Windows Artifacts Exercise

BitCuratorEdu
Last Updated: January 18, 2022

About This Exercise

Author
Cal Lee

Description
This hands-on exercise introduces students to forensic artifacts produced by Windows operating systems and tools to analyze them. These slides are excerpted from Cal Lee's SAA "Advanced Digital Forensics" class. The sample data referenced in these slides is available here:
https://github.com/BitCurator/bcc-dfa-sample-data/

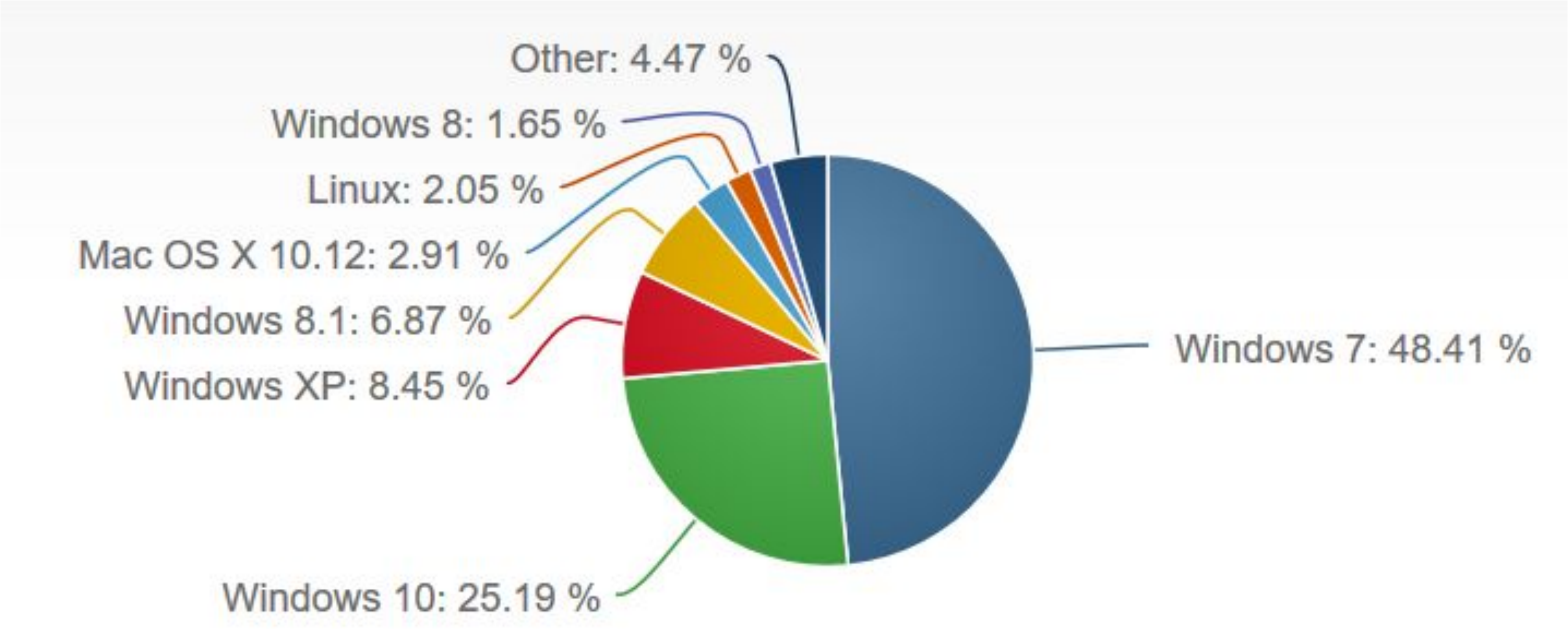
Learning object type
Lesson plan/materials

Learning objectives
This learning object might be used in a lesson to satisfy the following learning objectives:

- Practice using tools in the BitCurator Environment.

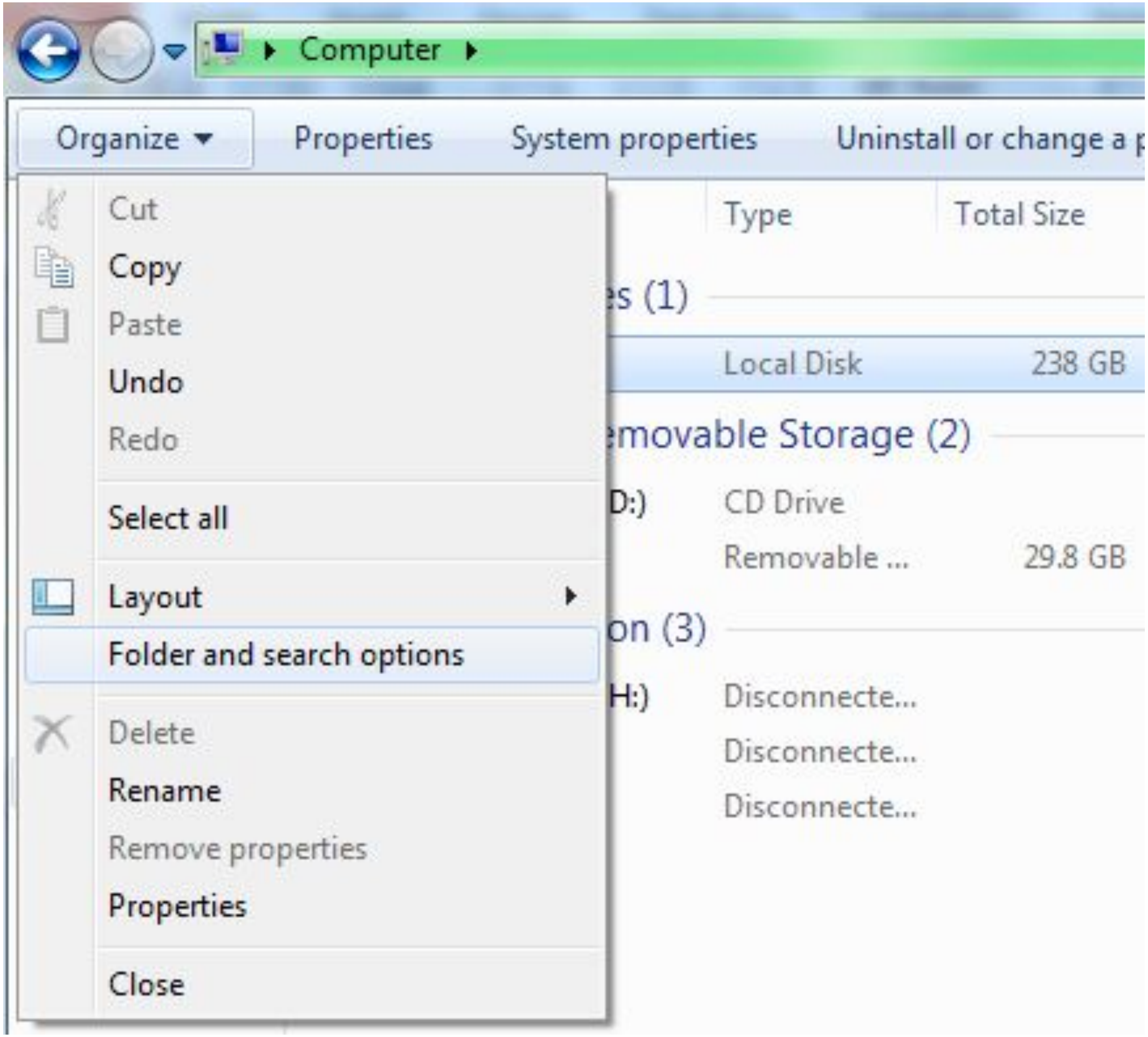
Windows Artifacts

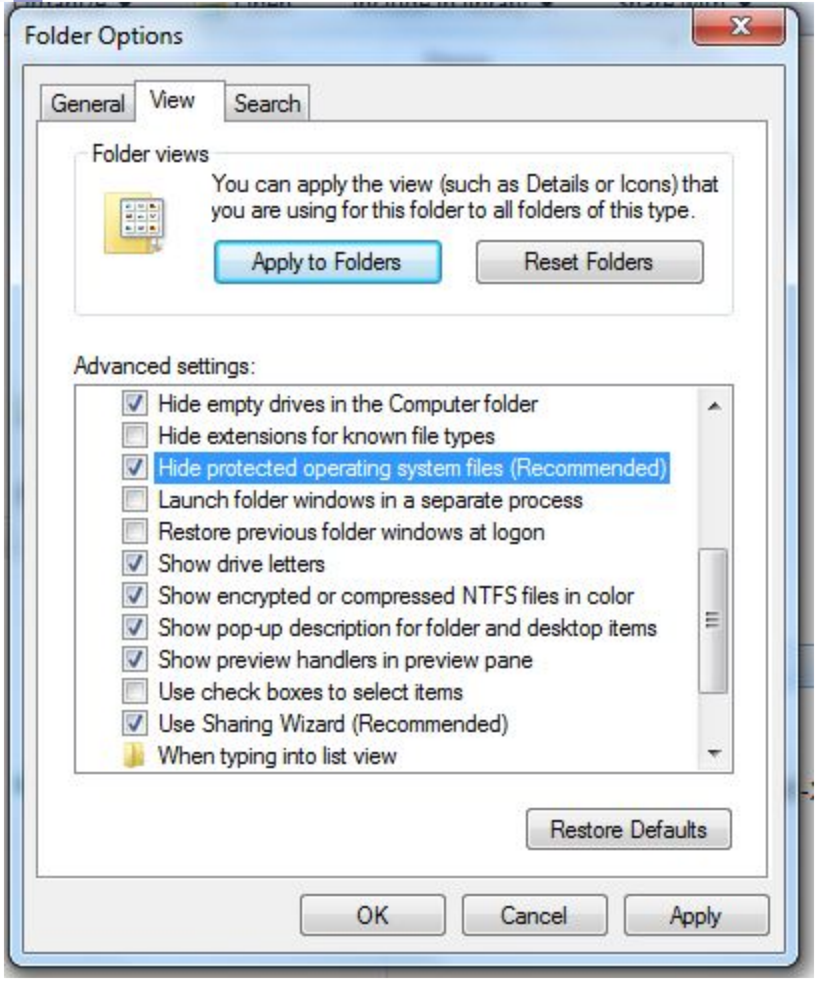
Desktop Operating System Market Share



https://www.netmarketshare.com/operating-system-market-share.aspx

Let’s make sure you can see all of the files on your computer.


Computer
Organize
Properties
System properties
Uninstall or change a p
Cut
Copy
Paste
Undo
Redo
Select all
Layout
Folder and search options
Delete
Rename
Remove properties
Properties
Close
Type
Total Size
s (1)
Local Disk
238 GB
movable Storage (2)
D:)
CD Drive
Removable ...
29.8 GB
on (3)
H:)
Disconnecte...
Disconnecte...
Disconnecte...

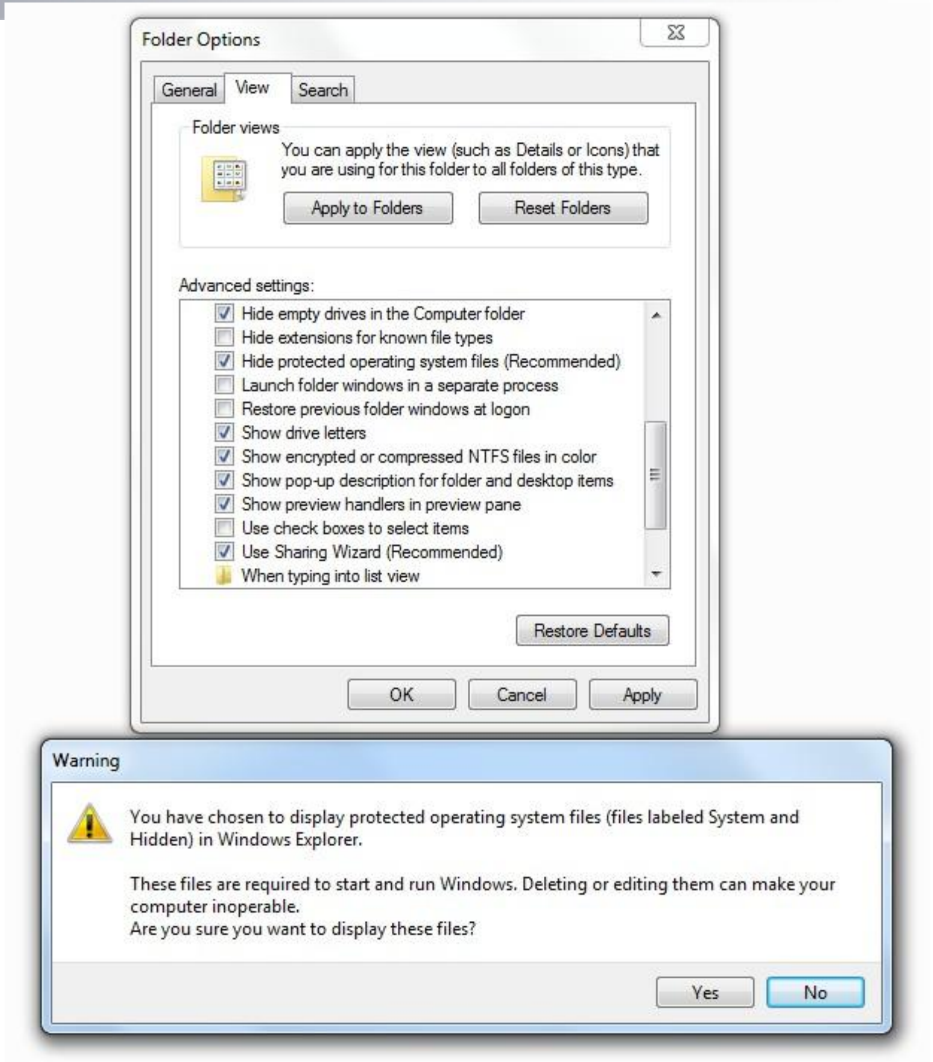


Folder views

You can apply the view (such as Details or Icons) that you are using for this folder to all folders of this type.

