DIGITAL FORENSICS LAB SERIES

Lab 4: Drive Letter Assignments in Linux

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.

Contents

Introduction

This lab includes the following tasks:

1. Examining Linux Drive Letter Assignments and Mounting Drives
2. Creating Primary and Extended Partitions in Linux
3. Formatting Disks in Linux and Utilizing the Storage

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.

The Linux operating system is often used to acquire drives. An incident responder can boot to a Live CD and mount and image disks. It is very important for the incident responder to understand Linux drive letter assignments and partition numbering. Without this understanding, they could accidently delete the drive they are acquiring.

fdisk – This Linux command allows users to view disks and partitions. This command can be utilized to create and delete partitions, as well as change the partition id of a disk.

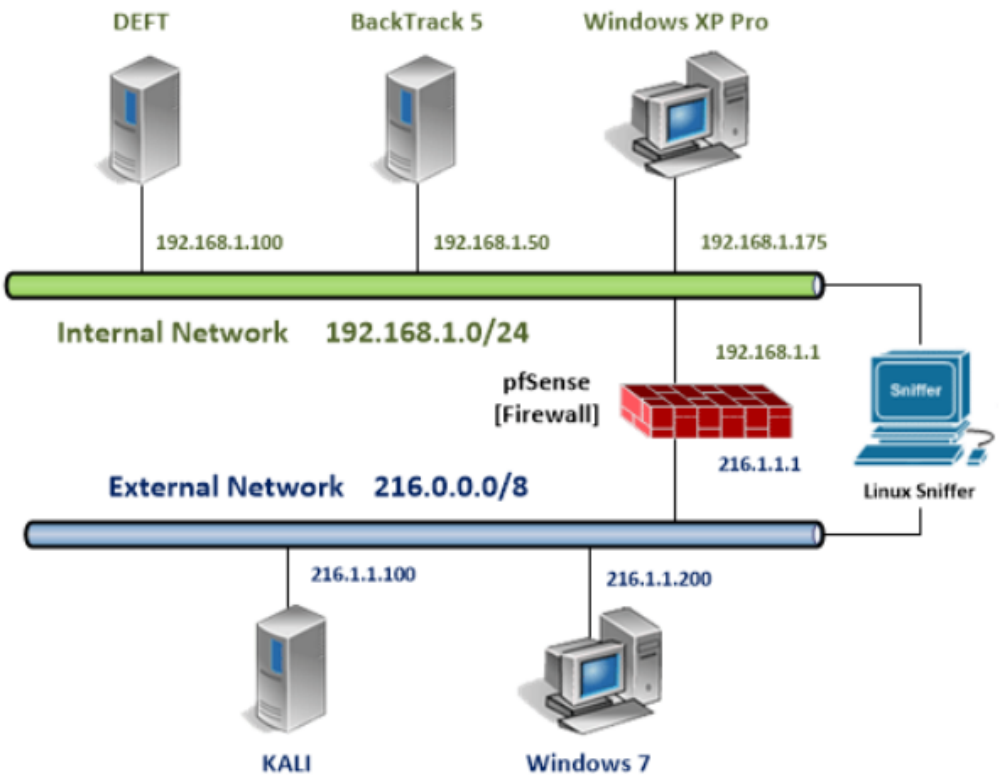
mount – This Linux command allows users to view which disks are currently mounted, as well as mount local or remote disks. Disks can be mounted as read-only in Linux.

umount – This Linux command will allow users to unmount disks currently mounted.

mkfs – This Linux command allows users to format unmounted partitions with various file systems including FAT, NTFS, EXT2, EXT3, EXT4, and the ReiserFS.

df – The Linux df command will display the available disk space on the system's drives.

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 Linux Drive Letter Assignments and Mounting Drives

In the Windows operating system, when disks are added to the system you can never be 100% confident which drive letter will be assigned to a disk. When a disk is added to a Linux system, you can be confident that the next available drive letter will be assigned to the disk. For this reason, Linux is often utilized by computer forensic examiners. Not only does Linux provide reliable results, it allows you to mount disks as read-only. Contamination of media can be avoided if disks are mounted as read-only.

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

1.1 Viewing and Mounting Disks

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

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

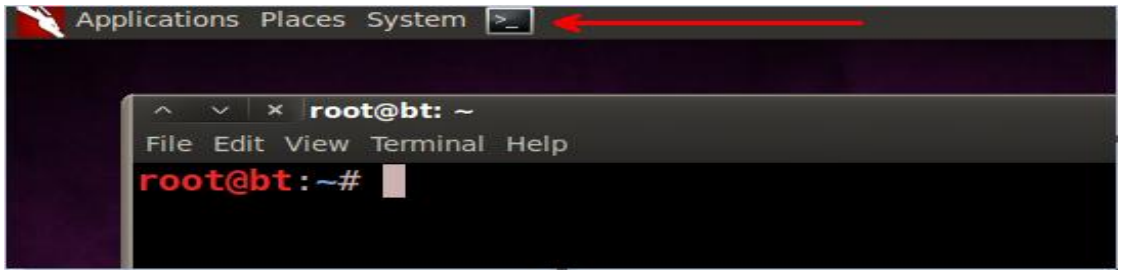
```
BackTrack 5 R3 - 32 Bit bt tty1
bt login: root
Password: toor
Last login: Tue Aug 13 22:37:12 EDT 2013 on tty1
Linux bt 3.2.6 #1 SMP Fri Feb 17 10:40:05 EST 2012 i686 GNU/Linux

 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. 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 in the BackTrack 5 R3 Internal Machine.



4. To view the disks and partitions on a Linux system, type the following command:
   root@bt:~**#fdisk -l**

Be aware that the command includes a lowercase "L", not the number "1".

