Nick Klein
Instructor, SANS Institute
Director, Klein & Co. Computer Forensics

Session ID: SANS

Session Classification: Intermediate

SHORTCUT / LINK FILES



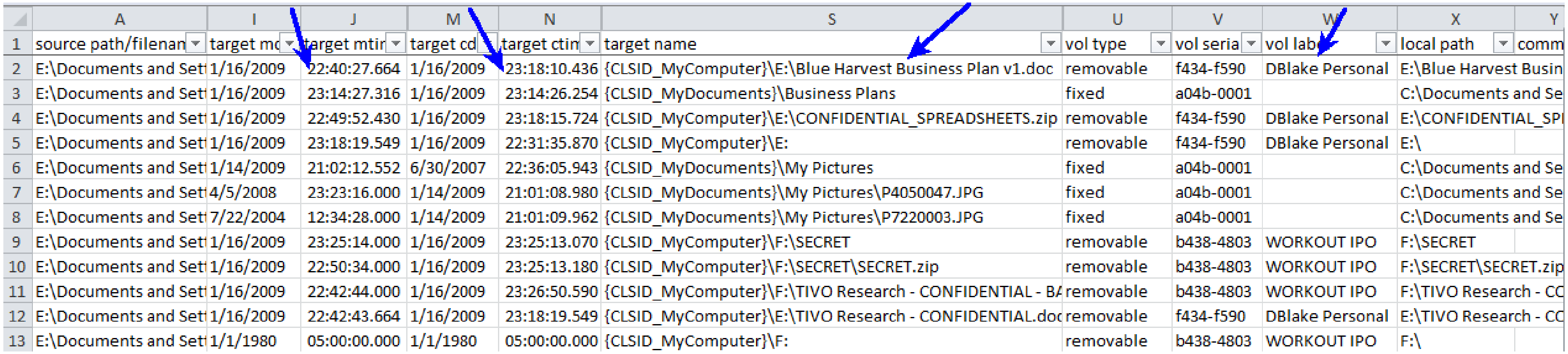


C:\Users\rob\AppData\Roaming\Microsoft\Windows\Recent

Name	Date created	Date modified
Day 2_3	7/24/2012 1:45 PM	7/25/2012 2:24 PM
FOR408-2_3_CWF_2012_0710_Ovie_Chad....	7/24/2012 1:45 PM	7/25/2012 2:24 PM
Day 4_5_6	7/24/2012 5:18 PM	7/25/2012 2:22 PM
For408.4_5_6_CWF_II_2012_0619_RSTR-C...	7/24/2012 5:59 PM	7/25/2012 2:22 PM
docs	7/25/2012 2:22 PM	7/25/2012 2:22 PM
FOR408.3_4_5_6_Appendix_A_2012_0619....	7/25/2012 2:22 PM	7/25/2012 2:22 PM
Downloads	11/14/2011 8:55 AM	7/25/2012 2:21 PM
DEADLIEST-HACK-SOS.pptx	7/25/2012 1:12 PM	7/25/2012 2:03 PM
en_windows_8_release_preview_with_app...	7/25/2012 9:05 AM	7/25/2012 9:05 AM
My Pictures	7/24/2012 5:19 PM	7/24/2012 5:19 PM
Picture1.png	7/24/2012 5:19 PM	7/24/2012 5:19 PM
For408.4_5_6_CWF_II_2012_0619_RSTR.pptx	7/24/2012 5:18 PM	7/24/2012 5:18 PM
Day 1	7/24/2012 4:03 PM	7/24/2012 4:03 PM
For408-1.1_DFF_and_EA_2012_0710_Ovie_...	7/24/2012 4:03 PM	7/24/2012 4:03 PM
SECTION_1-Rob-DFIR-Format-Changes....	7/23/2012 1:13 PM	7/23/2012 1:27 PM
Documents	5/19/2012 11:29 PM	7/23/2012 1:24 PM
For508.1_Windows_File_Systems_In-Dept...	7/23/2012 1:02 PM	7/23/2012 1:02 PM
FOR508.1-Windows_File_Systems_In-Dep...	7/23/2012 1:02 PM	7/23/2012 1:02 PM
408_Update_07_23_12.7z	7/23/2012 12:28 PM	7/23/2012 12:28 PM
526 email.docx	7/5/2012 1:10 PM	7/5/2012 1:15 PM
config	7/5/2012 11:29 AM	7/5/2012 12:07 PM

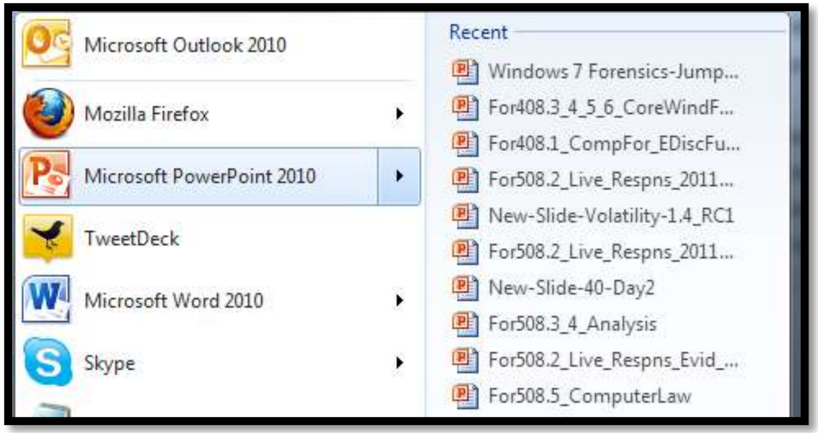
SHORTCUT / LINK FILES

- File and folder
- Full path
- Volume name
- Volume serial
- Shortcut timestamps
- Target timestamps

