Lab (Part A): Malware Analysis

You will be split into groups, and allocated an XP instance with Production -> DLP -> Group_xx. Malware can be a considerable cause of data loss. This lab is in two parts. The first part analyses the malware, and the next part looks at the forensic footprint.

1 Details

Aim: To provide a foundation in understanding malware.

A demo of this lab is here: http://youtu.be/t_P7IkJn748

2 Analysing Malware

L1.1 We are going to investigate a variant of **Worm.Win32.Dorkbot.**

Go to virustotal.com and search for a hash of:

82968586a463cf84f6dfc18980f2f69d

What are the key elements of the malware:

L1.2 **You will be assigned groups.** Run the Windows XP image for your group.

L1.3 Now try and connect from Windows XP to the Internet from a browser, and MAKE SURE YOU CANNOT CONNECT.

L1.4 Examine your IP address with IPCONFIG … MAKE SURE YOUR ADDRESS IS 10.0.0.1 AND THAT YOU DO NOT HAVE ANY PUBLIC IP ADDRESSES.

Can you verify that you are not connect to the Internet?

L1.5 Open up a command line console, and using DIR, you should see that you have a file named DQ.EXE.

L1.6 One of the first things we must do is to capture the hash signature of the malware.

Use openssl to determine the hash signature, such as:

```
openssl md5 dq.exe
```

Outline the MD5 and SHA signature

How many characters does MD5 signature have:

How many characters does SHA signature have:

L1.7 Start **Wireshark** and examine the basic flow of network traffic. There should be very little that is interesting in the traffic.

L1.8 Run **RegMon**, so that you can monitor the changes to the registry.

L1.9 Run **ProcMon**, so that you can monitor the changes to processes (reset all the filters).

L1.10 Run the DQ.EXE program from the command console.

What can you observe from running the program:

L1.11 Stop **RegMon** (Ctrl-E).

L1.12 Stop **ProcMon** (Ctrl-E).

L1.13 Go to the c:\recycler folder. Can you find the malware:

What is the c:\recycler folder normally used for:

How did you find the malware?

Run the attrib *.* command, and determine the attributes on the malware files in c:\recycler folder:

Which command do you need to delete the files:

Make sure you have deleted them … check with dir /ah**. Are they gone?**

L1.14 Go to the registry with REGEDIT.EXE. Now go to:

HKCU\Software\Microsoft\Windows\CurrentVersion\Run

Where is the malware located within the Registry:

What does the registry entry do on the system:

L1.15 Examine the Wireshark trace.

What can you observe from the trace that the malware has done:

L1.16 Using HexWin, examine the memory of DQ.EXE. Can you determine anything that you could produce a fingerprint of the malware with:

Possible fingerprint signs:

L1.17 With RegMon, can you find the change of the registry which enabled the malware to sustain itself on the system:

Outline the update:

L1.18 With RegMon, and determine:

The update to the registry to sustain the malware:

The creation of the malware on the file system:

The process running on the system:

4 Clean up virtual machine and restore

L1.19 Now clean up the VM:

Did you manage to delete the files in c:\recyler:

Did you manage to delete the registry key:

After you clean up, reboot the VM, and check that malware is not present:

L1.20 Restore the VM to its original state using **VM->Restore Snapshot**. Lab (Part B): Forensics

Part B (Forensic Analysis)

Analysing a computer using forensic software

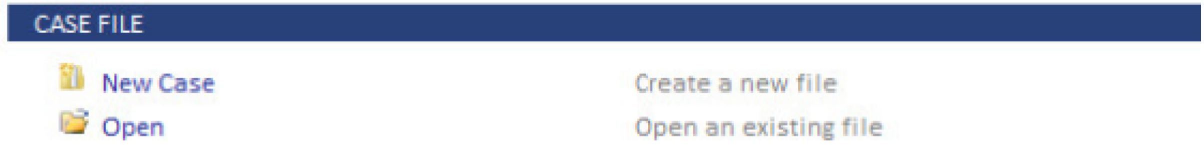
When a computer is forensically analysed by what is referred to as "dead" forensics the analyst is examining the contents of the storage devices once the computer has been turned off. Within this lab we will use, as our example, the Windows XP machine that was infected as part of an early lab on Host Analysis. In this case the computer has been "seized" and a forensic image has been taken of the internal hard drive. It is this forensic image that will be examined by the forensic software.

Log onto the EnCase virtual machine associated with your group number.
Username: napier, Password: psnapier

Start the EnCase application and click yes when/if you are asked about permissions.

Create a new case based on the Windows XP forensic image that has already been taken.

In the main EnCase browser window select "New Case".

