

Digital forensics in the archive

Windows Artifact Exercise –

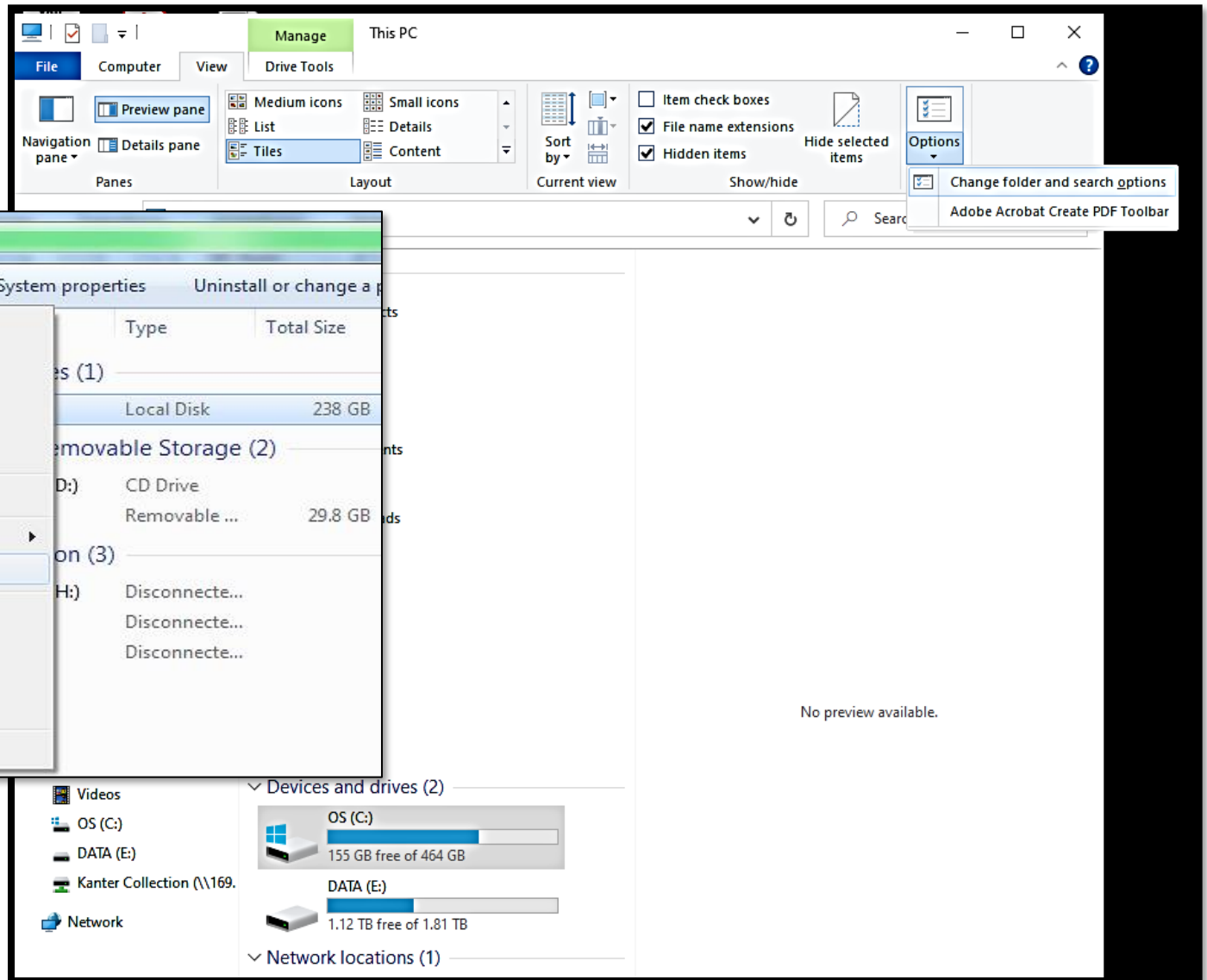
This exercise is modeled from Cal Lee’s presentation with sections and information added for the Lab 2 for this class. See below for Cal Lee’s information.

Author - [Cal Lee, University of North Carolina/Chapel Hill](#)

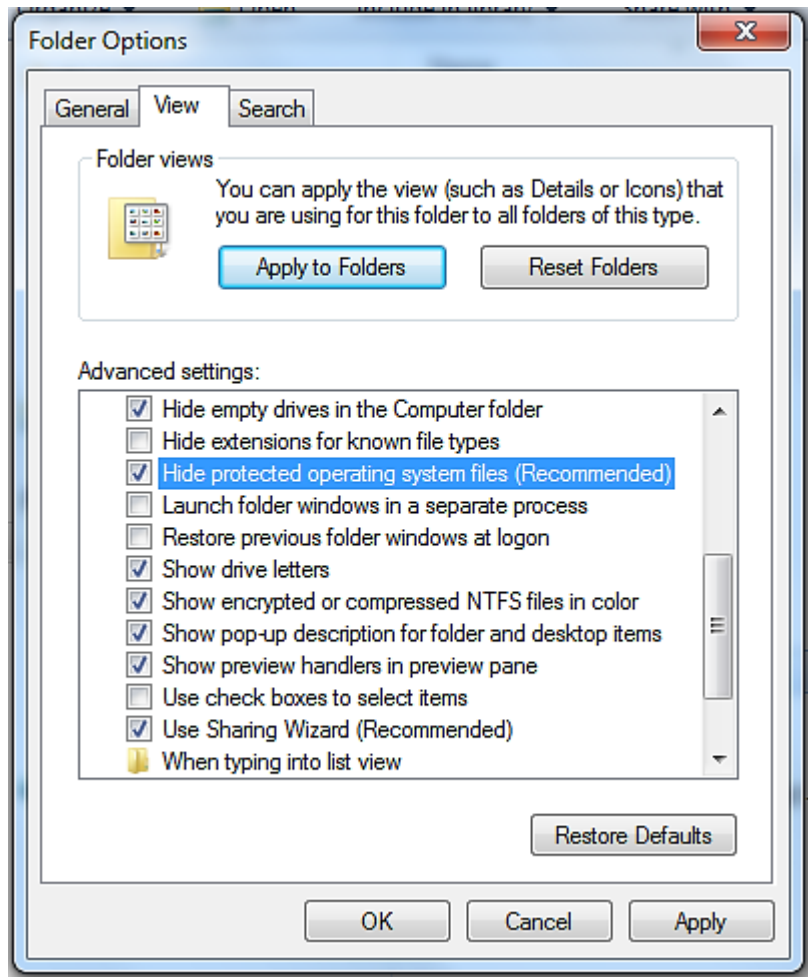
Description - This hands-on exercise introduces students to forensic artifacts produced by Windows operating systems and tools to analyze them.

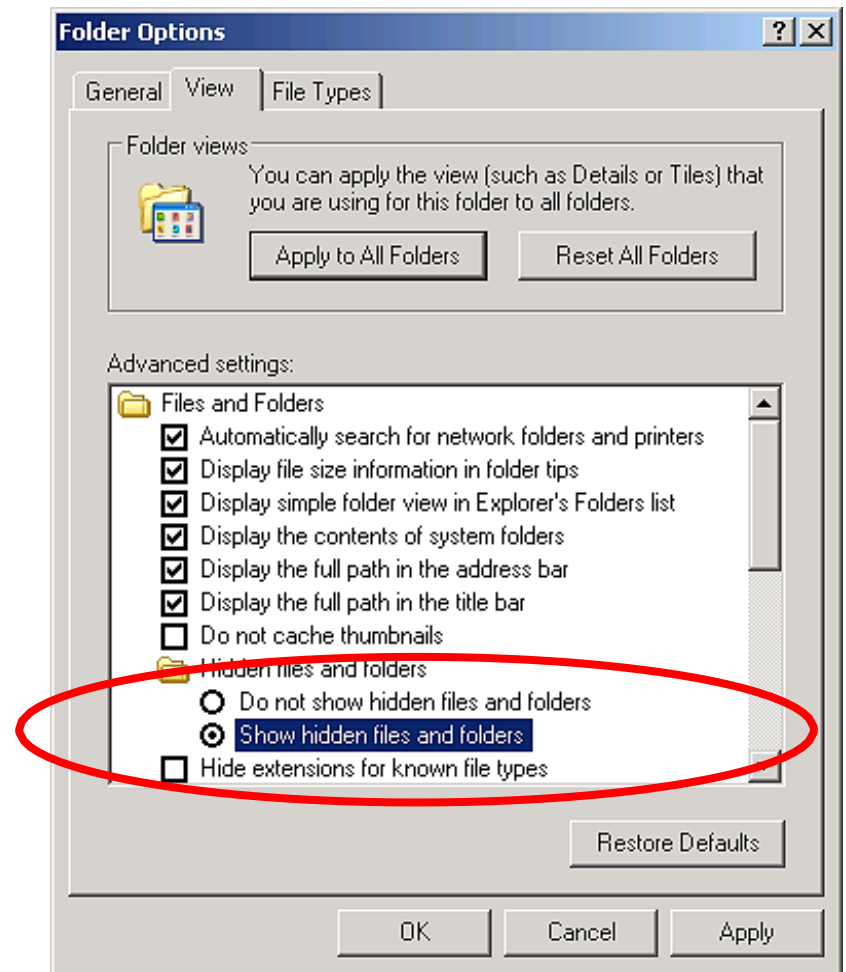
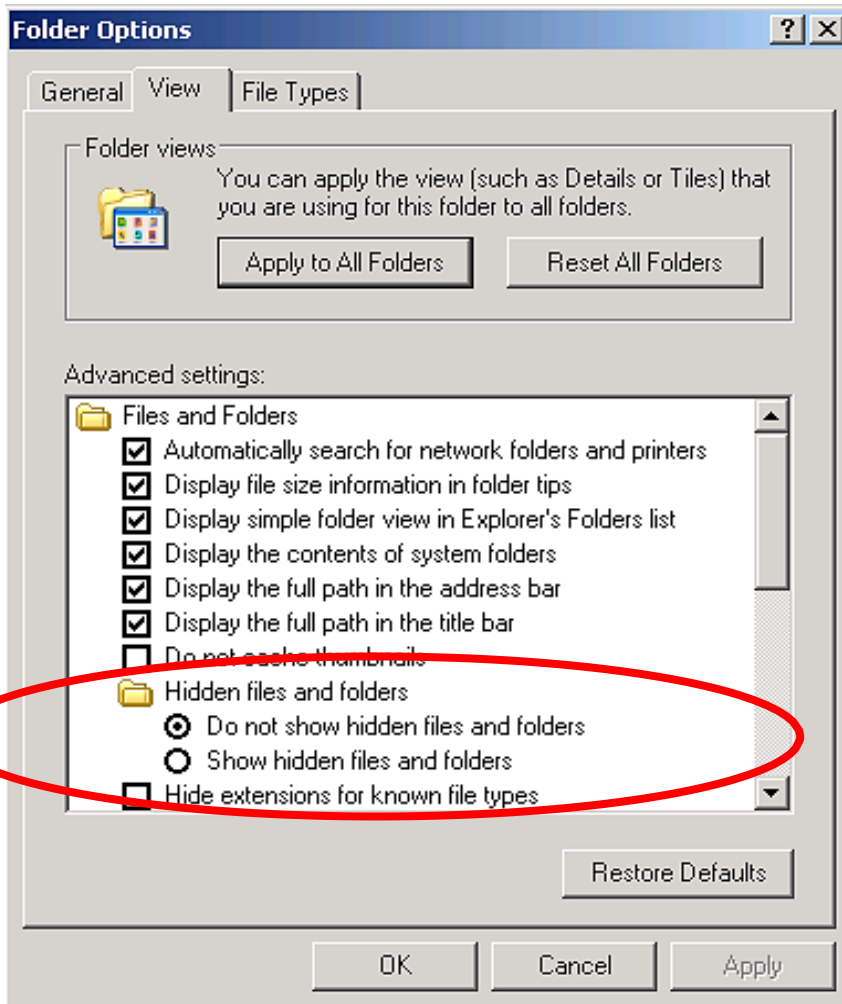
Notes – The template for these slides are excerpted from Cal Lee’s “Advanced Digital Forensics” presentation.