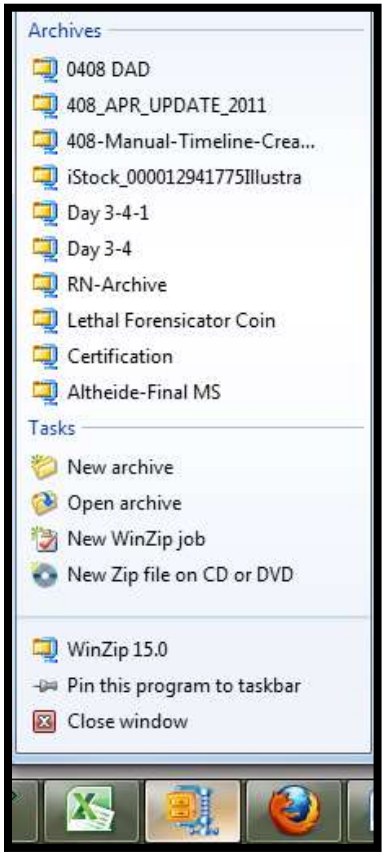


	A	I	J	M	N	S	U	V	W	X	Y
1	source path/filenan	target mc	target mtir	target cd	target ctin	target name	vol type	vol seria	vol labe	local path	comm
2	E:\Documents and Sett	1/16/2009	22:40:27.664	1/16/2009	23:18:10.436	{CLSID_MyComputer}\E:\Blue Harvest Business Plan v1.doc	removable	f434-f590	DBlake Personal	E:\Blue Harvest Busin	
3	E:\Documents and Sett	1/16/2009	23:14:27.316	1/16/2009	23:14:26.254	{CLSID_MyDocuments}\Business Plans	fixed	a04b-0001		C:\Documents and Se	
4	E:\Documents and Sett	1/16/2009	22:49:52.430	1/16/2009	23:18:15.724	{CLSID_MyComputer}\E:\CONFIDENTIAL_SPREADSHEETS.zip	removable	f434-f590	DBlake Personal	E:\CONFIDENTIAL_SPI	
5	E:\Documents and Sett	1/16/2009	23:18:19.549	1/16/2009	22:31:35.870	{CLSID_MyComputer}\E:	removable	f434-f590	DBlake Personal	E:\	
6	E:\Documents and Sett	1/14/2009	21:02:12.552	6/30/2007	22:36:05.943	{CLSID_MyDocuments}\My Pictures	fixed	a04b-0001		C:\Documents and Se	
7	E:\Documents and Sett	4/5/2008	23:23:16.000	1/14/2009	21:01:08.980	{CLSID_MyDocuments}\My Pictures\P4050047.JPG	fixed	a04b-0001		C:\Documents and Se	
8	E:\Documents and Sett	7/22/2004	12:34:28.000	1/14/2009	21:01:09.962	{CLSID_MyDocuments}\My Pictures\P7220003.JPG	fixed	a04b-0001		C:\Documents and Se	
9	E:\Documents and Sett	1/16/2009	23:25:14.000	1/16/2009	23:25:13.070	{CLSID_MyComputer}\F:\SECRET	removable	b438-4803	WORKOUT IPO	F:\SECRET	
10	E:\Documents and Sett	1/16/2009	22:50:34.000	1/16/2009	23:25:13.180	{CLSID_MyComputer}\F:\SECRET\SECRET.zip	removable	b438-4803	WORKOUT IPO	F:\SECRET\SECRET.zip	
11	E:\Documents and Sett	1/16/2009	22:42:44.000	1/16/2009	23:26:50.590	{CLSID_MyComputer}\F:\TIVO Research - CONFIDENTIAL - BA	removable	b438-4803	WORKOUT IPO	F:\TIVO Research - CC	
12	E:\Documents and Sett	1/16/2009	22:42:43.664	1/16/2009	23:18:19.549	{CLSID_MyComputer}\E:\TIVO Research - CONFIDENTIAL.doc	removable	f434-f590	DBlake Personal	E:\TIVO Research - CC	
13	E:\Documents and Sett	1/1/1980	05:00:00.000	1/1/1980	05:00:00.000	{CLSID_MyComputer}\F:	removable	b438-4803	WORKOUT IPO	F:\	

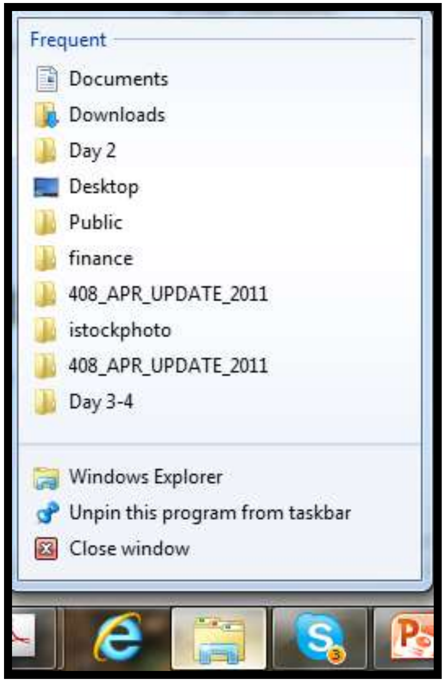
JUMP LISTS



Microsoft Outlook 2010
Mozilla Firefox
Microsoft PowerPoint 2010
TweetDeck
Microsoft Word 2010
Skype
Recent
Windows 7 Forensics-Jump...
For408.3_4_5_6_CoreWindF...
For408.1_CompFor_EDiscFu...
For508.2_Live_Respns_2011...
New-Slide-Volatility-1.4_RC1
For508.2_Live_Respns_2011...
New-Slide-40-Day2
For508.3_4_Analysis
For508.2_Live_Respns_Evid_...
For508.5_ComputerLaw

