Topic 3 Acquisition, examination and analysis of evidence in computers and networks Part 4

Learning Outcome

After successfully completing this lecture, you will be able to

- Examine and analyse computer files, web browsing history and event logs
- Perform events and timeline analysis

Road Map

- Events and Time Analysis
- Operating Systems Artifacts Analysis – Windows
  - Case-related data files and metadata
  - User activities/behaviors event logs
  - System configurations and logs
  - Application configurations and usage
  - Web browsing history

Digital Forensics Process

- Collection
  - Collection of media/devices at the scene
  - Identification and Preservation
  - Transportation
  - Data Acquisition and Duplication
- Examination
  - Extraction and searching of data
- Analysis
  - Event and Timeline analysis
- Reporting
  - Reporting and documentation

Event Analysis – Example

- Login/logout events in the auth.log file in an Linux computer

```
9 Jun 17:26:02 ubuntu successfully ssh login
from remote computer 192.168.112.132

9 Jun 18:10:02 ubuntu successfully ssh logout
from remote computer 192.168.112.132
```

Timeline Analysis – Files and Folders

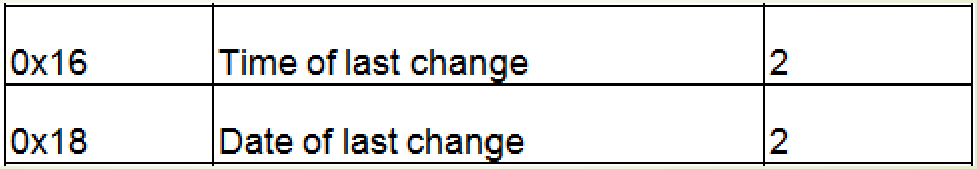
- Analysis of **MAC** times of files/folders
  - **Modified Time**
  - **Accessed Time**
  - **Creation Time/Birth Time**
- How to get these times? From the computer systems?

Timeline Analysis - Standard

- Singapore Standard Time (UTC+8:00:00) is the time reference used in the Singapore courts
- Coordinated Universal Time (UTC) is the primary time standard by which the world regulates clocks and time.
- UTC is one of several closely related successors to Greenwich Mean Time (GMT). For most purposes, UTC is synonymous with GMT, but GMT is no longer precisely defined by the scientific community.

Limitation of Computer System Date/Time

- FAT files system
  - Date range 1980-01-01 to 2099-12-31 in local time
  - **Resolution**
    - **2 seconds for last modified time**
    - **1 day for access date (read access)**
    - **10 ms for creation time**
  - Why? FAT uses only 2 bytes to store time and **2 bytes to store date information** whereas **NTFS uses 8 bytes** for date/time with 100ns resolution



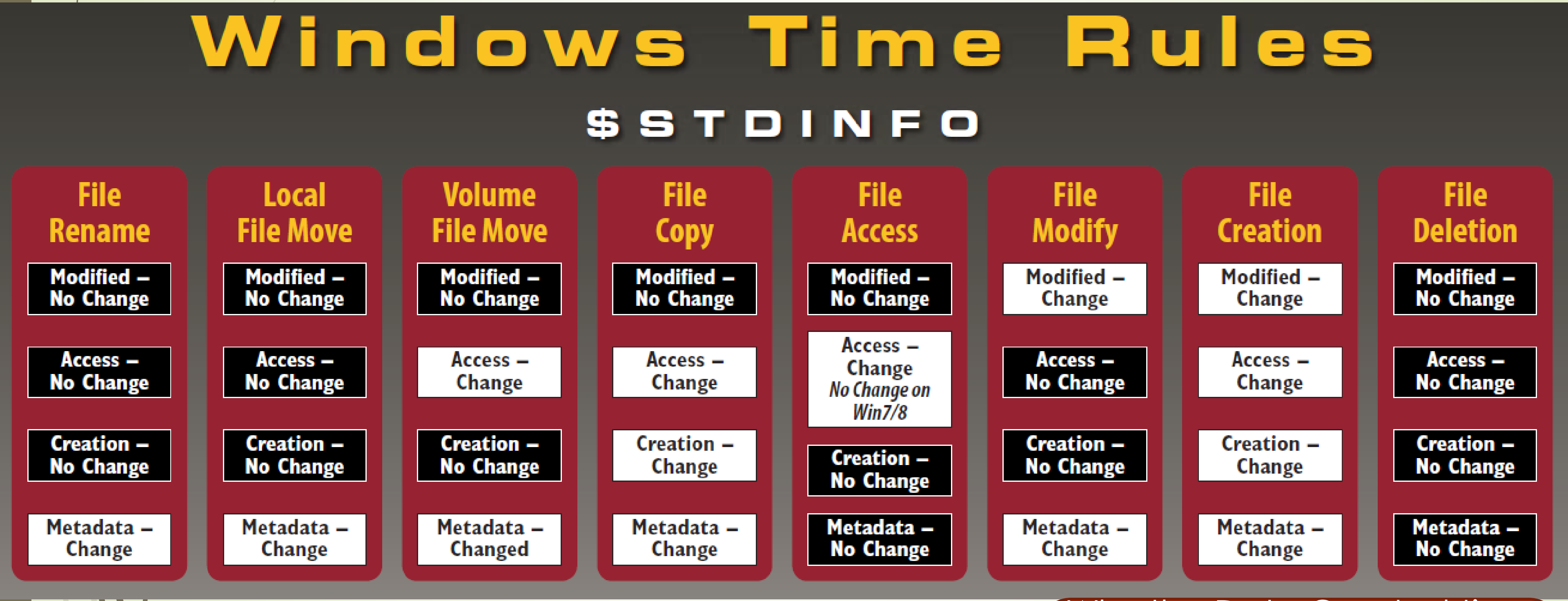
0x16	Time of last change	2
0x18	Date of last change	2

Limitation of Computer System Date/Time

- NTFS
  - Date/time information stored in 64-bits (8 bytes)
  - Date range 1 January 1601 – 28 May 60056, in UTC
  - Resolution – 100ns for modified, accessed and creation times (times are 64-bit numbers counting 100-nanosecond intervals, ten million per second, since 1 January1601)
  - Additional timestamp on MFT modification time for changes in file attributes

10

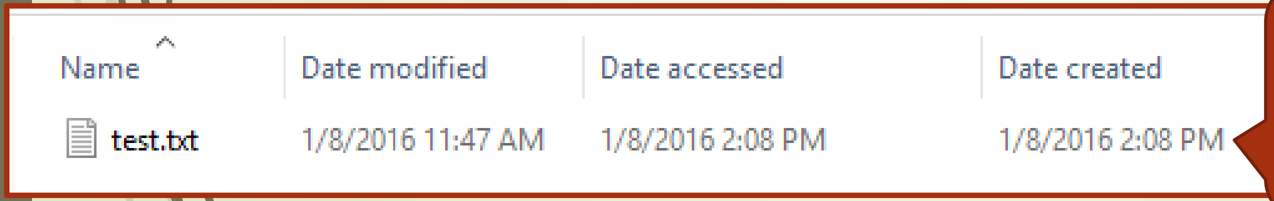
Why some files have a creation date/time later than that the modified date/time?



Windows Time Rules

$STDINFO

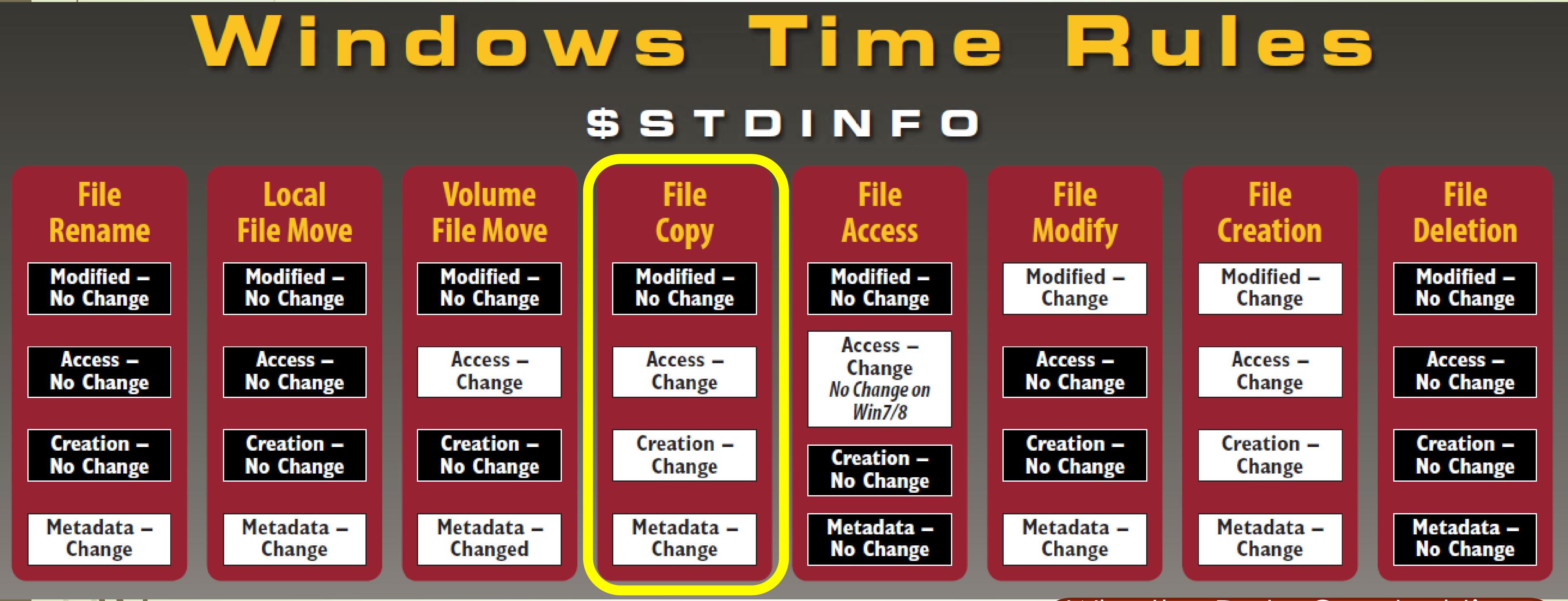
File Rename	Local File Move	Volume File Move	File Copy	File Access	File Modify	File Creation	File Deletion
Modified – No Change	Modified – No Change	Modified – No Change	Modified – No Change	Modified – No Change	Modified – Change	Modified – Change	Modified – No Change
Access – No Change	Access – No Change	Access – Change	Access – Change	Access – Change *No Change on Win7/8*	Access – No Change	Access – Change	Access – No Change
Creation – No Change	Creation – No Change	Creation – No Change	Creation – Change	Creation – No Change	Creation – No Change	Creation – Change	Creation – No Change
Metadata – Change	Metadata – Change	Metadata – Changed	Metadata – Change	Metadata – No Change	Metadata – Change	Metadata – Change	Metadata – No Change



Name	Date modified	Date accessed	Date created
test.txt	1/8/2016 11:47 AM	1/8/2016 2:08 PM	1/8/2016 2:08 PM

Why the Date Created time is later that the Date modified time? What happened to this file "test.txt"?

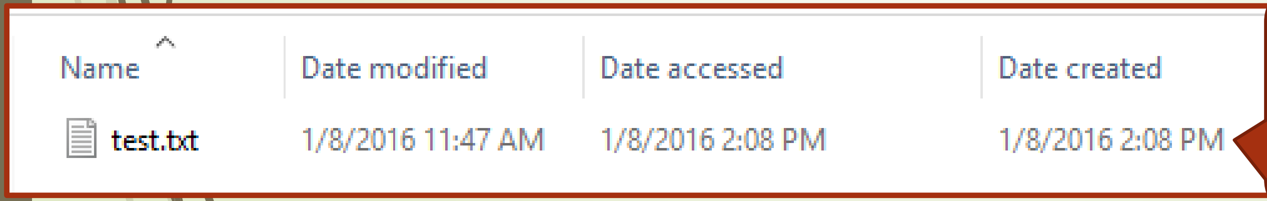
Why some files have a creation date/time later than that the modified date/time?



Windows Time Rules

$STDINFO

File Rename	Local File Move	Volume File Move	File Copy	File Access	File Modify	File Creation	File Deletion
Modified – No Change	Modified – No Change	Modified – No Change	Modified – No Change	Modified – No Change	Modified – Change	Modified – Change	Modified – No Change
Access – No Change	Access – No Change	Access – Change	Access – Change	Access – Change *No Change on Win7/8*	Access – No Change	Access – Change	Access – No Change
Creation – No Change	Creation – No Change	Creation – No Change	Creation – Change	Creation – No Change	Creation – No Change	Creation – Change	Creation – No Change
Metadata – Change	Metadata – Change	Metadata – Changed	Metadata – Change	Metadata – No Change	Metadata – Change	Metadata – Change	Metadata – No Change



Name	Date modified	Date accessed	Date created
test.txt	1/8/2016 11:47 AM	1/8/2016 2:08 PM	1/8/2016 2:08 PM

Why the Date Created time is later that the Date modified time? What happened to this file “test.txt”?

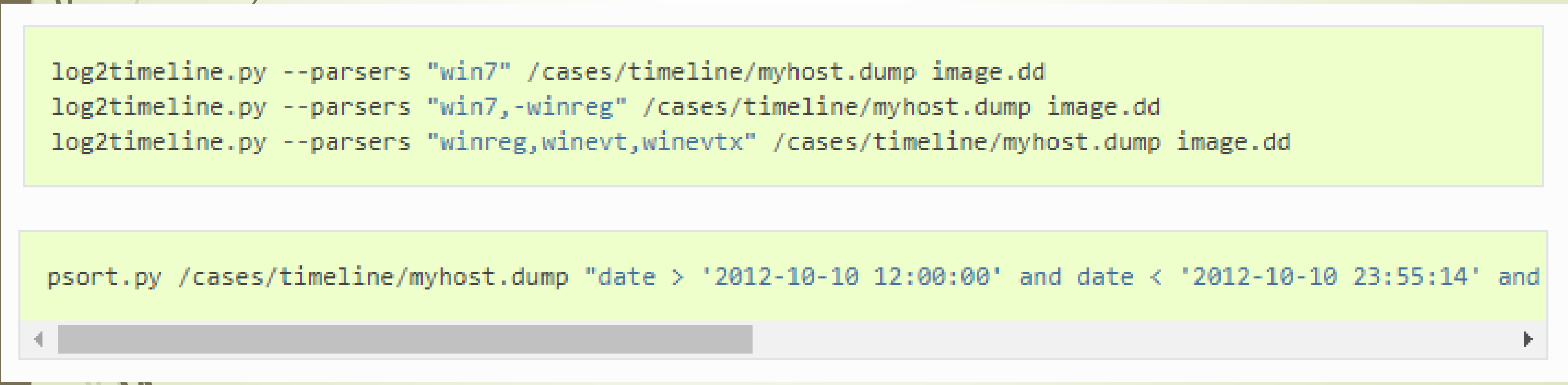
Timeline Analysis - Steps

1. Synchronize your watch to Singapore Standard time
2. Record the differences of the time between the Singapore Standard Time and the system time of the computers under investigation
3. Create image files of the memory and hard disk drives of the computers under investigation
4. Import the image files to a forensic tool
5. Sort files by MAC time
6. Recover the activities in the system during the incident from event logs
7. Re-construct the sequence of events occurred from the activities and MAC times of the files of interest

Log2timeline

a tool designed to extract timestamps from various files found on a typical computer system(s) and aggregate them. ... writing one-off scripts to automate repetitive tasks in computer forensic analysis or equivalent.