Advanced settings:

- ☑ Hide empty drives in the Computer folder
- ☐ Hide extensions for known file types
- ☑ Hide protected operating system files (Recommended)
- ☐ Launch folder windows in a separate process
- ☐ Restore previous folder windows at logon
- ☑ Show drive letters
- ☑ Show encrypted or compressed NTFS files in color
- ☑ Show pop-up description for folder and desktop items
- ☑ Show preview handlers in preview pane
- ☐ Use check boxes to select items
- ☑ Use Sharing Wizard (Recommended)
- When typing into list view



Folder views

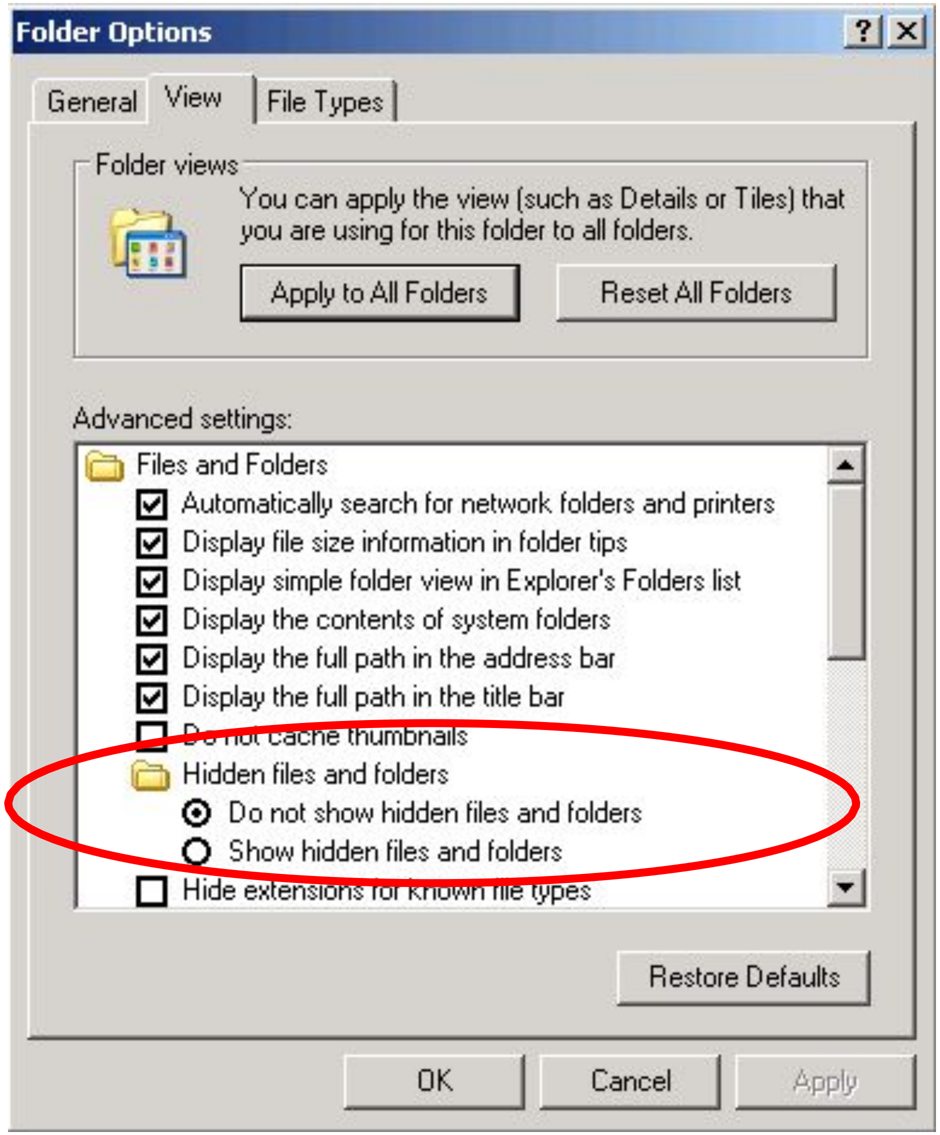
You can apply the view (such as Details or Icons) that you are using for this folder to all folders of this type.

Advanced settings:

- ☑ Hide empty drives in the Computer folder
- ☐ Hide extensions for known file types
- ☑ Hide protected operating system files (Recommended)
- ☐ Launch folder windows in a separate process
- ☐ Restore previous folder windows at logon
- ☑ Show drive letters
- ☑ Show encrypted or compressed NTFS files in color
- ☑ Show pop-up description for folder and desktop items
- ☑ Show preview handlers in preview pane
- ☐ Use check boxes to select items
- ☑ Use Sharing Wizard (Recommended)
- When typing into list view

You have chosen to display protected operating system files (files labeled System and Hidden) in Windows Explorer.

These files are required to start and run Windows. Deleting or editing them can make your computer inoperable.
Are you sure you want to display these files?



Folder Options

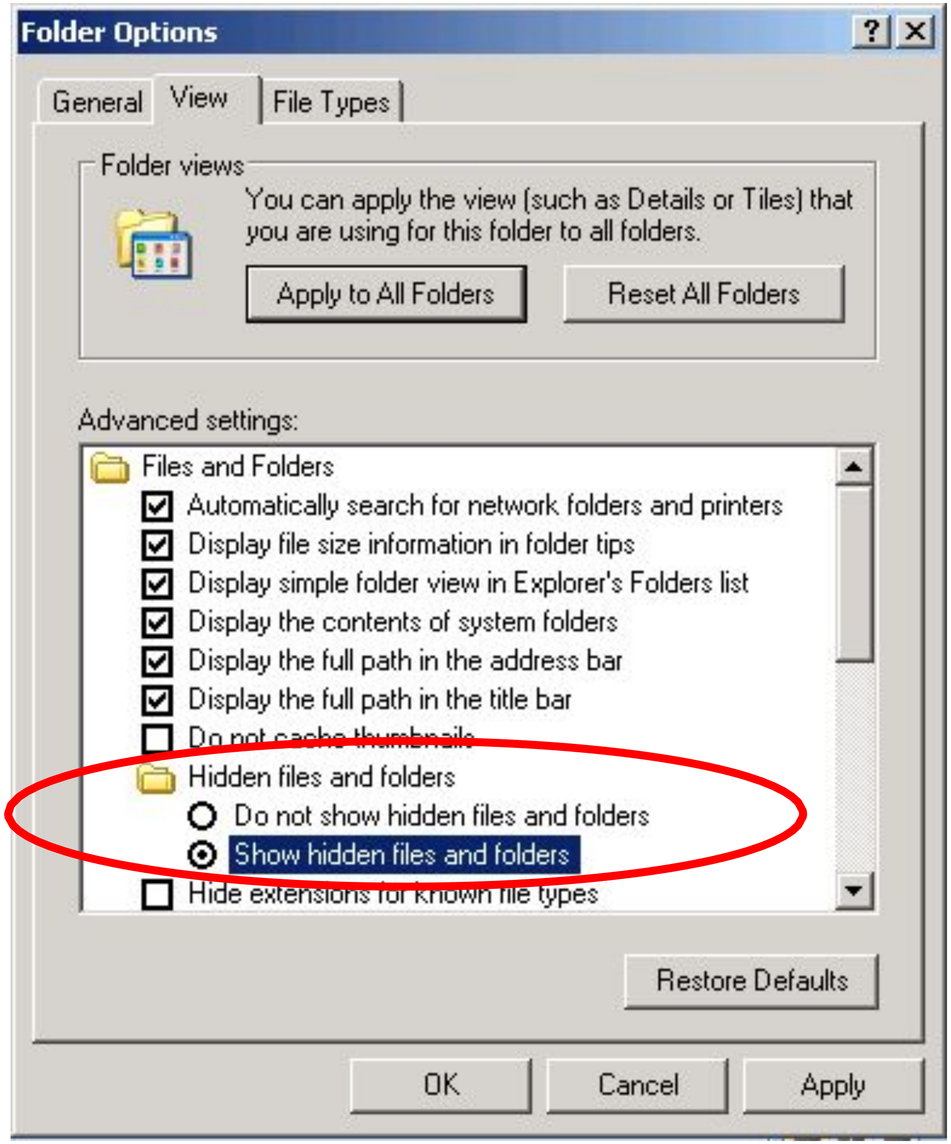
General | View | File Types

Folder views

You can apply the view (such as Details or Tiles) that you are using for this folder to all folders.

Advanced settings:

- Files and Folders
  - ☑ Automatically search for network folders and printers
  - ☑ Display file size information in folder tips
  - ☑ Display simple folder view in Explorer's Folders list
  - ☑ Display the contents of system folders
  - ☑ Display the full path in the address bar
  - ☑ Display the full path in the title bar
  - □ Do not cache thumbnails
  - Hidden files and folders
    - ● Do not show hidden files and folders
    - ○ Show hidden files and folders
  - □ Hide extensions for known file types



Folder Options

General | View | File Types

Folder views

You can apply the view (such as Details or Tiles) that you are using for this folder to all folders.

Advanced settings:

- Files and Folders
  - ☑ Automatically search for network folders and printers
  - ☑ Display file size information in folder tips
  - ☑ Display simple folder view in Explorer's Folders list
  - ☑ Display the contents of system folders
  - ☑ Display the full path in the address bar
  - ☑ Display the full path in the title bar
  - □ Do not cache thumbnails
  - Hidden files and folders
    - ○ Do not show hidden files and folders
    - ● Show hidden files and folders
  - □ Hide extensions for known file types

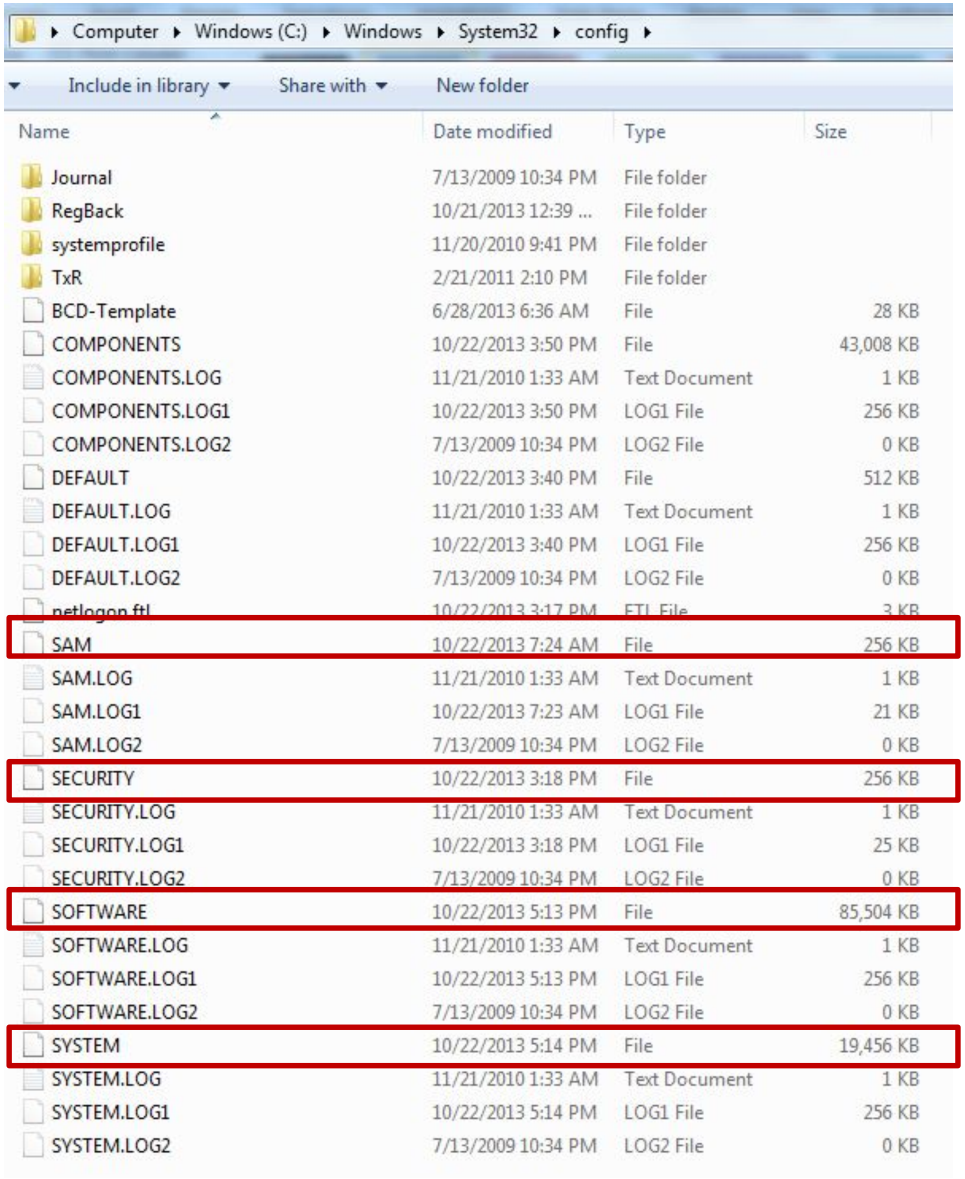
Windows Registry

- Information about:
  - Applications installed
  - Application settings
  - Hardware installed
  - Hardware settings
  - User interface and system preferences
  - User accounts
  - Locations of files and recent activities, e.g. Most Recently Used (MRU)
  - Lots of online activities, e.g. user names and passwords, browsing and search query history