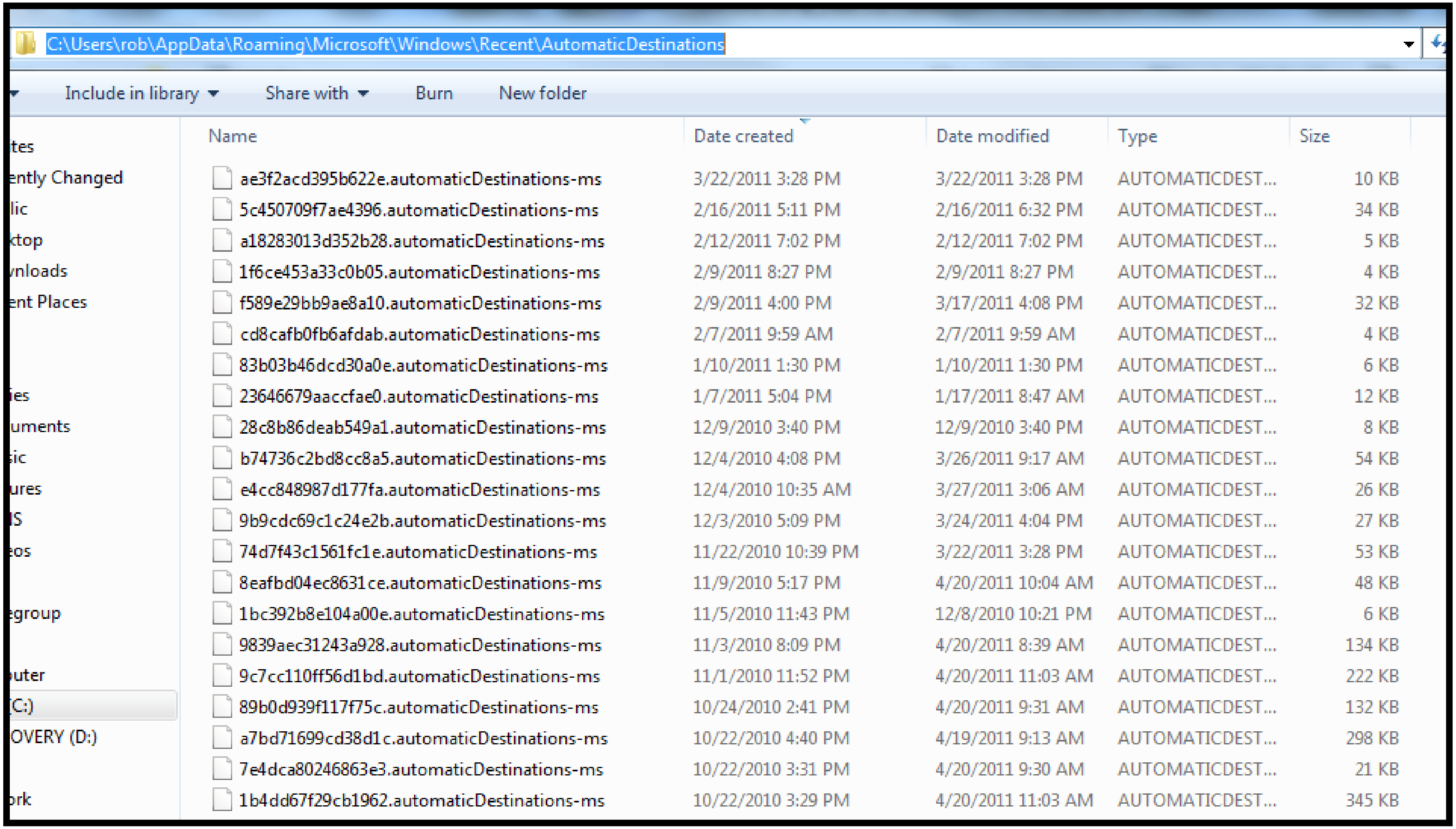


Archives
0408 DAD
408_APR_UPDATE_2011
408-Manual-Timeline-Crea...
iStock_000012941775Illustra
Day 3-4-1
Day 3-4
RN-Archive
Lethal Forensicator Coin
Certification
Altheide-Final MS
Tasks
New archive
Open archive
New WinZip job
New Zip file on CD or DVD
WinZip 15.0
Pin this program to taskbar
Close window



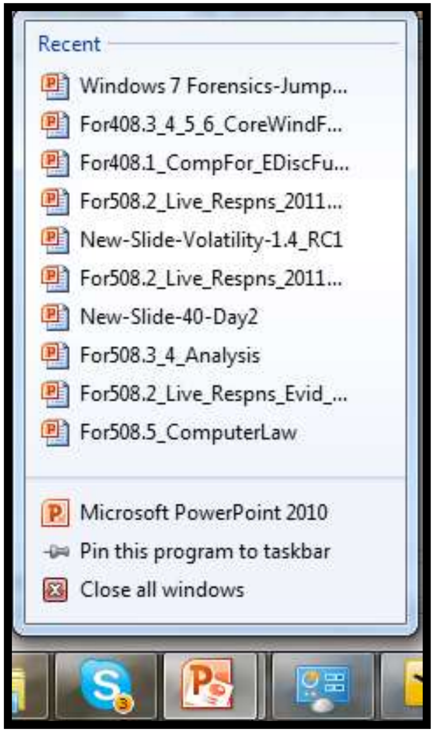
Frequent
Documents
Downloads
Day 2
Desktop
Public
finance
408_APR_UPDATE_2011
istockphoto
408_APR_UPDATE_2011
Day 3-4
Windows Explorer
Unpin this program from taskbar
Close window