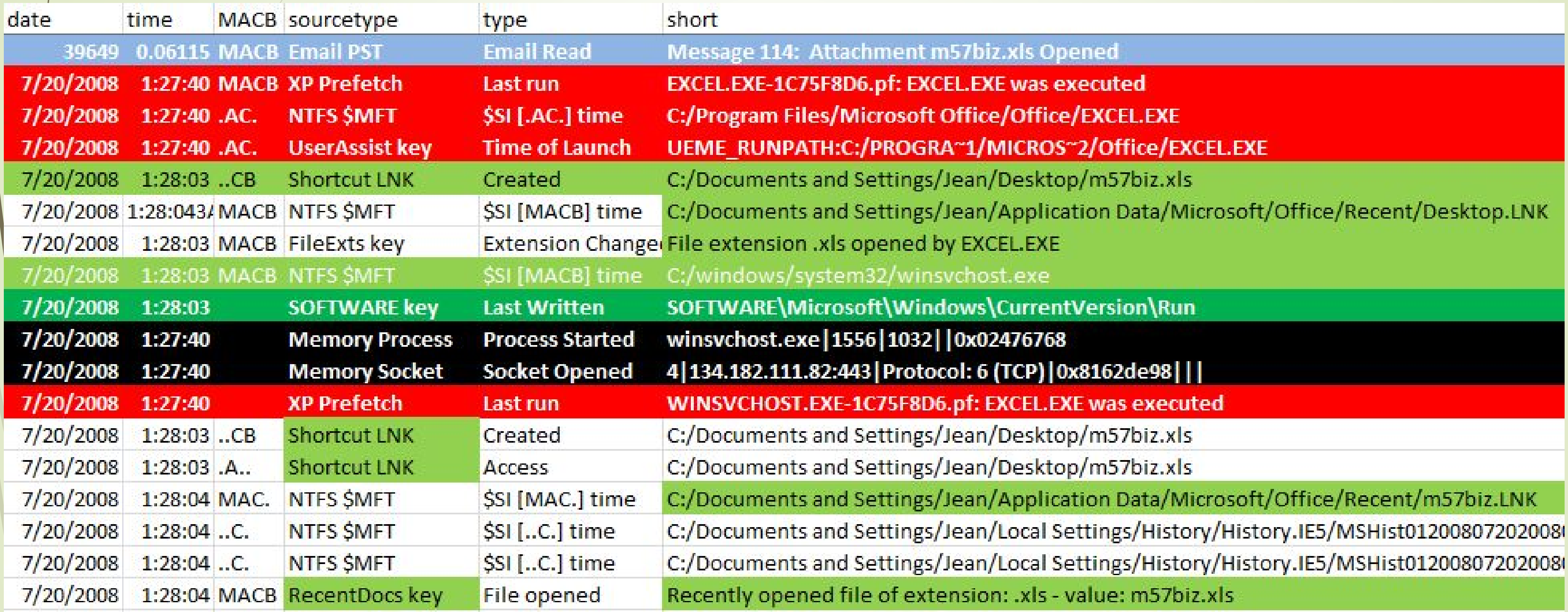
Record the differences of the time between the Singapore Standard Time and the system time of the computers under investigation



```
log2timeline.py --parsers "win7" /cases/timeline/myhost.dump image.dd
log2timeline.py --parsers "win7,-winreg" /cases/timeline/myhost.dump image.dd
log2timeline.py --parsers "winreg,winevt,winevtx" /cases/timeline/myhost.dump image.dd
```

```
psort.py /cases/timeline/myhost.dump "date > '2012-10-10 12:00:00' and date < '2012-10-10 23:55:14' and
```

Event Timeline from Log2timeline



date	time	MACB	sourcetype	type	short
39649	0.06115	MACB	Email PST	Email Read	Message 114: Attachment m57biz.xls Opened
7/20/2008	1:27:40	MACB	XP Prefetch	Last run	EXCEL.EXE-1C75F8D6.pf: EXCEL.EXE was executed
7/20/2008	1:27:40	.AC.	NTFS $MFT	$SI [.AC.] time	C:/Program Files/Microsoft Office/Office/EXCEL.EXE
7/20/2008	1:27:40	.AC.	UserAssist key	Time of Launch	UEME_RUNPATH:C:/PROGRA~1/MICROS~2/Office/EXCEL.EXE
7/20/2008	1:28:03	..CB	Shortcut LNK	Created	C:/Documents and Settings/Jean/Desktop/m57biz.xls
7/20/2008	1:28:043/	MACB	NTFS $MFT	$SI [MACB] time	C:/Documents and Settings/Jean/Application Data/Microsoft/Office/Recent/Desktop.LNK
7/20/2008	1:28:03	MACB	FileExts key	Extension Change	File extension .xls opened by EXCEL.EXE
7/20/2008	1:28:03	MACB	NTFS $MFT	$SI [MACB] time	C:/windows/system32/winsvchost.exe
7/20/2008	1:28:03		SOFTWARE key	Last Written	SOFTWARE\Microsoft\Windows\CurrentVersion\Run
7/20/2008	1:27:40		Memory Process	Process Started	winsvchost.exe|1556|1032||0x02476768
7/20/2008	1:27:40		Memory Socket	Socket Opened	4|134.182.111.82:443|Protocol: 6 (TCP)|0x8162de98||
7/20/2008	1:27:40		XP Prefetch	Last run	WINSVCHOST.EXE-1C75F8D6.pf: EXCEL.EXE was executed
7/20/2008	1:28:03	..CB	Shortcut LNK	Created	C:/Documents and Settings/Jean/Desktop/m57biz.xls
7/20/2008	1:28:03	.A..	Shortcut LNK	Access	C:/Documents and Settings/Jean/Desktop/m57biz.xls
7/20/2008	1:28:04	MAC.	NTFS $MFT	$SI [MAC.] time	C:/Documents and Settings/Jean/Application Data/Microsoft/Office/Recent/m57biz.LNK
7/20/2008	1:28:04	..C.	NTFS $MFT	$SI [..C.] time	C:/Documents and Settings/Jean/Local Settings/History/History.IE5/MSHist01200807202008
7/20/2008	1:28:04	..C.	NTFS $MFT	$SI [..C.] time	C:/Documents and Settings/Jean/Local Settings/History/History.IE5/MSHist01200807202008
7/20/2008	1:28:04	MACB	RecentDocs key	File opened	Recently opened file of extension: .xls - value: m57biz.xls

Source: http://computer-forensics.sans.org/blog/2012/01/25/digital-forensic-sifting-colorized-super-timeline-template-for-log2timeline-output-files

Operating Systems Artifacts Analysis

- Evidence found at an operating system
  - Case-related data files
    - Timestamps, status, location
  - User activities/behaviors
    - Login/logout events, personal profile
  - System configurations and logs
  - Application configurations and usage
  - OS-specific artifacts

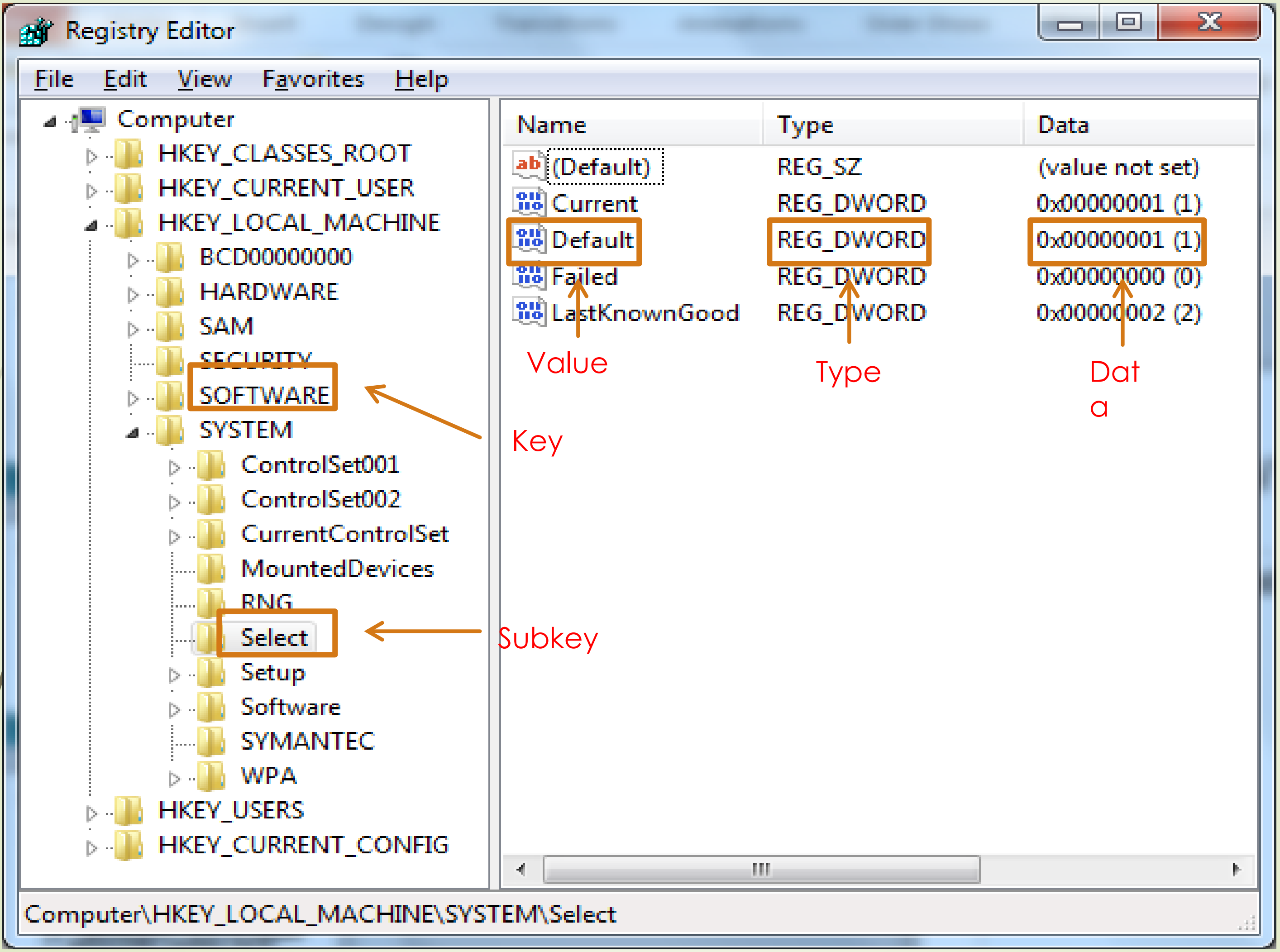
Windows Artifacts

- Windows
  - Registry (NTUSER, SAM, SOFTWARE, HARDWARE, SECURITY)
  - Event Logs (Application, System, Security, Custom…)
  - User profile folders (Recently accessed files, downloads…)
  - Jump list (Recently/frequently used files by the applications)
  - Prefetch (Executed programmes)
  - Recycle bin (Deleted files)
  - Thumbnails (Images)
  - Office document metadata
  - Browser (Internet activities: history, cache, cookies, downloads, bookmarks…)

Windows Registry

- A binary and hierarchal database for
  - User information (currently logged on)
  - System information (currently detected)
- Stored in registry files
  - Application information
  - Specific user preferences
  - System hardware settings
- Replaced the INI files of Windows 3.1
- Registry can be viewed and edited using Registry Editor (regedit.exe) or many 3rd-party tools, e.g. RegRipper