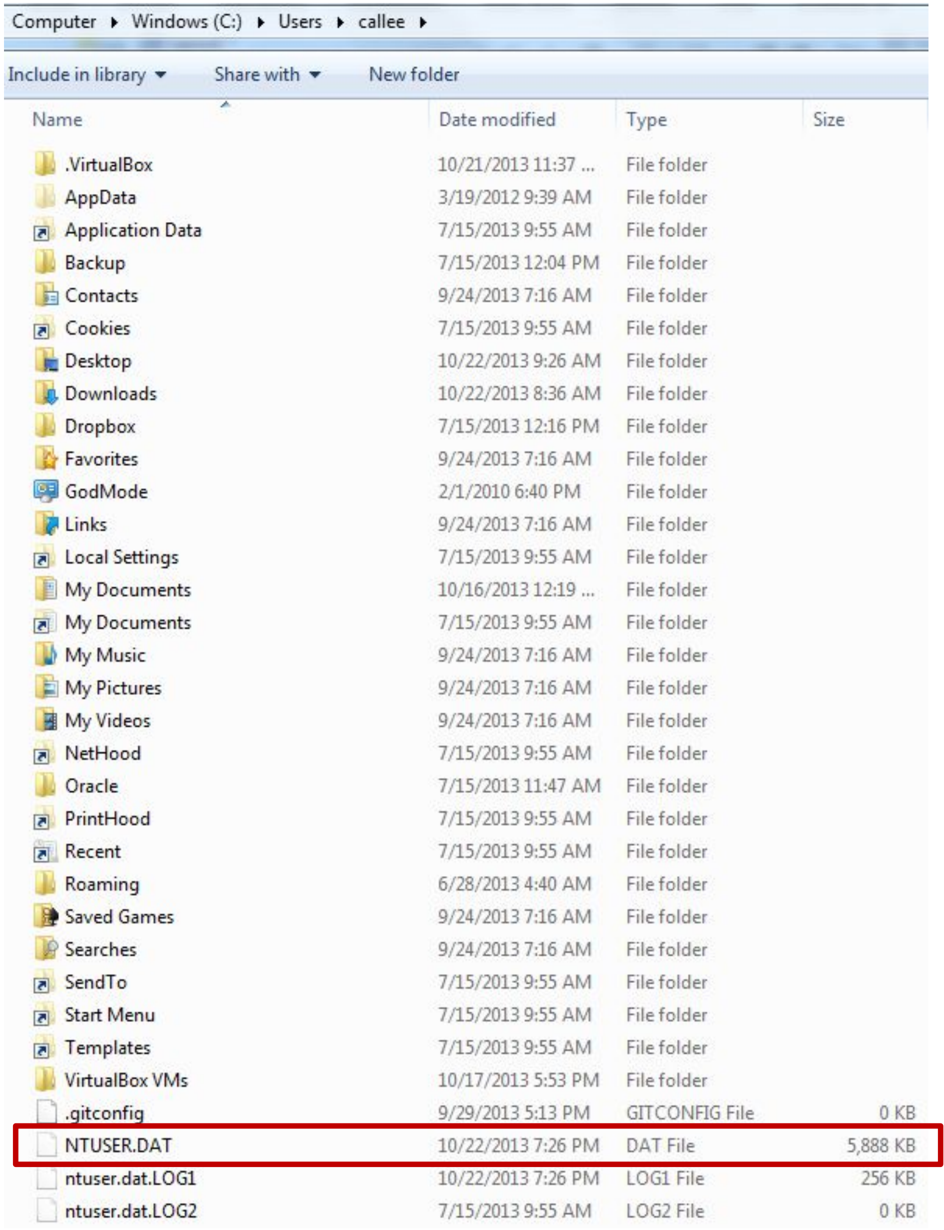
Five Main Registry Files

File	Description
NTUSER.DAT	One for each user account, includes information such as Most Recently Used (MRU) file lists, desktop settings, default application behaviors
SAM (Security Accounts Manager)	User account information (including passwords) and security settings
SECURITY	User and group security policies, e.g. which accounts can load device drivers, get remote access to the machine
SOFTWARE	Information about all install programs, including settings and directory paths
SYSTEM	Windows systems settings, such as drive letter mappings, storage volume information, system boot profile, last known good configuration, system name, Windows setup information, hardware profile information

Where are They Located?



Name	Date modified	Type	Size
Journal	7/13/2009 10:34 PM	File folder	
RegBack	10/21/2013 12:39 ...	File folder	
systemprofile	11/20/2010 9:41 PM	File folder	
TxR	2/21/2011 2:10 PM	File folder	
BCD-Template	6/28/2013 6:36 AM	File	28 KB
COMPONENTS	10/22/2013 3:50 PM	File	43,008 KB
COMPONENTS.LOG	11/21/2010 1:33 AM	Text Document	1 KB
COMPONENTS.LOG1	10/22/2013 3:50 PM	LOG1 File	256 KB
COMPONENTS.LOG2	7/13/2009 10:34 PM	LOG2 File	0 KB
DEFAULT	10/22/2013 3:40 PM	File	512 KB
DEFAULT.LOG	11/21/2010 1:33 AM	Text Document	1 KB
DEFAULT.LOG1	10/22/2013 3:40 PM	LOG1 File	256 KB
DEFAULT.LOG2	7/13/2009 10:34 PM	LOG2 File	0 KB
netlogon.ftl	10/22/2013 3:17 PM	FTL File	3 KB
SAM	10/22/2013 7:24 AM	File	256 KB
SAM.LOG	11/21/2010 1:33 AM	Text Document	1 KB
SAM.LOG1	10/22/2013 7:23 AM	LOG1 File	21 KB
SAM.LOG2	7/13/2009 10:34 PM	LOG2 File	0 KB
SECURITY	10/22/2013 3:18 PM	File	256 KB
SECURITY.LOG	11/21/2010 1:33 AM	Text Document	1 KB
SECURITY.LOG1	10/22/2013 3:18 PM	LOG1 File	25 KB
SECURITY.LOG2	7/13/2009 10:34 PM	LOG2 File	0 KB
SOFTWARE	10/22/2013 5:13 PM	File	85,504 KB
SOFTWARE.LOG	11/21/2010 1:33 AM	Text Document	1 KB
SOFTWARE.LOG1	10/22/2013 5:13 PM	LOG1 File	256 KB
SOFTWARE.LOG2	7/13/2009 10:34 PM	LOG2 File	0 KB
SYSTEM	10/22/2013 5:14 PM	File	19,456 KB
SYSTEM.LOG	11/21/2010 1:33 AM	Text Document	1 KB
SYSTEM.LOG1	10/22/2013 5:14 PM	LOG1 File	256 KB
SYSTEM.LOG2	7/13/2009 10:34 PM	LOG2 File	0 KB

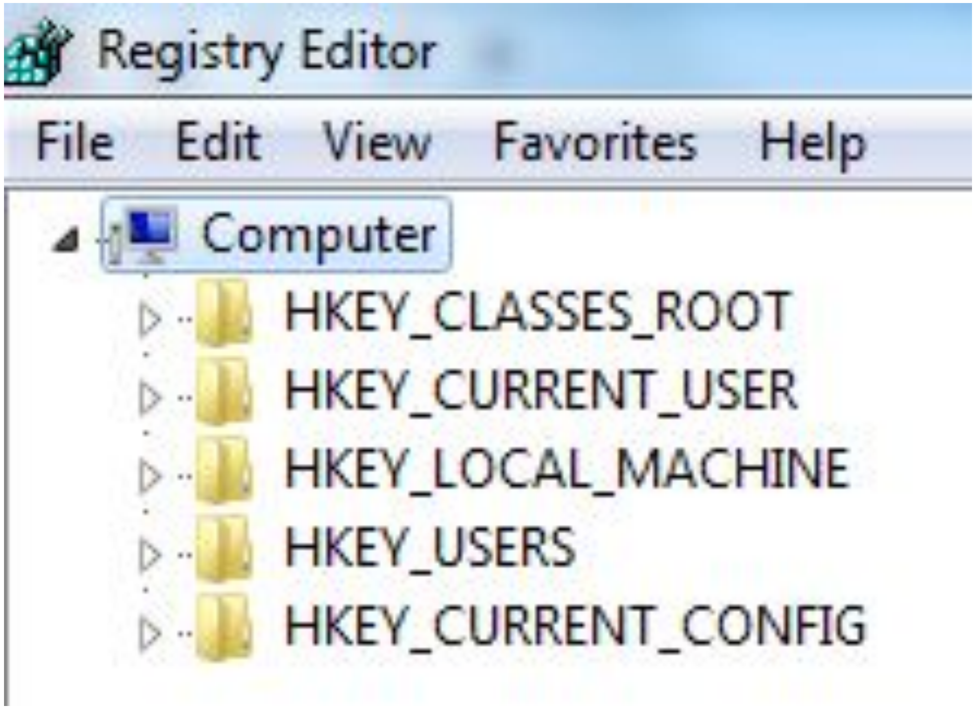


Name	Date modified	Type	Size
.VirtualBox	10/21/2013 11:37 ...	File folder	
AppData	3/19/2012 9:39 AM	File folder	
Application Data	7/15/2013 9:55 AM	File folder	
Backup	7/15/2013 12:04 PM	File folder	
Contacts	9/24/2013 7:16 AM	File folder	
Cookies	7/15/2013 9:55 AM	File folder	
Desktop	10/22/2013 9:26 AM	File folder	
Downloads	10/22/2013 8:36 AM	File folder	
Dropbox	7/15/2013 12:16 PM	File folder	
Favorites	9/24/2013 7:16 AM	File folder	
GodMode	2/1/2010 6:40 PM	File folder	
Links	9/24/2013 7:16 AM	File folder	
Local Settings	7/15/2013 9:55 AM	File folder	
My Documents	10/16/2013 12:19 ...	File folder	
My Documents	7/15/2013 9:55 AM	File folder	
My Music	9/24/2013 7:16 AM	File folder	
My Pictures	9/24/2013 7:16 AM	File folder	
My Videos	9/24/2013 7:16 AM	File folder	
NetHood	7/15/2013 9:55 AM	File folder	
Oracle	7/15/2013 11:47 AM	File folder	
PrintHood	7/15/2013 9:55 AM	File folder	
Recent	7/15/2013 9:55 AM	File folder	
Roaming	6/28/2013 4:40 AM	File folder	
Saved Games	9/24/2013 7:16 AM	File folder	
Searches	9/24/2013 7:16 AM	File folder	
SendTo	7/15/2013 9:55 AM	File folder	
Start Menu	7/15/2013 9:55 AM	File folder	
Templates	7/15/2013 9:55 AM	File folder	
VirtualBox VMs	10/17/2013 5:53 PM	File folder	
.gitconfig	9/29/2013 5:13 PM	GITCONFIG File	0 KB
NTUSER.DAT	10/22/2013 7:26 PM	DAT File	5,888 KB
ntuser.dat.LOG1	10/22/2013 7:26 PM	LOG1 File	256 KB
ntuser.dat.LOG2	7/15/2013 9:55 AM	LOG2 File	0 KB

Registry Hives

Structure:

Hive
- Key
  - Subkey
    - Value



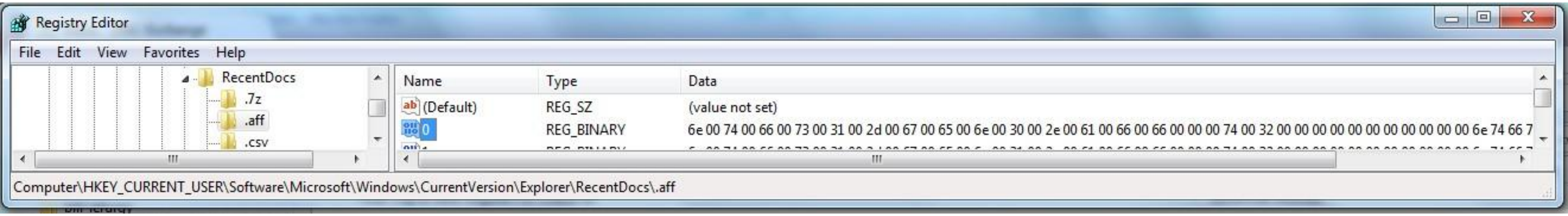
Example:
HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Explorer
\ RecentDocs

What do you think this is?