JUMP LISTS



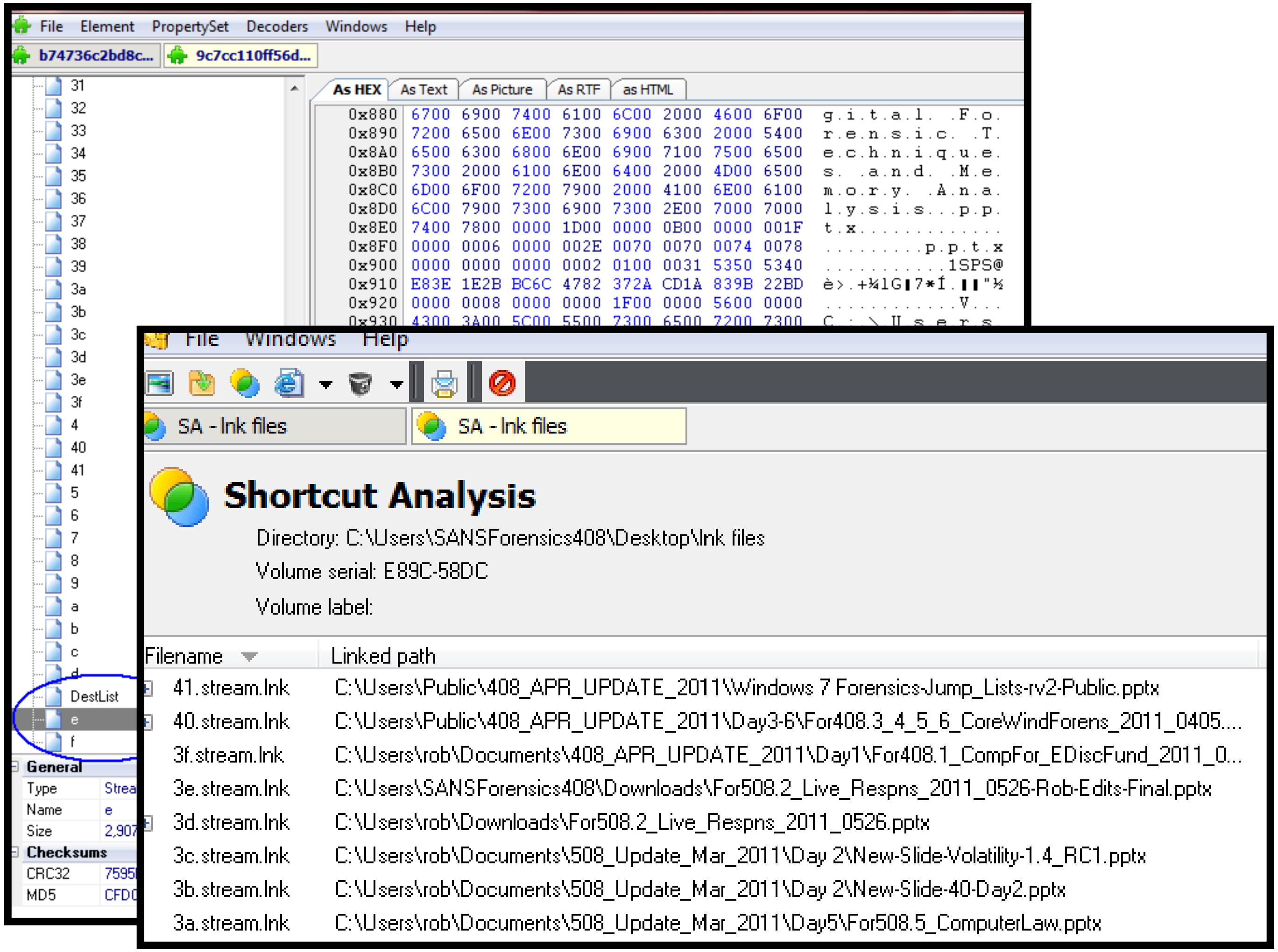
Name	Date created	Date modified	Type	Size
ae3f2acd395b622e.automaticDestinations-ms	3/22/2011 3:28 PM	3/22/2011 3:28 PM	AUTOMATICDEST...	10 KB
5c450709f7ae4396.automaticDestinations-ms	2/16/2011 5:11 PM	2/16/2011 6:32 PM	AUTOMATICDEST...	34 KB
a18283013d352b28.automaticDestinations-ms	2/12/2011 7:02 PM	2/12/2011 7:02 PM	AUTOMATICDEST...	5 KB
1f6ce453a33c0b05.automaticDestinations-ms	2/9/2011 8:27 PM	2/9/2011 8:27 PM	AUTOMATICDEST...	4 KB
f589e29bb9ae8a10.automaticDestinations-ms	2/9/2011 4:00 PM	3/17/2011 4:08 PM	AUTOMATICDEST...	32 KB
cd8cafb0fb6afdab.automaticDestinations-ms	2/7/2011 9:59 AM	2/7/2011 9:59 AM	AUTOMATICDEST...	4 KB
83b03b46dcd30a0e.automaticDestinations-ms	1/10/2011 1:30 PM	1/10/2011 1:30 PM	AUTOMATICDEST...	6 KB
23646679aaccfae0.automaticDestinations-ms	1/7/2011 5:04 PM	1/17/2011 8:47 AM	AUTOMATICDEST...	12 KB
28c8b86deab549a1.automaticDestinations-ms	12/9/2010 3:40 PM	12/9/2010 3:40 PM	AUTOMATICDEST...	8 KB
b74736c2bd8cc8a5.automaticDestinations-ms	12/4/2010 4:08 PM	3/26/2011 9:17 AM	AUTOMATICDEST...	54 KB
e4cc848987d177fa.automaticDestinations-ms	12/4/2010 10:35 AM	3/27/2011 3:06 AM	AUTOMATICDEST...	26 KB
9b9cdc69c1c24e2b.automaticDestinations-ms	12/3/2010 5:09 PM	3/24/2011 4:04 PM	AUTOMATICDEST...	27 KB
74d7f43c1561fc1e.automaticDestinations-ms	11/22/2010 10:39 PM	3/22/2011 3:28 PM	AUTOMATICDEST...	53 KB
8eafbd04ec8631ce.automaticDestinations-ms	11/9/2010 5:17 PM	4/20/2011 10:04 AM	AUTOMATICDEST...	48 KB
1bc392b8e104a00e.automaticDestinations-ms	11/5/2010 11:43 PM	12/8/2010 10:21 PM	AUTOMATICDEST...	6 KB
9839aec31243a928.automaticDestinations-ms	11/3/2010 8:09 PM	4/20/2011 8:39 AM	AUTOMATICDEST...	134 KB
9c7cc110ff56d1bd.automaticDestinations-ms	11/1/2010 11:52 PM	4/20/2011 11:03 AM	AUTOMATICDEST...	222 KB
89b0d939f117f75c.automaticDestinations-ms	10/24/2010 2:41 PM	4/20/2011 9:31 AM	AUTOMATICDEST...	132 KB
a7bd71699cd38d1c.automaticDestinations-ms	10/22/2010 4:40 PM	4/19/2011 9:13 AM	AUTOMATICDEST...	298 KB
7e4dca80246863e3.automaticDestinations-ms	10/22/2010 3:31 PM	4/20/2011 9:30 AM	AUTOMATICDEST...	21 KB
1b4dd67f29cb1962.automaticDestinations-ms	10/22/2010 3:29 PM	4/20/2011 11:03 AM	AUTOMATICDEST...	345 KB

