

Hands On Project

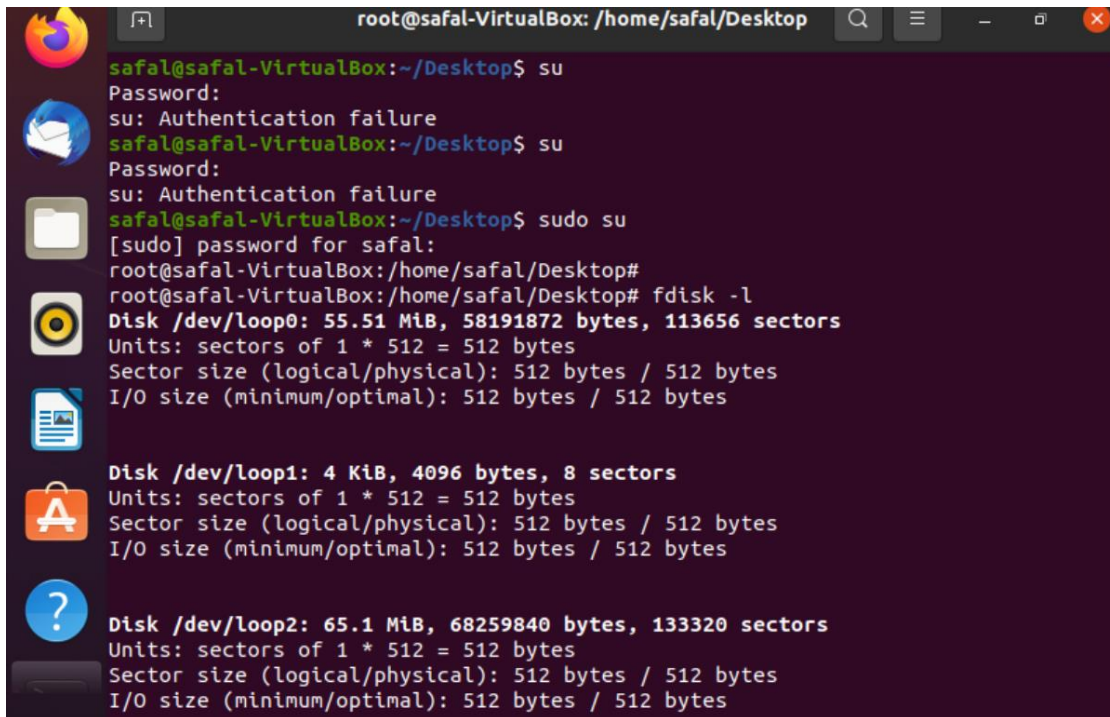
Hands-On Project 3-1

In this project, you prepare a drive and create a FAT32 disk partition using Linux. You need the following:

- A Linux distribution or Linux Live CD
- A disk drive
- A method of connecting a disk drive to your workstation, such as USB, FireWire, external SATA, or internal connections, such as PATA or SATA
- A review of the steps in the “Preparing a Target Drive for Acquisition in Linux” sectionA disk drive

To format a drive as FAT32 in Linux, follow these steps:

1. Connect the target drive to be partitioned and formatted as FAT32 to your workstation.
2. Start your workstation and log on or boot the Linux Live CD.
3. Follow the steps in the “Preparing a Target Disk for Acquisition in Linux” section.
4. When you’ve finished formatting the target drive, leave it connected for the next project.



```
root@safal-VirtualBox: /home/safal/Desktop
safal@safal-VirtualBox:~/Desktop$ su
Password:
su: Authentication failure
safal@safal-VirtualBox:~/Desktop$ su
Password:
su: Authentication failure
safal@safal-VirtualBox:~/Desktop$ sudo su
[sudo] password for safal:
root@safal-VirtualBox:/home/safal/Desktop#
root@safal-VirtualBox:/home/safal/Desktop# fdisk -l
Disk /dev/loop0: 55.51 MiB, 58191872 bytes, 113656 sectors
Units: sectors of 1 * 512 = 512 bytes
Sector size (logical/physical): 512 bytes / 512 bytes
I/O size (minimum/optimal): 512 bytes / 512 bytes

Disk /dev/loop1: 4 KiB, 4096 bytes, 8 sectors
Units: sectors of 1 * 512 = 512 bytes
Sector size (logical/physical): 512 bytes / 512 bytes
I/O size (minimum/optimal): 512 bytes / 512 bytes

Disk /dev/loop2: 65.1 MiB, 68259840 bytes, 133320 sectors
Units: sectors of 1 * 512 = 512 bytes
Sector size (logical/physical): 512 bytes / 512 bytes
I/O size (minimum/optimal): 512 bytes / 512 bytes
```

