Windows Registry Analysis

Computer Forensics, 2013

Registry Analysis

- Registry is central database of Windows systems
  - Configuration of system
  - Information about user activity
    - applications installed and opened
    - window positions and sizes
      - to provide user with a better experience
  - Information is time-stamped

Registry Analysis

- Used to get systems information
  - Example: System has no prefetch files
    - Investigate the corresponding registry key
      - Microsoft knowledge base 307498
      - HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Control\Session Manager\Memory Management\PrefetchParameters
- Used to establish timelines of activity

Registry Analysis

- What if there are no values?
  - "Absence of evidence is not evidence of absence"
    - E.g.: Antiforensics: Windows washer removes registry entries
      - Last runtime of Windows washer becomes evidence
    - E.g.: Malware dll not loaded through registry
      - But could be loaded through some other mechanism, such as a shell extension
      - (Registry remains a popular tool for malware to avoid repeat infections)

Registry Analysis

- Contents:
  - Basic structure remains fixed
  - Location of values changes
- Storage location depends on *hive* and system
  - Main hives in Windows\system32\config
  - Other in system32\config
  - User information in NTUSER.dat hive in User Profile
  - Parts are volatile:
    - Populated when need arises
      - HKEY_CURRENT_USER, HKEY
      - HKEY_LOCAL_MACHINE\System
      - HKEY_CLASSES_ROOT

Registry Analysis

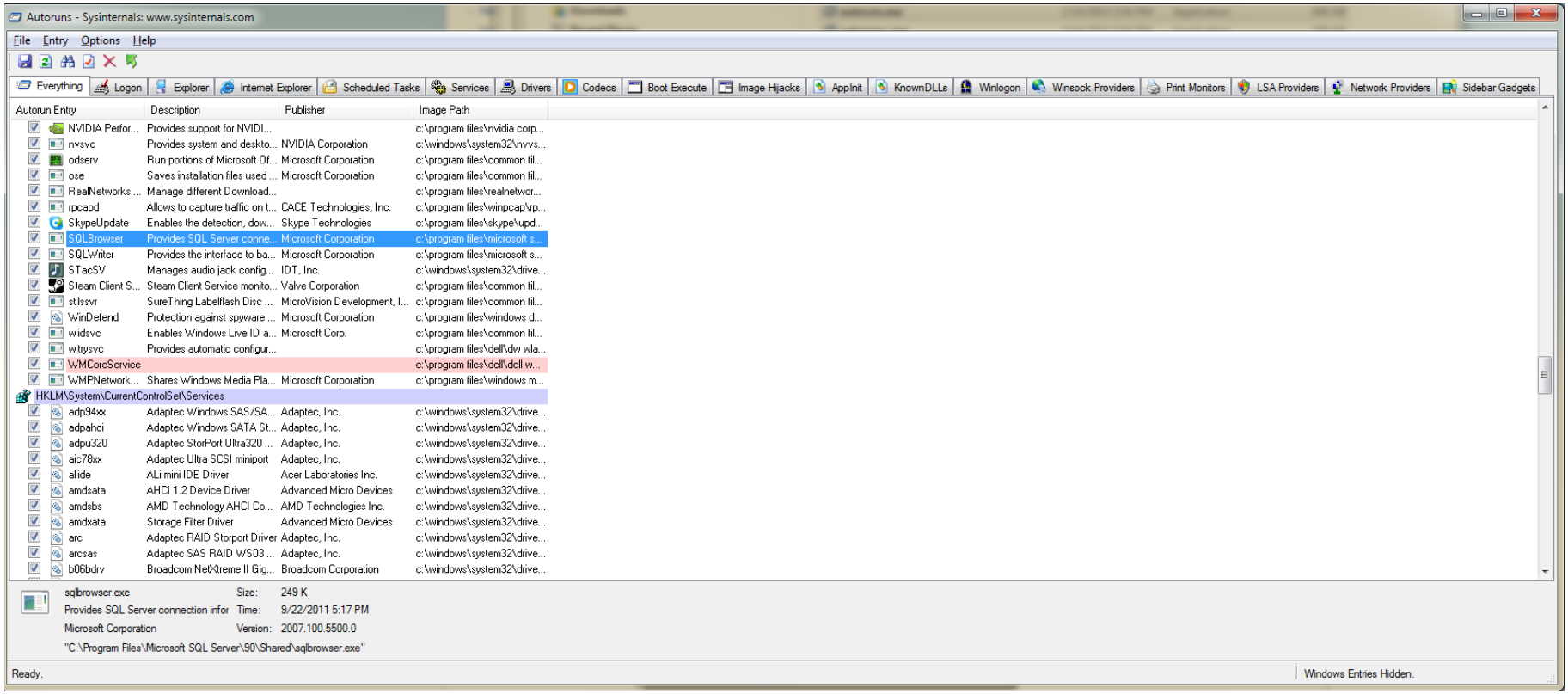
- Key Cell Structure
  - 0-3 Size
  - 4-5 Node ID
  - 6-7 Node Type
  - 8-15 LastWrite Time
  - …
- Value Cell Structure
  - 0-3 Size
  - 4-5 Node ID
  - 6-7 Value name length
  - 8-11 Data length
  - 12-15 Offset to data
  - 16-20 Value type

```
00002580  01 05 00 00 00 00 00 05  15 00 00 00 47 C0 1F 8C  F9 B6 06 4C A5 45 60 EB  F5 01 00 00 00 00 00 00
000025A0  A8 FF FF FF 6E 6B 20 00  B6 58 2B E9 C5 D8 CD 01  00 00 00 00 10 04 00 00  03 00 00 00 00 00 00 00
000025C0  B8 1A 00 00 FF FF FF FF  02 00 00 00 10 01 00 00  68 02 00 00 FF FF FF FF  0E 00 00 00 00 00 00 00
000025E0  02 00 00 00 10 01 00 00  00 00 00 00 07 00 00 00  41 63 63 6F 75 6E 74 00  E0 FF FF FF 76 6B 01 00
00002600  F0 00 00 00 18 16 00 00  03 00 00 00 01 00 00 00  46 00 00 00 00 00 00 00  08 FF FF FF 02 00 01 00
```

Registry Analysis Tools

- Life Analysis
  - regedit.exe
    - Native tool (use with caution)
    - Does not give all information (especially not time of last write)
  - reg.exe
    - Native command line tool
  - Autoruns.exe
    - Russinovich, SysInternals (now MS) investigates registry and other places for programs that run automatically
  - Scripting tools
    - E.g.: Using Perl Win32::TieRegistry

Registry Analysis Tools
Autoruns



Registry Analysis Tools

- Registry Monitoring
  - Observe changes to the registry while interacting with system
  - Regshot
  - RegMon (SysInternals)

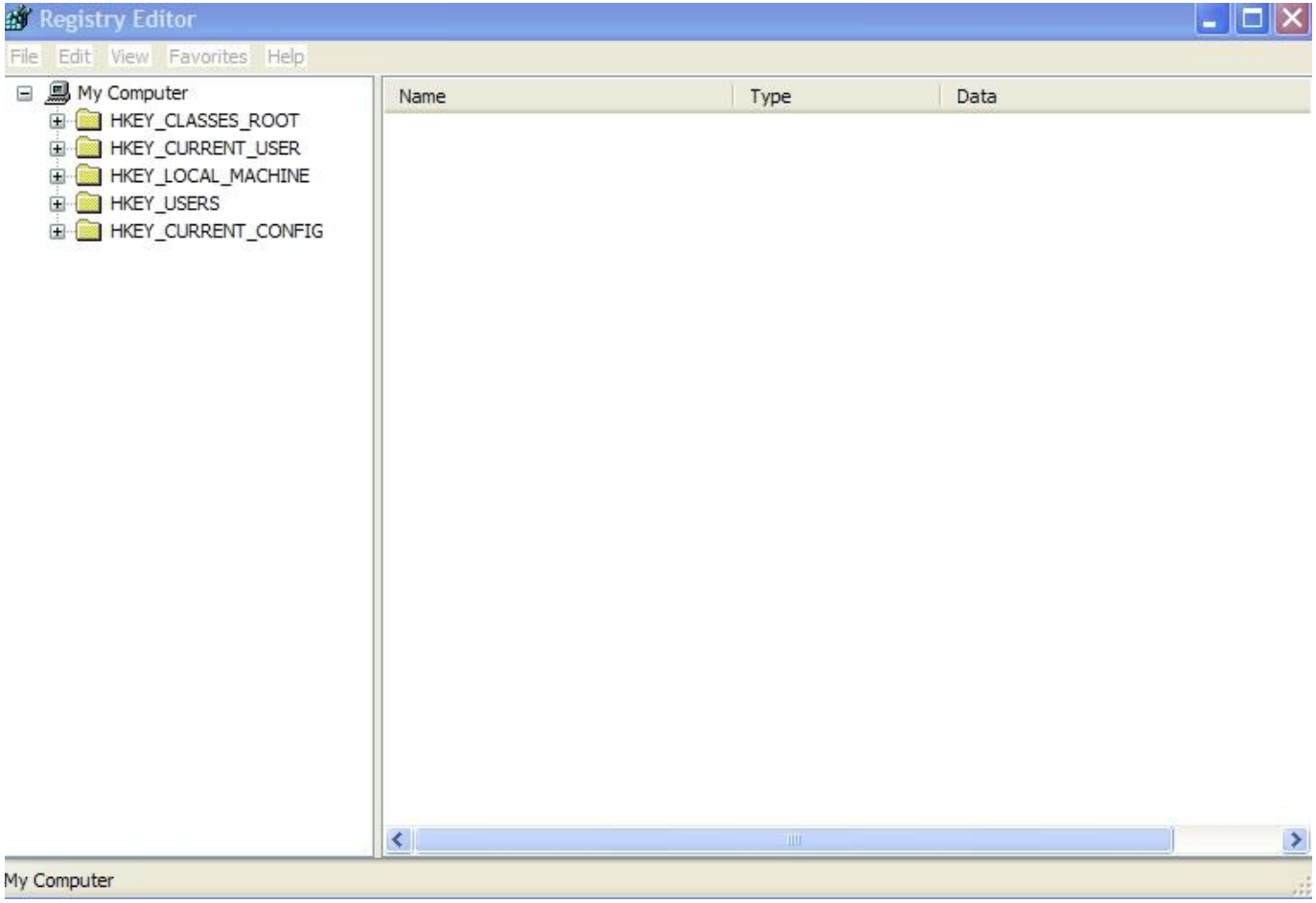
Registry Analysis Tools

- Forensics Analysis
  - Build into tools ProDiscover / Encase, F-Response, FTK
  - RegRipper, RIP.pl, regslack