```
root@bt:~# fdisk -l

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

Disk /dev/sdb: 10 MB, 10485760 bytes
64 heads, 32 sectors/track, 10 cylinders
Units = cylinders of 2048 * 512 = 1048576 bytes
Sector size (logical/physical): 512 bytes / 512 bytes
I/O size (minimum/optimal): 512 bytes / 512 bytes
Disk identifier: 0x7fcc4978

   Device Boot      Start         End      Blocks   Id  System
/dev/sdb1               1          10       10224   83  Linux

Disk /dev/sdd: 4 MB, 4194304 bytes
64 heads, 32 sectors/track, 4 cylinders
Units = cylinders of 2048 * 512 = 1048576 bytes
Sector size (logical/physical): 512 bytes / 512 bytes
I/O size (minimum/optimal): 512 bytes / 512 bytes
Disk identifier: 0xeaee9db8

   Device Boot      Start         End      Blocks   Id  System
/dev/sdd1               1           4        4080   83  Linux

Disk /dev/sdc: 5 MB, 5242880 bytes
64 heads, 32 sectors/track, 5 cylinders
Units = cylinders of 2048 * 512 = 1048576 bytes
Sector size (logical/physical): 512 bytes / 512 bytes
I/O size (minimum/optimal): 512 bytes / 512 bytes
Disk identifier: 0x204a67a0

   Device Boot      Start         End      Blocks   Id  System
/dev/sdc1               1           5        5104   83  Linux

Disk /dev/sde: 536 MB, 536870912 bytes
64 heads, 32 sectors/track, 512 cylinders
Units = cylinders of 2048 * 512 = 1048576 bytes
Sector size (logical/physical): 512 bytes / 512 bytes
I/O size (minimum/optimal): 512 bytes / 512 bytes
Disk identifier: 0xae83374d

   Device Boot      Start         End      Blocks   Id  System
/dev/sde1               1         512      524272   83  Linux
```

The chart below explains how the disks are arranged alphabetically.

Disk Number	Device Name and Partition Number
1	**/dev/sd**a
2	**/dev/sd**b
3	**/dev/sd**c
4	**/dev/sd**d
5	**/dev/sd**e

If another (sixth) disk were added to the system, it would be assigned the drive letters sdf. The chart below shows the drive letters that would be assigned as disks are added:

Disk Number	Device Name and Partition Number
6	**/dev/sd**f
7	**/dev/sd**g
26	**/dev/sd**z
27	**/dev/sd**aa
54	**/dev/sd**az
55	**/dev/sd**ba
81	**/dev/sd**cb
576	**/dev/sd**zz

Under previous Linux kernel versions, drive letter assignments hda-hdd were assigned for IDE drives. Under the most recent versions of the Linux kernel, the sd designation is used, even for IDE drives. Up to 576 drives can be supported using the Linux sd designation.

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

Be aware that the command includes a lowercase "L", not the number "1".