JUMP LISTS



Recent

- Windows 7 Forensics-Jump...
- For408.3_4_5_6_CoreWindF...
- For408.1_CompFor_EDiscFu...
- For508.2_Live_Respns_2011...
- New-Slide-Volatility-1.4_RC1
- For508.2_Live_Respns_2011...
- New-Slide-40-Day2
- For508.3_4_Analysis
- For508.2_Live_Respns_Evid_...
- For508.5_ComputerLaw



```
0x880  6700 6900 7400 6100 6C00 2000 4600 6F00   g.i.t.a.l. .F.o.
0x890  7200 6500 6E00 7300 6900 6300 2000 5400   r.e.n.s.i.c. .T.
0x8A0  6500 6300 6800 6E00 6900 7100 7500 6500   e.c.h.n.i.q.u.e.
0x8B0  7300 2000 6100 6E00 6400 2000 4D00 6500   s. .a.n.d. .M.e.
0x8C0  6D00 6F00 7200 7900 2000 4100 6E00 6100   m.o.r.y. .A.n.a.
0x8D0  6C00 7900 7300 6900 7300 2E00 7000 7000   l.y.s.i.s...p.p.
0x8E0  7400 7800 0000 1D00 0000 0B00 0000 001F   t.x.............
0x8F0  0000 0006 0000 002E 0070 0070 0074 0078   .........p.p.t.x
0x900  0000 0000 0000 0002 0100 0031 5350 5340   ...........1SPS@
0x910  E83E 1E2B BC6C 4782 372A CD1A 839B 22BD   è>.+¼lG▌7*Í.▌▌"½
0x920  0000 0008 0000 0000 1F00 0000 5600 0000   ............V...
0x930  4300 3A00 5C00 5500 7300 6500 7200 7300   C.:.\.U.s.e.r.s.
```

General
Type: Strea
Name: e
Size: 2,907

Checksums
CRC32: 7595
MD5: CFDC

Shortcut Analysis

Directory: C:\Users\SANSForensics408\Desktop\lnk files

Volume serial: E89C-58DC

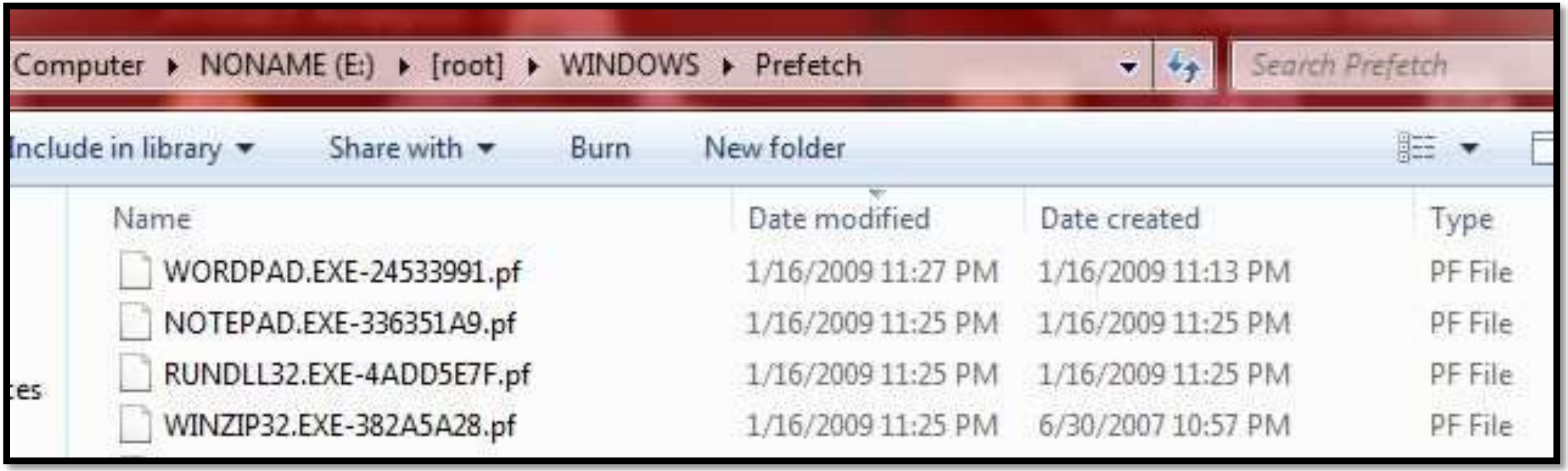
Volume label:

Filename	Linked path
41.stream.lnk	C:\Users\Public\408_APR_UPDATE_2011\Windows 7 Forensics-Jump_Lists-rv2-Public.pptx
40.stream.lnk	C:\Users\Public\408_APR_UPDATE_2011\Day3-6\For408.3_4_5_6_CoreWindForens_2011_0405....
3f.stream.lnk	C:\Users\rob\Documents\408_APR_UPDATE_2011\Day1\For408.1_CompFor_EDiscFund_2011_0...
3e.stream.lnk	C:\Users\SANSForensics408\Downloads\For508.2_Live_Respns_2011_0526-Rob-Edits-Final.pptx
3d.stream.lnk	C:\Users\rob\Downloads\For508.2_Live_Respns_2011_0526.pptx
3c.stream.lnk	C:\Users\rob\Documents\508_Update_Mar_2011\Day 2\New-Slide-Volatility-1.4_RC1.pptx
3b.stream.lnk	C:\Users\rob\Documents\508_Update_Mar_2011\Day 2\New-Slide-40-Day2.pptx
3a.stream.lnk	C:\Users\rob\Documents\508_Update_Mar_2011\Day5\For508.5_ComputerLaw.pptx

PREFETCH

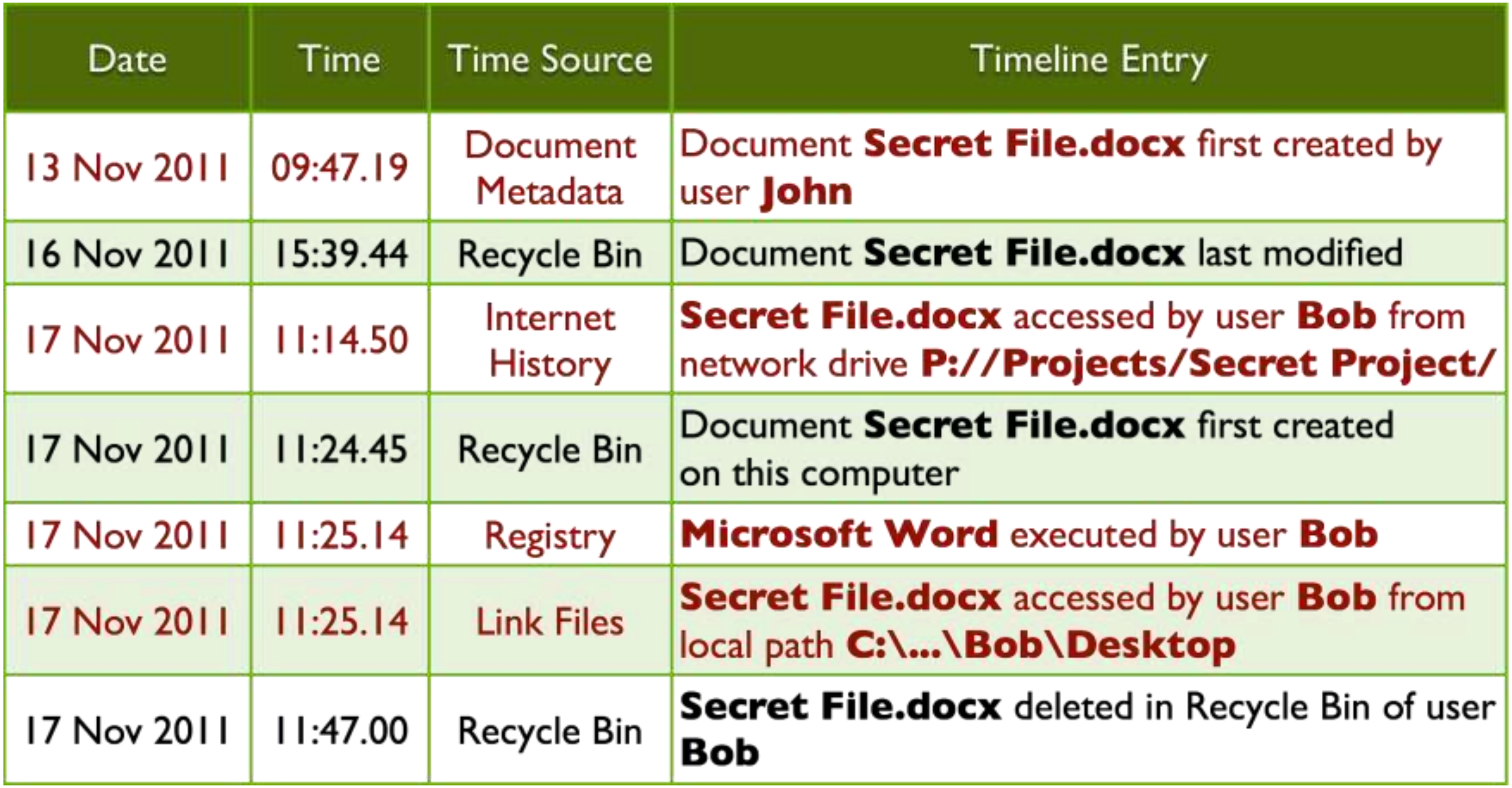
- Programs run
- First / last run times
- Run count

- Files, folders, devices accessed
- GUI and command line



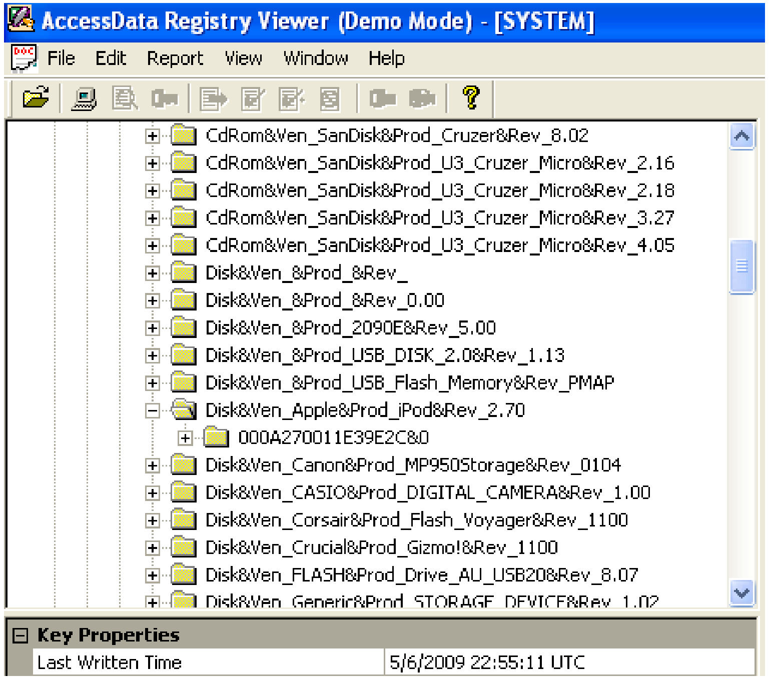
Name	Date modified	Date created	Type
WORDPAD.EXE-24533991.pf	1/16/2009 11:27 PM	1/16/2009 11:13 PM	PF File
NOTEPAD.EXE-336351A9.pf	1/16/2009 11:25 PM	1/16/2009 11:25 PM	PF File
RUNDLL32.EXE-4ADD5E7F.pf	1/16/2009 11:25 PM	1/16/2009 11:25 PM	PF File
WINZIP32.EXE-382A5A28.pf	1/16/2009 11:25 PM	6/30/2007 10:57 PM	PF File

“SUPER” TIMELINE



Date	Time	Time Source	Timeline Entry
13 Nov 2011	09:47.19	Document Metadata	Document **Secret File.docx** first created by user **John**
16 Nov 2011	15:39.44	Recycle Bin	Document **Secret File.docx** last modified
17 Nov 2011	11:14.50	Internet History	**Secret File.docx** accessed by user **Bob** from network drive **P://Projects/Secret Project/**
17 Nov 2011	11:24.45	Recycle Bin	Document **Secret File.docx** first created on this computer
17 Nov 2011	11:25.14	Registry	**Microsoft Word** executed by user **Bob**
17 Nov 2011	11:25.14	Link Files	**Secret File.docx** accessed by user **Bob** from local path **C:\...\Bob\Desktop**
17 Nov 2011	11:47.00	Recycle Bin	**Secret File.docx** deleted in Recycle Bin of user **Bob**

