Lab - Digital Forensics Using Autopsy Part II

Overview

In this lab, you will begin to analyze the forensic image your imported into Autopsy in a previous lab.

Hardware requirements for these labs:

- Virtual install of Kali Linux

Lab Requirements

- You have created a forensic image and built a new case file using Autopsy.

You are now ready to proceed with the analysis of the forensic image.

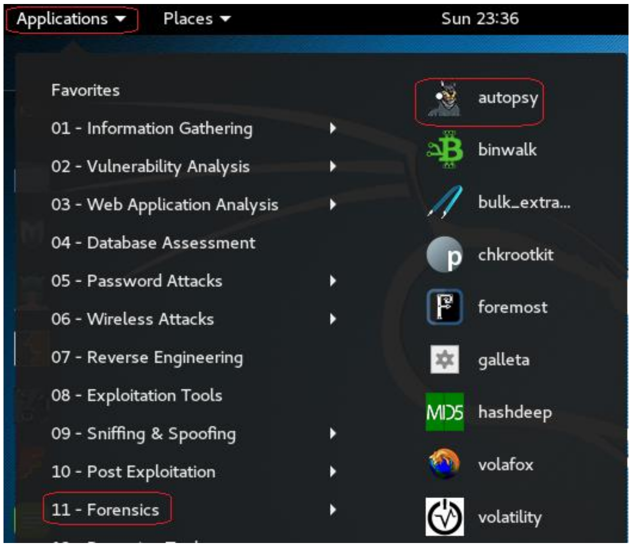
Objectives:

- Create a case in Autopsy. (Lab - Digital Forensics Using Autopsy Part I)
- Locate deleted/hidden images files
- Perform a deleted files search
- Create a case report with any evidence you find.

The lab takes off where Part I ended. To begin….

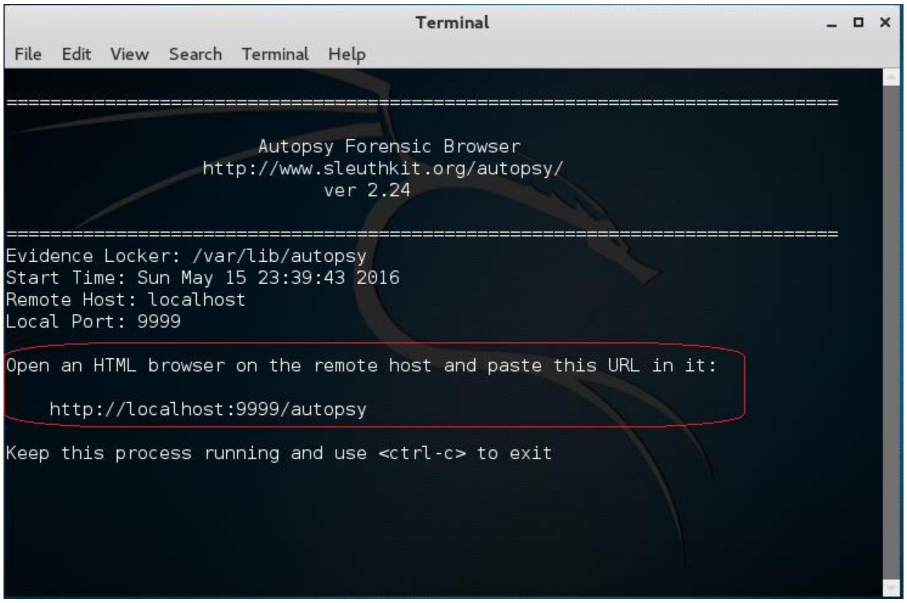
Open Autopsy

- In Kali, go to Applications -> Forensic and select autopsy from the list.



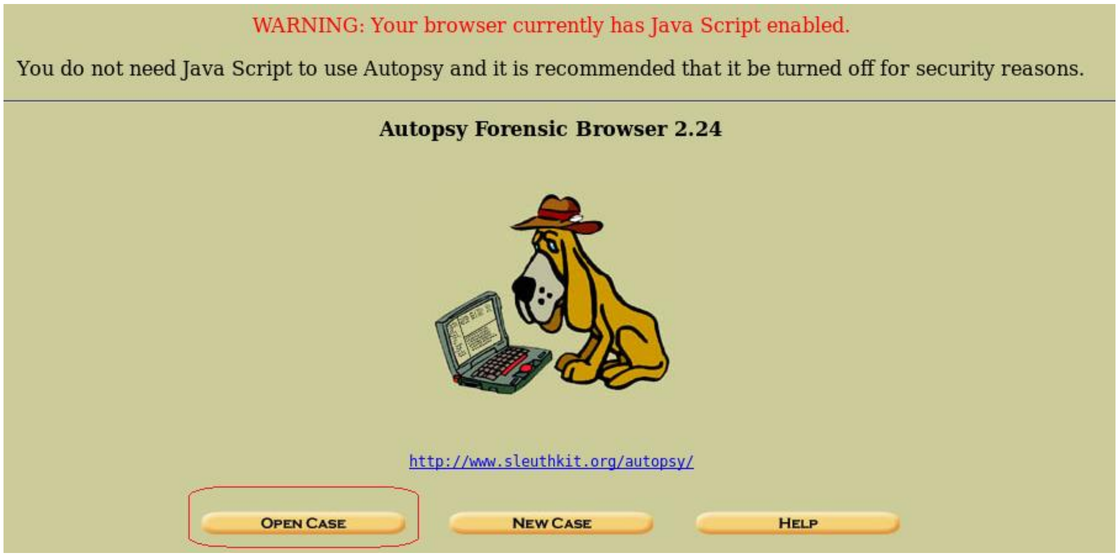
When you do so, you will open a screen that looks like that below. Notice that it asks you to open up a browser at http://localhost:9999/autopsy. (Hint: Hold down the Ctrl key and click on the URL in the terminal.)

Remember not to close the terminal session!



```
============================================================================

                       Autopsy Forensic Browser
                  http://www.sleuthkit.org/autopsy/
                             ver 2.24

============================================================================
Evidence Locker: /var/lib/autopsy
Start Time: Sun May 15 23:39:43 2016
Remote Host: localhost
Local Port: 9999

Open an HTML browser on the remote host and paste this URL in it:

    http://localhost:9999/autopsy

Keep this process running and use <ctrl-c> to exit
```

Open Autopsy. Click the Open Case button.

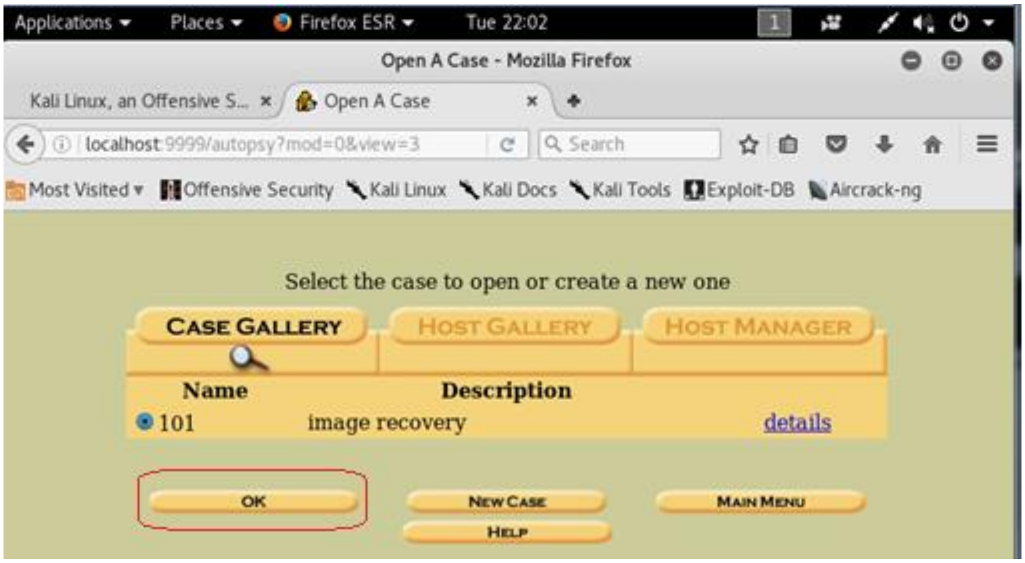


WARNING: Your browser currently has Java Script enabled.

You do not need Java Script to use Autopsy and it is recommended that it be turned off for security reasons.