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



Files explorer – View – Folder options
UNCHECK hide protected operating system files – we
must have this unchecked to see later steps





In the search box on the taskbar, type regedit, then select Registry Editor (Desktop app) from the results.

Right-click Start , then select Run. Type regedit in the Open: box, and then select OK

Windows Registry

Start+R → type regedit → open → registry editor

What is 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

Analogy of Window File System for Windows Registry

- If you look closely at the **Registry structure**, you'll notice that it **shares a resemblance with the Windows file system**. The first entry in the Registry Editor titled Computer, which can be used to collapse or expand the Registry Hives, is like your computer Hard Disk.
- The five **Registry Hives** under **Computer** act as Disk Partitions within a Hard Disk. Five Hives contain other Registry keys, subkeys, and values, just like Disk Partitions contain multiple folders and files within them.
- The **Registry Keys** under **Registry Hives**, represented with a folder icon, act like folders that can contain zero or more files.

Registry Hive

There are five Registry Hives in Windows.
A Registry Hive is the first level of Registry Key in Windows Registry.

A Registry Hive, unlike Registry keys present within it, **cannot be created, deleted or modified**

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?

Computer > Windows (C:) > Windows > System32 > config >

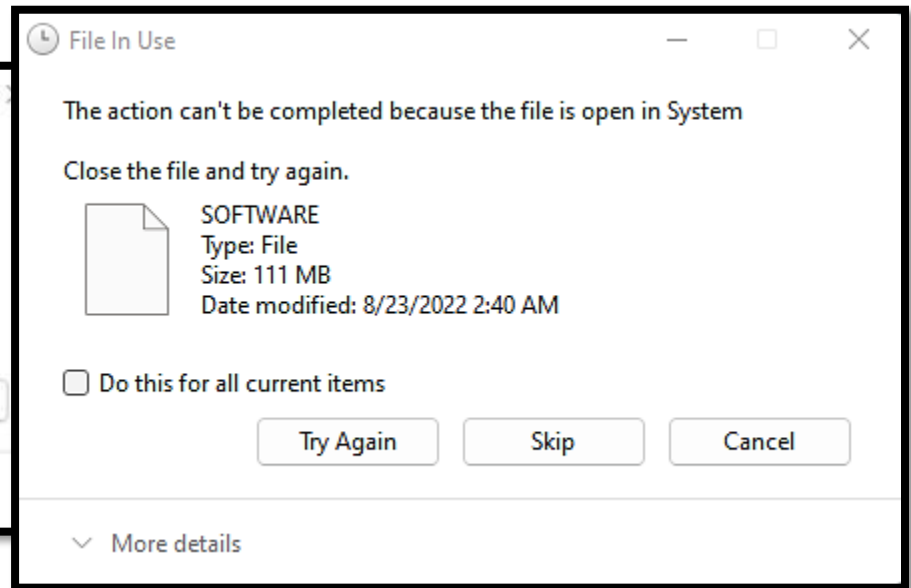
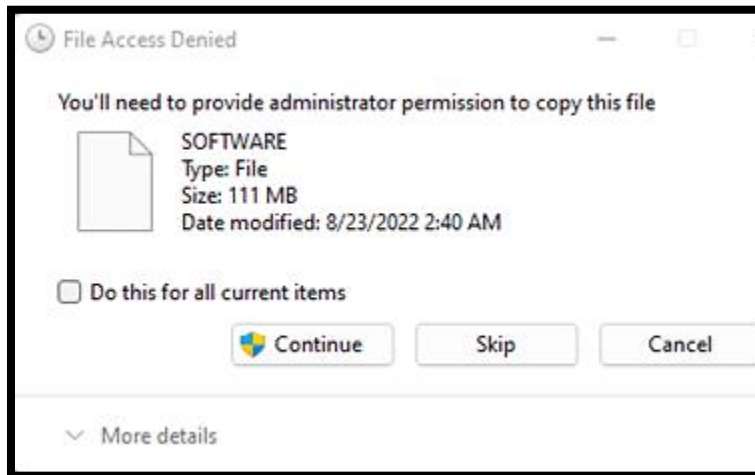
Name	Date modified	Type	Size
Journal	7/13/2009 10:34 PM	File folder	
RegBack	10/21/2013 12:39 ...	File folder	
systemprofile	11/20/2010 9:41 PM	File folder	
TxR	2/21/2011 2:10 PM	File folder	
BCD-Template	6/28/2013 6:36 AM	File	28 KB
COMPONENTS	10/22/2013 3:50 PM	File	43,008 KB
COMPONENTS.LOG	11/21/2010 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

Computer > Windows (C:) > Users > callee >

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

Copying Registry Hives

You cannot copy registry hives locally



System files are restricted (that is why we will use additional software)

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

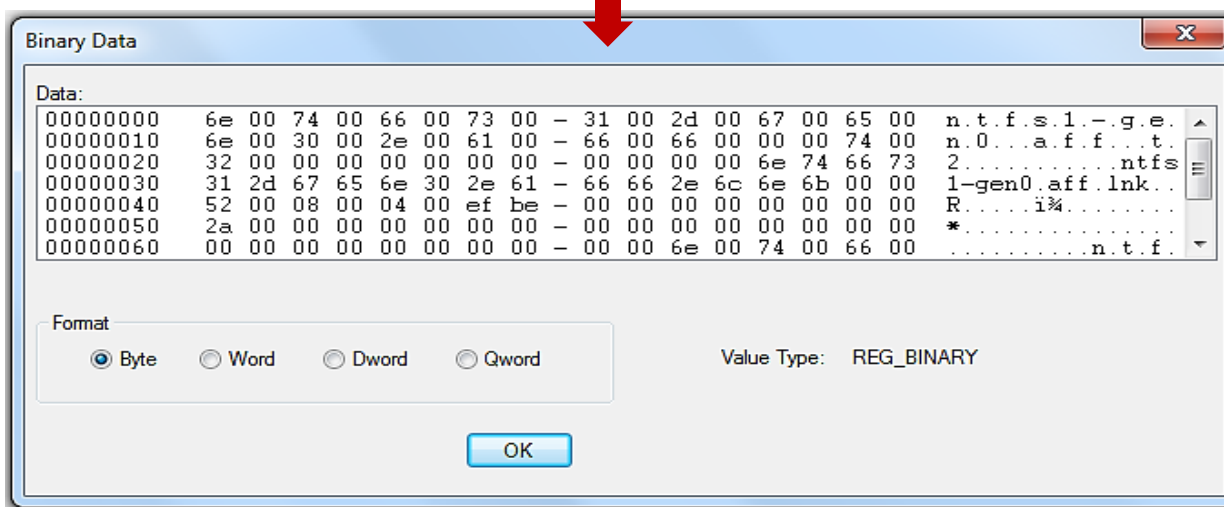
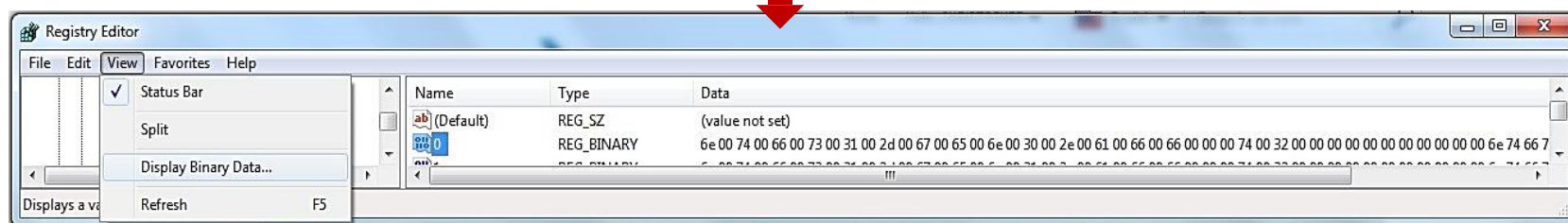
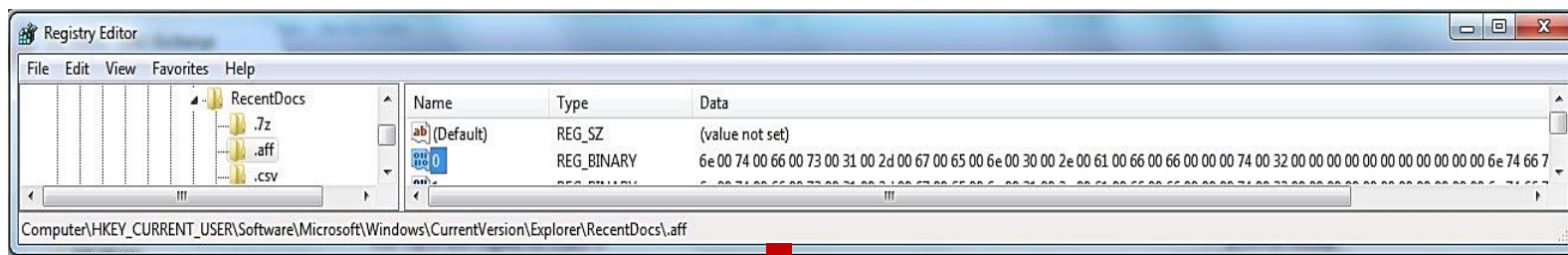
*Can open in hex viewer or hex editor using View and Edit menus, respectively.

Registry Hives

You cannot copy registry hives locally

Question: Where would you find these registry hives on a disk image?

Looking at the data for each file of HIVE first navigate to HKEY_CURRENT_USER → software → Microsoft → windows → current version → explorer → recentdocs
Click on the first file 0 → view → view binary data



Where is the current system build used in this image located in the registry hive?