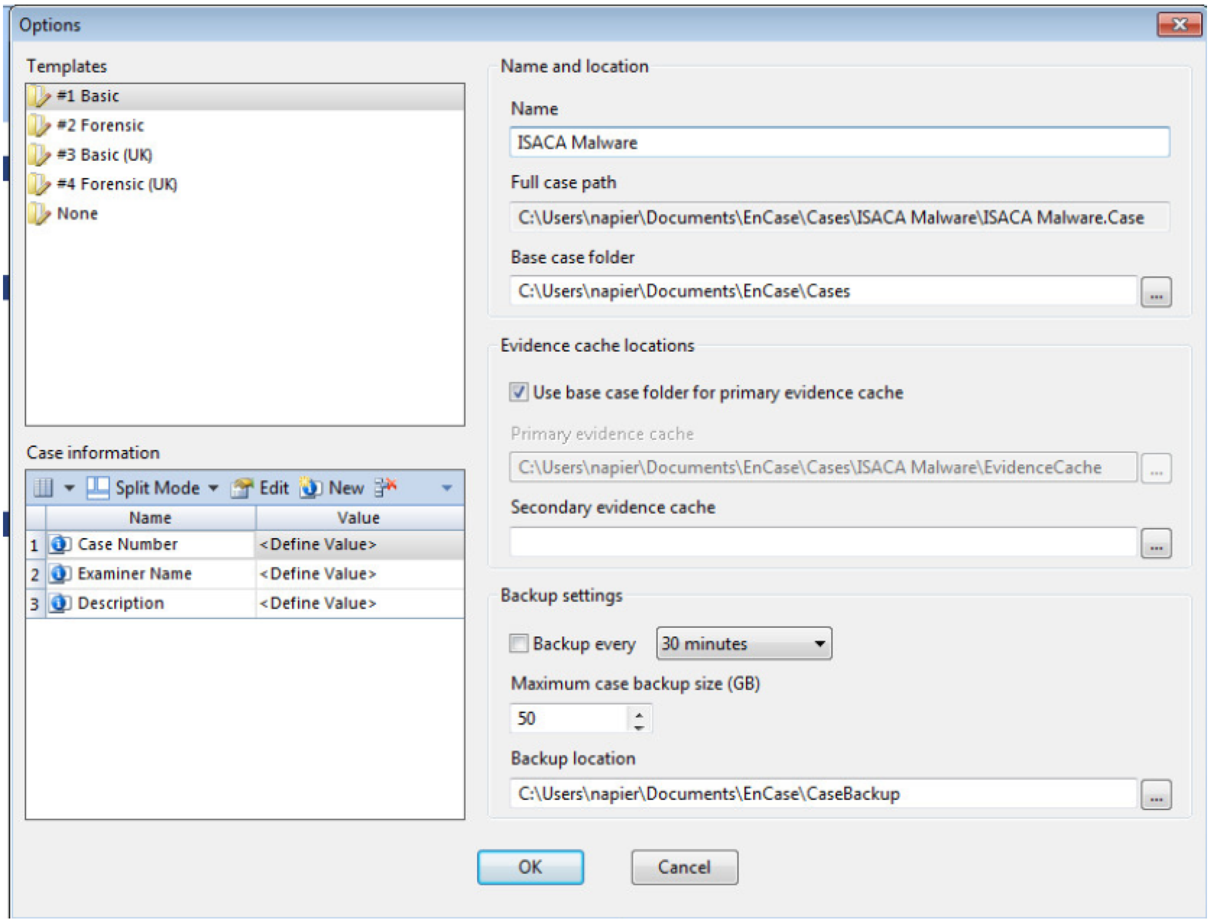


CASE FILE

New Case	Create a new file
Open	Open an existing file

At this point you will be presented with the "New Case" dialog. Select a name for your new case (I have chosen ISACA Malware). The rest of the options can be left with their defaults. We will not be looking at these here. Once completed your "New Case" dialog should have the values shown overleaf:

When you click OK you will be asked if you wish to disable the backups. Select Yes.



Options

Templates

- #1 Basic
- #2 Forensic
- #3 Basic (UK)
- #4 Forensic (UK)
- None

Case information

	Name	Value
1	Case Number	<Define Value>
2	Examiner Name	<Define Value>
3	Description	<Define Value>

Name and location

Name: ISACA Malware

Full case path: C:\Users\napier\Documents\EnCase\Cases\ISACA Malware\ISACA Malware.Case

Base case folder: C:\Users\napier\Documents\EnCase\Cases

Evidence cache locations

☑ Use base case folder for primary evidence cache

Primary evidence cache: C:\Users\napier\Documents\EnCase\Cases\ISACA Malware\EvidenceCache

Secondary evidence cache:

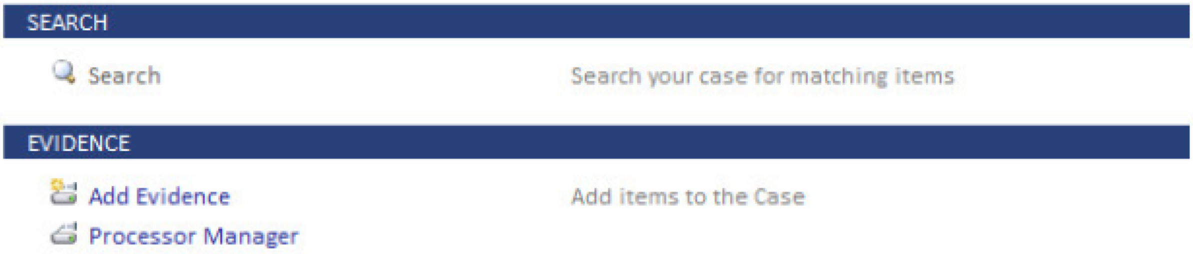
Backup settings

□ Backup every 30 minutes

Maximum case backup size (GB): 50

Backup location: C:\Users\napier\Documents\EnCase\CaseBackup

Add the forensic image.



SEARCH

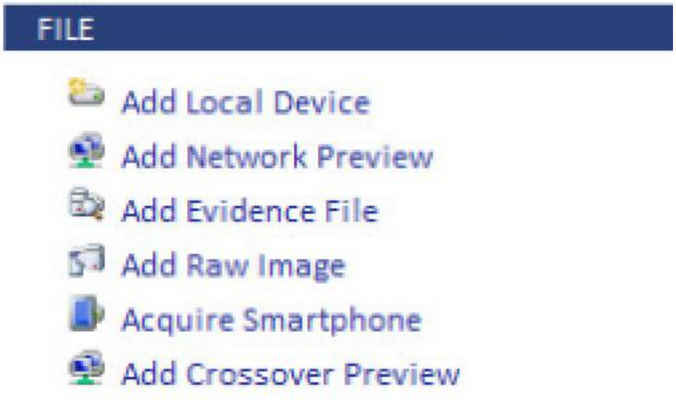
Search — Search your case for matching items