Windows Registry



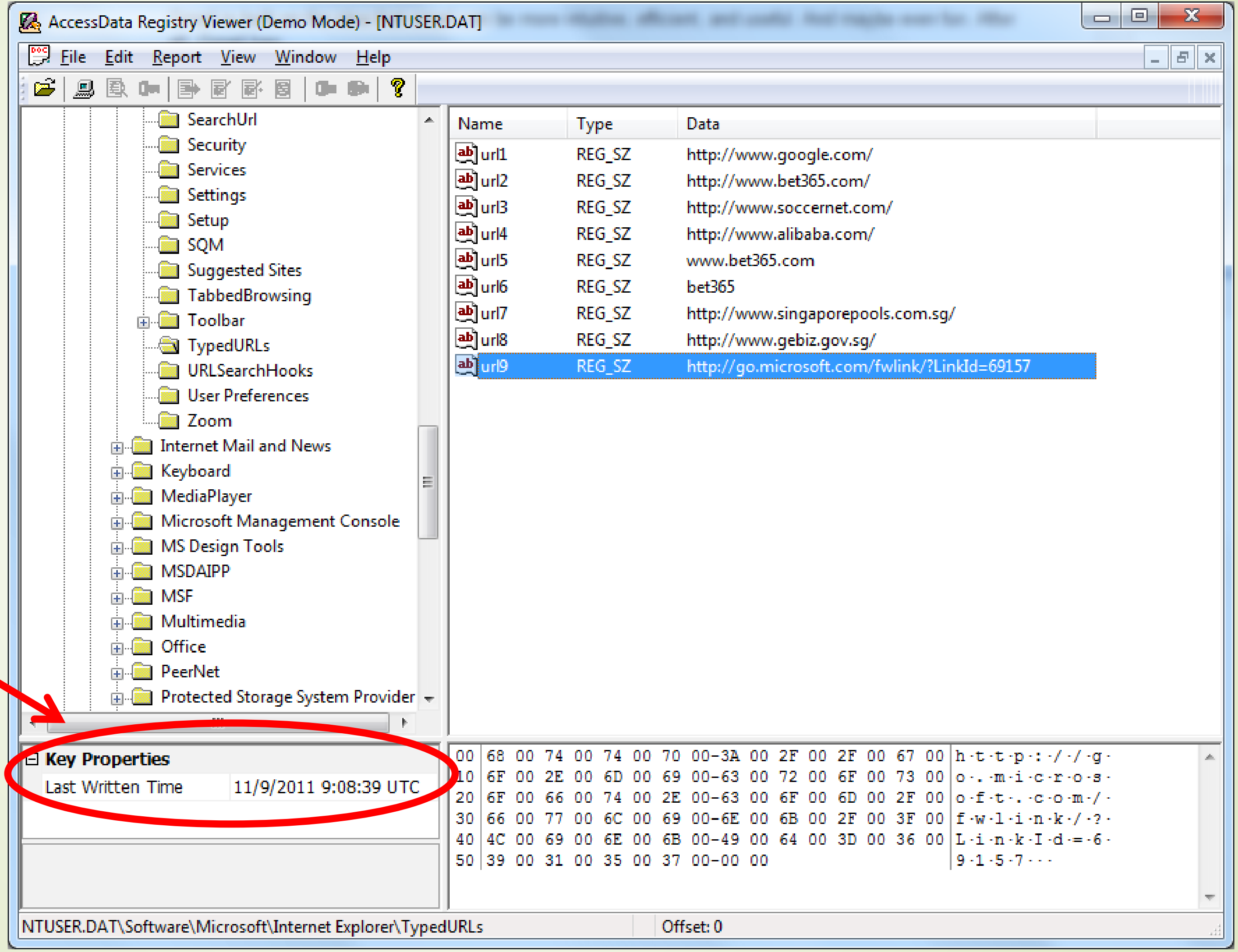
Name	Type	Data
(Default)	REG_SZ	(value not set)
Current	REG_DWORD	0x00000001 (1)
Default	REG_DWORD	0x00000001 (1)
Failed	REG_DWORD	0x00000000 (0)
LastKnownGood	REG_DWORD	0x00000002 (2)

Computer\HKEY_LOCAL_MACHINE\SYSTEM\Select

Windows Registry

Registry hive opened using Windows Registry viewer

- Each key has a "Last Written Time"
- It's update when a value is added or updated in the key



Name	Type	Data
url1	REG_SZ	http://www.google.com/
url2	REG_SZ	http://www.bet365.com/
url3	REG_SZ	http://www.soccernet.com/
url4	REG_SZ	http://www.alibaba.com/
url5	REG_SZ	www.bet365.com
url6	REG_SZ	bet365
url7	REG_SZ	http://www.singaporepools.com.sg/
url8	REG_SZ	http://www.gebiz.gov.sg/
url9	REG_SZ	http://go.microsoft.com/fwlink/?LinkId=69157

Key Properties

Last Written Time	11/9/2011 9:08:39 UTC

```
00  68 00 74 00 74 00 70 00-3A 00 2F 00 2F 00 67 00  h·t·t·p·:·/·/·g·
10  6F 00 2E 00 6D 00 69 00-63 00 72 00 6F 00 73 00  o·.·m·i·c·r·o·s·
20  6F 00 66 00 74 00 2E 00-63 00 6F 00 6D 00 2F 00  o·f·t·.·c·o·m·/·
30  66 00 77 00 6C 00 69 00-6E 00 6B 00 2F 00 3F 00  f·w·l·i·n·k·/·?·
40  4C 00 69 00 6E 00 6B 00-49 00 64 00 3D 00 36 00  L·i·n·k·I·d·=·6·
50  39 00 31 00 35 00 37 00-00 00                    9·1·5·7···
```

NTUSER.DAT\Software\Microsoft\Internet Explorer\TypedURLs   Offset: 0

20

Windows Registry

- Different names in different Windows systems
  - Windows 3.11
    - In C:\WINDOWS directory, reg.dat and system.dat
    - C:\windows\profiles\<username>\user.dat
  - Windows 95, 98 and Me
    - In %WINDIR%, SYSTEM.DAT and USER.DAT
  - Windows NT onwards
    - %SYSTEM_ROOT%\System32\Config\
    - %USER_HOME%\ntuser.dat e.g. C:\users\student\ntuser.dat

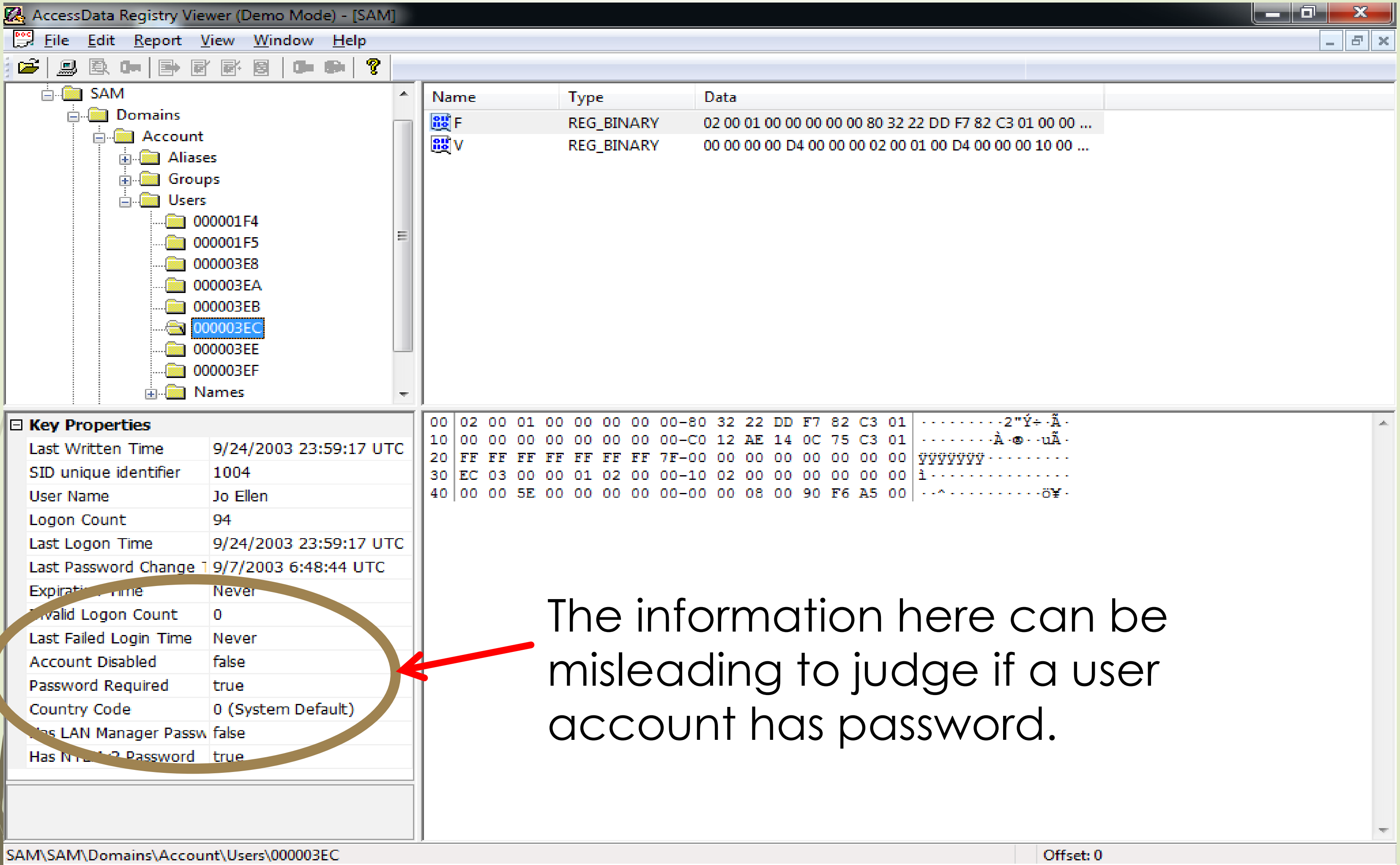
For System Information

- The four registry files are kept in Windows\System32\Config folder
  - SAM
  - SYSTEM
  - SECURITY
  - SOFTWARE
- RegIdleBackup scheduled task runs every 10 days to back up these registry hives at %WinDir%\System32\Config\RegBack.
  - But it does not back up the user hives
  - May be useful in the case data are cleared in the current hives

SAM

- Registry Hive HKEY_LOCAL_MACHINE\SAM
- The SAM Hive stores account information for users and groups on the system
  - Usernames
  - Security Identifier (SID)
  - User Login Information
  - Group Infromation

SAM



Name	Type	Data
F	REG_BINARY	02 00 01 00 00 00 00 00 80 32 22 DD F7 82 C3 01 00 00 ...
V	REG_BINARY	00 00 00 00 D4 00 00 00 02 00 01 00 D4 00 00 00 10 00 ...

Key Properties

Last Written Time	9/24/2003 23:59:17 UTC
SID unique identifier	1004
User Name	Jo Ellen
Logon Count	94
Last Logon Time	9/24/2003 23:59:17 UTC
Last Password Change T	9/7/2003 6:48:44 UTC
Expiration Time	Never
Invalid Logon Count	0
Last Failed Login Time	Never
Account Disabled	false
Password Required	true
Country Code	0 (System Default)
Has LAN Manager Passw	false
Has NTLMv2 Password	true

```
00 02 00 01 00 00 00 00 00-80 32 22 DD F7 82 C3 01 ·········2"Ý÷·Ã·
10 00 00 00 00 00 00 00 00-C0 12 AE 14 0C 75 C3 01 ········À·®··uÃ·
20 FF FF FF FF FF FF FF 7F-00 00 00 00 00 00 00 00 ÿÿÿÿÿÿÿ·········
30 EC 03 00 00 01 02 00 00-10 02 00 00 00 00 00 00 ì···············
40 00 00 5E 00 00 00 00 00-00 00 08 00 90 F6 A5 00 ··^·········ö¥·
```

SAM\SAM\Domains\Account\Users\000003EC

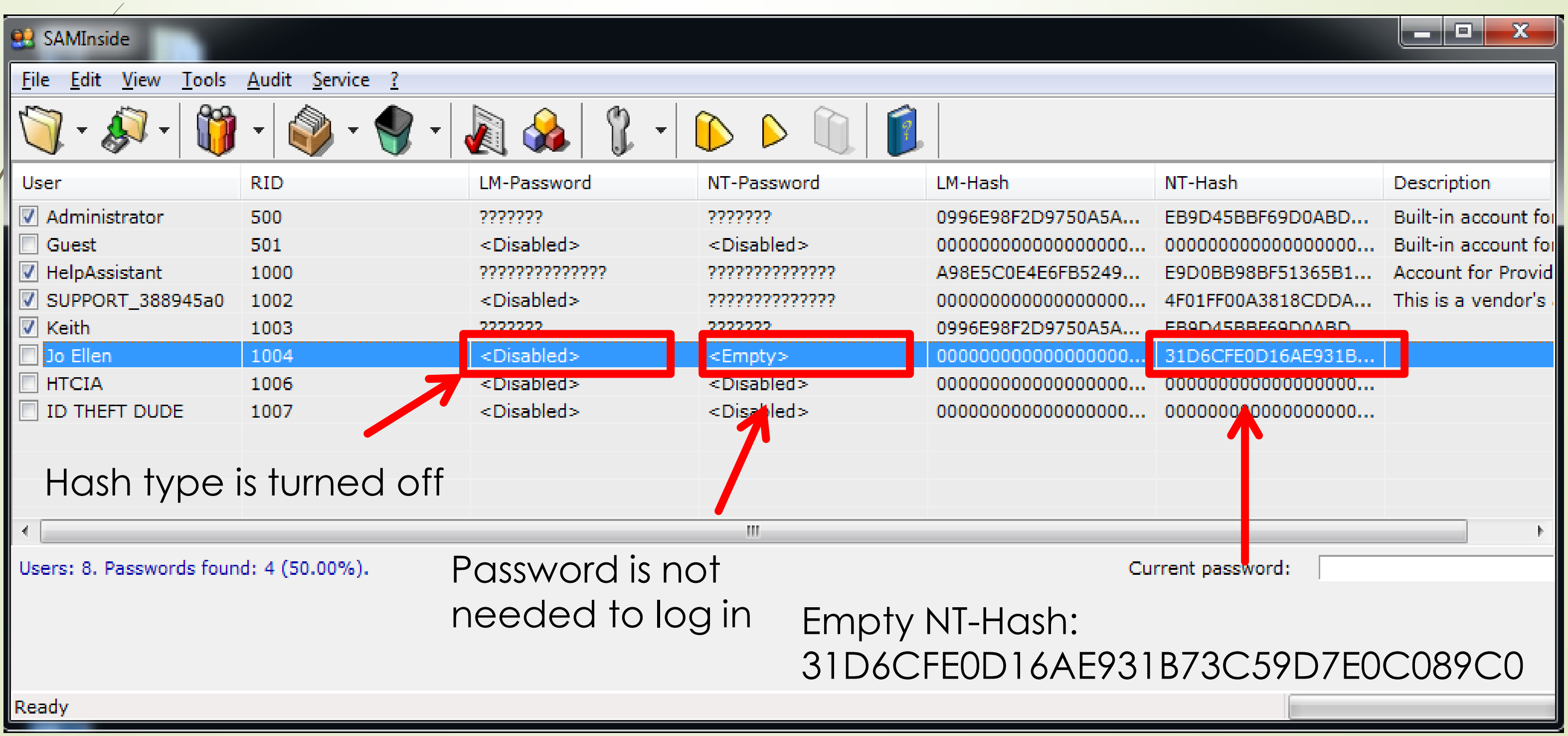
Offset: 0

The information here can be misleading to judge if a user account has password.

24

SAM

- The only way to be sure is to grab the actual hashed password.
  - Tool: SAMInside



User	RID	LM-Password	NT-Password	LM-Hash	NT-Hash	Description
☑ Administrator	500	???????	???????	0996E98F2D9750A5A...	EB9D45BBF69D0ABD...	Built-in account fo
□ Guest	501	<Disabled>	<Disabled>	000000000000000000...	000000000000000000...	Built-in account fo
☑ HelpAssistant	1000	??????????????	??????????????	A98E5C0E4E6FB5249...	E9D0BB98BF51365B1...	Account for Provid
☑ SUPPORT_388945a0	1002	<Disabled>	??????????????	000000000000000000...	4F01FF00A3818CDDA...	This is a vendor's
☑ Keith	1003	???????	???????	0996E98F2D9750A5A...	EB9D45BBF69D0ABD...	
□ Jo Ellen	1004	<Disabled>	<Empty>	000000000000000000...	31D6CFE0D16AE931B...	
□ HTCIA	1006	<Disabled>	<Disabled>	000000000000000000...	000000000000000000...	
□ ID THEFT DUDE	1007	<Disabled>	<Disabled>	000000000000000000...	000000000000000000...	