Windows XP Registry

Filename	Location	Content
ntuser.dat If there are multiple user profiles, each user has an individual user.dat file in windows\profiles\user account	\Documents and Settings\user account	Protected storage area for user Most Recently Used (MRU) files User preference settings
Default	\Windows\system32\config	System settings
SAM	\Windows\system32\config	User account management and security settings
Security	\Windows\system32\config	Security settings
Software	\Windows\system32\config	All installed programs and their settings
System	\Windows\system32\config	System settings

Registry Organization



Windows Security and Relative ID

- The Windows Registry utilizes a alphanumeric combination to uniquely identify a security principal or security group.
- The Security ID (SID) is used to identify the computer system.
- The Relative ID (RID) is used to identity the specific user on the computer system.
- The SID appears as:
  - S-1-5-21-927890586-3685698554-67682326-1005

SID Examples

SID: S-1-0
Name: Null Authority
Description: An identifier authority.

- SID: S-1-0-0
  Name: Nobody
  Description: No security principal.
- SID: S-1-1
  Name: World Authority
  Description: An identifier authority.
- SID: S-1-1-0
  Name: Everyone
  Description: A group that includes all users, even anonymous users and guests. Membership is controlled by the operating system.
- SID: S-1-2
  Name: Local Authority
  Description: An identifier authority.
- SID: S-1-3
  Name: Creator Authority
  Description: An identifier authority.

SID

- Security ID
  - NT/2000/XP/2003
    - HKLM>SAM>Domains>Accounts>Aliases>Members
      - **This key will provide information on the computer identifier**
    - HKLM>SAM>Domains>Users
      - **This key will provide information in hexadecimal**
    - User ID
      - Administrator – 500
      - Guest – 501
    - Global Groups ID
      - Administrators – 512
      - Users – 513
      - Guest - 514

MRU

- To identify the Most Recently Used (MRU) files on a suspect computer system:
  - Windows 9x/Me
    - User.dat
      - Search should be made for MRU, LRU, Recent
  - Windows NT/2000
    - Ntuser.dat
      - Search should be made for MRU, LRU, Recent
  - Windows XP/2003
    - HKU>UserSID>Software>Microsoft>Windows>CurrentVersion>Explorer>RecentDoc
    - Select file extension and select item

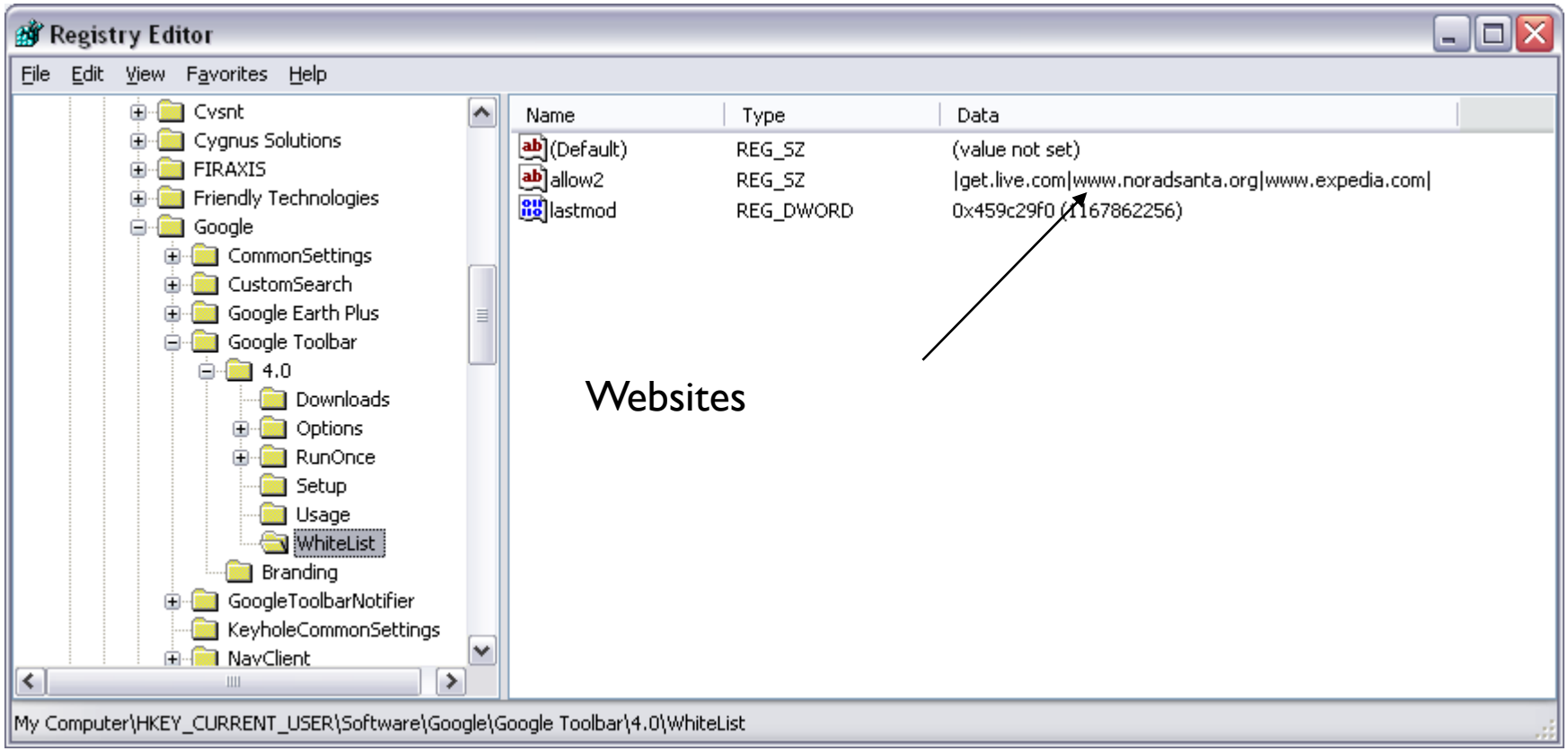
Registry Forensics

- Registry keys have last modified time-stamp
  - Stored as FILETIME structure
    - like MAC for files
  - Not accessible through reg-edit
  - Accessible in binary.

Registry Forensics

- Registry Analysis:
  - Perform a GUI-based live-system analysis.
    - Easiest, but most likely to incur changes.
    - Use regedit.
  - Perform a command-line live-system analysis
    - Less risky
    - Use "reg" command.
  - Remote live system analysis
    - regedit allows access to a remote registry
    - Superscan from Foundstone
  - Offline analysis on registry files.
    - Encase, FTK (Access data) have specialized tools
    - regedit on registry dump.

Registry Forensics



Registry Forensics: NTUSER.DAT

- AOL Instant Messenger Away messages
  - File Transfer & Sharing
  - Last User
  - Profile Info
  - Recent Contacts
  - Registered Users
  - Saved Buddy List

Registry Forensics: NTUSER.DAT

- ICQ
  - IM contacts, file transfer info etc.
  - User Identification Number
  - Last logged in user
  - Nickname of user

Registry Forensics: NTUSER.DAT

- Internet Explorer
  - IE auto logon and password
  - IE search terms
  - IE settings
  - Typed URLs
  - Auto-complete passwords

Registry Forensics: NTUSER.DAT IE explorer Typed URLs

Registry Editor

File Edit View Favorites Help

- Extensions
- Help_Menu_URLs
- InformationBar
- IntelliForms
- International
- Main
- Media
- MenuExt
- New Windows
- Search
- SearchUrl
- Security
- Services
- Settings
- Toolbar
- TypedURLs
- URLSearchHooks
- Internet Mail and News
- Java VM
- Keyboard
- MediaPlayer
- MessengerService
- MFC 3.0 Samples

Name	Type	Data
(Default)	REG_SZ	(value not set)
url1	REG_SZ	http://www.ucsc.edu
url10	REG_SZ	http://129.210.114.76/hello.cgi
url11	REG_SZ	http://localhost/hello.cgi
url12	REG_SZ	http://localhost/test.cgi
url13	REG_SZ	http://localhost/
url14	REG_SZ	http://hotmail.com/
url15	REG_SZ	http://httpd.apache.org/docs/2.2/mod/core.
url16	REG_SZ	http://www.google.com/
url17	REG_SZ	http://adm.lnpu.edu.ua/
url2	REG_SZ	http://www.amazon.com/
url3	REG_SZ	http://www.voroem.com/
url4	REG_SZ	http://www.msdewey.com/
url5	REG_SZ	http://www.scu.edu/
url6	REG_SZ	http://www.hotmail.com/
url7	REG_SZ	http://www.expedia.com/
url8	REG_SZ	http://www.cnn.com/
url9	REG_SZ	http://cnn.com/

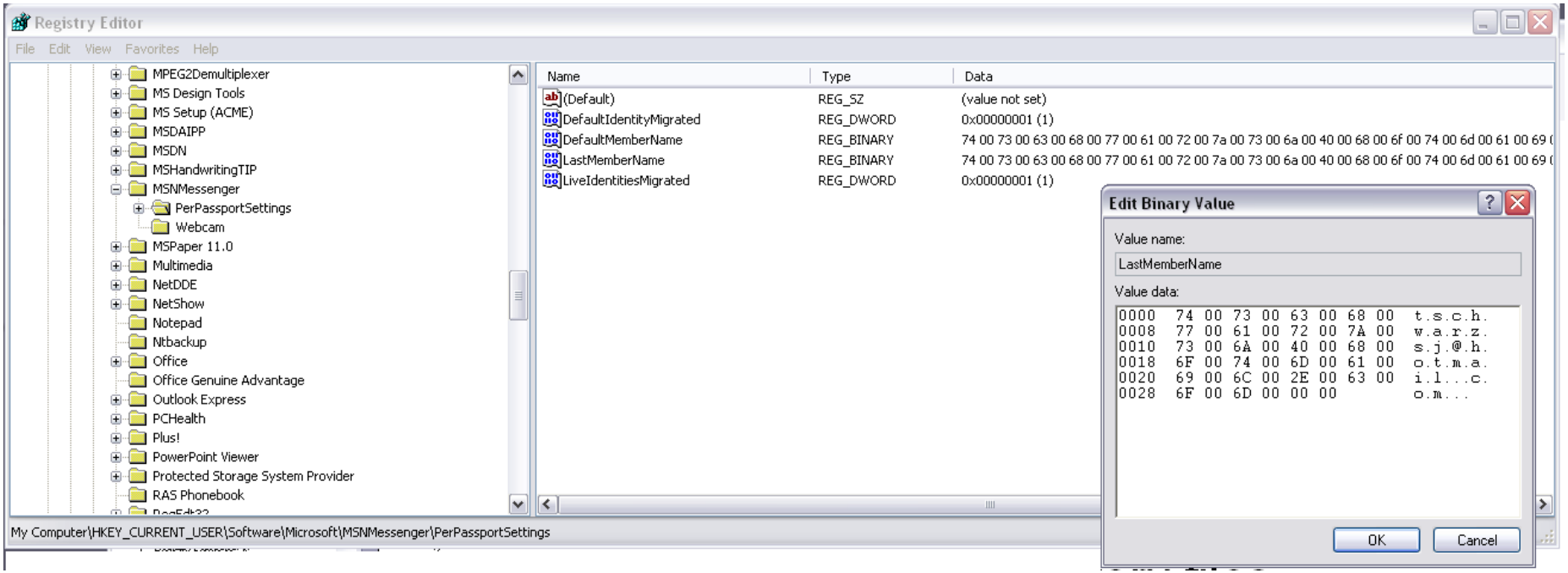
My Computer\HKEY_CURRENT_USER\Software\Microsoft\Internet Explorer\TypedURLs

Registry Forensics: NTUSER.DAT

- MSN Messenger
  - IM groups, contacts, …
  - Location of message history files
  - Location of saved contact list files

Registry Forensics: NTUSER.DAT

Last member name in MSN messenger



Registry Forensics: NTUSER.DAT

- Outlook express account passwords

Registry Forensics

- Yahoo messenger
  - Chat rooms
  - Alternate user identities
  - Last logged in user
  - Encrypted password
  - Recent contacts
  - Registered screen names

Registry Forensics

- System:
  - Computer name
  - Dynamic disks
  - Install dates
  - Last user logged in
  - Mounted devices
  - Windows OS product key
  - Registered owner
  - Programs run automatically
  - System's USB devices

Registry Forensics

Registry Editor

File Edit View Favorites Help

My Computer
- HKEY_CLASSES_ROOT
- HKEY_CURRENT_USER
- HKEY_LOCAL_MACHINE
  - HARDWARE
  - SAM
  - SECURITY
  - SOFTWARE
  - SYSTEM
    - ControlSet001
    - ControlSet003
    - CurrentControlSet
    - LastKnownGoodRecovery
    - MountedDevices
    - Select
    - Setup
    - WPA
- HKEY_USERS
- HKEY_CURRENT_CONFIG

Name	Type	Data
\??\Volume{5ad97000-2c33-11da-bc29-...	REG_BINARY	5c 00 3f 00 3f 00 5c 00 53 00 54 00 4f 00 52 00 41 00 47 00 45 00 23 00 52 00 65 00 6d 00 6f 00 7e
\??\Volume{7a8fcef0-fbe5-11da-bcf9-0...	REG_BINARY	5c 00 3f 00 3f 00 5c 00 53 00 54 00 4f 00 52 00 41 00 47 00 45 00 23 00 52 00 65 00 6d 00 6f 00 7e
\??\Volume{7f5b5670-c37b-11d9-9957-...	REG_BINARY	5c 00 3f 00 3f 00 5c 00 53 00 54 00 4f 00 52 00 41 00 47 00 45 00 23 00 52 00 65 00 6d 00 6f 00 7e
\??\Volume{830108b0-b907-11d9-9942-...	REG_BINARY	f1 4
\??\Volume{830108b1-b907-11d9-9942-...	REG_BINARY	5c 0
\??\Volume{830108b2-b907-11d9-9942-...	REG_BINARY	5c 0
\??\Volume{896ea932-0b8a-11db-bd1b-...	REG_BINARY	5c 0
\??\Volume{aacc637c-a0dd-11db-bdc3-...	REG_BINARY	5c 0
\??\Volume{eab559a0-f0c3-11d9-bbf1-8...	REG_BINARY	5c 0
\??\Volume{f0c04563-b58f-11db-bdde-0...	REG_BINARY	5c 0
\??\Volume{f0c04564-b58f-11db-bdde-0...	REG_BINARY	5c 0
\??\Volume{f0c04566-b58f-11db-bdde-0...	REG_BINARY	5c 0
\??\Volume{f8881840-bcf3-11d9-994c-0...	REG_BINARY	4d b
\DosDevices\A:	REG_BINARY	5c 0
\DosDevices\C:	REG_BINARY	f1 4
\DosDevices\D:	REG_BINARY	5c 0
\DosDevices\E:	REG_BINARY	5c 0
\DosDevices\F:	REG_BINARY	5c 0
\DosDevices\G:	REG_BINARY	5c 0

Edit Binary Value

Value name:

\DosDevices\G:

Value data:

```
0028  65 00 4D 00 65 00 64 00  e.M.e.d.
0030  69 00 61 00 23 00 37 00  i.a.#.7.
0038  26 00 31 00 37 00 32 00  &.1.7.2.
0040  34 00 37 00 62 00 32 00  4.7.b.2.
0048  63 00 26 00 30 00 26 00  c.&.0.&.
0050  52 00 4D 00 23 00 7B 00  R.M.#.{.
0058  35 00 33 00 66 00 35 00  5.3.f.5.
0060  36 00 33 00 30 00 64 00  6.3.0.d.
0068  2D 00 62 00 36 00 62 00  -.b.6.b.
0070  66 00 2D 00 31 00 31 00  f.-.1.1.
0078  64 00 30 00 2D 00 39 00  d.0.-.9.
0080  34 00 66 00 32 00 2D 00  4.f.2.-.
0088  30 00 30 00 61 00 30 00  0.0.a.0.
```

OK Cancel

My Computer\HKEY_LOCAL_MACHINE\SYSTEM\MountedDevices

Registry Forensics
USB Devices

Registry Editor

File Edit View Favorites Help

- Vid_413c&Pid_2002
- Vid_413c&Pid_20028MI_00
- Vid_413c&Pid_20028MI_01
- USBSTOR
  - Disk&Ven_&Prod_Memorex_TD_2B&Rev_1.07
  - Disk&Ven_&Prod_Secure_Guard&Rev_PMAP
  - Disk&Ven_&Prod_TS256MJFLASHA&Rev_1.00
  - Disk&Ven_&Prod_USB_DRIVE&Rev_2.00
  - Disk&Ven_&Prod_USB_Flash_Memory&Rev_1.00
  - Disk&Ven_ChipsBnk&Prod_Flash_Disk&Rev_2.00
  - Disk&Ven_Flash&Prod_Drive_SM_USB20&Rev_3000
  - Disk&Ven_Flash&Prod_Drive_UT_USB20&Rev_0.00
  - Disk&Ven_Generic&Prod_Flash_Disk&Rev_7.77
  - Disk&Ven_LEXAR&Prod_DIGITAL_FILM&Rev_/W1.
  - Disk&Ven_LEXAR&Prod_JUMPDRIVE&Rev_1.20
    - B1115318020208&0
  - Disk&Ven_LEXAR&Prod_JUMPDRIVE_SPORT&Rev_100
  - Disk&Ven_Prolific&Prod_USB_Flash_Disk&Rev_P1.0
  - Disk&Ven_SanDisk&Prod_Cruzer_Mini&Rev_0.2
  - Disk&Ven_Toshiba&Prod_USB_Memory&Rev_1.13
  - SFloppy&Ven_&Prod_Secure_Guard&Rev_PMAP
  - SFloppy&Ven_Y-E_DATA&Prod_USB-FDU&Rev_4.01

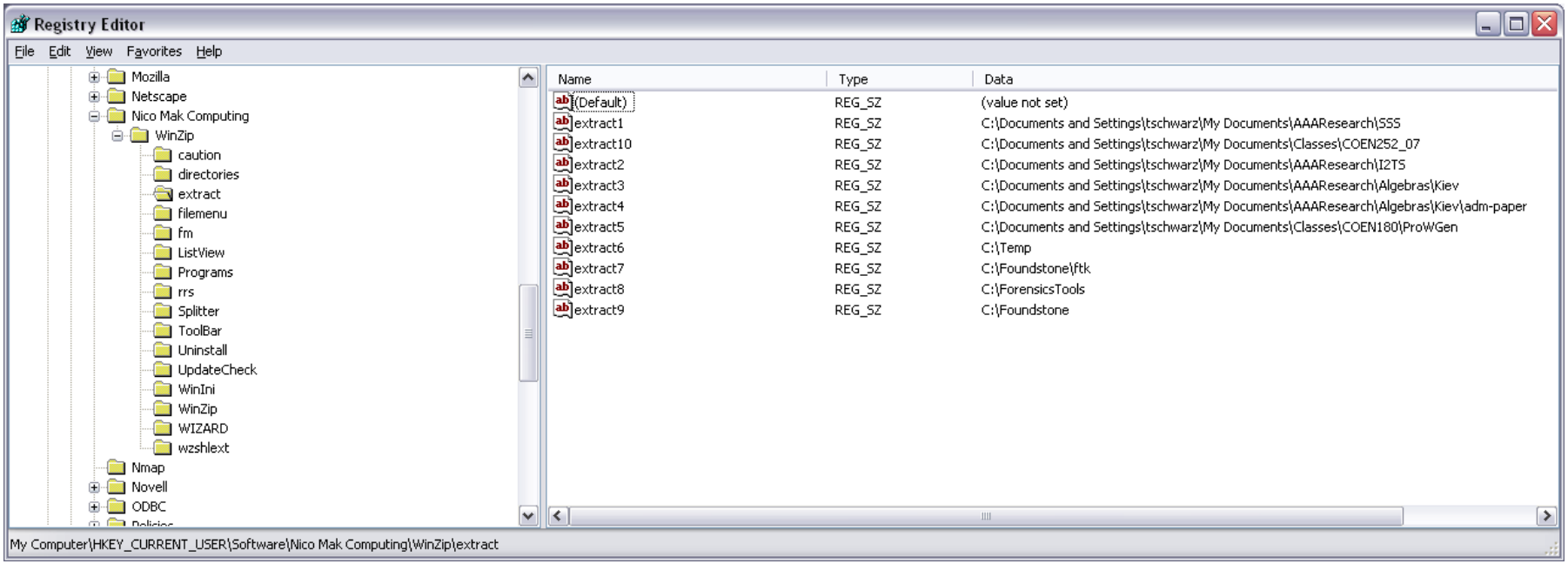
Name	Type	Data
(Default)	REG_SZ	(value not set)
Capabilities	REG_DWORD	0x00000010 (16)
Class	REG_SZ	DiskDrive
ClassGUID	REG_SZ	{4D36E967-E325-11CE-BFC1-08002BE10318}
CompatibleIDs	REG_MULTI_SZ	USBSTOR\Disk USBSTOR\RAW
ConfigFlags	REG_DWORD	0x00000000 (0)
DeviceDesc	REG_SZ	Disk drive
Driver	REG_SZ	{4D36E967-E325-11CE-BFC1-08002BE10318}\0020
FriendlyName	REG_SZ	LEXAR JUMPDRIVE USB Device
HardwareID	REG_MULTI_SZ	USBSTOR\DiskLEXAR___JUMPDRIVE_____1.20 USBSTOR\DiskLEXAR___JUMPI
Mfg	REG_SZ	(Standard disk drives)
ParentIdPrefix	REG_SZ	7&40500938&0
Service	REG_SZ	disk
UINumber	REG_DWORD	0x00000000 (0)

My Computer\HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Enum\USBSTOR\Disk&Ven_LEXAR&Prod_JUMPDRIVE&Rev_1.20\B1115318020208&0

Registry Forensics

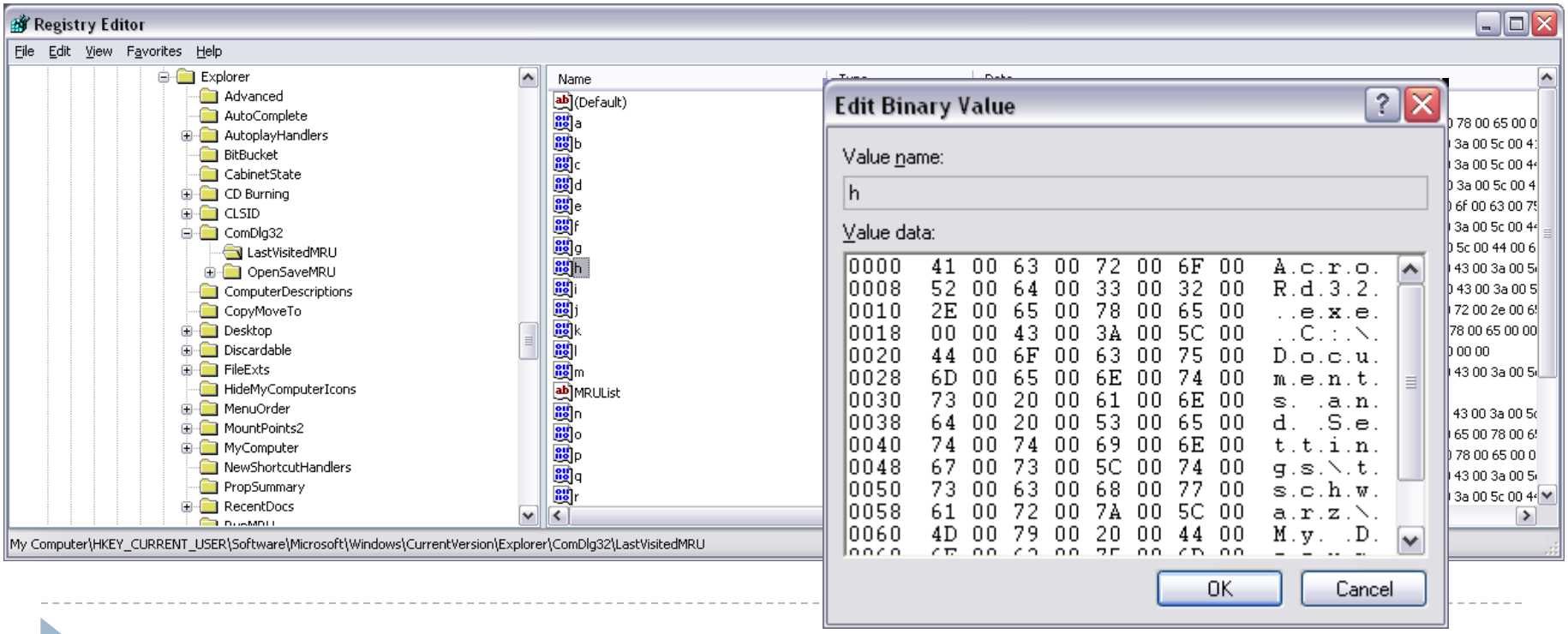
- Networking
  - Local groups
  - Local users
  - Map network drive MRU
  - Printers

Registry Forensics Winzip



Registry Forensics

List of applications and filenames of the most recent files opened in windows



Registry Forensics

Most recent saved (or copied) files

Registry Editor

File Edit View Favorites Help

OpenSaveMRU
- *
- bmp
- cgi
- conf
- cpp
- cpt
- dat
- doc
- dvi
- exe
- gif
- h
- HLP
- htm
- html
- ini
- jpg
- lnk
- log
- mac
- MDI
- nb

Name	Type	Data
(Default)	REG_SZ	(value not set)
a	REG_SZ	C:\Documents and Settings\tschwarz\My Documents\WebSites\Thomas Schwarz\coen350_07\index.html
b	REG_SZ	C:\Documents and Settings\tschwarz\My Documents\WebSites\Thomas Schwarz\coen252_07\homeworks\hw1.html
c	REG_SZ	C:\Temp\hi.html
d	REG_SZ	C:\Documents and Settings\tschwarz\My Documents\WebSites\Thomas Schwarz\coen1_07\Lectures\htmltables.html
e	REG_SZ	C:\Documents and Settings\tschwarz\My Documents\CV.html
f	REG_SZ	C:\Documents and Settings\tschwarz\My Documents\WebSites\Thomas Schwarz\coen1_07\index.html
g	REG_SZ	C:\Documents and Settings\tschwarz\My Documents\WebSites\Thomas Schwarz\coen351_2007\coen351_2007header.htm
h	REG_SZ	C:\Documents and Settings\tschwarz\My Documents\WebSites\Thomas Schwarz\coen351_07\LN\BeginningCGI.html
i	REG_SZ	C:\ApacheWS\doc\index.html
j	REG_SZ	C:\Documents and Settings\tschwarz\My Documents\WebSites\Thomas Schwarz\coen351_07\LN\CGI PM module.html
MRUList	REG_SZ	dcbajihgfe

My Computer\HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Explorer\ComDlg32\OpenSaveMRU\html

Registry Forensics

- System
  - Recent documents
  - Recent commands entered in Windows run box
  - Programs that run automatically
    - Startup software
    - Good place to look for Trojans

Registry Forensics

- User Application Data
  - Adobe products
  - IM contacts
  - Search terms in google
  - Kazaa data
  - Windows media player data
  - Word recent docs and user info
  - Access, Excel, Outlook, Powerpoint recent files

Registry Forensics

- Go to
  - Access Data's Registry Quick Find Chart

Registry Forensics

Case Study

(Chad Steel: Windows Forensics, Wiley)

Department manager alleges that individual copied confidential information on DVD.