Registry Hives

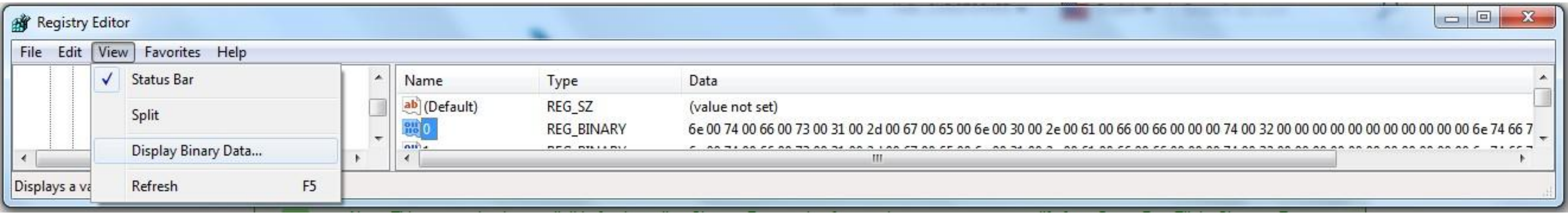
Name	Description
HKEY_CLASSES_ROOT	Just points to HKEY_LOCAL_MACHINE\Software\Classes
HKEY_CURRENT_USER	**User setting information, which is generated dynamically from HKEY_USERS when a user logs into Windows**
HKEY_LOCAL_MACHINE	**Hardware and software settings that are specific to this computer but shared across users (generated at startup from SYSTEM.DAT)**
HKEY_USERS	**Information about each of the user accounts on the computer, e.g. desktop settings, default software behaviors - generated at startup from NTUSER.DAT files, and when user logs out of applications or out of Windows, data are written back to the ntUSER.DAT files**
HKEY_CURRENT_CONFIG	Just points to HKEY_LOCAL_MACHINE\Config

Question: Where would you find these registry hives on a disk image? (Hint: This is a trick question)

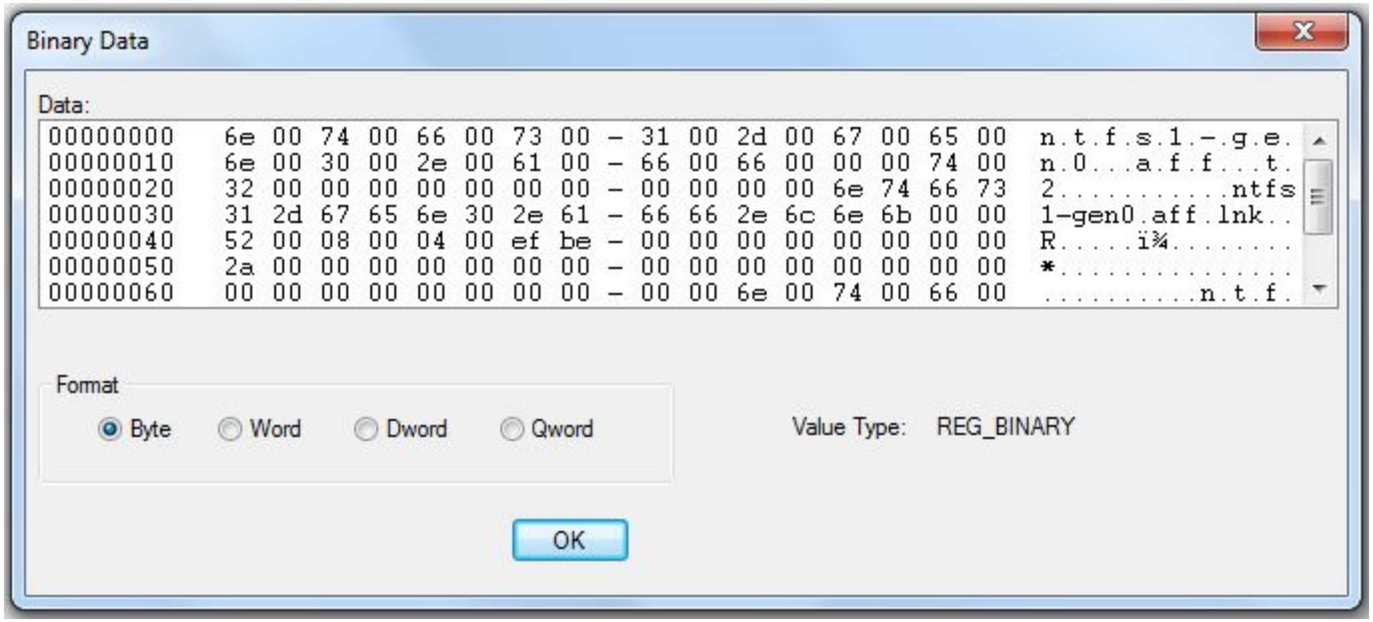


Name	Type	Data
(Default)	REG_SZ	(value not set)
0	REG_BINARY	6e 00 74 00 66 00 73 00 31 00 2d 00 67 00 65 00 6e 00 30 00 2e 00 61 00 66 00 66 00 00 00 74 00 32 00 00 00 00 00 00 00 00 00 00 00 6e 74 66 7

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



Name	Type	Data
(Default)	REG_SZ	(value not set)
0	REG_BINARY	6e 00 74 00 66 00 73 00 31 00 2d 00 67 00 65 00 6e 00 30 00 2e 00 61 00 66 00 66 00 00 00 74 00 32 00 00 00 00 00 00 00 00 00 00 00 6e 74 66 7



```
00000000   6e 00 74 00 66 00 73 00 - 31 00 2d 00 67 00 65 00   n.t.f.s.1.-.g.e.
00000010   6e 00 30 00 2e 00 61 00 - 66 00 66 00 00 00 74 00   n.0...a.f.f...t.
00000020   32 00 00 00 00 00 00 00 - 00 00 00 00 6e 74 66 73   2...........ntfs
00000030   31 2d 67 65 6e 30 2e 61 - 66 66 2e 6c 6e 6b 00 00   1-gen0.aff.lnk..
00000040   52 00 08 00 04 00 ef be - 00 00 00 00 00 00 00 00   R.....ï¾........
00000050   2a 00 00 00 00 00 00 00 - 00 00 00 00 00 00 00 00   *...............
00000060   00 00 00 00 00 00 00 00 - 00 00 6e 00 74 00 66 00   ..........n.t.f.
```

● Byte ○ Word ○ Dword ○ Qword

Value Type: REG_BINARY

Registry Hive Value Data Types

Type	Description
REG_BINARY	Raw binary data displayed as hexadecimal*
REG_DWORD	32-bit unsigned integer (4 bytes)
REG_EXPAND_SZ	Variable-length string, usually in UTF-16 (Unicode)
REG_FULL_RESOURCE_DESCRIPTOR	Series of nested arrays used by a hardware device, binary data displayed as hexadecimal*
REG_LINK	Symbolic link to another registry key (Unicode)
REG_MULTI_SZ	Ordered list of strings (multi-string value), usually in UTF-16
REG_NONE	No specific type – displayed as hexadecimal*
REG_QWORD	64-bit integer (8 bytes)
REG_RESOURCE_LIST	Series of nested arrays used by a hardware device, binary data displayed as hexadecimal*
REG_RESOURCE_REQUIREMENTS_LIST	Series of nested arrays used by a hardware device, binary data displayed as hexadecimal*
REG_SZ	Fixed-length text string, usually in UTF-16

*Can open in hex viewer or hex editor using View and Edit menus, respectively.

Security ID (SID)

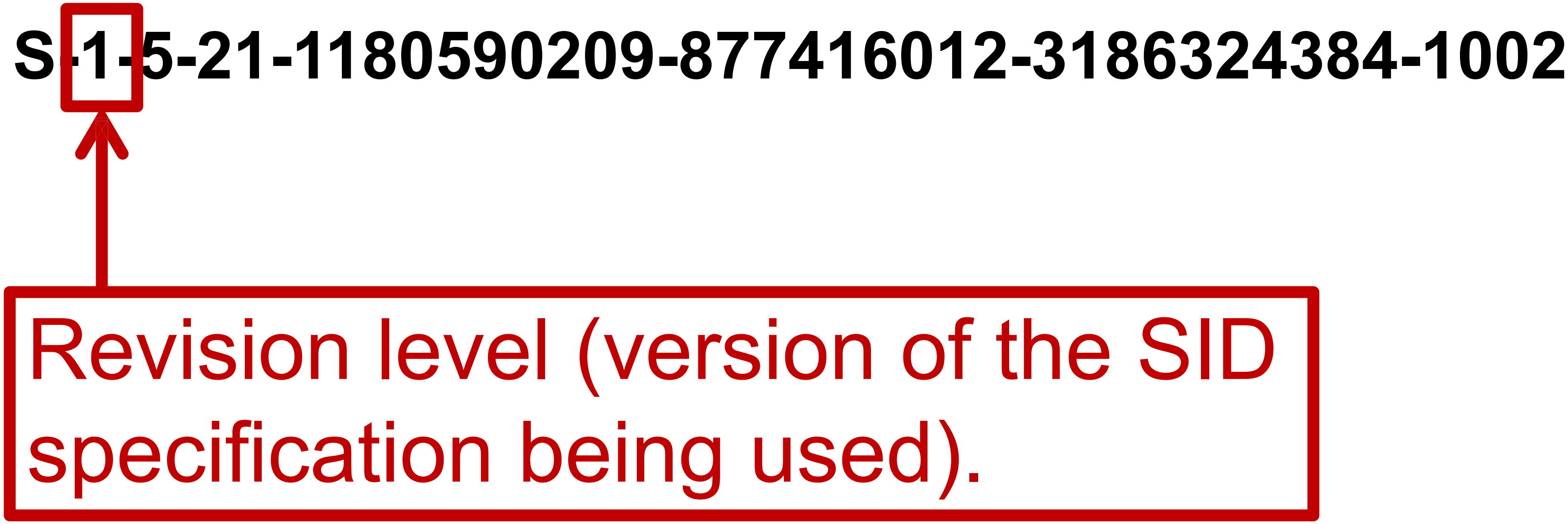
- One assigned to each user account
- Associated with various resources, including files, folders and Recycling Bins

SID Example

S-1-5-21-1180590209-877416012-3186324384-1002

S-1-5-21-1180590209-877416012-3186324384-1002

Always an “S”, indicating that this is an SID.



S-1-5-21-1180590209-877416012-3186324384-1002

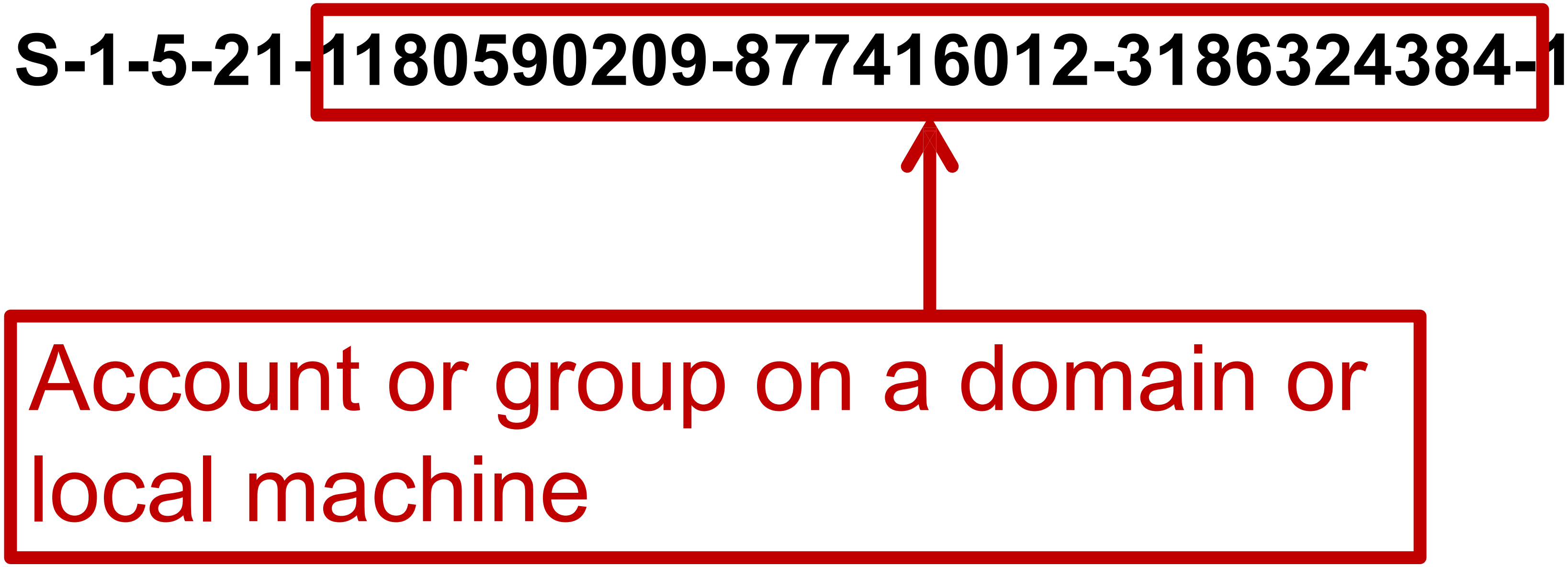
Revision level (version of the SID specification being used).

S-1-5-21-1180590209-877416012-3186324384-1002

Authority that issued the SID. Value is usually “5”, indicating NT Authority.

S-1-5-21-1180590209-877416012-3186324384-1002

Domain identifier – value can be up to 500.