Autopsy Forensic Browser 2.24

http://www.sleuthkit.org/autopsy/

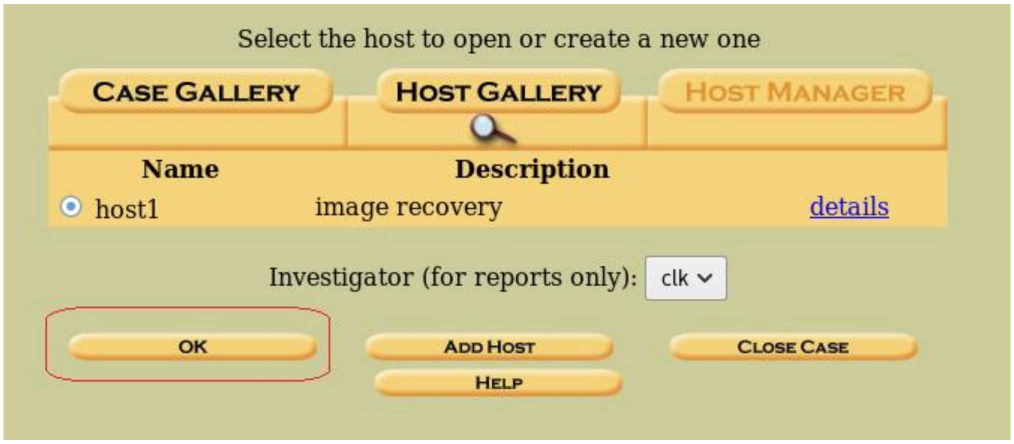


Select the case to open or create a new one

Name	Description	
● 101	image recovery	details

Click the OK button.

In the next window, you presented with the host ID. Click OK.



Select the host to open or create a new one

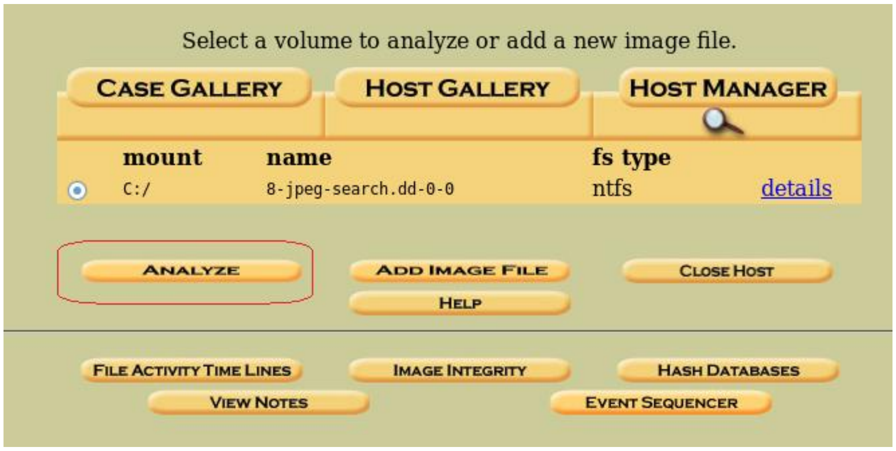
	Name	Description	
●	host1	image recovery	details

Investigator (for reports only): clk

In the next window, you're presented with the image and volume information. Click on Analyze.

If you cannot see the file needed from within the case, run the following command from a new terminal window within Kali:

```
ln -s /usr/bin/icat /usr/bin/icat-sleuthkit
```

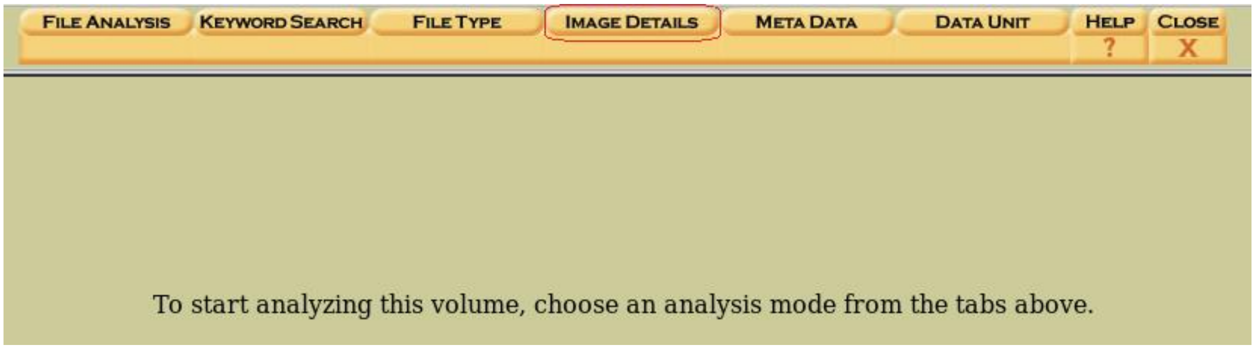


Select a volume to analyze or add a new image file.

	mount	name	fs type	
●	C:/	8-jpeg-search.dd-0-0	ntfs	details

Viewing Image Details with Autopsy

- Select the Image Details Button



To start analyzing this volume, choose an analysis mode from the tabs above.

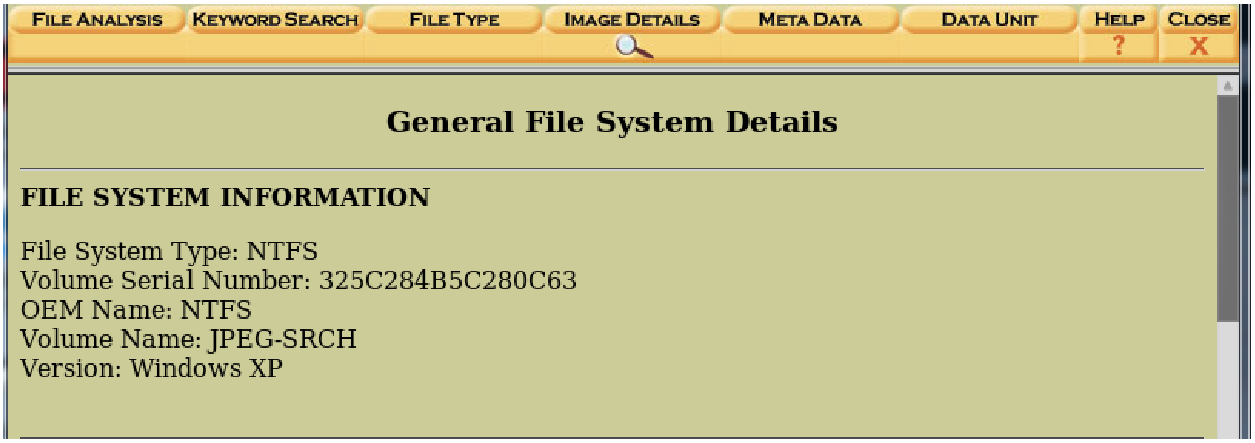
Viewing General File System Details with Autopsy

Your Image File System Type is NTFS

If you made a backup of the original image, your Volume Serial Number should remain the same.

This is important in a court of law, to demonstrate that the volume serial number of the image you analyzed is the same as the original copy.

The Operating System Version of the Image is Windows XP.



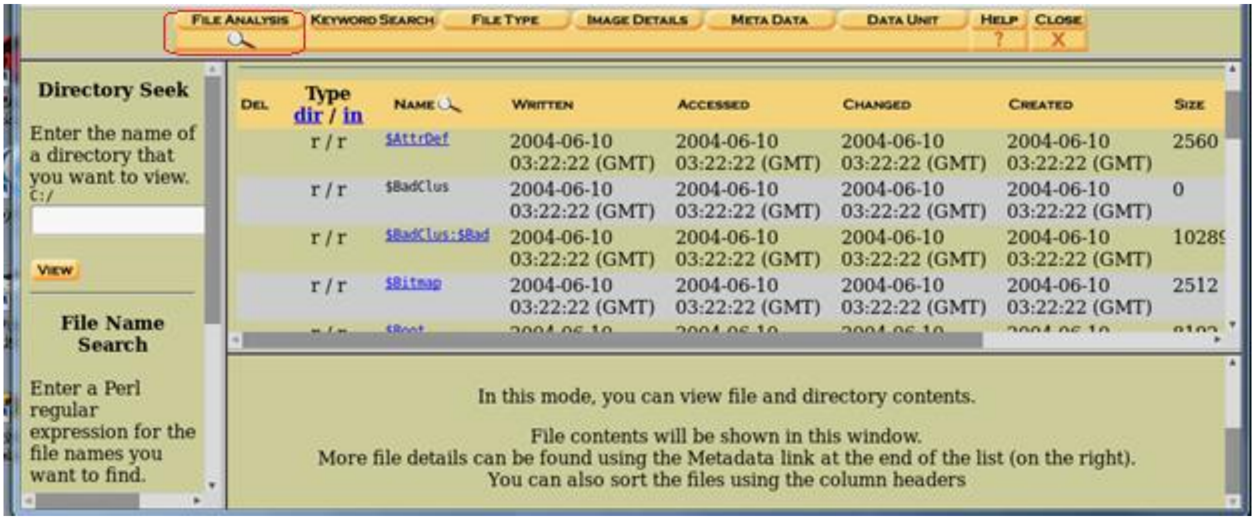
General File System Details

FILE SYSTEM INFORMATION

File System Type: NTFS
Volume Serial Number: 325C284B5C280C63
OEM Name: NTFS
Volume Name: JPEG-SRCH
Version: Windows XP

Viewing File Analysis Details with Autopsy

- Click the File Analysis Button



Directory Seek

Enter the name of a directory that you want to view.
C:/

File Name Search

Enter a Perl regular expression for the file names you want to find.