One way:

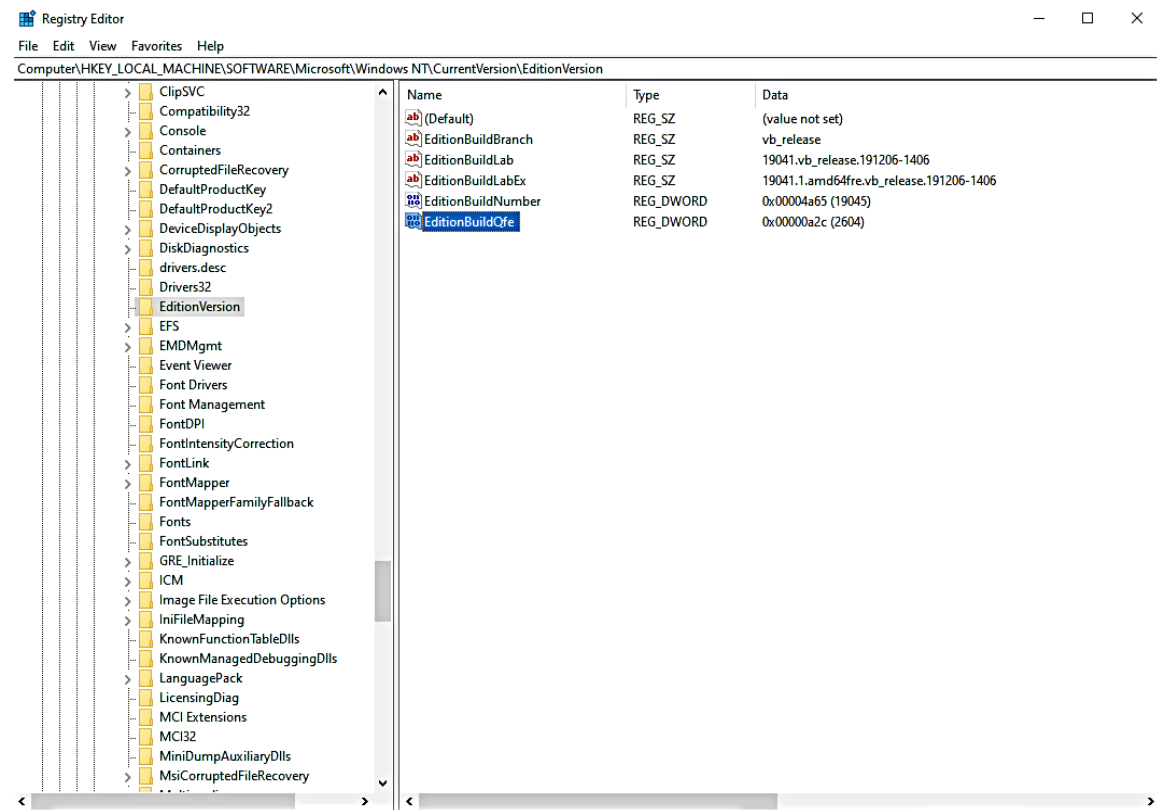
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows NT\CurrentVersion\EditionVersion

EditionBuildLab = 19041.vb_release.191206-1403

EditionBuildLabEx = 19041.1.amd64fre.vb_release.191206-1403

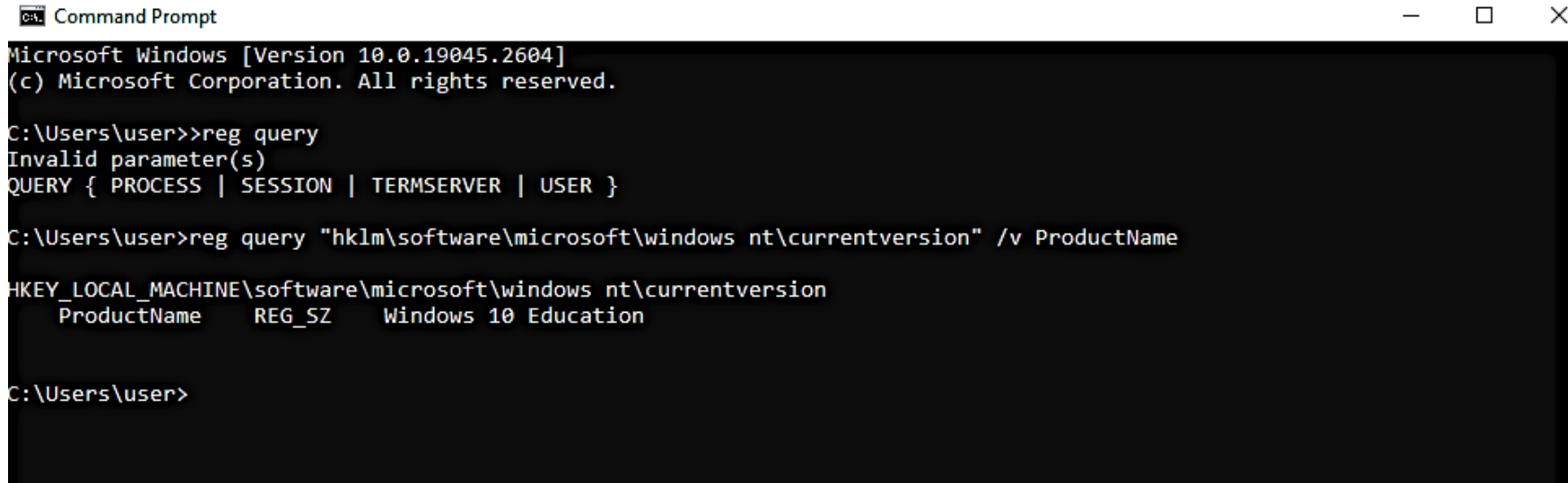
EditionBuildNumber = 19045

AMD64 is a 64-bit processor architecture that was developed by Advanced Micro Devices (AMD) to add 64-bit computing capabilities to the x86 architecture



Where is the current version of the system (windows) located in the registry hive?

Windows – cmd → type *reg query "hklm\software\microsoft\windows nt\currentversion" /v ProductName*



```
Command Prompt
Microsoft Windows [Version 10.0.19045.2604]
(c) Microsoft Corporation. All rights reserved.

C:\Users\user>>reg query
Invalid parameter(s)
QUERY { PROCESS | SESSION | TERMSERVER | USER }

C:\Users\user>reg query "hklm\software\microsoft\windows nt\currentversion" /v ProductName

HKEY_LOCAL_MACHINE\software\microsoft\windows nt\currentversion
    ProductName    REG_SZ    Windows 10 Education

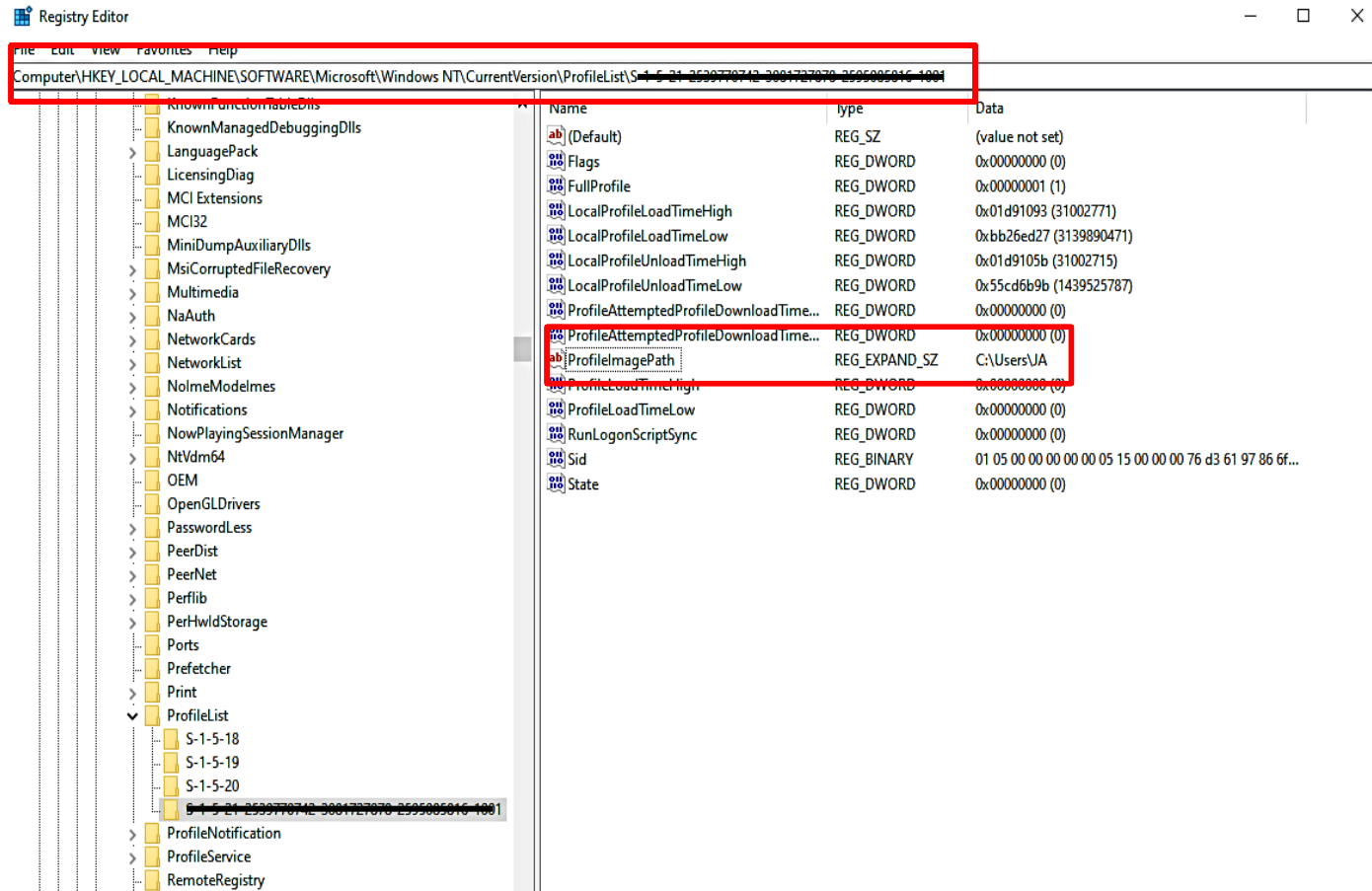
C:\Users\user>
```

Getting into the binary data

Security ID (SID)

- One assigned to each user account
- This is the user ID (i.e. if we received a PC hard drive from a donor and we want ONLY the information concerning that donor on this PC, we will specifically look into this SID)
- Associated with various resources,
 - including files, folders and Recycling Bins

Security ID (SID)



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 (network access) Authority.

