DIGITAL FORENSICS LAB SERIES

Lab 9: Analyzing a FAT Partition with Autopsy

Objective: File and Program Activity Analysis

Document Version: 2015-09-28

This work by the National Information Security and Geospatial Technologies Consortium (NISGTC), and except where otherwise noted, is licensed under the Creative Commons Attribution 3.0 Unported License.

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 3
Objective: File and Program Activity Analysis 3
Lab Topology 5
Lab Settings 6
1 Examining the FAT and NTFS File Systems 7
1.1 Viewing File Systems 7
1.2 Conclusion 14
1.3 Discussion Questions 14
2 Using a HEX Editor to Explore a FAT Partition 15
2.1 Explore a FAT Partition 15
2.2 Conclusion 19
2.3 Discussion Questions 19
3 Verifying and Viewing Image Details 20
3.1 Verifying Integrity 20
3.2 Conclusion 23
3.3 Discussion Questions 23
4 Analyzing a FAT Partition with Autopsy 24
4.1 Loading the FAT Image into Autopsy 24
4.2 Conclusion 32
4.3 Discussion Questions 32
References 33

This work by the National Information Security and Geospatial Technologies Consortium (NISGTC), and except where otherwise noted, is licensed under the Creative Commons Attribution 3.0 Unported License.

Introduction

This lab includes the following tasks:

1. Examining the FAT and NTFS File Systems
2. Using a HEX Editor to Explore a FAT Partition
3. Verifying and Viewing Image Details
4. Analyzing a FAT Partition with Autopsy

Objective: File and Program Activity Analysis

Performing this lab will provide the student with a hands-on lab experience meeting the File and Program Activity Analysis Objective:

The candidate will demonstrate an understanding of how the Windows registry, file metadata, memory, and filesystem artifacts can be used to trace user activities on suspect systems.

Understanding File Systems is key to understanding Computer Forensics investigations. File Systems store data in different ways. The FAT file system is commonly used, even in modern times, for devices like external USB drives, as well as Secure Digital (SD) cards.

Autopsy - The open source digital investigation tool (digital forensic tool), Autopsy, runs on Windows, Linux, OS X, and other UNIX systems. Autopsy can be used to analyze disk images and perform in-depth analysis of file systems, such as NTFS and FAT.

FAT – The acronym FAT stands for File Allocation Table. The FAT table holds information about where files are stored on a volume. When a file is deleted from the disk, the entry or entries for those files are removed from the table and the space is marked as available. However, the file, or parts of the file, will remain on the disk until overwritten by information from new files.

FAT12 – The FAT12 file system is typically used on floppy disks. A FAT12 partition is limited to 32 megabytes. The use of this file system is uncommon in modern times. However, FAT12 partitions can be read with modern operating systems like Windows 8.

FAT16 – A FAT16 partition can be up to 2 gigabytes. The FAT16 file system was used primarily with MS-DOS, Windows 3.11, Windows 95a and Windows NT. None of those operating systems can read the FAT32 file system without 3rd party drivers. Although FAT16 partitions can be read with modern operating systems like Windows 8 (as well as Linux and Mac OS X), its use is in decline because of the 2-gigabyte limitation.
FAT32 – A FAT32 partition can be up to 2 terabytes. (There are workarounds to make larger FAT32 partitions.) It is also important to know that a FAT32 volume cannot hold a file that is larger than 4 gigabytes. This limitation makes FAT32 less practical than NTFS.

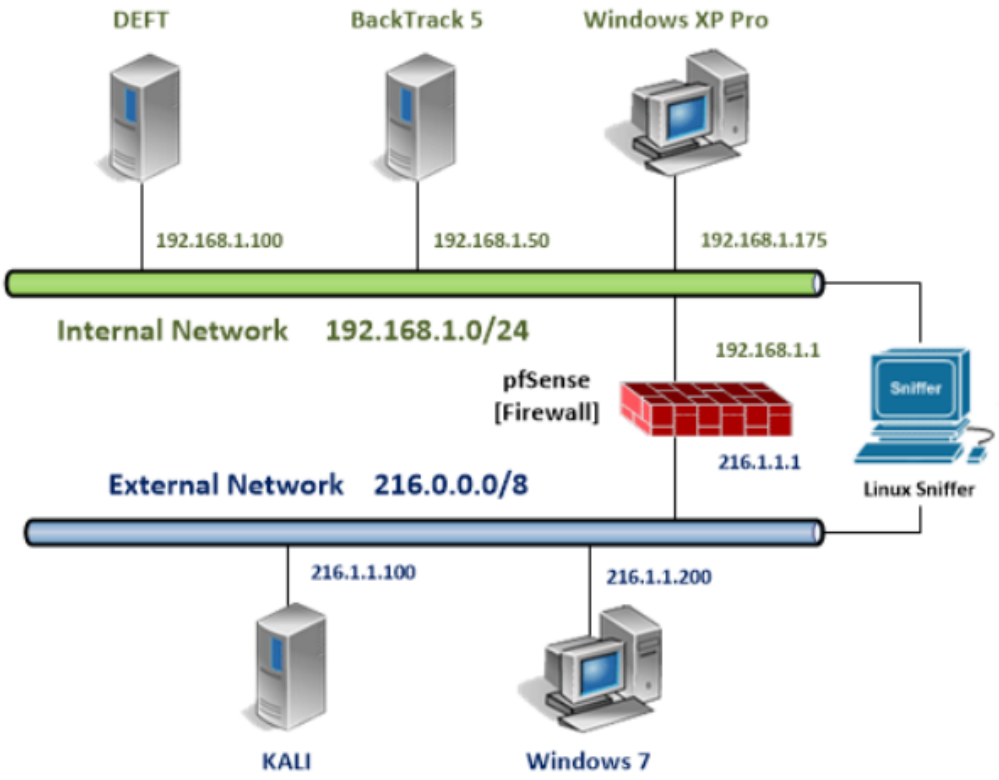
This work by the National Information Security and Geospatial Technologies Consortium (NISGTC), and except where otherwise noted, is licensed under the Creative Commons Attribution 3.0 Unported License.

NTFS – The New Technology File System (NTFS) was originally introduced with the Windows NT. NTFS is a journaling file system, which means it keeps a log of changes being written to the disk. If a computer is shutdown improperly, it will have a better chance of recovery if it has a journaling file system. Files and folder access can be restricted with the security feature of NTFS. Starting with Windows 2000, Microsoft included the Encrypted File System, or EFS, as an NTFS feature. EFS allows users to encrypt files to protect against unauthorized access.

Wipe – A wipe will erase all of the 0's and 1's written to the hard disk. If a wipe is done correctly, all data will be erased and recovery of artifacts will be near impossible.

This work by the National Information Security and Geospatial Technologies Consortium (NISGTC), and except where otherwise noted, is licensed under the Creative Commons Attribution 3.0 Unported License.

Lab Topology



This work by the National Information Security and Geospatial Technologies Consortium (NISGTC), and except where otherwise noted, is licensed under the Creative Commons Attribution 3.0 Unported License.

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)
Windows 7 External Machine	216.1.1.200	student	password
Kali Linux External Machine	216.1.1.100	root	toor

This work by the National Information Security and Geospatial Technologies Consortium (NISGTC), and except where otherwise noted, is licensed under the Creative Commons Attribution 3.0 Unported License.

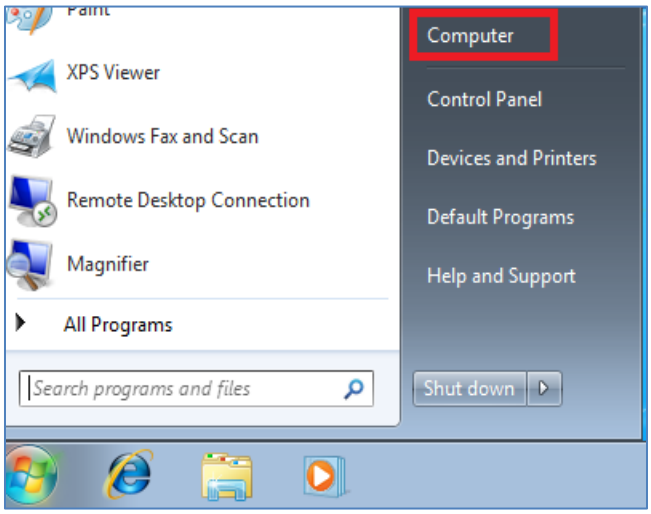
1 Examining the FAT and NTFS File Systems

File Systems store data on a disk. The most common Windows file systems are FAT and NTFS. There are several versions of FAT, including FAT12, FAT16, FAT32, exFAT, and FATx (XBOX). Some of the most common Linux file systems include EXT2, EXT3, EXT4 and ReiserFS. Mac OS X uses the HFS+ File system; older Macs use the HFS file system.

1.1 Viewing File Systems

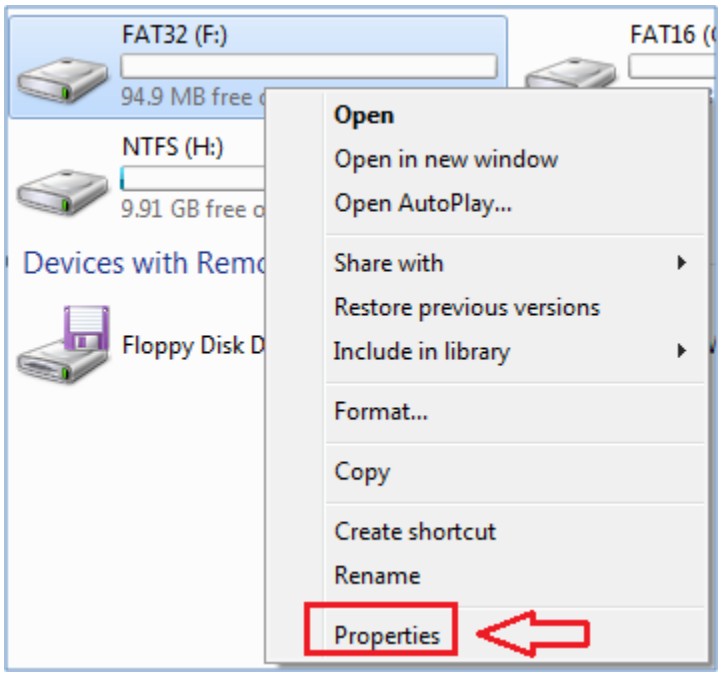
1. Login to the **Windows 7 External Machine** by clicking on the **Windows 7** icon on the topology.
2. If required, enter the username, **student**.
3. Type in the password, **password,** and press **Enter** to log in.

4. Click the Start icon in the lower-left corner and then select **Computer.**

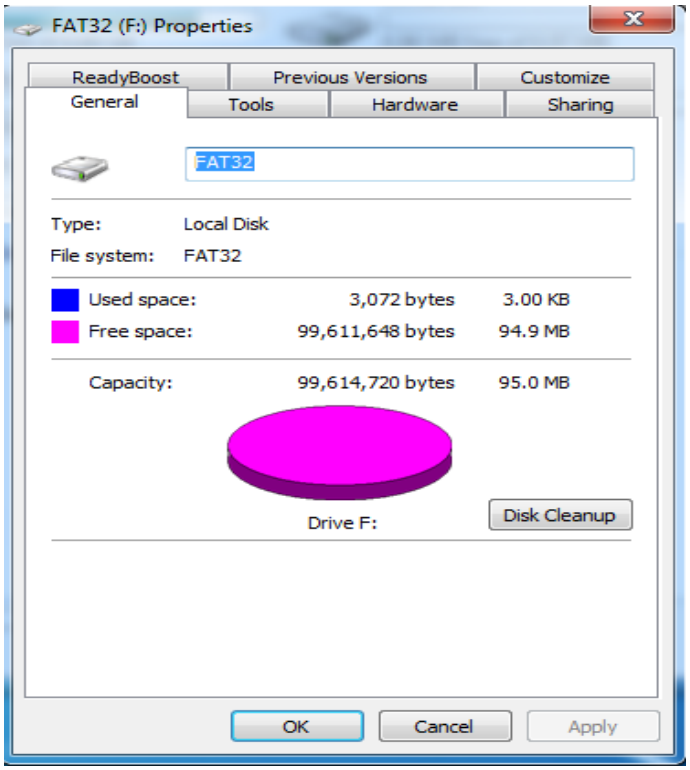


This work by the National Information Security and Geospatial Technologies Consortium (NISGTC), and except where otherwise noted, is licensed under the Creative Commons Attribution 3.0 Unported License.