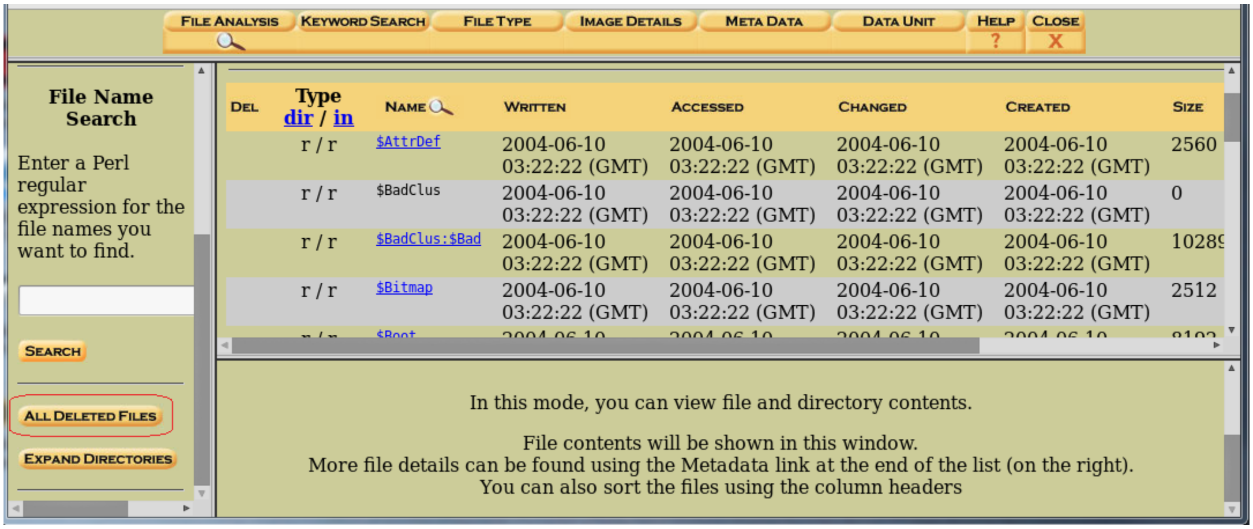
Del	Type dir / in	Name	Written	Accessed	Changed	Created	Size
	r / r	$AttrDef	2004-06-10 03:22:22 (GMT)	2004-06-10 03:22:22 (GMT)	2004-06-10 03:22:22 (GMT)	2004-06-10 03:22:22 (GMT)	2560
	r / r	$BadClus	2004-06-10 03:22:22 (GMT)	2004-06-10 03:22:22 (GMT)	2004-06-10 03:22:22 (GMT)	2004-06-10 03:22:22 (GMT)	0
	r / r	$BadClus:$Bad	2004-06-10 03:22:22 (GMT)	2004-06-10 03:22:22 (GMT)	2004-06-10 03:22:22 (GMT)	2004-06-10 03:22:22 (GMT)	1028
	r / r	$Bitmap	2004-06-10 03:22:22 (GMT)	2004-06-10 03:22:22 (GMT)	2004-06-10 03:22:22 (GMT)	2004-06-10 03:22:22 (GMT)	2512

In this mode, you can view file and directory contents.

File contents will be shown in this window.
More file details can be found using the Metadata link at the end of the list (on the right).
You can also sort the files using the column headers

Viewing deleted files with Autopsy

- Click the All Deleted Files Button at the bottom of the left frame.



File Name Search

Enter a Perl regular expression for the file names you want to find.

Del	Type dir / in	Name	Written	Accessed	Changed	Created	Size
	r / r	$AttrDef	2004-06-10 03:22:22 (GMT)	2004-06-10 03:22:22 (GMT)	2004-06-10 03:22:22 (GMT)	2004-06-10 03:22:22 (GMT)	2560
	r / r	$BadClus	2004-06-10 03:22:22 (GMT)	2004-06-10 03:22:22 (GMT)	2004-06-10 03:22:22 (GMT)	2004-06-10 03:22:22 (GMT)	0
	r / r	$BadClus:$Bad	2004-06-10 03:22:22 (GMT)	2004-06-10 03:22:22 (GMT)	2004-06-10 03:22:22 (GMT)	2004-06-10 03:22:22 (GMT)	1028
	r / r	$Bitmap	2004-06-10 03:22:22 (GMT)	2004-06-10 03:22:22 (GMT)	2004-06-10 03:22:22 (GMT)	2004-06-10 03:22:22 (GMT)	2512

In this mode, you can view file and directory contents.

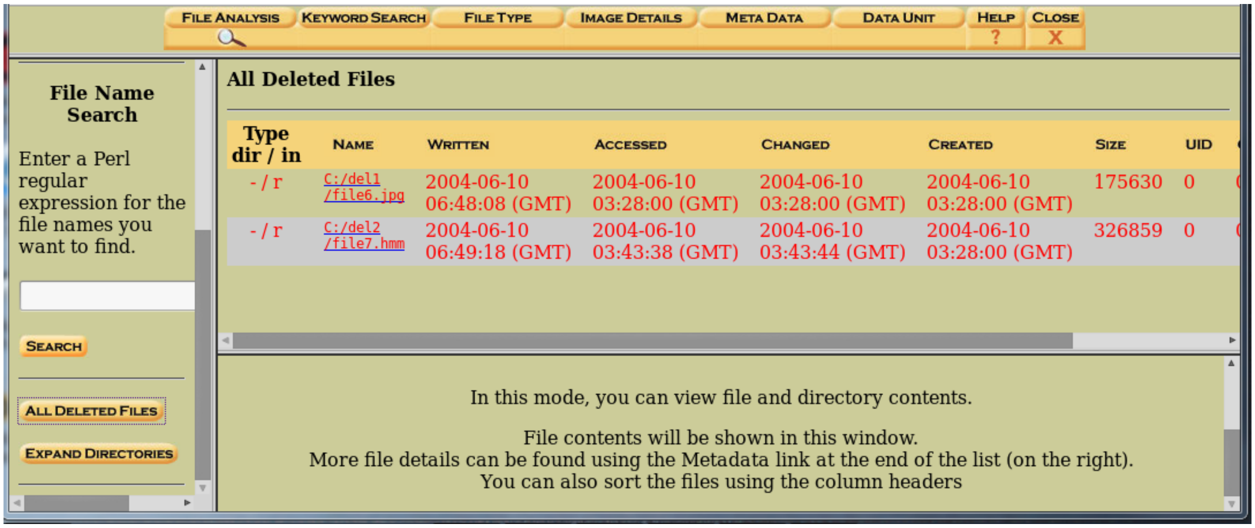
File contents will be shown in this window.
More file details can be found using the Metadata link at the end of the list (on the right).
You can also sort the files using the column headers

Viewing deleted files with Autopsy

Notice Autopsy found two files in our image that has been deleted.

The file named file6.jpg is obviously a JPEG, but what is file7.hmm?

- Click on the file named file6.jpg



File Name Search

Enter a Perl regular expression for the file names you want to find.

All Deleted Files

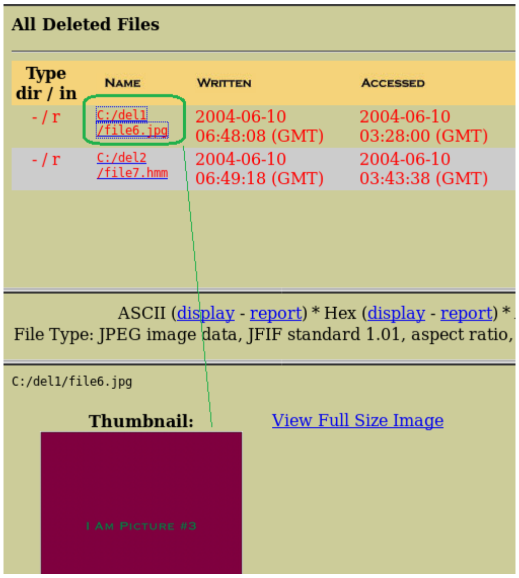
Type dir / in	Name	Written	Accessed	Changed	Created	Size	UID
- / r	C:/del1 /file6.jpg	2004-06-10 06:48:08 (GMT)	2004-06-10 03:28:00 (GMT)	2004-06-10 03:28:00 (GMT)	2004-06-10 03:28:00 (GMT)	175630	0
- / r	C:/del2 /file7.hmm	2004-06-10 06:49:18 (GMT)	2004-06-10 03:43:38 (GMT)	2004-06-10 03:43:44 (GMT)	2004-06-10 03:28:00 (GMT)	326859	0

In this mode, you can view file and directory contents.