No DVD burner was issued or found.

Laptop was analyzed.

Found USB device entry in registry:

PLEXTOR DVDR PX-708A

Found software key for Nero - Burning ROM in registry

Therefore, looked for and found Nero compilation files (.nrc). Found other compilation files, including ISO image files.

Image files contained DVD-format and AVI format versions of copyrighted movies.

Conclusion: No evidence that company information was burned to disk. However, laptop was used to burn copyrighted material and employee had lied.

Registry Forensics

- Intelliform:
  - Autocomplete feature for fast form filling
  - Uses values stored in the registry
    - HKEY_CURRENT_USER\Software\Microsoft\Protected Storage System Provider
    - Only visible to SYSTEM account
  - Accessible with tools such as Windows Secret Explorer.

Registry Forensics: AutoStart Viewer (DiamondCS)

DiamondCS Autostart Viewer 1.4 - Found 48

Main

Autostart File/Entry	Autostart Location
C:\WINDOWS\Explorer.exe	c:\windows\system.ini [boot]\shell
C:\WINDOWS\Explorer.exe	HKLM\Software\Microsoft\Windows NT\CurrentVersion\Winlogon\Shell
C:\WINDOWS\System32\WScript.exe "%1" %*	HKCR\vbsfile\shell\open\command\
C:\WINDOWS\System32\WScript.exe "%1" %*	HKCR\vbefile\shell\open\command\
C:\Program Files\Macromedia\Dreamweaver MX\Dream...	HKCR\jsfile\shell\open\command\
C:\WINDOWS\System32\WScript.exe "%1" %*	HKCR\jsefile\shell\open\command\
C:\WINDOWS\System32\WScript.exe "%1" %*	HKCR\wshfile\shell\open\command\
C:\WINDOWS\System32\WScript.exe "%1" %*	HKCR\wsffile\shell\open\command\
C:\WINDOWS\ATK0100\Hcontrol.exe	HKLM\Software\Microsoft\Windows\CurrentVersion\Run\Hcontrol
C:\Program Files\Apoint\Apoint.exe	HKLM\Software\Microsoft\Windows\CurrentVersion\Run\Apoint
C:\Program Files\ATI Technologies\ATI Control Panel\at...	HKLM\Software\Microsoft\Windows\CurrentVersion\Run\ATIPTA
C:\WINDOWS\system32\ICO.EXE	HKLM\Software\Microsoft\Windows\CurrentVersion\Run\Mouse Suite 98 Daemon
C:\Program Files\Java\jre1.5.0_10\bin\jusched.exe	HKLM\Software\Microsoft\Windows\CurrentVersion\Run\SunJavaUpdateSched
C:\Program Files\Sony\VAIO Power Management\SPMg...	HKLM\Software\Microsoft\Windows\CurrentVersion\Run\SonyPowerCfg
C:\Program Files\Sony\HotKey Utility\HKserv.exe	HKLM\Software\Microsoft\Windows\CurrentVersion\Run\HKSERV.EXE
C:\Program Files\Sony\Wireless Switch Setting Utility\S...	HKLM\Software\Microsoft\Windows\CurrentVersion\Run\Switcher.exe
C:\Program Files\Sony\ISB Utility\ISBMgr.exe	HKLM\Software\Microsoft\Windows\CurrentVersion\Run\ISBMgr.exe
C:\Program Files\Sony\VAIO Update 2\VAIOUpdt.exe	HKLM\Software\Microsoft\Windows\CurrentVersion\Run\VAIO Update 2
rundll32.exe bthprops.cpl,,BluetoothAuthenticationAgent	HKLM\Software\Microsoft\Windows\CurrentVersion\Run\BluetoothAuthenticationAgent
C:\WINDOWS\Sonysys\VAIO Recovery\PartSeal.exe	HKLM\Software\Microsoft\Windows\CurrentVersion\Run\VAIO Recovery
C:\Program Files\Common Files\Real\Update_OB\realsc...	HKLM\Software\Microsoft\Windows\CurrentVersion\Run\TkBellExe
C:\Program Files\iTunes\iTunesHelper.exe	HKLM\Software\Microsoft\Windows\CurrentVersion\Run\iTunesHelper
C:\Program Files\QuickTime\qttask.exe	HKLM\Software\Microsoft\Windows\CurrentVersion\Run\QuickTime Task
C:\Program Files\Messenger\msmsgs.exe	HKCU\Software\Microsoft\Windows\CurrentVersion\Run\MSMSGS
C:\WINDOWS\system32\ctfmon.exe	HKCU\Software\Microsoft\Windows\CurrentVersion\Run\ctfmon.exe
C:\Program Files\Google\GoogleToolbarNotifier\1.0.720....	HKCU\Software\Microsoft\Windows\CurrentVersion\Run\swg
C:\WINDOWS\system32\SHELL32.dll	HKLM\Software\Microsoft\Windows\CurrentVersion\ShellServiceObjectDelayLoad\
C:\WINDOWS\system32\SHELL32.dll	HKLM\Software\Microsoft\Windows\CurrentVersion\ShellServiceObjectDelayLoad\
C:\WINDOWS\system32\webcheck.dll	HKLM\Software\Microsoft\Windows\CurrentVersion\ShellServiceObjectDelayLoad\
C:\WINDOWS\system32\stobject.dll	HKLM\Software\Microsoft\Windows\CurrentVersion\ShellServiceObjectDelayLoad\
C:\WINDOWS\system32\upnpui.dll	HKLM\Software\Microsoft\Windows\CurrentVersion\ShellServiceObjectDelayLoad\
C:\Program Files\OpenOffice.org 2.1\program\quickstart...	C:\Documents and Settings\tschwarz\Start Menu\Programs\Startup\OpenOffice.org 2.1.lnk
C:\Program Files\Adobe\Acrobat 7.0\Reader\reader_sl....	C:\Documents and Settings\All Users\Start Menu\Programs\Startup\Adobe Reader Speed Launch.lnk
C:\Program Files\Sophos\AutoUpdate\ALMon.exe	C:\Documents and Settings\All Users\Start Menu\Programs\Startup\AutoUpdate Monitor.lnk
C:\Apache\bin\ApacheMonitor.exe	C:\Documents and Settings\All Users\Start Menu\Programs\Startup\Monitor Apache Servers.lnk
C:\Program Files\WinZip\WZQKPICK.EXE	C:\Documents and Settings\All Users\Start Menu\Programs\Startup\WinZip Quick Pick.lnk
autocheck autochk *	HKLM\System\CurrentControlSet\Control\Session Manager\BootExecute
C:\WINDOWS\system32\userinit.exe	HKLM\SOFTWARE\Microsoft\Windows NT\CurrentVersion\Winlogon\Userinit
C:\WINDOWS\system32\ntvdm.exe	HKLM\System\CurrentControlSet\Control\WOW\cmdline
C:\WINDOWS\system32\ntvdm.exe -a %SystemRoot%\...	HKLM\System\CurrentControlSet\Control\WOW\wowcmdline
C:\WINDOWS\system32\mswsock.dll	HKLM\System\CurrentControlSet\Services\Winsock2\Parameters\Protocol_Catalog9\Catalog_Entries\
C:\WINDOWS\system32\rsvpsp.dll	HKLM\System\CurrentControlSet\Services\Winsock2\Parameters\Protocol_Catalog9\Catalog_Entries\

http://www.diamondcs.com.au

Registry Research

- Use REGMON (MS Sysinternals) to monitor changes to the registry
  - Registry is accessed constantly
    - Need to set filter
    - Or enable Regmon's log boot record
      - Captures registry activity in a regmon file
- Do it yourself: Windows API
  - RegNotifyChangeKeyValue
- Many commercial products
  - DiamondCS RegProt
    - Intercepts changes to the registry

Registry Forensics Investigation

- Forensics tools allow registry investigation from image of drive
- Differences between life and offline view
  - No HARDWARE hive (HKLM)
    - Dynamic key, created at boot
  - No virtual keys such as HKEY_CURRENT_USER
    - Derived from SID key under HKEY_USERS
    - Source file is NTUSER.DAT
  - Do not confuse current and repair versions of registry files
    - %SystemRoot%\system32\config (TRUE registry)
    - %SystemRoot%\repair (repair version of registry)

Registry Forensics Investigation

- Forensics search can reveal backups of registry
  - Intruders leave these behind when resetting registry in order not to damage system

Registry Forensics Investigation

- Time is Universal Time Coordinated
  - a.k.a. Zulu
  - a.k.a Greenwhich Time

Registry Forensics Investigation

- Software Key
  - Installed Software
    - Registry keys are usually created with installation
    - But not deleted when program is uninstalled
    - Find them
      - Root of the software key
        - Beware of bogus names
      - HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\App Paths
      - HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Uninstall
    - If suspicious, use information from the registry to find the actual code
    - Registry time stamps will confirm the file MAC data or show them to be altered

Registry Forensics Investigation

- Software Key
  - Last Logon
    - HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows NT\CurrentVersion\WinLogon
  - Logon Banner Text / Legal Notice
    - HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows NT\CurrentVersion\WinLogon
  - Security Center Settings
    - HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Security Center
    - HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\SharedAccess\Parameters\FirewallPolicy
      - If firewall logging is enabled, the log is typically at %SystemRoot%/pfirewall.log

Registry Forensics Investigation

Registry Editor

File Edit View Favorites Help

- seclogon
- SENS
- Serial
- ServiceModelEndpoint 3.0.0.0
- ServiceModelOperation 3.0.0.0
- ServiceModelService 3.0.0.0
- Sfloppy
- SharedAccess
  - Enum
  - Epoch
  - Parameters
    - FirewallPolicy
      - DomainProfile
      - StandardProfile
        - AuthorizedApplications
          - List
        - GloballyOpenPorts
          - List
        - IcmpSettings
  - Setup
- ShellHWDetection
- Simbad
- SimpTcp
- SLIP
- SMSvcHost 3.0.0.0
- SMTPSVC
- SNC
- SNMP
- SNMPTRAP
- SONYTVC
- Sophos Agent
- Sophos AutoUpdate Service
- Sophos Message Router
- Sparrow
- SPI

Name	Type	Data
(Default)	REG_SZ	(value not set)
%windir%\Network Diagnostic\xpnetdia...	REG_SZ	%windir%\Network Diagnostic\xpnetdiag.exe:*:Enabled:@xpsp3res.dll,-20000
%windir%\system32\sessmgr.exe	REG_SZ	%windir%\system32\sessmgr.exe:*:enabled:@xpsp2res.dll,-22019
C:\Apache\bin\httpd.exe	REG_SZ	C:\Apache\bin\httpd.exe:*:Enabled:Apache HTTP Server
C:\ForensicsTools\nc.exe	REG_SZ	C:\ForensicsTools\nc.exe:*:Enabled:nc.exe
C:\Novell\GroupWise\grpwise.exe	REG_SZ	C:\Novell\GroupWise\grpwise.exe:*:Enabled:GroupWise
C:\Novell\GroupWise\notify.exe	REG_SZ	C:\Novell\GroupWise\notify.exe:*:Enabled:GroupWise Notify
C:\Program Files\Apache Group\Apache...	REG_SZ	C:\Program Files\Apache Group\Apache2\bin\Apache.exe:*:Enabled:Apache HTTP Server
C:\Program Files\Apache Software Foun...	REG_SZ	C:\Program Files\Apache Software Foundation\Apache2.2\bin\httpd.exe:*:Enabled:Apache HTTP Server
C:\Program Files\ForensicsTools\attacke...	REG_SZ	C:\Program Files\ForensicsTools\attacker.exe:*:Enabled:attacker
C:\Program Files\iTunes\iTunes.exe	REG_SZ	C:\Program Files\iTunes\iTunes.exe:*:Enabled:iTunes
C:\Program Files\Macromedia\Dreamwe...	REG_SZ	C:\Program Files\Macromedia\Dreamweaver MX\Dreamweaver.exe:*:Enabled:Dreamweaver MX
C:\Program Files\Maxis\SimCity 3000 Unl...	REG_SZ	C:\Program Files\Maxis\SimCity 3000 Unlimited\Apps\Updater\UPDATER.EXE:*:Enabled:SC3UpdaterMFC
C:\Program Files\Messenger\msmsgs.exe	REG_SZ	C:\Program Files\Messenger\msmsgs.exe:*:Enabled:Windows Messenger
C:\Program Files\MSN Messenger\livecall...	REG_SZ	C:\Program Files\MSN Messenger\livecall.exe:*:Enabled:Windows Live Messenger 8.1 (Phone)
C:\Program Files\MSN Messenger\msnca...	REG_SZ	C:\Program Files\MSN Messenger\msncall.exe:*:Enabled:Windows Live Messenger 8.0 (Phone)
C:\Program Files\MSN Messenger\msnm...	REG_SZ	C:\Program Files\MSN Messenger\msnmsgr.exe:*:Enabled:Windows Live Messenger 8.1
C:\Program Files\Paros\IEEmbed.exe	REG_SZ	C:\Program Files\Paros\IEEmbed.exe:*:Enabled:JDesktop Integration Components binary
C:\Program Files\QuickTime\QuickTimePl...	REG_SZ	C:\Program Files\QuickTime\QuickTimePlayer.exe:*:Enabled:QuickTime Player
C:\Program Files\Real\RealPlayer\realpl...	REG_SZ	C:\Program Files\Real\RealPlayer\realplay.exe:*:Enabled:RealPlayer
C:\Program Files\Skype\Phone\Skype.exe	REG_SZ	C:\Program Files\Skype\Phone\Skype.exe:*:Enabled:Skype
C:\Program Files\Sony\VAIO Media 4.0\...	REG_SZ	C:\Program Files\Sony\VAIO Media 4.0\Vc.exe:*:Disabled:[VAIO Media] VAIO Media
C:\Program Files\Wolfram Research\Mat...	REG_SZ	C:\Program Files\Wolfram Research\Mathematica\5.2\math.exe:*:Enabled:math.exe
C:\Program Files\Wolfram Research\Mat...	REG_SZ	C:\Program Files\Wolfram Research\Mathematica\5.2\Mathematica.exe:*:Enabled:Mathematica 5.2
C:\Program Files\Wolfram Research\Mat...	REG_SZ	C:\Program Files\Wolfram Research\Mathematica\5.2\MathKernel.exe:*:Enabled:Mathematica 5.2 Kernel
C:\WINDOWS\Stuff\svchost.exe	REG_SZ	C:\WINDOWS\Stuff\svchost.exe:*:Enabled:svchost
C:\WINDOWS\system32\dpvsetup.exe	REG_SZ	C:\WINDOWS\system32\dpvsetup.exe:*:Enabled:Microsoft DirectPlay Voice Test
C:\WINDOWS\system32\ftp.exe	REG_SZ	C:\WINDOWS\system32\ftp.exe:*:Enabled:File Transfer Program
C:\WINDOWS\system32\rundll32.exe	REG_SZ	C:\WINDOWS\system32\rundll32.exe:*:Enabled:Run a DLL as an App

My Computer\HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\SharedAccess\Parameters\FirewallPolicy\StandardProfile\Authori

Registry Forensics Investigation

- Analyze Restore Point Settings
  - Restore points developed for Win ME / XP
  - Restore point settings at
    - HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows NT\CurrentVersion\SystemRestore
  - Restore points created every RPGlobalInterval value seconds (~every 24h)
  - Retention period is RPLifeInterval seconds (default 90 days)
  - Restore point taking in ON by default
  - Restore points in System Volume Information\restore…

Registry Forensics Investigation

- Aside: How to access restore points
  - Restore points are protected from user, including administrator
  - Administrator can add her/himself to the access list of the system volume directory
    - Turn off "Use simple file sharing" in Control Panel → Folder Options
    - Click on "Properties" of the directory in Explorer and

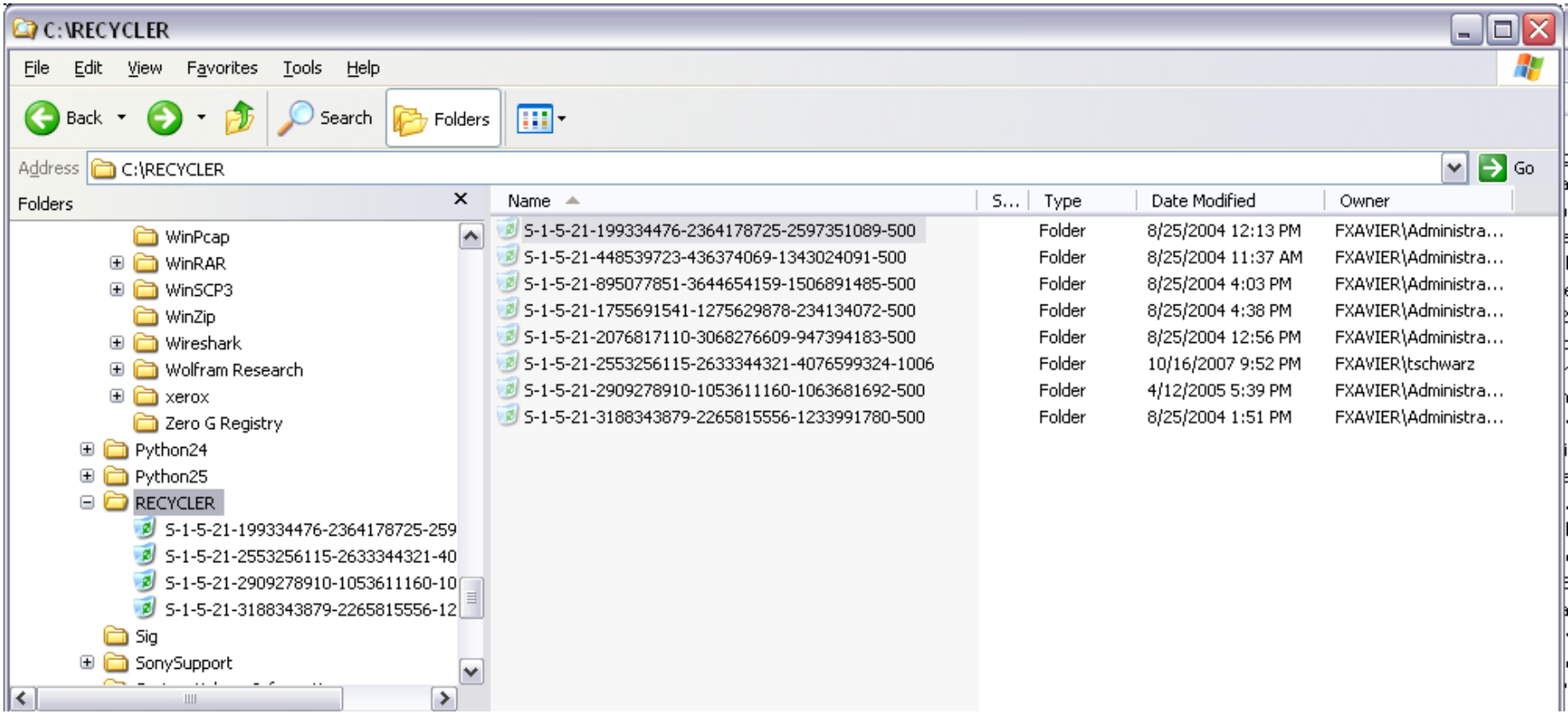
Registry Forensics Investigation

- Restore point
  - makes copies of important system and program files that were added since the last restore points
    - Files
      - Stored in root of RP#### folder
      - Names have changed
      - File extension is unchanged
      - Name changes kept in change.log file
    - Registry data
      - in Snapshot folder
      - Names have changed, but predictably so

Registry Forensics Investigation

- SID (security identifier)
  - Well-known SIDs
    - SID: S-1-0 Name: Null Authority
    - SID: S-1-5-2 Name: Network
  - S-1-5-21-2553256115-2633344321-4076599324-1006
    - S string is SID
    - 1 revision number
    - 5 authority level (from 0 to 5)
    - 21-2553256115-2633344321-4076599324 domain or local computer identifier
    - 1006 RID – Relative identifier
- Local SAM resolves SID for locally authenticated users (not domain users)
  - Use recycle bin to check for owners

Registry Forensics Investigation



Resolving local SIDs through the Recycle Bin

(life view)

Registry Forensics Investigation

- Protected Storage System Provider data
  - Located in NTUSER.DAT\Software\Microsoft\ Protected Storage System Provider
  - Various tools will reveal contents
    - Forensically, AccessData Registry Viewer
    - Secret Explorer
    - Cain & Abel
    - Protected Storage PassView v1.63

Registry Forensics Investigation

- MRU: Most Recently Used
  - HKEY_CURRENT_USER\SOFTWARE\Microsoft\Windows\CurrentVersion\Exlorer\RunMRU
  - HKEY_CURRENT_USER\SOFTWARE\Microsoft\Windows\CurrentVersion\Exlorer\Map Network Drive MRU
  - HKEY_CURRENT_USER\Printers\Settings\Wizard\ConnectMRU
  - HKEY_CURRENT_USER\SOFTWARE\Microsoft\Windows\CurrentVersion\Exlorer\ComDlg32
    - Programs and files opened by them
    - Files opened and saved
  - HKEY_CURRENT_USER\SOFTWARE\Microsoft\Search Assistant\ACMru

Registry Forensics Investigation

Registry Editor

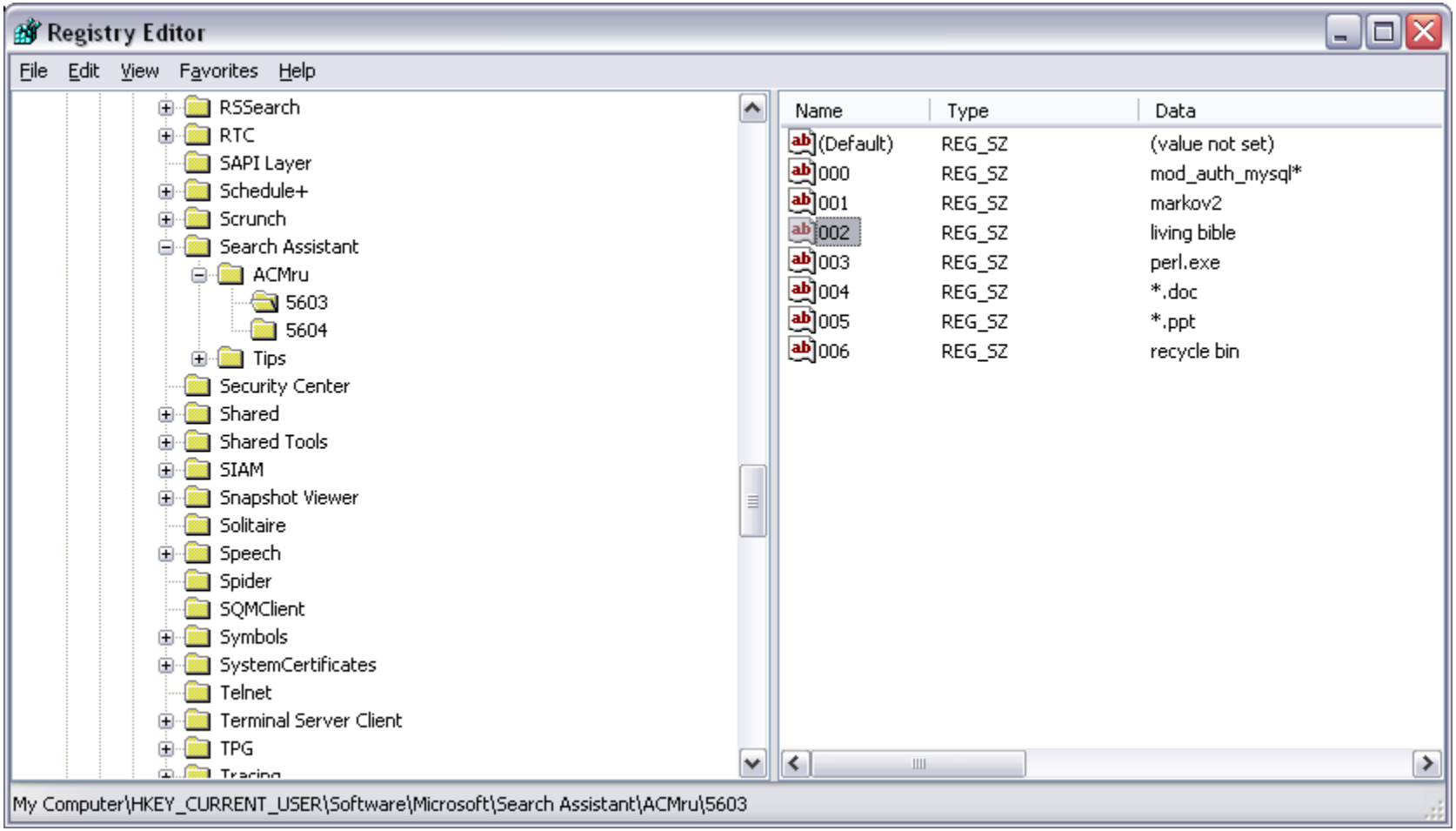
File Edit View Favorites Help

OpenSaveMRU
- *
- 001
- aux
- avi
- avt
- bmp
- cgi
- cls
- conf
- cpp
- cpt
- dat
- doc
- dvi
- emf
- exe
- gif
- h
- hdb
- HLP
- htm
- html
- ini
- jpg
- lnk
- log
- mac
- MDI
- nb
- ncb
- ns1
- out
- pdf
- php

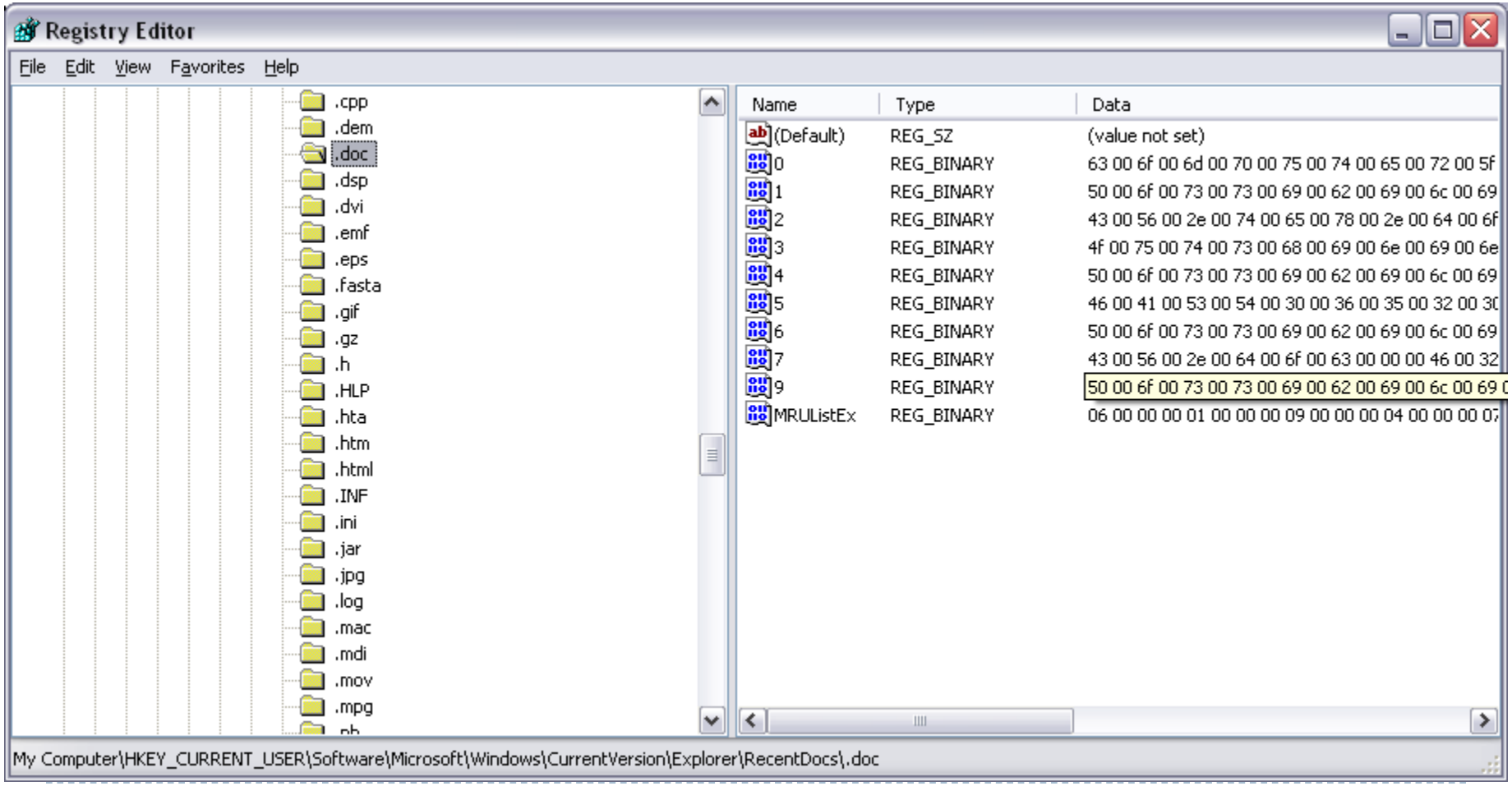
Name	Type	Data
(Default)	REG_SZ	(value not set)
a	REG_SZ	C:\Documents and Settings\tschwarz\Desktop\alexander.html
b	REG_SZ	C:\Documents and Settings\tschwarz\My Documents\WebSites\Thomas Schwarz\COEN250_07\HW\hw2.html
c	REG_SZ	C:\Documents and Settings\tschwarz\My Documents\WebSites\Thomas Schwarz\COEN250_07\HW\hw3.html
d	REG_SZ	C:\Documents and Settings\tschwarz\My Documents\WebSites\Thomas Schwarz\coen252_07Fall\ClassMaterials\phishOctober12007.html
e	REG_SZ	C:\Documents and Settings\tschwarz\My Documents\WebSites\Thomas Schwarz\coen252_07Fall\syllabus.html
f	REG_SZ	C:\Documents and Settings\tschwarz\My Documents\WebSites\Thomas Schwarz\coen252_07Fall\ClassMaterials\phishOctober12007a.html
g	REG_SZ	C:\Documents and Settings\tschwarz\My Documents\WebSites\Thomas Schwarz\Preview Day\index.html
h	REG_SZ	C:\Documents and Settings\tschwarz\My Documents\WebSites\Thomas Schwarz\coen252_07Fall\ClassMaterials\phishOctober12007b.html
i	REG_SZ	C:\Documents and Settings\tschwarz\My Documents\WebSites\Thomas Schwarz\COEN250_07\HW\hw4.html
j	REG_SZ	C:\Documents and Settings\tschwarz\My Documents\AAAResearch\Disk Layouts\INS.html
MRUList	REG_SZ	gihfdecbaj

My Computer\HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Explorer\ComDlg32\OpenSaveMRU\html

Registry Forensics Investigation



Registry Forensics Investigation



Registry Forensics Investigation

Registry Editor

File Edit View Favorites Help

- FIRAXIS
- Friendly Technologies
- Google
  - CommonSettings
  - CustomSearch
  - Google Earth Plus
  - Google Toolbar
  - GoogleToolbarNotifier
  - KeyholeCommonSettings
  - NavClient
    - 1.1
      - History
      - Options
      - RunOnce
      - Usage
      - whitelist
- HPS
- IADirectShow
- IM Providers
- Intel
- InterActual Technologies
- InterVideo
- JavaSoft
- Lake
- LeaderTech
- LicenseManager
- Logitech
- LuckaSoft

Name	Type	Data
(Default)	REG_SZ	(value not set)
asobrain	REG_BINARY	56 e3 0c 45
truth about beef jerky	REG_BINARY	18 e1 67 43
windows update	REG_BINARY	27 8f d5 42

DCode Date v2.07.000 written by Craig Wilson

Time Zone: UTC 00:00 — Window on top

Decode Format: Unix: 32 bit Hex Value - Little Endian

Value to Decode: 56E30C45

Date & Time: Sun, 17 September 2006 05:55:34 UTC

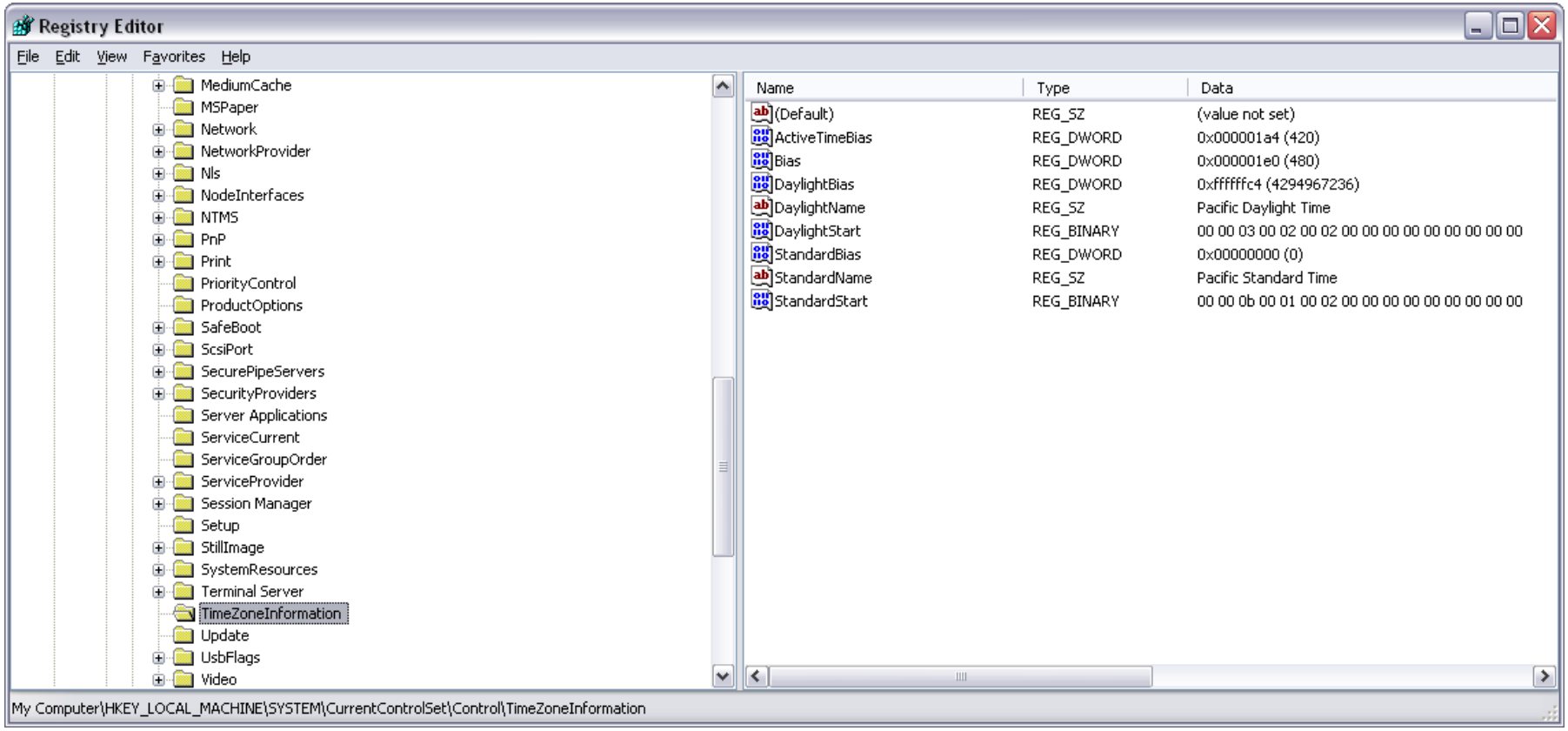
www.digital-detective.co.uk — Cancel — Clear — Decode

My Computer\HKEY_CURRENT_USER\Software\Google\NavClient\1.1\History

Registry Forensics Investigation

- HKEY_CURRENT_USER\SOFTWARE\Microsoft\Windows\CurrentVersion\Exlorer\UserAssist\{*********}\Count
  - ROT-13 encoding of data used to populate the User Assist Area of the start button
    - Contains most recently used programs

Registry Forensics Investigation



Registry Forensics Investigation

- AutoRun Programs
  - Long list of locations in registry
  - Long list of locations outside the registry
    - SystemDrive\autoexec.bat
    - SystemDrive\config.exe
    - Windir\wininit.ini
    - Windir\winstart.bat
    - Windir\win.ini
    - Windir\system.ini
    - Windir\dosstart.bat
    - Windir\system\autoexec.nt
    - Windir\system\config.nt
    - Windir\system32\autochk.exe

Registry Forensics Investigation

- Rootkit Enabler
  - Attacker can use AppInit_DLL key to run own DLL.