```
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
```

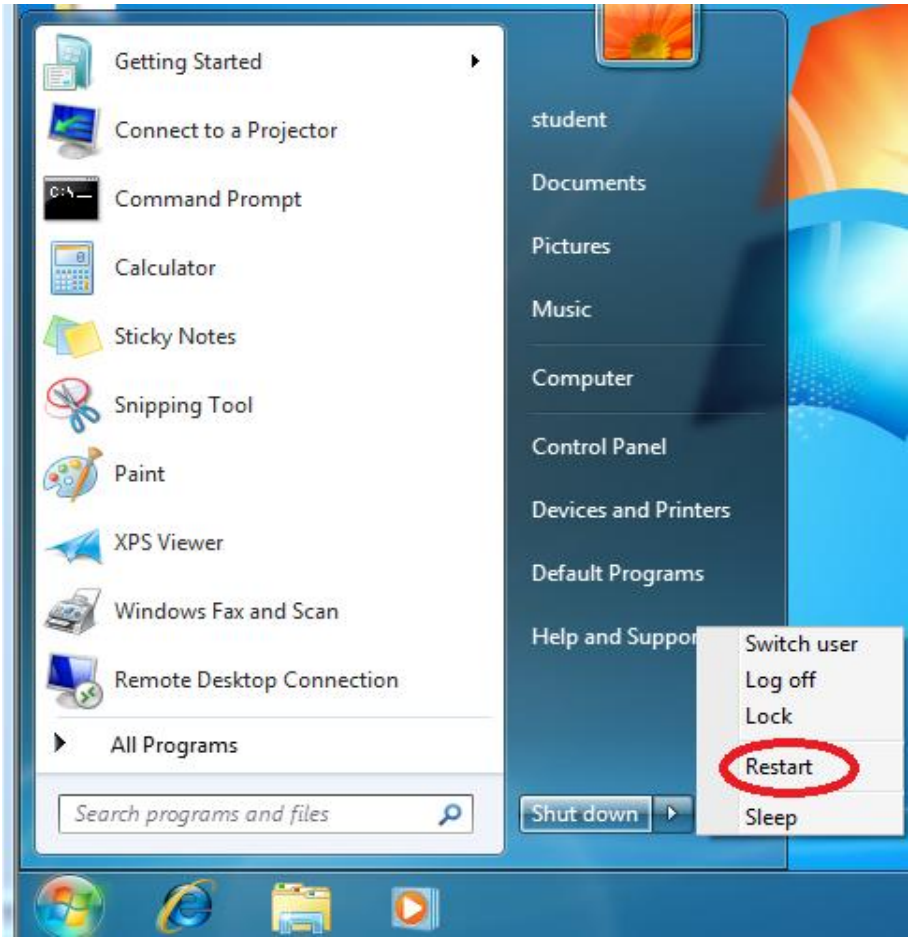
The table below describes partition numbering within the Linux operating system. Any of the partitions numbered 1-4 can be primary or extended. There can be up to four primary partitions, but there can only be one extended partition. Partitions numbered 5 and higher are logical drives that are contained within the extended partition.

Partition Number	Device Name and Partition Number
1	Can be Primary or Extended
2	Can be Primary or Extended
Root	Can be Primary or Extended
4	Can be Primary or Extended
5 and up	Logical Drives within an Extended Partition

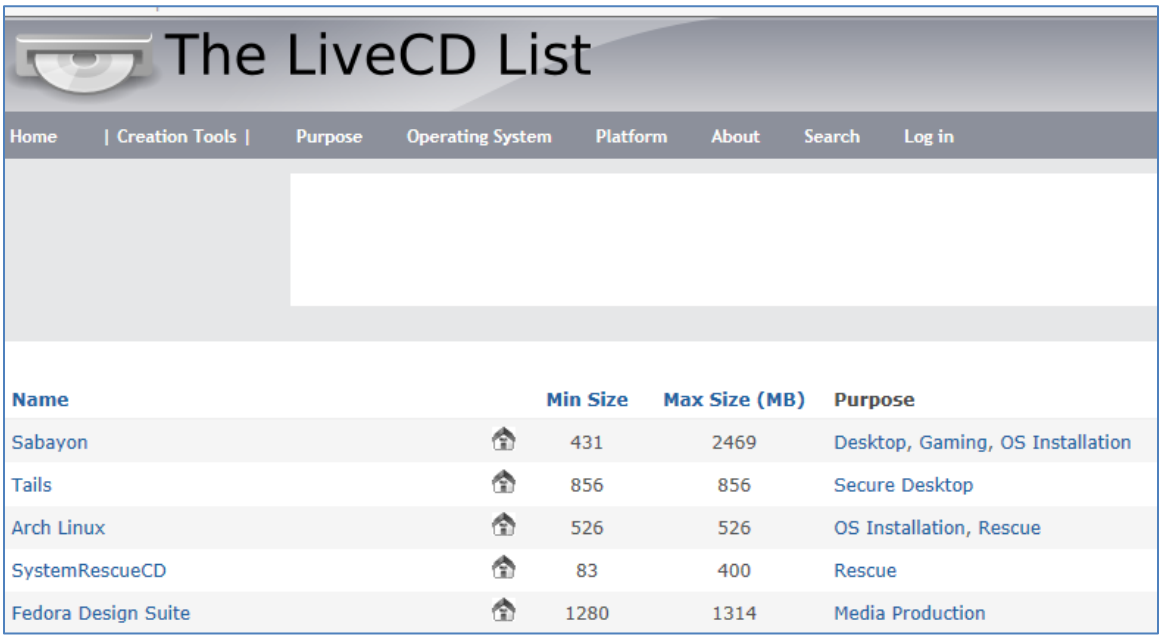
This partitioning layout is for disks using the Master Boot Record (MBR), not for disks utilizing GUID Partition Table (GPT), which allows for 128 primary partitions.

6. Log into the **Windows 7 External Machine** by clicking on the **Windows 7** icon on the topology.
7. If required, enter the username, **student**.
8. Type in the password, **password,** and press **Enter** to log in.

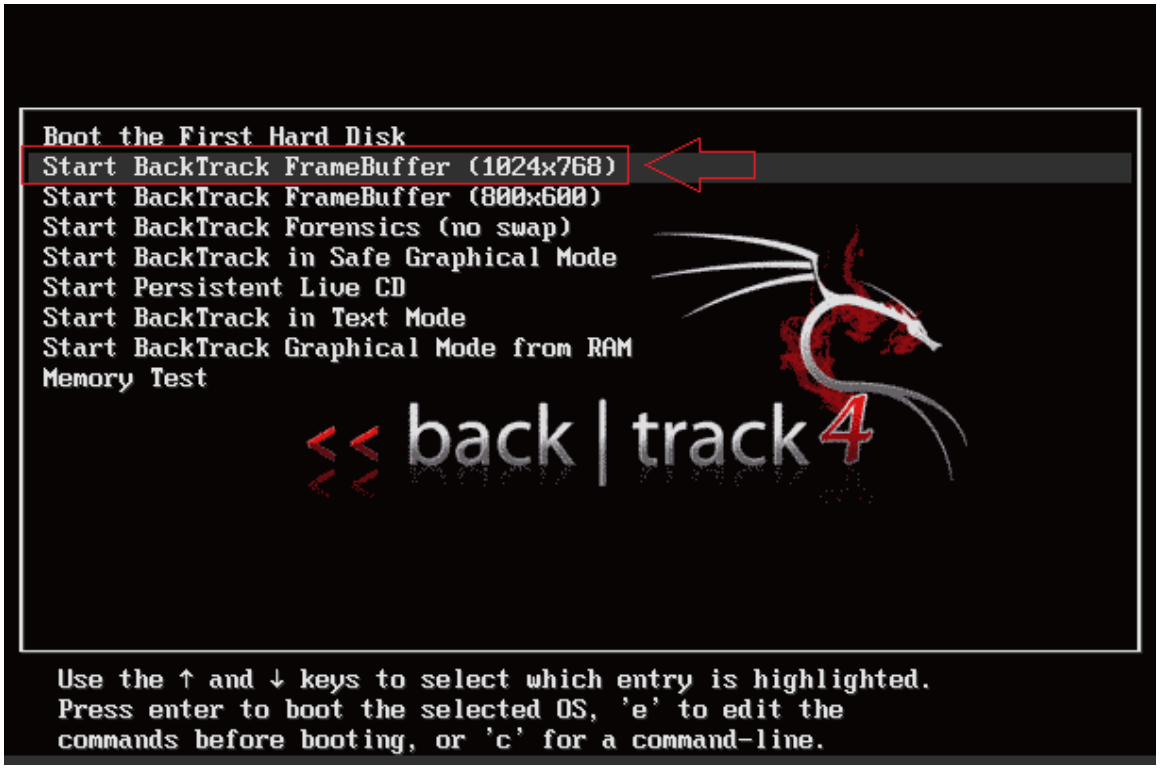
9. Click Start, click the arrow to the right of Shut down and click **Restart.**



The machine will be booting to a Linux Live DVD Distribution. A Live CD is an operating system that runs completely in Random Access Memory, or RAM. The website livecdlist.com has a large list of Linux Live CDs as well as download links.



10. Choose the second choice listed in the Boot menu. Press **Enter.**

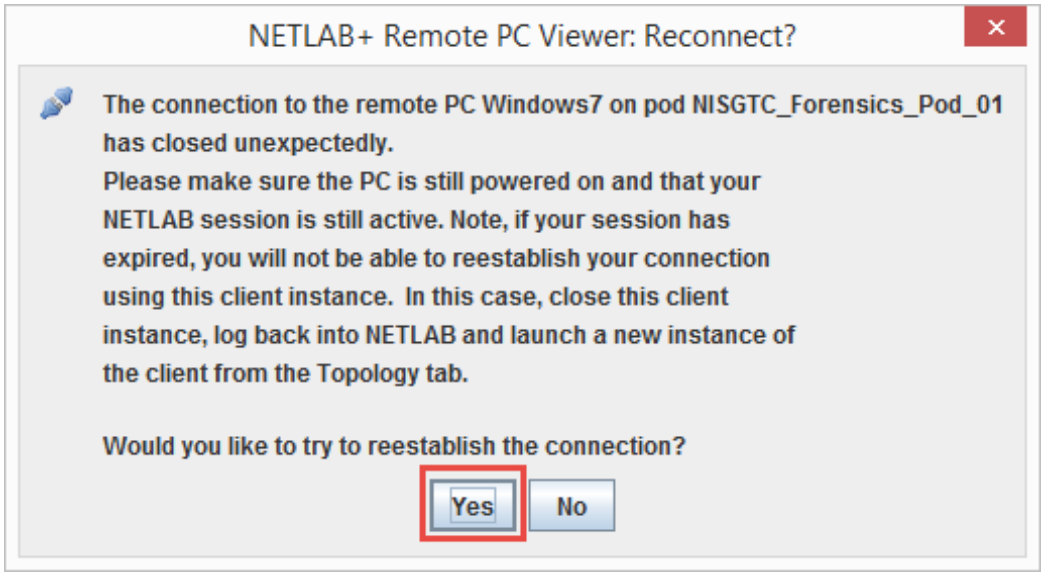


11. Type the following command to initialize the Graphical User Interface (GUI): root@bt:~# **startx**