File contents will be shown in this window.
More file details can be found using the Metadata link at the end of the list (on the right).
You can also sort the files using the column headers

Viewing deleted files with Autopsy

Once you click on file6.jpg, the bottom frame displays a thumbnail of the JPEG.



All Deleted Files

Type dir / in	Name	Written	Accessed
- / r	C:/del1 /file6.jpg	2004-06-10 06:48:08 (GMT)	2004-06-10 03:28:00 (GMT)
- / r	C:/del2 /file7.hmm	2004-06-10 06:49:18 (GMT)	2004-06-10 03:43:38 (GMT)

ASCII (display - report) * Hex (display - report) *
File Type: JPEG image data, JFIF standard 1.01, aspect ratio,

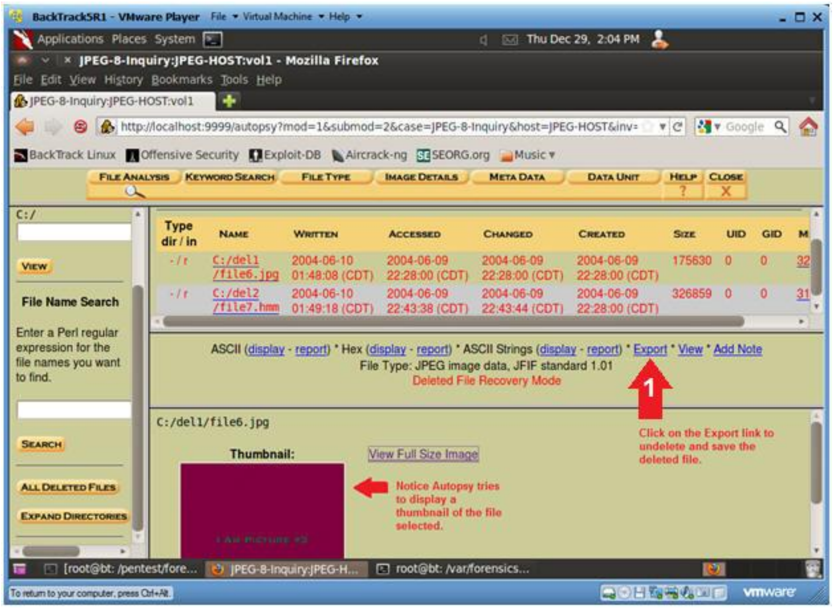
C:/del1/file6.jpg

Thumbnail: View Full Size Image

If you cannot see the file needed from within the case, run the following command from a new terminal in Kali: (Copy and paste)

```
ln -s /usr/bin/icat /usr/bin/icat-sleuthkit
```

- Click on the Export link to save a copy of the deleted file named file6.jpg.



BackTrack5R1 - VMware Player
JPEG-8-Inquiry:JPEG-HOST:vol1 - Mozilla Firefox
http://localhost:9999/autopsy?mod=1&submod=2&case=JPEG-8-Inquiry&host=JPEG-HOST&inv=
FILE ANALYSIS
KEYWORD SEARCH
FILE TYPE
IMAGE DETAILS
META DATA
DATA UNIT
HELP
CLOSE
VIEW
SEARCH
ALL DELETED FILES
EXPAND DIRECTORIES

File Name Search

Enter a Perl regular expression for the file names you want to find.

Type dir / in	NAME	WRITTEN	ACCESSED	CHANGED	CREATED	SIZE	UID	GID	M
-/r	C:/del1 /file6.jpg	2004-06-10 01:48:08 (CDT)	2004-06-09 22:28:00 (CDT)	2004-06-09 22:28:00 (CDT)	2004-06-09 22:28:00 (CDT)	175630	0	0	32
-/r	C:/del2 /file7.hmm	2004-06-10 01:49:18 (CDT)	2004-06-09 22:43:38 (CDT)	2004-06-09 22:43:44 (CDT)	2004-06-09 22:28:00 (CDT)	326859	0	0	31

ASCII (display - report) * Hex (display - report) * ASCII Strings (display - report) * Export * View * Add Note
File Type: JPEG image data, JFIF standard 1.01
Deleted File Recovery Mode

C:/del1/file6.jpg

Thumbnail: View Full Size Image

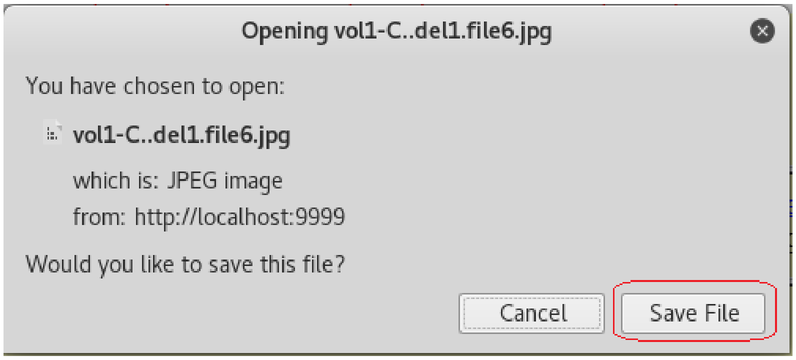
1

Click on the Export link to undelete and save the deleted file.

Notice Autopsy tries to display a thumbnail of the file selected.

Saving the deleted files with Autopsy

- Click the Save File radio button



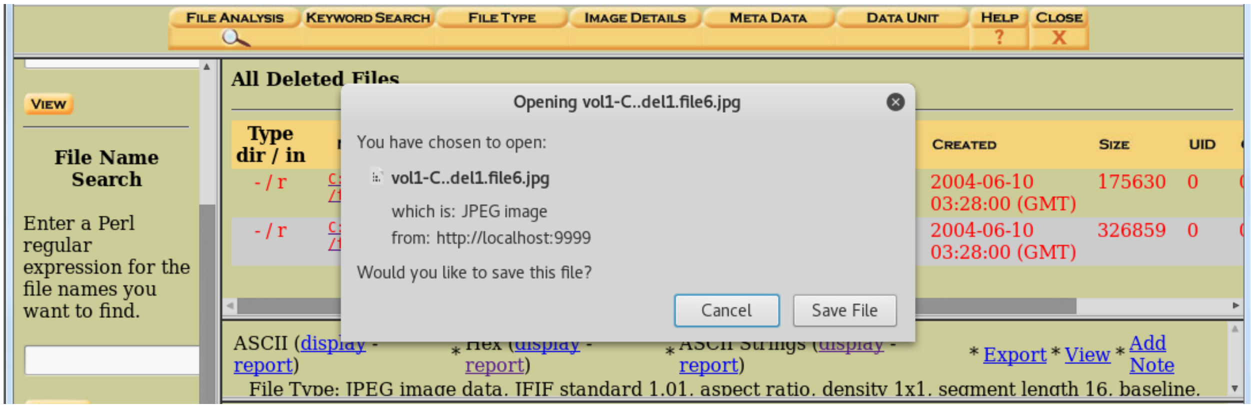
Opening vol1-C..del1.file6.jpg

You have chosen to open:

vol1-C..del1.file6.jpg

which is: JPEG image
from: http://localhost:9999

Would you like to save this file?



All Deleted Files

File Name Search

Enter a Perl regular expression for the file names you want to find.

Type dir / in		Created	Size	UID
- / r	C: /f	2004-06-10 03:28:00 (GMT)	175630	0
- / r	C: /f	2004-06-10 03:28:00 (GMT)	326859	0

Opening vol1-C..del1.file6.jpg

You have chosen to open:

vol1-C..del1.file6.jpg

which is: JPEG image

from: http://localhost:9999

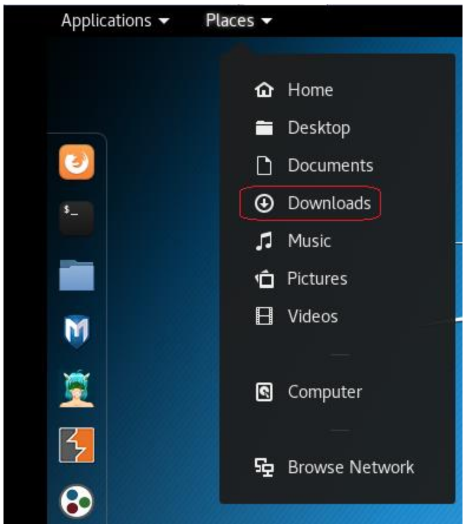
Would you like to save this file?