Hash type is turned off

Users: 8. Passwords found: 4 (50.00%).

Password is not needed to log in

Current password:

Empty NT-Hash: 31D6CFE0D16AE931B73C59D7E0C089C0

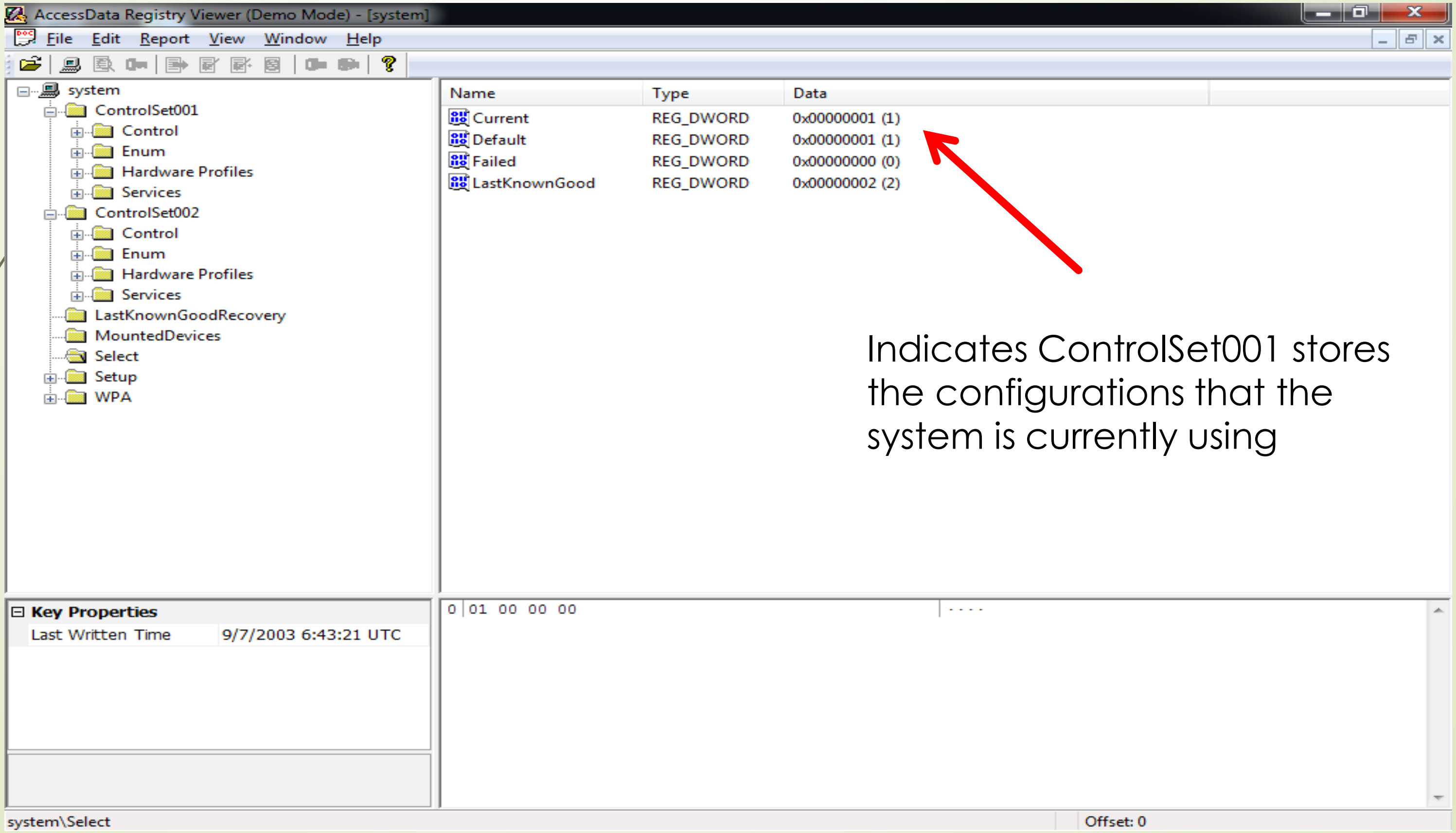
Ready

SYSTEM

- Registry Hive HKEY_LOCAL_MACHINE\SYSTEM
- The SYSTEM Hive contains Windows system settings such as
  - The system name
    - SYSTEM\CurrentControlSet\Control\ComputerName\ComputerName
  - Time zone information
    - SYSTEM\CurrentControlSet\Control\TimeZoneInformation
    - Critical in event correlation: UTC vs local time
  - Last access time on/off
    - SYSTEM\CurrentControlSet\Control\FileSystem
      - NtfsDisableLastAccessUpdate
    - Controls if Windows will update the last access time of files. Turn off at Windows Vista and onwards, probably due to performance concern.
  - Network interface
    - SYSTEM\CurrentControlSet\Service\Tcpip\Parameters\Interfaces
    - Rich network-based information
  - Device drivers information and many more

SYSTEM

- Which control set to use?



Name	Type	Data
Current	REG_DWORD	0x00000001 (1)
Default	REG_DWORD	0x00000001 (1)
Failed	REG_DWORD	0x00000000 (0)
LastKnownGood	REG_DWORD	0x00000002 (2)

Key Properties

Last Written Time	9/7/2003 6:43:21 UTC

```
0 | 01 00 00 00          ....
```

system\Select

Offset: 0

Indicates ControlSet001 stores the configurations that the system is currently using

SYSTEM

- Identifying the current control set
  - ControlSet001 is typically the control set that the computer just loaded to use. It's usually the most up-to-date version of the control set.
  - ControlSet002 is the "Last Known Good" version, which is considered good when the previous boot occurred.
  - More control sets imply that the system crashes often and it may be due to existence of malwares.

28

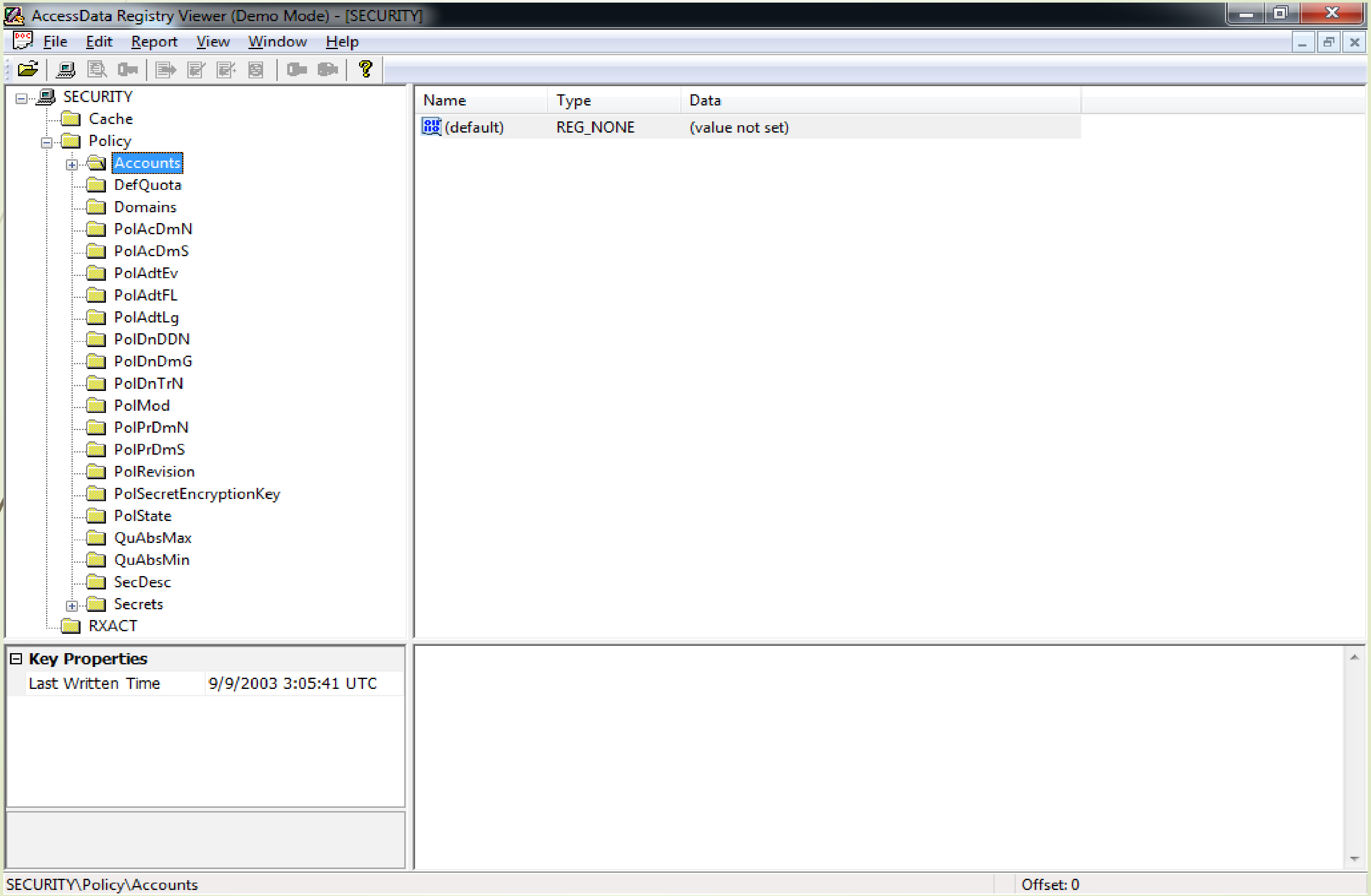
SOFTWARE

- Registry Hive HKEY_LOCAL_MACHINE\SOFTWARE
- The SOFTWARE Hive contains
  - OS information
    - SOFTWARE\Microsoft\Windows NT\CurrentVersionn
  - Current Version Settings
    - Evidence of the present of blaster worm is an entry “windows auto update"="msblast.exe“ in the registry key: SOFTWARE\Microsoft\Windows\CurrentVersion\Run so that the worm runs when you start Windows
  - All installed programs
    - Settings of each program
    - Paths to application files and directories
    - Software licensing
    - Expiration information

SECURITY

- Registry Hive HKEY_LOCAL_MACHINE\SECURITY
- The SECURITY Hive contains the following security settings
  - User and group policies
    - Examples of policies include whether a particular user is allowed to
      - reboot the computer,
      - load device drivers,
      - backup files,
      - access the system remotely.

SECURITY



AccessData Registry Viewer (Demo Mode) - [SECURITY]
File Edit Report View Window Help

SECURITY
- Cache
- Policy
  - Accounts
  - DefQuota
  - Domains
  - PolAcDmN
  - PolAcDmS
  - PolAdtEv
  - PolAdtFL
  - PolAdtLg
  - PolDnDDN
  - PolDnDmG
  - PolDnTrN
  - PolMod
  - PolPrDmN
  - PolPrDmS
  - PolRevision
  - PolSecretEncryptionKey
  - PolState
  - QuAbsMax
  - QuAbsMin
  - SecDesc
  - Secrets
- RXACT

Name	Type	Data
(default)	REG_NONE	(value not set)

Key Properties

Last Written Time	9/9/2003 3:05:41 UTC

SECURITY\Policy\Accounts

Offset: 0

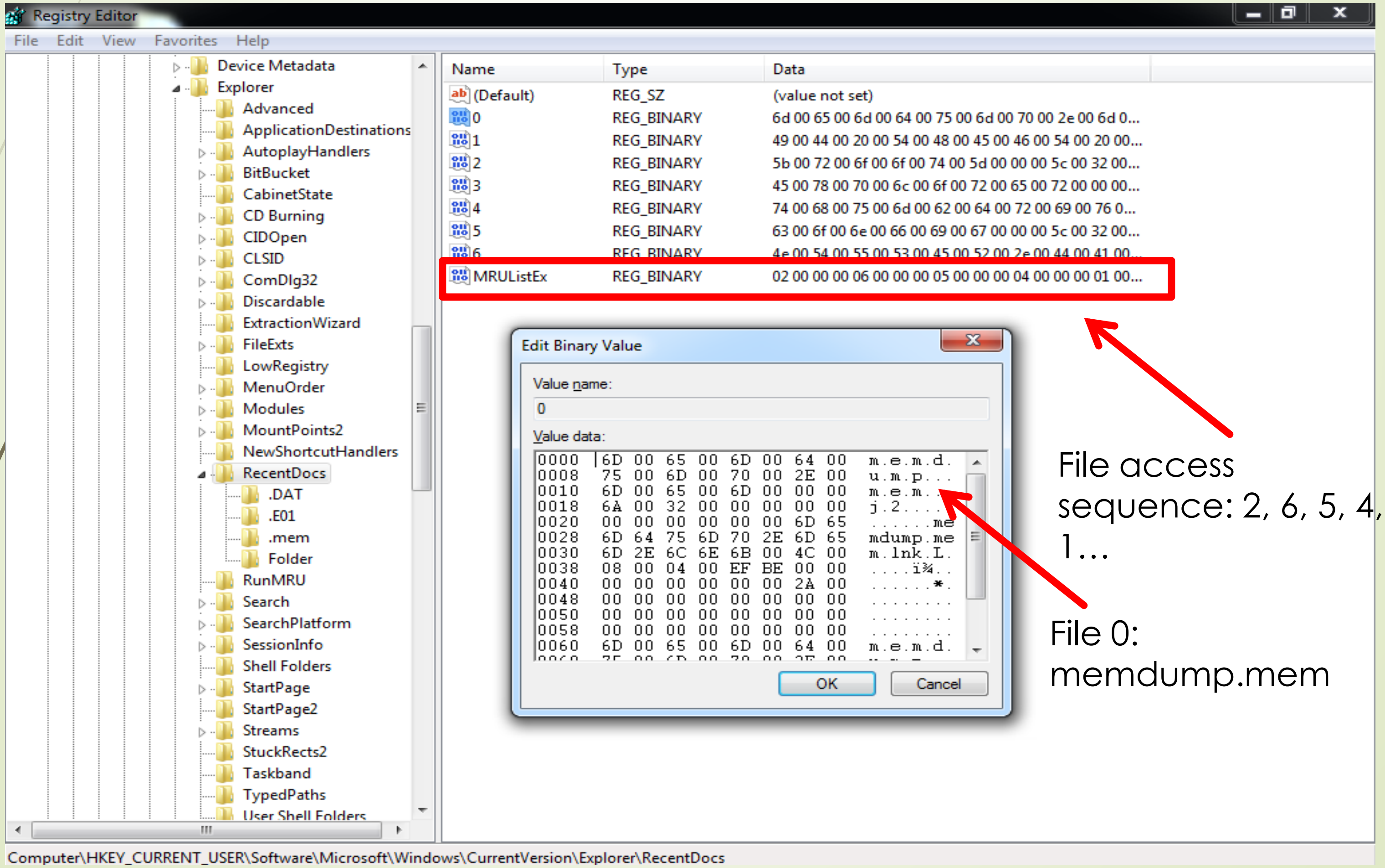
For User Information

- NTUSER.DAT
  - Data are populated to HKEY_CURRENT_USER
  - Additional hive UsrClass.dat to aid in virtualised registry root for User Account Control (UAC)
    - At %UserProfile%\AppData\Local\Microsoft\Windows\
    - Plugged into NTUSER.DAT/Software/Classes when displayed at Registry Editor