5. Right-click on the FAT 32 Drive (F:) and go to the **Properties** tab.

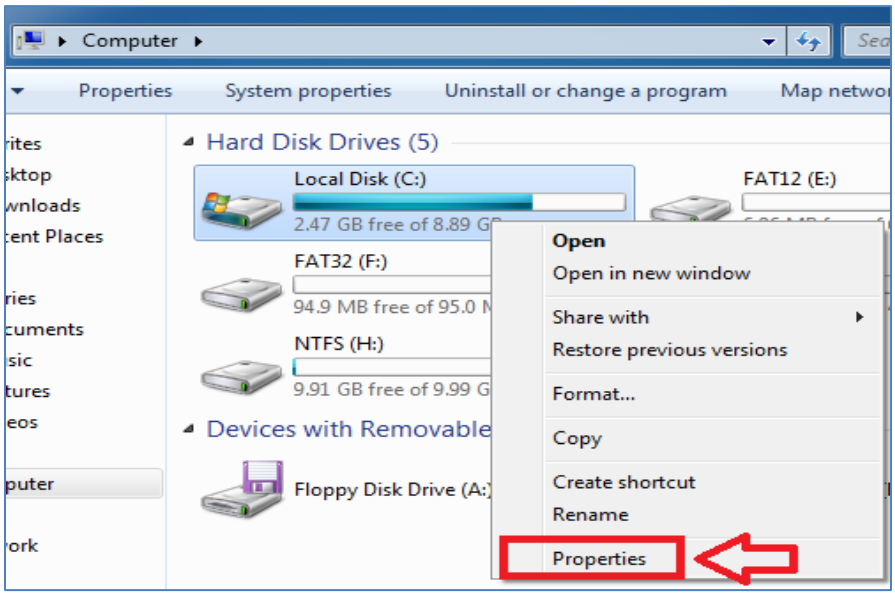


6. Notice that there is no Security or Quota tab on a FAT32 Volume. Close the FAT32 (F:) Properties window.

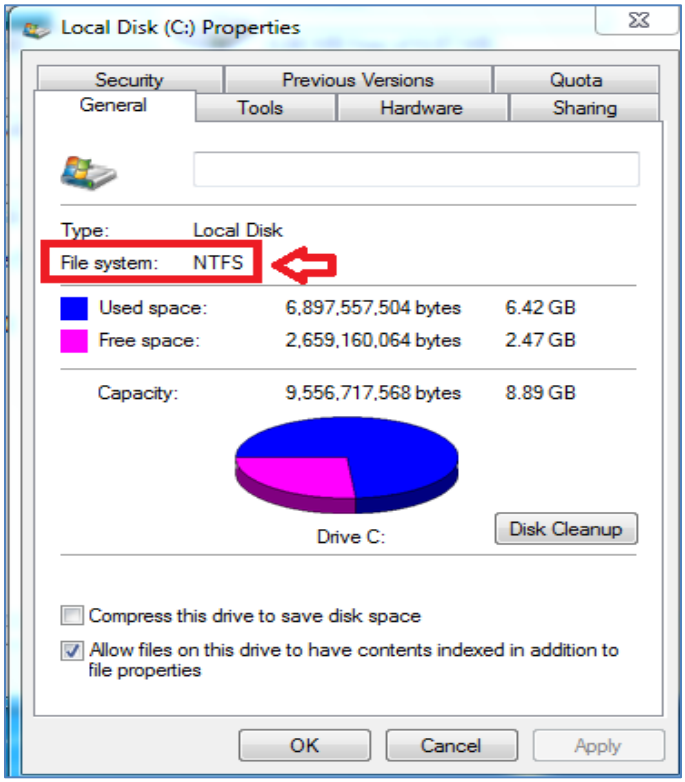


This work by the National Information Security and Geospatial Technologies Consortium (NISGTC), and except where otherwise noted, is licensed under the Creative Commons Attribution 3.0 Unported License.

7. Right-click on Local Disk (C:) and go to the **Properties** tab.



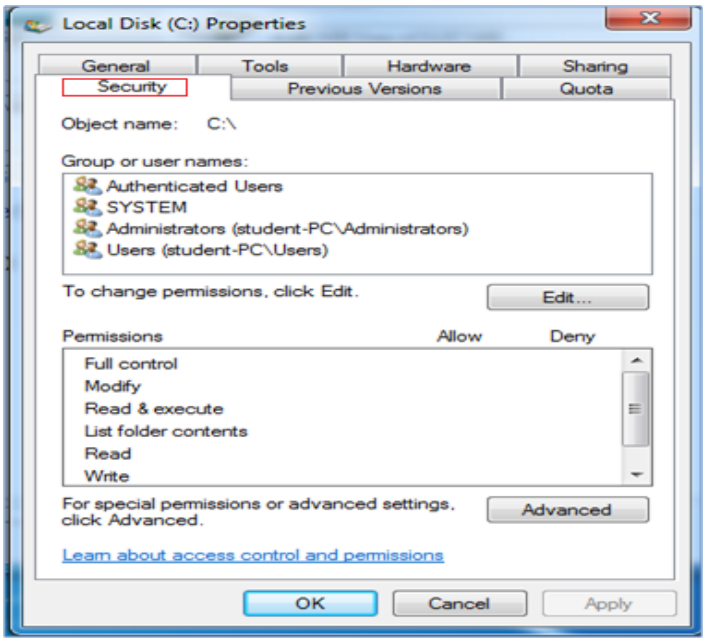
8. View the file system type, which should be listed as NTFS.



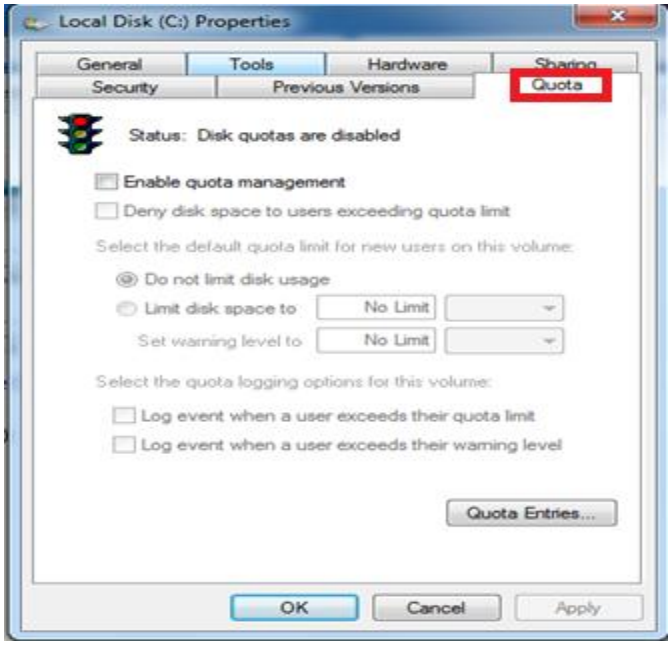
On NTFS volumes, security permissions and quotas can be configured. Security permissions can be configured to restrict access to files or folders. Quotas are used to restrict the amount of storage for each user to prevent a disk from running out of space.

This work by the National Information Security and Geospatial Technologies Consortium (NISGTC), and except where otherwise noted, is licensed under the Creative Commons Attribution 3.0 Unported License.

9. Click on the Security tab. This is where Access Control Lists can be configured.



10. Click on the **Quota** tab. This is where disk usage can be restricted for users.

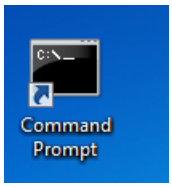


11. Close Local Disk (C:) Properties and Computer windows

There are many limitations to using FAT32. One is the fact that file sizes are limited to 4 GB. The other issue is that you cannot create a FAT32 volume larger than 32 GB in some versions of Windows, such as XP, Windows 7 and Windows 8. However, on a strange note, in Windows 98 or Windows ME, users can create a 127.53 GB FAT32 volume. The likely reason for this is that Windows 98 or Windows ME cannot read NTFS.

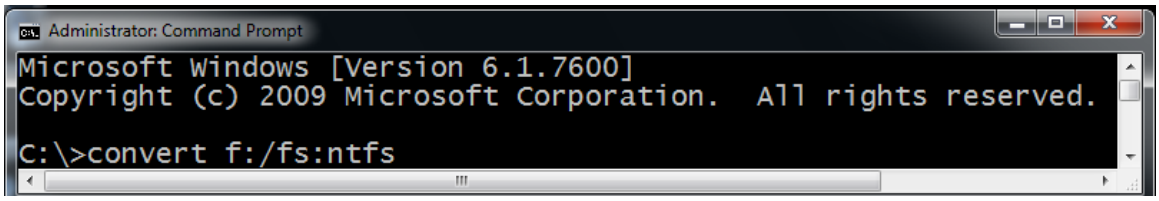
This work by the National Information Security and Geospatial Technologies Consortium (NISGTC), and except where otherwise noted, is licensed under the Creative Commons Attribution 3.0 Unported License.

12. Double-click on the shortcut to the Command Prompt on the desktop.

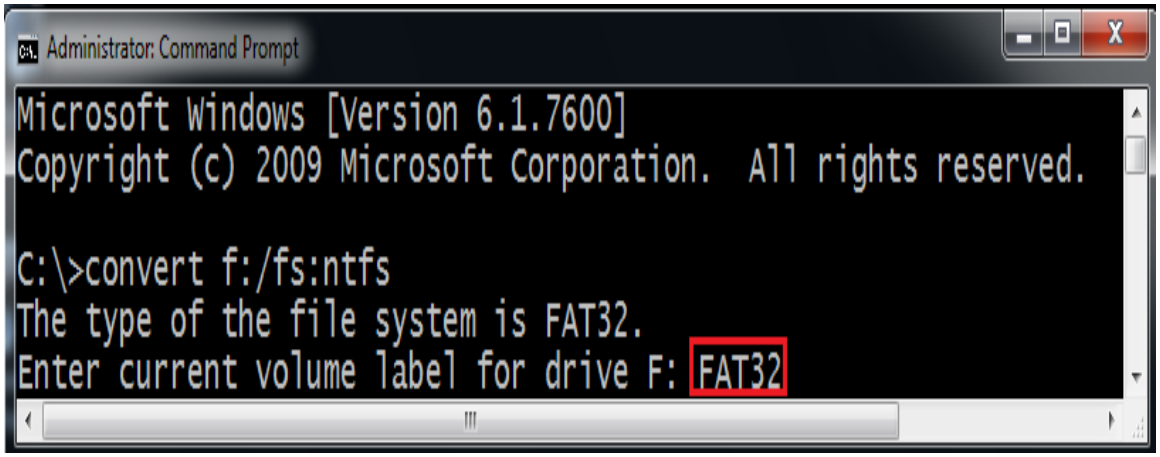


We can use the convert command to convert the FAT32 volume to a NTFS partition.

13. Type the following command to convert the FAT32 volume to NTFS:
    C:\>**convert f:/fs:ntfs**



14. When you are asked to Enter current volume label for drive F:, type **FAT32**.

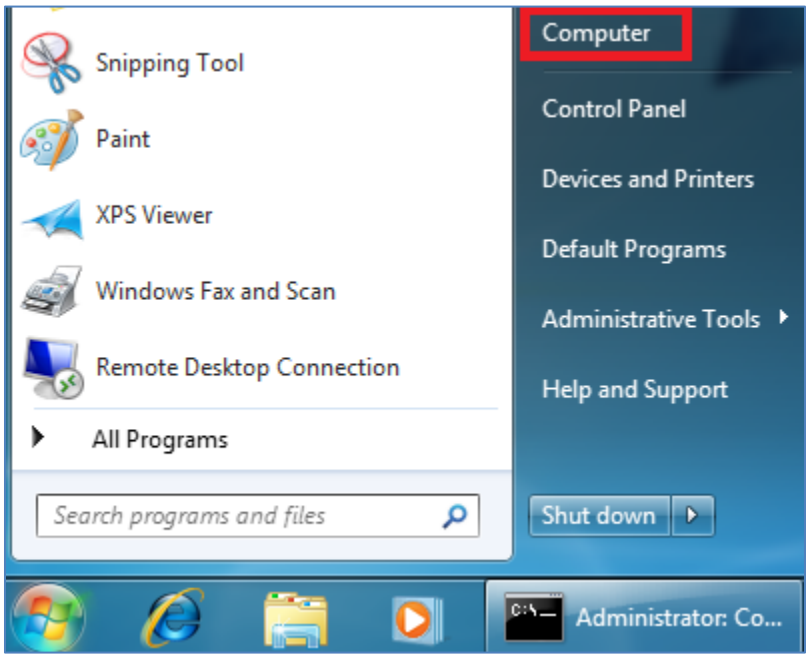


This work by the National Information Security and Geospatial Technologies Consortium (NISGTC), and except where otherwise noted, is licensed under the Creative Commons Attribution 3.0 Unported License.

15. You will receive a message from Windows 7 that the conversion is complete.

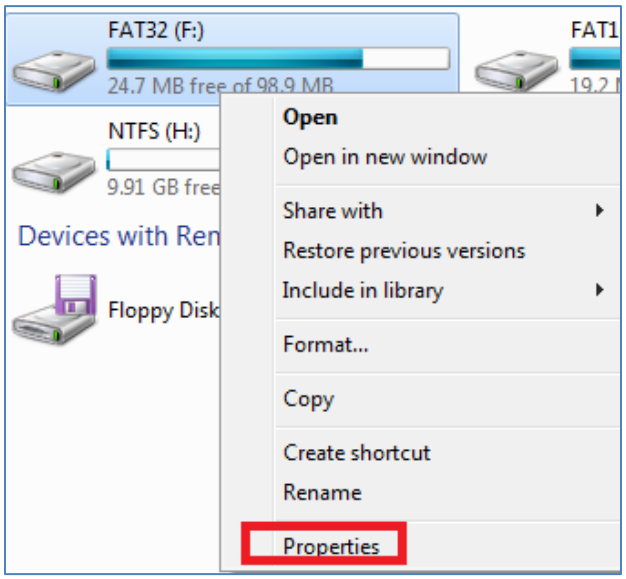
```
Microsoft Windows [Version 6.1.7600]
Copyright (c) 2009 Microsoft Corporation.  All rights reserved.

C:\>convert f:/fs:ntfs
The type of the file system is FAT32.
Enter current volume label for drive F: FAT32
Volume FAT32 created 7/12/2013 3:51 PM
Volume Serial Number is A675-6F6A
Windows is verifying files and folders...
File and folder verification is complete.
Windows has checked the file system and found no problems.

   99,614,720 bytes total disk space.
        2,048 bytes in 2 hidden files.
   63,617,024 bytes in 19 files.
   35,992,576 bytes available on disk.

        1,024 bytes in each allocation unit.
       97,280 total allocation units on disk.
       35,149 allocation units available on disk.

Determining disk space required for file system conversion...
Total disk space:                101376 KB
Free space on volume:             35149 KB
Space required for conversion:     2379 KB
Converting file system
Conversion complete
```

16. Click the Start icon in the lower-left corner and then select **Computer.**

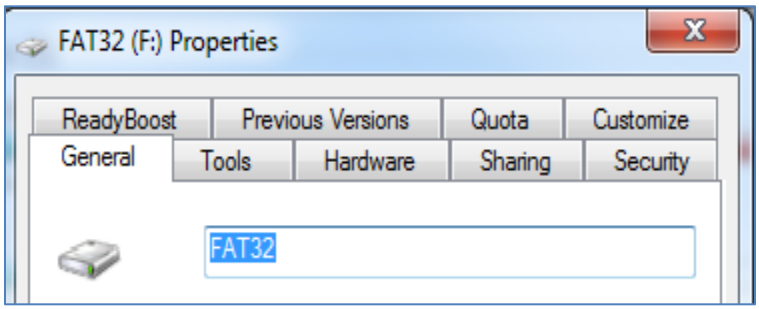


This work by the National Information Security and Geospatial Technologies Consortium (NISGTC), and except where otherwise noted, is licensed under the Creative Commons Attribution 3.0 Unported License.

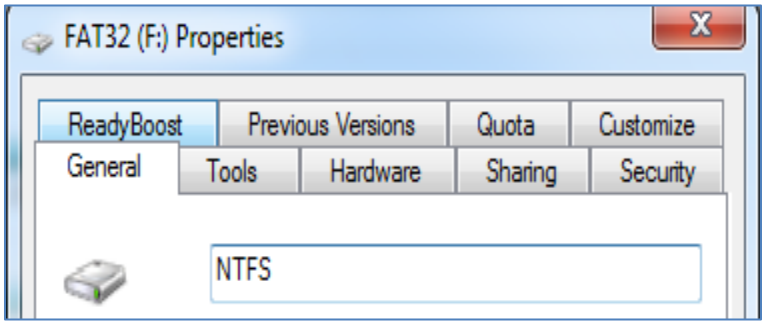
17. Right-click on the (F:) drive (labeled FAT 32) and go to the **Properties** tab.



18. Erase the current volume label of **FAT32.**

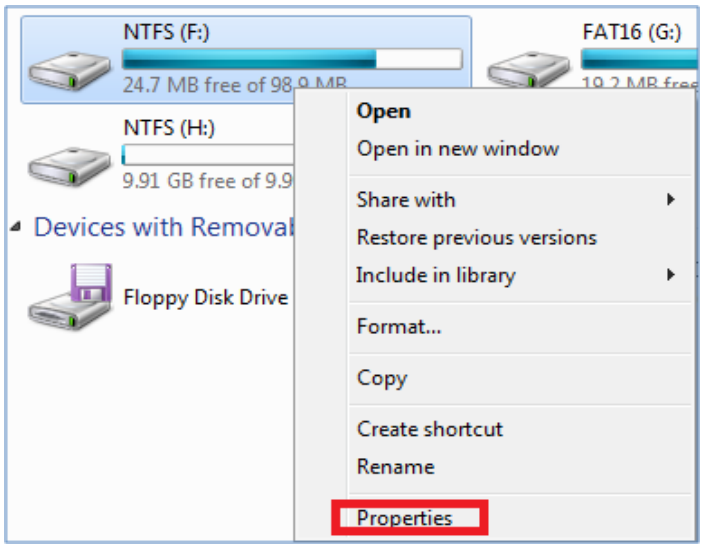


19. Change the Volume label to **NTFS** and then click on the OK button.

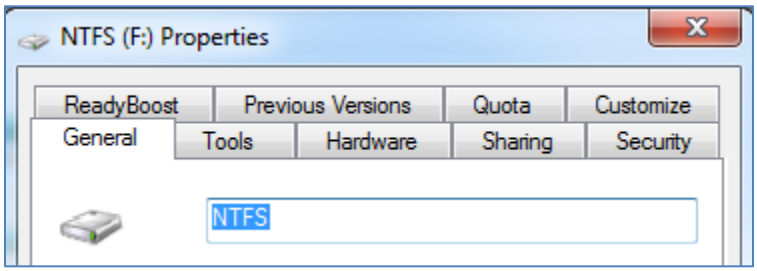


This work by the National Information Security and Geospatial Technologies Consortium (NISGTC), and except where otherwise noted, is licensed under the Creative Commons Attribution 3.0 Unported License.

20. Right-click on the NTFS (F:) Drive and navigate to **Properties**.



21. The Security and Quota tabs are now present because the volume is NTFS.



22. Close NTFS (F:) Properties, Computer and Command Prompt windows

1.2 Conclusion

There is a wide variety of file systems used on operating systems. File systems that are common to Microsoft operating systems include FAT (File Allocation Table) and NTFS (New Technology File System). There are several versions of FAT, including FAT12, FAT16, FAT32, exFAT, and FATx. The NTFS File System offers security while the FAT file system is known for its compatibility with many operating systems.

1.3 Discussion Questions

1. What is the largest FAT32 volume that can be formatted in Windows 8?
2. What is the largest FAT32 volume that can be formatted in Windows 98?
3. What are some of the different versions of the FAT file system?
4. Which version of the FAT file system are you least likely to come across today?

This work by the National Information Security and Geospatial Technologies Consortium (NISGTC), and except where otherwise noted, is licensed under the Creative Commons Attribution 3.0 Unported License.

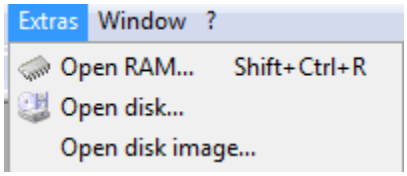
2 Using a HEX Editor to Explore a FAT Partition

The FAT (File Allocation Table) file system is a legacy file system designed in the late 70's for use with floppy disks. The FAT file system was adapted on hard disks and used extensively during the heyday of the DOS and Windows 9X operating systems. Today you can still find FAT file systems used on solid-state and flash memory cards.

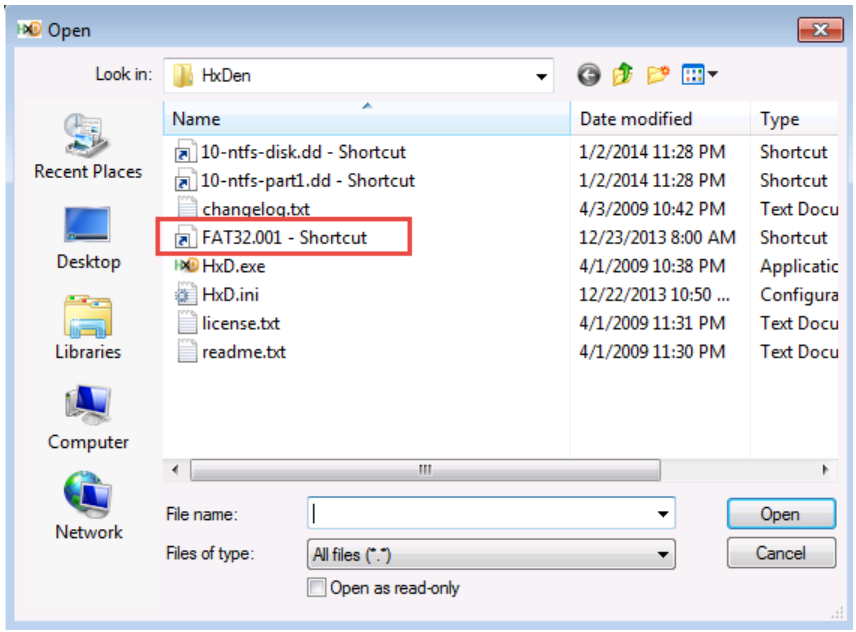
2.1 Explore a FAT Partition

1. Double click on the HxD icon on the desktop.

2. Click **Extras > Open disk image**.

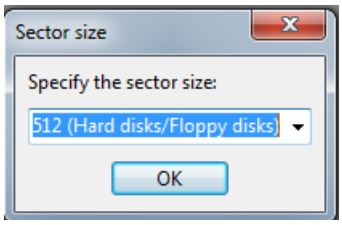


3. Click on the **fat32.001 - Shortcut** and click **Open**.

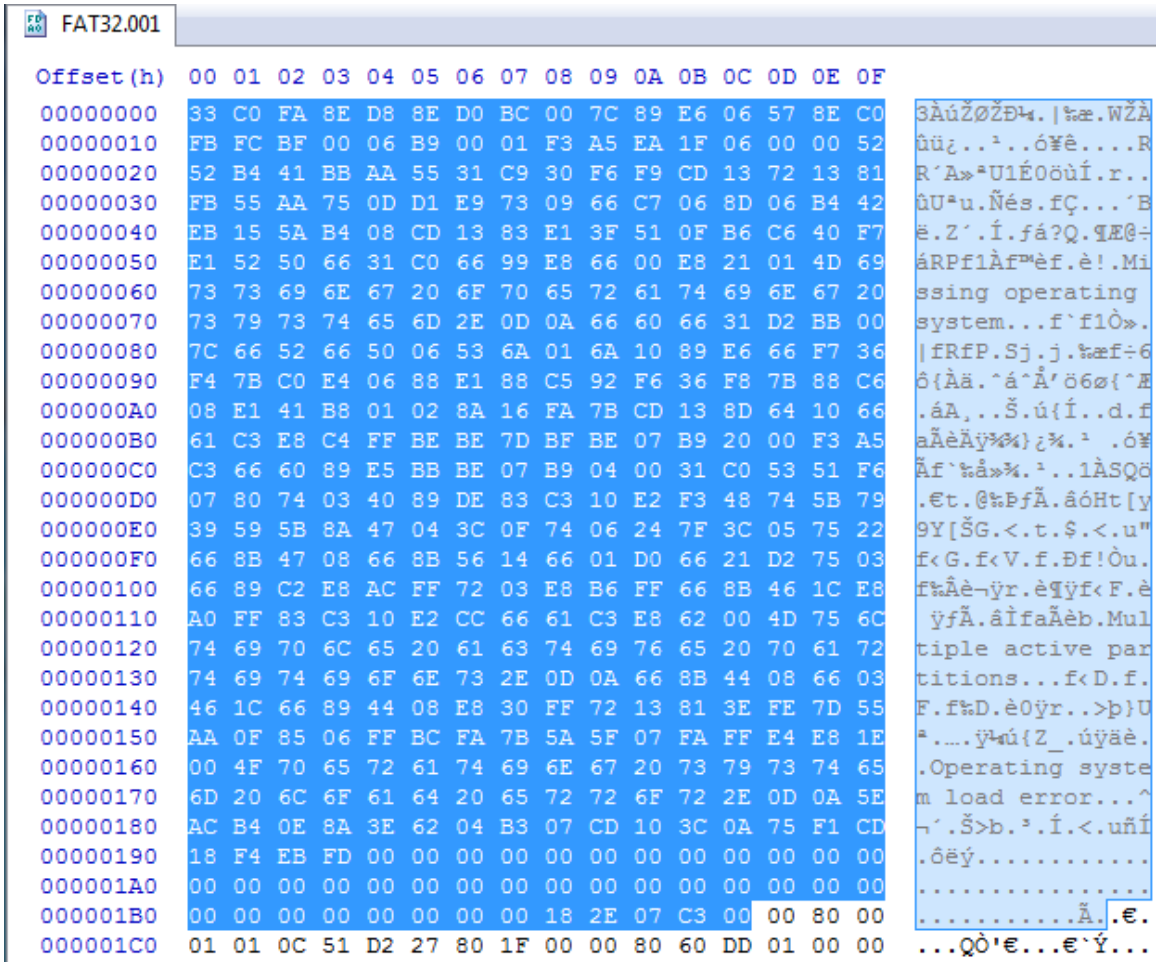


This work by the National Information Security and Geospatial Technologies Consortium (NISGTC), and except where otherwise noted, is licensed under the Creative Commons Attribution 3.0 Unported License.

4. Leave the default size as 512 bytes. Click **OK**.

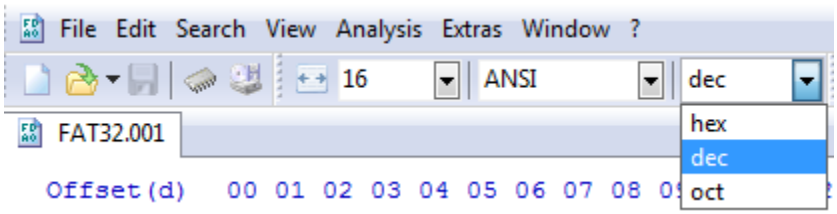


5. With DOS (Disk Operating System) based file structures, the first 446 bytes, 00000000 – 000001BC (or 00000000 – 00000445 in decimal) is the Boot Code. Highlight from 00000000 – 000001BC to examine this code in the right pane.

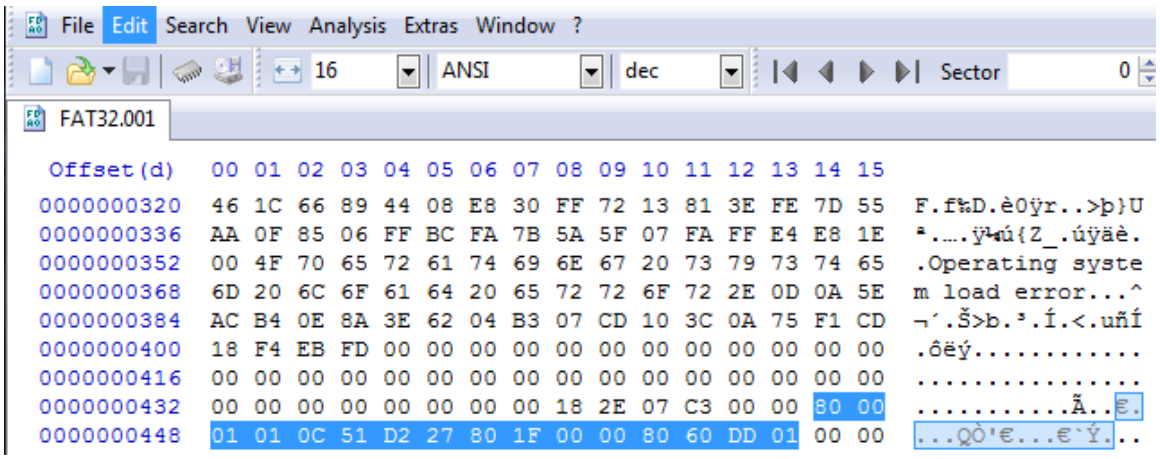


This work by the National Information Security and Geospatial Technologies Consortium (NISGTC), and except where otherwise noted, is licensed under the Creative Commons Attribution 3.0 Unported License.

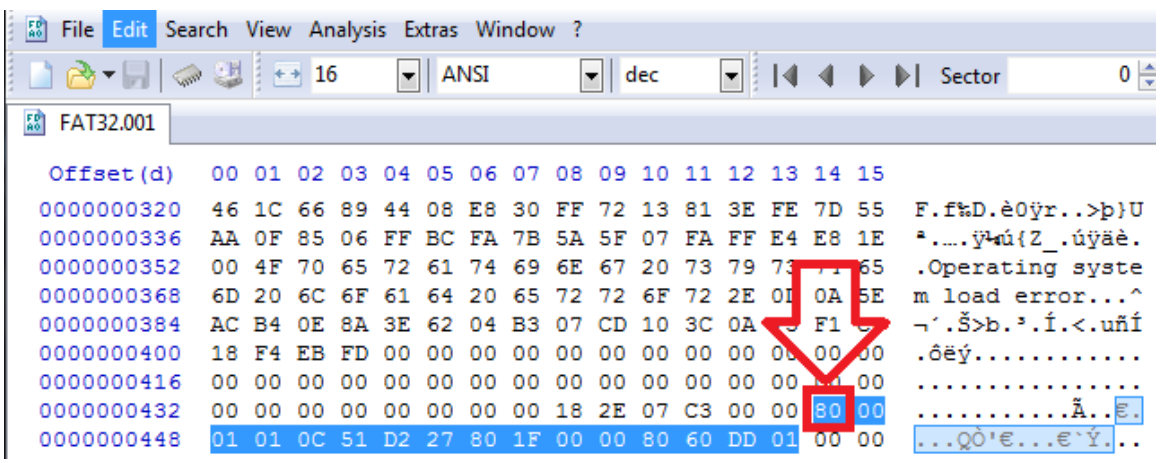
7. Change the offset base from hex to decimal in the rightmost drop-down box.



8. To examine the first partition, highlight offset 446-461 and view the right pane.

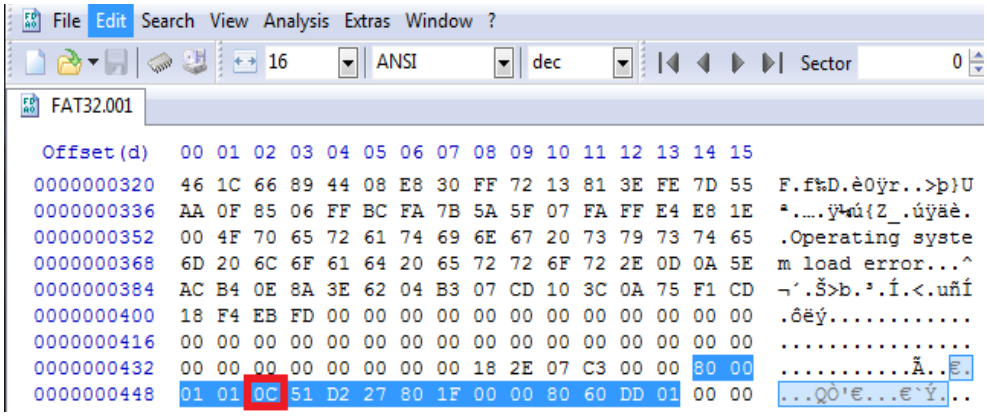


9. Within the partition information, notice that the first byte of this FAT32 image has the bootable flag value of **80,** which means that this is a bootable partition.

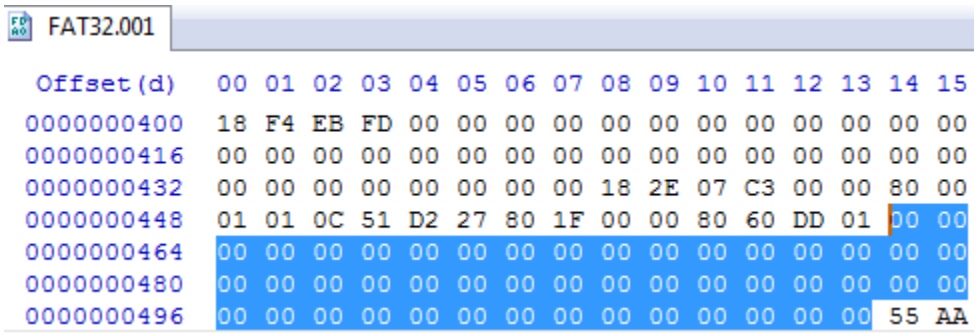


This work by the National Information Security and Geospatial Technologies Consortium (NISGTC), and except where otherwise noted, is licensed under the Creative Commons Attribution 3.0 Unported License.

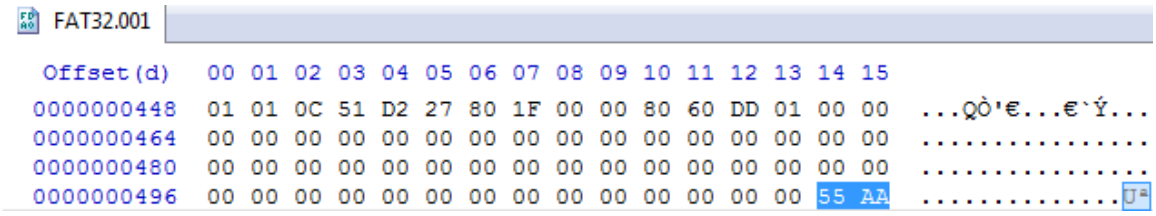
10. Move your cursor four bytes from the bootable flag, which is the location of the partition identifier. A value of **0C** means that this is a FAT32 partition set to LBA mode addressing. The acronym LBA stands for Logical Block Addressing, which is allowed for larger disks.



11. To examine the next 3 partitions, highlight from offset 462-509 and view the right pane. Notice that the next three partitions are unused, since they are all zeros.



12. Notice that the Master Boot Record (MBR) ends with the signature **55 AA**.



13. Close the HxD application and the Windows7 PC Viewer.

This work by the National Information Security and Geospatial Technologies Consortium (NISGTC), and except where otherwise noted, is licensed under the Creative Commons Attribution 3.0 Unported License.

2.2 Conclusion

The FAT file system was adapted on hard disks and used extensively during the heyday of the DOS and Windows 9X operating systems. Today, you can still find the FAT file system used on solid-state and flash memory cards. A hexadecimal (hex) editor like HxD will allow you to examine the details of FAT or FAT32 Partitions and disk images.

Below are some tables that provide key areas to examine when using a hex editor:

Data Structures for the DOS Partition Table

Byte Range (decimal)	Description
0-445	Boot Code
446-461	Partition Table 1
462-477	Partition Table 2
478-493	Partition Table 3
494-509	Partition Table 4
510-511	Signature

Data Structure for DOS Partition Entries

Byte Range	Description
0-0	Bootable Flag
1-3	Starting CHS address
4-4	Partition Type
5-7	Ending CHS address
8-11	Starting LBA address
12-15	Size in sectors

For information on partition types, see:
http://www.win.tue.nl/~aeb/partitions/partition_types-1.html

2.3 Discussion Questions

1. What is the byte range in decimal for the first partition?
2. What number indicated that a partition is bootable?
3. What does LBA stand for and what does it do?
4. The Master Boot Record ends with what signature?

This work by the National Information Security and Geospatial Technologies Consortium (NISGTC), and except where otherwise noted, is licensed under the Creative Commons Attribution 3.0 Unported License.

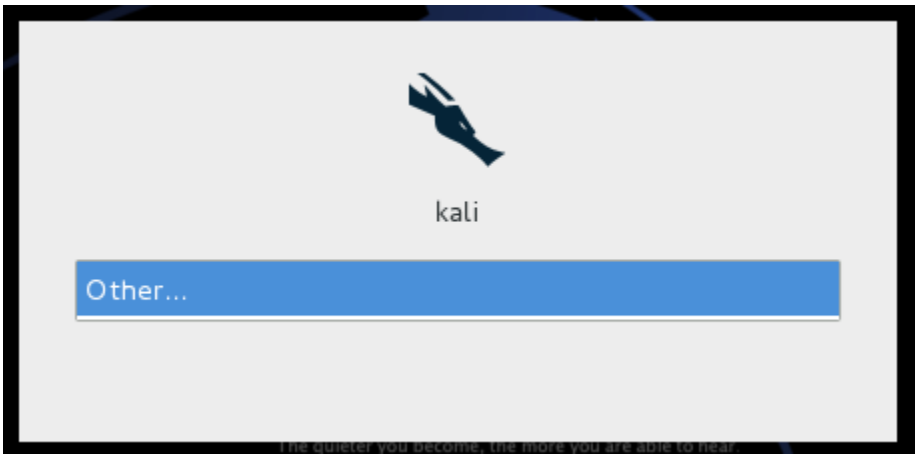
3 Verifying and Viewing Image Details

An image is a bit-by-bit copy of a disk. In this case, the FAT32 file system was used on a volume where the operating system was installed. With the Windows 2000, Windows 2003, and Windows XP operating systems, the user could choose between the FAT32 and NTFS file systems. Starting with Windows Vista, NTFS had to be used on the OS drive.

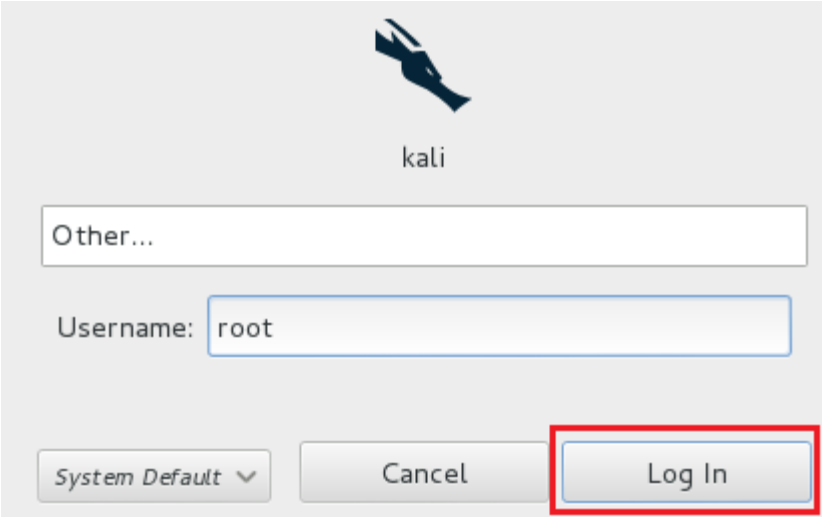
Keep in mind that **Linux commands are case sensitive**. The commands below must be entered exactly as shown.

3.1 Verifying Integrity

1. Click the **Kali Machine on the External Network** on the topology**.** Click the **Other** link.

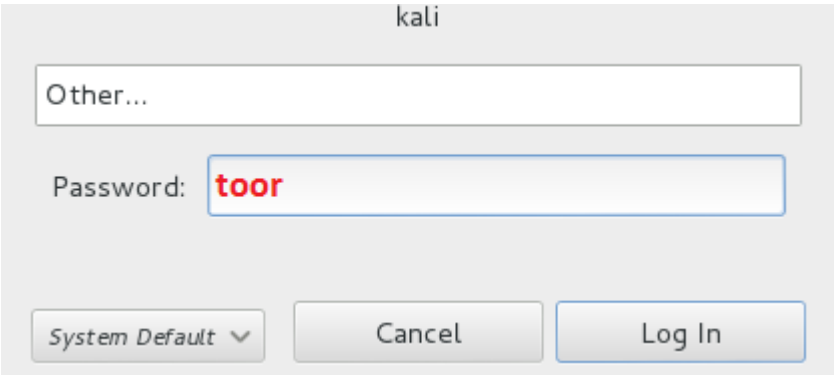


2. For the username for the Kali system, type **root**, then click the **Log In** button.

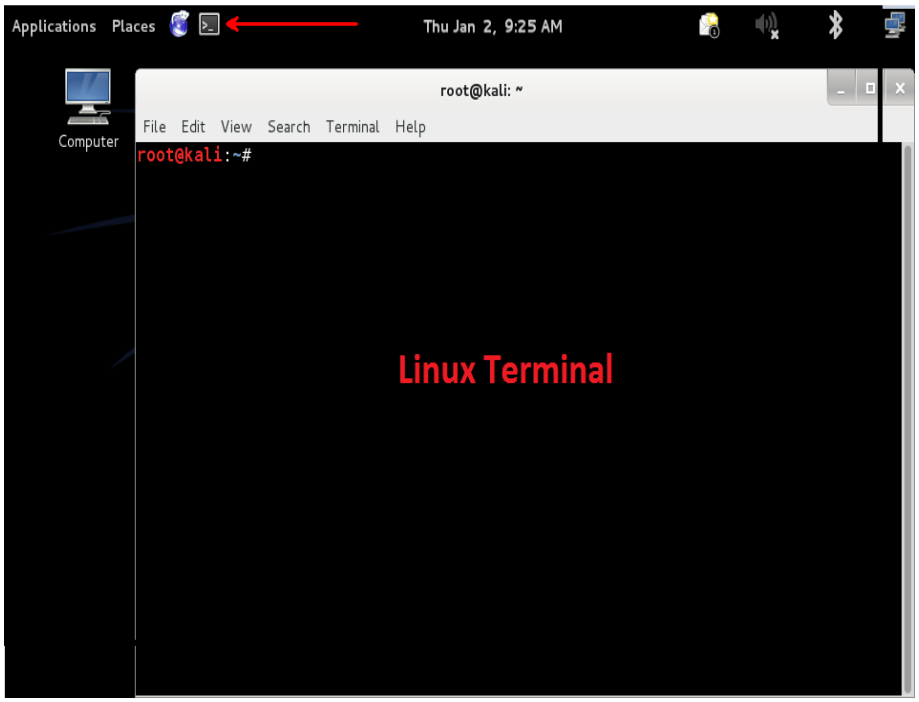


This work by the National Information Security and Geospatial Technologies Consortium (NISGTC), and except where otherwise noted, is licensed under the Creative Commons Attribution 3.0 Unported License.

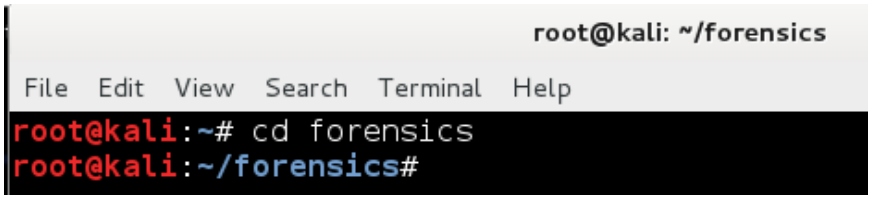
3. For the password, type **toor**, then click the **Log In** button.



4. Open a Linux terminal by clicking on the black icon to the right of the world icon.



5. Switch to the images directory by typing the following command:
root@kali:~# **cd forensics**



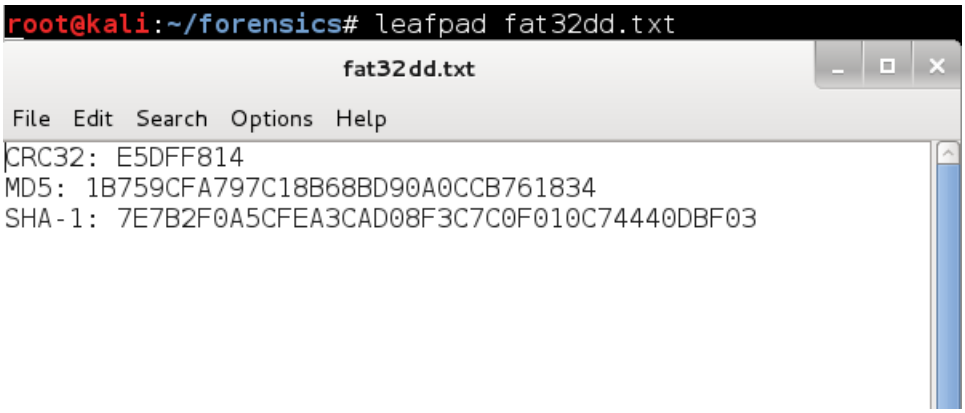
When an investigator collects an image, the SHA1 and MD5 hashes should be recorded. The hashes for the disk image are usually put into a text file that accompanies the image file.

This work by the National Information Security and Geospatial Technologies Consortium (NISGTC), and except where otherwise noted, is licensed under the Creative Commons Attribution 3.0 Unported License.

6. Type the following command to view the file with the hashing information:
   root@kali:~/forensics# **ls fat32dd.txt**

```
root@kali:~/forensics# ls fat32dd.txt
fat32dd.txt
```

7. Type the following command to view the file from the Graphical User Interface:
   root@kali:~/forensics# **leafpad fat32dd.txt**



8. Close the file when you are finished viewing it with the leafpad application.
9. Type the following command to view the file contents from the terminal :
   root@kali:~/forensics# **cat fat32dd.txt**

```
root@kali:~/forensics# cat fat32dd.txt
CRC32: E5DFF814
MD5: 1B759CFA797C18B68BD90A0CCB761834
SHA-1: 7E7B2F0A5CFEA3CAD08F3C7C0F010C74440DBF03
```

10. Type the following command to view the MD5 hash:
    root@kali:~/forensics# **cat fat32dd.txt | grep MD5**

```
root@kali:~/forensics# cat fat32dd.txt | grep MD5
MD5: 1B759CFA797C18B68BD90A0CCB761834
```

11. Type the following command to view the file with the hashing information:
    root@kali:~/forensics# **md5sum fat32.dd**

```
root@kali:~/forensics# md5sum fat32.dd
1b759cfa797c18b68bd90a0ccb761834  fat32.dd
```

12. Notice that the MD5 sum matches the sum from the acquisition text file.

This work by the National Information Security and Geospatial Technologies Consortium (NISGTC), and except where otherwise noted, is licensed under the Creative Commons Attribution 3.0 Unported License.

13. Type the following command to view the SHA1 hash:
    root@kali:~/forensics# **cat fat32dd.txt | grep SHA-1**

```
root@kali:~/forensics# cat fat32dd.txt | grep SHA-1
SHA-1: 7E7B2F0A5CFEA3CAD08F3C7C0F010C74440DBF03
```

14. Type the following command to view the file with the hashing information :
    root@kali:~/forensics# **sha1sum fat32.dd**

```
root@kali:~/forensics# cat fat32dd.txt | grep SHA-1
SHA-1: 7E7B2F0A5CFEA3CAD08F3C7C0F010C74440DBF03
root@kali:~/forensics# sha1sum fat32.dd
7e7b2f0a5cfea3cad08f3c7c0f010c74440dbf03  fat32.dd
```

15. Notice that the SHA1 sum matches the sum from the acquisition text file. Close the Linux terminal.

3.2 Conclusion

When an image is collected, the incident responder should generate a corresponding text file with the image MD5 and SHA1 hash values, as well as other information, including the cyclical redundancy check (CRC value). The md5sum and sha1sum utilities can be utilized from the terminal to hash a data set to verify the integrity of the data.

3.3 Discussion Questions

1. What Linux command can be used to parse information out of a txt file?
2. How many bits is the MD5 hashing algorithm?
3. How many bits is the SHA1 hashing algorithm?
4. Which hashing algorithm is more accurate, MD5 or SHA1?

This work by the National Information Security and Geospatial Technologies Consortium (NISGTC), and except where otherwise noted, is licensed under the Creative Commons Attribution 3.0 Unported License.

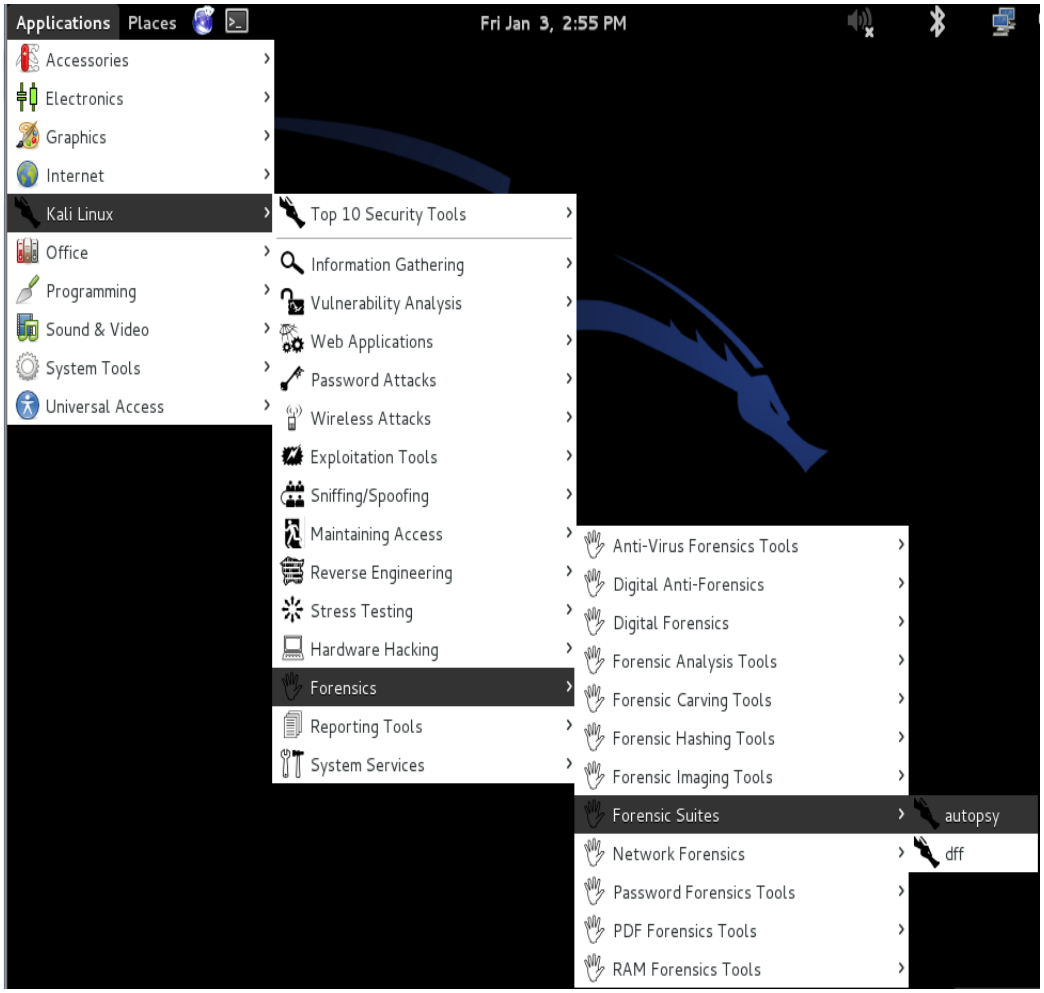
4 Analyzing a FAT Partition with Autopsy

Forensic analysis requires loading an image file into a forensic tool. The most widely used forensic tools are commercial tools, such as 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.

4.1 Loading the FAT Image into Autopsy

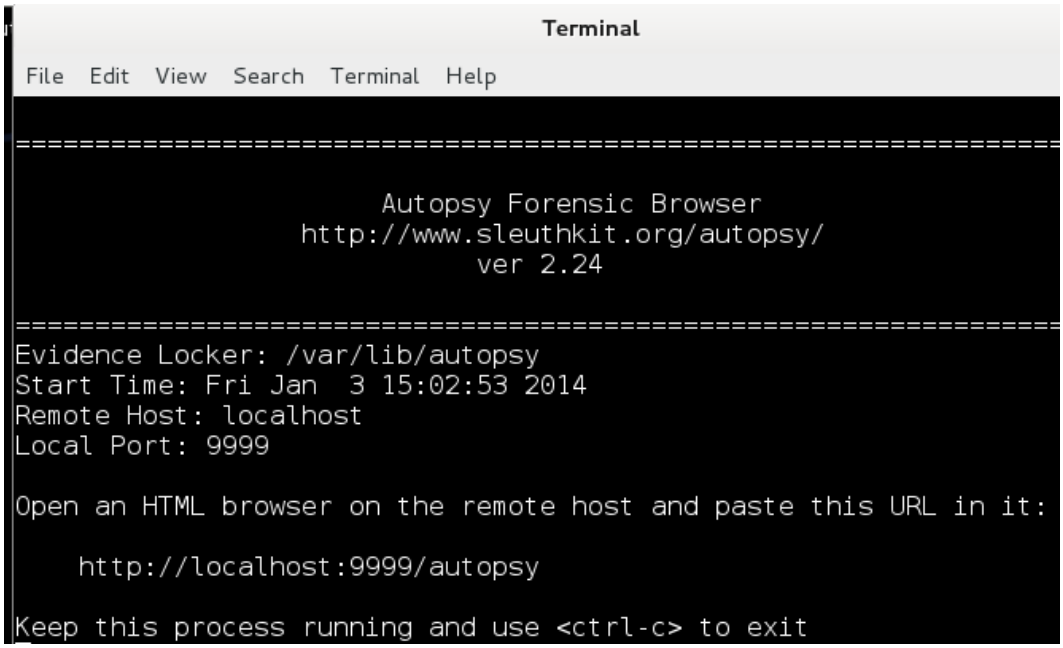
Autopsy and The Sleuthkit are already installed with almost every release of BackTrack.

1. To use the Autopsy forensic browser, you must first perform the following steps:
   a. Click **Applications > Kali Linux > Forensics > Forensic Suites > autopsy**.

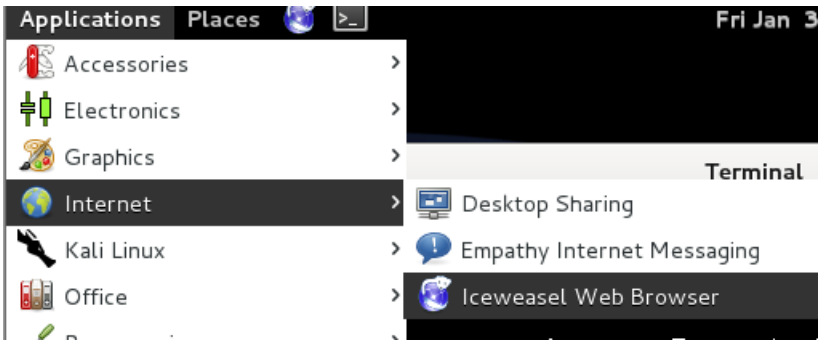


This work by the National Information Security and Geospatial Technologies Consortium (NISGTC), and except where otherwise noted, is licensed under the Creative Commons Attribution 3.0 Unported License.

b. A window with a link of http://localhost:9999/autopsy appears. Leave this window open.

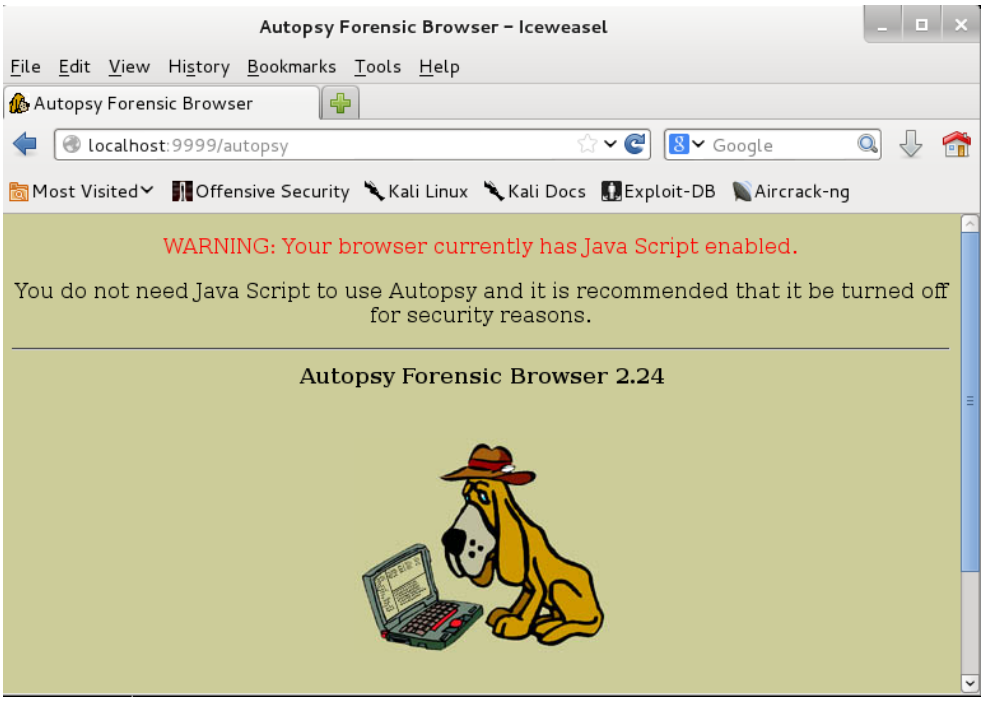


c. From the menu bar, click **Applications > Internet > Iceweasel Web Browser.**

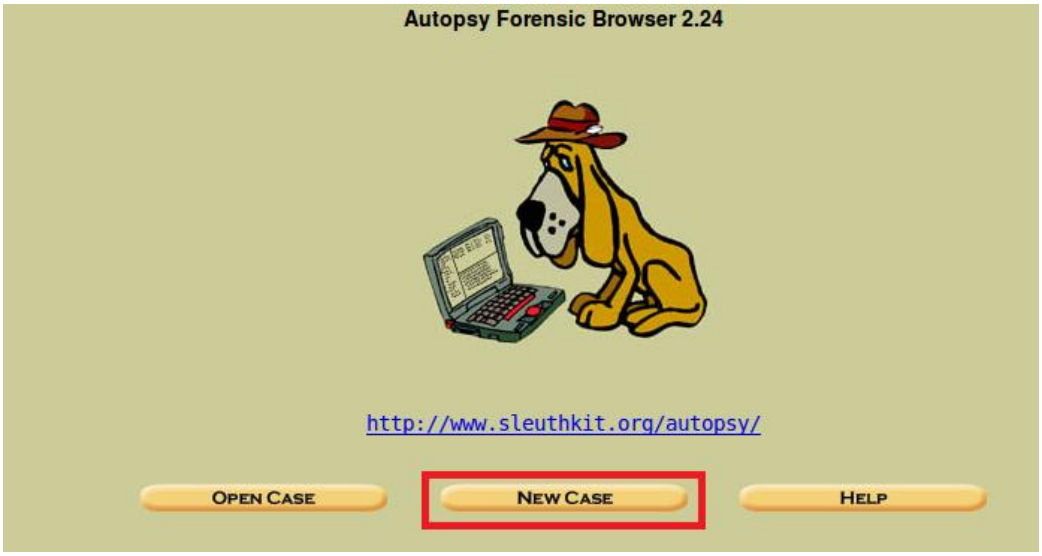


This work by the National Information Security and Geospatial Technologies Consortium (NISGTC), and except where otherwise noted, is licensed under the Creative Commons Attribution 3.0 Unported License.

d. Go to the following link within Iceweasel: http://localhost:9999/autopsy

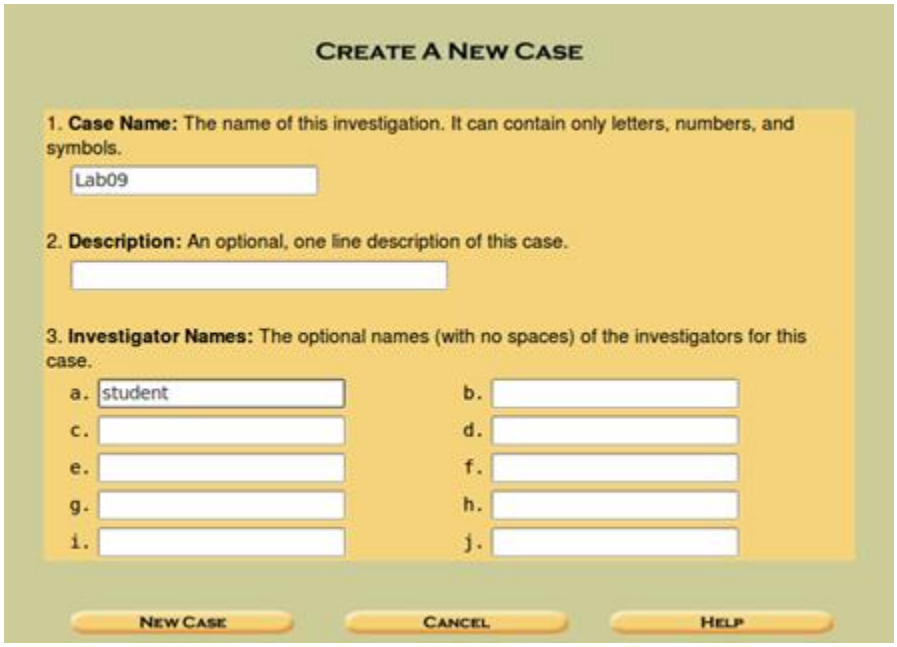


2. Click the **New Case** radio button to start a new case within Autopsy.

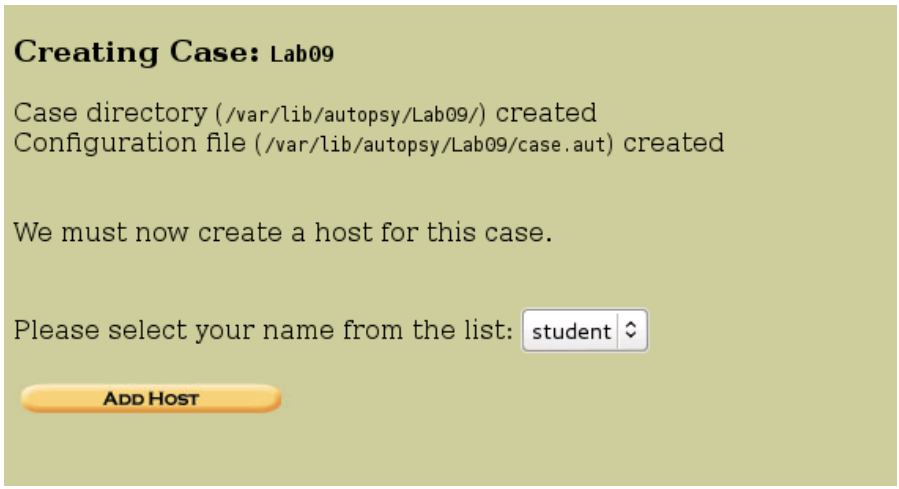


This work by the National Information Security and Geospatial Technologies Consortium (NISGTC), and except where otherwise noted, is licensed under the Creative Commons Attribution 3.0 Unported License.

3. Enter **Lab09** for the case name and **student** as an investigator name. Click **New Case**.



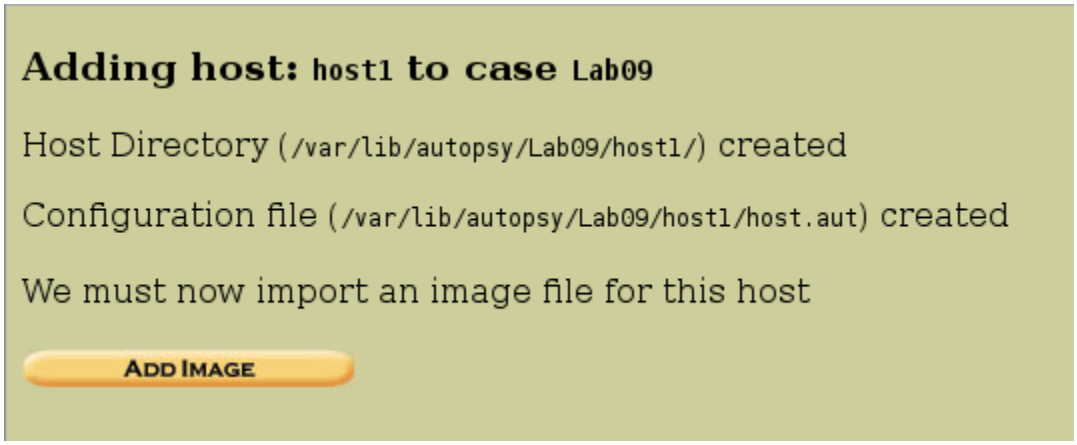
4. At the Creating Case: Lab09 screen, click **Add Host.**



This work by the National Information Security and Geospatial Technologies Consortium (NISGTC), and except where otherwise noted, is licensed under the Creative Commons Attribution 3.0 Unported License.

5. Click **Add Host** at the Add a New Host screen.

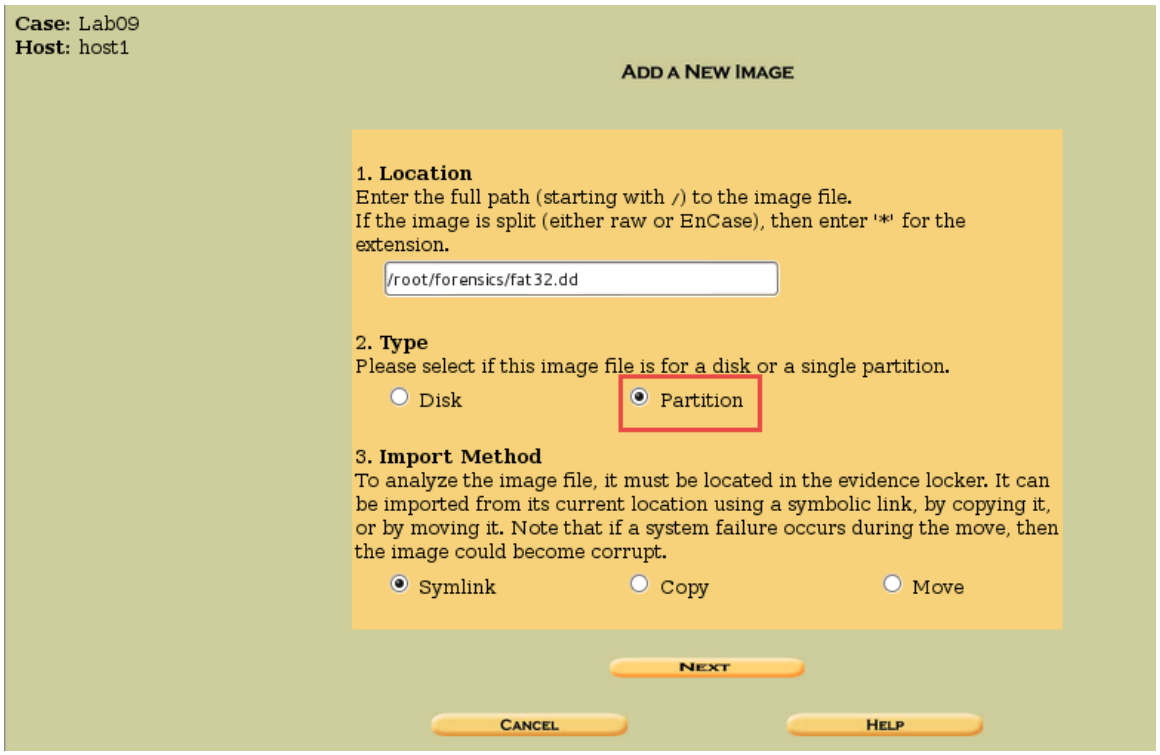
6. Click **Add Image** to import an image file to the host.



This work by the National Information Security and Geospatial Technologies Consortium (NISGTC), and except where otherwise noted, is licensed under the Creative Commons Attribution 3.0 Unported License.

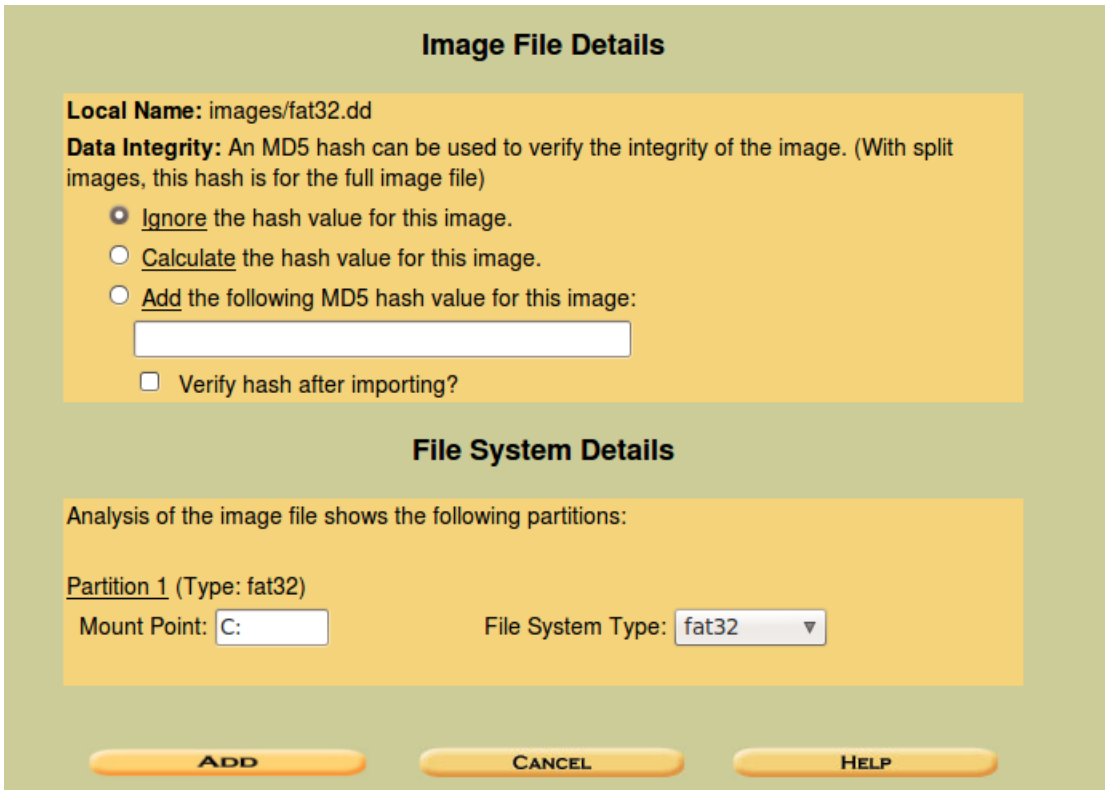
7. Click **Add Image File** to add the image to the Autopsy case.

8. **For location**, type **/root/forensics/fat32.dd.** For type, select **Partition**. Click **Next**.

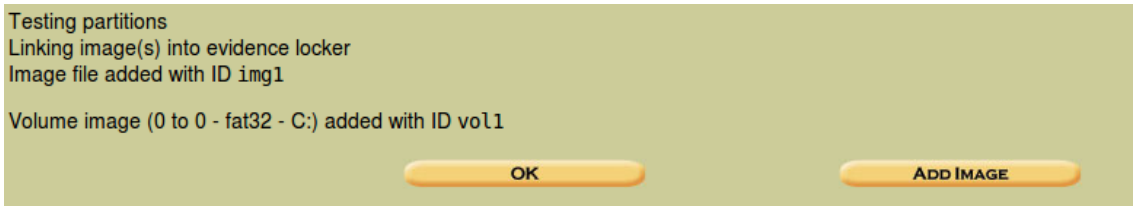


This work by the National Information Security and Geospatial Technologies Consortium (NISGTC), and except where otherwise noted, is licensed under the Creative Commons Attribution 3.0 Unported License.

9. Click **Add** on the Image File Details screen of Autopsy.

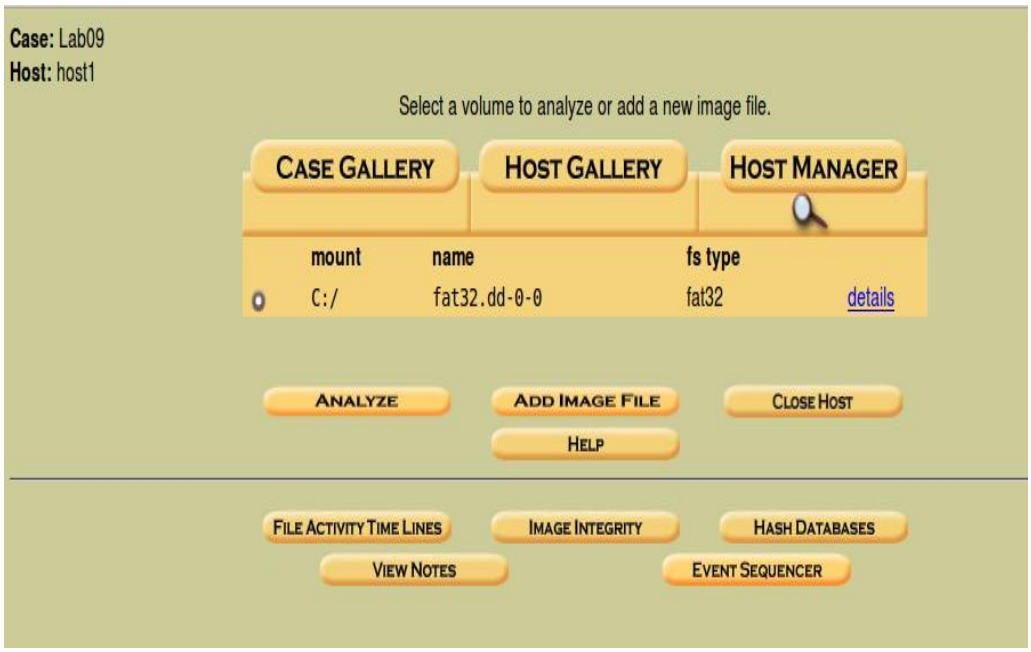


10. Click **OK** to the message that the Volume Image (FAT32) is added.

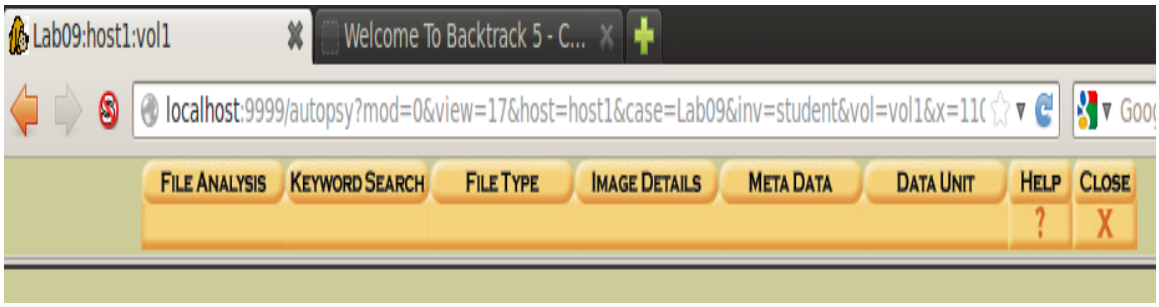


This work by the National Information Security and Geospatial Technologies Consortium (NISGTC), and except where otherwise noted, is licensed under the Creative Commons Attribution 3.0 Unported License.

11. Click the **Analyze** button to analyze the FAT32 image.

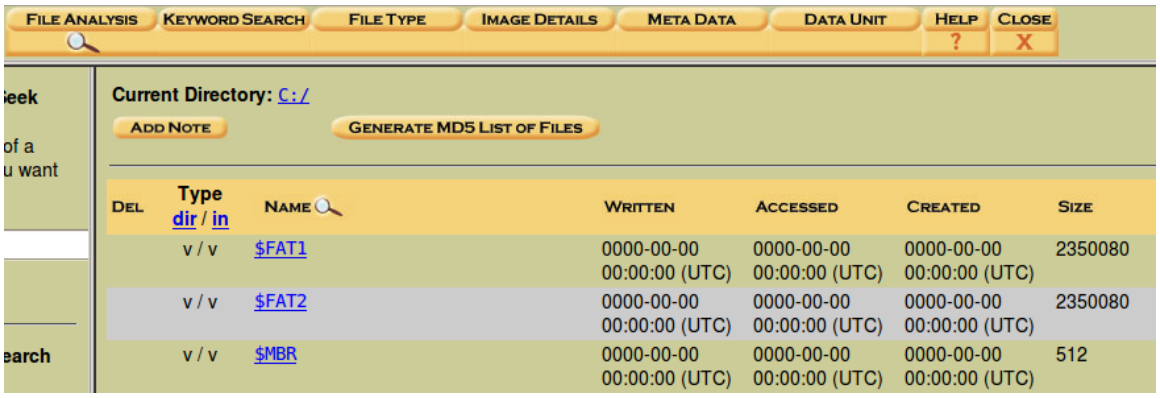


12. Click **File Analysis** to view the files and folders that exist on the FAT32 partition.



This work by the National Information Security and Geospatial Technologies Consortium (NISGTC), and except where otherwise noted, is licensed under the Creative Commons Attribution 3.0 Unported License.

13. Notice the FAT1 and FAT2 records, along with the Master Boot Record.



14. Close all open windows and the Kali PC Viewer.

4.2 Conclusion

Autopsy is a forensic analysis tool that is free to use. Commercial forensic products, like EnCase and FTK, are more widely used but are not free and require hardware dongles. Autopsy 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.

4.3 Discussion Questions

1. How do you setup Autopsy?
2. What link do you need to put in your browser to use Autopsy?
3. Name three files that should be on every FAT32 image.
4. What is the command to launch Autopsy from the command line?

This work by the National Information Security and Geospatial Technologies Consortium (NISGTC), and except where otherwise noted, is licensed under the Creative Commons Attribution 3.0 Unported License.

References

1. Comparing NTFS and FAT file systems:
   windows.microsoft.com/en-us/windows-vista/comparing-ntfs-and-fat-file-systems

2. Autopsy:
   http://www.sleuthkit.org/index.php

3. Journaling File System:
   http://searchsecurity.techtarget.com/definition/journaling-file-system

4. FAT File System:
   http://en.wikipedia.org/wiki/File_Allocation_Table

5. FAT32 vs. NTFS:
   http://www.pcmag.com/article2/0,2817,2421454,00.asp

6. FAT32 File System Description:
   http://support.microsoft.com/kb/154997

This work by the National Information Security and Geospatial Technologies Consortium (NISGTC), and except where otherwise noted, is licensed under the Creative Commons Attribution 3.0 Unported License.