- 5 list the current disk devices connected to the computer, type `fdisk -l`

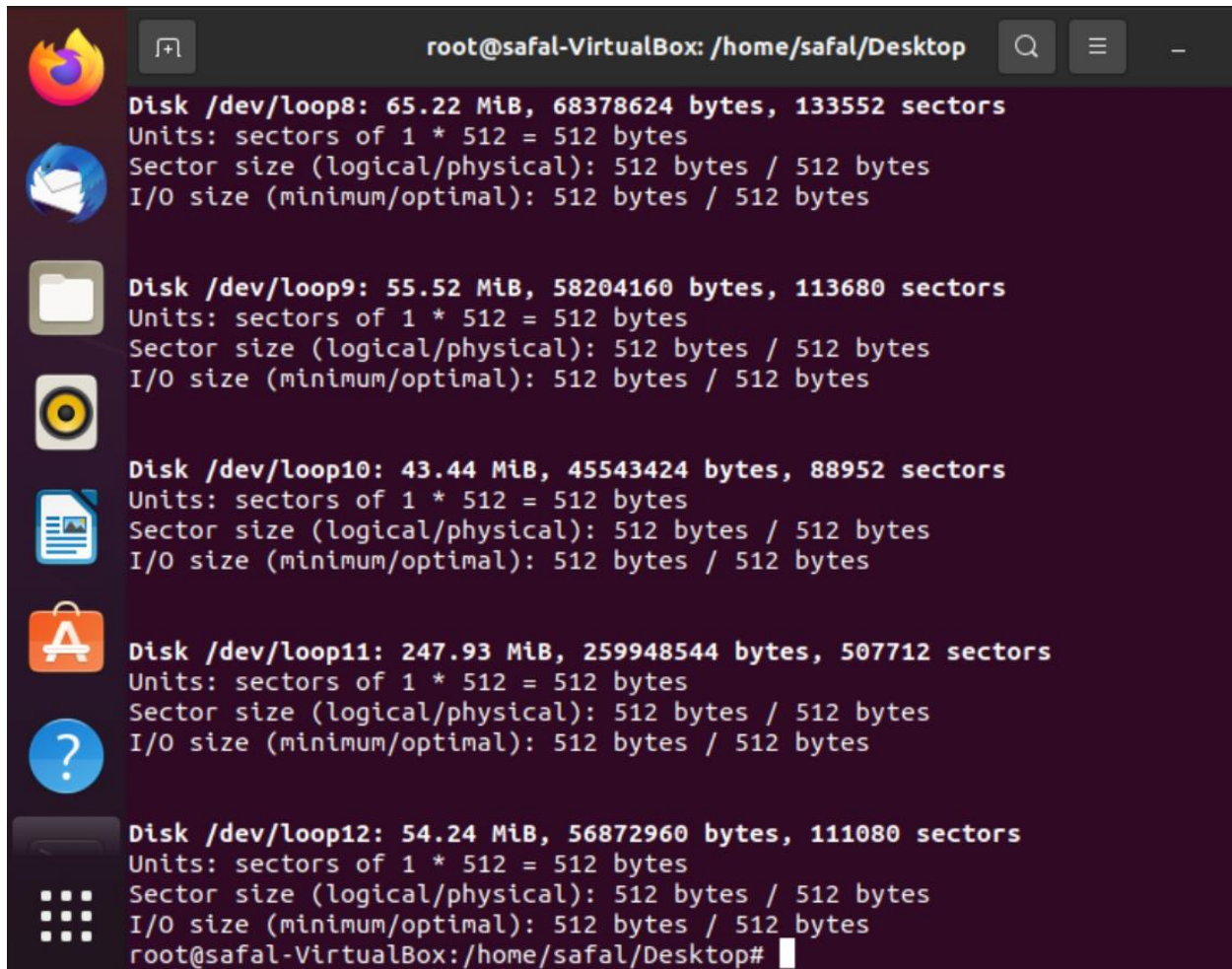
```
safal@safal-VirtualBox:~/Desktop$ su
Password:
su: Authentication failure
safal@safal-VirtualBox:~/Desktop$ sudo su
[sudo] password for safal:
root@safal-VirtualBox:/home/safal/Desktop#
root@safal-VirtualBox:/home/safal/Desktop# fdisk -l
Disk /dev/loop0: 55.51 MiB, 58191872 bytes, 113656 sectors
Units: sectors of 1 * 512 = 512 bytes
Sector size (logical/physical): 512 bytes / 512 bytes
I/O size (minimum/optimal): 512 bytes / 512 bytes

Disk /dev/loop1: 4 KiB, 4096 bytes, 8 sectors
Units: sectors of 1 * 512 = 512 bytes
Sector size (logical/physical): 512 bytes / 512 bytes
I/O size (minimum/optimal): 512 bytes / 512 bytes

Disk /dev/loop2: 65.1 MiB, 68259840 bytes, 133320 sectors
Units: sectors of 1 * 512 = 512 bytes
Sector size (logical/physical): 512 bytes / 512 bytes
I/O size (minimum/optimal): 512 bytes / 512 bytes

Disk /dev/loop3: 219 MiB, 229638144 bytes, 448512 sectors
Units: sectors of 1 * 512 = 512 bytes
Sector size (logical/physical): 512 bytes / 512 bytes
I/O size (minimum/optimal): 512 bytes / 512 bytes
```