EVIDENCE

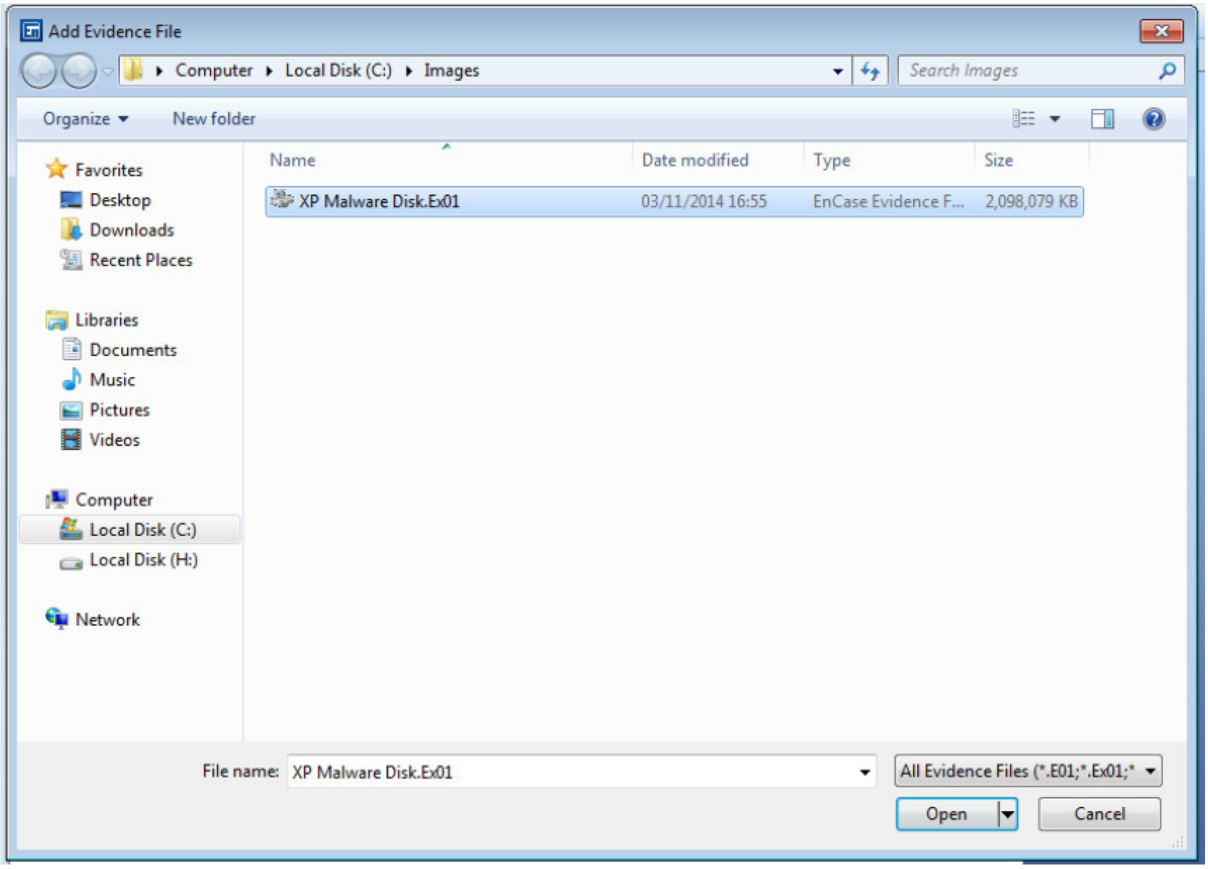
Add Evidence — Add items to the Case

Processor Manager

Next select “Add Evidence File”.



Select the file XP Malware Disk.Ex01 which is located within the folder C:\Images

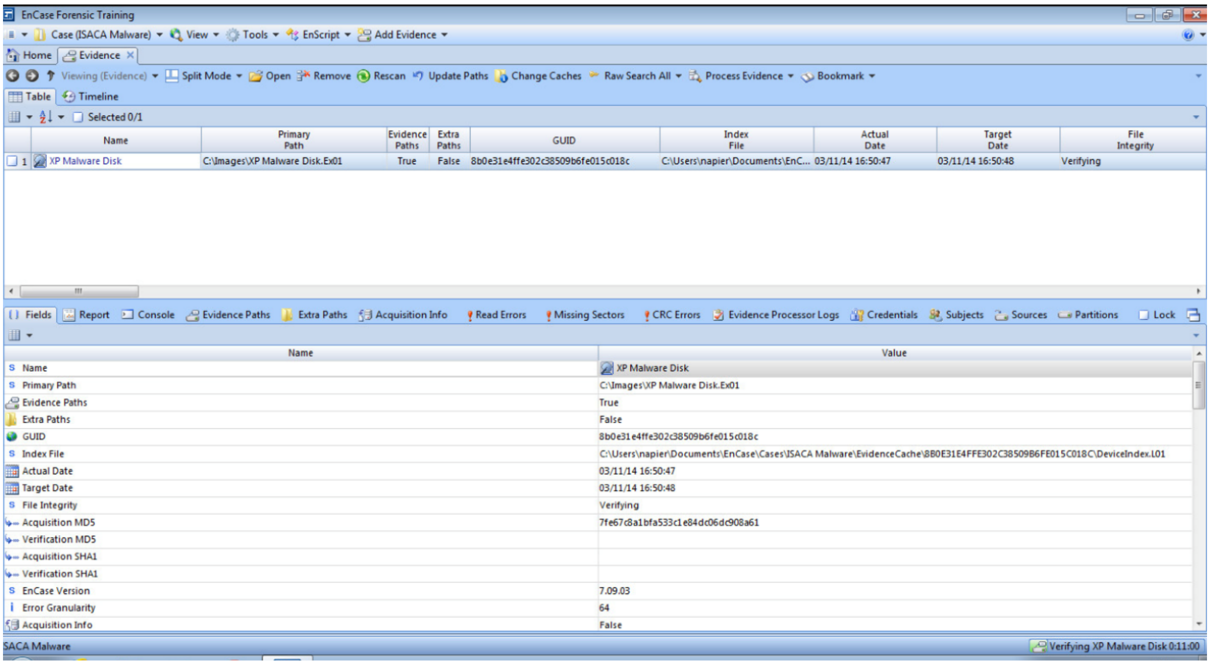


Name	Date modified	Type	Size
XP Malware Disk.Ex01	03/11/2014 16:55	EnCase Evidence F...	2,098,079 KB

File name: XP Malware Disk.Ex01

All Evidence Files (*.E01;*.Ex01;*

Once you select Open you will be presented with the evidence window.