S-1-5-21-1180590209-877416012-3186324384-1002

Account or group on a domain or local machine

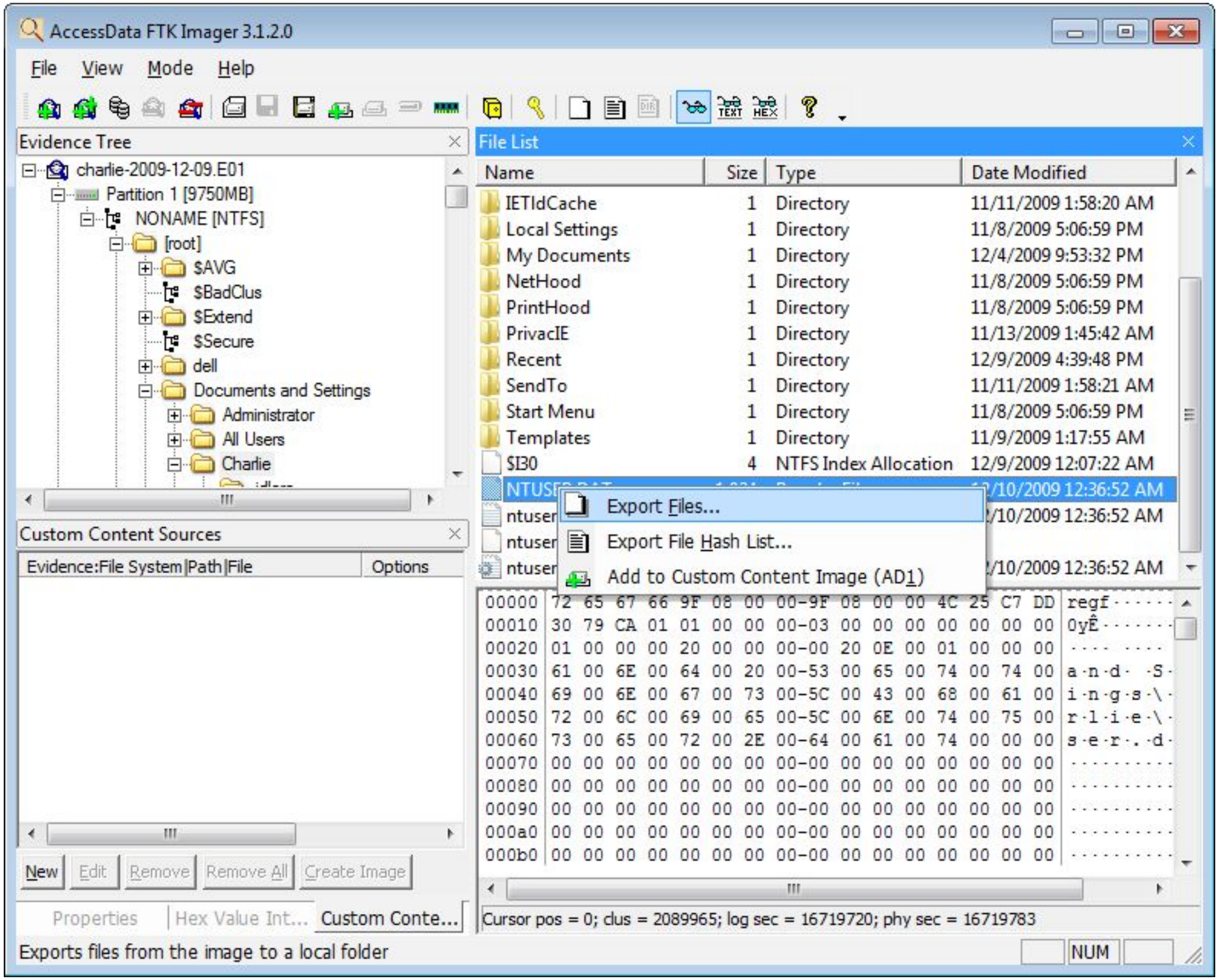
S-1-5-21-1180590209-877416012-3186324384-1002

Relative Identifier (RID), designating a specific user in the SAM file. Those below 1000 are default accounts (e.g. 500 = Administrator), and those 1000 or above are created for specific groups or users.

Examining an NTUSER.DAT File

- The files on your flash drive in registry.zip were extracted from a full-drive (including the operating system) disk image
- The following is an example of how these files can be extracted using FTK Imager

- Navigate to: Partition 1 > [root] > Documents and Settings > Charlie > NTUSER.DAT
- Right click on NTUSER.DAT and select Export Files.



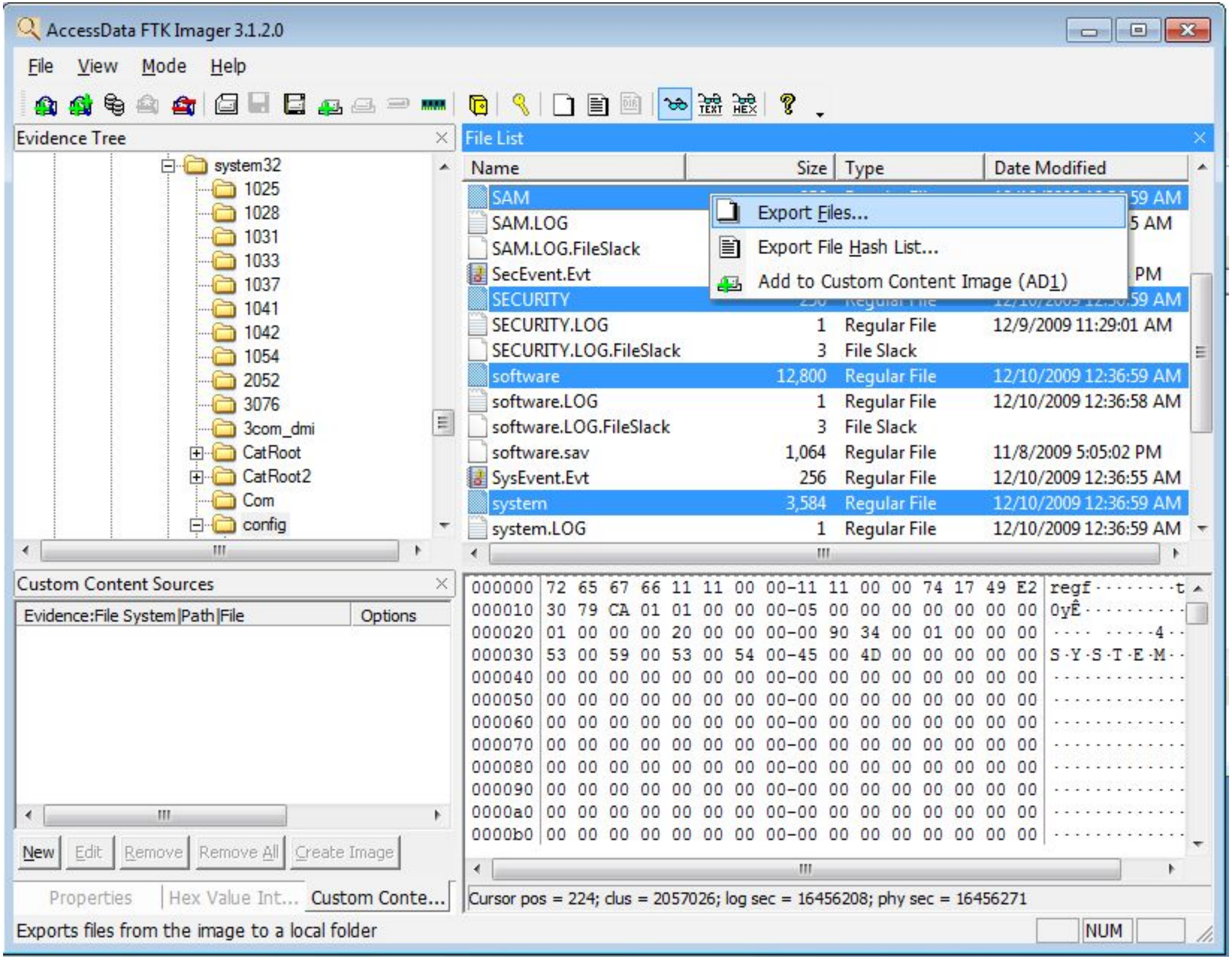
Name	Size	Type	Date Modified
IETldCache	1	Directory	11/11/2009 1:58:20 AM
Local Settings	1	Directory	11/8/2009 5:06:59 PM
My Documents	1	Directory	12/4/2009 9:53:32 PM
NetHood	1	Directory	11/8/2009 5:06:59 PM
PrintHood	1	Directory	11/8/2009 5:06:59 PM
PrivacIE	1	Directory	11/13/2009 1:45:42 AM
Recent	1	Directory	12/9/2009 4:39:48 PM
SendTo	1	Directory	11/11/2009 1:58:21 AM
Start Menu	1	Directory	11/8/2009 5:06:59 PM
Templates	1	Directory	11/9/2009 1:17:55 AM
$I30	4	NTFS Index Allocation	12/9/2009 12:07:22 AM
NTUSE			/10/2009 12:36:52 AM
ntuser			/10/2009 12:36:52 AM
ntuser			
ntuser			/10/2009 12:36:52 AM

```
00000 72 65 67 66 9F 08 00 00-9F 08 00 00 4C 25 C7 DD regf······
00010 30 79 CA 01 01 00 00 00-03 00 00 00 00 00 00 00 0yÊ·······
00020 01 00 00 00 20 00 00 00-00 20 0E 00 01 00 00 00 ····  ····
00030 61 00 6E 00 64 00 20 00-53 00 65 00 74 00 74 00 a·n·d· ·S·
00040 69 00 6E 00 67 00 73 00-5C 00 43 00 68 00 61 00 i·n·g·s·\·
00050 72 00 6C 00 69 00 65 00-5C 00 6E 00 74 00 75 00 r·l·i·e·\·
00060 73 00 65 00 72 00 2E 00-64 00 61 00 74 00 00 00 s·e·r·.·d·
00070 00 00 00 00 00 00 00 00-00 00 00 00 00 00 00 00 ··········
00080 00 00 00 00 00 00 00 00-00 00 00 00 00 00 00 00 ··········
00090 00 00 00 00 00 00 00 00-00 00 00 00 00 00 00 00 ··········
000a0 00 00 00 00 00 00 00 00-00 00 00 00 00 00 00 00 ··········
000b0 00 00 00 00 00 00 00 00-00 00 00 00 00 00 00 00 ··········
```

Cursor pos = 0; clus = 2089965; log sec = 16719720; phy sec = 16719783

Exports files from the image to a local folder

Then export the other four registry files from Windows\System32\config



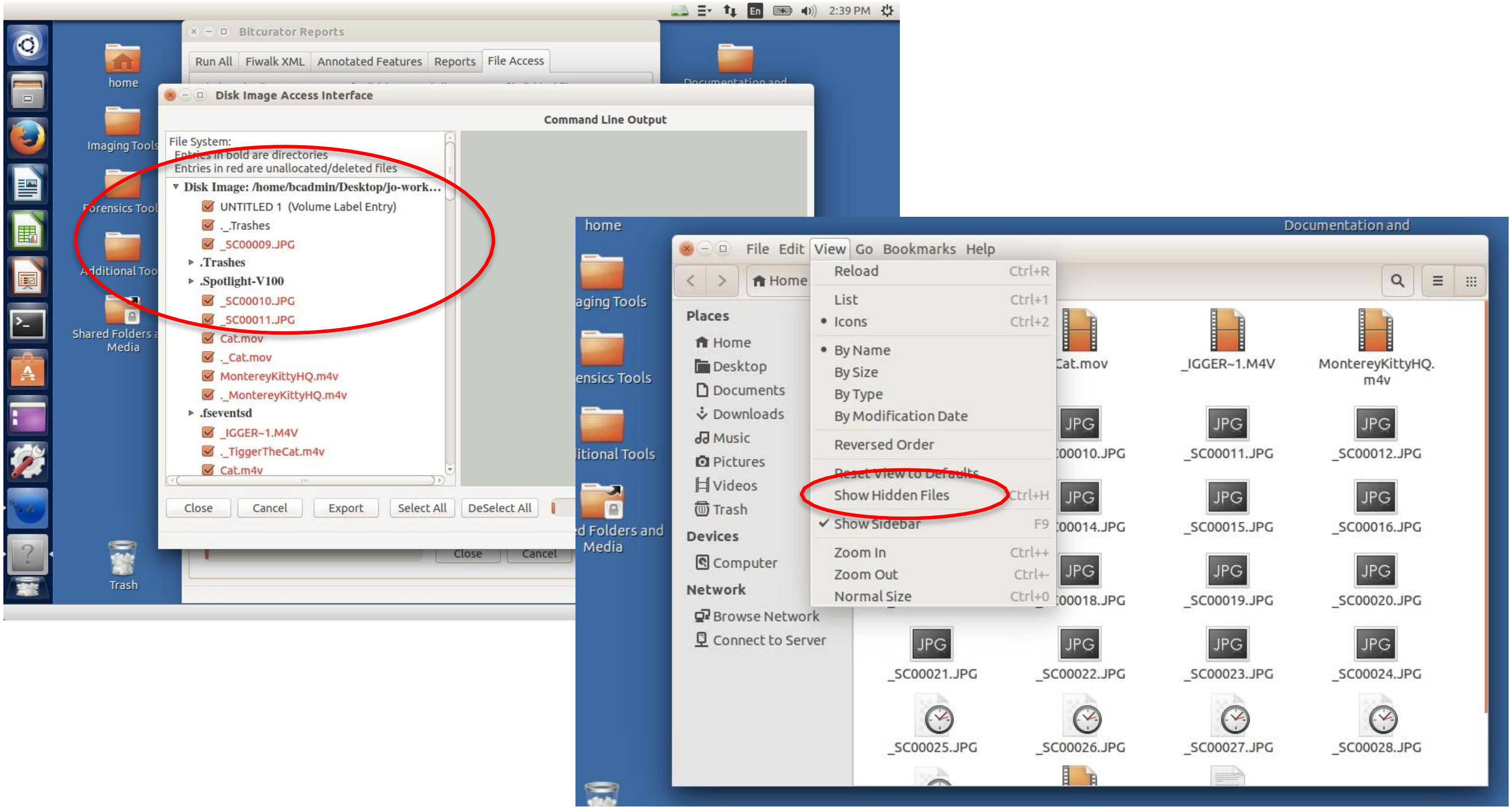
Name	Size	Type	Date Modified
SAM			59 AM
SAM.LOG			5 AM
SAM.LOG.FileSlack			
SecEvent.Evt			PM
SECURITY			59 AM
SECURITY.LOG	1	Regular File	12/9/2009 11:29:01 AM
SECURITY.LOG.FileSlack	3	File Slack	
software	12,800	Regular File	12/10/2009 12:36:59 AM
software.LOG	1	Regular File	12/10/2009 12:36:58 AM
software.LOG.FileSlack	3	File Slack	
software.sav	1,064	Regular File	11/8/2009 5:05:02 PM
SysEvent.Evt	256	Regular File	12/10/2009 12:36:55 AM
system	3,584	Regular File	12/10/2009 12:36:59 AM
system.LOG	1	Regular File	12/10/2009 12:36:59 AM

```
000000  72 65 67 66 11 11 00 00-11 11 00 00 74 17 49 E2  regf········t·
000010  30 79 CA 01 01 00 00 00-05 00 00 00 00 00 00 00  0yÊ···········
000020  01 00 00 00 20 00 00 00-00 90 34 00 01 00 00 00  ····  ·····4··
000030  53 00 59 00 53 00 54 00-45 00 4D 00 00 00 00 00  S·Y·S·T·E·M··
000040  00 00 00 00 00 00 00 00-00 00 00 00 00 00 00 00  ·············
000050  00 00 00 00 00 00 00 00-00 00 00 00 00 00 00 00  ·············
000060  00 00 00 00 00 00 00 00-00 00 00 00 00 00 00 00  ·············
000070  00 00 00 00 00 00 00 00-00 00 00 00 00 00 00 00  ·············
000080  00 00 00 00 00 00 00 00-00 00 00 00 00 00 00 00  ·············
000090  00 00 00 00 00 00 00 00-00 00 00 00 00 00 00 00  ·············
0000a0  00 00 00 00 00 00 00 00-00 00 00 00 00 00 00 00  ·············
0000b0  00 00 00 00 00 00 00 00-00 00 00 00 00 00 00 00  ·············
```