Violations of academic honesty represent a serious breach of discipline and may be considered grounds for disciplinary action, including dismissal from the University. The University requires that all assignments submitted to faculty members by students be the work of the individual student submitting the work. An exception would be group projects assigned by the instructor. (Source: SEMO website)

A screenshot of a terminal window titled 'root@safal-VirtualBox: /home/safal/Desktop'. The terminal displays the output of the 'lsblk' command, showing details for five loop devices: /dev/loop8, /dev/loop9, /dev/loop10, /dev/loop11, and /dev/loop12. Each entry includes its size in MiB, total bytes, number of sectors, units, sector size, and I/O size. The terminal has a dark purple background with white and yellow text. On the left side of the terminal window, there is a vertical sidebar with icons for various applications like Firefox, LibreOffice, and the Dash application.

```
root@safal-VirtualBox: /home/safal/Desktop

Disk /dev/loop8: 65.22 MiB, 68378624 bytes, 133552 sectors
Units: sectors of 1 * 512 = 512 bytes
Sector size (logical/physical): 512 bytes / 512 bytes
I/O size (minimum/optimal): 512 bytes / 512 bytes

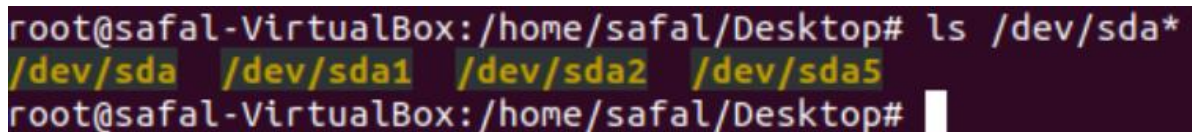
Disk /dev/loop9: 55.52 MiB, 58204160 bytes, 113680 sectors
Units: sectors of 1 * 512 = 512 bytes
Sector size (logical/physical): 512 bytes / 512 bytes
I/O size (minimum/optimal): 512 bytes / 512 bytes

Disk /dev/loop10: 43.44 MiB, 45543424 bytes, 88952 sectors
Units: sectors of 1 * 512 = 512 bytes
Sector size (logical/physical): 512 bytes / 512 bytes
I/O size (minimum/optimal): 512 bytes / 512 bytes

Disk /dev/loop11: 247.93 MiB, 259948544 bytes, 507712 sectors
Units: sectors of 1 * 512 = 512 bytes
Sector size (logical/physical): 512 bytes / 512 bytes
I/O size (minimum/optimal): 512 bytes / 512 bytes

Disk /dev/loop12: 54.24 MiB, 56872960 bytes, 111080 sectors
Units: sectors of 1 * 512 = 512 bytes
Sector size (logical/physical): 512 bytes / 512 bytes
I/O size (minimum/optimal): 512 bytes / 512 bytes
root@safal-VirtualBox: /home/safal/Desktop#
```

- 6 Type `fdisk/dev/sda` and press Enter to partition the disk drive as a FAT file system.