EnCase Forensic Training
Case (ISACA Malware) View Tools EnScript Add Evidence
Home Evidence
Viewing (Evidence) Split Mode Open Remove Rescan Update Paths Change Caches Raw Search All Process Evidence Bookmark
Table Timeline
Selected 0/1
Fields Report Console Evidence Paths Extra Paths Acquisition Info Read Errors Missing Sectors CRC Errors Evidence Processor Logs Credentials Subjects Sources Partitions Lock

	Name	Primary Path	Evidence Paths	Extra Paths	GUID	Index File	Actual Date	Target Date	File Integrity
1	XP Malware Disk	C:\Images\XP Malware Disk.Ex01	True	False	8b0e31e4ffe302c38509b6fe015c018c	C:\Users\napier\Documents\EnC...	03/11/14 16:50:47	03/11/14 16:50:48	Verifying

Name	Value
Name	XP Malware Disk
Primary Path	C:\Images\XP Malware Disk.Ex01
Evidence Paths	True
Extra Paths	False
GUID	8b0e31e4ffe302c38509b6fe015c018c
Index File	C:\Users\napier\Documents\EnCase\Cases\ISACA Malware\EvidenceCache\8B0E31E4FFE302C38509B6FE015C018C\DeviceIndex.L01
Actual Date	03/11/14 16:50:47
Target Date	03/11/14 16:50:48
File Integrity	Verifying
Acquisition MD5	7fe67c8a1bfa533c1e84dc06dc908a61
Verification MD5	
Acquisition SHA1	
Verification SHA1	
EnCase Version	7.09.03
Error Granularity	64
Acquisition Info	False

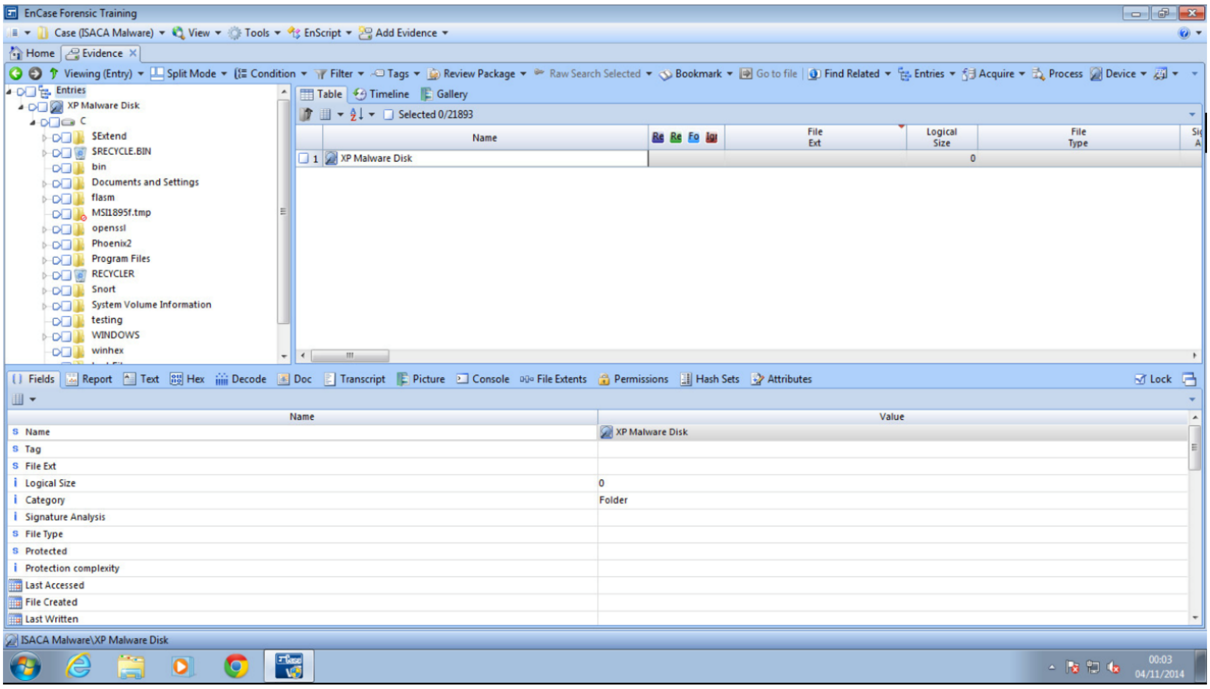
SACA Malware

Verifying XP Malware Disk 0:11:00

The evidence we have loaded is listed at the top of the window. The information about the evidence item is shown in the lower half of the window.

Next click on the evidence item we just loaded so that it scanned by the software.