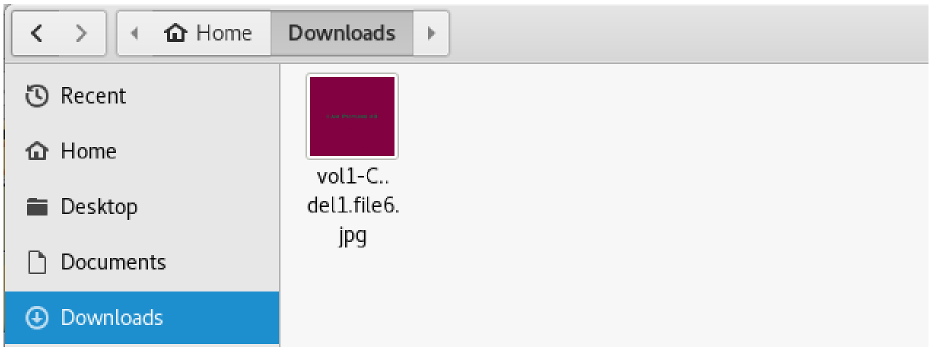
ASCII (display - report) * Hex (display - report) * ASCII Strings (display - report) * Export * View * Add Note

File Type: JPEG image data, JFIF standard 1.01, aspect ratio, density 1x1, segment length 16, baseline.

Saving the deleted files with Autopsy

- Single Click on Save File
- Minimize your browser (do not close!
- From the desktop, click on Places and select Downloads.

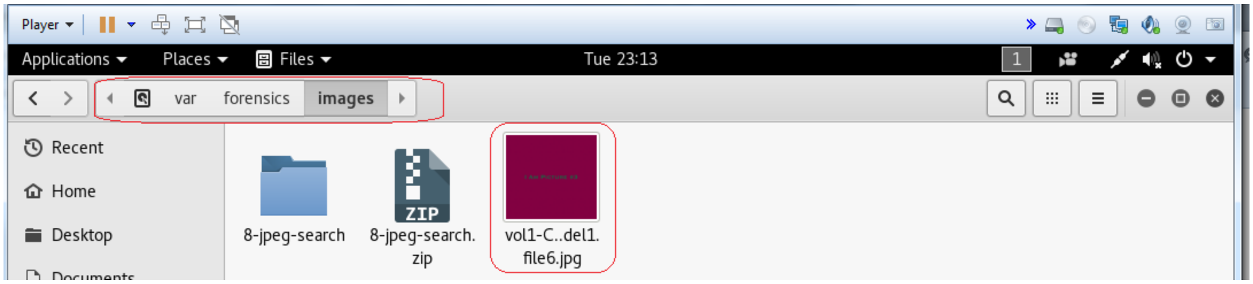




Move image to Forensics folder

- Right click on the image and select Move to…
- From the bottom of the folder locations, select + Other Locations
- Click on Computer, scroll to bottom of the folder list and click on Var
- Click on the forensics Folder
- Click on Images

In the top right corner, click on Select. This brings you back to the original location, note the file has been moved. You can verify the new location of the file by backtracking your steps starting with +Other Locations.

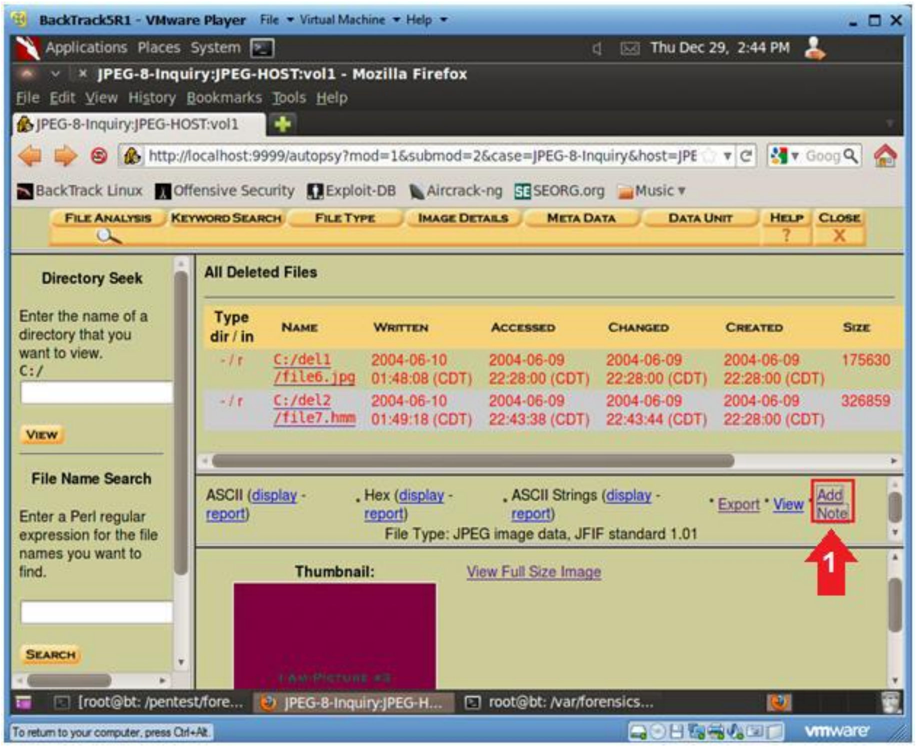


Add Note to file6.jpg

Warning! If you cannot add a note and kept receiving the following error (or any error)....run the following command from the terminal.

```
ln -s /usr/bin/ils /usr/bin/ils-sleuthkit
```

- Click on Add Note


BackTrack5R1 - VMware Player File Virtual Machine Help
Applications Places System
Thu Dec 29, 2:44 PM
JPEG-8-Inquiry:JPEG-HOST:vol1 - Mozilla Firefox
File Edit View History Bookmarks Tools Help
JPEG-8-Inquiry:JPEG-HOST:vol1
http://localhost:9999/autopsy?mod=1&submod=2&case=JPEG-8-Inquiry&host=JPE
BackTrack Linux Offensive Security Exploit-DB Aircrack-ng SEORG.org Music
FILE ANALYSIS KEYWORD SEARCH FILE TYPE IMAGE DETAILS META DATA DATA UNIT HELP ? CLOSE X
VIEW
SEARCH
Thumbnail:
View Full Size Image
1
[root@bt: /pentest/fore... JPEG-8-Inquiry:JPEG-H... root@bt: /var/forensics...
To return to your computer, press Ctrl+Alt.
vmware

Directory Seek

Enter the name of a directory that you want to view.
C:/

File Name Search

Enter a Perl regular expression for the file names you want to find.

All Deleted Files

Type dir / in	NAME	WRITTEN	ACCESSED	CHANGED	CREATED	SIZE
-/r	C:/del1 /file6.jpg	2004-06-10 01:48:08 (CDT)	2004-06-09 22:28:00 (CDT)	2004-06-09 22:28:00 (CDT)	2004-06-09 22:28:00 (CDT)	175630
-/r	C:/del2 /file7.hmm	2004-06-10 01:49:18 (CDT)	2004-06-09 22:43:38 (CDT)	2004-06-09 22:43:44 (CDT)	2004-06-09 22:28:00 (CDT)	326859

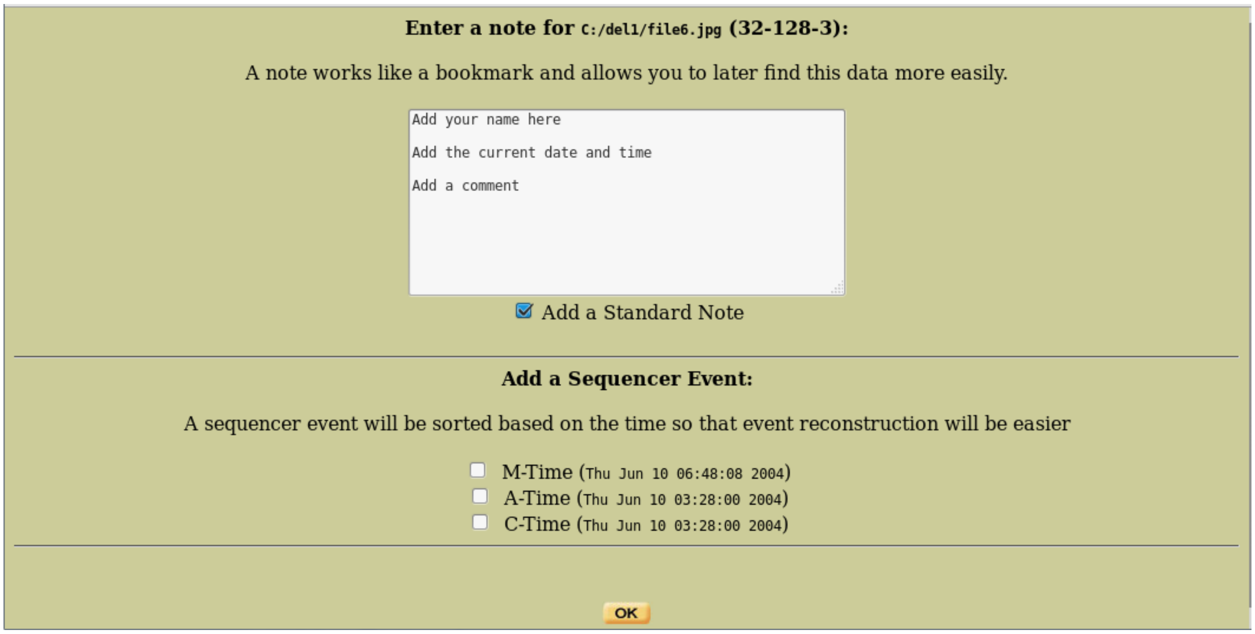
ASCII (display - report) • Hex (display - report) • ASCII Strings (display - report) • Export • View • Add Note

File Type: JPEG image data, JFIF standard 1.01

Add Note to file6.jpg

Add the following information to the Note Text Box

- Your Actual Name
- Current Date and Time
- Add a Comment
- Click the OK button.