A screenshot of a terminal window showing the command 'ls /dev/sda*' being executed. The output lists the files /dev/sda, /dev/sda1, /dev/sda2, and /dev/sda5. The terminal has a dark purple background with white and yellow text.

```
root@safal-VirtualBox: /home/safal/Desktop# ls /dev/sda*
/dev/sda  /dev/sda1  /dev/sda2  /dev/sda5
root@safal-VirtualBox: /home/safal/Desktop#
```



```
root@safal-VirtualBox:/home/safal/Desktop# ls /dev/sda*
/dev/sda /dev/sda1 /dev/sda2 /dev/sda5
root@safal-VirtualBox:/home/safal/Desktop# df -h
Filesystem      Size  Used Avail Use% Mounted on
udev            838M   0  838M   0% /dev
tmpfs           174M  1.4M  172M   1% /run
/dev/sda5       9.3G  7.7G  1.2G  88% /
tmpfs           867M   0  867M   0% /dev/shm
tmpfs           5.0M  4.0K  5.0M   1% /run/lock
tmpfs           867M   0  867M   0% /sys/fs/cgroup
/dev/loop1      128K  128K   0 100% /snap/bare/5
/ LibreOffice Writer 56M   56M   0 100% /snap/core18/2246
/dev/loop3      219M  219M   0 100% /snap/gnome-3-34-1804/72
/dev/loop2       66M   66M   0 100% /snap/gtk-common-themes/1515
/dev/loop7       33M   33M   0 100% /snap/snapd/13640
/dev/loop5       51M   51M   0 100% /snap/snap-store/547
/dev/loop8       66M   66M   0 100% /snap/gtk-common-themes/1519
/dev/sda1       511M  4.0K  511M   1% /boot/efi
/dev/loop9       56M   56M   0 100% /snap/core18/2284
/dev/loop10      44M   44M   0 100% /snap/snapd/14549
/dev/loop4       62M   62M   0 100% /snap/core20/1328
/dev/loop6      219M  219M   0 100% /snap/gnome-3-34-1804/77
/dev/loop11     248M  248M   0 100% /snap/gnome-3-38-2004/87
/dev/loop12      55M   55M   0 100% /snap/snap-store/558
tmpfs           174M  44K  174M   1% /run/user/1000
```

- 7 Display fdisk menu options by typing m and pressing Enter.

```
Thunderbird Mail found
root@safal-VirtualBox:/home/safal/Desktop# fdisk /dev/sda

Welcome to fdisk (util-linux 2.34).
Changes will remain in memory only, until you decide to write them.
Be careful before using the write command.

Command (m for help): m

Help:

DOS (MBR)
a toggle a bootable flag
b edit nested BSD disklabel
c toggle the dos compatibility flag

Generic
d delete a partition
F list free unpartitioned space
l list known partition types
n add a new partition
p print the partition table
t change a partition type
v verify the partition table
i print information about a partition
```

Violations of academic honesty represent a serious breach of discipline and may be considered grounds for disciplinary action, including dismissal from the University. The University requires that all assignments submitted to faculty members by students be the work of the individual student submitting the work. An exception would be group projects assigned by the instructor. (Source: SEMO website)

- 8 Determine whether there are any partitions on /dev/sda by typing p and pressing Enter. You should see output similar to the following

```
Command (m for help): p
Disk /dev/sda: 10 GiB, 10737418240 bytes, 20971520 sectors
Disk model: VBOX HARDDISK
Units: sectors of 1 * 512 = 512 bytes
Sector size (logical/physical): 512 bytes / 512 bytes
I/O size (minimum/optimal): 512 bytes / 512 bytes
Disklabel type: dos
Disk identifier: 0x43cea034

Device      Boot  Start      End  Sectors  Size Id Type
/dev/sda1   *      2048    1050623    1048576   512M  b W95 FAT32
/dev/sda2             1052670  20969471   19916802    9.5G  5 Extended
/dev/sda5             1052672  20969471   19916800    9.5G  83 Linux
```