Cursor pos = 224; clus = 2057026; log sec = 16456208; phy sec = 16456271

Exports files from the image to a local folder

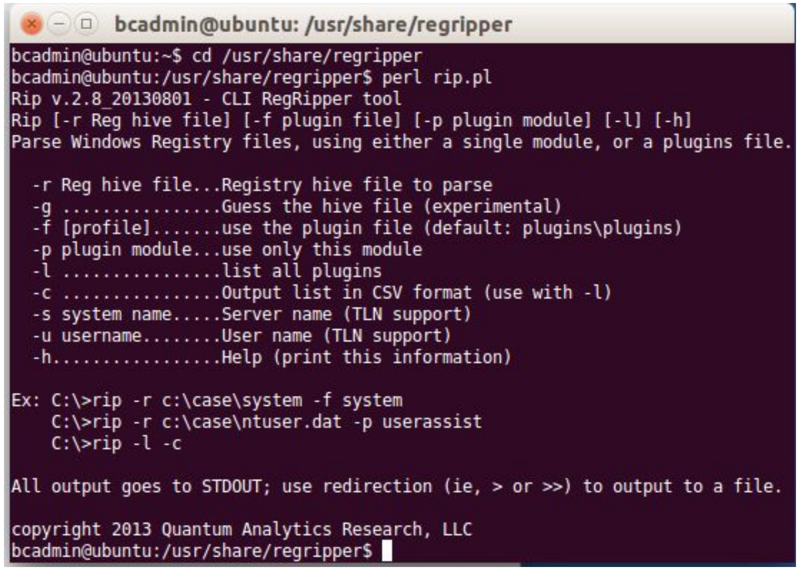
Performing these same tasks using the BitCurator environment



File System:
Entries in bold are directories
Entries in red are unallocated/deleted files

```
▾ Disk Image: /home/bcadmin/Desktop/jo-work…
    ☑ UNTITLED 1  (Volume Label Entry)
    ☑ ._Trashes
    ☑ _SC00009.JPG
  ▸ .Trashes
  ▸ .Spotlight-V100
    ☑ _SC00010.JPG
    ☑ _SC00011.JPG
    ☑ Cat.mov
    ☑ ._Cat.mov
    ☑ MontereyKittyHQ.m4v
    ☑ ._MontereyKittyHQ.m4v
  ▸ .fseventsd
    ☑ _IGGER~1.M4V
    ☑ ._TiggerTheCat.m4v
    ☑ Cat.m4v
```

RegRipper Instructions – BitCurator



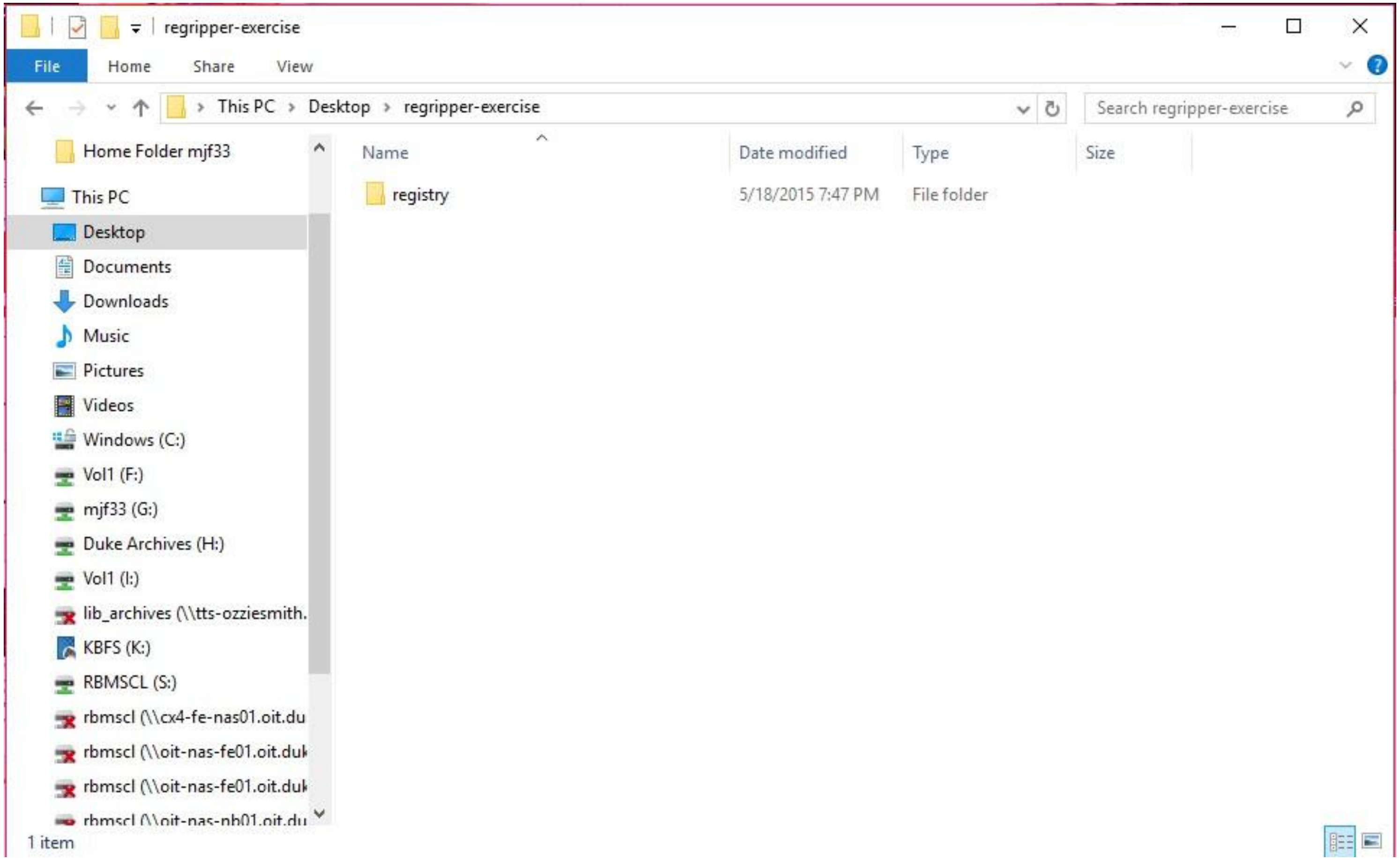
```
bcadmin@ubuntu:~$ cd /usr/share/regripper
bcadmin@ubuntu:/usr/share/regripper$ perl rip.pl
Rip v.2.8_20130801 - CLI RegRipper tool
Rip [-r Reg hive file] [-f plugin file] [-p plugin module] [-l] [-h]
Parse Windows Registry files, using either a single module, or a plugins file.

  -r Reg hive file...Registry hive file to parse
  -g ................Guess the hive file (experimental)
  -f [profile].......use the plugin file (default: plugins\plugins)
  -p plugin module...use only this module
  -l ................list all plugins
  -c ................Output list in CSV format (use with -l)
  -s system name.....Server name (TLN support)
  -u username........User name (TLN support)
  -h.................Help (print this information)

Ex: C:\>rip -r c:\case\system -f system
    C:\>rip -r c:\case\ntuser.dat -p userassist
    C:\>rip -l -c

All output goes to STDOUT; use redirection (ie, > or >>) to output to a file.

copyright 2013 Quantum Analytics Research, LLC
bcadmin@ubuntu:/usr/share/regripper$
```

- Navigate to Forensics Tools and double-click on the RegRipper icon
- NOTE: <u>**IGNORE**</u> examples that it presents, because they use commands and syntax for Windows, not Linux
- Issue each of the following commands:*

  - perl rip.pl -r ~/Desktop/sample-data/registry/NTUSER.DAT > ~/Desktop/ntuser-report -f ntuser
  - perl rip.pl -r ~/Desktop/sample-data/registry/SAM > ~/Desktop/sam-report -f sam
  - perl rip.pl -r ~/Desktop/sample-data/registry/SECURITY > ~/Desktop/security-report -f security
  - perl rip.pl -r ~/Desktop/sample-data/registry/SOFTWARE > ~/Desktop/software-report -f software
  - perl rip.pl -r ~/Desktop/sample-data/registry/SYSTEM > ~/Desktop/system-report -f system

*Enter each command in its entirety before hitting enter (line breaks above are simply to fit the text onto the slide, not ones that you should type yourself). Remember that the up arrow and tab can save you time when typing commands.

RegRipper Instructions – Windows I

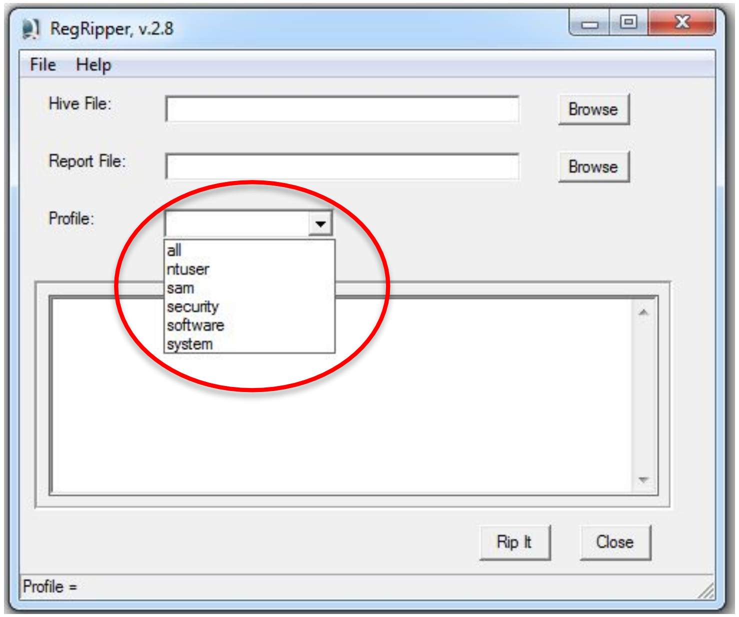

regripper-exercise
File
Home
Share
View
This PC › Desktop › regripper-exercise
Search regripper-exercise
Home Folder mjf33
This PC
Desktop
Documents
Downloads
Music
Pictures
Videos
Windows (C:)
Vol1 (F:)
mjf33 (G:)
Duke Archives (H:)
Vol1 (I:)
lib_archives (\\tts-ozziesmith.
KBFS (K:)
RBMSCL (S:)
rbmscl (\\cx4-fe-nas01.oit.du
rbmscl (\\oit-nas-fe01.oit.duk
rbmscl (\\oit-nas-fe01.oit.duk
rbmscl (\\oit-nas-nb01.oit.du
1 item

Name	Date modified	Type	Size
registry	5/18/2015 7:47 PM	File folder	

- Create a folder on your desktop called regripper-exercise
- Go to \das-forensics-flash-drive-files\Sample Data\
- Extract contents of registry.zip to Desktop\regripper-exercise

RegRipper Instructions – Windows II

- Navigate to \das-forensics-flash-drive-files\reg-ripper
- Run rr.exe
- The next set of steps will be run 5 times—once for each of the files in regripper-exercise\registry
- Next to the Hive File window, select Browse
  - Navigate to regripper-exercise\registry and select the first Hive File
  - E.g., NTUSER.DAT
- Next to Report File, select Browse
  - Create a new file in regripper-exercise that corresponds to the Hive File above
  - E.g., NTUSER_report.txt
- In the Profile dropdown, select the appropriate profile
  - E.g., ntuser
- Select Rip It.
- Repeat the above steps for SAM, SECURITY, SOFTWARE, and SYSTEM



RegRipper Output Questions

Examine ntuser-report.txt	Are you able to identify files that the user recently opened? If so, what were they? Can you determine what the most recently opened files of specific types (e.g. txt) were?
Examine sam-report.txt	How many accounts were there on the computer that is represented in the disk image? What is the Relative Identifier (RID) for the user account you're examining? What other interesting information can you gain from the SAM report about this user account and how might you use that information?
Examine security-report.txt	What is the Machine SID for the computer represented in the disk image? Why would you want to know this? How does it relate to the RID that you identified above?
Examine software-report.txt	Identify three different applications that were installed on the computer and the file paths where the applications were stored.
Examine system-report.txt	Find the devclass output. What does this output tell you? How might this information be useful?