Enter a note for `C:/del1/file6.jpg` **(32-128-3):**

A note works like a bookmark and allows you to later find this data more easily.

```
Add your name here

Add the current date and time

Add a comment
```

☑ Add a Standard Note

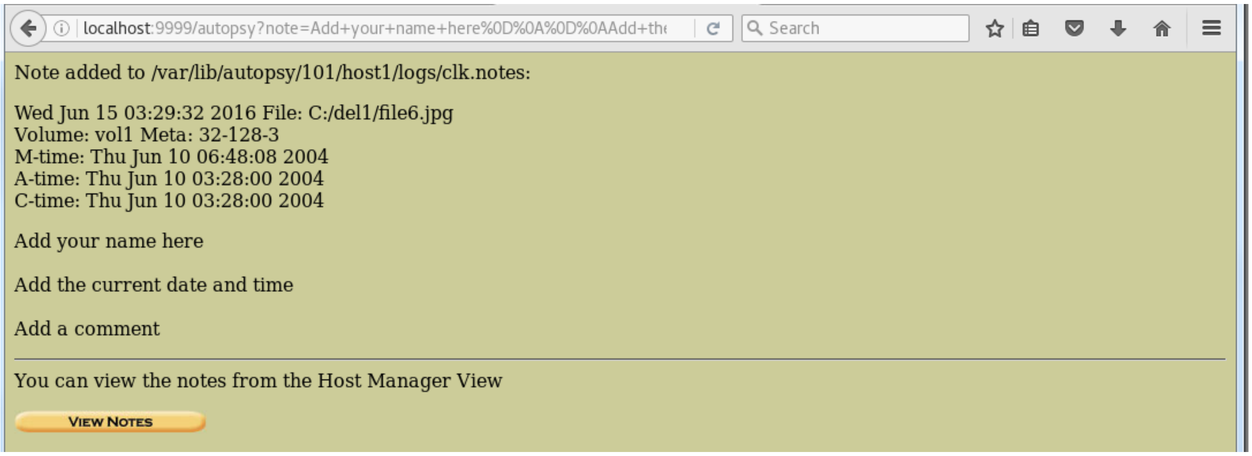
Add a Sequencer Event:

A sequencer event will be sorted based on the time so that event reconstruction will be easier

☐ M-Time (Thu Jun 10 06:48:08 2004)
☐ A-Time (Thu Jun 10 03:28:00 2004)
☐ C-Time (Thu Jun 10 03:28:00 2004)

Verify Notes

- Click the View Notes Button.



localhost:9999/autopsy?note=Add+your+name+here%0D%0A%0D%0AAdd+the
Search

Note added to /var/lib/autopsy/101/host1/logs/clk.notes:

Wed Jun 15 03:29:32 2016 File: C:/del1/file6.jpg
Volume: vol1 Meta: 32-128-3
M-time: Thu Jun 10 06:48:08 2004
A-time: Thu Jun 10 03:28:00 2004
C-time: Thu Jun 10 03:28:00 2004

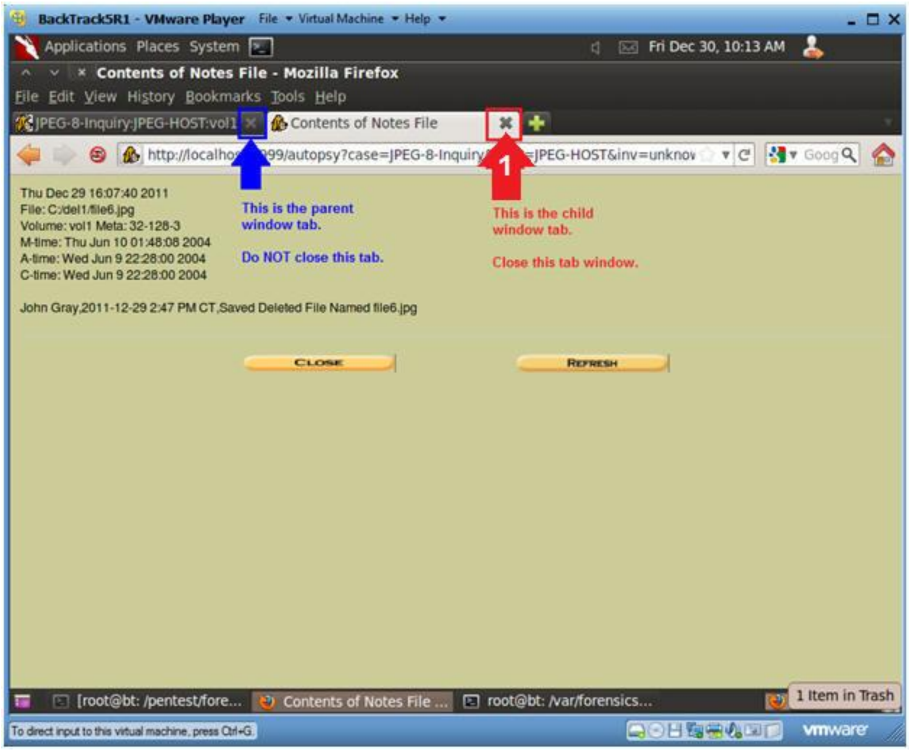
Add your name here

Add the current date and time

Add a comment

You can view the notes from the Host Manager View

- Close the Child Window.
- Click the "X" on the child window. (See Below)


BackTrack5R1 - VMware Player
File
Virtual Machine
Help
Applications
Places
System
Fri Dec 30, 10:13 AM
Contents of Notes File - Mozilla Firefox
File
Edit
View
History
Bookmarks
Tools
Help
JPEG-8-Inquiry:JPEG-HOST:vol1
Contents of Notes File
http://localhost:9999/autopsy?case=JPEG-8-Inquiry&host=JPEG-HOST&inv=unknow
Goog
1
CLOSE
REFRESH
[root@bt: /pentest/fore...
Contents of Notes File ...
root@bt: /var/forensics...
1 Item in Trash
To direct input to this virtual machine, press Ctrl+G.
vmware

Thu Dec 29 16:07:40 2011
File: C:/del1/file6.jpg
Volume: vol1 Meta: 32-128-3
M-time: Thu Jun 10 01:48:08 2004
A-time: Wed Jun 9 22:28:00 2004
C-time: Wed Jun 9 22:28:00 2004

John Gray,2011-12-29 2:47 PM CT,Saved Deleted File Named file6.jpg

This is the parent window tab.

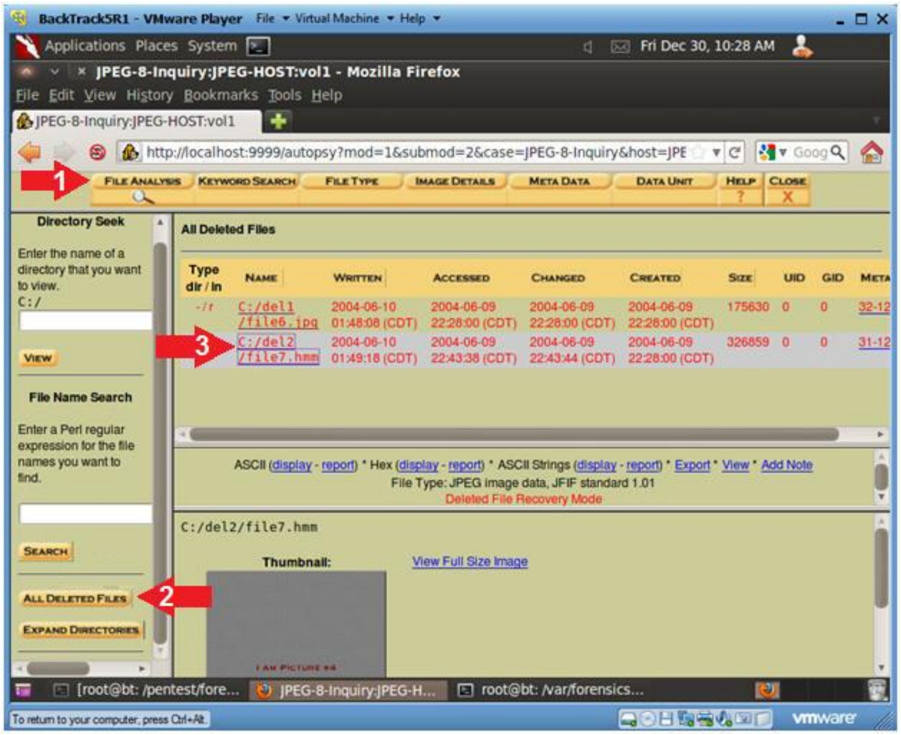
Do NOT close this tab.

This is the child window tab.

Close this tab window.

View Deleted File named file7.hmm

- Click on file7.hmm


BackTrack5R1 - VMware Player File Virtual Machine Help
Applications Places System
Fri Dec 30, 10:28 AM
JPEG-8-Inquiry:JPEG-HOST:vol1 - Mozilla Firefox
File Edit View History Bookmarks Tools Help
JPEG-8-Inquiry:JPEG-HOST:vol1
1
FILE ANALYSIS
KEYWORD SEARCH
FILE TYPE
IMAGE DETAILS
META DATA
DATA UNIT
HELP
CLOSE
Directory Seek
VIEW
File Name Search
SEARCH
ALL DELETED FILES
2
EXPAND DIRECTORIES
3
Thumbnail:
View Full Size Image
I AM PICTURE #4
[root@bt: /pentest/fore...
JPEG-8-Inquiry:JPEG-H...
root@bt: /var/forensics...
To return to your computer, press Ctrl+Alt.
vmware

http://localhost:9999/autopsy?mod=1&submod=2&case=JPEG-8-Inquiry&host=JPE

Enter the name of a directory that you want to view.
C:/

Enter a Perl regular expression for the file names you want to find.

All Deleted Files

Type dir / in	NAME	WRITTEN	ACCESSED	CHANGED	CREATED	SIZE	UID	GID	META
-/r	C:/del1 /file6.jpg	2004-06-10 01:48:08 (CDT)	2004-06-09 22:28:00 (CDT)	2004-06-09 22:28:00 (CDT)	2004-06-09 22:28:00 (CDT)	175630	0	0	32-12
	C:/del2 /file7.hmm	2004-06-10 01:49:18 (CDT)	2004-06-09 22:43:38 (CDT)	2004-06-09 22:43:44 (CDT)	2004-06-09 22:28:00 (CDT)	326859	0	0	31-12

ASCII (display - report) * Hex (display - report) * ASCII Strings (display - report) * Export * View * Add Note
File Type: JPEG image data, JFIF standard 1.01
Deleted File Recovery Mode

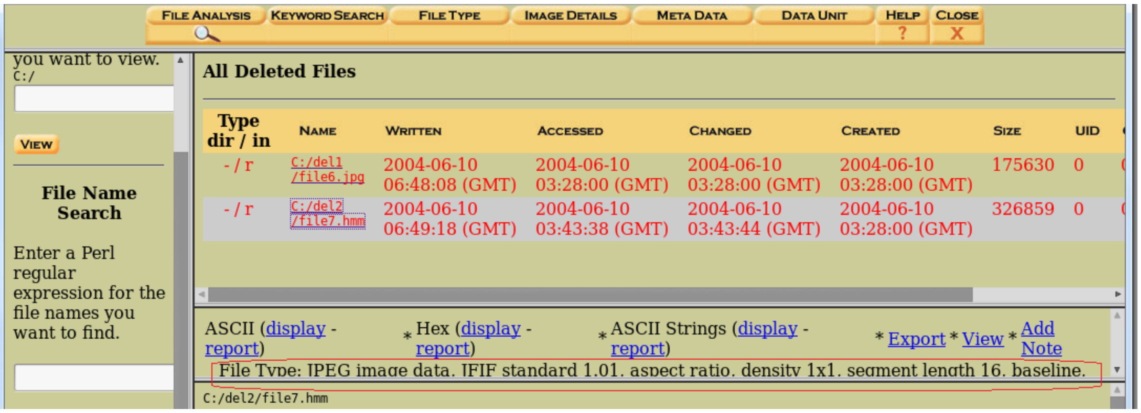
C:/del2/file7.hmm

Save the deleted File named file7.hmm

Autopsy identified the file type of file file7.hmm as a JPEG, even though the extension is ".hmm" instead of ".jpg." Trying to hide a file or an image is difficult when using the right set of forensic tools.

Also, you can view the thumbnail.

- Click on the Export Link to save the filename file7.hmm.



All Deleted Files

Type dir / in	Name	Written	Accessed	Changed	Created	Size	UID
-/r	C:/del1 /file6.jpg	2004-06-10 06:48:08 (GMT)	2004-06-10 03:28:00 (GMT)	2004-06-10 03:28:00 (GMT)	2004-06-10 03:28:00 (GMT)	175630	0
-/r	C:/del2 /file7.hmm	2004-06-10 06:49:18 (GMT)	2004-06-10 03:43:38 (GMT)	2004-06-10 03:43:44 (GMT)	2004-06-10 03:28:00 (GMT)	326859	0

ASCII (display - report) * Hex (display - report) * ASCII Strings (display - report) * Export * View * Add Note

File Type: JPEG image data, JFIF standard 1.01, aspect ratio, density 1x1, segment length 16, baseline,

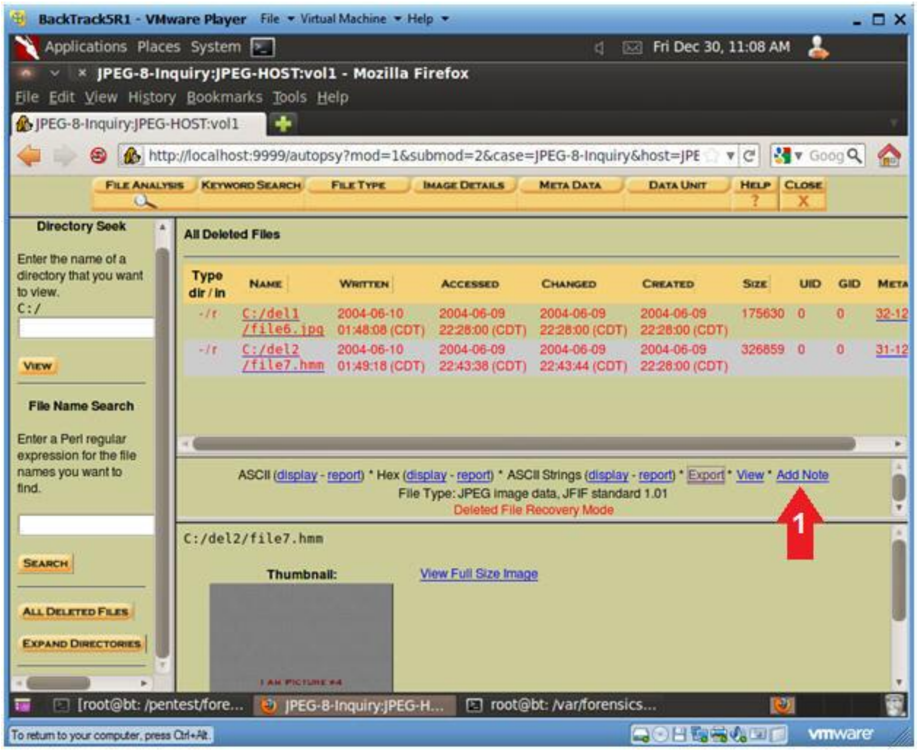
C:/del2/file7.hmm

Save Deleted File named file7.hmm

- Click the Save File and repeat the steps used to save the first file.

Add Note to file7.hmm

- Click on the Add Note link.



http://localhost:9999/autopsy?mod=1&submod=2&case=JPEG-8-Inquiry&host=JPE

All Deleted Files

Type dir / in	Name	Written	Accessed	Changed	Created	Size	UID	GID	Meta
-/r	C:/del1 /file6.jpg	2004-06-10 01:48:08 (CDT)	2004-06-09 22:28:00 (CDT)	2004-06-09 22:28:00 (CDT)	2004-06-09 22:28:00 (CDT)	175630	0	0	32-12
-/r	C:/del2 /file7.hmm	2004-06-10 01:49:18 (CDT)	2004-06-09 22:43:38 (CDT)	2004-06-09 22:43:44 (CDT)	2004-06-09 22:28:00 (CDT)	326859	0	0	31-12

ASCII (display - report) * Hex (display - report) * ASCII Strings (display - report) * Export * View * Add Note

File Type: JPEG image data, JFIF standard 1.01

Deleted File Recovery Mode

C:/del2/file7.hmm

Add Note to file6.jpg

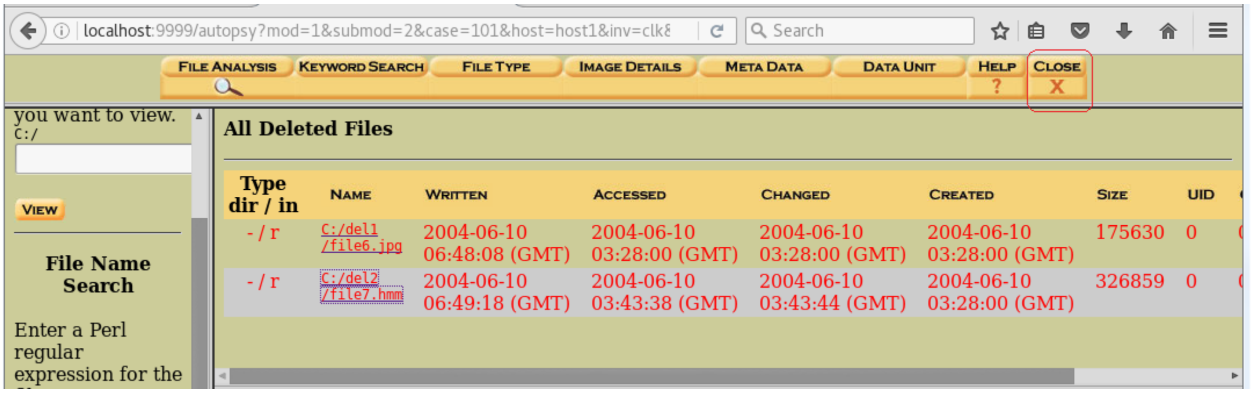
Add the following information to the Note Text Box

- Your Actual Name
- Current Date and Time
- Add a Comment

Click the OK button.

Verify Notes

- Click the View Notes Button.
- Close the child window, close Autopsy

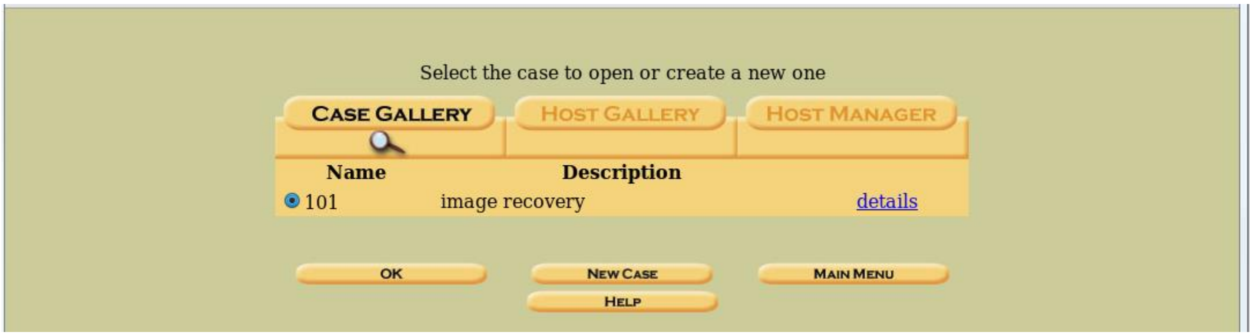


localhost:9999/autopsy?mod=1&submod=2&case=101&host=host1&inv=clk8

All Deleted Files

Type dir / in	NAME	WRITTEN	ACCESSED	CHANGED	CREATED	SIZE	UID
- / r	C:/del1 /file6.jpg	2004-06-10 06:48:08 (GMT)	2004-06-10 03:28:00 (GMT)	2004-06-10 03:28:00 (GMT)	2004-06-10 03:28:00 (GMT)	175630	0
- / r	C:/del2 /file7.hmm	2004-06-10 06:49:18 (GMT)	2004-06-10 03:43:38 (GMT)	2004-06-10 03:43:44 (GMT)	2004-06-10 03:28:00 (GMT)	326859	0

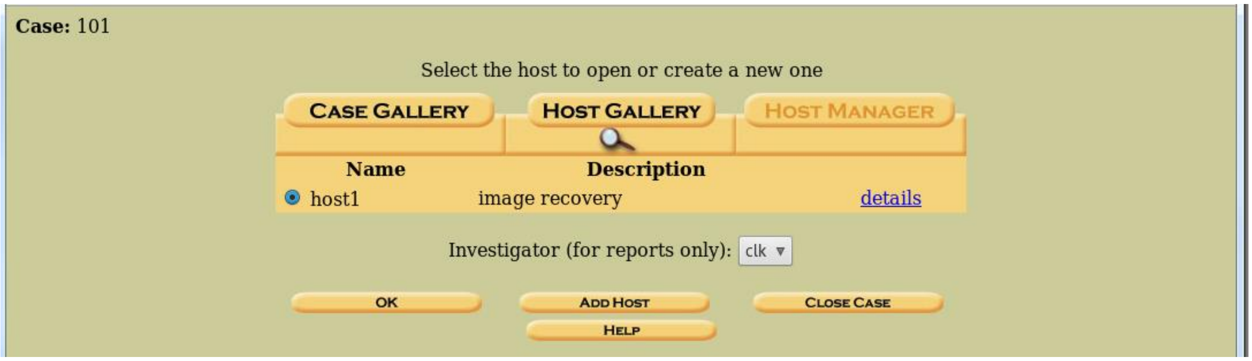
- Close the host
- Close the case
- From the Case Gallery, find your existing case and click the OK button



Select the case to open or create a new one

Name	Description	
● 101	image recovery	details

- From the Host Gallery, click the OK button



Case: 101

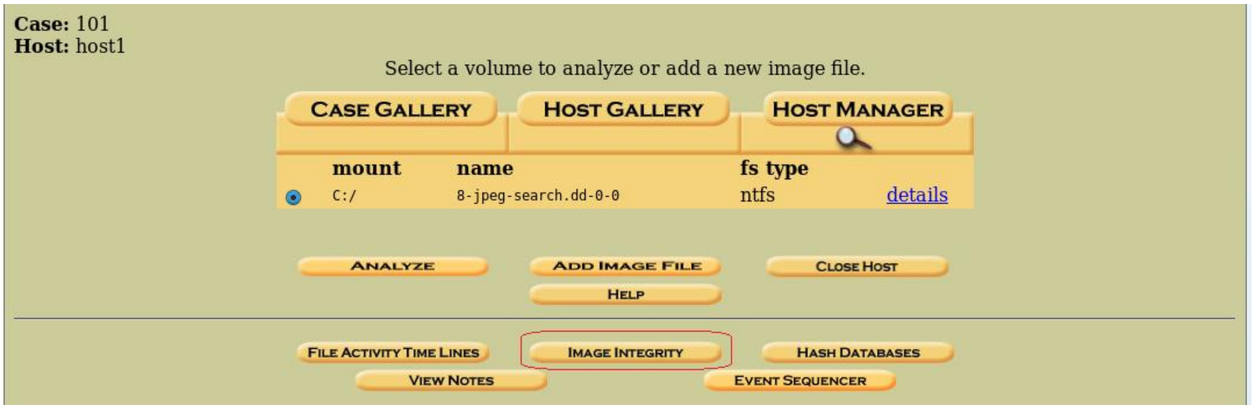
Select the host to open or create a new one

Name	Description	
● host1	image recovery	details

Investigator (for reports only): clk

Image Integrity Check

- Click on the Image Integrity Button.



Case: 101
Host: host1

Select a volume to analyze or add a new image file.

mount	name	fs type	
● C:/	8-jpeg-search.dd-0-0	ntfs	details

Image Integrity Check

Notice the "original" MD5 Check Sum immediately follows the 8-jpeg-search.dd image.

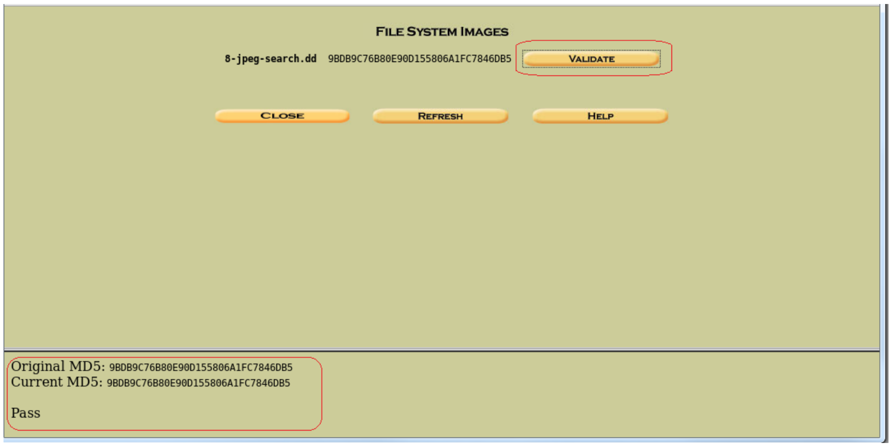
Click on the Validate Button.

Below Autopsy compares the original MD5 Check Sum with the current MD5 Check Sum.

Note: (Why are we doing this?)

In general, you want to make sure that your work did not compromise the image.

This is particularly important in a court of law, especially evidence law when both integrity and chain of custody can be challenged and scrutinized.



8-jpeg-search.dd 9BDB9C76B80E90D155806A1FC7846DB5

Original MD5: 9BDB9C76B80E90D155806A1FC7846DB5
Current MD5: 9BDB9C76B80E90D155806A1FC7846DB5

Pass

End of the Lab!