# DIGITAL FORENSICS LAB SERIES

# Lab 1: Introduction to File Systems

**Objective: Digital Forensics Fundamentals**

**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.

# Contents

## Introduction

This lab includes the following tasks:

1. Examining Different Windows and Linux File Systems
2. Partitioning and Formatting File Systems in Windows
3. Formatting and Wiping Linux File Systems

## Objective: Digital Forensics Fundamentals

Performing this lab will provide the student with a hands-on lab experience meeting the Digital Forensics Fundamentals Objective:

*The candidate will demonstrate an understanding of forensic methodology, key forensics concepts, and identifying types of evidence on current Windows operating systems.*

In order to understand computer forensics, you must be aware of the common file systems that are utilized by Windows, Mac, and Linux operating systems.

**FAT** – File Allocation Table is a table that 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 that are written to the disk.

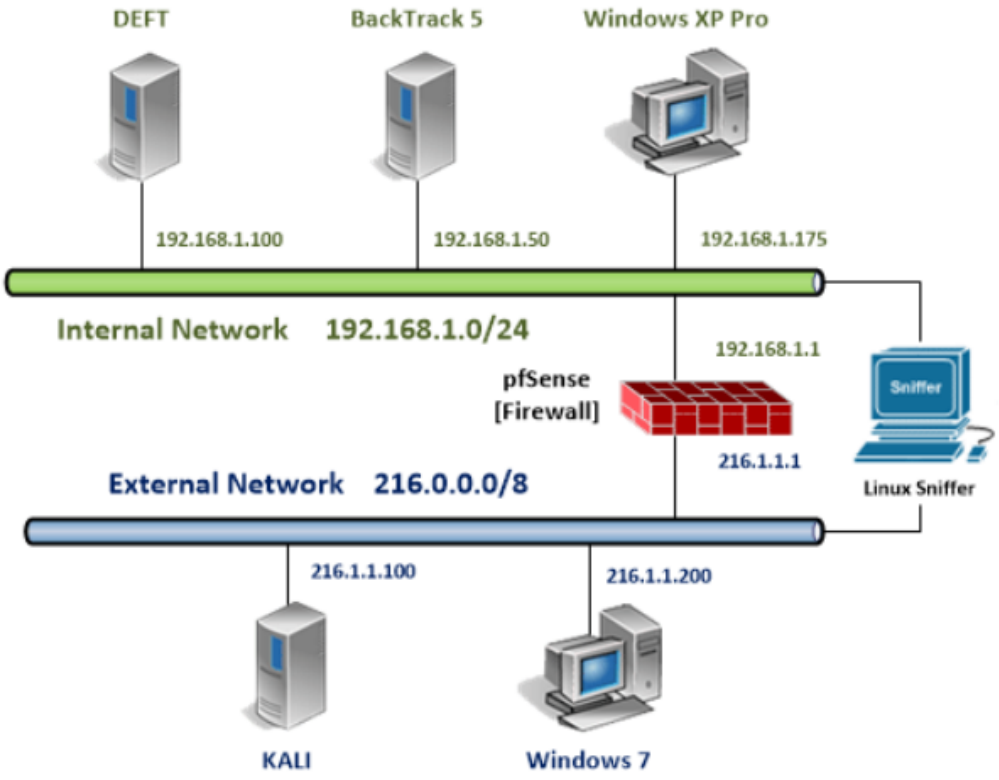
**NTFS** – New Technology File System was originally introduced with the Windows NT. NTFS is a journaling file system which means it keeps a log of changes being written to the disk. If a computer is shutdown improperly, it will have a better chance of recovery if it has a journaling file system. Files 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.

**EXT2/3/4** – The Extended File Systems 2, 3, and 4 are utilized by the Linux operating systems. Both EXT3 and EXT4 are journaling file systems. EXT2 does not have journaling.

**format** – A format will not erase the data from the volume. Rather, it will delete the references to the file in the FAT or Master File Table ($MFT) and make those spaces on the disk as available. Forensic recovery of files may be possible on a formatted disk.

**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.

## 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 |
| Windows 7 External Machine | 216.1.1.200 | student | password |

# 1 Examining Different Windows and Linux File Systems

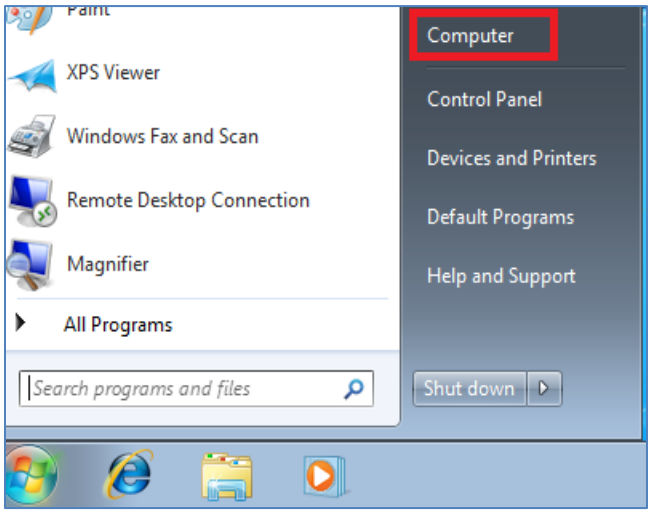
File Systems store data on a disk. The most common Windows file systems are FAT and NTFS. There are several versions of FAT, including FAT12, FAT16, FAT32, exFAT, and FATx (XBOX). Some of the most common Linux file systems include EXT2, EXT3, EXT4 and ReiserFS. Mac OS X uses the HFS+ File system, older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

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

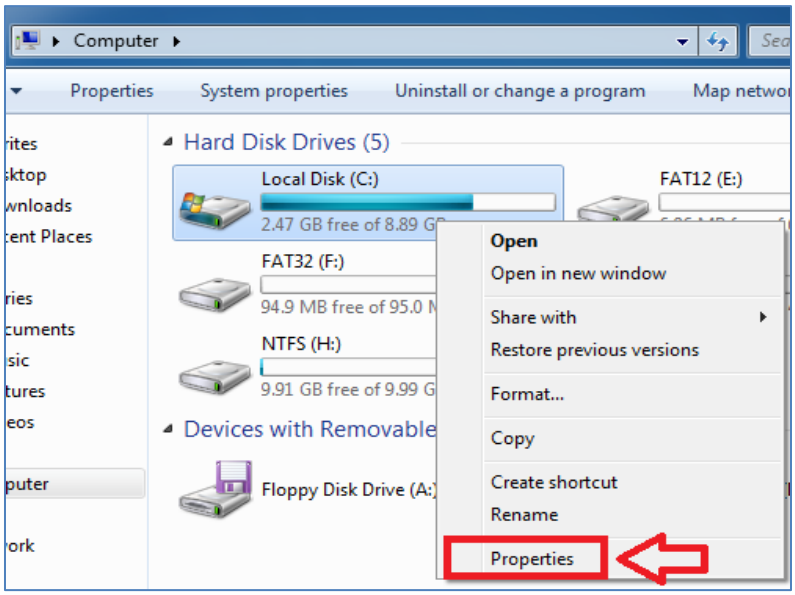
## 1.1 Viewing File Systems

1. To log into the **Windows 7 Machine on the External Network**, click 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.

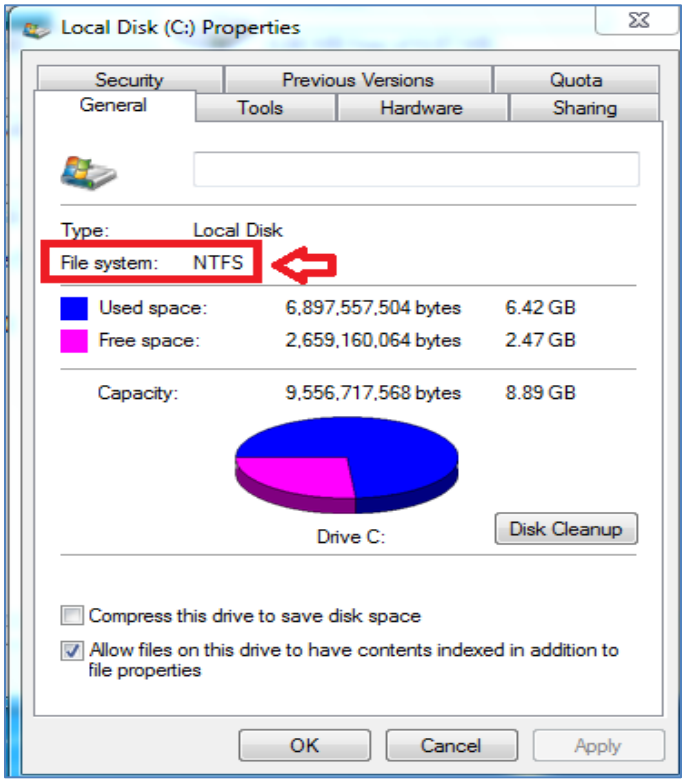

4. Click the Start icon in the lower-left corner and then select **Computer.**



5. Right-click on the local disk (C:) and go to the Properties tab.

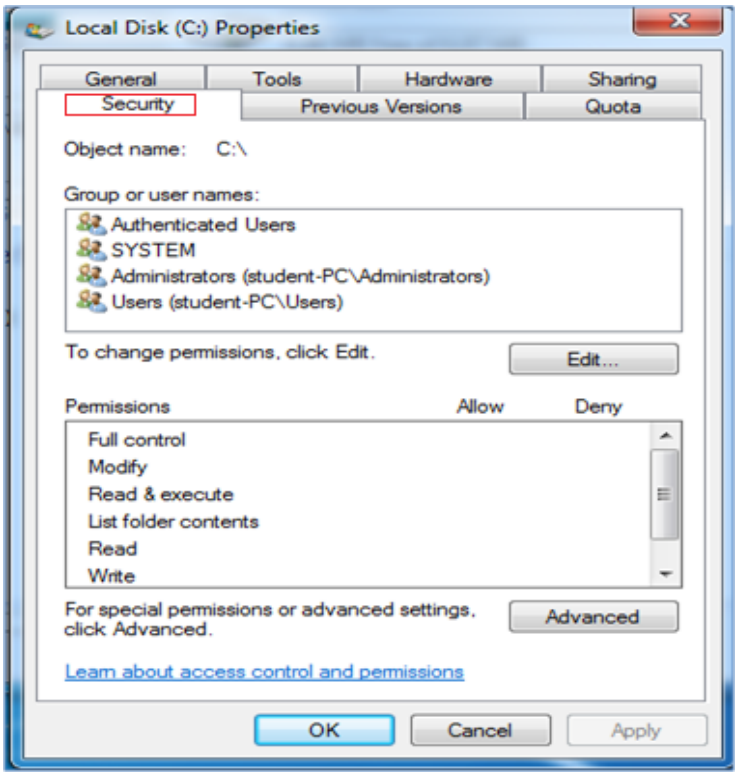



6. View the file system type, which should be listed as NTFS.

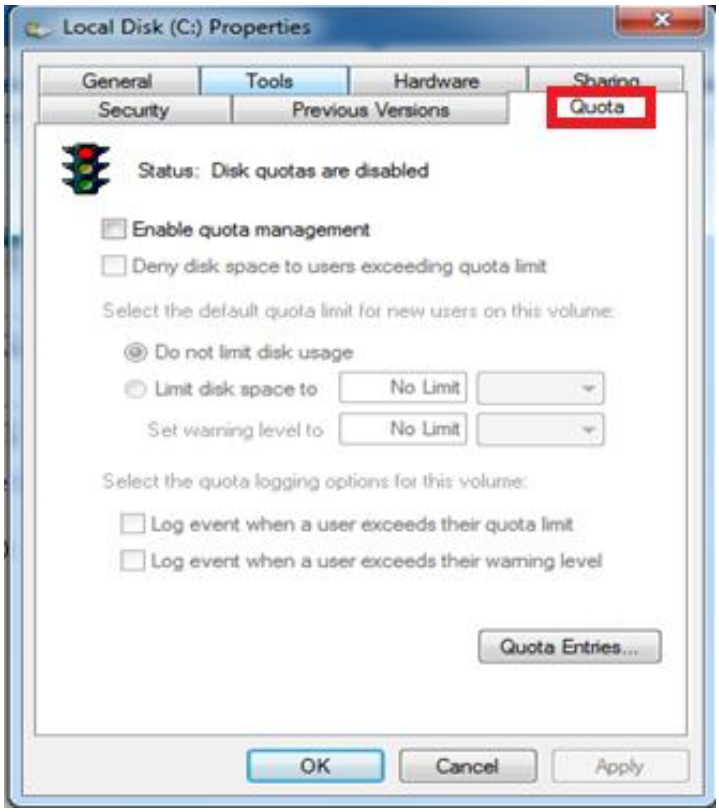



On NTFS volumes, security permissions and quotas can be configured. Security permissions can be configured to restrict access to files or folders. Quotas are used to restrict the amount of storage for each user to prevent a disk from running out of space.

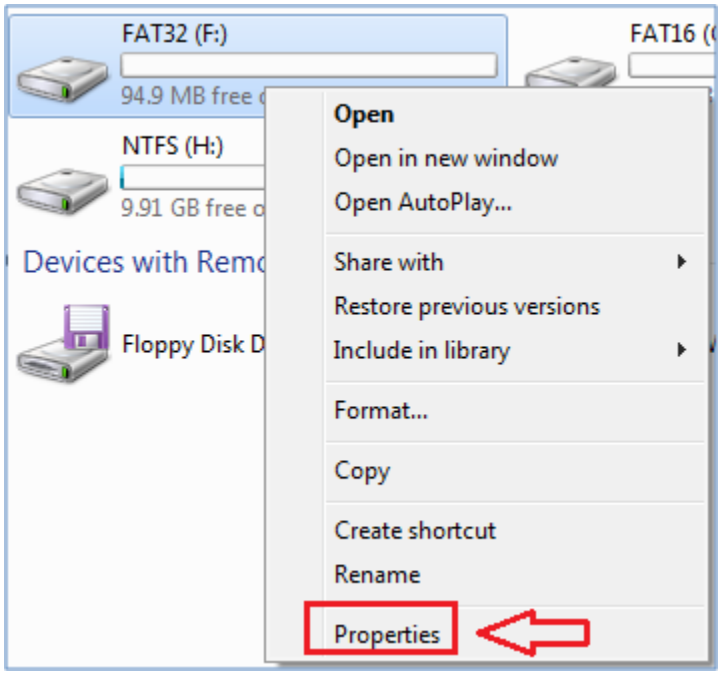
7. Click on the Security tab. This is where access control can be configured.



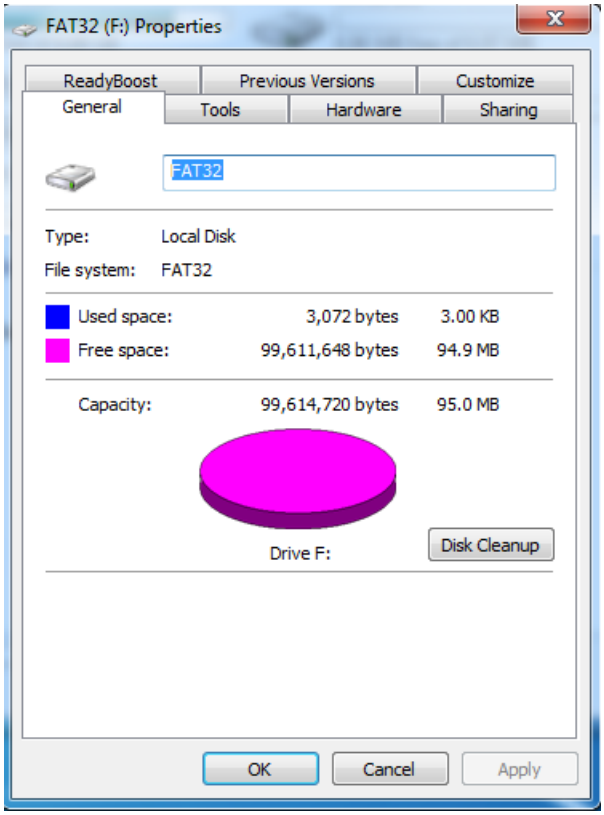

8. Click on the Quota tab. This is where disk usage can be restricted for users.



9. Close local disk (C:) Properties. Right-click on the FAT32 drive and go to the Properties tab.




10. Notice that there is no Security or Quota tab on a FAT32 volume.



11. Close all open windows and minimize the Windows 7 Remote PC Viewer.

Next, we will examine file systems that are common to the Linux operating system, including EXT2, EXT3, EXT4, and ReiserFS. Linux supports a large number of file systems.

12. Open the **BackTrack 5 Machine on the Internal Network**. Type **root** for the login and **toor** *(root spelled backwards)* for the password. You may need to press Enter before you see anything on the screen.

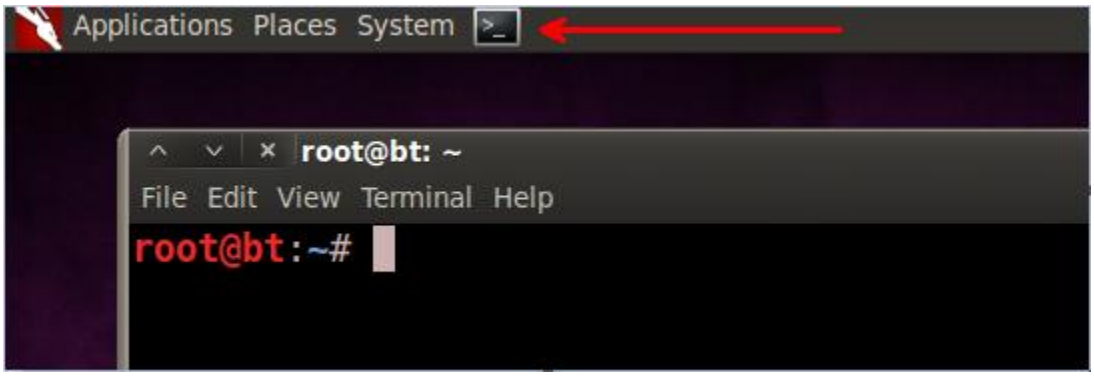
The password will not be displayed when you type it, for security purposes.

```
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:~# _
```

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

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

14. 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.



15. To view the file systems that have been mounted, type the following command:
    root@bt:~#**mount**

```
root@bt: ~
File Edit View Terminal Help
root@bt:~# mount
/dev/sda1 on / type ext4 (rw,errors=remount-ro)
proc on /proc type proc (rw,noexec,nosuid,nodev)
none on /sys type sysfs (rw,noexec,nosuid,nodev)
none on /sys/fs/fuse/connections type fusectl (rw)
none on /sys/kernel/debug type debugfs (rw)
none on /sys/kernel/security type securityfs (rw)
none on /dev type devtmpfs (rw,mode=0755)
none on /dev/pts type devpts (rw,noexec,nosuid,gid=5,mode=0620)
none on /dev/shm type tmpfs (rw,nosuid,nodev)
none on /var/run type tmpfs (rw,nosuid,mode=0755)
none on /var/lock type tmpfs (rw,noexec,nosuid,nodev)
none on /lib/init/rw type tmpfs (rw,nosuid,mode=0755)
/dev/sdb1 on /mnt/sdb1 type ext2 (rw)
/dev/sdc1 on /mnt/sdc1 type ext3 (rw)
/dev/sdd1 on /mnt/sdd1 type ext4 (rw)
/dev/sde1 on /mnt/sde1 type reiserfs (rw)
```

There are 5 disks on the Linux system. Their mount points are listed in the chart below.

| Disk Number | Device Name and Partition Number | Mount Point |
|---|---|---|
| 1 | /dev/sda1 | / |
| 2 | /dev/sdb1 | /mnt/sda1 |
| 3 | /dev/sdc1 | /mnt/sdb1 |
| 4 | /dev/sdd1 | /mnt/sdc1 |
| 5 | /dev/sde1 | /mnt/sdd1 |

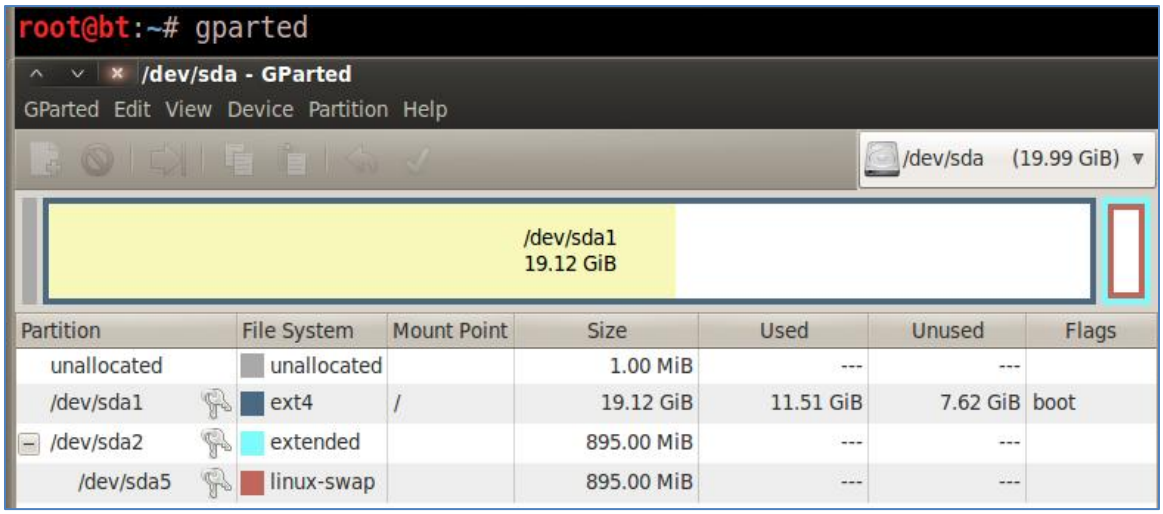
16. Type the following command to view the partitions on the first disk:
    root@bt:~# **fdisk –l /dev/sda**

```
root@bt:~# fdisk -l /dev/sda

Disk /dev/sda: 21.5 GB, 21474836480 bytes
255 heads, 63 sectors/track, 2610 cylinders
Units = cylinders of 16065 * 512 = 8225280 bytes
Sector size (logical/physical): 512 bytes / 512 bytes
I/O size (minimum/optimal): 512 bytes / 512 bytes
Disk identifier: 0x000f1335

   Device Boot      Start         End      Blocks   Id  System
/dev/sda1   *           1        2497    20051968   83  Linux
/dev/sda2            2497        2611      916481    5  Extended
/dev/sda5            2497        2611      916480   82  Linux swap / Solaris
```

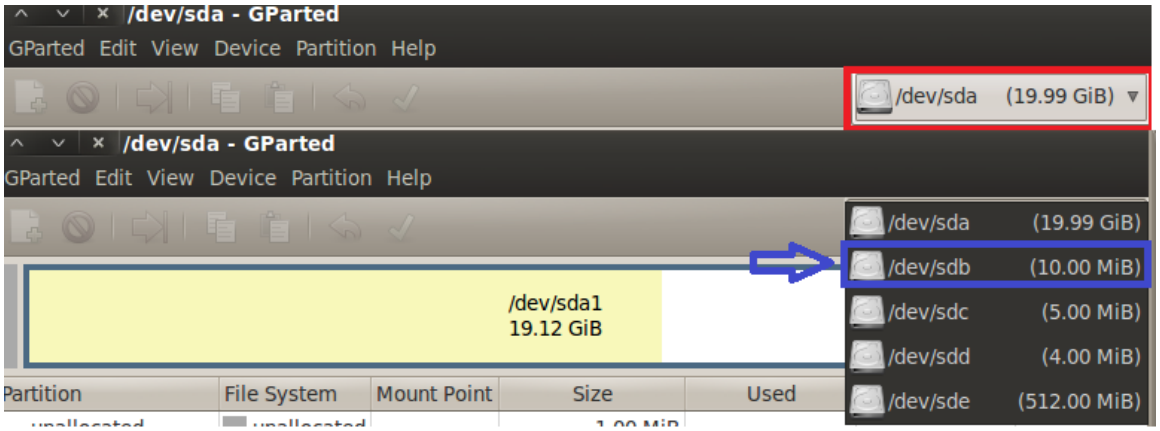
| Device Name and Partition Number | Description |
|---|---|
| /dev/sda1 | Boot and Root (/) Primary Partition |
| /dev/sda2 | Extended Partition |
| /dev/sda5 | Logical Drive within the Extended Partition - Virtual Memory |

Next, we will use a free tool called GParted to view the disks and various file systems.

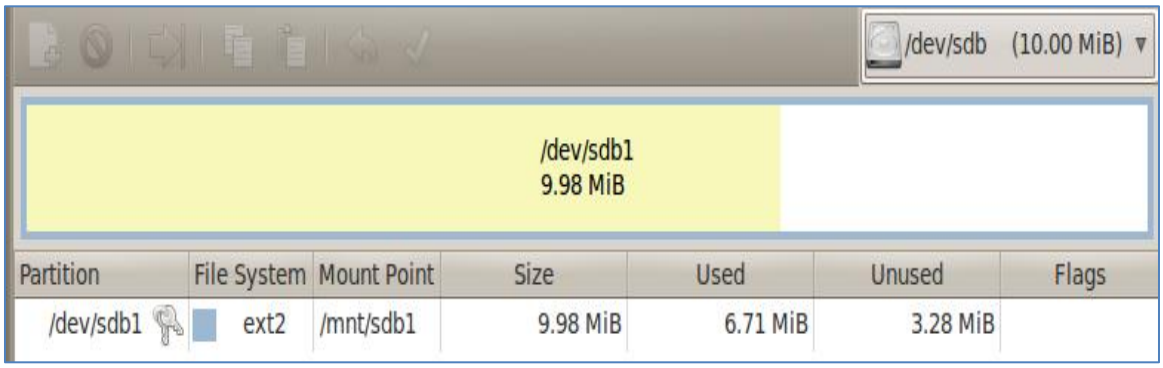
17. Type the following command to launch the GParted utility on the system.
    root@bt:~# **gparted**



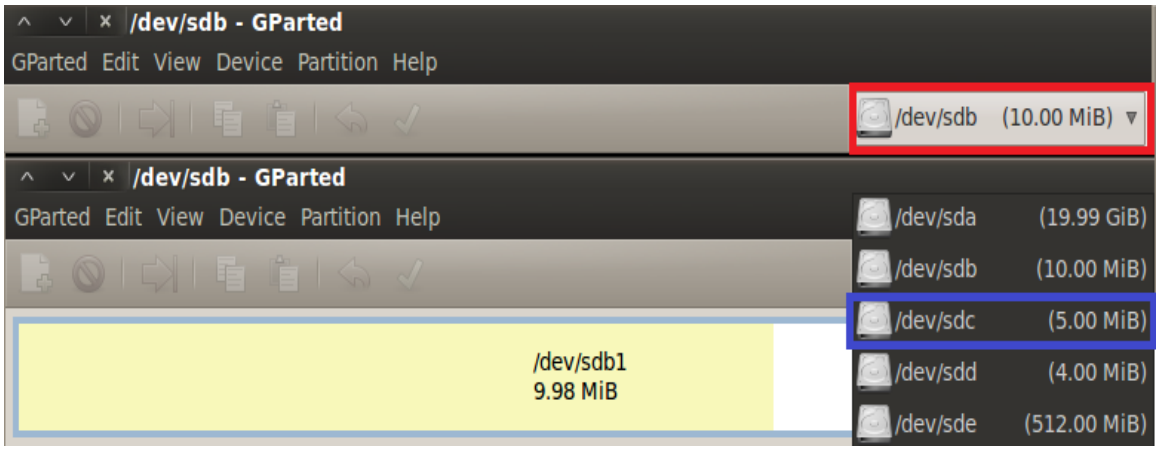
18. Click the arrow on the top-right of the program. Select **/dev/sdb** from the list.



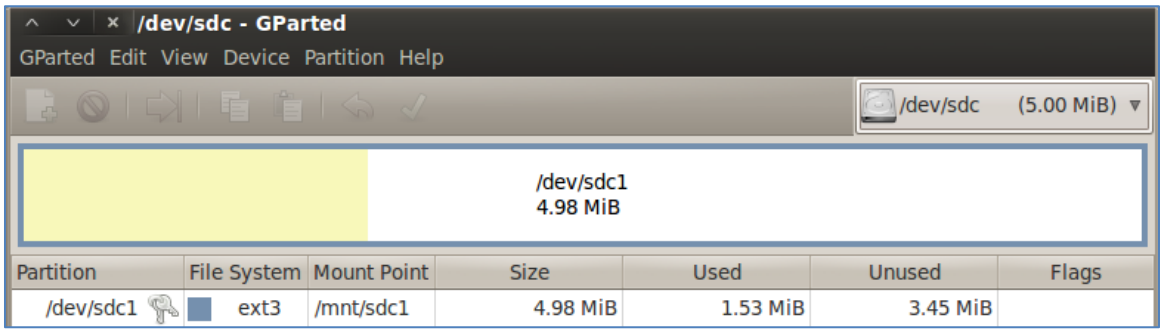

The file system of disk 2 is EXT2. The size of the disk and amount of free space is listed.



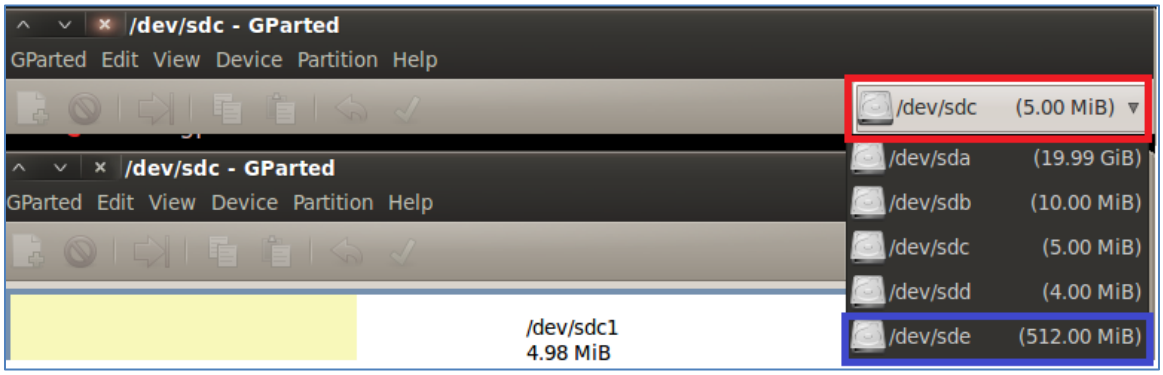

19. Click the arrow on the top-right of the program. Select **/dev/sdc** from the list.



The file system of disk 3 is EXT3. The EXT3 and EXT4 file systems have journaling, while EXT2 does not. Journaling will help the file system recover from unclean shutdowns. If a file system becomes corrupt, it can cause problems during the forensic analysis phase.

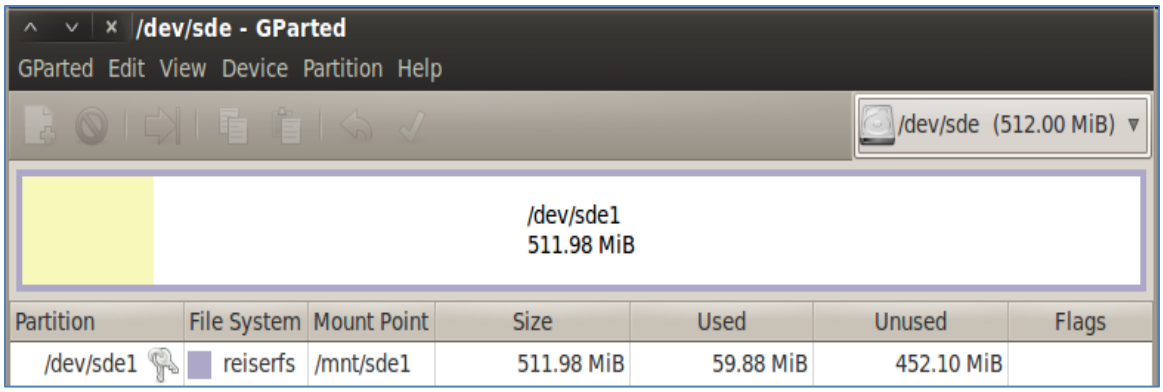



20. Click the arrow on the top-right of the program. Select **/dev/sde** from the list.

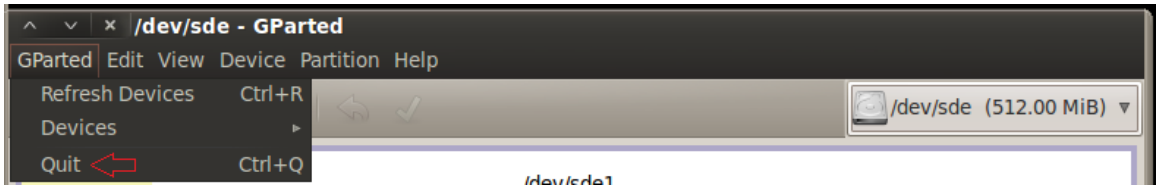



The file system of disk 5 is ReiserFS, which also has journaling.

The ReiserFS file system was developed by Hans Reiser.



21. Exit the GParted program by selecting GParted from the menu and then selecting Quit.




While EXT2, EXT3, EXT4, and ReiserFS are the most common Linux file systems, Linux supports a large number of file systems. Many distros (Linux distributions) have support for FAT and NTFS.

22. Type the following command to launch the fdisk utility on the BackTrack 5 R3 Internal Machine:
root@bt:~# **fdisk /dev/sde**

```
root@bt:~# fdisk /dev/sde

WARNING: DOS-compatible mode is deprecated. It's strongly recommended to
         switch off the mode (command 'c') and change display units to
         sectors (command 'u').
```

23. Type the letter **m** and press enter to view the help menu within the fdisk sub-menu:

```
Command (m for help): m
Command action
   a   toggle a bootable flag
   b   edit bsd disklabel
   c   toggle the dos compatibility flag
   d   delete a partition
   l   list known partition types
   m   print this menu
   n   add a new partition
   o   create a new empty DOS partition table
   p   print the partition table
   q   quit without saving changes
   s   create a new empty Sun disklabel
   t   change a partition's system id
   u   change display/entry units
   v   verify the partition table
   w   write table to disk and exit
   x   extra functionality (experts only)
```

24. Type the letter **t** then press enter to change a partition's system id.

```
Command (m for help): t
Selected partition 1
Hex code (type L to list codes):
```

25. Type the letter **L**(capital) then enter to view the codes for the partition types.

```
Hex code (type L to list codes): L

 0  Empty           24  NEC DOS         81  Minix / old Lin bf  Solaris
 1  FAT12           39  Plan 9          82  Linux swap / So c1  DRDOS/sec (FAT-
 2  XENIX root      3c  PartitionMagic  83  Linux           c4  DRDOS/sec (FAT-
 3  XENIX usr       40  Venix 80286     84  OS/2 hidden C:  c6  DRDOS/sec (FAT-
 4  FAT16 <32M      41  PPC PReP Boot   85  Linux extended  c7  Syrinx
 5  Extended        42  SFS             86  NTFS volume set da  Non-FS data
 6  FAT16           4d  QNX4.x          87  NTFS volume set db  CP/M / CTOS / .
 7  HPFS/NTFS       4e  QNX4.x 2nd part 88  Linux plaintext de  Dell Utility
 8  AIX             4f  QNX4.x 3rd part 8e  Linux LVM       df  BootIt
 9  AIX bootable    50  OnTrack DM      93  Amoeba          e1  DOS access
 a  OS/2 Boot Manag 51  OnTrack DM6 Aux 94  Amoeba BBT      e3  DOS R/O
 b  W95 FAT32       52  CP/M            9f  BSD/OS          e4  SpeedStor
 c  W95 FAT32 (LBA) 53  OnTrack DM6 Aux a0  IBM Thinkpad hi eb  BeOS fs
 e  W95 FAT16 (LBA) 54  OnTrackDM6      a5  FreeBSD         ee  GPT
 f  W95 Ext'd (LBA) 55  EZ-Drive        a6  OpenBSD         ef  EFI (FAT-12/16/
10  OPUS            56  Golden Bow      a7  NeXTSTEP        f0  Linux/PA-RISC b
11  Hidden FAT12    5c  Priam Edisk     a8  Darwin UFS      f1  SpeedStor
12  Compaq diagnost 61  SpeedStor       a9  NetBSD          f4  SpeedStor
14  Hidden FAT16 <3 63  GNU HURD or Sys ab  Darwin boot     f2  DOS secondary
16  Hidden FAT16    64  Novell Netware  af  HFS / HFS+      fb  VMware VMFS
17  Hidden HPFS/NTF 65  Novell Netware  b7  BSDI fs         fc  VMware VMKCORE
18  AST SmartSleep  70  DiskSecure Mult b8  BSDI swap       fd  Linux raid auto
1b  Hidden W95 FAT3 75  PC/IX           bb  Boot Wizard hid fe  LANstep
1c  Hidden W95 FAT3 80  Old Minix       be  Solaris boot    ff  BBT
1e  Hidden W95 FAT1
```

There are 95 different file systems listed that are supported on this version of Linux.

26. Hold down **Ctrl** and press the **C** key to exit the fdisk sub-menu.

```
Hex code (type L to list codes): ^C
root@bt:~#
```

## 1.2 Conclusion

There are many variations 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 better known for its compatibility. The journaling feature of NTFS makes it a much more stable file system.

Linux supports a large number of file systems. Common Linux file systems include EXT2, EXT3, and EXT4, as well as ReiserFS. The EXT3 and EXT4 file systems and ReiserFS are all journaling file systems.

## 1.3 Discussion Questions

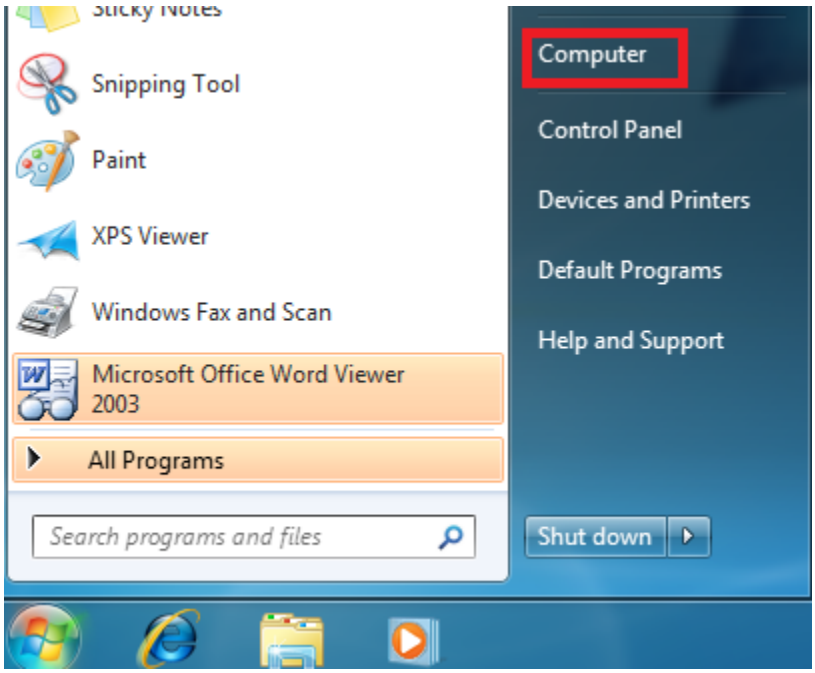
1. What command will allow you to see the mounted file systems in Linux?
2. What is the name of a GUI tool in Linux that allows you to view disks?
3. What are the file systems that are supported by Microsoft operating systems?
4. How many file systems are supported by the Linux operating system?

# 2 Partitioning and Formatting File Systems in Windows

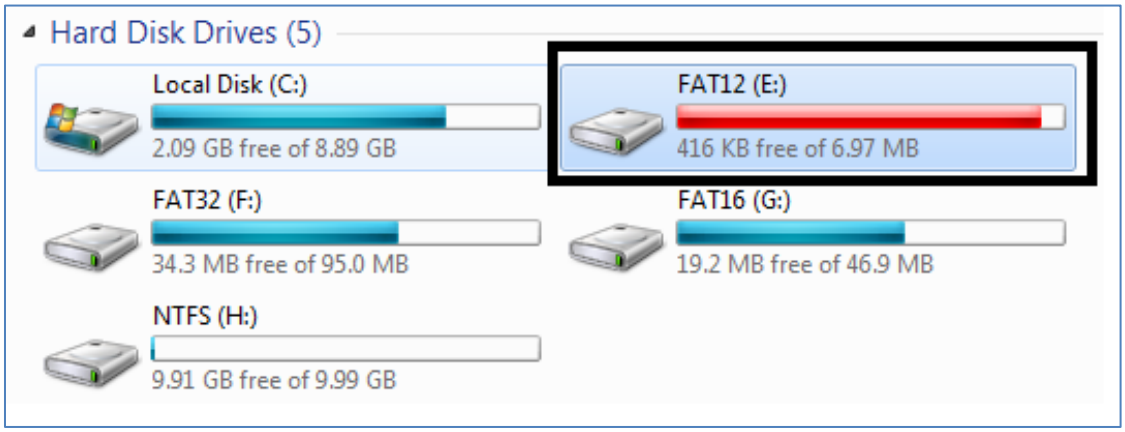
It is critical that a forensic investigator understand the difference between formatting a disk and wiping a disk. If a disk is formatted quickly (Microsoft Windows default), the data is not erased. Rather, the table, such as the File Allocation Table, with the information that points to the area of the disk where the information is stored is "reset". During this task, you will format the file system (quickly), then recover the data.

## 2.1 Formatting File Systems in Windows

1. On the **Windows 7 Machine on the External Network**, click the Start icon in the lower-left corner and then select **Computer.**



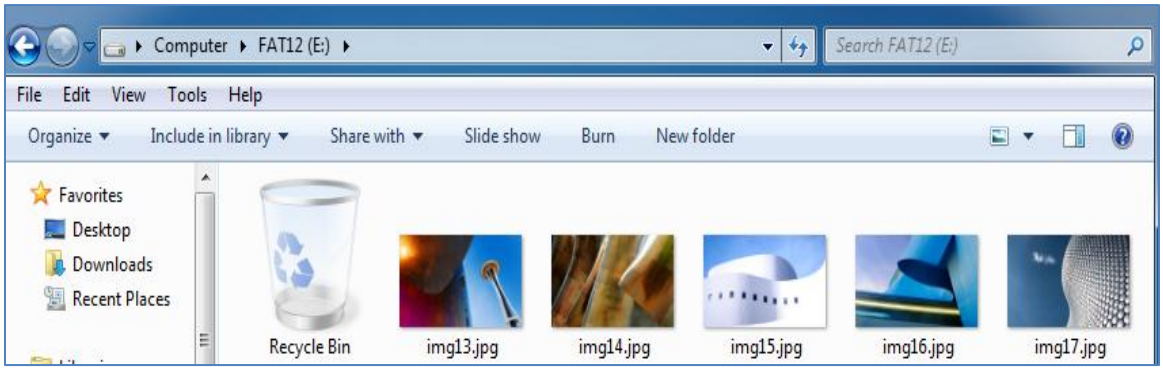

2. Double-click on the **FAT12 (E:)** drive to view the contents of the hard disk.



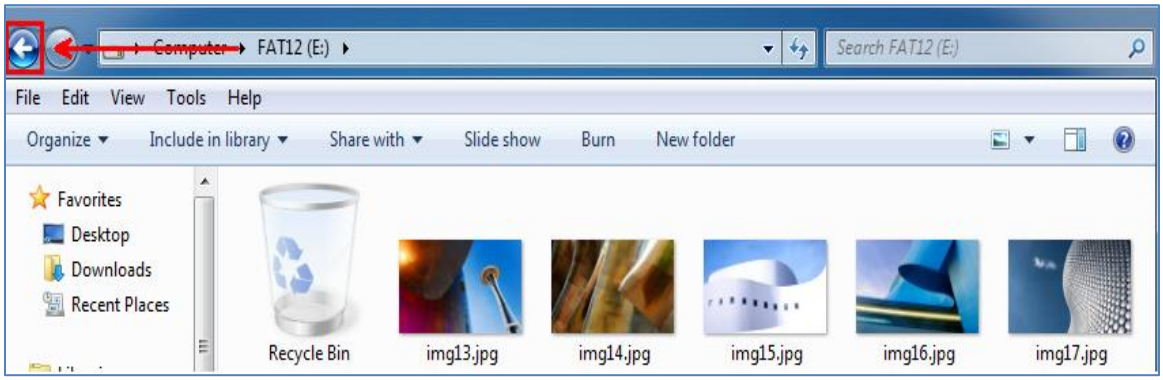
The FAT12 file system is typically used on floppy disks. A FAT12 partition is limited to 32 megabytes. A FAT16 partition can be up to 2 gigabytes and a FAT32 partition can be up to 2 terabytes. (There are workarounds to make large FAT32 partitions.) It is also important to know that a FAT32 volume cannot hold a file that is larger than 4 gigabytes.

| FAT Version Name | Size Limit |
|---|---|
| FAT12 | 32 MB |
| FAT16 | 2 GB |
| FAT32 | 2 TB |

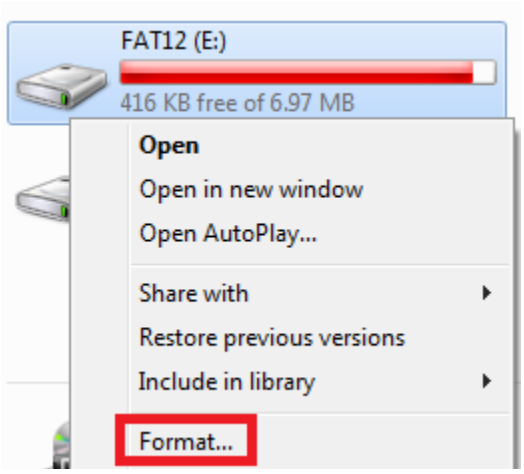
3. View the 5 jpeg files that are present within the FAT12 volume on the system.



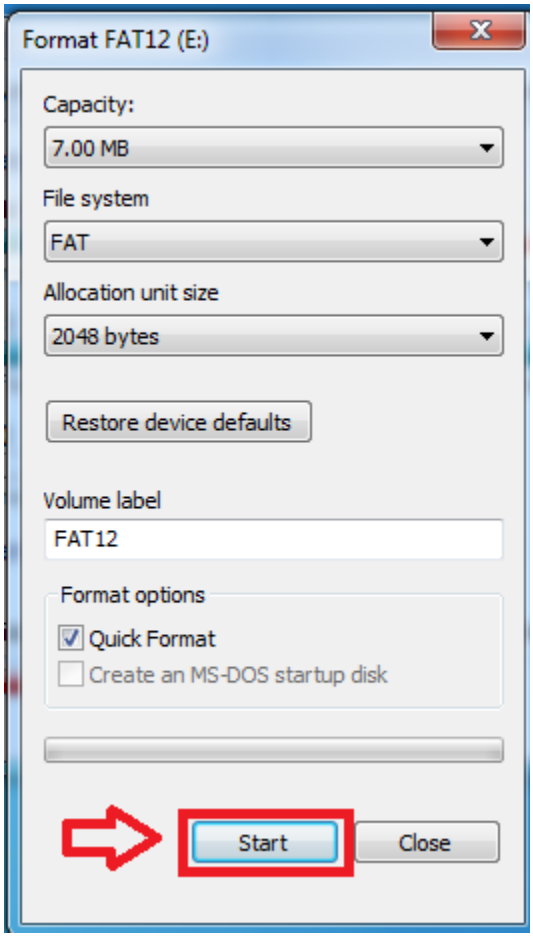

4. Click the **Back** button on the left side of the screen above the word **File**.



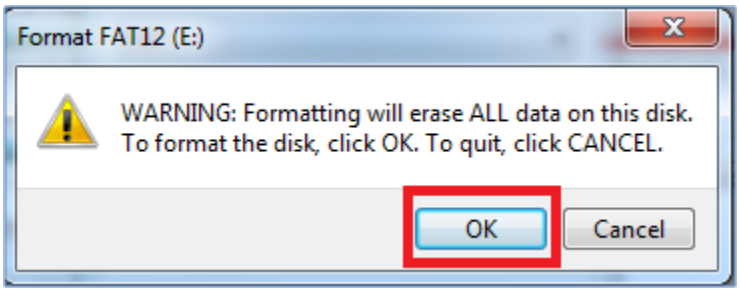
5. Right-click on the FAT12 (E:) drive and select **Format...** on the menu list.



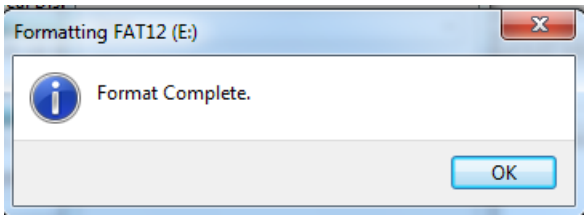

6. Note that the **Quick Format** option is selected. (Default). Click **Start** to format the disk.



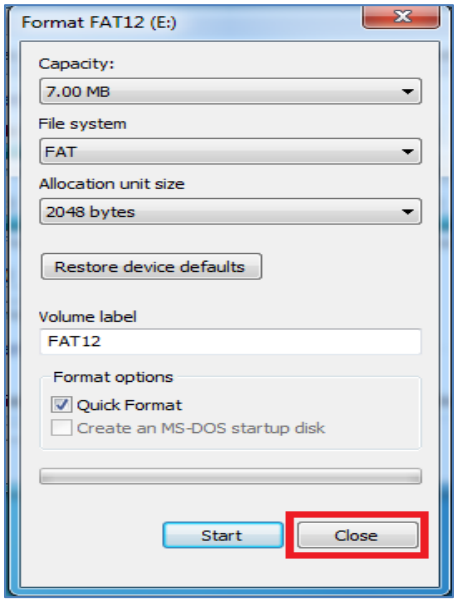
7. Click **OK** when you are warned that ALL data will be erased.



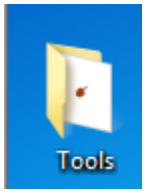

8. Click **OK** after you receive the message that the format is complete.



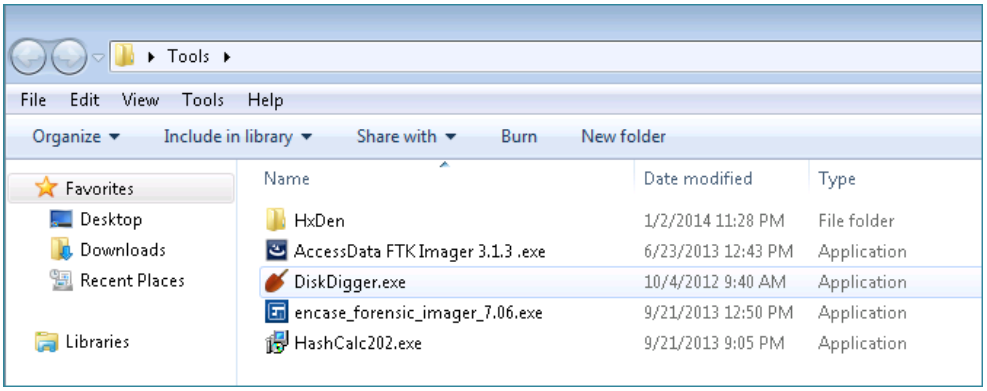

9. Click **Close** to close the format window:



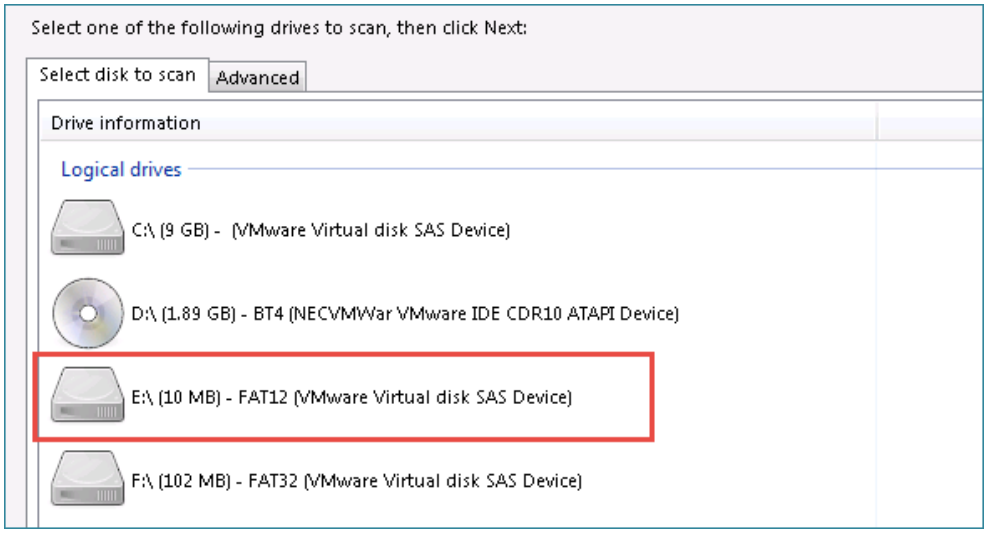

10. Double-click on the **Tools** folder on the desktop.



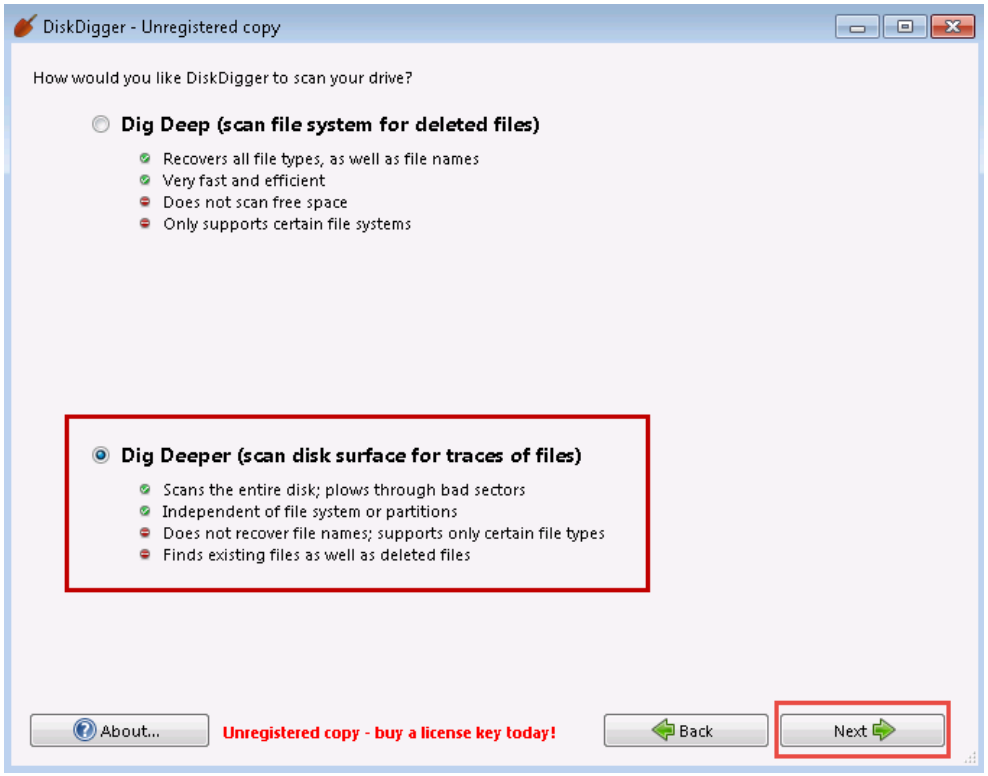
11. Open the DiskDigger® utility by double-click on the **DiskDigger.exe** application. If the DiskDigger 1.5 License Agreement window appears, click **Agree**.



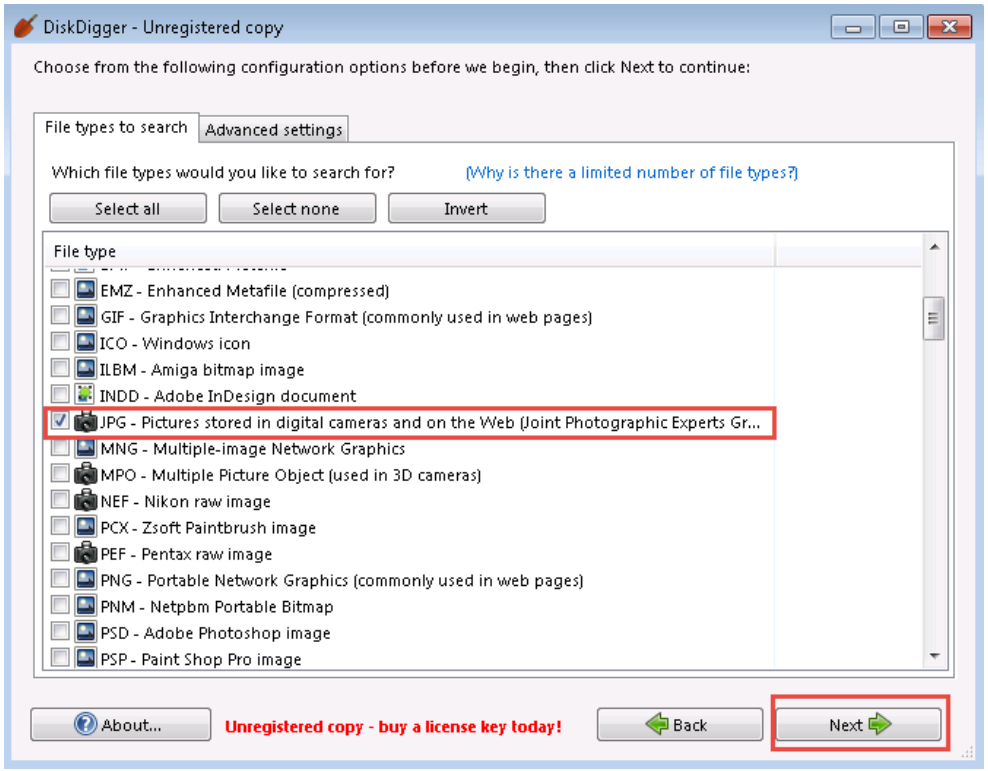

12. Select the **E:\ (10 MB) - Fat12** drive under the Logical drives section. You may have to scroll down to see under Logical Drives. Click **Next.**



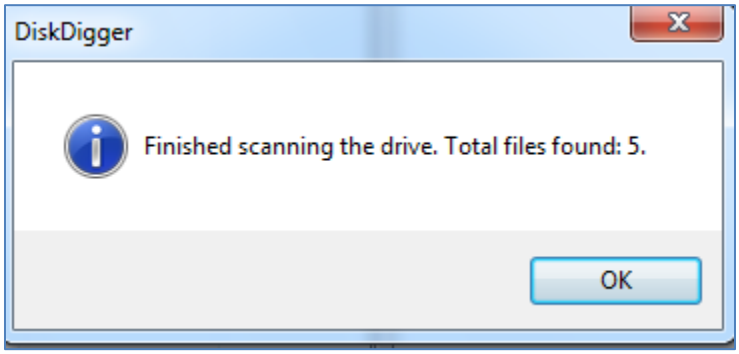
13. Select the Radio Button next to **Dig Deeper** (scan disk surface area for traces of files). Click **Next.**



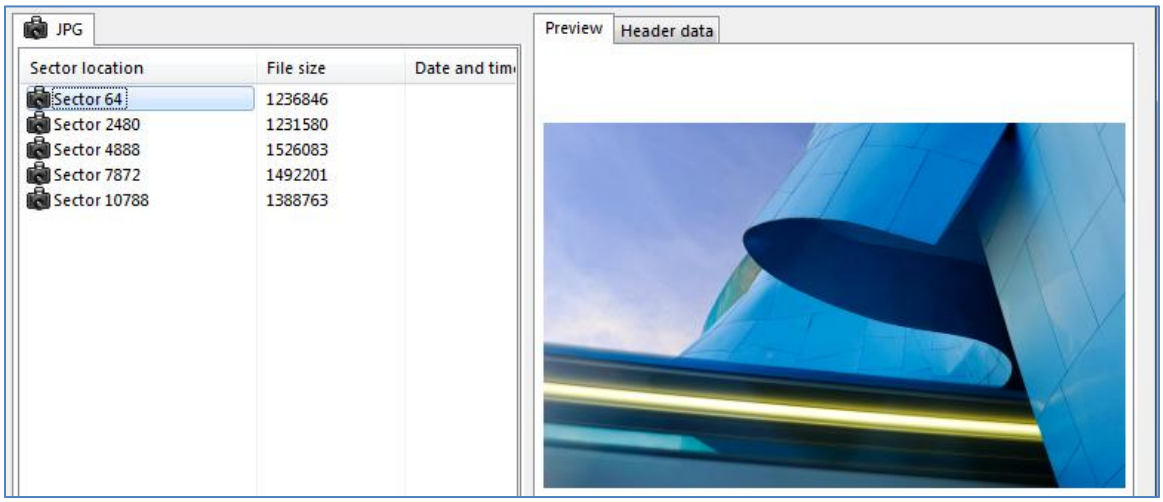

14. Click the **Select none** button. Select the checkbox to the left of **JPG**. Click **Next**.



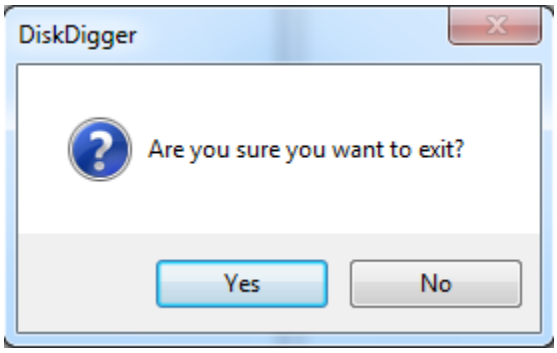
15. Click **OK** to the message box that states, *Finished scanning the drive. Total files found: 5.*




16. Click on **Sector 64** to view the deleted picture. Click on each of the other sector locations listed to see the recovered photos from the FAT12 volume.

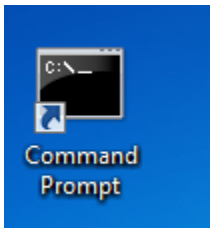



17. Close **DiskDigger**. Answer **Yes** to the question, *are you sure you want to exit?*




While a quick format does not destroy all data, a disk wipe will destroy all data. There are many utilities that can be used to wipe a disk such as Darik's Boot and Nuke (DBAN) disk. You can also wipe disks with the format utility built into Windows

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




19. Type the following command to wipe the FAT12 volume E:
    C:\> **format e: /p:1**

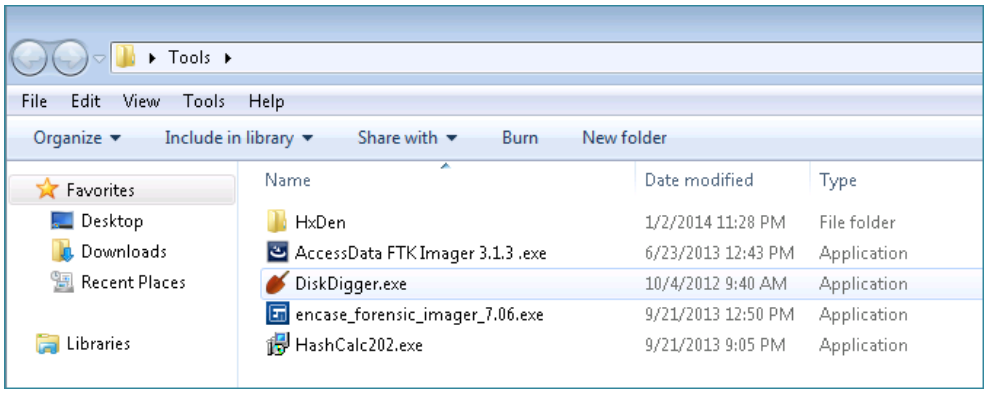
Enter **FAT12** for the current volume label. Click **Y** to Proceed with the Format.

```
C:\>format e: /p:1
The type of the file system is FAT.
Enter current volume label for drive E: FAT12

WARNING, ALL DATA ON NON-REMOVABLE DISK
DRIVE E: WILL BE LOST!
Proceed with Format (Y/N)? y
```

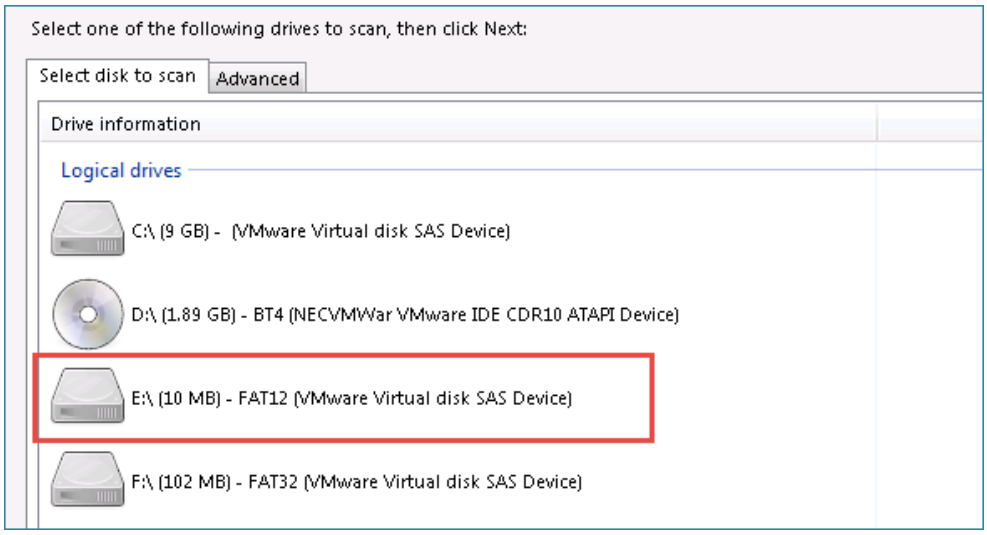
20. Type **FAT12** when asked for the Volume label and press **Enter**.

```
Formatting 7M
Initializing the File Allocation Table (FAT)...
Volume label (11 characters, ENTER for none)? FAT12
Format complete.
       7.0 MB total disk space.
       7.0 MB are available.

        2,048 bytes in each allocation unit.
        3,570 allocation units available on disk.

           12 bits in each FAT entry.

Volume Serial Number is 58C5-B7CB
```

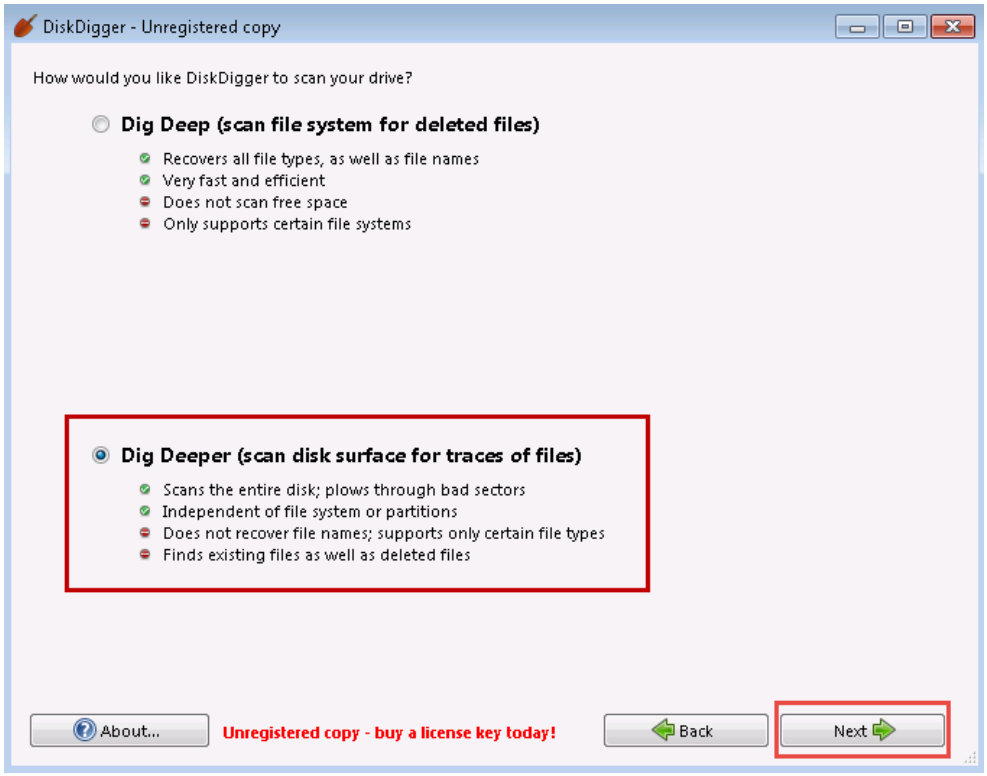
21. Close the Command Prompt window. Open the Tools folder on the desktop and double-click on the **DiskDigger.exe** application again.



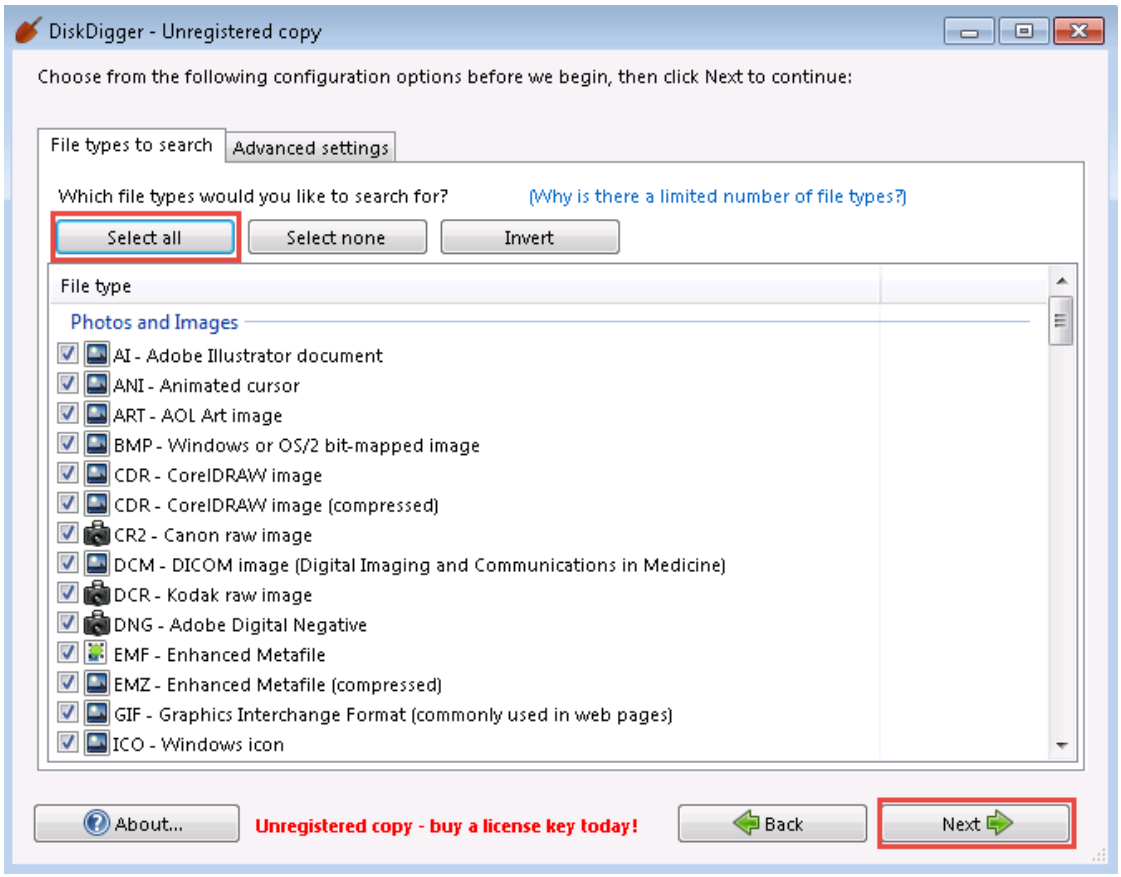
22. Select the **E:\ (10 MB) - Fat12 Drive** under the Logical drives section. Click **Next.**



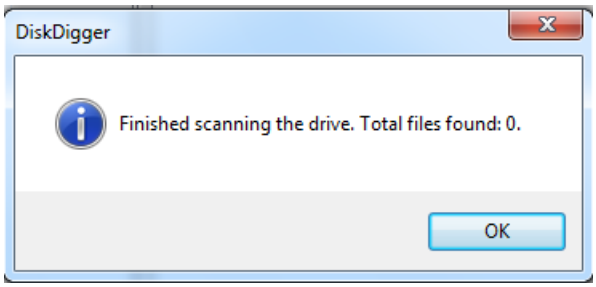

23. Select the Radio Button next to **Dig Deeper** (scan disk surface area for traces of files). Click **Next**.



24. Verify that all file types are selected and then click the **Next** button.




25. Click OK to the message box that states, *Finished scanning the drive. Total files found: 0.*




26. Close the DiskDigger application, other open windows and minimize the Windows 7 Remote PC Viewer.

## 2.2 Conclusion

People can have the misconception that a formatted disk is an erased disk. In this task, we formatted a disk using the default quick format option and received a warning message from the operating system that all data would be lost. However, we were able to recover all of the pictures from the volume using the DiskDigger utility. When a wipe is performed, zeros (or another character) are written to every sector of the disk. After wiping, we were unable to recover any of the data that previously existed.

## 2.3 Discussion Questions

1. Does a quick format really erase all of the data on the disk?
2. When a volume is quick formatted, what exactly is erased?
3. What sort of tools can be used to wipe a disk?
4. What tool can be used to recover data from a disk that was quick formatted?

# 3 Formatting and Wiping Linux File Systems

Many people have experience formatting disks within Microsoft Windows. In contrast, Linux is a robust operating system that allows users to manage and view the status of disks and partitions from the command line. Linux has a large number of built-in disk commands.

## 3.1 Formatting and Wiping in Linux

1. Return to the **BackTrack 5 Desktop** and open a Terminal window.
2. To view the file systems that have been mounted, type the following command:
   root@bt:~#**mount**

```
root@bt:~# mount
/dev/sda1 on / type ext4 (rw,errors=remount-ro)
proc on /proc type proc (rw,noexec,nosuid,nodev)
none on /sys type sysfs (rw,noexec,nosuid,nodev)
none on /sys/fs/fuse/connections type fusectl (rw)
none on /sys/kernel/debug type debugfs (rw)
none on /sys/kernel/security type securityfs (rw)
none on /dev type devtmpfs (rw,mode=0755)
none on /dev/pts type devpts (rw,noexec,nosuid,gid=5,mode=0620)
none on /dev/shm type tmpfs (rw,nosuid,nodev)
none on /var/run type tmpfs (rw,nosuid,mode=0755)
none on /var/lock type tmpfs (rw,noexec,nosuid,nodev)
none on /lib/init/rw type tmpfs (rw,nosuid,mode=0755)
/dev/sdb1 on /mnt/sdb1 type ext2 (rw)
/dev/sdc1 on /mnt/sdc1 type ext3 (rw)
/dev/sdd1 on /mnt/sdd1 type ext4 (rw)
/dev/sde1 on /mnt/sde1 type reiserfs (rw)
vmware-vmblock on /var/run/vmblock-fuse type fuse.vmware-vmblock (rw,nosuid,nodev,default
```

3. View the names of the files on **/dev/sde1** disk by typing:
   root@bt:~#**ls /mnt/sde1**

```
root@bt:~# ls /mnt/sde1
Security_Plus_Lab_01.pdf  Security_Plus_Lab_07.pdf  Security_Plus_Lab_13.pdf
Security_Plus_Lab_02.pdf  Security_Plus_Lab_08.pdf  Security_Plus_Lab_14.pdf
Security_Plus_Lab_03.pdf  Security_Plus_Lab_09.pdf  Security_Plus_Lab_15.pdf
Security_Plus_Lab_04.pdf  Security_Plus_Lab_10.pdf  Security_Plus_Lab_16.pdf
Security_Plus_Lab_05.pdf  Security_Plus_Lab_11.pdf
Security_Plus_Lab_06.pdf  Security_Plus_Lab_12.pdf
```

4. A disk cannot be formatted within Linux when it is currently mounted. To unmount the first partition on the fifth disk, type the following command:
   root@bt:~#**umount /dev/sde1**

```
root@bt:~# umount /dev/sde1
```

5. Type the following command to verify that /dev/sde1 is no longer mounted:
   root@bt:~#**mount | grep /dev/sd**

```
root@bt:~# mount | grep dev/sd
/dev/sda1 on / type ext4 (rw,errors=remount-ro)
/dev/sdb1 on /mnt/sdb1 type ext2 (rw)
/dev/sdc1 on /mnt/sdc1 type ext3 (rw)
/dev/sdd1 on /mnt/sdd1 type ext4 (rw)
```

6. Type the following to format the 5th disk's 1st Partition with the reiserfs file system:
   root@bt:~#**mkfs.reiserfs /dev/sde1**

```
root@bt:~# mkfs.reiserfs /dev/sde1
mkfs.reiserfs 3.6.21 (2009 www.namesys.com)

A pair of credits:
BigStorage  (www.bigstorage.com)  contributes to our general fund
and has done so for quite a long time.

Oleg Drokin was the debugger for  V3 during most of the time that
development,  and was quite  skilled and fast at it.  He wrote  the
optimization of V3.


Guessing about desired format.. Kernel 3.2.6 is running.
Format 3.6 with standard journal
Count of blocks on the device: 131056
Number of blocks consumed by mkreiserfs formatting process: 8215
Blocksize: 4096
Hash function used to sort names: "r5"
Journal Size 8193 blocks (first block 18)
Journal Max transaction length 1024
inode generation number: 0
UUID: c4748930-f0d3-42ef-88d8-128d5512babe
ATTENTION: YOU SHOULD REBOOT AFTER FDISK!
        ALL DATA WILL BE LOST ON '/dev/sde1'!
Continue (y/n):y
```

7. Type **y** and press Enter. You will receive the message that *ReiserFS is successfully created on /dev/sde1*.

```
Initializing journal - 0%....20%....40%....60%....80%....100%
Syncing..ok
ReiserFS is successfully created on /dev/sde1.
```

8. Type the following command to switch into the scalpel directory within /etc.
   root@bt:~#**cd /etc/scalpel**

```
root@bt:~# cd /etc/scalpel
```

9. Type **gedit scalpel.conf**
   root@bt:/etc/scapel# **gedit scalpel.conf**

```
root@bt:/etc/scalpel# gedit scalpel.conf
```

10. Scroll down the file until you find Adobe PDF. Remove the # signs in front of the two pdf lines and select **Save**. Close the file.


11. At the prompt, type **mkdir forensics** to make a directory named forensics:
    root@bt:/etc/scapel# **mkdir forensics**

```
root@bt:/etc/scalpel# mkdir forensics
```

12. Type the following to attempt to recover the PDF files with scalpel:
    root@bt:/etc/scapel# **scalpel /dev/sde -o forensics**

```
root@bt:/etc/scalpel# scalpel /dev/sde -o forensics
Scalpel version 2.0
Written by Golden G. Richard III and Lodovico Marziale.
Multi-core CPU threading model enabled.
Initializing thread group data structures.
Creating threads...
Thread creation completed.

Opening target "/dev/sde"

Image file pass 1/2.
/dev/sde: 100.0% |***************************************|  512.0 MB    00:00 ETA
Allocating work queues...
Work queues allocation complete. Building work queues...
Work queues built.  Workload:
pdf with header "%PDF" and footer "%EOF\x0d" --> 15 files
pdf with header "%PDF" and footer "%EOF\x0a" --> 0 files
Carving files from image.
Image file pass 2/2.
/dev/sde: 100.0% |***************************************|  512.0 MB    00:00 ETA
Processing of image file complete. Cleaning up...
Done.
Scalpel is done, files carved = 15, elapsed  = 3 secs.
```

13. Type the following command to change into the forensics directory:
    root@bt:/etc/scapel# **cd forensics**

```
root@bt:/etc/scalpel# cd forensics/
```

14. Type the following command to change into the pdf-0-0 directory:
    root@bt:/etc/scapel/forensics# **cd pdf-0-0**

```
root@bt:/etc/scalpel/forensics# cd pdf-0-0
```

15. Type the following command to view all of the files in the pdf-0-0 directory:
    root@bt:/etc/scapel/forensics/pdf-0-0**# ls**

```
root@bt:/etc/scalpel/forensics/pdf-0-0# ls
00000000.pdf  00000003.pdf  00000006.pdf  00000009.pdf  00000012.pdf  00000015.pdf
00000001.pdf  00000004.pdf  00000007.pdf  00000010.pdf  00000013.pdf
00000002.pdf  00000005.pdf  00000008.pdf  00000011.pdf  00000014.pdf
```

16. Type the following to open the "deleted" PDF file from the formatted volume:
    root@bt:/etc/scapel/forensics/pdf-0-0# **xpdf 00000000.pdf**


To wipe the disk, the **dd** or **dcfldd** commands can be utilized. A pattern of zeros or other characters can be written to each sector so that data recovery is not possible.

17. Close the PDF. Type the following command to zero out the 5th disk:
    root@bt:/etc/scalpel/forensics/pdf-0-0# **dcfldd if=/dev/zero of=/dev/sde**

```
root@bt:/etc/scalpel/forensics/pdf-0-0# dcfldd if=/dev/zero of=/dev/sde
16384 blocks (512Mb) written.
16385+0 records in
16384+0 records out
```

18. To verify the disk has been wiped with zeros, type the following command:
    root@bt:/etc/scalpel/forensics/pdf-0-0# **xxd /dev/sde**

```
root@bt:/etc/scalpel/forensics/pdf-0-0# xxd /dev/sde
0000000: 0000 0000 0000 0000 0000 0000 0000 0000  ................
0000010: 0000 0000 0000 0000 0000 0000 0000 0000  ................
0000020: 0000 0000 0000 0000 0000 0000 0000 0000  ................
0000030: 0000 0000 0000 0000 0000 0000 0000 0000  ................
0000040: 0000 0000 0000 0000 0000 0000 0000 0000  ................
0000050: 0000 0000 0000 0000 0000 0000 0000 0000  ................
0000060: 0000 0000 0000 0000 0000 0000 0000 0000  ................
0000070: 0000 0000 0000 0000 0000 0000 0000 0000  ................
0000080: 0000 0000 0000 0000 0000 0000 0000 0000  ................
0000090: 0000 0000 0000 0000 0000 0000 0000 0000  ................
00000a0: 0000 0000 0000 0000 0000 0000 0000 0000  ................
00000b0: 0000 0000 0000 0000 0000 0000 0000 0000  ................
00000c0: 0000 0000 0000 0000 0000 0000 0000 0000  ................
00000d0: 0000 0000 0000 0000 0000 0000 0000 0000  ................
00000e0: 0000 0000 0000 0000 0000 0000 0000 0000  ................
00000f0: 0000 0000 0000 0000 0000 0000 0000 0000  ................
0000100: 0000 0000 0000 0000 0000 0000 0000 0000  ................
0000110: 0000 0000 0000 0000 0000 0000 0000 0000  ................
0000120: 0000 0000 0000 0000 0000 0000 0000 0000  ................
0000130: 0000 0000 0000 0000 0000 0000 0000 0000  ................
0000140: 0000 0000 0000 0000 0000 0000 0000 0000  ................
0000150: 0000 0000 0000 0000 0000 0000 0000 0000  ................
```

It may take a long time for the xxd program to scroll through all the disk's zeros.

## 3.2 Conclusion

Simply formatting a partition will not erase all data on the drive. Tools like scalpel will allow users to recover files from a formatted partition. In order to make sure any evidence is wiped from a drive, a pattern of zeros or other characters should be written to the disk. Tools such as dd and dcfldd can be used to wipe a disk to prevent data recovery.

## 3.3 Discussion Questions

1. What is the command to view all of the mounted file systems?
2. How would you unmount the 1st partition on the 5th disk in Linux?
3. What is the command to format the 1st partition on the 5th disk with ReiserFS?
4. What Linux command allows you to verify that the drive has been zeroed out?

## References


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

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

3. xxd:
   http://linuxcommand.org/man_pages/xxd1.html

4. dcfldd:
   http://dcfldd.sourceforge.net/

5. BackTrack Linux:
   http://www.backtrack-linux.org/