During the opening process EnCase scans the hard drive and performs some pre-processing. This includes looking for easily recoverable files that have previously been deleted. This windows looks like:


EnCase Forensic Training
Case (ISACA Malware) View Tools EnScript Add Evidence
Home Evidence
Viewing (Entry) Split Mode Condition Filter Tags Review Package Raw Search Selected Bookmark Go to file Find Related Entries Acquire Process Device
Table Timeline Gallery
Selected 0/21893
Fields Report Text Hex Decode Doc Transcript Picture Console File Extents Permissions Hash Sets Attributes Lock

Entries
XP Malware Disk
C
$Extend
$RECYCLE.BIN
bin
Documents and Settings
flasm
MSI1895f.tmp
openssl
Phoenix2
Program Files
RECYCLER
Snort
System Volume Information
testing
WINDOWS
winhex

	Name	File Ext	Logical Size	File Type
1	XP Malware Disk		0	

Name	Value
Name	XP Malware Disk
Tag	
File Ext	
Logical Size	0
Category	Folder
Signature Analysis	
File Type	
Protected	
Protection complexity	
Last Accessed	
File Created	
Last Written	

ISACA Malware\XP Malware Disk

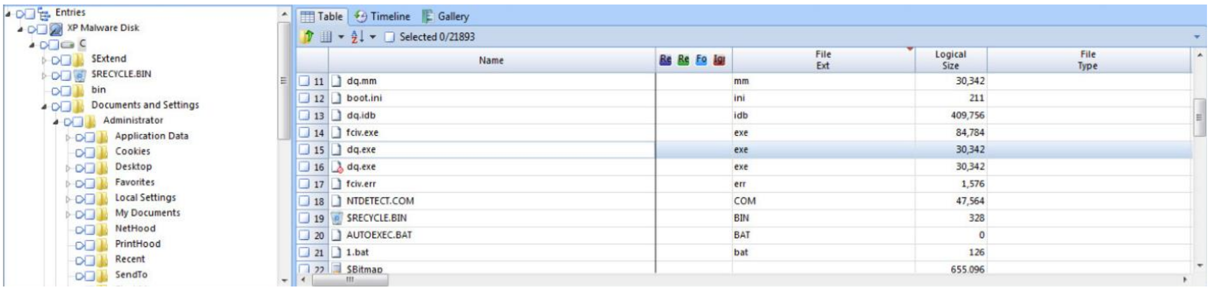
00:03
04/11/2014

The contents of the evidence item can be seen on the top left (tree) pane. Whatever is highlighted in this window is displayed in the top right (list) pane. Finally whatever is highlighted in the list pane is displayed within the lower (view) pane.

Get used to the interface by answering the following questions:
How many files are present within the Administrators account My Documents folder?

How many folders are present within the Administrators account My Documents folder?

Next we will look at the dq.exe executable which was the malware file we looked at in the earlier lab. This is located within the C:\ folder.



- Entries
  - XP Malware Disk
    - C
      - $Extend
      - $RECYCLE.BIN
      - bin
      - Documents and Settings
        - Administrator
          - Application Data
          - Cookies
          - Desktop
          - Favorites
          - Local Settings
          - My Documents
          - NetHood
          - PrintHood
          - Recent
          - SendTo

	Name	Re Re Fo Igi	File Ext	Logical Size	File Type
11	dq.mm		mm	30,342	
12	boot.ini		ini	211	
13	dq.idb		idb	409,756	
14	fciv.exe		exe	84,784	
15	dq.exe		exe	30,342	
16	dq.exe		exe	30,342	
17	fciv.err		err	1,576	
18	NTDETECT.COM		COM	47,564	
19	$RECYCLE.BIN		BIN	328	
20	AUTOEXEC.BAT		BAT	0	
21	1.bat		bat	126	
22	$Bitmap			655,096	

Why do you think there are two different listings for the dq.exe file?

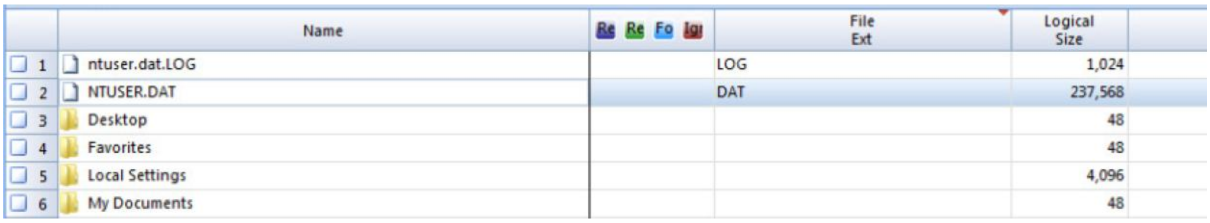
Next we will take a look at the file that was located within Recycle Bin.

Can you find the file within the recycle bin?

Why do you think there is both a Recycler folder and a $RECYCLE.BIN folder?