RegRipper Output Discussion: ntuser-report

- Are you able to identify the files that the user recently opened? If so, what were they?
  - How did you go about finding this information?
  - What line number(s) points to this information?

- Can you determine what the most recently open files of specific types (e.g. txt) were?
  - How did you go about finding these?
  - What line numbers have this information?

- Look at lines 1109-1117—what type of information are you looking at?

- Is there any other information you find particularly compelling in this report?

- What might you do with this information?

RegRipper Output Discussion: sam-report

- How many accounts were there on the this computer?
  - How did you go about finding this information?
  - What line number(s) points to this information?

- What was the Relative Identifier (RID) for the user account you’re examining?
  - How did you go about finding this?

- How many logins did Pat make on this machine?

- Is there any other information you find particularly compelling in this report?

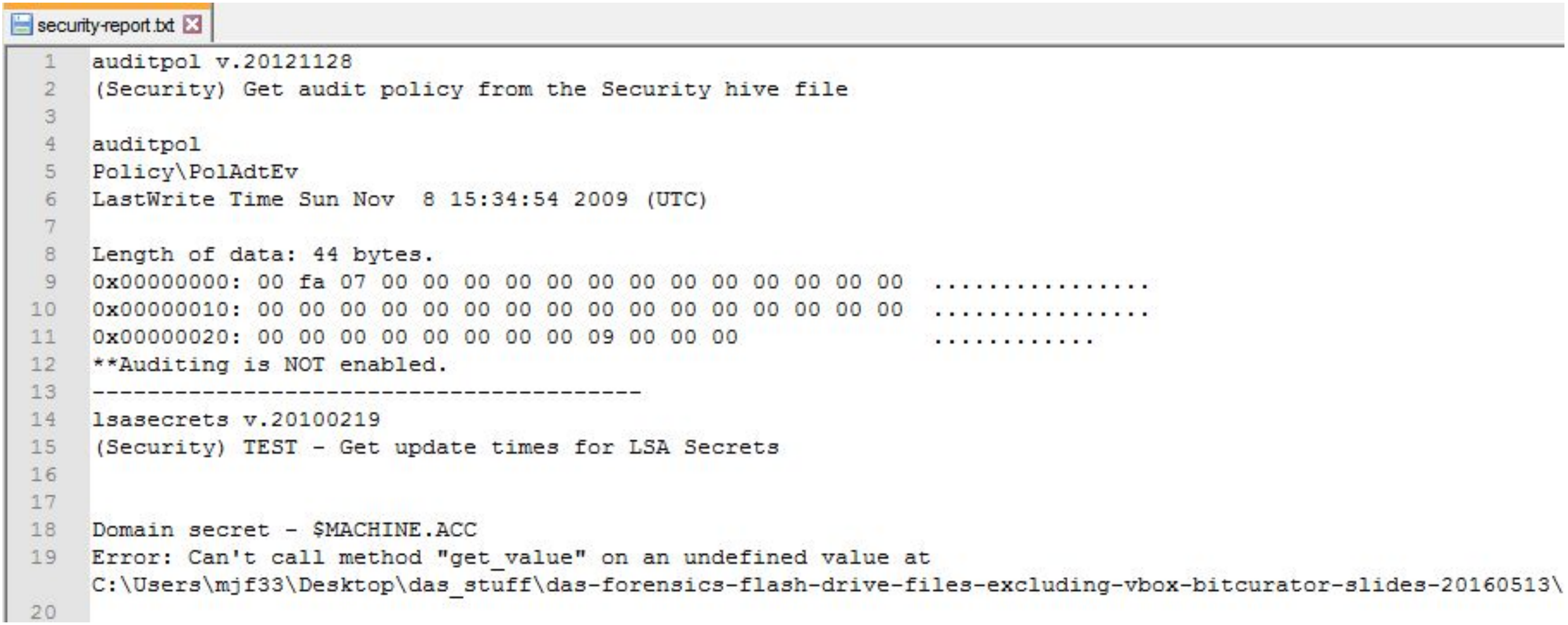
- What might you do with this information?

RegRipper Output Discussion: security-report

- What is the Machine SID for the computer represented here?
  - How did you go about finding this information?
  - What line number(s) points to this information?

- Why would you want to know this information

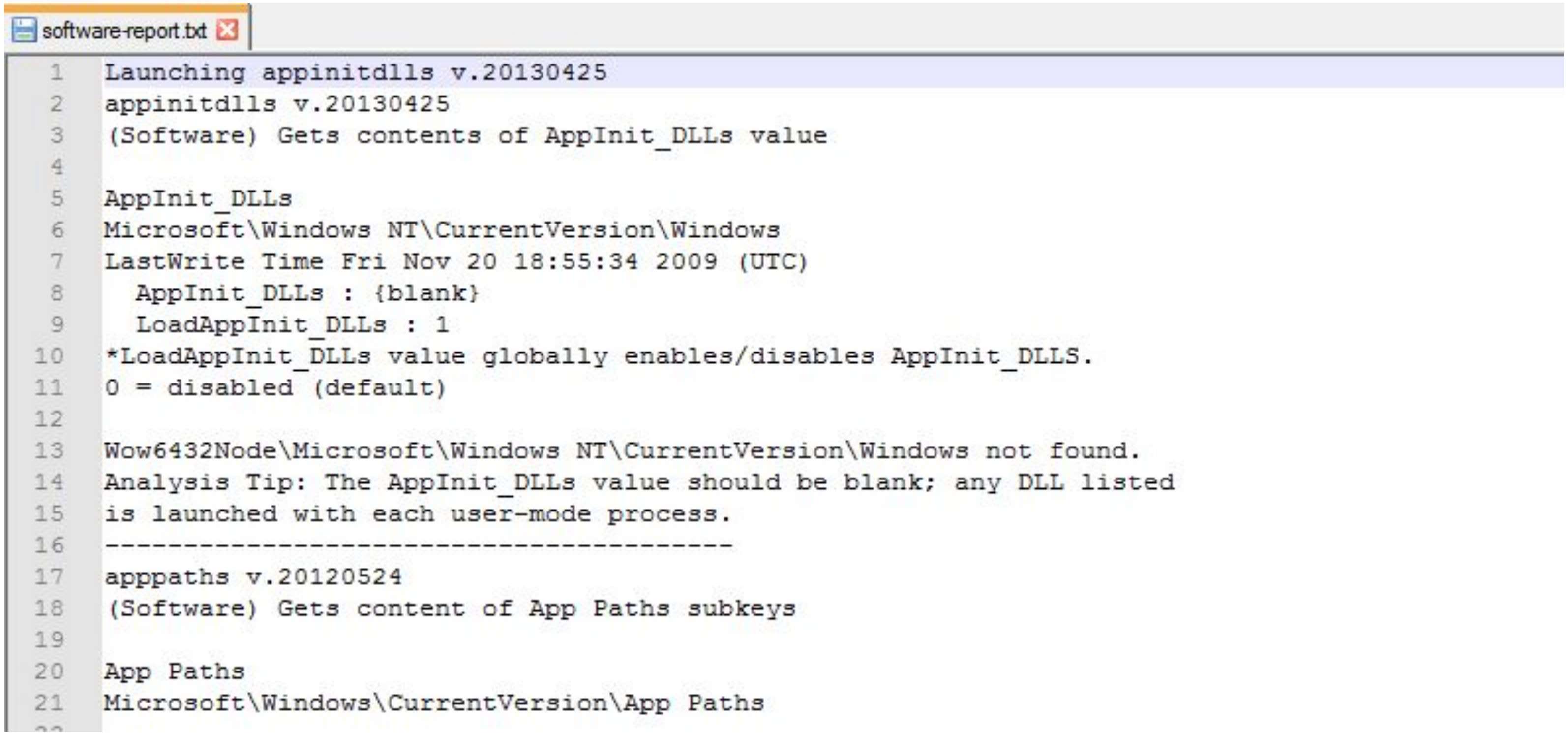
- How does this relate to the RID in the previous report?



```
 1  auditpol v.20121128
 2  (Security) Get audit policy from the Security hive file
 3
 4  auditpol
 5  Policy\PolAdtEv
 6  LastWrite Time Sun Nov  8 15:34:54 2009 (UTC)
 7
 8  Length of data: 44 bytes.
 9  0x00000000: 00 fa 07 00 00 00 00 00 00 00 00 00 00 00 00 00  ................
10  0x00000010: 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00  ................
11  0x00000020: 00 00 00 00 00 00 00 00 09 00 00 00              ............
12  **Auditing is NOT enabled.
13  ----------------------------------------
14  lsasecrets v.20100219
15  (Security) TEST - Get update times for LSA Secrets
16
17
18  Domain secret - $MACHINE.ACC
19  Error: Can't call method "get_value" on an undefined value at
    C:\Users\mjf33\Desktop\das_stuff\das-forensics-flash-drive-files-excluding-vbox-bitcurator-slides-20160513\
20
```

RegRipper Output Discussion: software-report

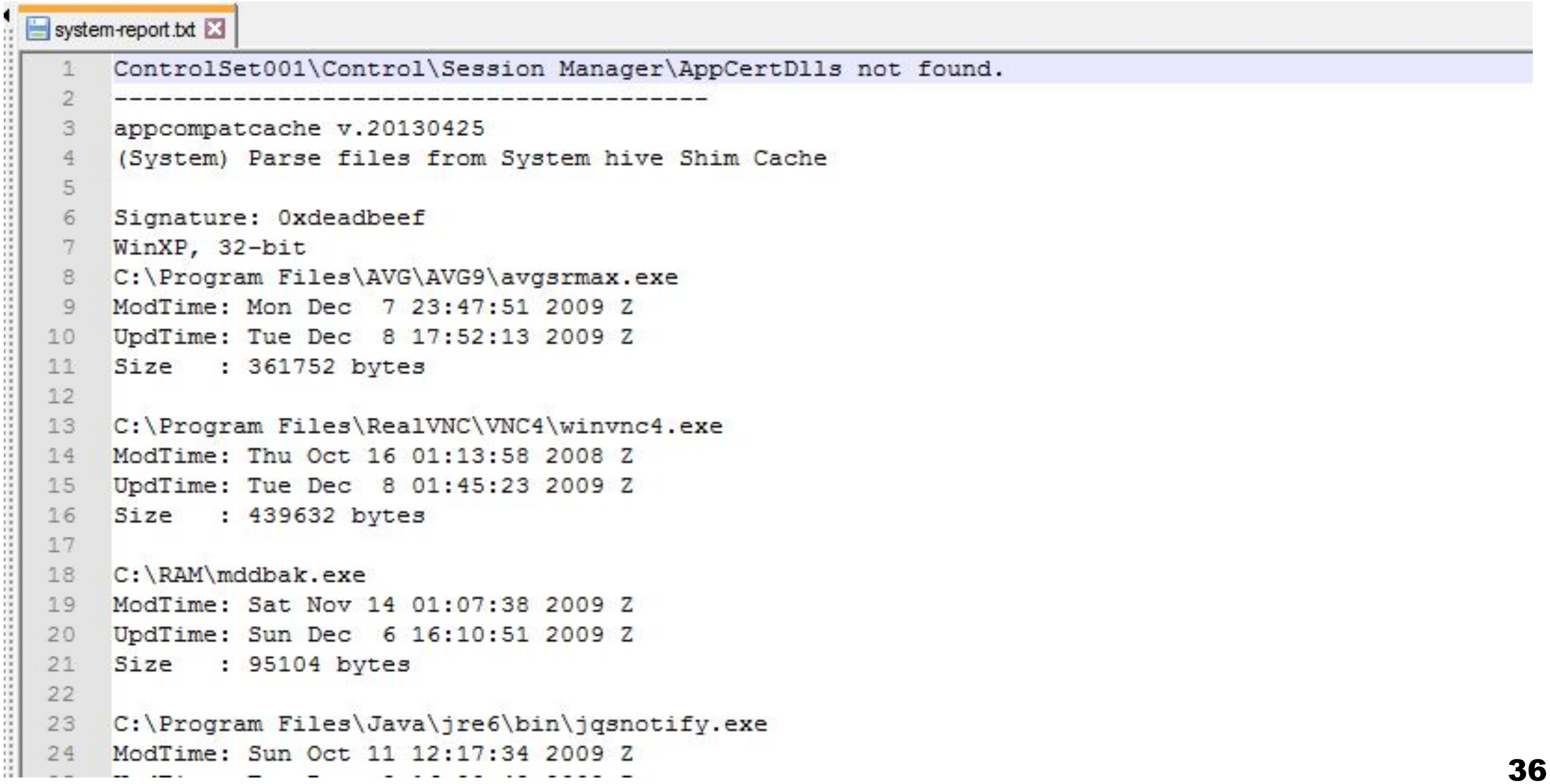
- Identify three different applications that were installed on this computer
  - How did you go about finding this information?
  - What line number(s) points to this information?
- Why would you want to know this information?
- How might it aid description?



```
 1  Launching appinitdlls v.20130425
 2  appinitdlls v.20130425
 3  (Software) Gets contents of AppInit_DLLs value
 4
 5  AppInit_DLLs
 6  Microsoft\Windows NT\CurrentVersion\Windows
 7  LastWrite Time Fri Nov 20 18:55:34 2009 (UTC)
 8    AppInit_DLLs : {blank}
 9    LoadAppInit_DLLs : 1
10  *LoadAppInit_DLLs value globally enables/disables AppInit_DLLS.
11  0 = disabled (default)
12
13  Wow6432Node\Microsoft\Windows NT\CurrentVersion\Windows not found.
14  Analysis Tip: The AppInit_DLLs value should be blank; any DLL listed
15  is launched with each user-mode process.
16  ----------------------------------------
17  apppaths v.20120524
18  (Software) Gets content of App Paths subkeys
19
20  App Paths
21  Microsoft\Windows\CurrentVersion\App Paths
```

RegRipper Output Discussion: system-report

- Find the devclass output
- What does this output tell you?
- How might this information be useful?



```
ControlSet001\Control\Session Manager\AppCertDlls not found.
----------------------------------------
appcompatcache v.20130425
(System) Parse files from System hive Shim Cache

Signature: 0xdeadbeef
WinXP, 32-bit
C:\Program Files\AVG\AVG9\avgsrmax.exe
ModTime: Mon Dec  7 23:47:51 2009 Z
UpdTime: Tue Dec  8 17:52:13 2009 Z
Size    : 361752 bytes

C:\Program Files\RealVNC\VNC4\winvnc4.exe
ModTime: Thu Oct 16 01:13:58 2008 Z
UpdTime: Tue Dec  8 01:45:23 2009 Z
Size    : 439632 bytes

C:\RAM\mddbak.exe
ModTime: Sat Nov 14 01:07:38 2009 Z
UpdTime: Sun Dec  6 16:10:51 2009 Z
Size    : 95104 bytes

C:\Program Files\Java\jre6\bin\jqsnotify.exe
ModTime: Sun Oct 11 12:17:34 2009 Z
```

Viewing and Copying Registry Information if You’re Running the Original Environment

- What if you’re actually running the original computer? How might you get information out of the registry?
- What if you wanted to replicate that registry information on another computer?
- Hint: There are tools built into Windows for this.

Restore Points

- Snapshots of Registry hives and some other essential system (including .EXE, . INI, . LNK) files. They're created:
  - when there are major system changes, e.g. installing software
  - at regularly scheduled intervals
  - if the user manually creates one
- Let's look at some restore points: Start Button > All Programs > Accessories > System Tools > System Restore [or just "System Restore" in the Start box]

Examining the Recycle Bin

1. In the start menu box, type “cmd”
2. Type: “cd c:\$recycle.bin” (What is this doing?)
3. Type “dir /a” (What is this doing?)
4. Type “dir *.* /s” (What is this doing?)
5. Put one or more files into the Recycle Bin (by moving there or by deleting)
6. Repeats steps 2-4. What do you see now?

A Brief Discussion of Mac Forensics

- No Registry, so where is all the good stuff stored?
- See:

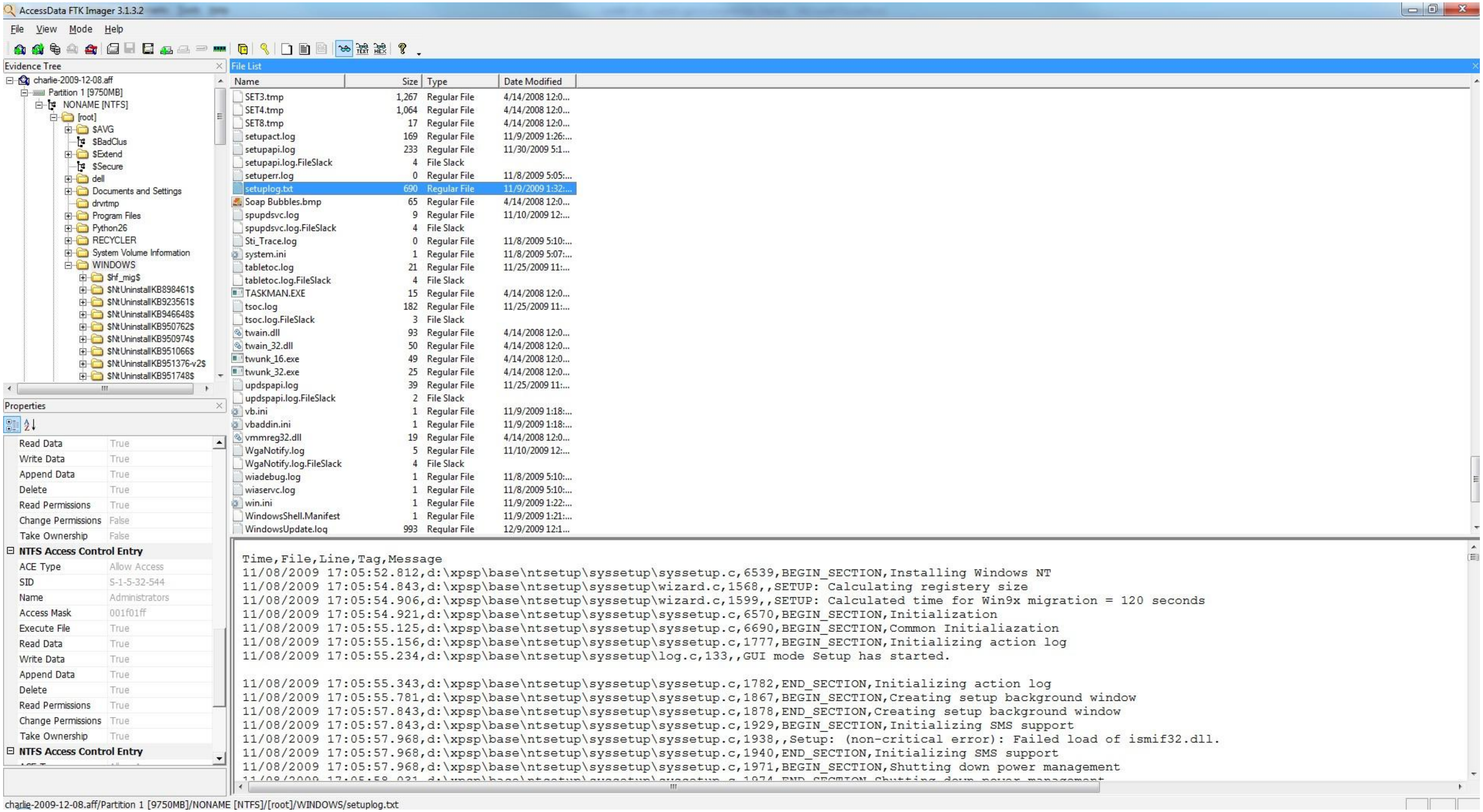
https://forensicswiki.xyz/wiki/index.php?title=Mac_OS_X_10.9_-_Artifacts_Location

Archival Importance and Role of SID

- If the volume is NTFS, you can find the SID associated with a specific file
- If you also have registry files from the original computer (particularly SAM.DAT), you can get information associated with that SID, such as the name of the user/group, last time he/she logged in, and various other account details

setuplog.txt

- See disk image example below: Partition 1 > [root] > WINDOWS > setuplog.txt



- charlie-2009-12-08.aff
  - Partition 1 [9750MB]
    - NONAME [NTFS]
      - [root]
        - $AVG
        - $BadClus
        - $Extend
        - $Secure
        - dell
        - Documents and Settings
        - drvrtmp
        - Program Files
        - Python26
        - RECYCLER
        - System Volume Information
        - WINDOWS
          - hf_mig
          - $NtUninstallKB898461$
          - $NtUninstallKB923561$
          - $NtUninstallKB946648$
          - $NtUninstallKB950762$
          - $NtUninstallKB950974$
          - $NtUninstallKB951066$
          - $NtUninstallKB951376-v2$
          - $NtUninstallKB951748$

Name	Size	Type	Date Modified
SET3.tmp	1,267	Regular File	4/14/2008 12:0...
SET4.tmp	1,064	Regular File	4/14/2008 12:0...
SET8.tmp	17	Regular File	4/14/2008 12:0...
setupact.log	169	Regular File	11/9/2009 1:26:...
setupapi.log	233	Regular File	11/30/2009 5:1...
setupapi.log.FileSlack	4	File Slack	
setuperr.log	0	Regular File	11/8/2009 5:05:...
setuplog.txt	690	Regular File	11/9/2009 1:32:...
Soap Bubbles.bmp	65	Regular File	4/14/2008 12:0...
spupdsvc.log	9	Regular File	11/10/2009 12:...
spupdsvc.log.FileSlack	4	File Slack	
Sti_Trace.log	0	Regular File	11/8/2009 5:10:...
system.ini	1	Regular File	11/8/2009 5:07:...
tabletoc.log	21	Regular File	11/25/2009 11:...
tabletoc.log.FileSlack	4	File Slack	
TASKMAN.EXE	15	Regular File	4/14/2008 12:0...
tsoc.log	182	Regular File	11/25/2009 11:...
tsoc.log.FileSlack	3	File Slack	
twain.dll	93	Regular File	4/14/2008 12:0...
twain_32.dll	50	Regular File	4/14/2008 12:0...
twunk_16.exe	49	Regular File	4/14/2008 12:0...
twunk_32.exe	25	Regular File	4/14/2008 12:0...
updspapi.log	39	Regular File	11/25/2009 11:...
updspapi.log.FileSlack	2	File Slack	
vb.ini	1	Regular File	11/9/2009 1:18:...
vbaddin.ini	1	Regular File	11/9/2009 1:18:...
vmmreg32.dll	19	Regular File	4/14/2008 12:0...
WgaNotify.log	5	Regular File	11/10/2009 12:...
WgaNotify.log.FileSlack	4	File Slack	
wiadebug.log	1	Regular File	11/8/2009 5:10:...
wiaservc.log	1	Regular File	11/8/2009 5:10:...
win.ini	1	Regular File	11/9/2009 1:22:...
WindowsShell.Manifest	1	Regular File	11/9/2009 1:21:...
WindowsUpdate.log	993	Regular File	12/9/2009 12:1...

Read Data	True
Write Data	True
Append Data	True
Delete	True
Read Permissions	True
Change Permissions	False
Take Ownership	False
NTFS Access Control Entry	
ACE Type	Allow Access
SID	S-1-5-32-544
Name	Administrators
Access Mask	001f01ff
Execute File	True
Read Data	True
Write Data	True
Append Data	True
Delete	True
Read Permissions	True
Change Permissions	True
Take Ownership	True
NTFS Access Control Entry	

```
Time,File,Line,Tag,Message
11/08/2009 17:05:52.812,d:\xpsp\base\ntsetup\syssetup\syssetup.c,6539,BEGIN_SECTION,Installing Windows NT
11/08/2009 17:05:54.843,d:\xpsp\base\ntsetup\syssetup\wizard.c,1568,,SETUP: Calculating registery size
11/08/2009 17:05:54.906,d:\xpsp\base\ntsetup\syssetup\wizard.c,1599,,SETUP: Calculated time for Win9x migration = 120 seconds
11/08/2009 17:05:54.921,d:\xpsp\base\ntsetup\syssetup\syssetup.c,6570,BEGIN_SECTION,Initialization
11/08/2009 17:05:55.125,d:\xpsp\base\ntsetup\syssetup\syssetup.c,6690,BEGIN_SECTION,Common Initialiazation
11/08/2009 17:05:55.156,d:\xpsp\base\ntsetup\syssetup\syssetup.c,1777,BEGIN_SECTION,Initializing action log
11/08/2009 17:05:55.234,d:\xpsp\base\ntsetup\syssetup\log.c,133,,GUI mode Setup has started.

11/08/2009 17:05:55.343,d:\xpsp\base\ntsetup\syssetup\syssetup.c,1782,END_SECTION,Initializing action log
11/08/2009 17:05:55.781,d:\xpsp\base\ntsetup\syssetup\syssetup.c,1867,BEGIN_SECTION,Creating setup background window
11/08/2009 17:05:57.843,d:\xpsp\base\ntsetup\syssetup\syssetup.c,1878,END_SECTION,Creating setup background window
11/08/2009 17:05:57.843,d:\xpsp\base\ntsetup\syssetup\syssetup.c,1929,BEGIN_SECTION,Initializing SMS support
11/08/2009 17:05:57.968,d:\xpsp\base\ntsetup\syssetup\syssetup.c,1938,,Setup: (non-critical error): Failed load of ismif32.dll.
11/08/2009 17:05:57.968,d:\xpsp\base\ntsetup\syssetup\syssetup.c,1940,END_SECTION,Initializing SMS support
11/08/2009 17:05:57.968,d:\xpsp\base\ntsetup\syssetup\syssetup.c,1971,BEGIN_SECTION,Shutting down power management
11/08/2009 17:05:58.031,d:\xpsp\base\ntsetup\syssetup\syssetup.c,1974,END_SECTION,Shutting down power management
```

charlie-2009-12-08.aff/Partition 1 [9750MB]/NONAME [NTFS]/[root]/WINDOWS/setuplog.txt

- What do you see in this file?
- What information could be useful for digital curation?   When/how might you use it?

BitCuratorEdu
Advancing the adoption of digital forensics tools and methods in libraries and archives through professional education efforts
EDUCOPIA INSTITUTE
Community Cultivators
INSTITUTE of Museum and Library SERVICES

The BitCuratorEdu project is a three-year effort funded by the Institute of Museum and Library Services (IMLS) to study and advance the adoption of digital forensics tools and methods in libraries and archives through professional education efforts. This project is a partnership between Educopia Institute and the School of Information and Library Science at the University of North Carolina at Chapel Hill, along with the Council of State Archivists (CoSA) and several Masters-level programs in library and information science.