NTUSER.DAT

- File opening or creation
  - NTUSER.DAT\Software\Microsoft\Windows\CurrentVersion\Explorer\RecentDocs
  - MRUList tells the order the file access
    - 1st in the list: file opened/created most recently
    - Last in the list: file that was opened/created the furthest back in time

NTUSER.DAT



Name	Type	Data
(Default)	REG_SZ	(value not set)
0	REG_BINARY	6d 00 65 00 6d 00 64 00 75 00 6d 00 70 00 2e 00 6d 0...
1	REG_BINARY	49 00 44 00 20 00 54 00 48 00 45 00 46 00 54 00 20 00...
2	REG_BINARY	5b 00 72 00 6f 00 6f 00 74 00 5d 00 00 00 5c 00 32 00...
3	REG_BINARY	45 00 78 00 70 00 6c 00 6f 00 72 00 65 00 72 00 00 00...
4	REG_BINARY	74 00 68 00 75 00 6d 00 62 00 64 00 72 00 69 00 76 0...
5	REG_BINARY	63 00 6f 00 6e 00 66 00 69 00 67 00 00 00 5c 00 32 00...
6	REG_BINARY	4e 00 54 00 55 00 53 00 45 00 52 00 2e 00 44 00 41 00...
MRUListEx	REG_BINARY	02 00 00 00 06 00 00 00 05 00 00 00 04 00 00 00 01 00...

Edit Binary Value

Value name:

0

Value data:

```
0000  6D 00 65 00 6D 00 64 00   m.e.m.d.
0008  75 00 6D 00 70 00 2E 00   u.m.p...
0010  6D 00 65 00 6D 00 00 00   m.e.m...
0018  6A 00 32 00 00 00 00 00   j.2.....
0020  00 00 00 00 00 00 6D 65   ......me
0028  6D 64 75 6D 70 2E 6D 65   mdump.me
0030  6D 2E 6C 6E 6B 00 4C 00   m.lnk.L.
0038  08 00 04 00 EF BE 00 00   ....ï¾..
0040  00 00 00 00 00 00 2A 00   ......*.
0048  00 00 00 00 00 00 00 00   ........
0050  00 00 00 00 00 00 00 00   ........
0058  00 00 00 00 00 00 00 00   ........
0060  6D 00 65 00 6D 00 64 00   m.e.m.d.
```

Computer\HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Explorer\RecentDocs

File access sequence: 2, 6, 5, 4, 1…

File 0: memdump.mem

NTUSER.DAT

- Programme Execution
  - NTUSER.DAT\Software\Microsoft\Windows\CurrentVersion\Explorer\RunMRU
  - GUI applications executed from Start -> Run
  - Does NOT record commands ran at command line, e.g. dir
- Internet Surfing History
  - NTUSER.DAT\Software\Microsoft\Internet Explorer\TypedURL
  - The contents typed at IE address bar

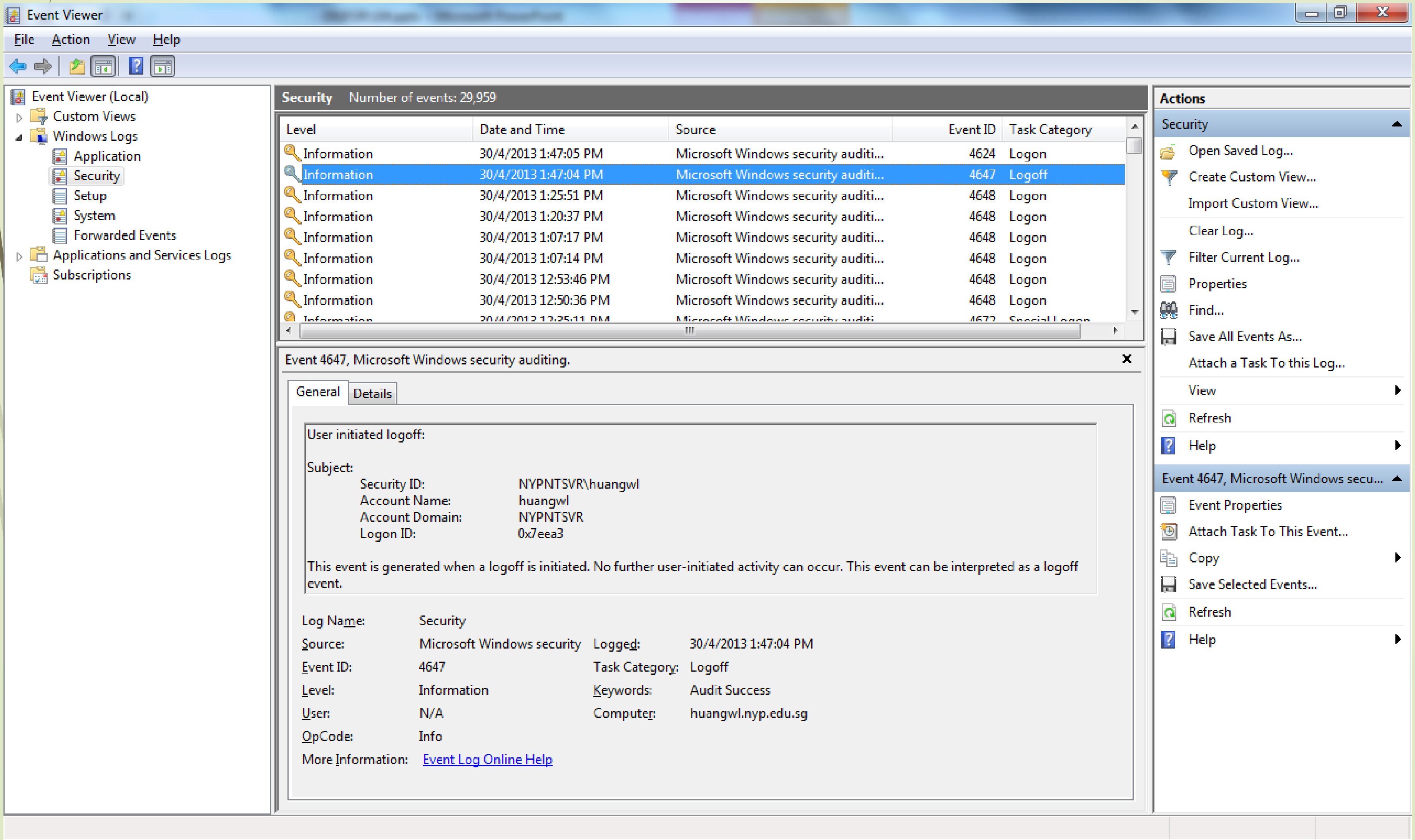
Event Logs

- Types of event logs
  - Application
    - Software events unrelated to Operating System
    - Logged by application or programs
    - e.g. SQL Server fails to access a database
  - Security
    - Access control and security setting information based on audit and group policy
    - Security events like logon attempts as well as folder access
  - System
    - Events related to Windows services, system components, drivers, resources etc
    - Logged by Windows system components, e.g. loading a driver, system rebooted
  - Custom
    - Custom application logs
    - e.g. DNS server logs record DNS queries, responses and other DNS activities

Event Logs

- Where to find the event log file?
  - Windowx NT/2000/XP/Server 2003
    - %SYSTEM ROOT%\System32\config
    - SecEvent.evt, AppEvent.evt, SysEvent.evt
  - Windows Vista/7/8/Server 2008
    - %SYSTEM ROOT%\System32\winevt\logs
    - Security.evtx, Application.evtx, System.evtx, etc
  - These default locations can be changed at Windows Registry
  - Event IDs changed at Windows Vista and later
    - Old Event ID + 4096 = New Event ID, should work for most cases

Event Logs



Security Number of events: 29,959

Level	Date and Time	Source	Event ID	Task Category
Information	30/4/2013 1:47:05 PM	Microsoft Windows security auditi...	4624	Logon
Information	30/4/2013 1:47:04 PM	Microsoft Windows security auditi...	4647	Logoff
Information	30/4/2013 1:25:51 PM	Microsoft Windows security auditi...	4648	Logon
Information	30/4/2013 1:20:37 PM	Microsoft Windows security auditi...	4648	Logon
Information	30/4/2013 1:07:17 PM	Microsoft Windows security auditi...	4648	Logon
Information	30/4/2013 1:07:14 PM	Microsoft Windows security auditi...	4648	Logon
Information	30/4/2013 12:53:46 PM	Microsoft Windows security auditi...	4648	Logon
Information	30/4/2013 12:50:36 PM	Microsoft Windows security auditi...	4648	Logon
Information	30/4/2013 12:35:11 PM	Microsoft Windows security auditi...	4672	Special Logon

Event 4647, Microsoft Windows security auditing.

General | Details

User initiated logoff:

Subject:

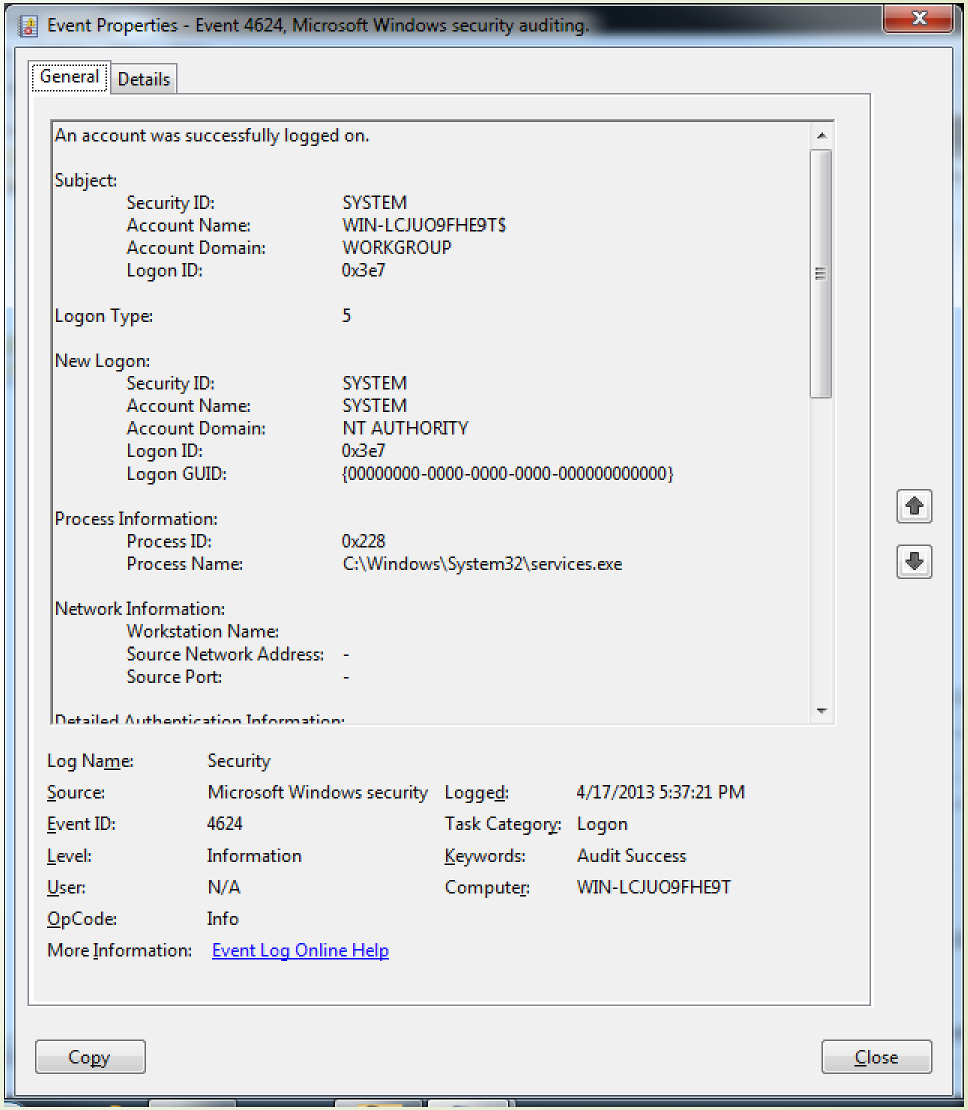
```
	Security ID:		NYPNTSVR\huangwl
	Account Name:		huangwl
	Account Domain:		NYPNTSVR
	Logon ID:		0x7eea3
```

This event is generated when a logoff is initiated. No further user-initiated activity can occur. This event can be interpreted as a logoff event.

Log Name:	Security		
Source:	Microsoft Windows security	Logged:	30/4/2013 1:47:04 PM
Event ID:	4647	Task Category:	Logoff
Level:	Information	Keywords:	Audit Success
User:	N/A	Computer:	huangwl.nyp.edu.sg
OpCode:	Info		
More Information:	Event Log Online Help		

Event Logs

- Event Viewer


Event Properties - Event 4624, Microsoft Windows security auditing.
General
Details
Copy
Close

```
An account was successfully logged on.

Subject:
        Security ID:            SYSTEM
        Account Name:           WIN-LCJUO9FHE9T$
        Account Domain:         WORKGROUP
        Logon ID:               0x3e7

Logon Type:                     5

New Logon:
        Security ID:            SYSTEM
        Account Name:           SYSTEM
        Account Domain:         NT AUTHORITY
        Logon ID:               0x3e7
        Logon GUID:             {00000000-0000-0000-0000-000000000000}

Process Information:
        Process ID:             0x228
        Process Name:           C:\Windows\System32\services.exe

Network Information:
        Workstation Name:
        Source Network Address: -
        Source Port:            -

Detailed Authentication Information:
```

```
Log Name:         Security
Source:           Microsoft Windows security   Logged:          4/17/2013 5:37:21 PM
Event ID:         4624                         Task Category:   Logon
Level:            Information                  Keywords:        Audit Success
User:             N/A                          Computer:        WIN-LCJUO9FHE9T
OpCode:           Info
More Information: Event Log Online Help
```

Event Codes

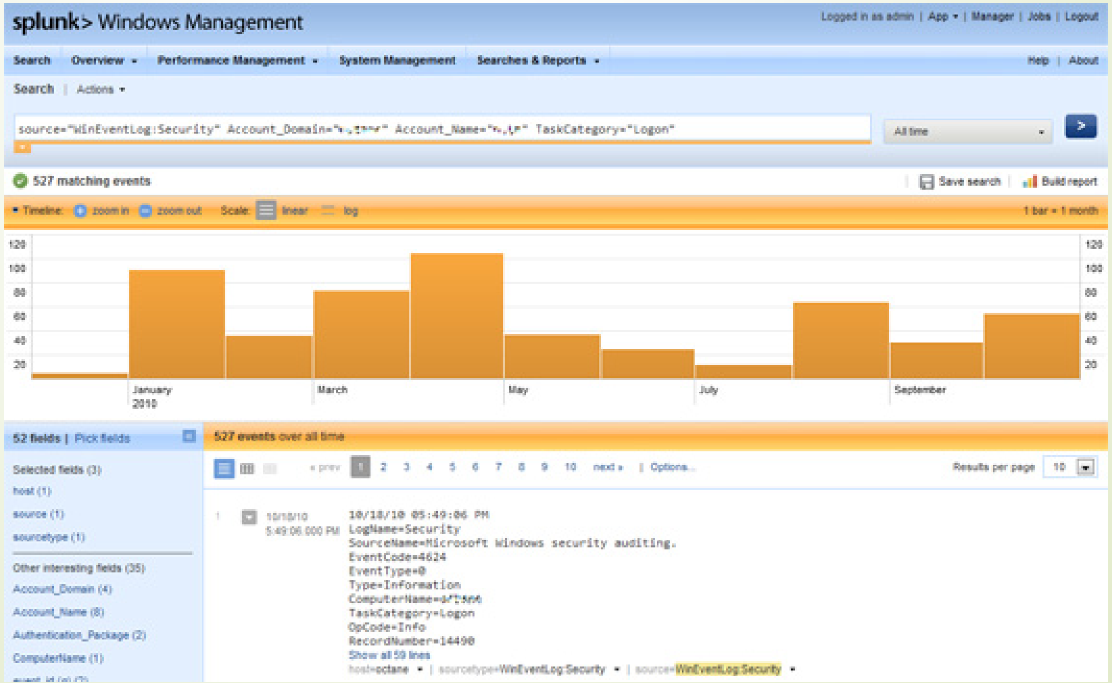
- Forensic Usage
  - **Track account usage**
    - **Successful Logon: 528/4624, 540/4636**
    - **Failed Logon: 529/4625**
    - **Successful Logoff: 4634**
  - Analyze file and folder access
    - Object accessed: 560/4656
    - Object deleted: 564/4660
    - Permission exercised on object (read, write…): 567/4663
  - Malware execution
    - New process created: 592/4688
  - Suspicious services
    - Service crashed unexpectedly: 7034
    - Service sent a start/stop control: 7035
    - Service started or stopped: 7036
    - Start type c hanged: 7040

Event Codes

- Forensic Usage (cont)
  - Application installation
    - Installation completed: 1033
    - Application removal completed: 1034
    - Installation completed successfully: 11707
    - Installation operation failed: 11708
    - Application removal completed successfully: 11724
  - Event log clearing
    - Event ID 517
  - Unauthorised hardware devices (Vista and later)
    - Plug and play driver install attempted: 20001
  - Geolocation information (Vista and later)
    - Wireless network association started: 11000
    - Successful connection to wireless network: 8001
    - Failed connection to wireless network: 8002

Machine Log Analysis Tool

- Splunk
  - It supports the monitoring of Windows event log channels. It can monitor event log channels and files stored on the local machine, as well as collect logs from remote machines.



splunk> Windows Management
Logged in as admin | App ▾ | Manager | Jobs | Logout
Search | Overview ▾ | Performance Management ▾ | System Management | Searches & Reports ▾
Help | About
Search | Actions ▾
All time
527 matching events
Save search | Build report
Timeline: zoom in | zoom out | Scale: linear | log
1 bar = 1 month
120
100
80
60
40
20
January 2010
March
May
July
September
52 fields | Pick fields
527 events over all time
« prev 1 2 3 4 5 6 7 8 9 10 next » | Options...
Results per page 10
Selected fields (3)
host (1)
source (1)
sourcetype (1)
Other interesting fields (35)
Account_Domain (4)
Account_Name (8)
Authentication_Package (2)
ComputerName (1)
event_id (n) (7)
Show all 59 lines

```
source="WinEventLog:Security" Account_Domain="[illegible]" Account_Name="[illegible]" TaskCategory="Logon"
```

```
1   10/18/10             10/18/10 05:49:06 PM
    5:49:06.000 PM       LogName=Security
                         SourceName=Microsoft Windows security auditing.
                         EventCode=4624
                         EventType=0
                         Type=Information
                         ComputerName=[illegible]
                         TaskCategory=Logon
                         OpCode=Info
                         RecordNumber=14490
                         host=octane ▾ | sourcetype=WinEventLog:Security ▾ | source=WinEventLog:Security ▾
```

Source: http://www.digitalthreat.net/2010/10/splunk-log-storage-search-and-reporting/

Metadata

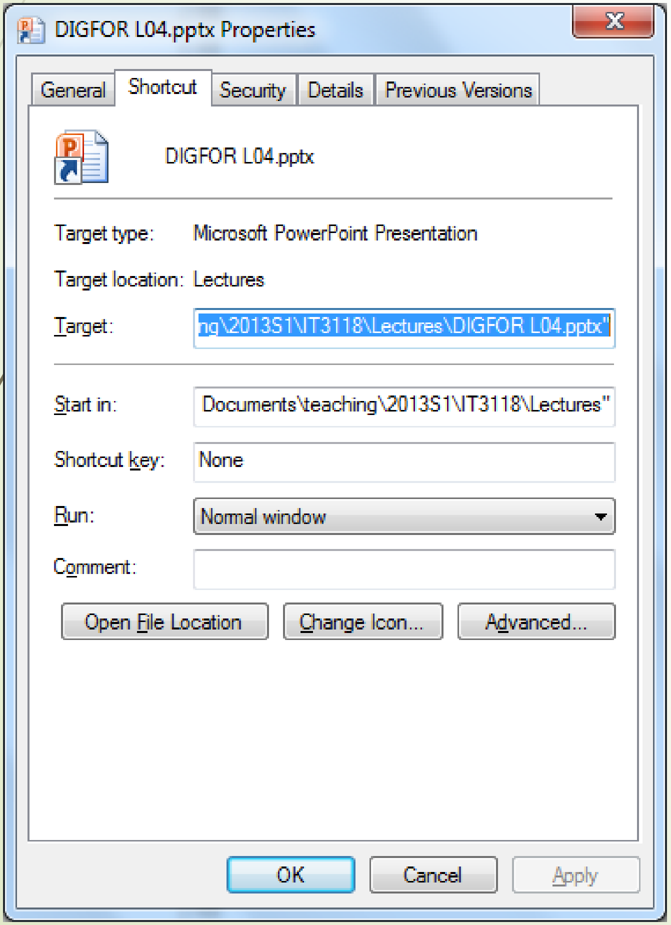
- Metadata contains file information that is not the actual data in the file.
- Metadata includes
  - Who created the file
  - Who modified the file
  - What the information in the file is about
- Common File Metadata
  - Shortcut files (.lnk)
  - Office documents
  - Picture/Media files
    - EXIF data
- Analysis tools: FTK, EXIFTool

Metadata

- Shortcut Files
  - Created when local and remote files are opened
  - Location: %USER_HOME%\Recent
    - Windows XP
      - \Documents and Settings\<username>\Recent
    - Vista and onwards
      - Drive:\Users\<user>\AppData\Roaming\Microsoft\Windows\Recent
  - What it keeps
    - MAC times of the shortcut file
    - Path to the source file
    - Volume information
      (e.g. drive letter, network share)

Metadata

- Shortcut Files



DIGFOR L04.pptx Properties

DIGFOR L04.pptx

Target type: Microsoft PowerPoint Presentation

Target location: Lectures

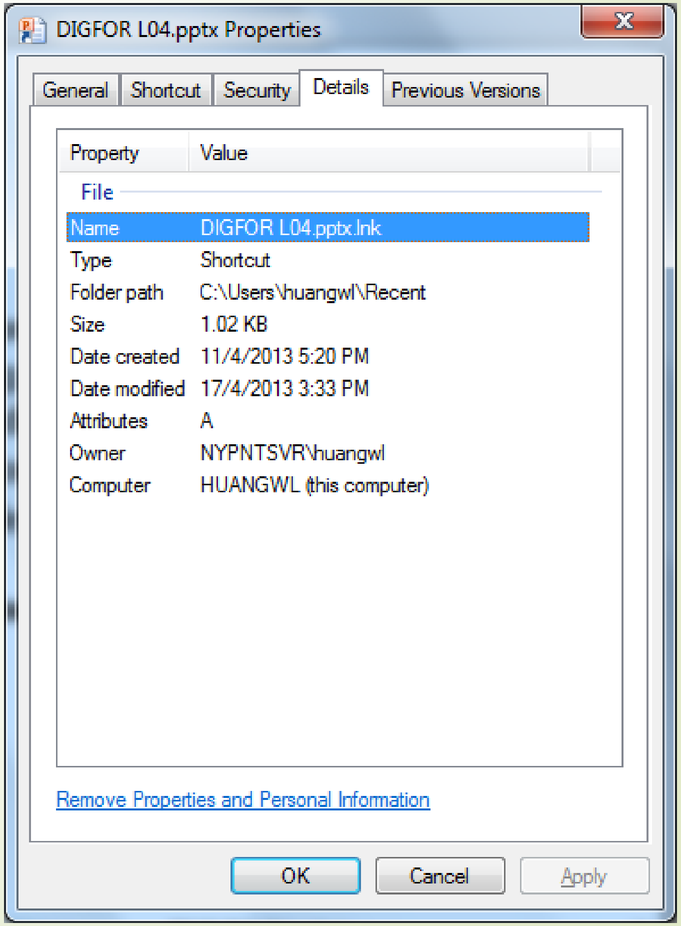
Target: ng\2013S1\IT3118\Lectures\DIGFOR L04.pptx"

Start in: Documents\teaching\2013S1\IT3118\Lectures"

Shortcut key: None

Run: Normal window

Comment:



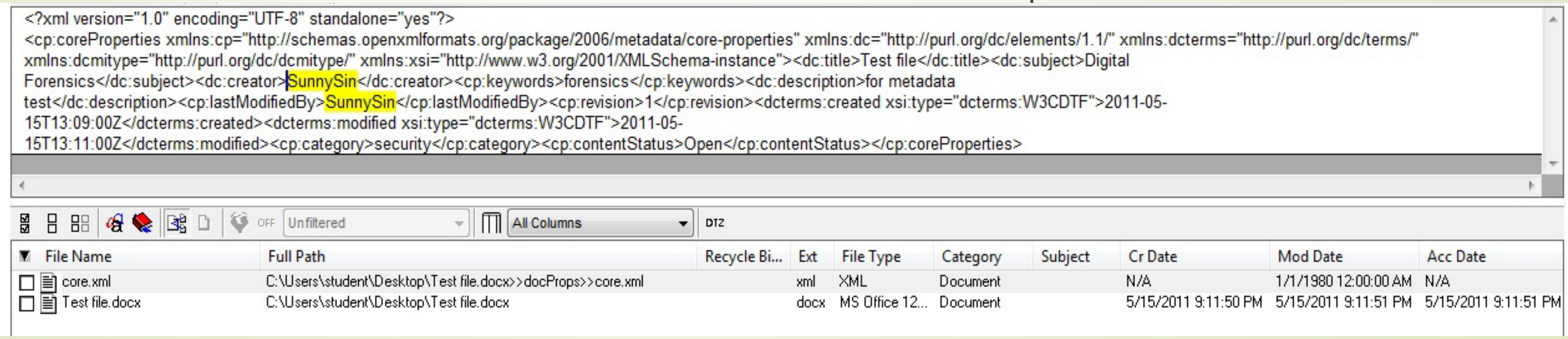
DIGFOR L04.pptx Properties

Property	Value
File	
Name	DIGFOR L04.pptx.lnk
Type	Shortcut
Folder path	C:\Users\huangwl\Recent
Size	1.02 KB
Date created	11/4/2013 5:20 PM
Date modified	17/4/2013 3:33 PM
Attributes	A
Owner	NYPNTSVR\huangwl
Computer	HUANGWL (this computer)

Remove Properties and Personal Information

Metadata

- Office Documents
  - Some metadata is updated by the users. Other metadata is created by the office applications and the Windows operating system
  - Metadata contain evidence on
    - Authoring history
    - Hidden Text and Comments
    - Files Properties/File Summaries
    - Document Revisions and Versions
    - Location of the where the file was saved
    - The NetBIOS name of the computer



```
<?xml version="1.0" encoding="UTF-8" standalone="yes"?>
<cp:coreProperties xmlns:cp="http://schemas.openxmlformats.org/package/2006/metadata/core-properties" xmlns:dc="http://purl.org/dc/elements/1.1/" xmlns:dcterms="http://purl.org/dc/terms/"
xmlns:dcmitype="http://purl.org/dc/dcmitype/" xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance"><dc:title>Test file</dc:title><dc:subject>Digital
Forensics</dc:subject><dc:creator>SunnySin</dc:creator><cp:keywords>forensics</cp:keywords><dc:description>for metadata
test</dc:description><cp:lastModifiedBy>SunnySin</cp:lastModifiedBy><cp:revision>1</cp:revision><dcterms:created xsi:type="dcterms:W3CDTF">2011-05-
15T13:09:00Z</dcterms:created><dcterms:modified xsi:type="dcterms:W3CDTF">2011-05-
15T13:11:00Z</dcterms:modified><cp:category>security</cp:category><cp:contentStatus>Open</cp:contentStatus></cp:coreProperties>
```

File Name	Full Path	Recycle Bi...	Ext	File Type	Category	Subject	Cr Date	Mod Date	Acc Date
□ core.xml	C:\Users\student\Desktop\Test file.docx>>docProps>>core.xml		xml	XML	Document		N/A	1/1/1980 12:00:00 AM	N/A
□ Test file.docx	C:\Users\student\Desktop\Test file.docx		docx	MS Office 12...	Document		5/15/2011 9:11:50 PM	5/15/2011 9:11:51 PM	5/15/2011 9:11:51 PM

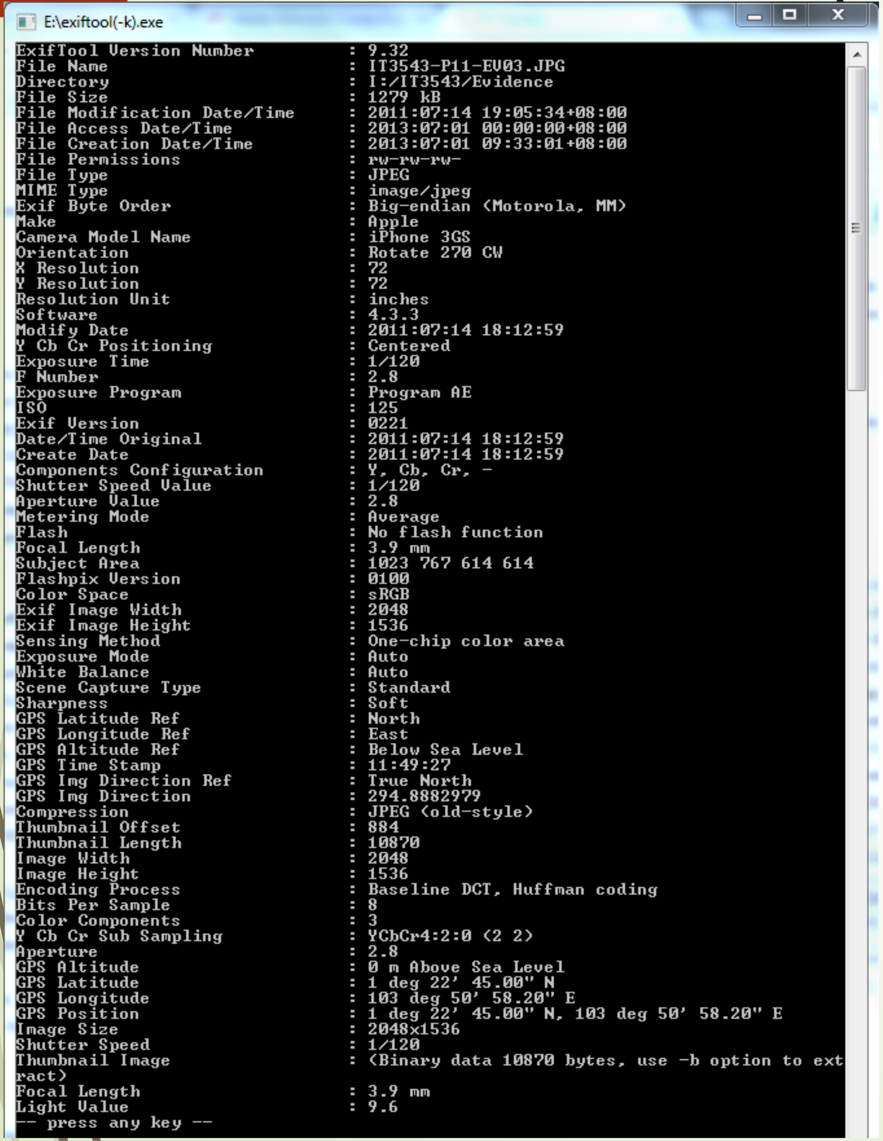
Metadata

- Metadata has been used in several high-profile cases to prove or disprove claims made.
  - Hutton Inquiry: In 2003, the British government announced an inquiry following the death of scientist David Kelly. Kelly allegedly had been exaggerated and added to the report after its original creation.
  - Through examination of the document's metadata, it was proved that several people has altered the document and that the information in question could have been added on a later date by another author.

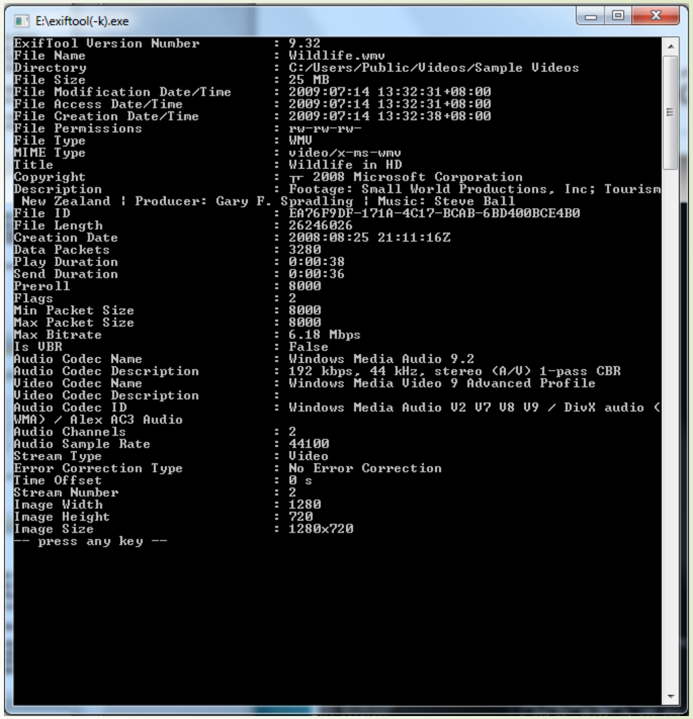
Metadata

- Exchangeable image file standard (EXIF)
  - Standard used by digital camera (including smartphones), scanners and other system handling image and sound files recorded by digital cameras
  - Metadata tags include
    - Date and time information
    - Camera settings, e.g. camera model and make, shutter speed, ISO speed etc
    - Thumbnail for previewing
    - Descriptions
    - Copyright information
    - Geolocation!!!

Exiftool Output



```
ExifTool Version Number         : 9.32
File Name                       : IT3543-P11-EV03.JPG
Directory                       : I:/IT3543/Evidence
File Size                       : 1279 kB
File Modification Date/Time     : 2011:07:14 19:05:34+08:00
File Access Date/Time           : 2013:07:01 00:00:00+08:00
File Creation Date/Time         : 2013:07:01 09:33:01+08:00
File Permissions                : rw-rw-rw-
File Type                       : JPEG
MIME Type                       : image/jpeg
Exif Byte Order                 : Big-endian (Motorola, MM)
Make                            : Apple
Camera Model Name               : iPhone 3GS
Orientation                     : Rotate 270 CW
X Resolution                    : 72
Y Resolution                    : 72
Resolution Unit                 : inches
Software                        : 4.3.3
Modify Date                     : 2011:07:14 18:12:59
Y Cb Cr Positioning             : Centered
Exposure Time                   : 1/120
F Number                        : 2.8
Exposure Program                : Program AE
ISO                             : 125
Exif Version                    : 0221
Date/Time Original              : 2011:07:14 18:12:59
Create Date                     : 2011:07:14 18:12:59
Components Configuration        : Y, Cb, Cr, -
Shutter Speed Value             : 1/120
Aperture Value                  : 2.8
Metering Mode                   : Average
Flash                           : No flash function
Focal Length                    : 3.9 mm
Subject Area                    : 1023 767 614 614
Flashpix Version                : 0100
Color Space                     : sRGB
Exif Image Width                : 2048
Exif Image Height               : 1536
Sensing Method                  : One-chip color area
Exposure Mode                   : Auto
White Balance                   : Auto
Scene Capture Type              : Standard
Sharpness                       : Soft
GPS Latitude Ref                : North
GPS Longitude Ref               : East
GPS Altitude Ref                : Below Sea Level
GPS Time Stamp                  : 11:49:27
GPS Img Direction Ref           : True North
GPS Img Direction               : 294.8882979
Compression                     : JPEG (old-style)
Thumbnail Offset                : 884
Thumbnail Length                : 10870
Image Width                     : 2048
Image Height                    : 1536
Encoding Process                : Baseline DCT, Huffman coding
Bits Per Sample                 : 8
Color Components                : 3
Y Cb Cr Sub Sampling            : YCbCr4:2:0 (2 2)
Aperture                        : 2.8
GPS Altitude                    : 0 m Above Sea Level
GPS Latitude                    : 1 deg 22' 45.00" N
GPS Longitude                   : 103 deg 50' 58.20" E
GPS Position                    : 1 deg 22' 45.00" N, 103 deg 50' 58.20" E
Image Size                      : 2048x1536
Shutter Speed                   : 1/120
Thumbnail Image                 : (Binary data 10870 bytes, use -b option to ext
ract)
Focal Length                    : 3.9 mm
Light Value                     : 9.6
-- press any key --
```



```
ExifTool Version Number         : 9.32
File Name                       : Wildlife.wmv
Directory                       : C:/Users/Public/Videos/Sample Videos
File Size                       : 25 MB
File Modification Date/Time     : 2009:07:14 13:32:31+08:00
File Access Date/Time           : 2009:07:14 13:32:31+08:00
File Creation Date/Time         : 2009:07:14 13:32:38+08:00
File Permissions                : rw-rw-rw-
File Type                       : WMV
MIME Type                       : video/x-ms-wmv
Title                           : Wildlife in HD
Copyright                       : ╥ 2008 Microsoft Corporation
Description                     : Footage: Small World Productions, Inc; Tourism
 New Zealand | Producer: Gary F. Spradling | Music: Steve Ball
File ID                         : EA76F9DF-171A-4C17-BCAB-6BD400BCE4B0
File Length                     : 26246026
Creation Date                   : 2008:08:25 21:11:16Z
Data Packets                    : 3280
Play Duration                   : 0:00:38
Send Duration                   : 0:00:36
Preroll                         : 8000
Flags                           : 2
Min Packet Size                 : 8000
Max Packet Size                 : 8000
Max Bitrate                     : 6.18 Mbps
Is VBR                          : False
Audio Codec Name                : Windows Media Audio 9.2
Audio Codec Description         : 192 kbps, 44 kHz, stereo (A/V) 1-pass CBR
Video Codec Name                : Windows Media Video 9 Advanced Profile
Video Codec Description         :
Audio Codec ID                  : Windows Media Audio V2 V7 V8 V9 / DivX audio (
WMA) / Alex AC3 Audio
Audio Channels                  : 2
Audio Sample Rate               : 44100
Stream Type                     : Video
Error Correction Type           : No Error Correction
Time Offset                     : 0 s
Stream Number                   : 2
Image Width                     : 1280
Image Height                    : 720
Image Size                      : 1280x720
-- press any key --
```

EXIF Audio File Metadata

EXIF JPEG File Metadata

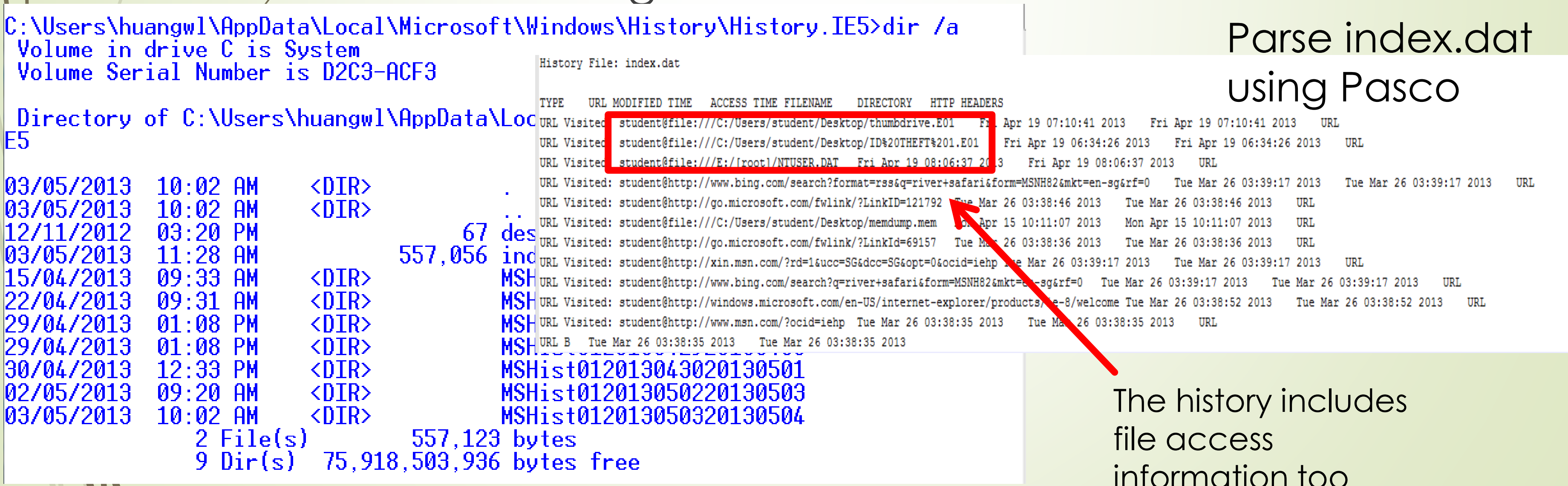
Browser Forensic - IE

- URL Cache Containers
  - Data files used by various components of IE, Explorer, and Search
  - Used for
    - Temporary Internet Files
    - Browsing History
    - Cookies
    - HTTP response objects and redirects
    - RSS feeds
    - InPrivate browsing and more
  - It contains
    - A directory
    - An Index file (index.dat)
    - Files for cached data (may be in sub-directories)
  - Can be examined using free "Pasco"