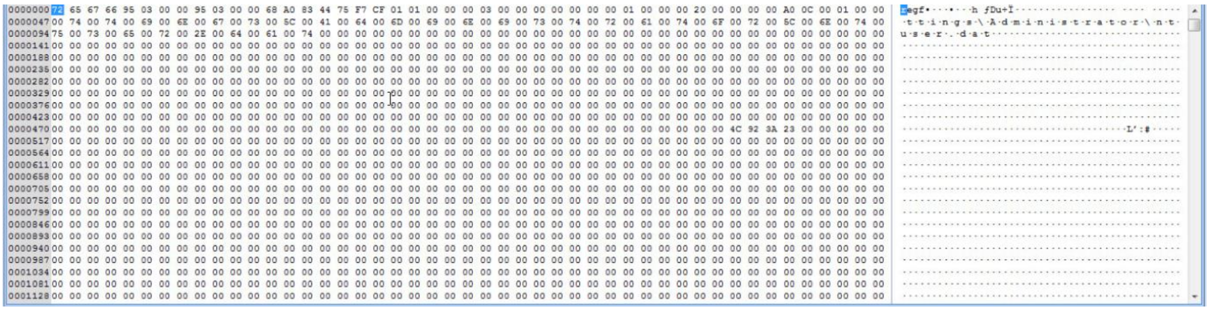
Next we will take a look at the information we previously found within the registry. We know that original location was: HKCU\Software\Microsoft\Windows\CurrentVersion\Run

We know (from the lecture) that the Software Key which is located within the Current User hive is actually stored within the file NTUSER.DAT located within the folder C:\Document and Settings\Administrator.



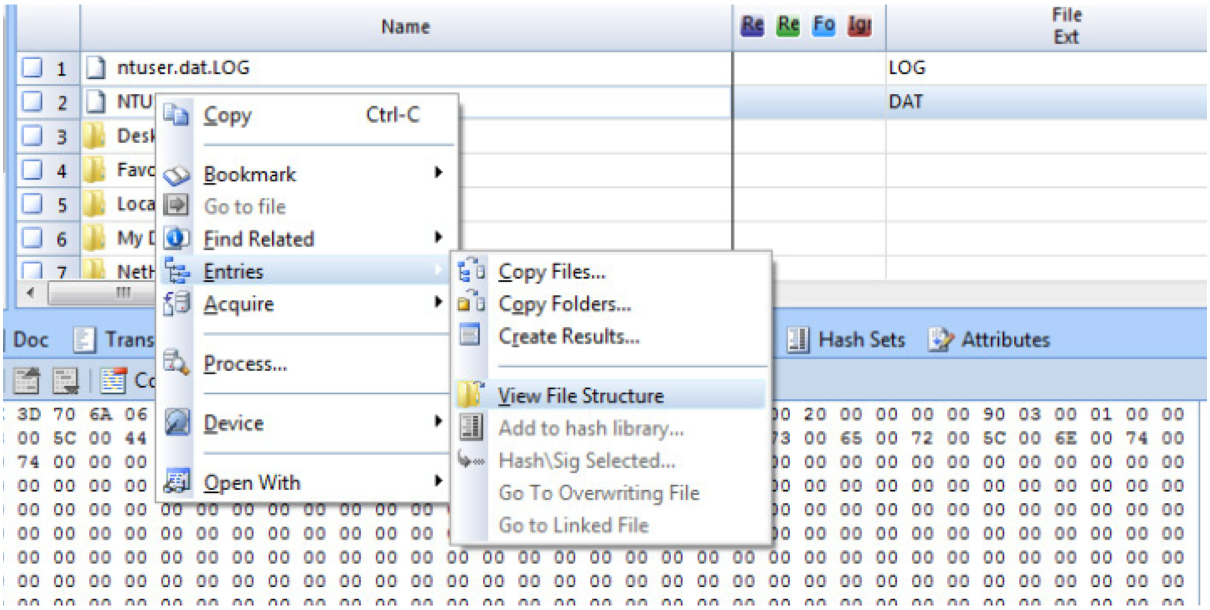
	Name	Re Re Fo Igi	File Ext	Logical Size
1	ntuser.dat.LOG		LOG	1,024
2	NTUSER.DAT		DAT	237,568
3	Desktop			48
4	Favorites			48
5	Local Settings			4,096
6	My Documents			48

Select the hex tab in the lower pane. This will show us the hexadecimal representation of the contents of the file. The beginning of these contents is shown here:

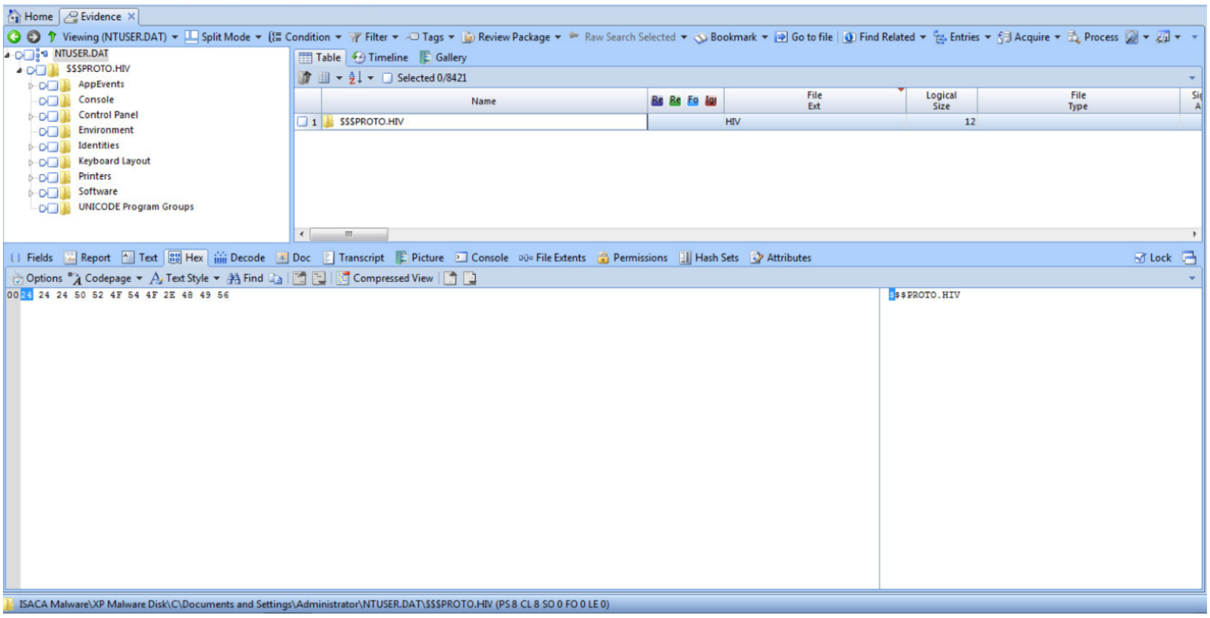


```
0000000 72 65 67 66 95 03 00 00 95 03 00 00 68 A0 83 44 75 F7 CF 01 01 00 00 00 03 00 00 00 00 00 00 00 01 00 00 00 20 00 00 00 00 A0 0C 00 01 00 00  regf•···•···h ƒDu÷Ï················· ···· ·····
0000047 00 74 00 74 00 69 00 6E 00 67 00 73 00 5C 00 41 00 64 00 6D 00 69 00 6E 00 69 00 73 00 74 00 72 00 61 00 74 00 6F 00 72 00 5C 00 6E 00 74 00  ·t·t·i·n·g·s·\·A·d·m·i·n·i·s·t·r·a·t·o·r·\·n·t·
0000094 75 00 73 00 65 00 72 00 2E 00 64 00 61 00 74 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00  u·s·e·r·.·d·a·t·······························
0000141 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00  ···············································
0000188 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00  ···············································
0000235 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00  ···············································
0000282 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00  ···············································
0000329 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00  ···············································
0000376 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00  ···············································
0000423 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00  ···············································
0000470 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 4C 92 3A 23 00 00 00 00 00  ······································L':#·····
0000517 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00  ···············································
0000564 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00  ···············································
0000611 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00  ···············································
0000658 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00  ···············································
0000705 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00  ···············································
0000752 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00  ···············································
0000799 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00  ···············································
0000846 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00  ···············································
0000893 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00  ···············································
0000940 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00  ···············································
0000987 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00  ···············································
0001034 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00  ···············································
0001081 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00  ···············································
0001128 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00  ···············································
```

We can see from the above (or from the interface) that the first 4 characters are “regf”. This is the file signature of the registry file type. Internally it has a complicated structure but we can get EnCase to decode it. This is done by right clicking on the software entry and selecting Entries->View File Structure.



A progress bar will appear at the lower right hand side of the screen. Once that is complete the software entry within the tree view will turn blue. This indicates that it is now a link to additional information and can be selected. If you select this now it will show you contents of the file.



- NTUSER.DAT
  - $$$PROTO.HIV
    - AppEvents
    - Console
    - Control Panel
    - Environment
    - Identities
    - Keyboard Layout
    - Printers
    - Software
    - UNICODE Program Groups

	Name		File Ext	Logical Size	File Type
1	$$$PROTO.HIV		HIV	12	

```
0024 24 24 50 52 4F 54 4F 2E 48 49 56          $$$PROTO.HIV
```

ISACA Malware\XP Malware Disk\C\Documents and Settings\Administrator\NTUSER.DAT\$$$PROTO.HIV (PS 8 CL 8 SO 0 FO 0 LE 0)

Verify that the malware discovered in the earlier lab is present in this version of the registry: