DIGITAL FORENSICS LAB SERIES

Lab 8: Introduction to PTK Forensics Basic Edition

Objective: Evidence Acquisition, Preparation and Preservation

Document Version: 2015-09-28

Development was funded by the Department of Labor (DOL) Trade Adjustment Assistance Community College and Career Training (TAACCCT) Grant No. TC-22525-11-60-A-48; The National Information Security, Geospatial Technologies Consortium (NISGTC) is an entity of Collin College of Texas, Bellevue College of Washington, Bunker Hill Community College of Massachusetts, Del Mar College of Texas, Moraine Valley Community College of Illinois, Rio Salado College of Arizona, and Salt Lake Community College of Utah.

This workforce solution was funded by a grant awarded by the U.S. Department of Labor's Employment and Training Administration. The solution was created by the grantee and does not necessarily reflect the official position of the U.S. Department of Labor. The Department of Labor makes no guarantees, warranties or assurances of any kind, express or implied, with respect to such information, including any information on linked sites, and including, but not limited to accuracy of the information or its completeness, timeliness, usefulness, adequacy, continued availability or ownership.

Contents

Introduction

This lab includes the following tasks:

1. Loading and Verifying an Image
2. Exploring Image Details
3. Extracting Files
4. Forensic Reporting with PTK

Objective: Evidence Acquisition, Preparation and Preservation

Performing this lab will provide the student with a hands-on lab experience meeting the Evidence Acquisition, Preparation and Preservation Objective:

The candidate will demonstrate understanding of evidence chain-of-custody and integrity, E-discovery concepts, evidence acquisition and preservation, and the tools and techniques used by computer forensic examiners.

Understanding file systems is key to understanding Computer Forensics investigations. File systems store data in different ways. The NTFS file system is commonly used on Microsoft Windows operating systems. It can also be utilized by Linux and Mac OS X.

PTK – An open source forensic suite that will allow you to analyze disk images.

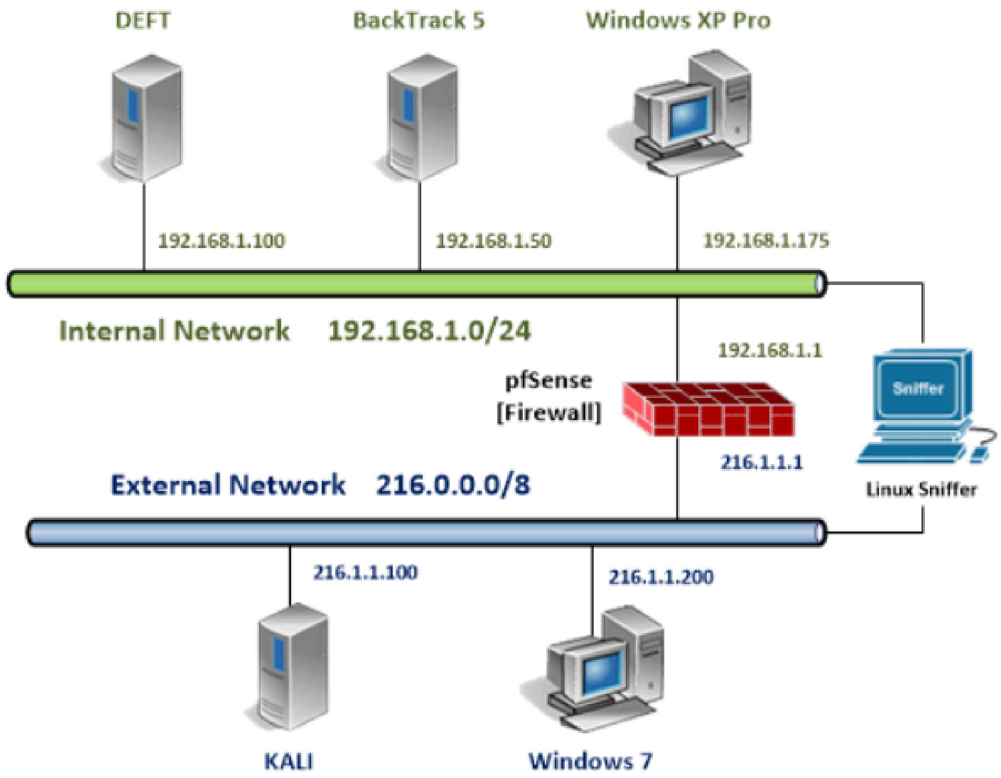
The Sleuth Kit – The Sleuth Kit (TSK) is a collection of command line tools that are utilized by the Autopsy forensic browser. The Sleuth Kit tools can be utilized without Autopsy.

$MFT – The Master File Table is similar to a Table of Contents for an NTFS volume.

MD5 – Message Digest 5 is a 128-bit hashing algorithm that aids forensic examiners by “proving” that the copy of the media they are working on is "equivalent" to the original. Other hashes, like SHA-1, which is 160 bits, are more accurate than the 128 bit MD5.

SHA1 – Secure Hash Algorithm is a 160-bit hashing algorithm that aids forensic examiners by “proving” that the copy of the media they are working on is "equivalent" to the original. There are also 256, 384, and 512-bit versions of SHA that are more accurate.

Lab Topology



Lab Settings

The information in the table below will be needed in order to complete the lab. The task sections below provide details on the use of this information.

Virtual Machine	IP Address	Account (if needed)	Password (if needed)
BackTrack 5 R3 Internal Machine	192.168.1.50	root	toor

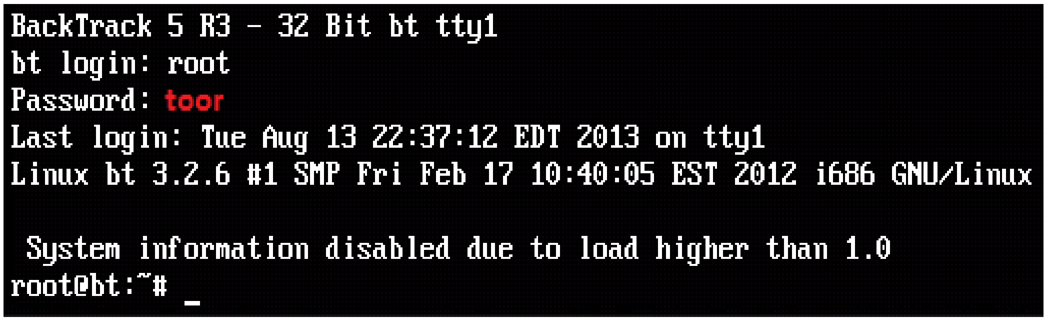
1 Loading and Verifying an Image

An image is a bit-by-bit copy of a disk. Starting with Windows Vista, NTFS had to be used on the OS drive. NTFS is also commonly utilized on data drives. PTK is included with Release 5 of BackTrack. It is not included with the Kali distribution.

1.1 Verifying and Viewing Image Details

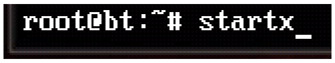
1. Open the **BackTrack 5 R3 Internal Machine**. Type **root** for the login and **toor** *(root spelled backwards)* for the password.

The password will not be displayed when you type it, for security purposes.



```
BackTrack 5 R3 - 32 Bit bt tty1
bt login: root
Password: toor
Last login: Tue Aug 13 22:37:12 EDT 2013 on tty1
Linux bt 3.2.6 #1 SMP Fri Feb 17 10:40:05 EST 2012 i686 GNU/Linux

 System information disabled due to load higher than 1.0
root@bt:~# _
```

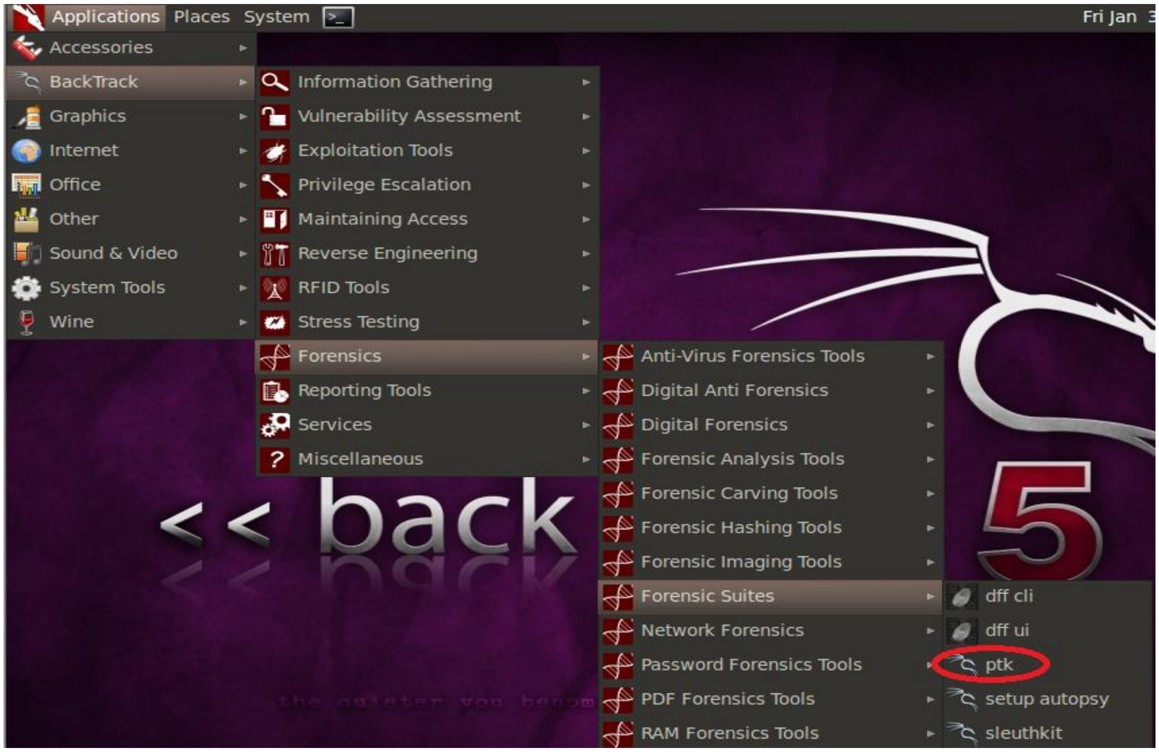
2. Type the following command to start the Graphical User Interface (GUI):
root@bt:~# **startx**



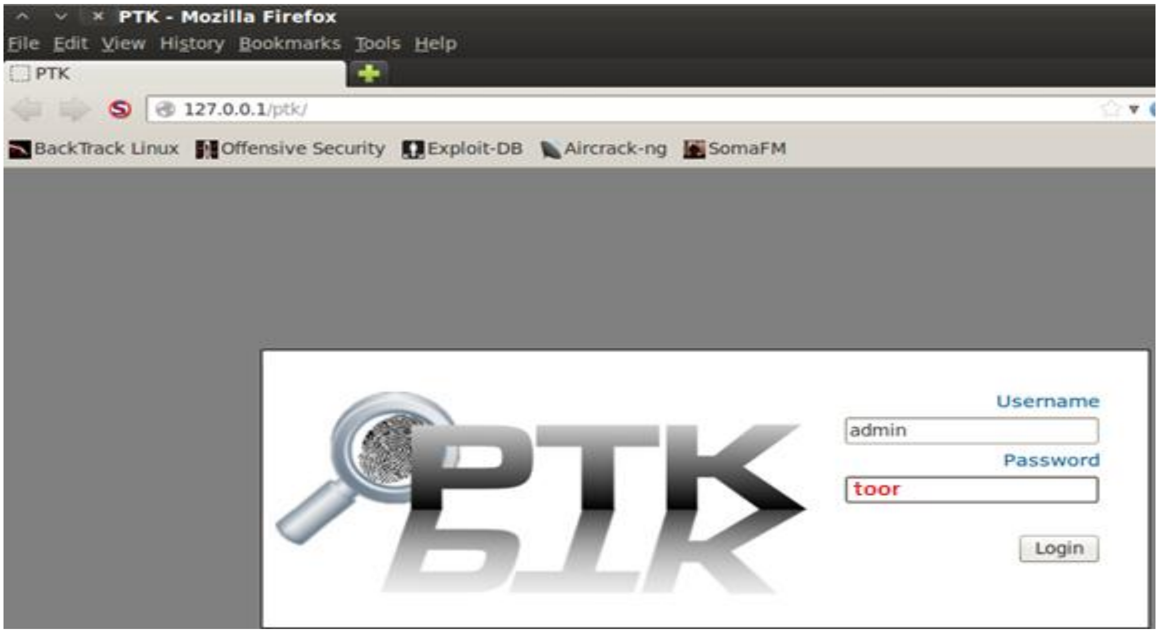
```
root@bt:~# startx_
```

3. The BackTrack 5 GUI screen may appear in a few seconds after loading.

4. To use the PTK forensic suite, click **Applications > BackTrack > Forensics > Forensic Suites > PTK.**



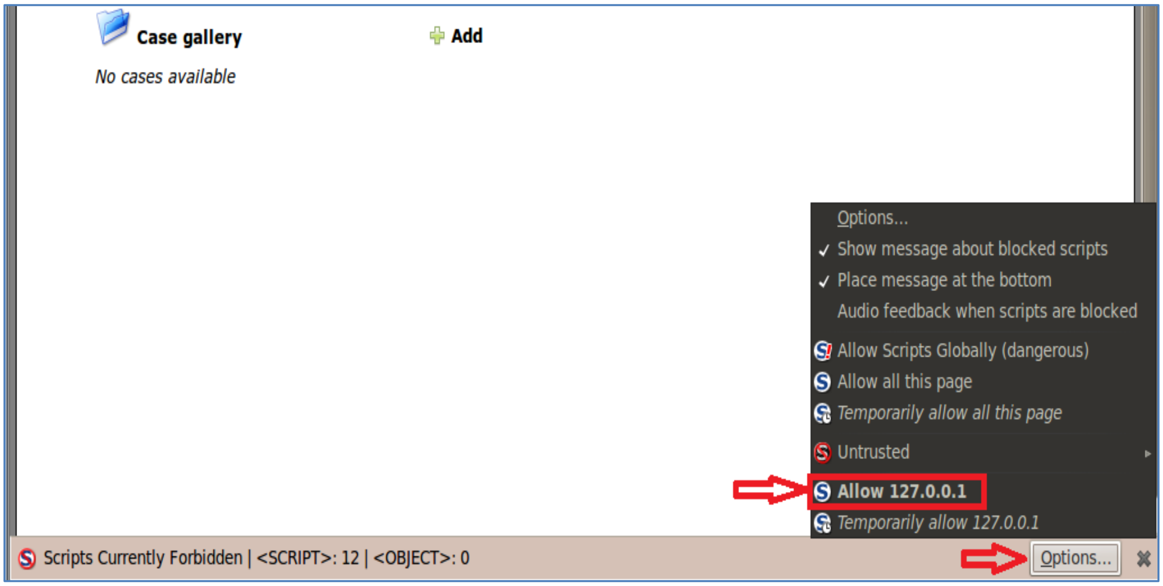
5. For the username, type **admin** and for the password, type **toor.**



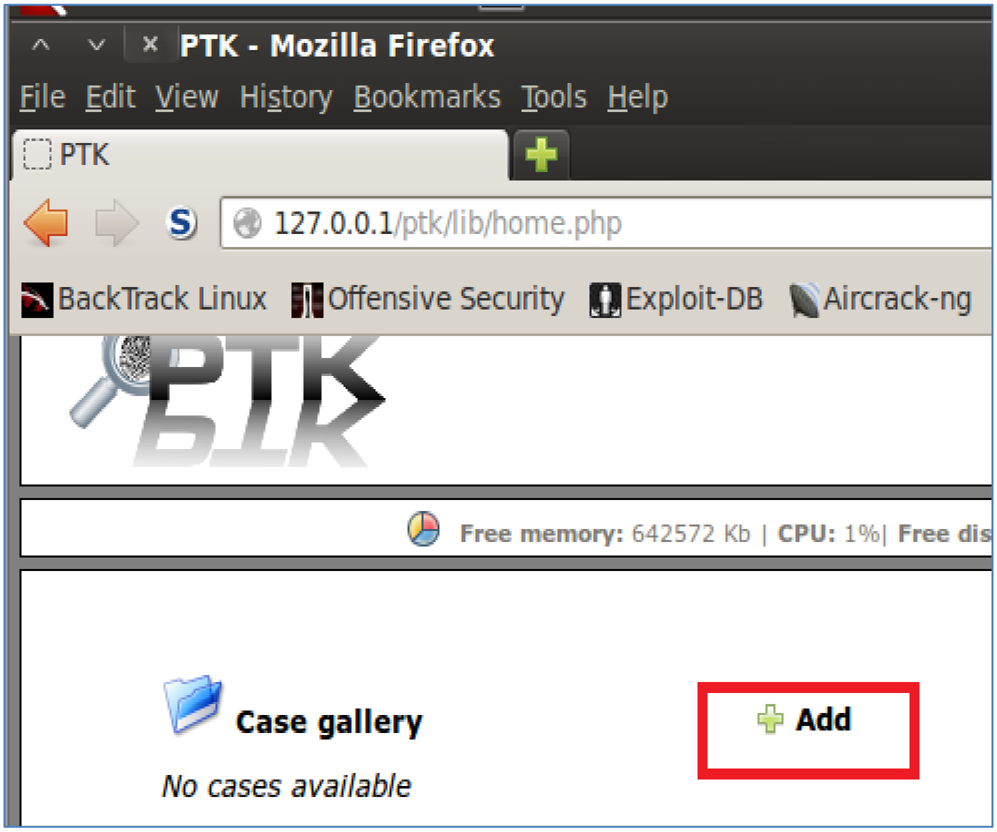
Username: admin

Password: toor

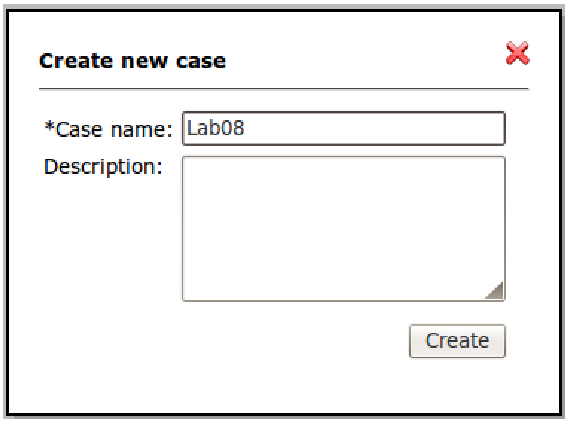
6. In the bottom-right corner of Firefox, click **Options** and click **Allow 127.0.0.1**.


Case gallery
Add
No cases available
Options...
✓ Show message about blocked scripts
✓ Place message at the bottom
Audio feedback when scripts are blocked
Allow Scripts Globally (dangerous)
Allow all this page
Temporarily allow all this page
Untrusted
Allow 127.0.0.1
Temporarily allow 127.0.0.1
Scripts Currently Forbidden | <SCRIPT>: 12 | <OBJECT>: 0
Options...

7. Click the **Add** button to start a new case within PTK.



8. Enter **Lab08** as the Case name. Click **Create**.

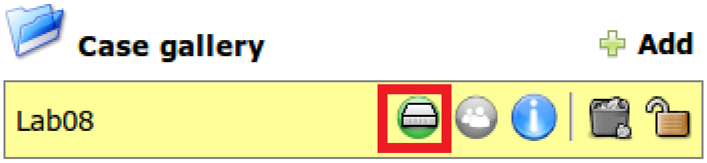


Create new case

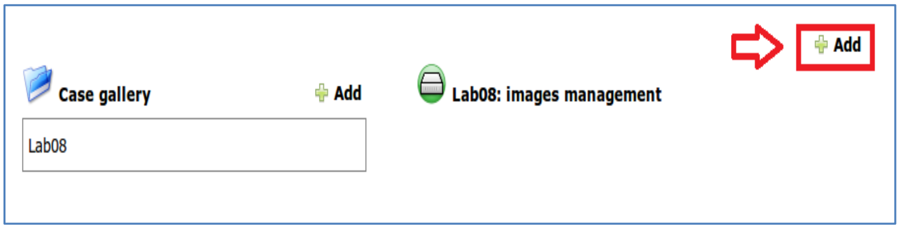
*Case name: Lab08

Description:

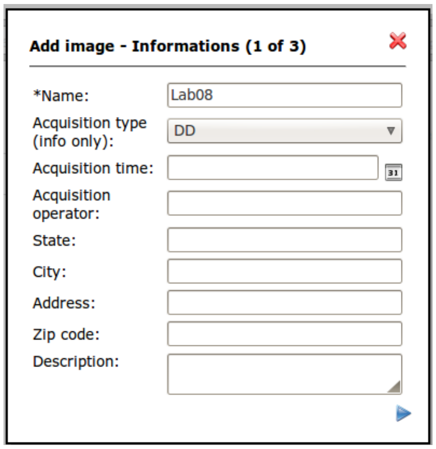
9. Hover mouse pointer over the Lab08 box under Case gallery and click the green icon to **Manage images**.



10. Click **Add** on the far right to add an image to the Case gallery.



11. Type **Lab08** for the name and select DD for acquisition type. Click the blue arrow to continue.



Add image - Informations (1 of 3)

*Name: Lab08

Acquisition type (info only): DD

Acquisition time:

Acquisition operator:

State:

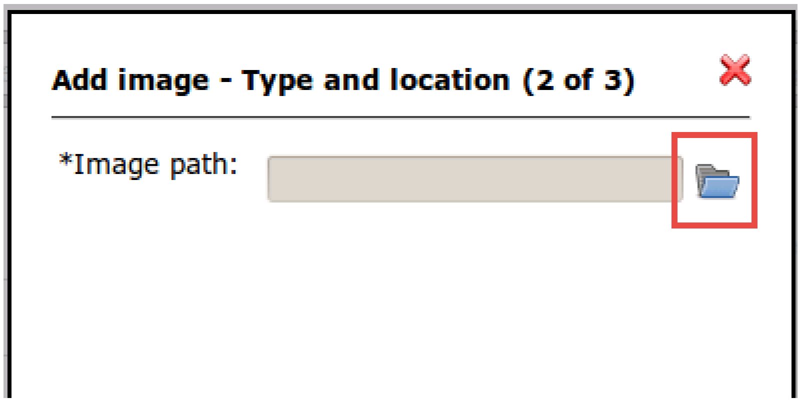
City:

Address:

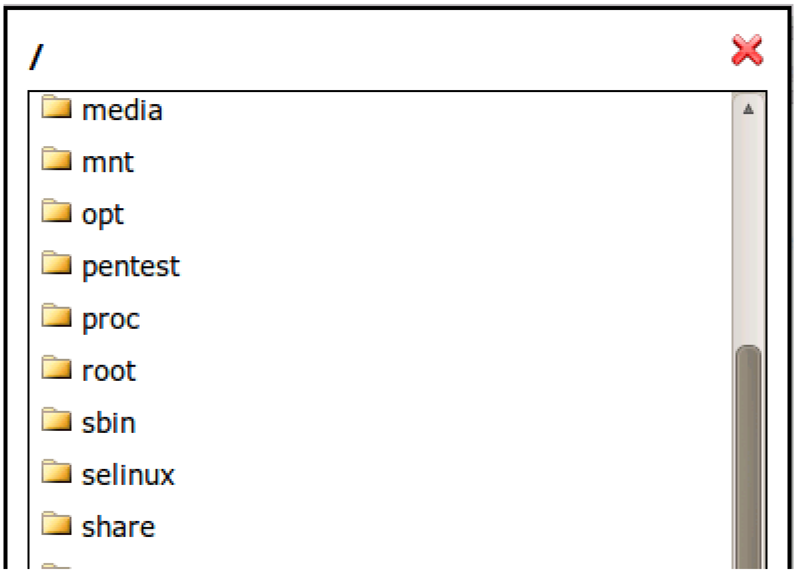
Zip code:

Description:

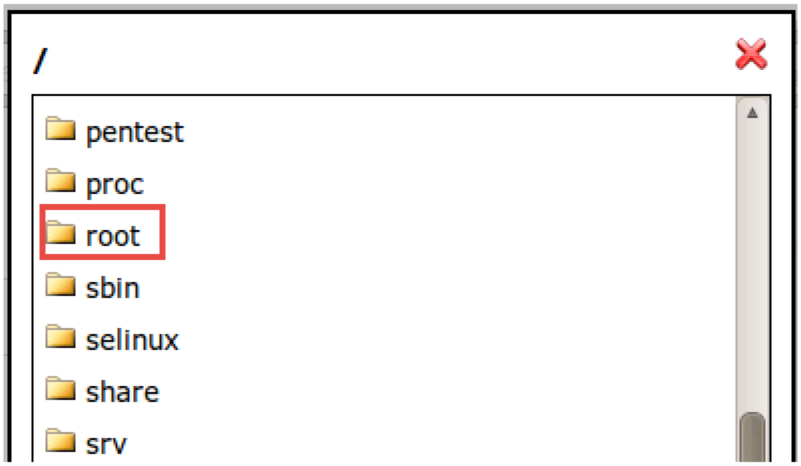
12. Click the blue folder to start browsing.



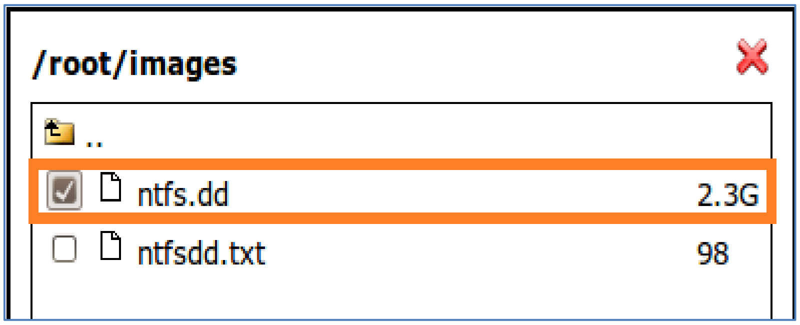
13. Click the yellow folder icon four times to move up to the / root directory.



14. Click the **root** folder, and then click the **images** folder.



15. Check the **ntfs.dd** file and click the blue arrow on the right to continue.



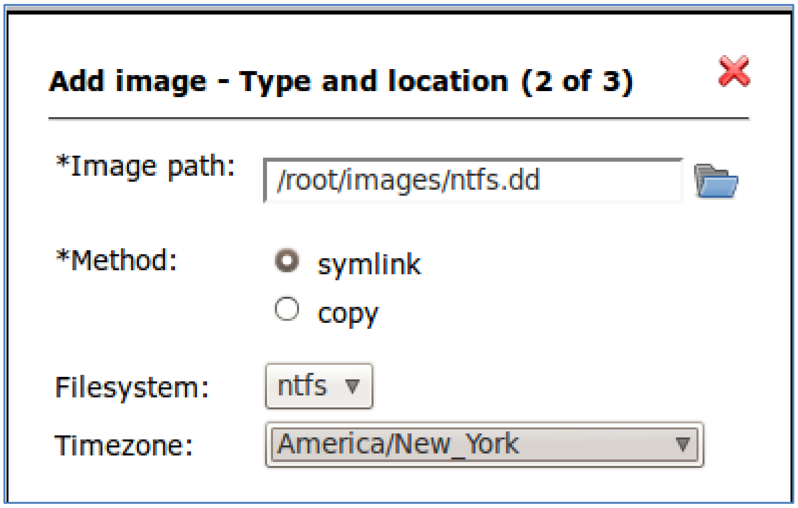
/root/images

..

☑ ntfs.dd 2.3G

□ ntfsdd.txt 98

16. Verify that **symlink** is checked and that the filesystem is recognized as NTFS. Use the drop-down box to change the Timezone to **America/New_York**. Click the blue arrow on the right to continue.



Add image - Type and location (2 of 3)

*Image path: /root/images/ntfs.dd

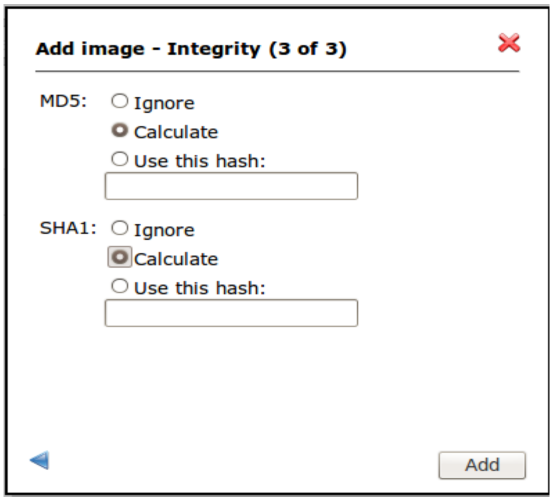
*Method: ● symlink ○ copy

Filesystem: ntfs ▾

Timezone: America/New_York ▾

17. For the MD5 and the SHA1 images, select **Calculate**. Click **Add**.

The images will take approximately 5-10 minutes to calculate.

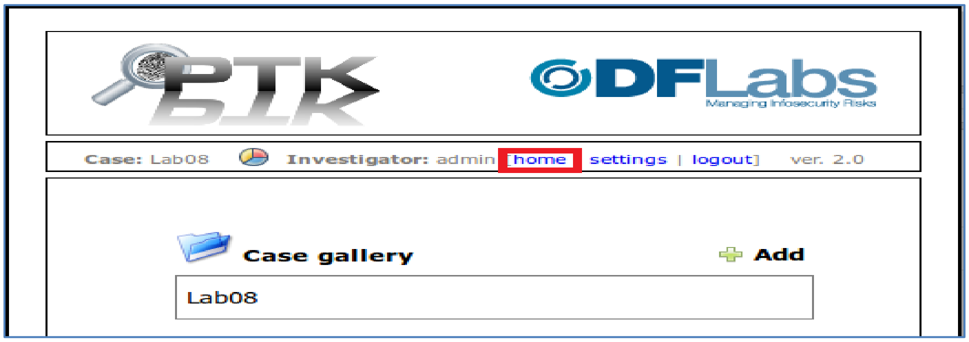


Add image - Integrity (3 of 3)

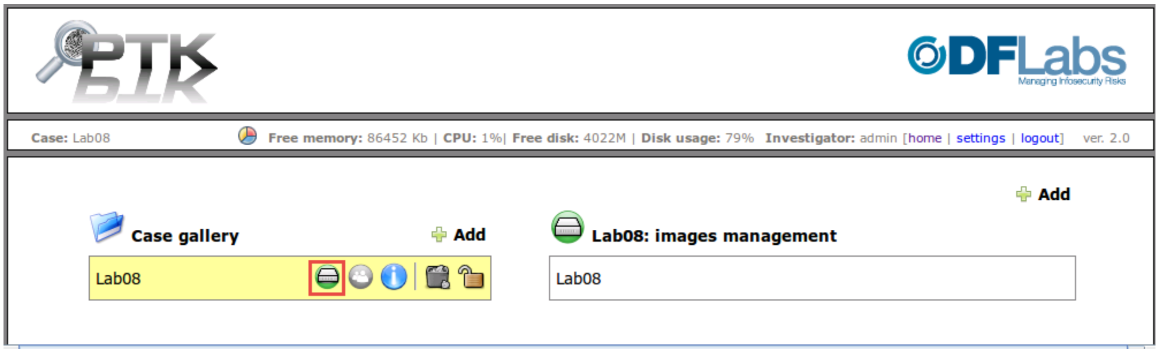
MD5: ○ Ignore ● Calculate ○ Use this hash:

SHA1: ○ Ignore ● Calculate ○ Use this hash:

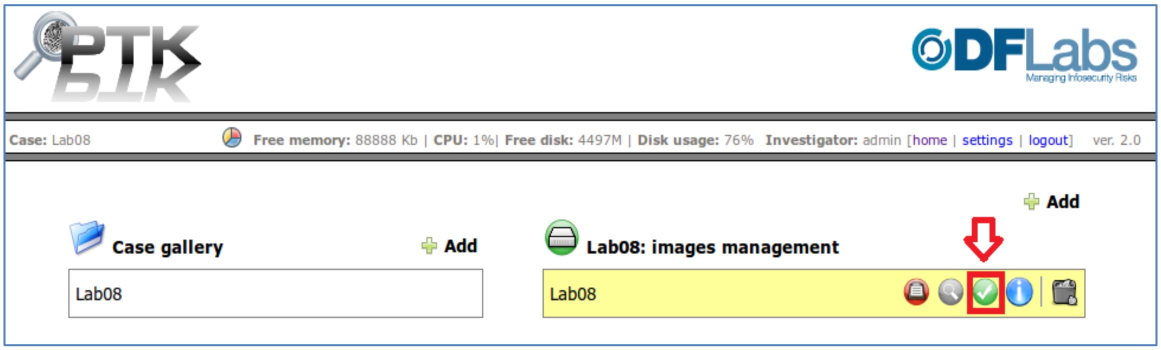
18. Click the home link to go back a page.


PTK
DFLabs
Managing Infosecurity Risks
Case: Lab08
Investigator: admin [home | settings | logout]
ver. 2.0
Case gallery
Add
Lab08

19. Hover over the Lab08 box under **Case gallery** and click **Manage Images.**


PTK
DFLabs
Managing Infosecurity Risks
Case: Lab08
Free memory: 86452 Kb | CPU: 1%| Free disk: 4022M | Disk usage: 79%
Investigator: admin [home | settings | logout]
ver. 2.0
Case gallery
Add
Lab08
Add
Lab08: images management
Lab08

20. On the right side of the screen, click the green check icon under Lab08: images management.


PTK
DFLabs
Managing Infosecurity Risks
Case: Lab08
Free memory: 88888 Kb | CPU: 1%| Free disk: 4497M | Disk usage: 76%
Investigator: admin [home | settings | logout]
ver. 2.0
Case gallery
Add
Lab08
Add
Lab08: images management
Lab08

21. After clicking the image integrity check button, you will see the calculated hashes.

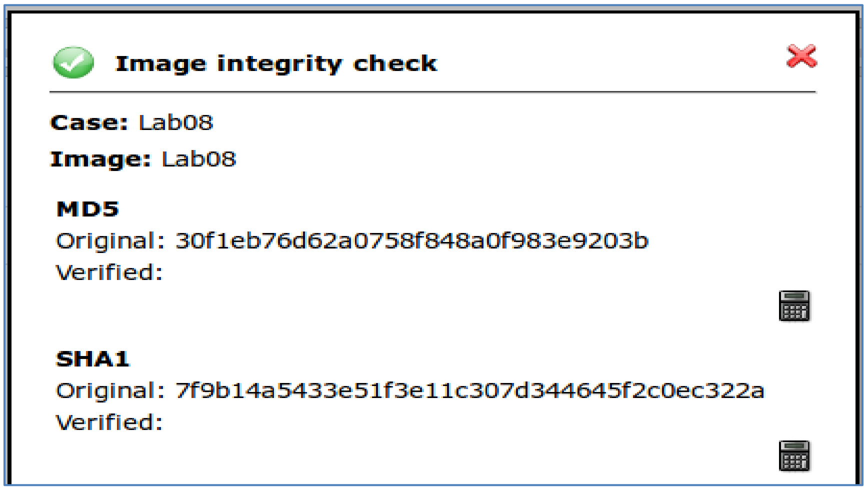


Image integrity check

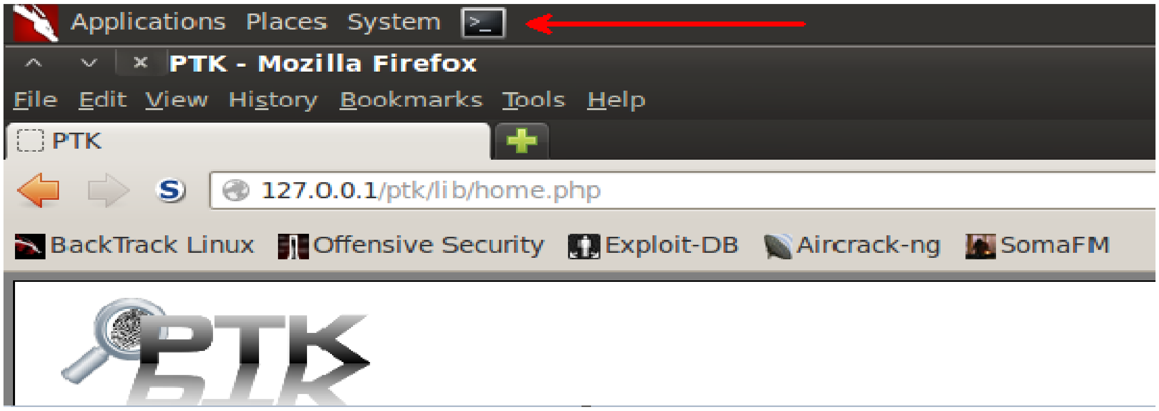
Case: Lab08

Image: Lab08

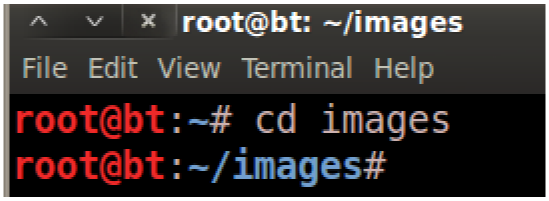
MD5
Original: 30f1eb76d62a0758f848a0f983e9203b
Verified:

SHA1
Original: 7f9b14a5433e51f3e11c307d344645f2c0ec322a
Verified:

22. Open a terminal on the Linux system by clicking on the picture to the right of the word **System** in the task bar in the top of the screen of the BackTrack 5 R3 Internal Machine.

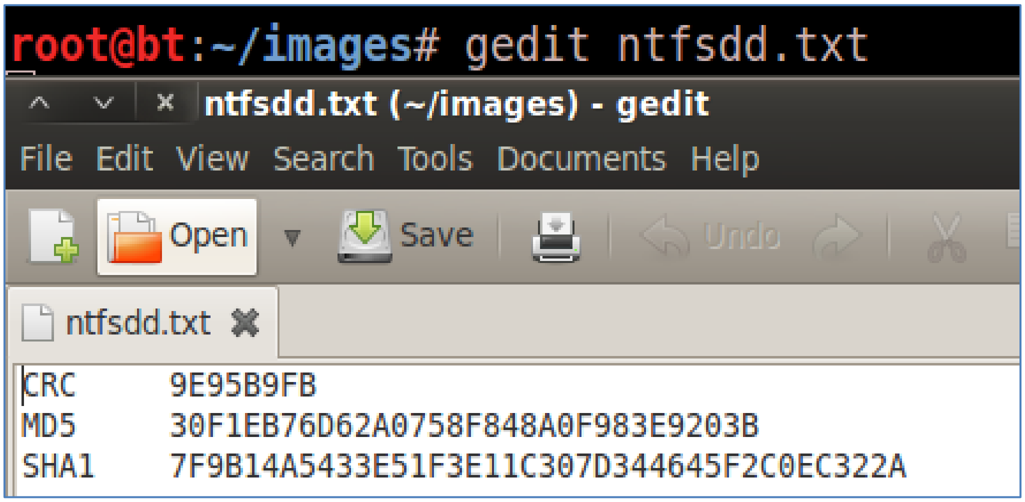

Applications Places System
PTK - Mozilla Firefox
File Edit View History Bookmarks Tools Help
PTK
127.0.0.1/ptk/lib/home.php
BackTrack Linux
Offensive Security
Exploit-DB
Aircrack-ng
SomaFM
PTK

23. Switch to the images directory by typing the following command:
root@bt:~# **cd images**



```
root@bt:~# cd images
root@bt:~/images#
```

24. Type the following command to view the file from the Graphical User Interface: root@bt:~/images# **gedit ntfsdd.txt**

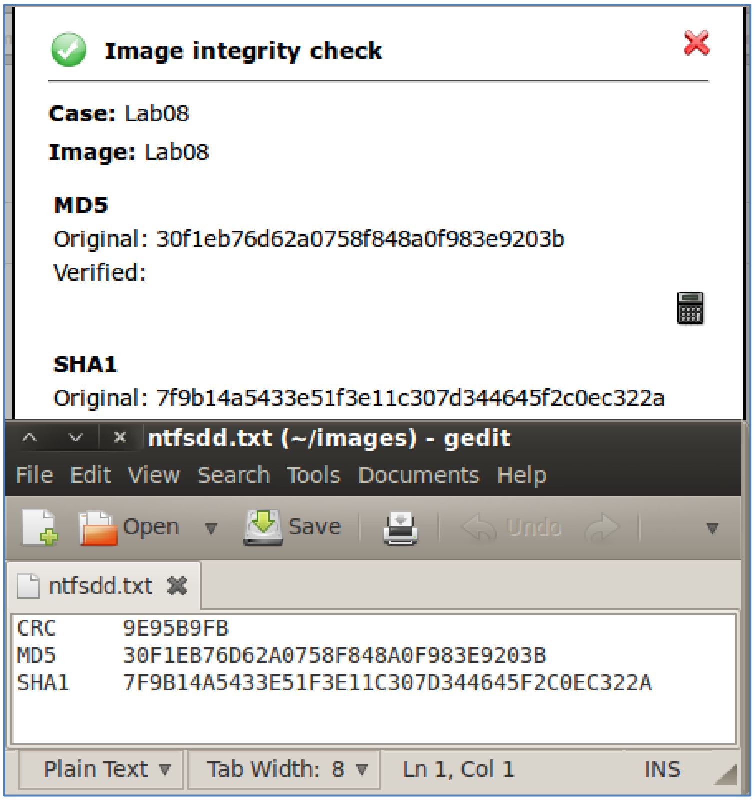


```
root@bt:~/images# gedit ntfsdd.txt
```

ntfsdd.txt (~/images) - gedit
File Edit View Search Tools Documents Help
Open
Save
Undo
ntfsdd.txt

```
CRC     9E95B9FB
MD5     30F1EB76D62A0758F848A0F983E9203B
SHA1    7F9B14A5433E51F3E11C307D344645F2C0EC322A
```

25. Examine the PTK and ntfsdd.txt hash values. Both the MD5 and SHA1 hash values from PTK should match the hash values reported by the incident responder.



Case: Lab08

Image: Lab08

MD5

Original: 30f1eb76d62a0758f848a0f983e9203b

Verified:

SHA1

Original: 7f9b14a5433e51f3e11c307d344645f2c0ec322a

ntfsdd.txt (~/images) - gedit
File Edit View Search Tools Documents Help
Open
Save
Undo
ntfsdd.txt

```
CRC     9E95B9FB
MD5     30F1EB76D62A0758F848A0F983E9203B
SHA1    7F9B14A5433E51F3E11C307D344645F2C0EC322A
```

26. Close the ntfsdd.txt file when you are finished viewing it with the gedit application. Close the Linux terminal. Also, close the Image Integrity check window, but leave PTK running.

1.2 Conclusion

PTK comes installed on BackTrack, but the end user still needs to do some configuration, including specifying the image location and where evidence will be stored.

1.3 Discussion Questions

1. Why do you need to verify image integrity?
2. What are the most common types of hash values used in computer forensics?
3. What types of things are done in PTK during the initial case setup?
4. Describe a method to determine that an image has been successfully recognized.

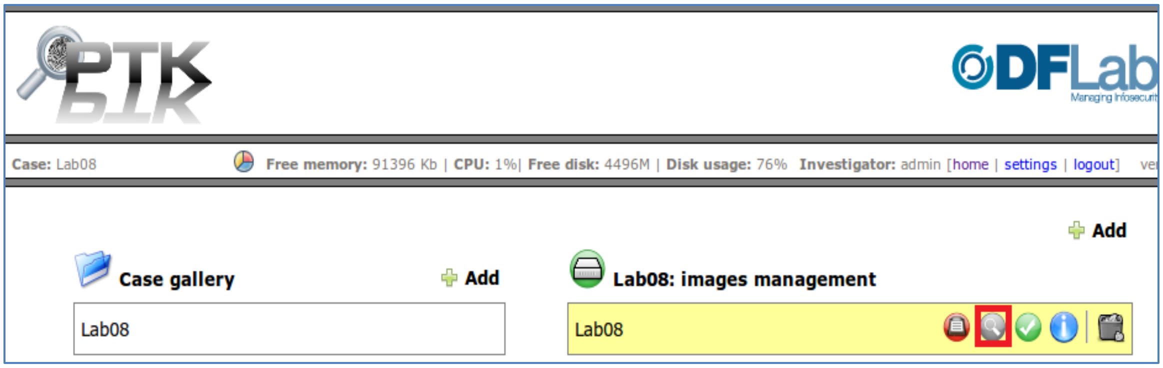
2 Exploring the Image Details

Performing forensic analysis requires loading an image file into a forensic tool. The most widely used forensic tools are commercial tools like EnCase and FTK (Forensic Tool Kit). EnCase is made by Guidance software and FTK is made by Access Data. Both tools require hardware dongles, which helps to prevent illegal copies of the software. There are some free tools, such as Autopsy and PTK, which also can be used to perform forensic analysis.

2.1 Loading the NTFS Image into PTK

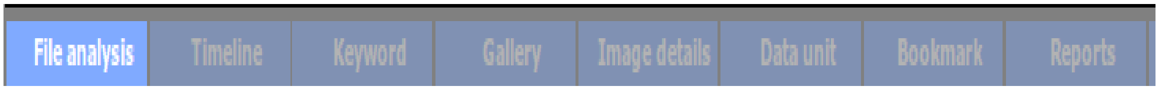
PTK is included with Release 5 of BackTrack. It is not included with the Kali distribution.

1. In the right pane, under lab 8: images management, click the gray **magnifying glass** icon. This button is used to analyze the NTFS image loaded into the case.



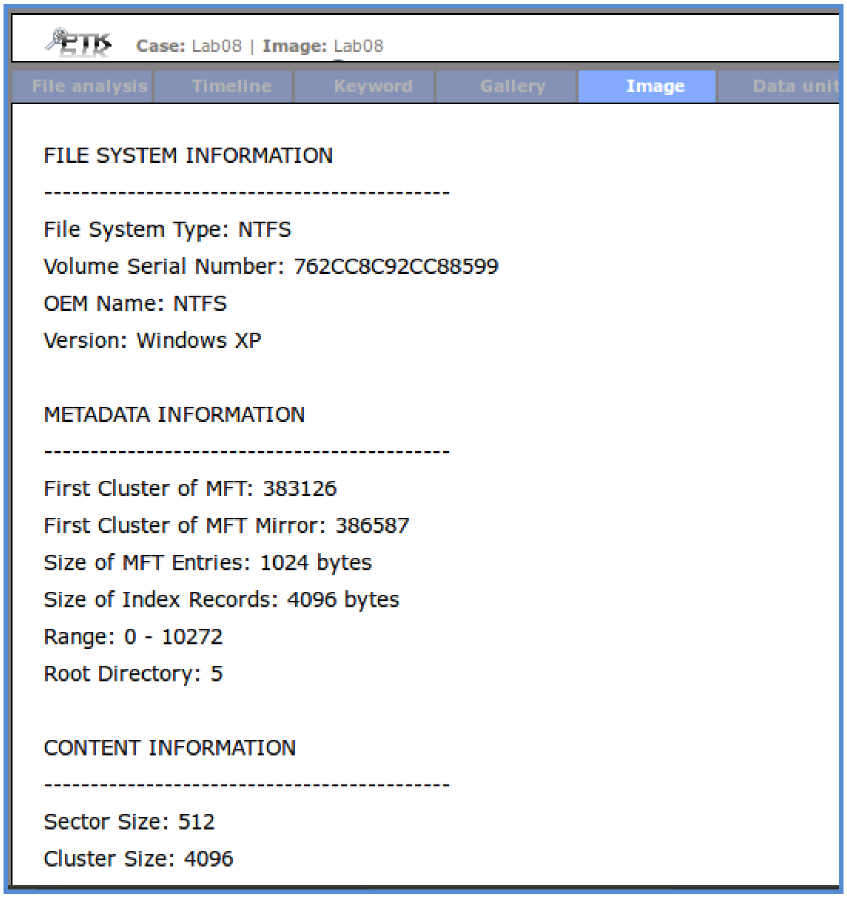
Case: Lab08 Free memory: 91396 Kb | CPU: 1%| Free disk: 4496M | Disk usage: 76% Investigator: admin [home | settings | logout] ve

2. View all of the available tabs within the PTK menu.



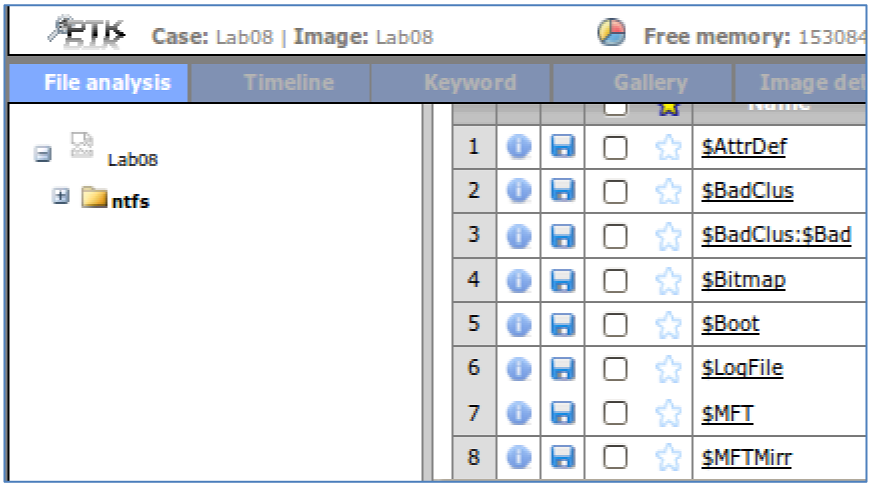
List of Tabs
File Analysis
Timeline
Keyword
Gallery
Image Details
Data Unit
Bookmark
Data Unit

3. Click the **Image** tab of PTK and examine the details of the image.



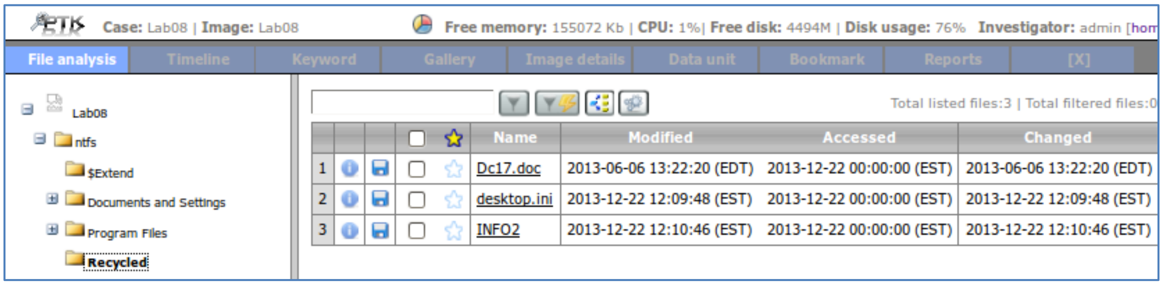
```
FILE SYSTEM INFORMATION
--------------------------------------------
File System Type: NTFS
Volume Serial Number: 762CC8C92CC88599
OEM Name: NTFS
Version: Windows XP

METADATA INFORMATION
--------------------------------------------
First Cluster of MFT: 383126
First Cluster of MFT Mirror: 386587
Size of MFT Entries: 1024 bytes
Size of Index Records: 4096 bytes
Range: 0 - 10272
Root Directory: 5

CONTENT INFORMATION
--------------------------------------------
Sector Size: 512
Cluster Size: 4096
```

4. Click the **File Analysis** tab of PTK, Expand Lab08, and then click on **NTFS**. Notice the NTFS system files including the Master File Table ($MFT) and $MFTMirr. These files cannot be seen within Windows, even if hidden files are shown.



1	☐	☆	$AttrDef
2	☐	☆	$BadClus
3	☐	☆	$BadClus:$Bad
4	☐	☆	$Bitmap
5	☐	☆	$Boot
6	☐	☆	$LogFile
7	☐	☆	$MFT
8	☐	☆	$MFTMirr

5. Within the File Analysis tab of PTK, expand NTFS, and select the **Recycled** folder. In the right pane, you will see a list of the files that are present. There are 3 files.

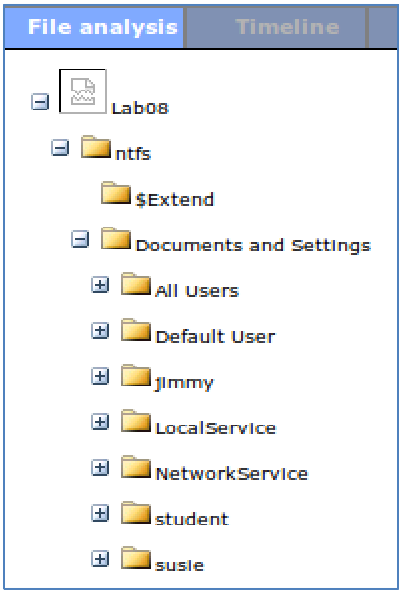


Case: Lab08 | **Image:** Lab08 **Free memory:** 155072 Kb | **CPU:** 1%| **Free disk:** 4494M | **Disk usage:** 76% **Investigator:** admin [hom

Total listed files:3 | Total filtered files:0

			□	☆	Name	Modified	Accessed	Changed
1			□	☆	Dc17.doc	2013-06-06 13:22:20 (EDT)	2013-12-22 00:00:00 (EST)	2013-06-06 13:22:20 (EDT)
2			□	☆	desktop.ini	2013-12-22 12:09:48 (EST)	2013-12-22 00:00:00 (EST)	2013-12-22 12:09:48 (EST)
3			□	☆	INFO2	2013-12-22 12:10:46 (EST)	2013-12-22 00:00:00 (EST)	2013-12-22 12:10:46 (EST)

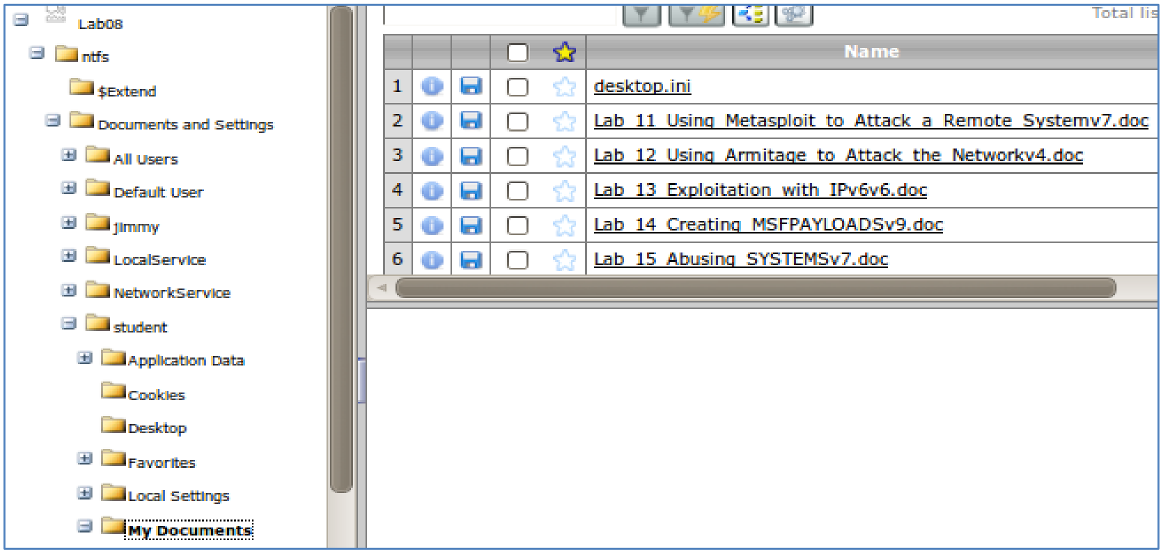
6. Within the File Analysis tab of PTK, expand NTFS, and expand the Documents and Settings folder. This will allow you to determine what user profiles have been loaded on to the system. In this case, three users have logged on to this system.



Documents and Settings Folder Breakdown

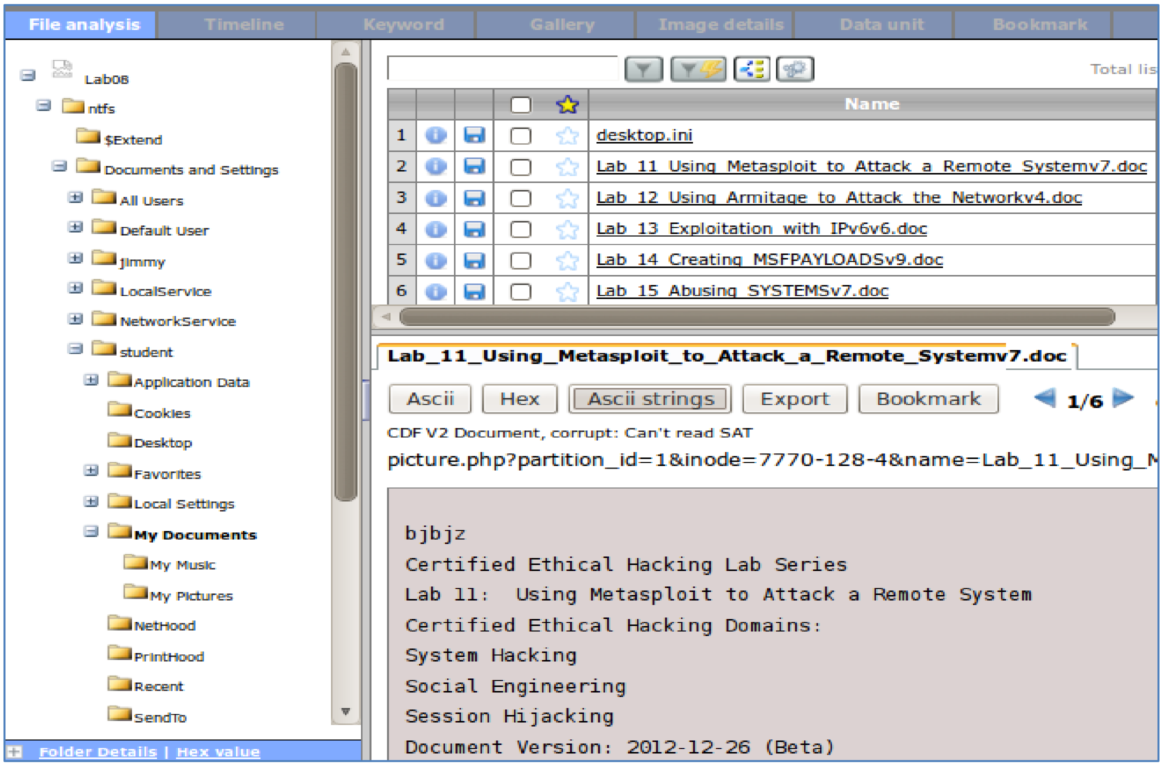
User(s)	Status
All Users	Present on All Windows XP/2003 Systems
Default User	Present on All Windows XP/2003 Systems
jimmy	This Account has Logged On to the System
LocalService	Present on All Windows XP/2003 Systems
NetworkService	Present on All Windows XP/2003 Systems
student	This Account has Logged On to the System
susie	This Account has Logged On to the System

7. Within the File Analysis tab of PTK, expand NTFS, expand Documents and Settings, student, and click on My Documents. This will allow us to view the items within the **My Documents** folder for this user account. There are several documents.



					Name
1			□	☆	desktop.ini
2			□	☆	Lab_11_Using_Metasploit_to_Attack_a_Remote_Systemv7.doc
3			□	☆	Lab_12_Using_Armitage_to_Attack_the_Networkv4.doc
4			□	☆	Lab_13_Exploitation_with_IPv6v6.doc
5			□	☆	Lab_14_Creating_MSFPAYLOADSv9.doc
6			□	☆	Lab_15_Abusing_SYSTEMSv7.doc

8. Click on the link to **Lab 11** within PTK. In the bottom pane, click the **ACSII strings** tab to view information within the Word document.



					Name
1			□	☆	desktop.ini
2			□	☆	Lab_11_Using_Metasploit_to_Attack_a_Remote_Systemv7.doc
3			□	☆	Lab_12_Using_Armitage_to_Attack_the_Networkv4.doc
4			□	☆	Lab_13_Exploitation_with_IPv6v6.doc
5			□	☆	Lab_14_Creating_MSFPAYLOADSv9.doc
6			□	☆	Lab_15_Abusing_SYSTEMSv7.doc

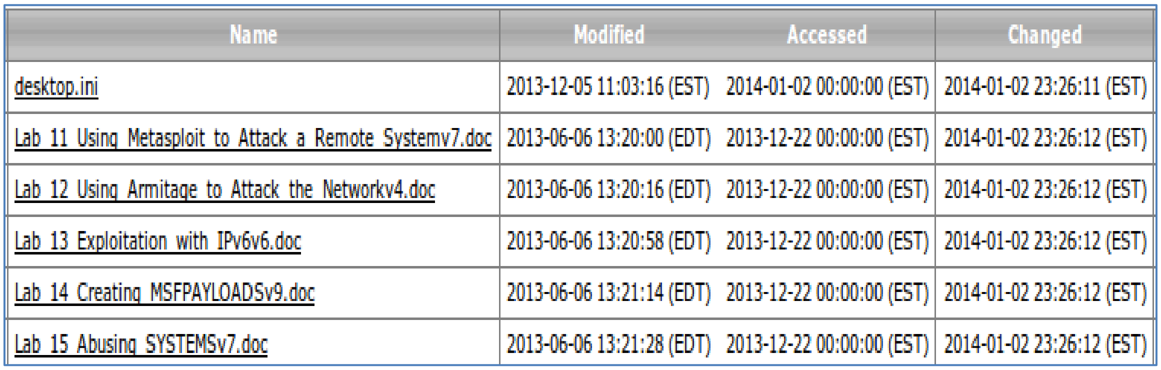
Lab_11_Using_Metasploit_to_Attack_a_Remote_Systemv7.doc

CDF V2 Document, corrupt: Can't read SAT

picture.php?partition_id=1&inode=7770-128-4&name=Lab_11_Using_M

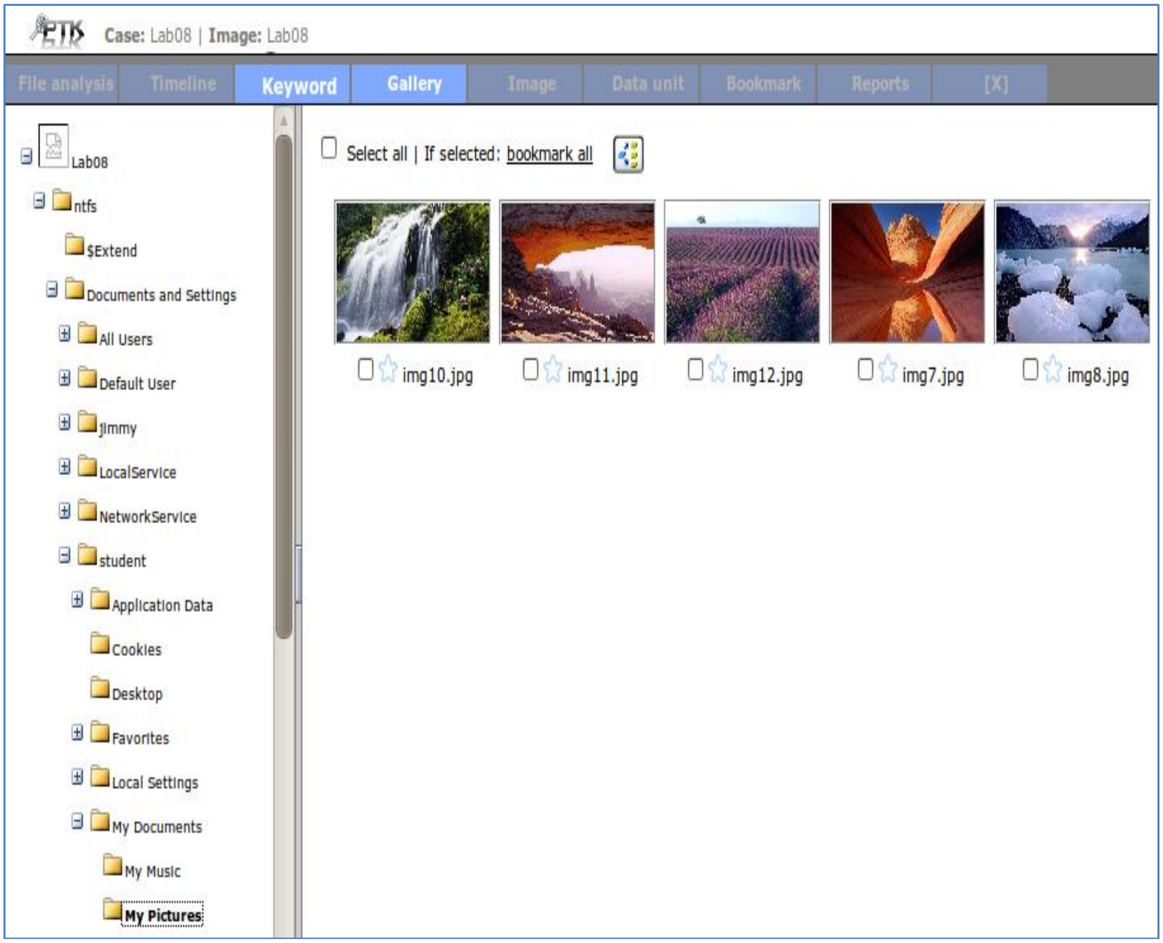
```
bjbjz
Certified Ethical Hacking Lab Series
Lab 11:  Using Metasploit to Attack a Remote System
Certified Ethical Hacking Domains:
System Hacking
Social Engineering
Session Hijacking
Document Version: 2012-12-26 (Beta)
```

9. View the date and time stamps that are displayed by PTK for the documents.

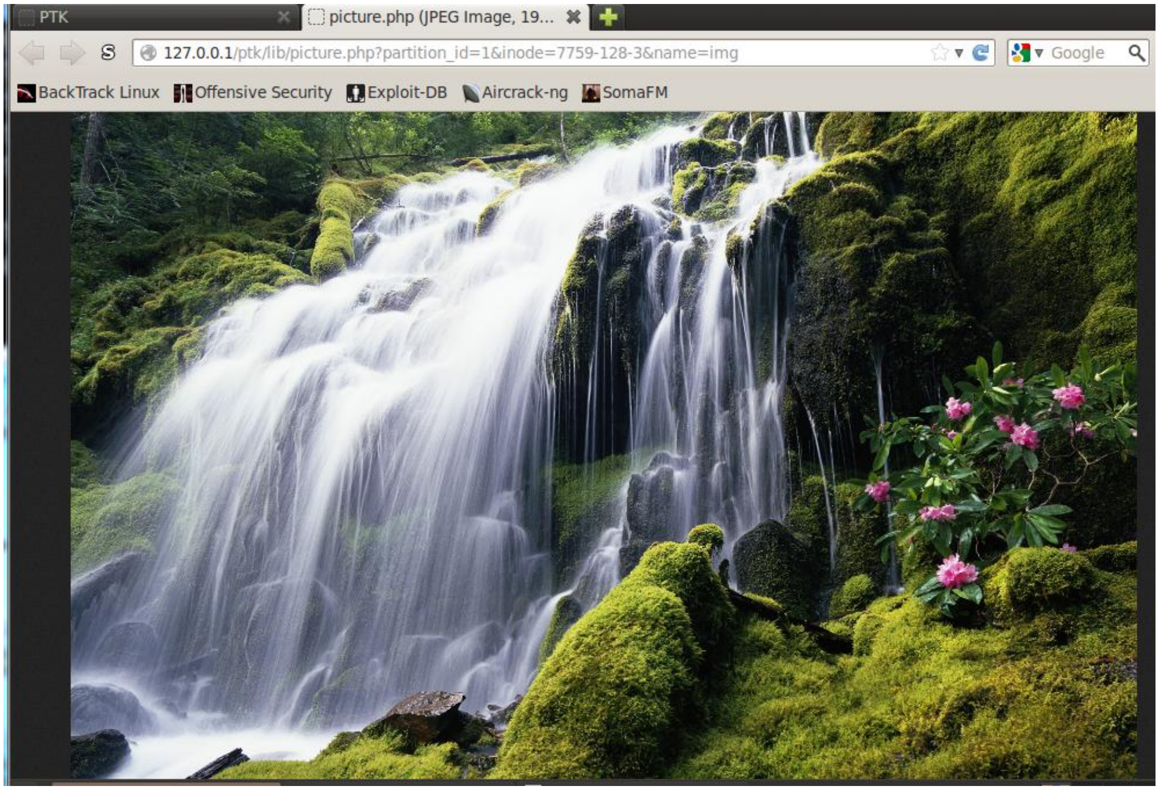


Name	Modified	Accessed	Changed
desktop.ini	2013-12-05 11:03:16 (EST)	2014-01-02 00:00:00 (EST)	2014-01-02 23:26:11 (EST)
Lab 11 Using Metasploit to Attack a Remote Systemv7.doc	2013-06-06 13:20:00 (EDT)	2013-12-22 00:00:00 (EST)	2014-01-02 23:26:12 (EST)
Lab 12 Using Armitage to Attack the Networkv4.doc	2013-06-06 13:20:16 (EDT)	2013-12-22 00:00:00 (EST)	2014-01-02 23:26:12 (EST)
Lab 13 Exploitation with IPv6v6.doc	2013-06-06 13:20:58 (EDT)	2013-12-22 00:00:00 (EST)	2014-01-02 23:26:12 (EST)
Lab 14 Creating MSFPAYLOADSv9.doc	2013-06-06 13:21:14 (EDT)	2013-12-22 00:00:00 (EST)	2014-01-02 23:26:12 (EST)
Lab 15 Abusing SYSTEMSv7.doc	2013-06-06 13:21:28 (EDT)	2013-12-22 00:00:00 (EST)	2014-01-02 23:26:12 (EST)

10. Click on the Gallery tab. Expand Lab08, NTFS, Documents and Settings, student, My Documents, and select My Pictures. View the pictures in the **Gallery**.



11. Click on one of the pictures in the Gallery to open it in full screen in a new tab.


PTK
picture.php (JPEG Image, 19...
127.0.0.1/ptk/lib/picture.php?partition_id=1&inode=7759-128-3&name=img
Google
BackTrack Linux
Offensive Security
Exploit-DB
Aircrack-ng
SomaFM

12. Close the newly opened tab with the picture when you are finished viewing it.

2.2 Conclusion

PTK gives you detailed information about an image file. It allows you to browse through files and folders, and view documents and picture files.

2.3 Discussion Questions

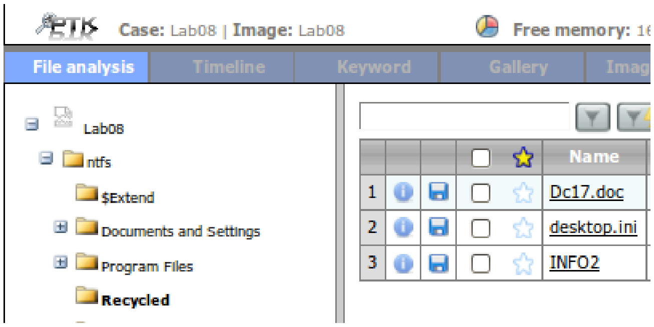
1. Where do you go within PTK to find out details about the image file?
2. What can be done if you want to examine text within a Word document in PTK?
3. What tab is used to view picture files?
4. What is the function of the $MFT?

3 Extracting Files

Forensic investigators often need to export files from an image to examine them for more detail or to perform additional analysis. With the correct application software, files that are exported from images can be opened by the investigator. Sometimes investigators need to be cautious because files extracted from images can be malicious. For that reason, their forensic workstation may not be connected to the Internet.

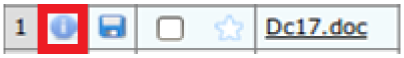
3.1 Extracting Files from PTK

1. Within the File Analysis Tab of PTK, expand Lab08, NTFS, and select the **Recycled** folder.

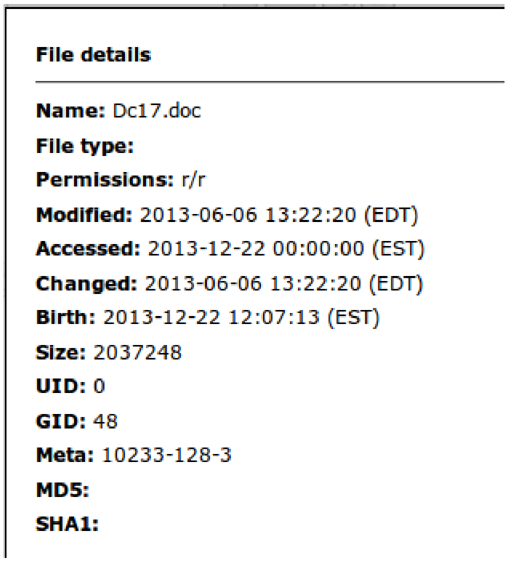


					Name
1			□		Dc17.doc
2			□		desktop.ini
3			□		INFO2

2. You will see 3 files listed on the right. Click the information (i) icon for the **DC17.doc** file.



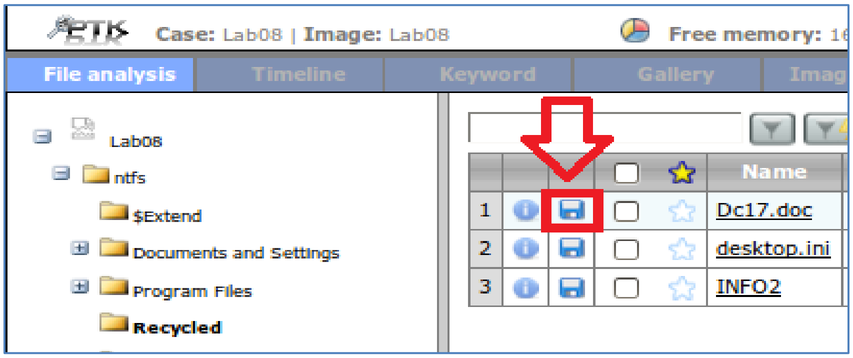
3. View the file details. Notice md5 and sha1 are not provided by default. Close the **File Details** window.



File details

Name: Dc17.doc
File type:
Permissions: r/r
Modified: 2013-06-06 13:22:20 (EDT)
Accessed: 2013-12-22 00:00:00 (EST)
Changed: 2013-06-06 13:22:20 (EDT)
Birth: 2013-12-22 12:07:13 (EST)
Size: 2037248
UID: 0
GID: 48
Meta: 10233-128-3
MD5:
SHA1:

4. Click the floppy drive icon for the **DC17.doc** file.

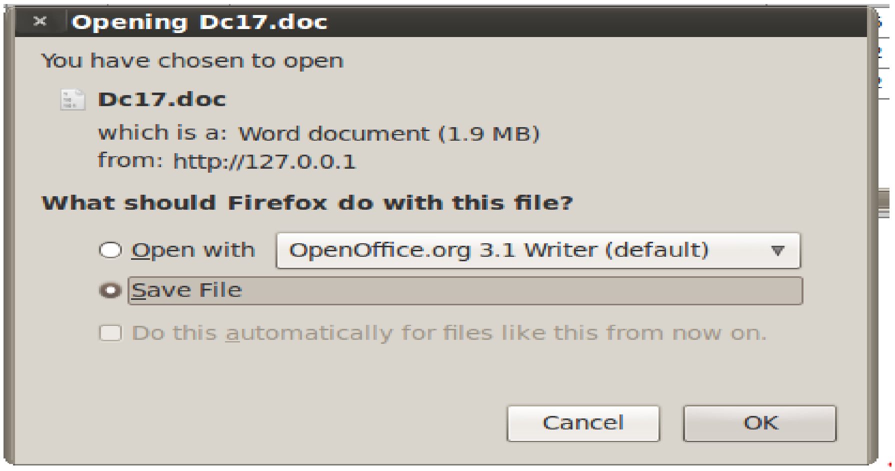


Case: Lab08 | Image: Lab08 Free memory: 1

- Lab08
  - ntfs
    - $Extend
    - Documents and Settings
    - Program Files
    - Recycled

			□	☆	Name
1			□	☆	Dc17.doc
2			□	☆	desktop.ini
3			□	☆	INFO2

5. Click the **Save File** button and click OK.



Opening Dc17.doc

You have chosen to open

Dc17.doc

which is a: Word document (1.9 MB)
from: http://127.0.0.1

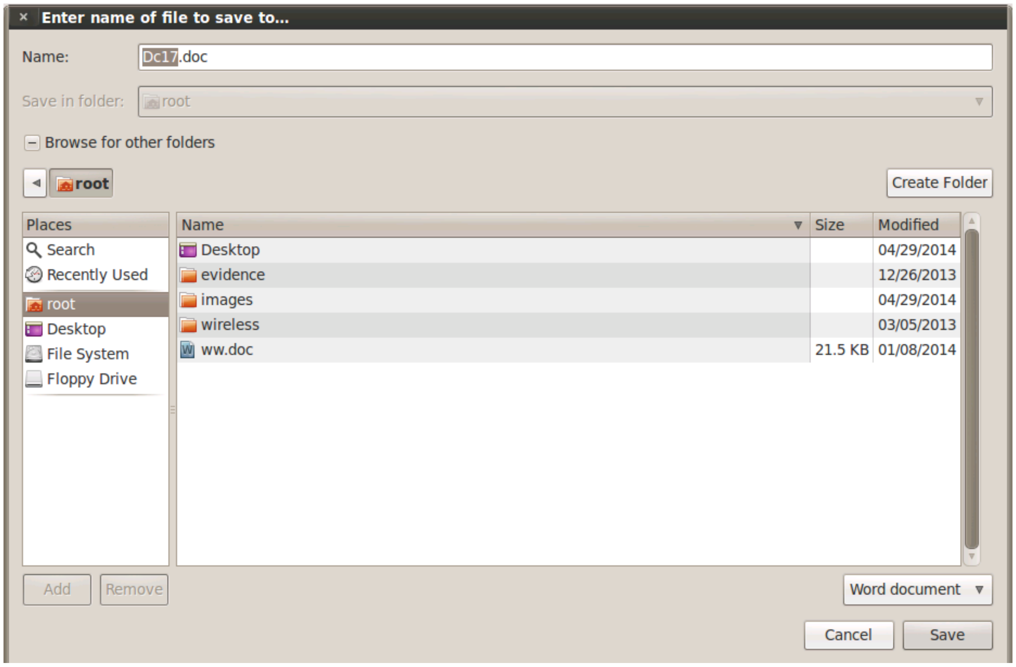
What should Firefox do with this file?

○ Open with OpenOffice.org 3.1 Writer (default)

● Save File

□ Do this automatically for files like this from now on.

6. Click **Save** to save the Dc17.doc file.



Enter name of file to save to...

Name: Dc17.doc

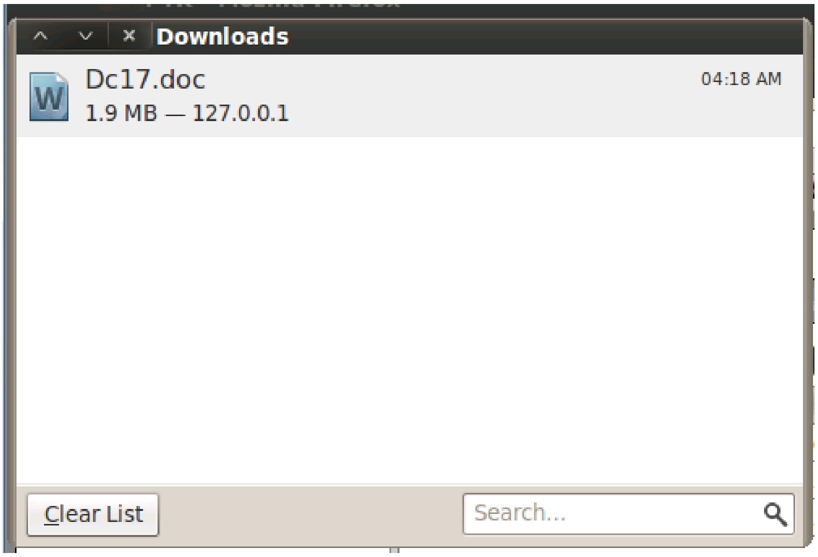
Save in folder: root

Browse for other folders

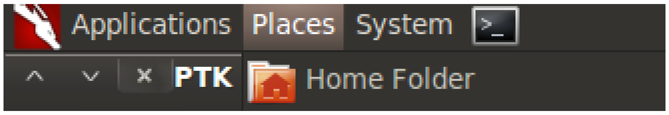
Places
Search
Recently Used
root
Desktop
File System
Floppy Drive

Name	Size	Modified
Desktop		04/29/2014
evidence		12/26/2013
images		04/29/2014
wireless		03/05/2013
ww.doc	21.5 KB	01/08/2014

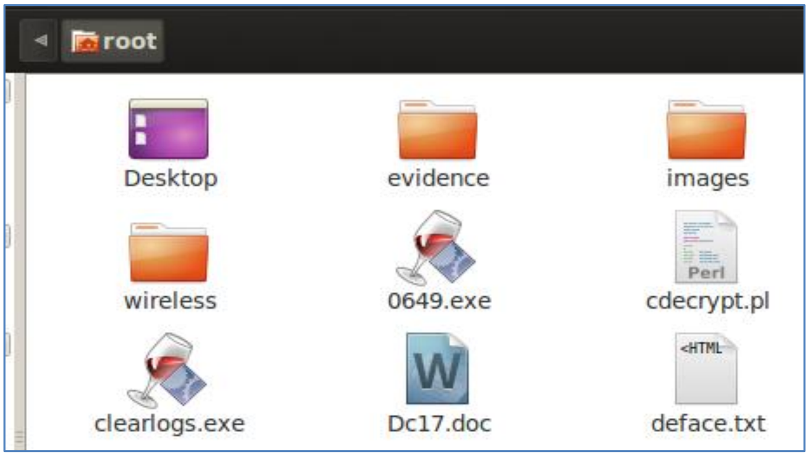
7. Close the Downloads window.



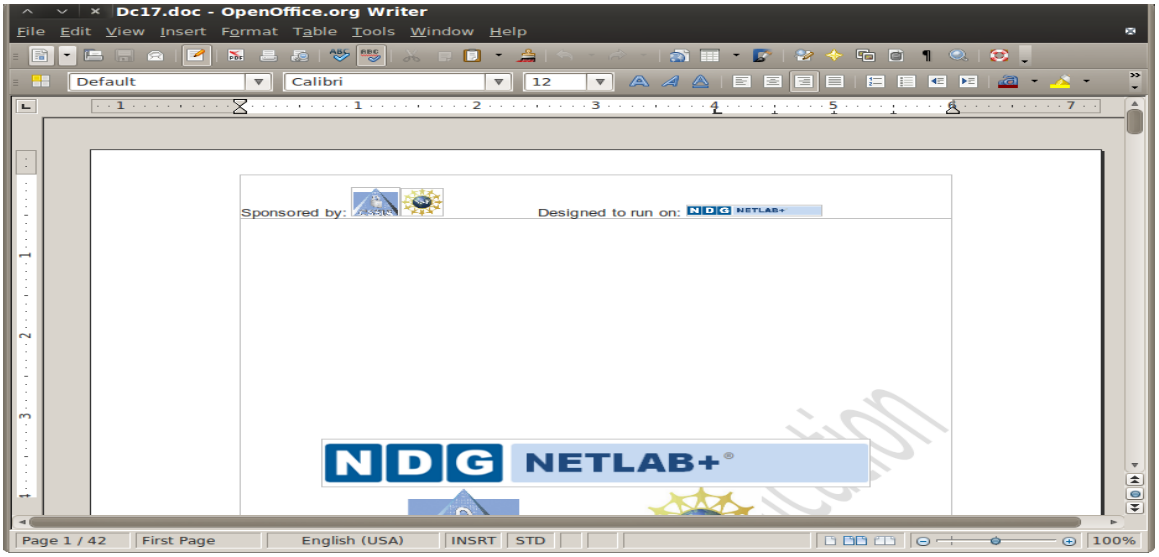
8. Click on Places and select the **Home folder**.



9. Double-click on **DC17.doc** file to open it with Open Office.

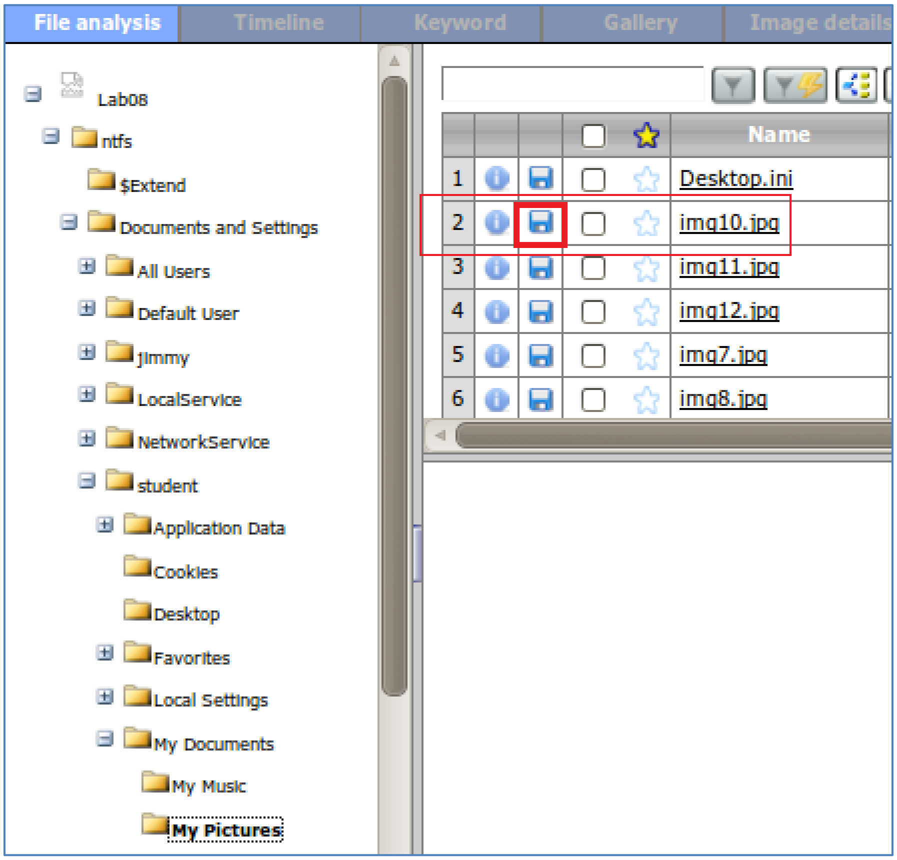


10. View the exported document file.



11. Close the document when you are finished viewing it and Open Office. Close root’s home folder.

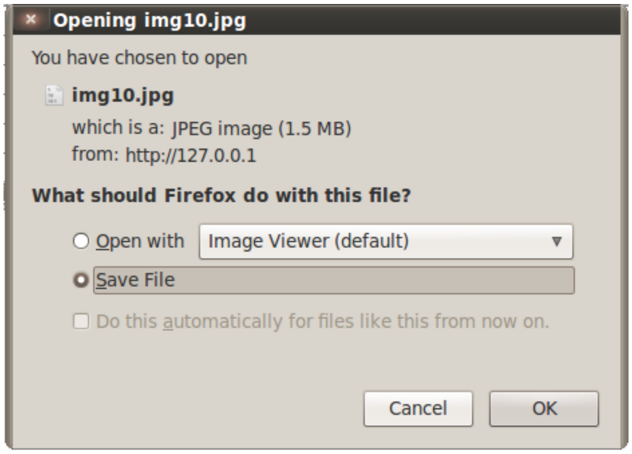
12. Under the File Analysis tab, expand NTFS, Documents and Settings, student, My Documents and select My Pictures. Click the floppy disk button for the **img10.jpg** file.



- Lab08
  - ntfs
    - $Extend
    - Documents and Settings
      - All Users
      - Default User
      - jimmy
      - LocalService
      - NetworkService
      - student
        - Application Data
        - Cookies
        - Desktop
        - Favorites
        - Local Settings
        - My Documents
          - My Music
          - My Pictures

			□	★	Name
1	ⓘ	💾	□	☆	Desktop.ini
2	ⓘ	💾	□	☆	img10.jpg
3	ⓘ	💾	□	☆	img11.jpg
4	ⓘ	💾	□	☆	img12.jpg
5	ⓘ	💾	□	☆	img7.jpg
6	ⓘ	💾	□	☆	img8.jpg

13. Click the **Save File** button and click **OK**.



Opening img10.jpg

You have chosen to open

img10.jpg

which is a: JPEG image (1.5 MB)

from: http://127.0.0.1

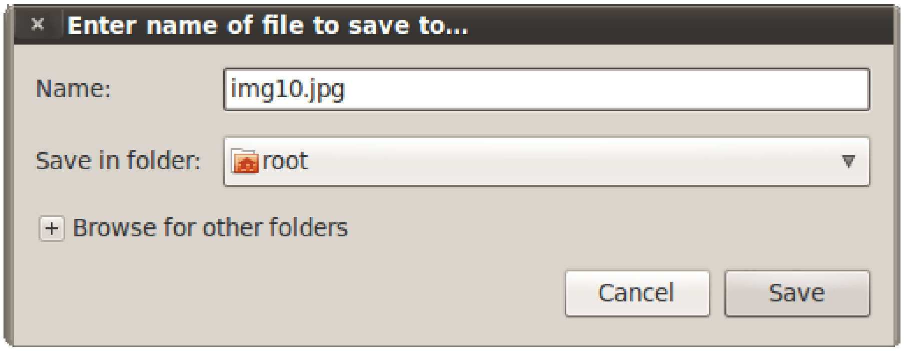
What should Firefox do with this file?

○ Open with Image Viewer (default)

● Save File

□ Do this automatically for files like this from now on.

14. Click **Save** to save the img10.jpg file.

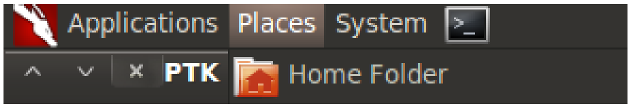


Enter name of file to save to...

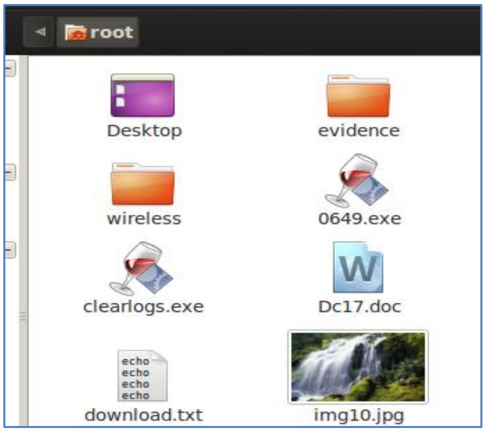
Name: img10.jpg

Save in folder: root

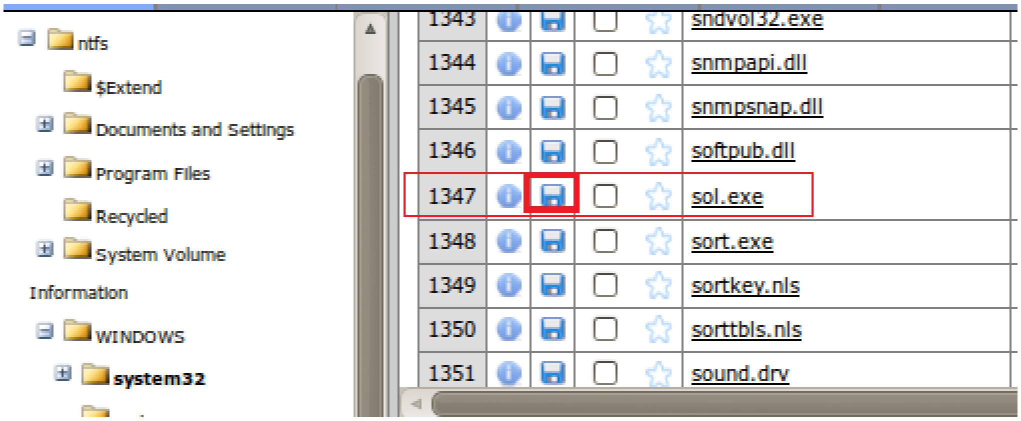
15. Close the Downloads window.
16. Click on Places and select the Home Folder.



17. View the exported JPG image file.



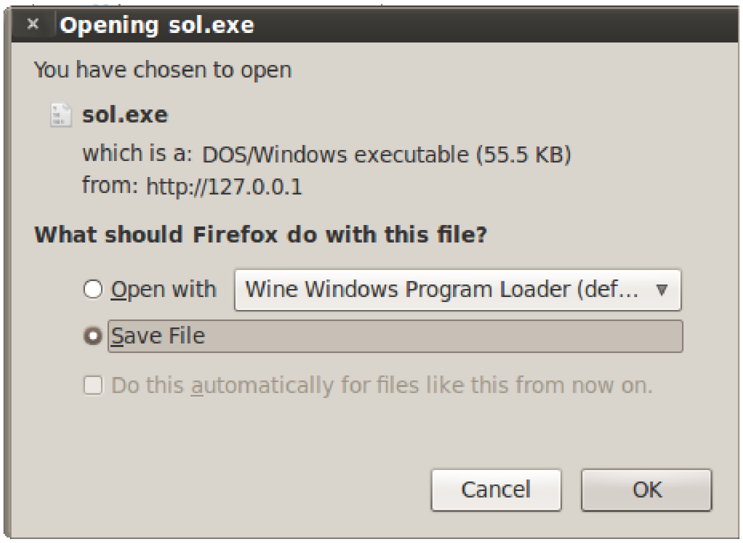
18. Close root's home folder when you are finished viewing the JPEG file.
19. Under the File Analysis Tab, expand NTFS, Windows, and select system32. In the long list of files, find **sol.exe**. Click the floppy disk button to the left of sol.exe.



- ntfs
  - $Extend
  - Documents and Settings
  - Program Files
  - Recycled
  - System Volume Information
  - WINDOWS
    - system32

1343	sndvol32.exe
1344	snmpapi.dll
1345	snmpsnap.dll
1346	softpub.dll
1347	sol.exe
1348	sort.exe
1349	sortkey.nls
1350	sorttbls.nls
1351	sound.drv

20. Click the **Save file** button and click **OK**.



Opening sol.exe

You have chosen to open

sol.exe

which is a: DOS/Windows executable (55.5 KB)
from: http://127.0.0.1

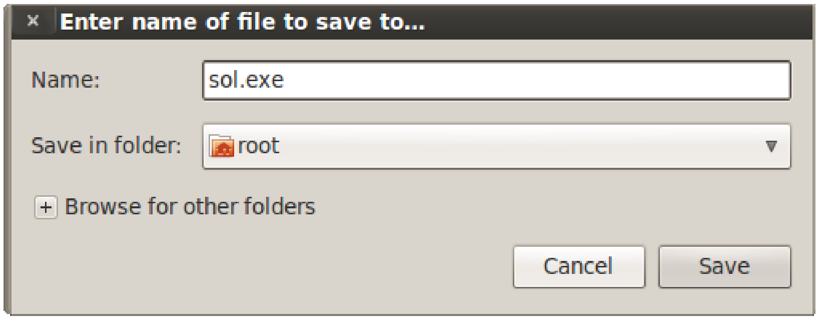
What should Firefox do with this file?

○ Open with Wine Windows Program Loader (def...

● Save File

□ Do this automatically for files like this from now on.

21. Click **Save** to save the sol.exe file.

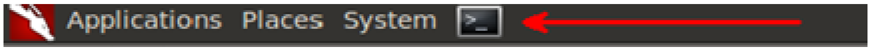


Enter name of file to save to...

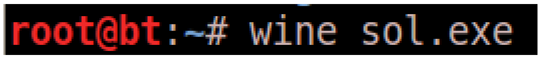
Name: sol.exe

Save in folder: root

22. Open a terminal on the Linux system by clicking on the picture to the right of the word **System** in the task bar in the top of the screen of the BackTrack 5 R3 Internal Machine.

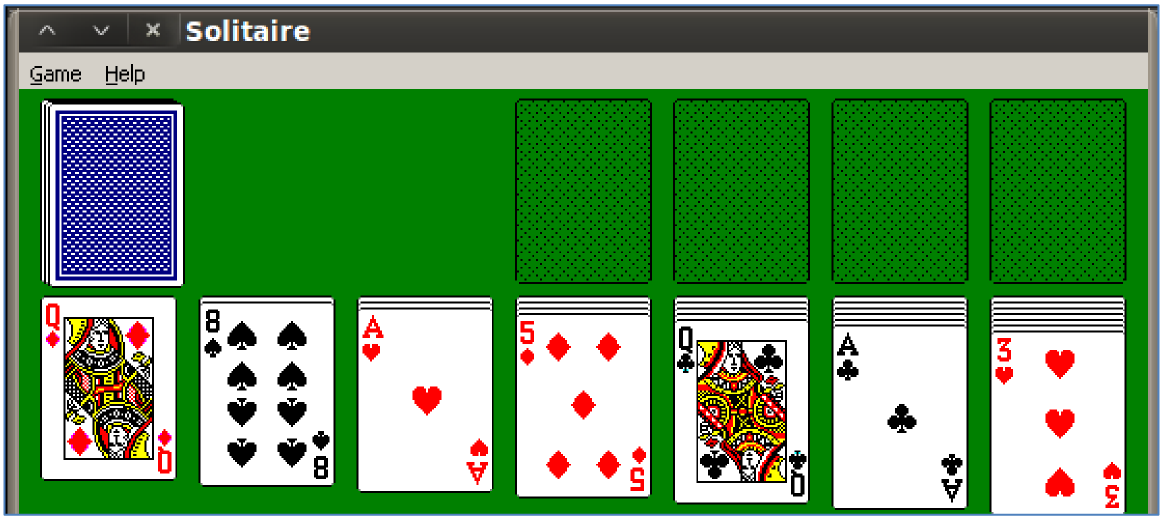


23. Type the following command to run the Windows solitaire program in Linux: root@bt:~# **wine sol.exe**



```
root@bt:~# wine sol.exe
```

24. Solitaire will eventually open. Close **solitaire**, close the **terminal** window and close the **download** window.



3.2 Conclusion

PTK is a forensic analysis tool that allows you to export files. Investigators may want to export files so they can be further examined or to determine a program's function.

3.3 Discussion Questions

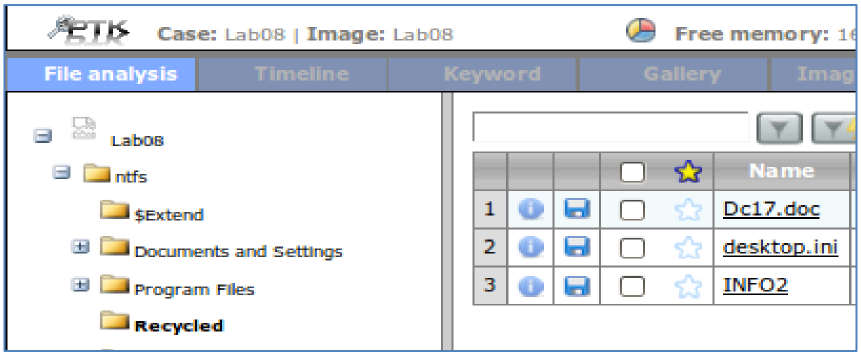
1. How do you export a file within PTK?
2. What program makes it possible to run a Windows program in Linux?
3. Why do you need to exercise caution when exporting files from an image?
4. Why might an investigator disconnect their workstation from the Internet?

4 Forensic Reporting with PTK

One of the most important tasks for an investigator is to produce a report of his/her findings. A built-in report generator in PTK reports on any tagged items.

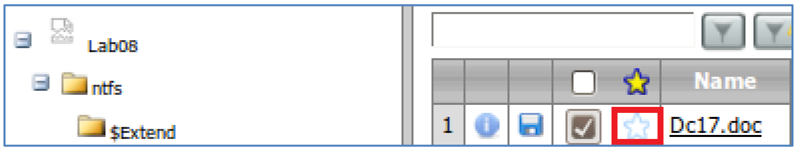
4.1 Generate a Forensic Report

1. Within the File Analysis tab of PTK, expand NTFS, and select the Recycled folder.



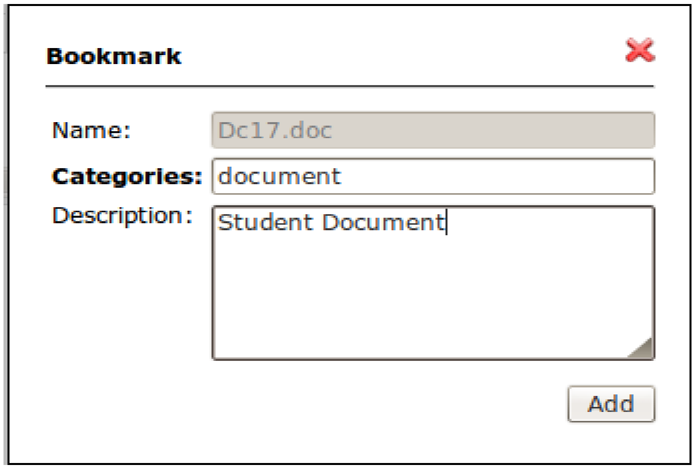
			□	☆	Name
1	ⓘ	💾	□	☆	Dc17.doc
2	ⓘ	💾	□	☆	desktop.ini
3	ⓘ	💾	□	☆	INFO2

2. You see 3 files on the right. Click the star icon to the left of DC17.doc.



			□	☆	Name
1	ⓘ	💾	☑	☆	Dc17.doc

3. For the category, put **document**. Enter **Student Document** for the Description. Click **Add**.

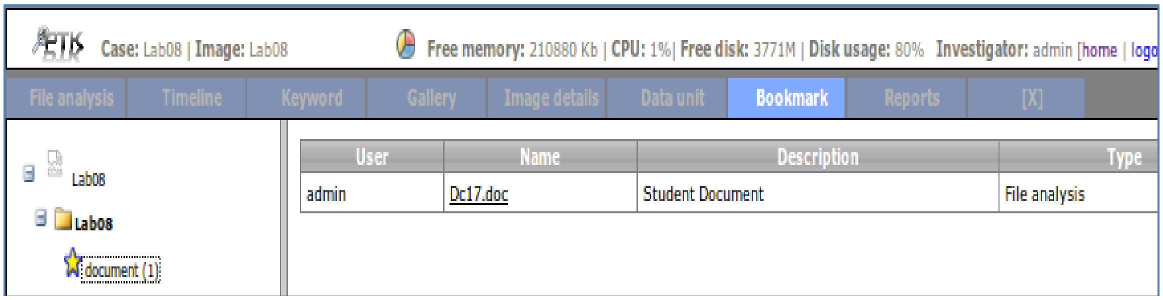


Name: Dc17.doc

Categories: document

Description: Student Document

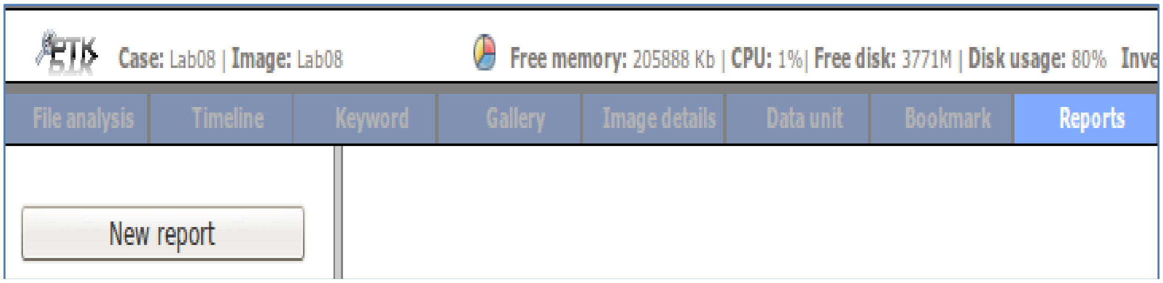
4. Click the Bookmark tab in PTK. Expand Lab08, Lab08, click on document (1) and you will see the document.



Case: Lab08 | Image: Lab08 Free memory: 210880 Kb | CPU: 1%| Free disk: 3771M | Disk usage: 80% Investigator: admin [home | logo

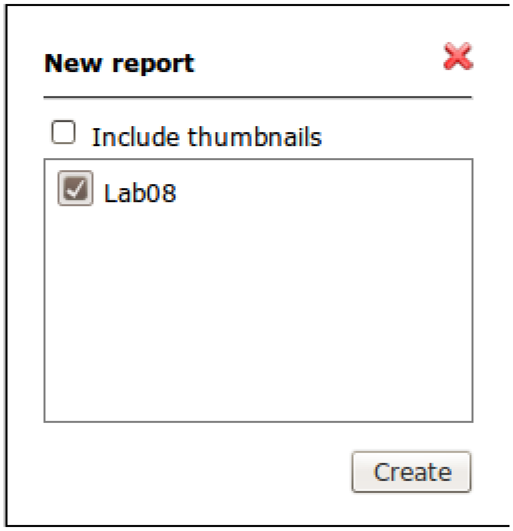
User	Name	Description	Type
admin	Dc17.doc	Student Document	File analysis

5. Click the Reports tab in PTK. Click the **New Report** button.



Case: Lab08 | Image: Lab08 Free memory: 205888 Kb | CPU: 1%| Free disk: 3771M | Disk usage: 80% Inve

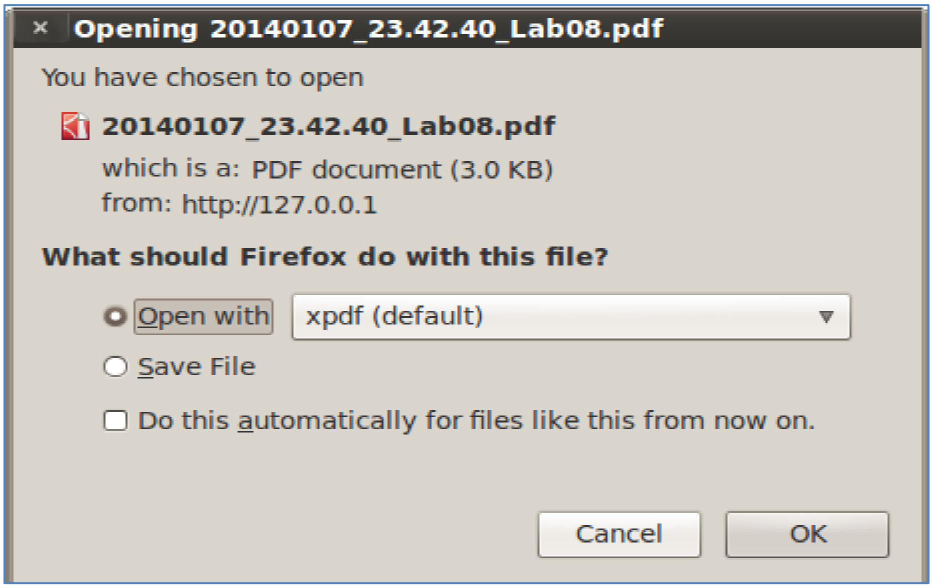
6. Click the box next to Lab08 and click **Create**. Click **Include thumbnails** if pictures are bookmarked.



□ Include thumbnails

☑ Lab08

7. Click **OK** to open the report with the PDF reader.



Opening 20140107_23.42.40_Lab08.pdf

You have chosen to open

20140107_23.42.40_Lab08.pdf

which is a: PDF document (3.0 KB)

from: http://127.0.0.1

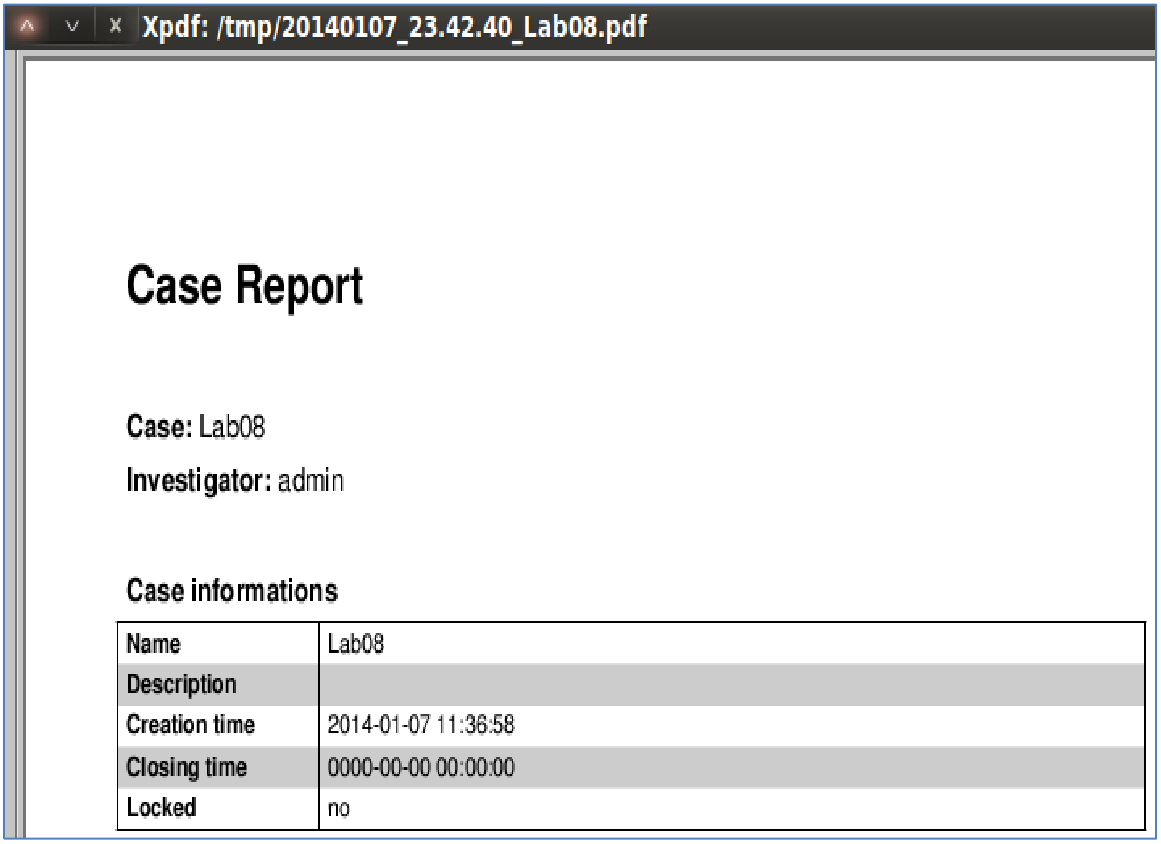
What should Firefox do with this file?

● Open with xpdf (default)

○ Save File

□ Do this automatically for files like this from now on.

8. View the first page of the generated Case Report.



Xpdf: /tmp/20140107_23.42.40_Lab08.pdf

Case Report

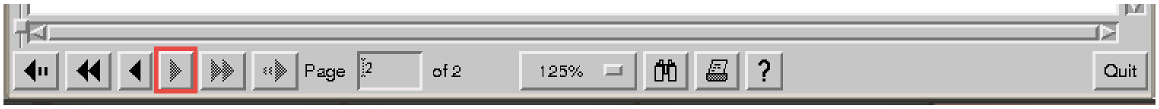
Case: Lab08

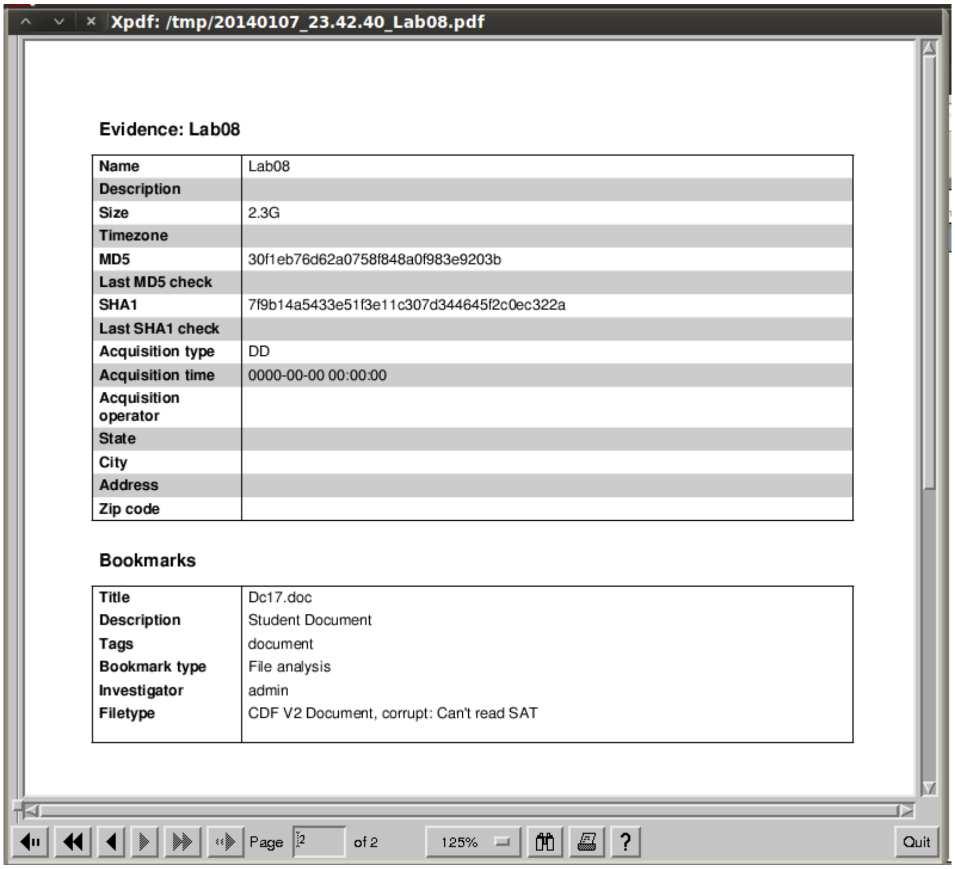
Investigator: admin

Case informations

Name	Lab08
Description	
Creation time	2014-01-07 11:36:58
Closing time	0000-00-00 00:00:00
Locked	no

9. Click the **Next** arrow to view the second page of the Case Report.





Evidence: Lab08

Name	Lab08
Description	
Size	2.3G
Timezone	
MD5	30f1eb76d62a0758f848a0f983e9203b
Last MD5 check	
SHA1	7f9b14a5433e51f3e11c307d344645f2c0ec322a
Last SHA1 check	
Acquisition type	DD
Acquisition time	0000-00-00 00:00:00
Acquisition operator	
State	
City	
Address	
Zip code	

Bookmarks

Title	Dc17.doc
Description	Student Document
Tags	document
Bookmark type	File analysis
Investigator	admin
Filetype	CDF V2 Document, corrupt: Can't read SAT

10. Close all open windows and the BackTrack 5 PC Viewer.

4.2 Conclusion

PTK has a reporting feature that will allow an investigator to bookmark items within a case. The report can be generated in a PDF format. Once the report is opened, you will get a summary of information within your case, including items that were bookmarked. Thumbnail images can be also added to the report.

4.3 Discussion Questions

1. In what format is a report generated in PTK?
2. Where do you navigate to within PTK to generate a report?
3. How do you bookmark an item?
4. Where do you navigate to within the PTK to view bookmarked items?

References

1. MD5 Hash:
   http://en.wikipedia.org/wiki/MD5

2. SHA1 Hash:
   http://en.wikipedia.org/wiki/SHA-1

3. How to Write a Forensic Report:
   http://www.ehow.com/how_5858380_write-forensic-report.html

4. Forensic Reporting:
   http://www.eteraconsulting.com/12/07/forensic-reporting-how-it-works-and-why-it-important