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



Domain identifier – value can be up to 500 (21)

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

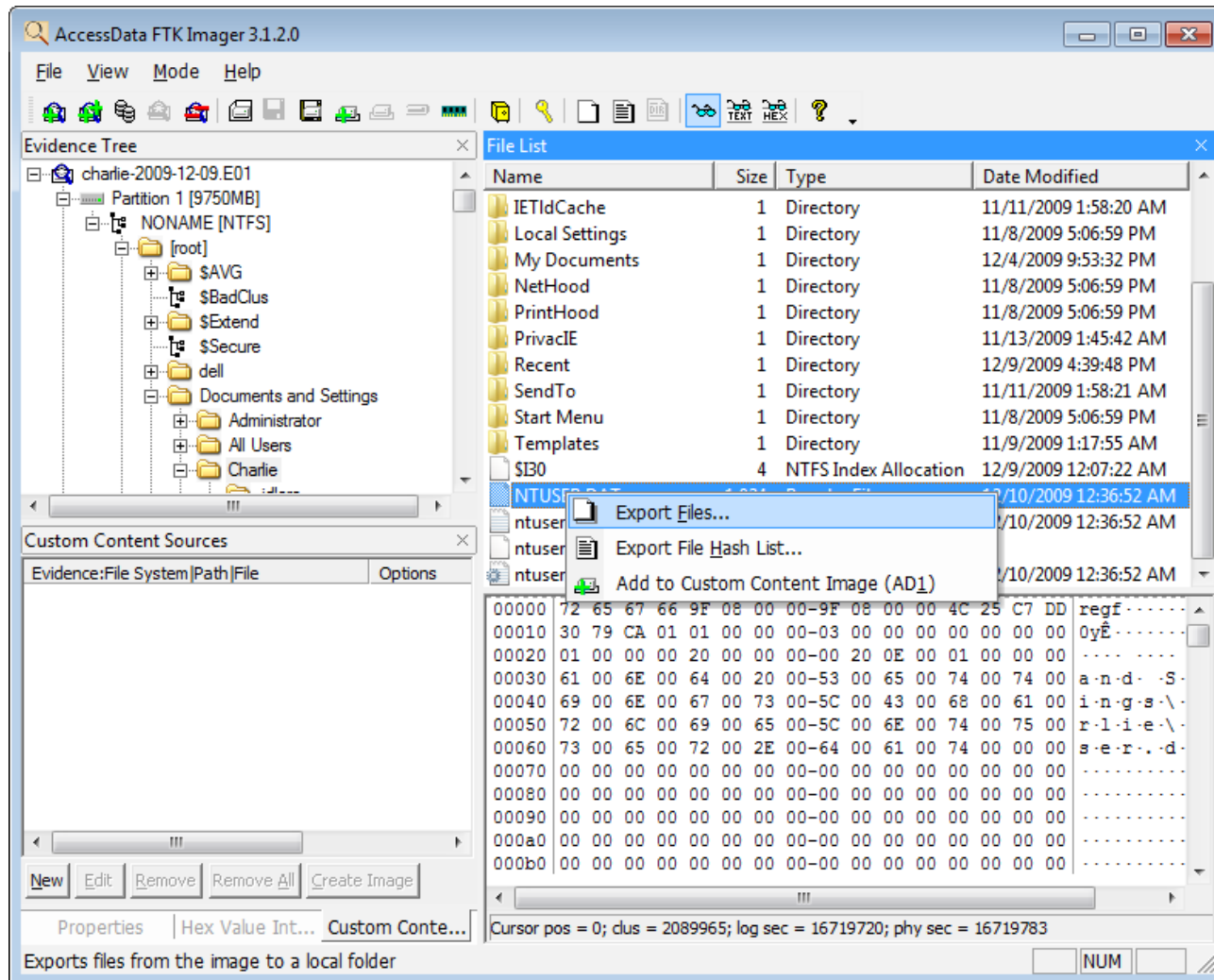
Relative Identifier (RID), designating a specific user in the SAM file. Those below 1000 are default accounts (e.g. 500 = Administrator), and those 1000 or above are created for specific groups or users.

Examining an NTUSER.DAT File

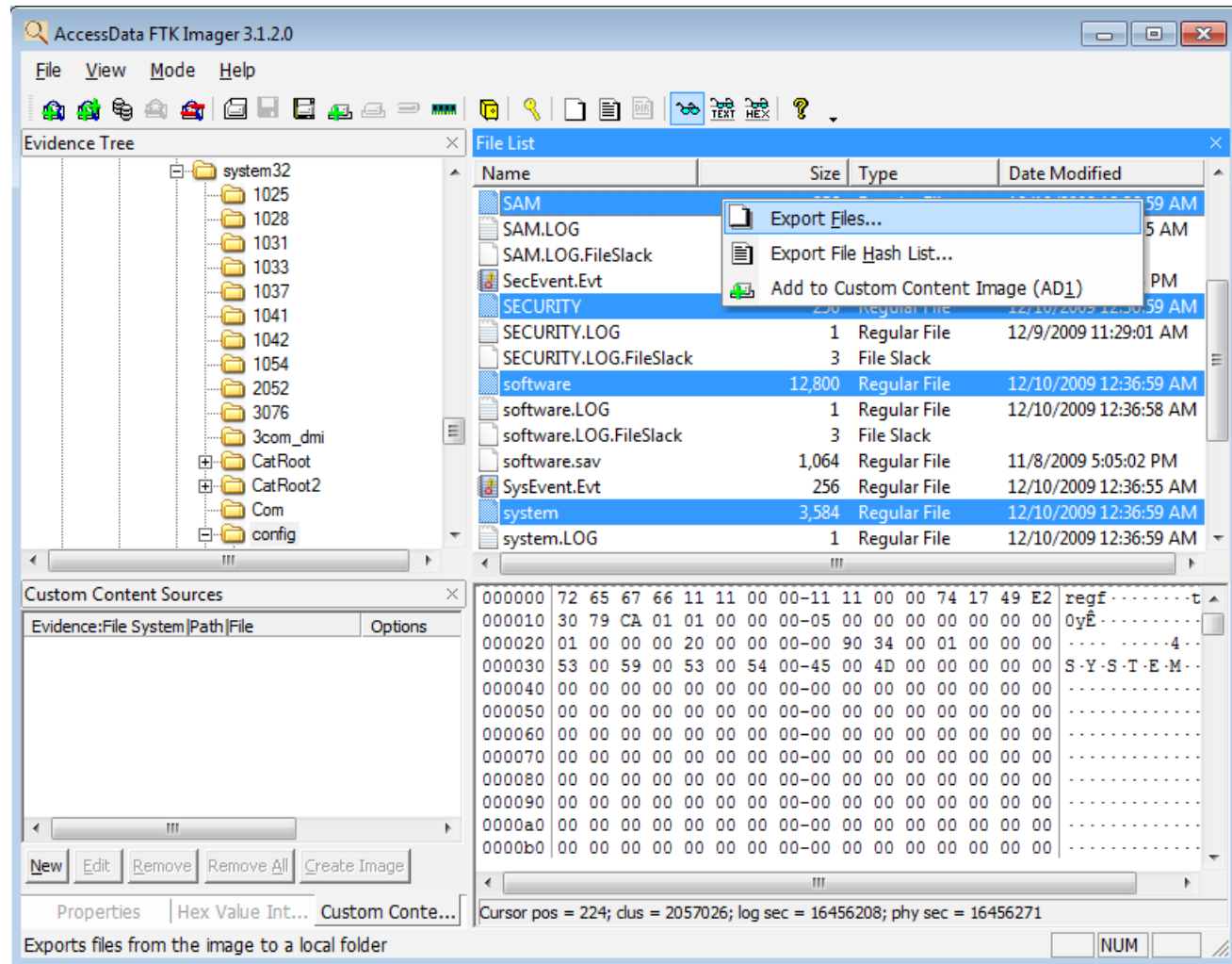
- The files used for this exercise in registry.zip were extracted from a full-drive (including the operating system) disk image
- The following is an example of how these files can be extracted using FTK Imager

FTK Imager

- Navigate to: Partition 1 [*or you basic partition] > [root] > user > NTUSER.DAT
- Right click on NTUSER.DAT and select Export Files.

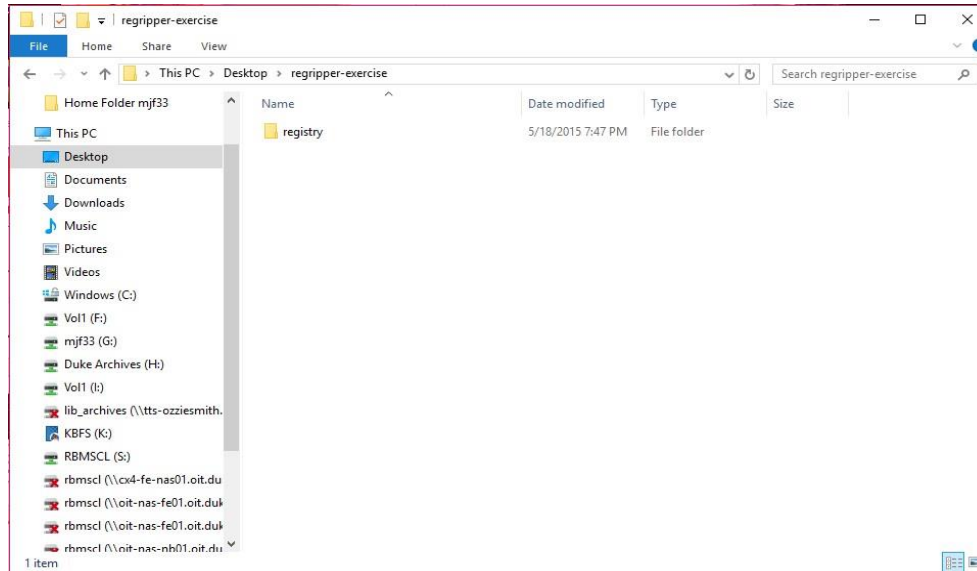


Then export the other four registry files from Windows\System32\config



RegRipper

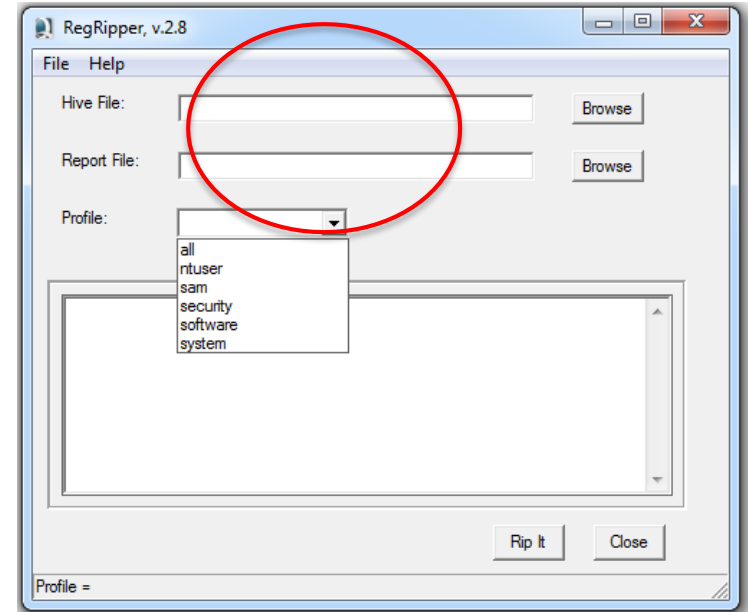
RegRipper Instructions – Windows I



- 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?
- Is there any other information you find particularly compelling in this report?
- What might you do with this information?

- Are you able to identify the files that the user (Pat) recently opened? If so, what were they?

```

153 -----
154 comdlg32 v.20200517
155
156 Software\Microsoft\Windows\CurrentVersion\Explorer\ComDlg32
157 LastWrite Time 2009-11-18 17:28:10Z
158 LastVisitedMRU
159 LastWrite: 2009-12-07 21:57:15Z
160 MRUList = abgfedc
161 a -> EXE: soffice.bin
162   -> Last Dir: C:\Documents and Settings\Pat\My Documents
163 b -> EXE: iexplore.exe
164   -> Last Dir: C:\Documents and Settings\Pat\Desktop
165 g -> EXE: ToolKeylogger.exe
166   -> Last Dir: C:\Documents and Settings\Pat\Desktop\logs\20091203
167 f -> EXE: firefox.exe
168   -> Last Dir: C:\Documents and Settings\Pat\My Documents
169 e -> EXE: AcroRd32.exe
170   -> Last Dir: C:\Documents and Settings\Pat\My Documents
171 d -> EXE: msimn.exe
172   -> Last Dir: C:\Documents and Settings\Pat\My Documents\Other Patent
173 c -> EXE: rundll32.exe
174   -> Last Dir: C:\Documents and Settings\Pat\My Documents
175
176
177 OpenSaveMRU
178 LastWrite: 2009-12-07 16:08:55Z
179 OpenSaveMRU\OpenSaveMRU
180 LastWrite time: 2009-12-07 16:08:55Z
181 OpenSaveMRU has no values.
182
183 OpenSaveMRU\*
184 LastWrite time: 2009-12-07 16:08:55Z
185 MRUList = gfedcbajih
186 g -> C:\Documents and Settings\Pat\Desktop\avg_free_stb_all_9_40_cnet.exe
187 f -> C:\Documents and Settings\Pat\Desktop\logs\20091203\2009-12-03.htm
188 e -> C:\WINDOWS\WinSxS\2009-12-03.htm
189 d -> C:\Documents and Settings\Pat\My Documents\QuantCryptStuff\Method_
190 c -> C:\Documents and Settings\Pat\My Documents\QuantCryptStuff\Free_sp
191 b -> C:\Documents and Settings\Pat\My Documents\Quantum_cryptography.pdf
192 a -> C:\Documents and Settings\Pat\My Documents\DMC_03302007_2-05cv184_
193 j -> C:\Documents and Settings\Pat\My Documents\Patent.Misc\26-apc-145_
194 i -> C:\Documents and Settings\Pat\My Documents\Patent.Misc\E5R8_600.pd
195 h -> C:\Documents and Settings\Pat\My Documents\Patent.Misc\Ch700.Exami
196
197 OpenSaveMRU\exe
198
199
200
201
202 OpenSaveMRU\htm
203 LastWrite time: 2009-12-07 16:03:19Z
204 MRUList = ba
205 b -> C:\Documents and Settings\Pat\Desktop\logs\20091203\2009-12-03.htm
206 a -> C:\WINDOWS\WinSxS\2009-12-03.htm
207
208 OpenSaveMRU\JPG
209 LastWrite time: 2009-11-20 16:49:19Z
210 MRUList = a
211 a -> C:\Documents and Settings\Pat\My Documents\ABCTECH_RECEIPT_pat.JPG
212
213 OpenSaveMRU\pdf
214 LastWrite time: 2009-12-02 17:02:51Z
215 MRUList = cbajihgfed
216 c -> C:\Documents and Settings\Pat\My Documents\QuantCryptStuff\Method_for_key_dis
217 b -> C:\Documents and Settings\Pat\My Documents\QuantCryptStuff\Free_space_quantum
218 a -> C:\Documents and Settings\Pat\My Documents\Quantum_cryptography.pdf
219 j -> C:\Documents and Settings\Pat\My Documents\DMC_03302007_2-05cv184_ITI_v_Profe
220 i -> C:\Documents and Settings\Pat\My Documents\Patent.Misc\26-apc-145.pdf
221 h -> C:\Documents and Settings\Pat\My Documents\Patent.Misc\E5R8_600.pdf
222 g -> C:\Documents and Settings\Pat\My Documents\Patent.Misc\Ch700.ExaminationOf_Ap
223 f -> C:\Documents and Settings\Pat\My Documents\Other Patent\DBGT_council_report_2
224 e -> C:\Documents and Settings\Pat\My Documents\104416fireextinguishersDFMmetriciz
225 d -> C:\Documents and Settings\Pat\My Documents\Other Patent\String_vibration_tran
226
227
228

```

Normal text file | length: 45,196 | lines: 1,025 | Ln: 156 | Col: 60

- Can you determine what the most recently open files of specific types (e.g. txt) were?

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?

- How many accounts were there on this computer?

```

7  User Information
8
9  Username       : Administrator [500]
10 SID           : S-1-5-21-1292428093-1645522239-1547161642-500
11 Full Name     :
12 User Comment   : Built-in account for administering the computer/domain
13 Account Type   : Default Admin User
14 Account Created : Sun Nov  8 15:35:15 2009 Z
15 Name          :
16 Last Login Date : Tue Nov 10 01:21:04 2009 Z
17 Pwd Reset Date  : Sun Dec  6 16:23:59 2009 Z
18 Pwd Fail Date   : Tue Nov 10 19:18:30 2009 Z
19 Login Count    : 4
20 --> Password does not expire
21 --> Normal user account
22
23 Username       : Guest [501]
24 SID           : S-1-5-21-1292428093-1645522239-1547161642-50
25 Full Name     :
26 User Comment   : Built-in account for guest access to the com
27 Account Type   : Default Guest Acct
28 Account Created : Sun Nov  8 15:35:15 2009 Z
29 Name          :
30 Last Login Date : Never
31 Pwd Reset Date  : Never
32 Pwd Fail Date   : Never
33 Login Count    : 0
34 --> Password does not expire
35 --> Account Disabled
36 --> Password not required
37 --> Normal user account
38
39 Username       : HelpAssistant [1000]
40 SID           : S-1-5-21-1292428093-1645522239-1547161642-10
41 Full Name     : Remote Desktop Help Assistant Account
42 User Comment   : Account for Providing Remote Assistance
43 Account Type   : Custom Limited Acct
44 Account Created : Mon Nov  9 00:23:19 2009 Z
45 Name          :
46 Last Login Date : Never
47 Pwd Reset Date  : Mon Nov  9 00:23:19 2009 Z
48 Pwd Fail Date   : Never
49 Login Count    : 0
50 --> Password does not expire
51 --> Account Disabled
52 --> Normal user account
53
54 Username       : SUPPORT_388945a0 [1002]
55 SID           : S-1-5-21-1292428093-1645522239-1547161642-1002
56 Full Name     : CN=Microsoft Corporation,L=Redmond,S=Washington,C=US
57 User Comment   : This is a vendor's account for the Help and Support Service
58 Account Type   : Custom Limited Acct
59 Account Created : Mon Nov  9 00:27:58 2009 Z
60 Name          :
61 Last Login Date : Never
62 Pwd Reset Date  : Mon Nov  9 00:27:58 2009 Z
63 Pwd Fail Date   : Never
64 Login Count    : 0
65 --> Password does not expire
66 --> Account Disabled
67 --> Normal user account
68
69 Username       : Pat [1003]
70 SID           : S-1-5-21-1292428093-1645522239-1547161642-1003
71 Full Name     : Pat
72 User Comment   :
73 Account Type   : Default Admin User
74 Account Created : Tue Nov 10 19:18:56 2009 Z
75 Name          :
76 Last Login Date : Tue Dec  8 01:45:07 2009 Z
77 Pwd Reset Date  : Never
78 Pwd Fail Date   : Never
79 Login Count    : 86
80 --> Password does not expire
81 --> Normal user account
82
83 -----

```


- How many logins did Pat make on this machine?

```
C:\Users\JA\Desktop\private_staff\Training Folder\Classes\Digital Curation - Lifecycle Management\NTUserReport\SamReport.txt - Notepad++
File Edit Search View Encoding Language Settings Tools Macro Run TextFX Plugins Window ?
NTUserreport_1.txt SamReport.txt SecurityReport.txt softwarereport.txt systemreport.txt
54 Username      : SUPPORT_388945a0 [1002]
55 SID          : S-1-5-21-1292428093-1645522239-1547161642-1002
56 Full Name    : CN=Microsoft Corporation,L=Redmond,S=Washington,C=US
57 User Comment : This is a vendor's account for the Help and Support Service
58 Account Type : Custom Limited Acct
59 Account Created : Mon Nov  9 00:27:58 2009 Z
60 Name         :
61 Last Login Date : Never
62 Pwd Reset Date  : Mon Nov  9 00:27:58 2009 Z
63 Pwd Fail Date   : Never
64 Login Count    : 0
65 --> Password does not expire
66 --> Account Disabled
67 --> Normal user account
68
69 Username      : Pat [1003]
70 SID          : S-1-5-21-1292428093-1645522239-1547161642-1003
71 Full Name    : Pat
72 User Comment :
73 Account Type : Default Admin User
74 Account Created : Tue Nov 10 19:18:56 2009 Z
75 Name         :
76 Last Login Date : Tue Dec  8 01:45:07 2009 Z
77 Pwd Reset Date  : Never
78 Pwd Fail Date   : Never
79 Login Count    : 86
80 --> Password does not expire
81 --> Normal user account
82
83
84 Group Membership Information
85 -----
86 Group Name    : Power Users [0]
87 LastWrite     : Sun Nov  8 15:35:15 2009 Z
88 Group Comment : Power Users possess most administrative powers with some restrictions. Thus, Power Users can run legacy applications in addition to certified applications
89 Users        : None
90
91 Group Name    : Users [3]
92 LastWrite     : Sun Dec  6 17:22:28 2009 Z
93 Group Comment : Users are prevented from making accidental or intentional system-wide changes. Thus, Users can run certified applications, but not most legacy applications
94 Users :
95 S-1-5-4
96 S-1-5-11
97 S-1-5-21-1292428093-1645522239-1547161642-1003
98
99 Group Name    : Replicator [0]
100 LastWrite     : Sun Nov  8 15:35:15 2009 Z
101 Group Comment : Supports file replication in a domain
102 Users        : None
103
104 Group Name    : Guests [1]
```

- What was the Relative Identifier (RID) for the user account you're examining?

```

C:\Users\JA\Desktop\private_staff\Training Folder\Classes\Digital Curation - Lifecycle Management\NTUserReport\SamReport.txt - Notepad++
File Edit Search View Encoding Language Settings Tools Macro Run TextFX Plugins Window ?
NTUserReport_1.txt SamReport.txt SecurityReport.txt softwarereport.txt systemreport.txt
54 Username      : SUPPORT_388945a0 [1002]
55 SID          : S-1-5-21-1292428093-1645522239-1547161642-1002
56 Full Name    : CN=Microsoft Corporation,L=Redmond,S=Washington,C=US
57 User Comment : This is a vendor's account for the Help and Support Service
58 Account Type : Custom Limited Acct
59 Account Created : Mon Nov  9 00:27:58 2009 Z
60 Name        :
61 Last Login Date : Never
62 Pwd Reset Date : Mon Nov  9 00:27:58 2009 Z
63 Pwd Fail Date  : Never
64 Login Count   : 0
65 --> Password does not expire
66 --> Account Disabled
67 --> Normal user account
68
69 Username      : Pat [1003]
70 SID          : S-1-5-21-1292428093-1645522239-1547161642-1003
71 Full Name     : Pat
72 User Comment  :
73 Account Type  : Default Admin User
74 Account Created : Tue Nov 10 19:18:56 2009 Z
75 Name         :
76 Last Login Date : Tue Dec  8 01:45:07 2009 Z
77 Pwd Reset Date : Never
78 Pwd Fail Date  : Never
79 Login Count   : 86
80 --> Password does not expire
81 --> Normal user account
82
83 -----
84 Group Membership Information
85 -----
86 Group Name    : Power Users [0]
87 LastWrite     : Sun Nov  8 15:35:15 2009 Z
88 Group Comment : Power Users possess most administrative powers with some restrictions. Thus, Power Users can run legacy applications in addition to certified applications
89 Users        : None
90
91 Group Name    : Users [3]
92 LastWrite     : Sun Dec  6 17:22:28 2009 Z
93 Group Comment : Users are prevented from making accidental or intentional system-wide changes. Thus, Users can run certified applications, but not most legacy applications
94 Users :
95   S-1-5-4
96   S-1-5-11
97   S-1-5-21-1292428093-1645522239-1547161642-1003
98
99 Group Name    : Replicator [0]
100 LastWrite     : Sun Nov  8 15:35:15 2009 Z
101 Group Comment : Supports file replication in a domain
102 Users        : None
103
104 Group Name    : Guests [1]

```

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?

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?

- Identify three different applications that were installed on this computer

```
NTUserreport_1.txt SecurityReport.txt softwarereport.txt systemreport.txt
9945 -----
9946
9947 Launching installer v.20200517
9948 (Software) Determines product install information
9949
9950 Installer
9951 Microsoft\Windows\CurrentVersion\Installer\UserData
9952
9953 User SID: S-1-5-18
9954 Key : 0B79C053C7D38EE4AB9A00CB3B5D2472
9955 LastWrite: 2009-11-20 20:00:19Z
9956 20091120 - WebFldrs XP 9.50.7523 (Microsoft Corporation)
9957
9958 Key : 3e43b73803c7c394f8a6b2f0402e19c2
9959 LastWrite: 2009-11-20 18:55:34Z
9960 20091120 - Microsoft Visual C++ 2005 Redistributable 8.0.59193 (Microsoft Corporation)
9961
9962 Key : 4CD78B6ED3B23844DAFF4E38FB179819
9963 LastWrite: 2009-11-20 19:38:28Z
9964 20091120 - OpenOffice.org 3.1 3.1.9420 (OpenOffice.org)
9965
9966 Key : 4EA42A62D9304AC4784BF238120661FF
9967 LastWrite: 2009-11-20 19:36:06Z
9968 20091120 - Java(TM) 6 Update 16 6.0.160 (Sun Microsystems, Inc.)
9969
9970 Key : 68AB67CA7DA73301B7449A0200000010
9971 LastWrite: 2009-11-30 16:51:35Z
9972 20091130 - Adobe Reader 9.2 9.2.0 (Adobe Systems Incorporated)
9973
9974 Key : B6ED15411EBA26F4EBA93B361A57882A
9975 LastWrite: 2009-11-24 22:11:29Z
9976 20091124 - QuickTime 7.65.17.80 (Apple Inc.)
9977
9978 Key : F0A4937E08F31B5478CFBADC15982364
9979 LastWrite: 2009-11-23 18:23:53Z
9980 20091123 - Python 2.6.4 2.6.4150 (Python Software Foundation)
9981
9982 Key : F65865963B6B0EB4ABB0F894B53E0233
9983 LastWrite: 2009-11-24 22:09:32Z
9984 20091124 - Apple Software Update 2.1.1.116 (Apple Inc.)
9985
9986 Key : FD563AF386D2DE54F838C8A8336E1534
9987 LastWrite: 2009-11-24 22:09:59Z
9988 20091124 - Apple Application Support 1.1.0 (Apple Inc.)
9989
<
Normal text file length: 633,106 lines: 10,779 Ln: 1 Col: 1 Pos: 1 Winc
```

RegRipper Output Discussion: **system-report**


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

- Find the devclass output

```

204
205 ControlSet001\Enum\SWD\DAFUFPProvider not found.
206 -----
207 devclass v.20200525
208 (System) Get USB device info from the DeviceClasses keys in the System hive
209
210 DevClasses - Disks
211 ControlSet001\Control\DeviceClasses\{53f56307-b6bf-11d0-94f2-00a0c91efb8b}
212
213 2009-12-07 16:05:04Z
214 Disk&Ven_USB_2.0&Prod_Flash_Disk&Rev_8.00,51491E64&0
215 2009-11-25 03:46:50Z
216 Disk&Ven_&Prod_&Rev_,152D203380B6&0
217 2009-11-17 20:52:34Z
218 Disk&Ven_SanDisk&Prod_Cruzer&Rev_7.01,43175107A4C24AD4&0
219 2009-11-17 00:06:21Z
220 Disk&Ven_LaCie&Prod_Rugged_FW,USB&Rev_
221 2009-11-10 23:41:25Z
222 Disk&Ven_LaCie&Prod_Rugged_FW,USB&Rev_
223
224 DevClasses - Volumes
225 ControlSet001\Control\DeviceClasses\{53f5630d-b6bf-11d0-94f2-00a0c91efb8b}
226
227 2009-12-07 16:05:04Z
228 ParentIdPrefix: 7&18ec28b&0&RM
229 2009-11-17 20:52:34Z
230 ParentIdPrefix: 7&71229d7&0&RM
231 ControlSet001\Control\DeviceClasses\{10497b1b-ba51-44e5-8318-a65c837b6661} not found.
232 -----
233 disablelastaccess v.20200517
234 (System) Get NTFSDisableLastAccessUpdate value
235
236 NtfsDisableLastAccessUpdate
237 ControlSet001\Control\FileSystem
238 Key LastWrite time: 2009-11-08 15:37:47Z
239 NtfsDisableLastAccessUpdate value not found.
240 -----
241 disableremotescm v.20200513
242 (System) Gets DisableRemoteScmEndpoints value from System hive
243
244 DisableRemoteScmEndpoints value not found.
245 -----
246 environment v.20200512
247 (System, NTUSER.DAT) Get environment vars from NTUSER.DAT & System hives
248

```



Normal text file Length: 165,074 Lines: 2,204 Loc: 307 Cols: 20 Rows: 12,030 Window

Bulk Extractor

BULK EXTRACTOR

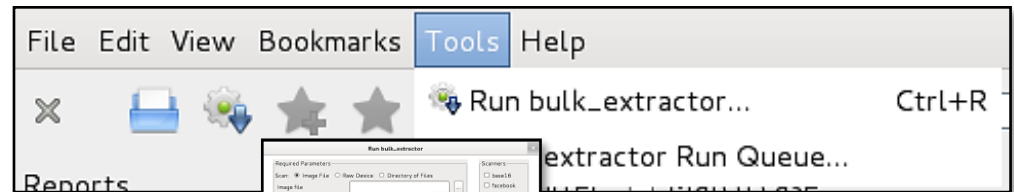
The current version of **bulk_extractor** is 1.5.5

https://downloads.digitalcorpora.org/downloads/bulk_extractor/

- The program is a computer **forensics tool** that scans a disk image, a file, or a directory of files and extracts useful information without parsing the file system or file system structures (https://forensics.wiki/bulk_extractor/)
- **Bulk Extractor** is used for law enforcement, defense, intelligence, and cyber-investigation applications.

BULK EXTRACTOR

Click on the Tools option and
then run bulk_extractor



Click the location to scan



BULK EXTRACTOR

Scanners

- ☐ base16
- ☐ facebook
- ☐ outlook
- ☐ sceadan
- ☐ wordlist
- ☐ xor
- ☒ accts
- ☒ aes
- ☒ base64
- ☒ elf
- ☒ email
- ☒ exif
- ☒ find
- ☒ gps
- ☒ gzip
- ☒ hiberfile
- ☒ httplogs
- ☒ json
- ☒ kml
- ☒ msxml
- ☒ net
- ☒ pdf
- ☒ rar
- ☒ sqlite
- ☒ vcard
- ☒ windirs
- ☒ winlnk
- ☒ winpe
- ☒ winprefetch
- ☒ zip

- **Accts** searches for credit card numbers, track data, phone numbers, and other numbers
- **AES** finds AES keys
- **Base64** Searches for Base64 encoded text
- **Elf** Searches for ELF type files.
- **Email** Searches for headers, cookies, hostnames, IPs, emails, and URLs.
- **Exif** Finds images and their metadata
- **Find** Used for finding specific regular expressions
- **GPS** finds Garmin-formatted XML containing GPS coordinates
- **Gzip** Finds gzip compressed files
- **Hiberfile** Finds the Windows hibernation file
- **Httplogs** Finds HTTP log files
- **Json** Searches for JSON type files
- **Kml** Finds KML type files.
- **Msxml** Searches for Microsoft XML Core Services
- **Net** Finds packets in memory
- **Pdf** Searches for text from PDF files
- **Rar** Searches for RAR compressed files
- **Sqlite** Finds SQLite3 database files
- **Vcard** Finds vCard type files
- **Windirs** Searches for Windows directories
- **Winlnk** Finds Windows LNK files
- **Winpe** Searches for windows executables and dlls.
- **Winprefetch** Searches for prefetch files.
- **Zip** Searches for ZIP compressed files

Click the scanners/file-types

BULK EXTRACTOR

Bulk Extractor Viewer
File Edit View Bookmarks Tools Help

Highlight: ☒ Match case

Reports

- Report
- domain.txt
- domain_histogram.txt
- email.txt
- email_domain_histogram.txt
- email_histogram.txt
- hex.txt
- rfc822.txt
- url.txt
- url_histogram.txt
- url_services.txt
- winlnk.txt
- wordlist.txt

Feature Filter ☐ Match case

Feature File email.txt

Inning Folder\Classes\Digital Curation - Lifecycle Management\LAB	2\bcc-dfa-sample-data-main\bcc-dfa-sample-data-main\registry\NTUSER.DAT00000000-660076	pat@m57.biz
Inning Folder\Classes\Digital Curation - Lifecycle Management\LAB	2\bcc-dfa-sample-data-main\bcc-dfa-sample-data-main\registry\NTUSER.DAT00000000-670152	pat@m57.biz
Inning Folder\Classes\Digital Curation - Lifecycle Management\LAB	2\bcc-dfa-sample-data-main\bcc-dfa-sample-data-main\registry\NTUSER.DAT00000000-708964	pat@m57.biz
Inning Folder\Classes\Digital Curation - Lifecycle Management\LAB	2\bcc-dfa-sample-data-main\bcc-dfa-sample-data-main\registry\SOFTWARE00000000-7943661	personal.freemal@thawte.com
Inning Folder\Classes\Digital Curation - Lifecycle Management\LAB	2\bcc-dfa-sample-data-main\bcc-dfa-sample-data-main\registry\SOFTWARE00000000-7943905	personal.freemal@thawte.com
Inning Folder\Classes\Digital Curation - Lifecycle Management\LAB	2\bcc-dfa-sample-data-main\bcc-dfa-sample-data-main\registry\SOFTWARE00000000-7946391	ips@mail.ips.es
Inning Folder\Classes\Digital Curation - Lifecycle Management\LAB	2\bcc-dfa-sample-data-main\bcc-dfa-sample-data-main\registry\SOFTWARE00000000-7948589	ips@mail.ips.es
Inning Folder\Classes\Digital Curation - Lifecycle Management\LAB	2\bcc-dfa-sample-data-main\bcc-dfa-sample-data-main\registry\SOFTWARE00000000-7950791	server-cert@thawte.com
Inning Folder\Classes\Digital Curation - Lifecycle Management\LAB	2\bcc-dfa-sample-data-main\bcc-dfa-sample-data-main\registry\SOFTWARE00000000-7951022	server-cert@thawte.com
Inning Folder\Classes\Digital Curation - Lifecycle Management\LAB	2\bcc-dfa-sample-data-main\bcc-dfa-sample-data-main\registry\SOFTWARE00000000-7953175	info@valicert.com
Inning Folder\Classes\Digital Curation - Lifecycle Management\LAB	2\bcc-dfa-sample-data-main\bcc-dfa-sample-data-main\registry\SOFTWARE00000000-7953397	info@valicert.com
Inning Folder\Classes\Digital Curation - Lifecycle Management\LAB	2\bcc-dfa-sample-data-main\bcc-dfa-sample-data-main\registry\SOFTWARE00000000-7954924	personal-premium@thawte.com
Inning Folder\Classes\Digital Curation - Lifecycle Management\LAB	2\bcc-dfa-sample-data-main\bcc-dfa-sample-data-main\registry\SOFTWARE00000000-7960000	premium@thawte.com
Inning Folder\Classes\Digital Curation - Lifecycle Management\LAB	2\bcc-dfa-sample-data-main\bcc-dfa-sample-data-main\registry\SOFTWARE00000000-7969180	ste.org
Inning Folder\Classes\Digital Curation - Lifecycle Management\LAB	2\bcc-dfa-sample-data-main\bcc-dfa-sample-data-main\registry\SOFTWARE00000000-7980503	ste.org
Inning Folder\Classes\Digital Curation - Lifecycle Management\LAB	2\bcc-dfa-sample-data-main\bcc-dfa-sample-data-main\registry\SOFTWARE00000000-7980744	s@saunalahti.fi
Inning Folder\Classes\Digital Curation - Lifecycle Management\LAB	2\bcc-dfa-sample-data-main\bcc-dfa-sample-data-main\registry\SOFTWARE00000000-7988695	gaurous@saunalahti.fi
Inning Folder\Classes\Digital Curation - Lifecycle Management\LAB	2\bcc-dfa-sample-data-main\bcc-dfa-sample-data-main\registry\SOFTWARE00000000-7988917	gold-cert@saunalahti.fi
Inning Folder\Classes\Digital Curation - Lifecycle Management\LAB	2\bcc-dfa-sample-data-main\bcc-dfa-sample-data-main\registry\SOFTWARE00000000-8006582	premium-server@thawte.com
Inning Folder\Classes\Digital Curation - Lifecycle Management\LAB	2\bcc-dfa-sample-data-main\bcc-dfa-sample-data-main\registry\SOFTWARE00000000-8010150	premium-server@thawte.com
Inning Folder\Classes\Digital Curation - Lifecycle Management\LAB	2\bcc-dfa-sample-data-main\bcc-dfa-sample-data-main\registry\SOFTWARE00000000-8010365	info@valicert.com
Inning Folder\Classes\Digital Curation - Lifecycle Management\LAB	2\bcc-dfa-sample-data-main\bcc-dfa-sample-data-main\registry\SOFTWARE00000000-8013089	info@valicert.com
Inning Folder\Classes\Digital Curation - Lifecycle Management\LAB	2\bcc-dfa-sample-data-main\bcc-dfa-sample-data-main\registry\SOFTWARE00000000-8013270	certificate@trustcenter.de
Inning Folder\Classes\Digital Curation - Lifecycle Management\LAB	2\bcc-dfa-sample-data-main\bcc-dfa-sample-data-main\registry\SOFTWARE00000000-8013824	certificate@trustcenter.de
Inning Folder\Classes\Digital Curation - Lifecycle Management\LAB	2\bcc-dfa-sample-data-main\bcc-dfa-sample-data-main\registry\SOFTWARE00000000-8030279	certificate@trustcenter.de
Inning Folder\Classes\Digital Curation - Lifecycle Management\LAB	2\bcc-dfa-sample-data-main\bcc-dfa-sample-data-main\registry\SOFTWARE00000000-8030502	correo_cer@correo.com.uy
Inning Folder\Classes\Digital Curation - Lifecycle Management\LAB	2\bcc-dfa-sample-data-main\bcc-dfa-sample-data-main\registry\SOFTWARE00000000-8042943	correo_cer@correo.com.uy
Inning Folder\Classes\Digital Curation - Lifecycle Management\LAB	2\bcc-dfa-sample-data-main\bcc-dfa-sample-data-main\registry\SOFTWARE00000000-8043166	ellenorzes@netlock.net
Inning Folder\Classes\Digital Curation - Lifecycle Management\LAB	2\bcc-dfa-sample-data-main\bcc-dfa-sample-data-main\registry\SOFTWARE00000000-8043166	ops@netlock.net
Inning Folder\Classes\Digital Curation - Lifecycle Management\LAB	2\bcc-dfa-sample-data-main\bcc-dfa-sample-data-main\registry\SOFTWARE00000000-8043166	adman@digisigtrust.com
Inning Folder\Classes\Digital Curation - Lifecycle Management\LAB	2\bcc-dfa-sample-data-main\bcc-dfa-sample-data-main\registry\SOFTWARE00000000-8043166	adman@digisigtrust.com
Inning Folder\Classes\Digital Curation - Lifecycle Management\LAB	2\bcc-dfa-sample-data-main\bcc-dfa-sample-data-main\registry\SOFTWARE00000000-8043166	certificate@trustcenter.de
Inning Folder\Classes\Digital Curation - Lifecycle Management\LAB	2\bcc-dfa-sample-data-main\bcc-dfa-sample-data-main\registry\SOFTWARE00000000-8043166	certificate@trustcenter.de
Inning Folder\Classes\Digital Curation - Lifecycle Management\LAB	2\bcc-dfa-sample-data-main\bcc-dfa-sample-data-main\registry\SOFTWARE00000000-8043166	certificate@trustcenter.de
Inning Folder\Classes\Digital Curation - Lifecycle Management\LAB	2\bcc-dfa-sample-data-main\bcc-dfa-sample-data-main\registry\SOFTWARE00000000-8043166	certificate@trustcenter.de

Image File registry
Feature File email.txt
Forensic Path C:\Users\JA\Desktop\private_staff\Trainin...
Feature pat@m57.biz

Image

After scanning all of the information outputs into new window

Referenced Feature File None
Referenced Feature None

BULK EXTRACTOR

The screenshot displays the Bulk Extractor application window. The left pane shows a 'Report' list of files, with 'email_domain_histogram.txt' selected. The main pane shows the contents of this file, listing email addresses and their frequencies. An orange text box is overlaid on the main pane with the text: 'The same information is in the local output file in individual text documents'. The right pane shows a file explorer view of the output files, including 'email_domain_histogram.txt' and 'report.xml'.

Report

- domain.txt
- domain_histogram.txt
- email.txt
- email_domain_histogram.txt
- email_histogram.txt
- hex.txt
- rfc822.txt
- url.txt
- url_histogram.txt
- url_services.txt
- winlink.txt
- wordlist.txt

Feature Filter ☐ Match case

Histogram File email_domain_histogram.txt

n	email
n=12	@thawte.com
n=8	@trustcenter.de
n=6	@netlock.net
n=6	@saunalahti.fi
n=6	@valicert.com
n=4	@feste.org
n=2	@correo.com.uy
n=2	@digistrust.com
n=2	@e-trust.be

Referenced Feature File email.txt

Referenced Feature None

C:\Users\JA\Desktop\private_staff\Training Folder\Classes\Digital Curation - Lifecycle Management\LAB 2\bcc-dfa-sample-data-main\registry\SO...

51 items 1 item selected 559 bytes

Report

File Home Share View

Pin to Quick access Copy Paste Cut Copy path Move to Copy to Delete Rename New folder New item Easy access Properties Edit History Select all Select none Invert selection

Clipboard Organize New Open Select

LAB 2 > Bulk Extractor > Report

Search Report

Name

- aes_keys.txt
- alerts.txt
- ccn.txt
- ccn_histogram.txt
- ccn_track2.txt
- ccn_track2_histogram.txt
- domain.txt
- domain_histogram.txt
- elf.txt
- email.txt
- email_domain_histogram.txt
- email_histogram.txt
- ether.txt
- ether_histogram.txt
- exif.txt
- facebook.txt
- find.txt
- find_histogram.txt
- gps.txt
- hex.txt
- httplogs.txt
- ip.txt
- ip_histogram.txt
- jpeg_carved.txt
- json.txt
- kml.txt
- pii.txt
- pii_teamviewer.txt
- rar.txt
- report.xml
- rfc822.txt
- sqlite_carved.txt
- telephone.txt
- telephone_histogram.txt

BANNER FILE NOT PROVIDED (-b option)

BULK_EXTRACTOR-Version: 1.5.5 (\$Rev: 10844 \$)

Feature-Recorder: email

Filename: C:\Users\JA\Desktop\private_staff\Training Folder\Classes\Digital Curation - Lifecycle Management\LAB 2\bcc-dfa-sample-data-main\registry\SO...

Histogram-File-Version: 1.1

n	email
n=12	@thawte.com
n=8	@trustcenter.de
n=6	@netlock.net
n=6	@saunalahti.fi
n=6	@valicert.com
n=4	@feste.org
n=2	@correo.com.uy
n=2	@digistrust.com
n=2	@e-trust.be
n=2	@mail.ips.es
n=2	@verisign.com
n=1	@m57.biz
n=1	@sun.com

**DataAccessioner – as of 2023
this is no longer supporter by
DUKE University**

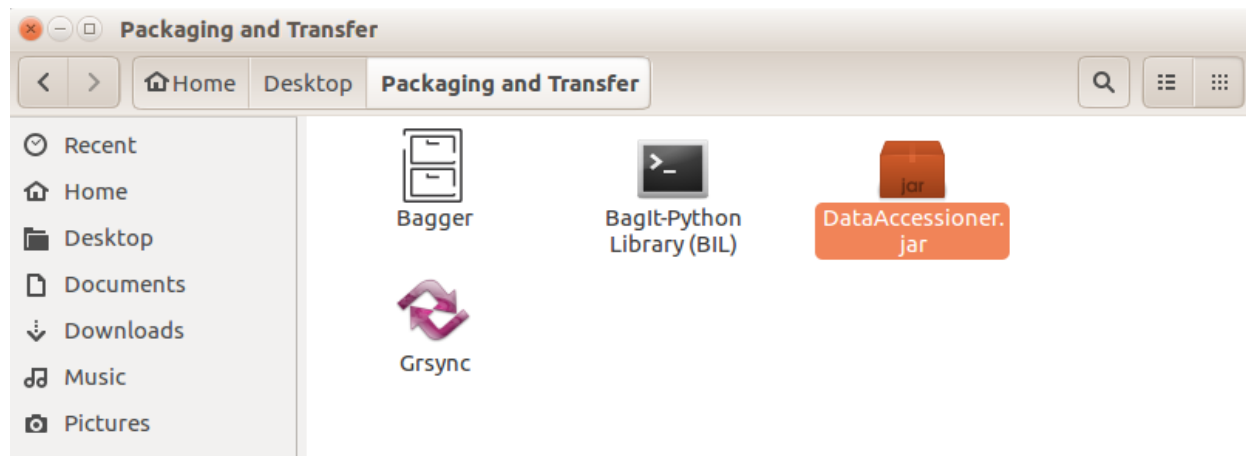
Data Accessioner

Data Accessioner is an archival forensics tool that enables you to securely migrate data by making disk images (bit-level copies) or logical copies from storage media without altering the files in the process. This is important because it helps preserve provenance.

Additional information about Data Accessioner can be found [here](#).

Data Accessioner

1. Open DataAcessioner.jar file

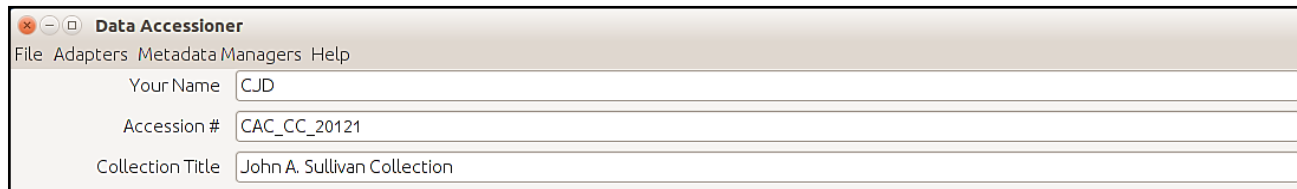


Data Accessioner

2. Create two folders

- Name the folder according to the UnitID, followed by “_master.”
- Make a copy titled in the same manner followed by “_working.”

3. Enter Collection Information



The screenshot shows a window titled "Data Accessioner" with a menu bar containing "File", "Adapters", "Metadata Managers", and "Help". Below the menu bar are three text input fields:

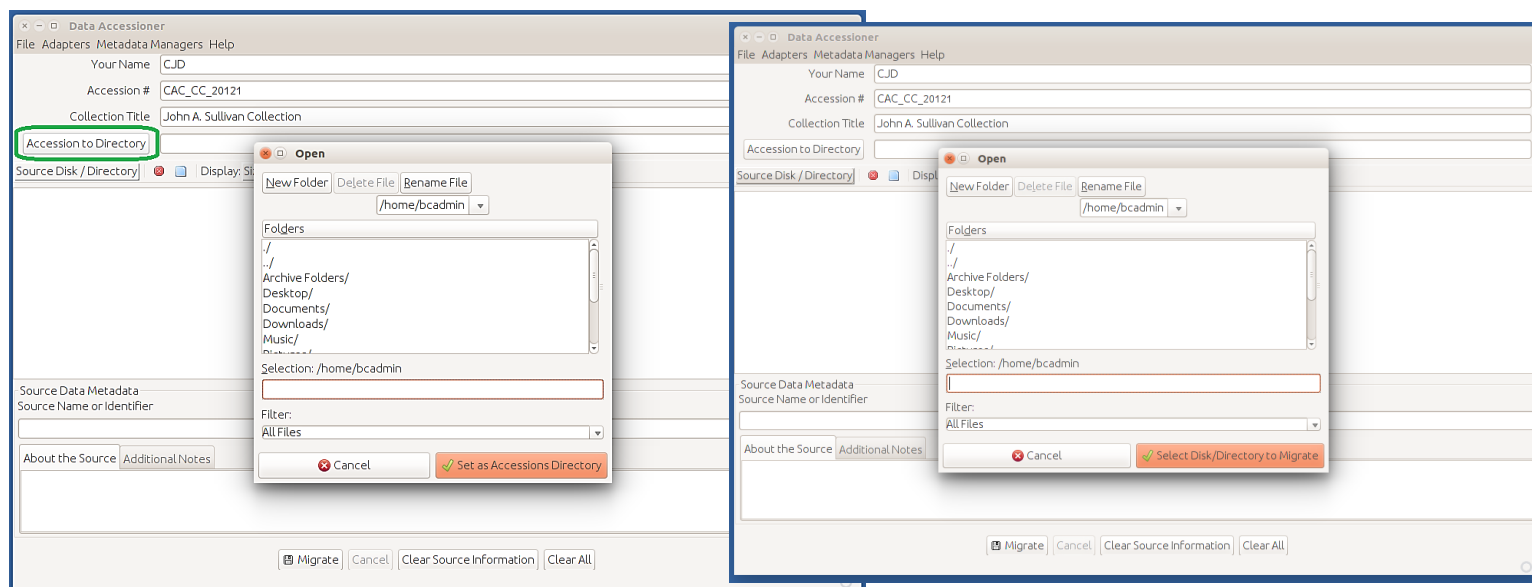
- "Your Name" with the text "CJD" entered.
- "Accession #" with the text "CAC_CC_20121" entered.
- "Collection Title" with the text "John A. Sullivan Collection" entered.

Field	Enter	Example
Name	Archivist Name	PryseJA
Accession #	Collection #	2023_5970
Collection Title	Collection Name	Lab2

Data Accessioner

4. Specify input/output directories

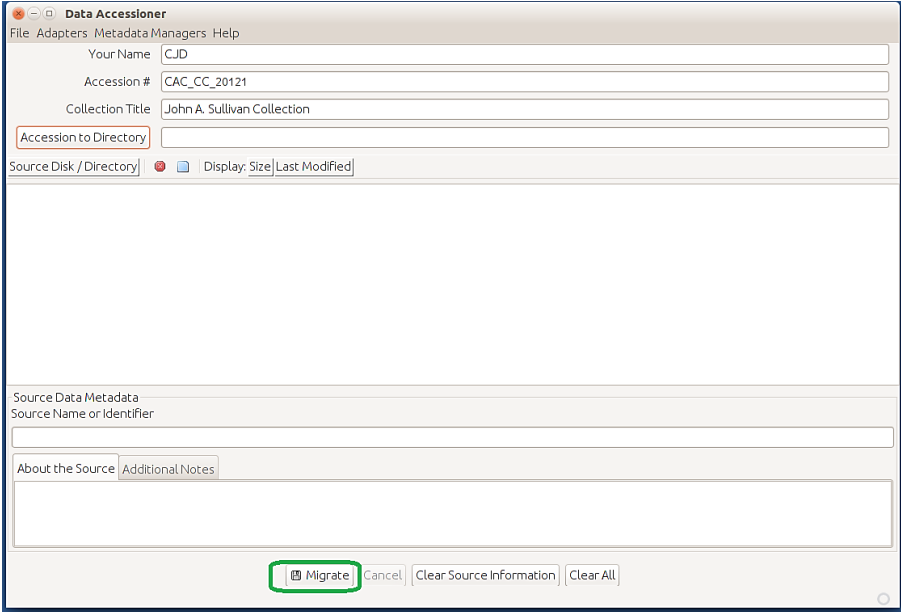
- Where the migrated files will go
- Select “Set as Accessions Directory”
- Select “Source Disk / Directory”



Data Accessioner

6. Migrate data

- Select the “Migrate” button at the bottom of the window.
- The files will be migrated to the specified output directory unless there is an issue



The screenshot shows the 'Data Accessioner' application window. The title bar includes a menu bar with 'File', 'Adapters', 'Metadata Managers', and 'Help'. Below the menu bar, there are four text input fields: 'Your Name' (containing 'CJD'), 'Accession #' (containing 'CAC_CC_20121'), 'Collection Title' (containing 'John A. Sullivan Collection'), and 'Accession to Directory' (which is highlighted with a red box). Below these fields is a section labeled 'Source Disk / Directory' with a red error icon and a 'Display: Size | Last Modified' button. The main area of the window is empty. At the bottom, there is a section labeled 'Source Data Metadata' with a 'Source Name or Identifier' field. Below this is a tabbed interface with 'About the Source' and 'Additional Notes' tabs. The 'Additional Notes' tab is active, showing a large text area. At the very bottom, there is a row of buttons: 'Migrate' (highlighted with a green box), 'Cancel', 'Clear Source Information', and 'Clear All'.

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



BitCuratorEdu

Advancing the adoption of digital forensics tools and methods in libraries and archives through professional education efforts

EDUCOPIA
INSTITUTE
Community Cultivators



This resource was released by the BitCuratorEdu project and is licensed under a [Creative Commons Attribution 4.0 International License](#).

Most resources from the BitCuratorEdu project are intentionally left with basic formatting and without project branding. We encourage educators, practitioners, and students to adapt these materials as much as needed and share them widely.

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.