Common browser artifacts

Browser Forensic - IE

- Browsing History
  - \Users\<username>\AppData\Local\Miscrosoft\Windows\History\History.IE5
  - Subdirectories are name MSHist01<start date><end date> for records within different date range



```
C:\Users\huangwl\AppData\Local\Microsoft\Windows\History\History.IE5>dir /a
 Volume in drive C is System
 Volume Serial Number is D2C3-ACF3

 Directory of C:\Users\huangwl\AppData\Loc
E5

03/05/2013  10:02 AM    <DIR>          .
03/05/2013  10:02 AM    <DIR>          ..
12/11/2012  03:20 PM                67 des
03/05/2013  11:28 AM           557,056 ind
15/04/2013  09:33 AM    <DIR>          MSH
22/04/2013  09:31 AM    <DIR>          MSH
29/04/2013  01:08 PM    <DIR>          MSH
29/04/2013  01:08 PM    <DIR>          MSH
30/04/2013  12:33 PM    <DIR>          MSHist012013043020130501
02/05/2013  09:20 AM    <DIR>          MSHist012013050220130503
03/05/2013  10:02 AM    <DIR>          MSHist012013050320130504
               2 File(s)        557,123 bytes
               9 Dir(s)  75,918,503,936 bytes free
```

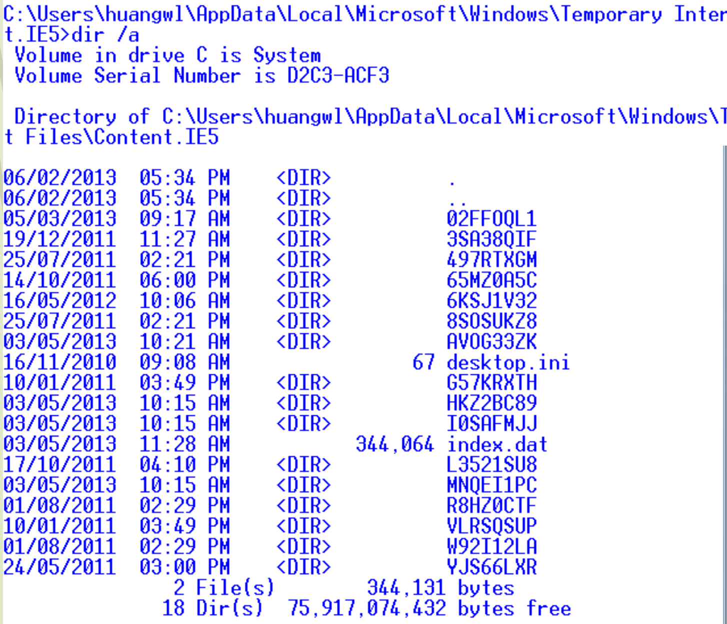
```
History File: index.dat

TYPE    URL MODIFIED TIME   ACCESS TIME FILENAME    DIRECTORY   HTTP HEADERS
URL Visited: student@file:///C:/Users/student/Desktop/thumbdrive.E01    Fri Apr 19 07:10:41 2013    Fri Apr 19 07:10:41 2013    URL
URL Visited: student@file:///C:/Users/student/Desktop/ID%20THEFT%201.E01    Fri Apr 19 06:34:26 2013    Fri Apr 19 06:34:26 2013    URL
URL Visited: student@file:///E:/[root]/NTUSER.DAT   Fri Apr 19 08:06:37 2013    Fri Apr 19 08:06:37 2013    URL
URL Visited: student@http://www.bing.com/search?format=rss&q=river+safari&form=MSNH82&mkt=en-sg&rf=0    Tue Mar 26 03:39:17 2013    Tue Mar 26 03:39:17 2013    URL
URL Visited: student@http://go.microsoft.com/fwlink/?LinkID=121792  Tue Mar 26 03:38:46 2013    Tue Mar 26 03:38:46 2013    URL
URL Visited: student@file:///C:/Users/student/Desktop/memdump.mem   Mon Apr 15 10:11:07 2013    Mon Apr 15 10:11:07 2013    URL
URL Visited: student@http://go.microsoft.com/fwlink/?LinkId=69157   Tue Mar 26 03:38:36 2013    Tue Mar 26 03:38:36 2013    URL
URL Visited: student@http://xin.msn.com/?rd=1&ucc=SG&dcc=SG&opt=0&ocid=iehp Tue Mar 26 03:39:17 2013    Tue Mar 26 03:39:17 2013    URL
URL Visited: student@http://www.bing.com/search?q=river+safari&form=MSNH82&mkt=en-sg&rf=0   Tue Mar 26 03:39:17 2013    Tue Mar 26 03:39:17 2013    URL
URL Visited: student@http://windows.microsoft.com/en-US/internet-explorer/products/ie-8/welcome Tue Mar 26 03:38:52 2013    Tue Mar 26 03:38:52 2013    URL
URL Visited: student@http://www.msn.com/?ocid=iehp  Tue Mar 26 03:38:35 2013    Tue Mar 26 03:38:35 2013    URL
URL B   Tue Mar 26 03:38:35 2013    Tue Mar 26 03:38:35 2013
```

Parse index.dat using Pasco

The history includes file access information too

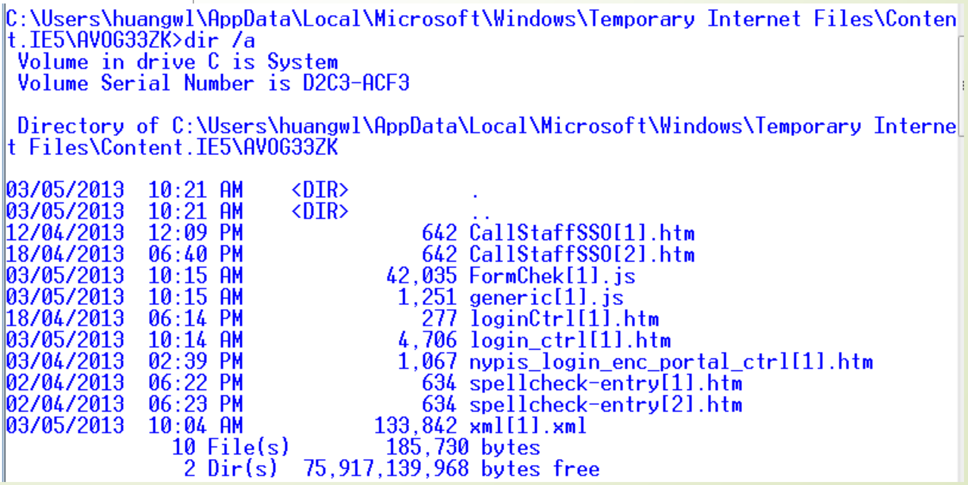
Browser Forensic - IE

- Temporary Internet Files
  - Cache of recently viewed web pages
  - \Users\<username>\AppData\Local\Microsoft\Windows\Temporary Internet Files\Content.IE5
  - Subdirectories are named randomly



```
C:\Users\huangwl\AppData\Local\Microsoft\Windows\Temporary Internet Files\Conten
t.IE5>dir /a
 Volume in drive C is System
 Volume Serial Number is D2C3-ACF3

 Directory of C:\Users\huangwl\AppData\Local\Microsoft\Windows\Temporary Interne
t Files\Content.IE5

06/02/2013  05:34 PM    <DIR>          .
06/02/2013  05:34 PM    <DIR>          ..
05/03/2013  09:17 AM    <DIR>          02FFOQL1
19/12/2011  11:27 AM    <DIR>          3SA38QIF
25/07/2011  02:21 PM    <DIR>          497RTXGM
14/10/2011  06:00 PM    <DIR>          65MZ0A5C
16/05/2012  10:06 AM    <DIR>          6KSJ1V32
25/07/2011  02:21 PM    <DIR>          8SOSUKZ8
03/05/2013  10:21 AM    <DIR>          AVOG33ZK
16/11/2010  09:08 AM                67 desktop.ini
10/01/2011  03:49 PM    <DIR>          G57KRXTH
03/05/2013  10:15 AM    <DIR>          HKZ2BC89
03/05/2013  10:15 AM    <DIR>          I0SAFMJJ
03/05/2013  11:28 AM           344,064 index.dat
17/10/2011  04:10 PM    <DIR>          L3521SU8
03/05/2013  10:15 AM    <DIR>          MNQEI1PC
01/08/2011  02:29 PM    <DIR>          R8HZ0CTF
10/01/2011  03:49 PM    <DIR>          VLRSQSUP
01/08/2011  02:29 PM    <DIR>          W92I12LA
24/05/2011  03:00 PM    <DIR>          YJS66LXR
               2 File(s)        344,131 bytes
              18 Dir(s)  75,917,074,432 bytes free
```

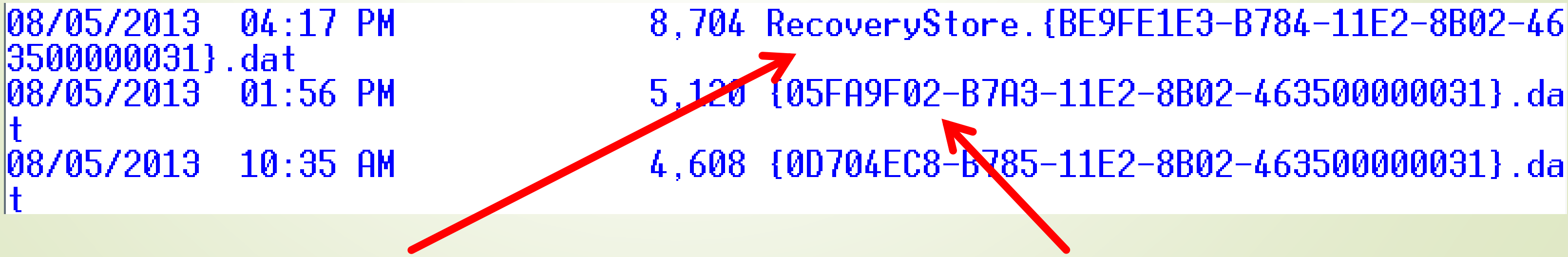
Why don’t we visit the website directly based on the surfing history?



```
C:\Users\huangwl\AppData\Local\Microsoft\Windows\Temporary Internet Files\Conten
t.IE5\AVOG33ZK>dir /a
 Volume in drive C is System
 Volume Serial Number is D2C3-ACF3

 Directory of C:\Users\huangwl\AppData\Local\Microsoft\Windows\Temporary Interne
t Files\Content.IE5\AVOG33ZK

03/05/2013  10:21 AM    <DIR>          .
03/05/2013  10:21 AM    <DIR>          ..
12/04/2013  12:09 PM               642 CallStaffSSO[1].htm
18/04/2013  06:40 PM               642 CallStaffSSO[2].htm
03/05/2013  10:15 AM            42,035 FormChek[1].js
03/05/2013  10:15 AM             1,251 generic[1].js
18/04/2013  06:14 PM               277 loginCtrl[1].htm
03/05/2013  10:14 AM             4,706 login_ctrl[1].htm
03/04/2013  02:39 PM             1,067 nypis_login_enc_portal_ctrl[1].htm
02/04/2013  06:22 PM               634 spellcheck-entry[1].htm
02/04/2013  06:23 PM               634 spellcheck-entry[2].htm
03/05/2013  10:04 AM           133,842 xml[1].xml
              10 File(s)        185,730 bytes
               2 Dir(s)  75,917,139,968 bytes free
```

Browser Forensic - IE

- Automatic Crash Recovery
  - Records information on the current and previous browsing sessions
  - Normal:\Users\<username>\AppData\Local\Microsoft\Internet Explorer\Recovery\Active
  - Admin:\Users\<username>\AppData\Local\Microsoft\Internet Explorer\Recovery\High\Active



```
08/05/2013  04:17 PM             8,704 RecoveryStore.{BE9FE1E3-B784-11E2-8B02-46
3500000031}.dat
08/05/2013  01:56 PM             5,120 {05FA9F02-B7A3-11E2-8B02-463500000031}.da
t
08/05/2013  10:35 AM             4,608 {0D704EC8-B785-11E2-8B02-463500000031}.da
t
```

Session file, references tab files for the session

Tab file, state of the tab

53

Browser Forensic - IE

- Downloads
  - Most files at \Users\<username>\Downloads
  - Some exception, e.g. picture files are downloaded to \Users\<username>\Pictures

54

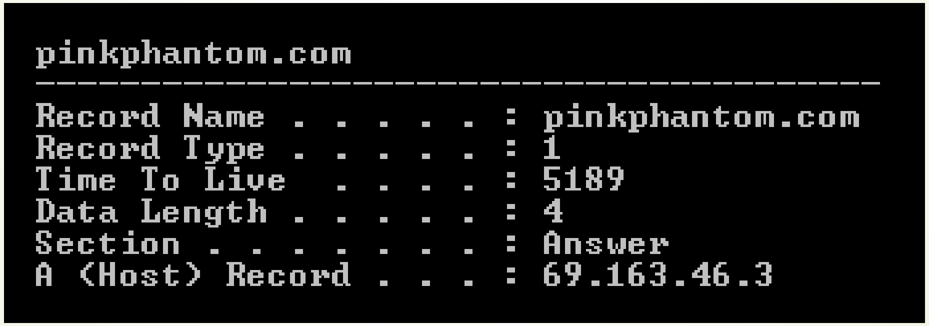
InPrivate Browsing at IE

- New feature since IE8
- Designed primarily for accessing the web from a shared computer
  - What is not stored?
    - History, form data, password, address bar, search autocomplete, search queries
  - What are still recorded but will be deleted upon closing the browser?
    - Cookies used as "session" cookies
    - Temporary internet files

What if the browser crashes when user is using InPrivate browsing mode?

InPrivate Browsing at IE

- Investigation approaches
  - Local DNS cache



```
pinkphantom.com
----------------------------------------
Record Name . . . . . : pinkphantom.com
Record Type . . . . . : 1
Time To Live  . . . . : 5189
Data Length . . . . . : 4
Section . . . . . . . : Answer
A (Host) Record . . . : 69.163.46.3
```

  - Temp data at index.dat
    - Before the browser is closed, or restarted in the case of crashing

Summary

- Events and Time Analysis
- Operating Systems Artifacts Analysis – Windows
  - Case-related data files and metadata
  - User activities/behaviors event logs
  - System configurations and logs
  - Application configurations and usage
  - Web browsing history

References

1. Section 5 “Using Data from Operating Systems”, Guide to Integrating Forensic Techniques into Incident Response SP800-86 NIST, csrc.nist.org
2. File System Forensic Analysis, Brian Carrier, 2005, Addison Wesley
3. Windows Forensics and Incident Recovery, Harlan Carvey, 2005, Addison Wesley
4. New Windows Features for Forensic Investigators, Brian Catlin, Jamie Hanrahan, 2010
5. AccessData FTK Forensic Toolkits 1.81.6 manual