```
BackTrack 4 R2 (CodeName Nemesis) Security Auditing

For more information visit: http://www.backtrack-linux.org/
root@bt:~# startx
```

12. If the PC viewer loses its connection, click **Yes** to reestablish the connection to the PC.



13. Open a terminal on the Linux system by clicking on the black square icon (to the right of Firefox) in the task bar in the bottom.

14. Type the following to display the disks and their corresponding partitions:
    root@bt:~# **fdisk –l | grep sd**

```
root@bt:~# fdisk -l | grep sd
Disk /dev/sda: 9663 MB, 9663676416 bytes
/dev/sda1   *           1          13      102400    7  HPFS/NTFS
/dev/sda2              13        1175     9332736    7  HPFS/NTFS
Disk /dev/sdb: 10 MB, 10485760 bytes
/dev/sdb1               1           2        7168    1  FAT12
Disk /dev/sdc: 106 MB, 106954752 bytes
/dev/sdc1               1          64      101376    b  W95 FAT32
Disk /dev/sdd: 10.7 GB, 10737418240 bytes
/dev/sdd1               1        1306    10482688    7  HPFS/NTFS
```

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

```
root@bt:~# mount
tmpfs on /lib/init/rw type tmpfs (rw,nosuid,mode=0755)
/proc on /proc type proc (rw,noexec,nosuid,nodev)
sysfs on /sys type sysfs (rw,noexec,nosuid,nodev)
varrun on /var/run type tmpfs (rw,nosuid,mode=0755)
varlock on /var/lock type tmpfs (rw,noexec,nosuid,nodev,mode=1777)
udev on /dev type tmpfs (rw,mode=0755)
tmpfs on /dev/shm type tmpfs (rw,nosuid,nodev)
devpts on /dev/pts type devpts (rw,noexec,nosuid,gid=5,mode=620)
rootfs on / type rootfs (rw)
fusectl on /sys/fs/fuse/connections type fusectl (rw,relatime)
/dev/hdc on /media/cdrom0 type iso9660 (ro,noatime)
/dev/loop0 on /rofs type squashfs (ro,noatime)
tmpfs on /tmp type tmpfs (rw,nosuid,nodev)
```

None of the disks are currently mounted. The fact that some Live CD/DVD distributions do not automatically mount disks makes them desirable to people imaging disks. If a disk is automatically mounted as read/write, and the disk is written to, the evidence could be changed resulting in contamination of the disk. Linux Live CD/DVD distributions such as HELIX and some versions of BackTrack do not automatically mount disks.

16. Type the following to make a directory called sda2 in the mnt directory.
    root@bt:~# **mkdir /mnt/sda2**

```
root@bt:~# mkdir  /mnt/sda2
```

Next, we will mount the sda2 partition to the /mnt/sda2 directory. The partition will be mounted as read-only by adding the ro option to the mount command.

17. Type the following command to launch the GParted utility on the system:
    root@bt:~# **mount –o ro /dev/sda2 /mnt/sda2**

```
root@bt:~# mount -o ro  /dev/sda2  /mnt/sda2/
```

18. Type the following command to view the newly mounted partition:
    root@bt:~# **mount**

```
root@bt:~# mount
tmpfs on /lib/init/rw type tmpfs (rw,nosuid,mode=0755)
/proc on /proc type proc (rw,noexec,nosuid,nodev)
sysfs on /sys type sysfs (rw,noexec,nosuid,nodev)
varrun on /var/run type tmpfs (rw,nosuid,mode=0755)
varlock on /var/lock type tmpfs (rw,noexec,nosuid,nodev,mode=1777)
udev on /dev type tmpfs (rw,mode=0755)
tmpfs on /dev/shm type tmpfs (rw,nosuid,nodev)
devpts on /dev/pts type devpts (rw,noexec,nosuid,gid=5,mode=620)
rootfs on / type rootfs (rw)
fusectl on /sys/fs/fuse/connections type fusectl (rw,relatime)
/dev/hdc on /media/cdrom0 type iso9660 (ro,noatime)
/dev/loop0 on /rofs type squashfs (ro,noatime)
tmpfs on /tmp type tmpfs (rw,nosuid,nodev)
/dev/sda2 on /mnt/sda2 type fuseblk (ro,nosuid,nodev,allow_other,blksize=4096)
```

The ro indicates that the /dev/sda2 partition is mounted as read-only.

19. List all of the files on that partition by typing the following command:
    root@bt:~# **ls /mnt/sda2**

```
root@bt:~# ls /mnt/sda2
autoexec.bat            pagefile.sys   Program Files   System Volume Information
config.sys              PerfLogs       Recovery        Users
Documents and Settings  ProgramData    $Recycle.Bin    Windows
```

This is the C: drive of the Windows 7 system. Hidden files and folder are displayed.

20. Try to write to the partition by typing the following command:
    root@bt:~# **ifconfig > /mnt/sda2/if.txt**

```
root@bt:~# ifconfig > /mnt/sda2/if.txt
bash: /mnt/sda2/if.txt: Read-only file system
```

You should receive the message indicating it is a read-only file system.

21. You can unmount the disk by typing the following command:
    root@bt:~# **umount /dev/sda2**

```
root@bt:~# umount /dev/sda2
```

22. Type the mount command again to verify that the disk is no longer mounted:
    root@bt:~# **mount**

```
root@bt:~# mount
tmpfs on /lib/init/rw type tmpfs (rw,nosuid,mode=0755)
/proc on /proc type proc (rw,noexec,nosuid,nodev)
sysfs on /sys type sysfs (rw,noexec,nosuid,nodev)
varrun on /var/run type tmpfs (rw,nosuid,mode=0755)
varlock on /var/lock type tmpfs (rw,noexec,nosuid,nodev,mode=1777)
udev on /dev type tmpfs (rw,mode=0755)
tmpfs on /dev/shm type tmpfs (rw,nosuid,nodev)
devpts on /dev/pts type devpts (rw,noexec,nosuid,gid=5,mode=620)
rootfs on / type rootfs (rw)
fusectl on /sys/fs/fuse/connections type fusectl (rw,relatime)
/dev/hdc on /media/cdrom0 type iso9660 (ro,noatime)
/dev/loop0 on /rofs type squashfs (ro,noatime)
tmpfs on /tmp type tmpfs (rw,nosuid,nodev)
```

1.2 Conclusion

The fdisk command can be used to display the disks and partitions on a system. Linux supports up to 576 drives with the sd naming convention (sda –sdzz). A disk can have up to four primary partitions or 3 primary partitions and one extended partition. Logical drives, which exist in the extended partition, use numbers 5 and higher. Disks can be mounted as read-only in Linux. A user can boot to a Linux Live DVD and mount disks.

1.3 Discussion Questions

1. What command will allow you to view disks and partitions in Linux?
2. What is a Linux Live CD?
3. Provide at least one example of a Linux Live CD that does not automount.
4. What Linux command is used to unmount a disk?

2 Creating Primary and Extended Partitions in Linux

Disks in Linux are usually partitioned from the command line, although they can be partitioned with a GUI tool such as GParted. During this task, you will create primary and extended partitions, as well as logical drives within the extended partition. All of the partitions of a disk should be unmounted, prior to changing the partition layout.

2.1 Formatting File Systems in Windows

1. On the **Windows 7** machine booted to BackTrack 4, type the following command to verify that sdd is not mounted:
   root@bt:~# **mount**

```
root@bt:~# mount
tmpfs on /lib/init/rw type tmpfs (rw,nosuid,mode=0755)
/proc on /proc type proc (rw,noexec,nosuid,nodev)
sysfs on /sys type sysfs (rw,noexec,nosuid,nodev)
varrun on /var/run type tmpfs (rw,nosuid,mode=0755)
varlock on /var/lock type tmpfs (rw,noexec,nosuid,nodev,mode=1777)
udev on /dev type tmpfs (rw,mode=0755)
tmpfs on /dev/shm type tmpfs (rw,nosuid,nodev)
devpts on /dev/pts type devpts (rw,noexec,nosuid,gid=5,mode=620)
rootfs on / type rootfs (rw)
fusectl on /sys/fs/fuse/connections type fusectl (rw,relatime)
/dev/hdc on /media/cdrom0 type iso9660 (ro,noatime)
/dev/loop0 on /rofs type squashfs (ro,noatime)
tmpfs on /tmp type tmpfs (rw,nosuid,nodev)
```

2. Type the following command to partition the fourth disk:
   root@bt:~# **fdisk /dev/sdd**

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

The number of cylinders for this disk is set to 1305.
There is nothing wrong with that, but this is larger than 1024,
and could in certain setups cause problems with:
1) software that runs at boot time (e.g., old versions of LILO)
2) booting and partitioning software from other OSs
   (e.g., DOS FDISK, OS/2 FDISK)

Command (m for help):
```

Ignore the message regarding the number of cylinders for the disk.

3. Type **m** to display the help menu and display all available fdisk options:
   Command (m for help): **m** (press the Enter key following each command)

```
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)
```

4. To delete the existing partition, type: **d**

```
Command (m for help): d
```

5. To add a new partition to the selected disk, type: **n**

```
Command (m for help): n
```

6. When you are asked to add an extended or primary partition, type: **p**

```
Command action
   e   extended
   p   primary partition (1-4)
p
```

7. For the partition number of the primary partition, type the number **1**

```
Partition number (1-4): 1
```

8. For the first cylinder, press Enter. (The value will default to 1.)

```
First cylinder (1-1958, default 1):
Using default value 1
Last cylinder, +cylinders or +size{K,M,G} (1-1958, default 1958):
```

9. For the last cylinder, type 500 and then press Enter.

```
Last cylinder, +cylinders or +size{K,M,G} (1-1958, default 1958): 500
```

10. To change the partition type id, type the following command:
    Command (m for help): **t**

```
Command (m for help): t
```

11. To list the hexadecimal codes of all of the partition types, type the following:
    Hex code (type L to list codes): **L**

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

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

12. In the next step, we will change the partition type to New Technology File System (NTFS). Type **7** then press Enter to change the system type of partition type to (HPFS/NTFS).
    Hex code (type L to list codes): **7**

```
Hex code (type L to list codes): 7
Changed system type of partition 1 to 7 (HPFS/NTFS)
```

13. To print the partition table and verify you have one partition, type: **p**
    Command (m for help): **p**

```
Command (m for help): p

Disk /dev/sdd: 10.7 GB, 10737418240 bytes
255 heads, 63 sectors/track, 1305 cylinders
Units = cylinders of 16065 * 512 = 8225280 bytes
Disk identifier: 0xab96e0e5

   Device Boot      Start         End      Blocks   Id  System
/dev/sdd1               1         500     4016218+   7  HPFS/NTFS
```

14. To add a new partition to the selected disk, type the following command:
    Command (m for help): **n**

```
Command (m for help): n
```

15. When you are asked to add an extended or primary partition, type: **p**

```
Command action
   e   extended
   p   primary partition (1-4)
p
```

16. For the partition number of the primary partition, type the number: **2**

```
Partition number (1-4): 2
```

17. For the first cylinder, press Enter. (The value will default to 501.)

```
First cylinder (501-1305, default 501):
Using default value 501
```

18. For the last cylinder, type **1000** and then press Enter.

```
Last cylinder, +cylinders or +size{K,M,G} (501-1305, default 1305): 1000
```

19. To change the partition type id, type the following command:
    Command (m for help): **t**

```
Command (m for help): t
```

20. Type the following to select the partition whose type you are changing:
    Partition number (1-4): **2**

```
Partition number (1-4): 2
```

21. To list the hexadecimal codes of all of the partition types, type the following:
    Hex code (type L to list codes): **L**

```
Session  Edit  View  Bookmarks  Settings  Help

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

Shell
```

22. In the next step, we will change the partition type to FAT (File Allocation Table)
    Type **b** to change the system type of partition type to FAT32.
    Hex code (type L to list codes): **b**

```
Changed system type of partition 2 to b (W95 FAT32)
```

23. To print the partition table and verify you have two partitions, type: **p**
    Command (m for help): **p**

```
   Device Boot      Start         End      Blocks   Id  System
/dev/sdd1               1         500     4016218+   7  HPFS/NTFS
/dev/sdd2             501        1000     4016250    b  W95 FAT32
```

24. To add a new partition to the selected disk, type the following command:
    Command (m for help): **n**

```
Command (m for help): n
```

25. When you are asked to add an extended or primary partition, type: **e**

```
Command action
   e   extended
   p   primary partition (1-4)
e
```

26. For the partition number of the primary partition, type the number: **3**

```
Partition number (1-4): 3
```

27. For the first cylinder, press **Enter**. (The value will default to 1001.)

```
First cylinder (1001-1305, default 1001):
Using default value 1001
```

28. For the last cylinder, press **Enter** to use the default value (remainder of disk).

```
Last cylinder, +cylinders or +size{K,M,G} (1001-1958, default 1958):
Using default value 1958
```

29. To print the partition table and verify you have three partitions, type p:
    Command (m for help): **p**

```
Command (m for help): p

Disk /dev/sdd: 16.1 GB, 16106127360 bytes
255 heads, 63 sectors/track, 1958 cylinders
Units = cylinders of 16065 * 512 = 8225280 bytes
Disk identifier: 0xab96e0e5

   Device Boot      Start         End      Blocks   Id  System
/dev/sdd1               1         500     4016218+   7  HPFS/NTFS
/dev/sdd2             501        1000     4016250    b  W95 FAT32
/dev/sdd3            1001        1958     7695135    5  Extended
```

Next, we will create a logical drive. Logical drives, which start at number 5, exist within the extended partition. You can have multiple logical drives within an extended partition.

30. To add a new partition to the selected disk, type the following command:
    Command (m for help): **n**

```
Command (m for help): n
```

31. When you are asked to add a logical or primary partition, type **l**

```
Command action
   l   logical (5 or over)
   p   primary partition (1-4)
l
```

32. For the first cylinder, press **Enter**. (The value will default to **1001**.)

```
First cylinder (1001-1958, default 1001): 1001
```

33. For the last cylinder, type **1002**.

```
Last cylinder, +cylinders or +size{K,M,G} (1001-1958, default 1958): 1002
```

34. To change the partition type id, type the following command:
    Command (m for help): **t**

```
Command (m for help): t
```

35. Type the following to select the partition whose type you are changing:
    Partition number (1-5): **5**

```
Partition number (1-5): 5
```

36. To list the hexadecimal codes of all of the partition types, type the following:
    Hex code (type L to list codes): **L**

```
Session   Edit   View   Bookmarks   Settings   Help

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

37. Type **1** to change the system type of partition type to FAT12.
    Hex code (type L to list codes): **1**

```
Hex code (type L to list codes): 1
Changed system type of partition 5 to 1 (FAT12)
```

38. To print the partition table and verify your disk structure, type the following:
    Command (m for help): **p**

```
Disk /dev/sdd: 16.1 GB, 16106127360 bytes
255 heads, 63 sectors/track, 1958 cylinders
Units = cylinders of 16065 * 512 = 8225280 bytes
Disk identifier: 0xab96e0e5

   Device Boot      Start         End      Blocks   Id  System
/dev/sdd1               1         500     4016218+   7  HPFS/NTFS
/dev/sdd2             501        1000     4016250    b  W95 FAT32
/dev/sdd3            1001        1958     7695135    5  Extended
/dev/sdd5            1001        1002       16033+   1  FAT12
```

39. To save the changes written to the partition table, type the following command:
    Command (m for help): **w**

```
Command (m for help): w
The partition table has been altered!

Calling ioctl() to re-read partition table.

WARNING: If you have created or modified any DOS 6.x
partitions, please see the fdisk manual page for additional
information.
Syncing disks.
```

2.2 Conclusion

Most people who have done disk partitioning have used the Microsoft Windows Disk Management Tool. The Linux fdisk command is a powerful tool that lets users create and delete primary and extended partitions and create logical drives.

2.3 Discussion Questions

1. How many primary partitions can a disk have (MBR-based)?
2. How many extended partitions can a disk have?
3. In order to store data, what must be created in the extended partition?
4. At what number do logical drives within the extended partition start?

3 Formatting Drives in Linux and Utilizing the Storage

Many people have experience formatting disks with a simple right-click within the Microsoft Windows operating systems. Of course, after formatting, the disk in Windows, the disk is ready to use for data storage. With Linux, the mkfs command can be utilized to format the disk. After formatting with the mkfs command, the disk will need to be mounted manually using the mount command in order for you to store data.

3.1 Formatting in Linux

1. To view the partition table for the fourth disk in the system, type the following:
   root@bt:~# **fdisk –l /dev/sdd**

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

Disk /dev/sdd: 10.7 GB, 10737418240 bytes
255 heads, 63 sectors/track, 1305 cylinders
Units = cylinders of 16065 * 512 = 8225280 bytes
Disk identifier: 0xab96e0e5

   Device Boot      Start         End      Blocks   Id  System
/dev/sdd1               1         500     4016218+   7  HPFS/NTFS
/dev/sdd2             501        1000     4016250    b  W95 FAT32
/dev/sdd3            1001        1305     2449912+   5  Extended
/dev/sdd5            1001        1002       16033+   1  FAT12
```

2. Type the following so the OS will recognize the changes to the disk structure:
   root@bt:~# **partprobe**

```
root@bt:~# partprobe
Warning: Unable to open /dev/hdc read-write (Read-only file system).
  /dev/hdc has been opened read-only.
```

3. Format the first partition on the fourth disk by typing the following command:
   root@bt:~# **mkfs.ntfs –Q /dev/sdd1**

```
root@bt:~# mkfs.ntfs -Q /dev/sdd1
Cluster size has been automatically set to 4096 bytes.
Creating NTFS volume structures.
mkntfs completed successfully. Have a nice day.
```

4. Format the fifth partition on the fourth disk by typing the following command:
   root@bt:~# **mkfs.vfat /dev/sdd2**

```
root@bt:~# mkfs.vfat /dev/sdd2
mkfs.vfat 2.11 (12 Mar 2005)
```

5. Format the fifth partition on the fourth disk by typing the following command:
   root@bt:~# **mkfs.vfat /dev/sdd5**

```
root@bt:~# mkfs.vfat /dev/sdd5
mkfs.vfat 2.11 (12 Mar 2005)
```

6. Type the following to make a directory named **sdd1** in the mnt directory.
   root@bt:~# **mkdir /mnt/sdd1**

```
root@bt:~# mkdir /mnt/sdd1
```

7. Type the following to make a directory named **sdd2** in the mnt directory.
   root@bt:~# **mkdir /mnt/sdd2**

```
root@bt:~# mkdir /mnt/sdd2
```

8. Type the following to make a directory named **sdd5** in the mnt directory.
   root@bt:~# **mkdir /mnt/sdd5**

```
root@bt:~# mkdir /mnt/sdd5
```

9. Create a file by typing the following command in the Linux terminal:
   root@bt:~# **echo hello world > hello.txt**

```
root@bt:~# echo hello world > hello.txt
```

10. Type the following command to view contents of the directory:
    root@bt:~# **ls**

```
root@bt:~# ls
hello.txt  install.sh
```

11. Type the following command to view the information in the hello.txt file:
    root@bt:~# **cat hello.txt**

```
root@bt:~# cat hello.txt
hello world
```

12. Type the following command to mount the newly created NTFS partition:
    root@bt:~# **mount /dev/sdd1 /mnt/sdd1**

```
root@bt:~# mount  /dev/sdd1  /mnt/sdd1
```

13. Type the following command to view the list of mounted partitions:
    root@bt:~# **mount**

```
root@bt:~# mount
tmpfs on /lib/init/rw type tmpfs (rw,nosuid,mode=0755)
/proc on /proc type proc (rw,noexec,nosuid,nodev)
sysfs on /sys type sysfs (rw,noexec,nosuid,nodev)
varrun on /var/run type tmpfs (rw,nosuid,mode=0755)
varlock on /var/lock type tmpfs (rw,noexec,nosuid,nodev,mode=1777)
udev on /dev type tmpfs (rw,mode=0755)
tmpfs on /dev/shm type tmpfs (rw,nosuid,nodev)
devpts on /dev/pts type devpts (rw,noexec,nosuid,gid=5,mode=620)
rootfs on / type rootfs (rw)
fusectl on /sys/fs/fuse/connections type fusectl (rw,relatime)
/dev/hdc on /media/cdrom0 type iso9660 (ro,noatime)
/dev/loop0 on /rofs type squashfs (ro,noatime)
tmpfs on /tmp type tmpfs (rw,nosuid,nodev)
/dev/sdd1 on /mnt/sdd1 type fuseblk (rw,nosuid,nodev,allow other,blksize=4096)
```

14. Type the following command to copy hello.txt to the mounted NTFS partition:
    root@bt:~# **cp hello.txt /mnt/sdd1**

```
root@bt:~# cp hello.txt /mnt/sdd1
```

15. Type the following command to list the contents of the mounted NTFS partition:
    root@bt:~# **ls /mnt/sdd1**

```
root@bt:~# ls /mnt/sdd1
hello.txt
```

16. Type the following command to mount the newly created FAT32 partition:
    root@bt:~# **mount /dev/sdd2 /mnt/sdd2**

```
root@bt:~# mount  /dev/sdd2  /mnt/sdd2
```

17. Type the following command to view the list of mounted partitions:
    root@bt:~# **mount**

```
root@bt:~# mount
tmpfs on /lib/init/rw type tmpfs (rw,nosuid,mode=0755)
/proc on /proc type proc (rw,noexec,nosuid,nodev)
sysfs on /sys type sysfs (rw,noexec,nosuid,nodev)
varrun on /var/run type tmpfs (rw,nosuid,mode=0755)
varlock on /var/lock type tmpfs (rw,noexec,nosuid,nodev,mode=1777)
udev on /dev type tmpfs (rw,mode=0755)
tmpfs on /dev/shm type tmpfs (rw,nosuid,nodev)
devpts on /dev/pts type devpts (rw,noexec,nosuid,gid=5,mode=620)
rootfs on / type rootfs (rw)
fusectl on /sys/fs/fuse/connections type fusectl (rw,relatime)
/dev/hdc on /media/cdrom0 type iso9660 (ro,noatime)
/dev/loop0 on /rofs type squashfs (ro,noatime)
tmpfs on /tmp type tmpfs (rw,nosuid,nodev)
/dev/sdd1 on /mnt/sdd1 type fuseblk (rw,nosuid,nodev,allow_other,blksize=4096)
/dev/sdd2 on /mnt/sdd2 type vfat (rw)
```

18. Type the following command to copy hello.txt to the mounted FAT32 partition:
    root@bt:~# **cp hello.txt /mnt/sdd2**

```
root@bt:~# cp hello.txt /mnt/sdd2
```

19. Type the following command to list the contents of /mnt/sdd2:
    root@bt:~# **ls /mnt/sdd2**

```
root@bt:~# ls /mnt/sdd2
hello.txt
```

20. Type the following command to mount the newly created NTFS partition:
    root@bt:~# **mount /dev/sdd5 /mnt/sdd5**

```
root@bt:~# mount  /dev/sdd5  /mnt/sdd5
```

21. Type the following command to view the list of mounted partitions:
    root@bt:~# **mount**

```
root@bt:~# mount
tmpfs on /lib/init/rw type tmpfs (rw,nosuid,mode=0755)
/proc on /proc type proc (rw,noexec,nosuid,nodev)
sysfs on /sys type sysfs (rw,noexec,nosuid,nodev)
varrun on /var/run type tmpfs (rw,nosuid,mode=0755)
varlock on /var/lock type tmpfs (rw,noexec,nosuid,nodev,mode=1777)
udev on /dev type tmpfs (rw,mode=0755)
tmpfs on /dev/shm type tmpfs (rw,nosuid,nodev)
devpts on /dev/pts type devpts (rw,noexec,nosuid,gid=5,mode=620)
rootfs on / type rootfs (rw)
fusectl on /sys/fs/fuse/connections type fusectl (rw,relatime)
/dev/hdc on /media/cdrom0 type iso9660 (ro,noatime)
/dev/loop0 on /rofs type squashfs (ro,noatime)
tmpfs on /tmp type tmpfs (rw,nosuid,nodev)
/dev/sdd1 on /mnt/sdd1 type fuseblk (rw,nosuid,nodev,allow_other,blksize=4096)
/dev/sdd2 on /mnt/sdd2 type vfat (rw)
/dev/sdd5 on /mnt/sdd5 type vfat (rw)
```

22. Type the following command to copy hello.txt to the mounted FAT12 partition:
    root@bt:~# **cp hello.txt /mnt/sdd5**

```
root@bt:~# cp hello.txt /mnt/sdd5
```

23. Type the following command to list the contents of /mnt/sdd5:
    root@bt:~# **ls /mnt/sdd5**

```
root@bt:~# ls /mnt/sdd5
```

Close all open window and PC Viewers.

3.2 Conclusion

In Linux, formatting drives is typically done from the terminal using the mkfs command. The mkfs.vfat will format a FAT partition and the mkfs.ntfs will format an NTFS partition. After formatting, partitions must be mounted in order to be used for data storage.

3.3 Discussion Questions

1. What is the command to view all of the mounted file systems?
2. What Linux command allows you to scan the disk for partition changes?
3. What is the command to format a partition with the NTFS files system?
4. What is the command to format a partition with the FAT files system?

References

1. The mkfs Command:
   http://linux.die.net/man/8/mkfs

2. The partprobe Command:
   http://linux.about.com/library/cmd/blcmdl8_partprobe.htm

3. The mount Command:
   http://linux.die.net/man/8/mount

4. Partitioning in Linux:
   http://tldp.org/HOWTO/Partition/