USB DEVICES



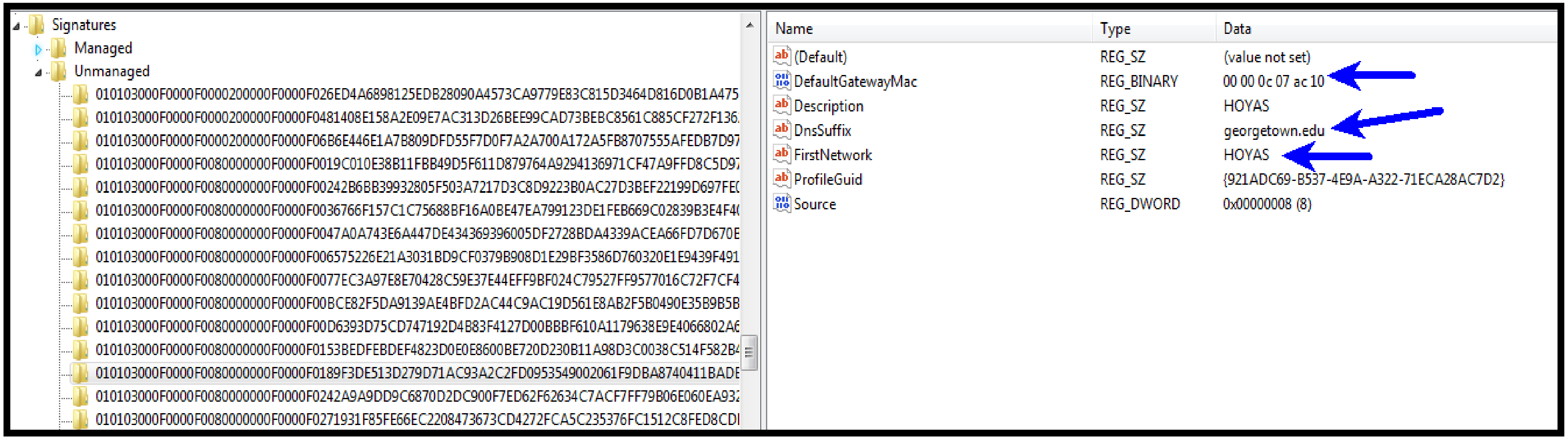
```
⊞ CdRom&Ven_SanDisk&Prod_Cruzer&Rev_8.02
⊞ CdRom&Ven_SanDisk&Prod_U3_Cruzer_Micro&Rev_2.16
⊞ CdRom&Ven_SanDisk&Prod_U3_Cruzer_Micro&Rev_2.18
⊞ CdRom&Ven_SanDisk&Prod_U3_Cruzer_Micro&Rev_3.27
⊞ CdRom&Ven_SanDisk&Prod_U3_Cruzer_Micro&Rev_4.05
⊞ Disk&Ven_&Prod_&Rev_
⊞ Disk&Ven_&Prod_&Rev_0.00
⊞ Disk&Ven_&Prod_2090E&Rev_5.00
⊞ Disk&Ven_&Prod_USB_DISK_2.0&Rev_1.13
⊞ Disk&Ven_&Prod_USB_Flash_Memory&Rev_PMAP
⊟ Disk&Ven_Apple&Prod_iPod&Rev_2.70
    ⊞ 000A270011E39E2C&0
⊞ Disk&Ven_Canon&Prod_MP950Storage&Rev_0104
⊞ Disk&Ven_CASIO&Prod_DIGITAL_CAMERA&Rev_1.00
⊞ Disk&Ven_Corsair&Prod_Flash_Voyager&Rev_1100
⊞ Disk&Ven_Crucial&Prod_Gizmo!&Rev_1100
⊞ Disk&Ven_FLASH&Prod_Drive_AU_USB20&Rev_8.07
⊞ Disk&Ven_Generic&Prod_STORAGE_DEVICE&Rev_1.02
```

⊟ **Key Properties**

Last Written Time	5/6/2009 22:55:11 UTC

- Vendor, make, model
- Physical device serial no.
- Last used drive letter
- Volume name
- Last user of device
- Times of:
  - First connection
  - Last connection
  - First connection after last reboot

WIRELESS GEOLOCATION



```
Signatures
    Managed
    Unmanaged
        010103000F0000F0000200000F0000F026ED4A6898125EDB28090A4573CA9779E83C815D3464D816D0B1A475
        010103000F0000F0000200000F0000F0481408E158A2E09E7AC313D26BEE99CAD73BEBC8561C885CF272F136
        010103000F0000F0000200000F0000F06B6E446E1A7B809DFD55F7D0F7A2A700A172A5FB8707555AFEDB7D97
        010103000F0000F0080000000F0000F0019C010E38B11FBB49D5F611D879764A9294136971CF47A9FFD8C5D9
        010103000F0000F0080000000F0000F00242B6BB39932805F503A7217D3C8D9223B0AC27D3BEF22199D697FE
        010103000F0000F0080000000F0000F0036766F157C1C75688BF16A0BE47EA799123DE1FEB669C02839B3E4F4
        010103000F0000F0080000000F0000F0047A0A743E6A447DE434369396005DF2728BDA4339ACEA66FD7D670E
        010103000F0000F0080000000F0000F006575226E21A3031BD9CF0379B908D1E29BF3586D760320E1E9439F491
        010103000F0000F0080000000F0000F0077EC3A97E8E70428C59E37E44EFF9BF024C79527FF9577016C72F7CF4
        010103000F0000F0080000000F0000F00BCE82F5DA9139AE4BFD2AC44C9AC19D561E8AB2F5B0490E35B9B5B
        010103000F0000F0080000000F0000F00D6393D75CD747192D4B83F4127D00BBBF610A1179638E9E4066802A
        010103000F0000F0080000000F0000F0153BEDFEBDEF4823D0E0E8600BE720D230B11A98D3C0038C514F582B
        010103000F0000F0080000000F0000F0189F3DE513D279D71AC93A2C2FD0953549002061F9DBA8740411BADE
        010103000F0000F0080000000F0000F0242A9A9DD9C6870D2DC900F7ED62F62634C7ACF7FF79B06E060EA93
        010103000F0000F0080000000F0000F0271931F85FE66EC2208473673CD4272FCA5C235376FC1512C8FED8CD
```

Name	Type	Data
(Default)	REG_SZ	(value not set)
DefaultGatewayMac	REG_BINARY	00 00 0c 07 ac 10
Description	REG_SZ	HOYAS
DnsSuffix	REG_SZ	georgetown.edu
FirstNetwork	REG_SZ	HOYAS
ProfileGuid	REG_SZ	{921ADC69-B537-4E9A-A322-71ECA28AC7D2}
Source	REG_DWORD	0x00000008 (8)

- Domain / intranet name
- Wireless SSID
- MAC address of AP
- First and last connection times
- Possible geolocation

WHAT HAVE WE FOUND?

- Access by users to files and folders, target file metadata, times of use
- Access to network and local drives, times of use
- USB devices connected, times of use, volume names, serial numbers
- Files accessed through programs, times and context of use
- GUI and terminal program execution, run count and execution context, resources used
- Temporal reconstruction from a wide range of artefacts
- Connected networks, times of connection, gateway MAC address, possible geolocation
- Artefacts that survive even if a user tries to delete them

THANK YOU!