- 9 Next, you create a new primary partition on /dev/sda. To use the defaults and select the entire drive, type n and press Enter. To create a primary partition table, type p and press Enter, and then type 1 (the numeral) to select the first partition and press Enter.

```
Command (m for help): t
Partition number (1,2,5, default 5): 1
Hex code (type L to list all codes): L

 0 Empty                24 NEC DOS               81 Minix / old Lin  bf Solaris
 1 FAT12                 27 Hidden NTFS Win    82 Linux swap / So c1 DRDOS/sec (FAT-
 2 XENIX root            39 Plan 9              83 Linux             c4 DRDOS/sec (FAT-
 3 XENIX usr             3c PartitionMagic     84 OS/2 hidden or   c6 DRDOS/sec (FAT-
 4 FAT16 <32M           40 Venix 80286         85 Linux extended   c7 Syrix
 5 Extended              41 PPC PReP Boot      86 NTFS volume set  da Non-FS data
 6 FAT16                 42 SFS                 87 NTFS volume set  db CP/M / CTOS / .
 7 HPFS/NTFS/exFAT      4d QNX4.x              88 Linux plaintext  de Dell Utility
 8 AIX                   4e QNX4.x 2nd part    8e Linux LVM         df BootIt
 9 AIX bootable          4f QNX4.x 3rd part    93 Amoeba            e1 DOS access
 a OS/2 Boot Manag     50 OnTrack DM         94 Amoeba BBT        e3 DOS R/O
 b W95 FAT32            51 OnTrack DM6 Aux   9f BSD/OS            e4 SpeedStor
 c W95 FAT32 (LBA)     52 CP/M               a0 IBM Thinkpad hi  ea Rufus alignment
 e W95 FAT16 (LBA)     53 OnTrack DM6 Aux   a5 FreeBSD          eb BeOS fs
 f W95 Ext'd (LBA)     54 OnTrackDM6        a6 OpenBSD          ee GPT
10 OPUS                 55 EZ-Drive           a7 NeXTSTEP         ef EFI (FAT-12/16/
11 Hidden FAT12         56 Golden Bow         a8 Darwin UFS        f0 Linux/PA-RISC b
12 Compaq diagnost     5c Priam Edisk        a9 NetBSD            f1 SpeedStor
14 Hidden FAT16 <3     61 SpeedStor          ab Darwin boot       f4 SpeedStor
16 Hidden FAT16         63 GNU HURD or Sys   af HFS / HFS+        f2 DOS secondary
17 Hidden HPFS/NTF     64 Novell Netware    b7 BSDI fs           fb VMware VMFS
18 AST SmartSleep      65 Novell Netware    b8 BSDI swap         fc VMware VMKCORE
1b Hidden W95 FAT3      70 DiskSecure Mult   bb Boot Wizard hid  fd Linux raid auto
```

Violations of academic honesty represent a serious breach of discipline and may be considered grounds for disciplinary action, including dismissal from the University. The University requires that all assignments submitted to faculty members by students be the work of the individual student submitting the work. An exception would be group projects assigned by the instructor. (Source: SEMO website)

- 10 List the newly defined partitions by typing p
- 11 To list the menu again so that you can select the change partition ID, type m and press Enter.

```
root@ubuntu: /  
File Edit View Search Terminal Help  
Command (m for help): p  
Disk /dev/sda: 20 GB, 21474836480 bytes, 41943040 sectors  
Disk model: VMware Virtual S  
Units: sectors of 1 * 512 = 512 bytes  
Sector size (logical/physical): 512 bytes / 512 bytes  
I/O size (minimum/optimal): 512 bytes / 512 bytes  
Disklabel type: dos  
Disk identifier: 0x92fdbaf8  


| Device    | Boot | Start   | End      | Sectors  | Size  | Id | Type      |
|-----------|------|---------|----------|----------|-------|----|-----------|
| /dev/sda1 | *    | 2048    | 1050623  | 1048576  | 512M  | b  | W95 FAT32 |
| /dev/sda2 |      | 1052670 | 41940991 | 40888322 | 19.5G | 5  | Extended  |
| /dev/sda5 |      | 1052672 | 41940991 | 40888320 | 19.5G | 83 | Linux     |

  
Command (m for help): n  
All space for primary partitions is in use.  
Adding logical partition 6  
No free sectors available.  
Command (m for help): p  
Disk /dev/sda: 20 GB, 21474836480 bytes, 41943040 sectors  
Disk model: VMware Virtual S  
Units: sectors of 1 * 512 = 512 bytes  
Sector size (logical/physical): 512 bytes / 512 bytes  
I/O size (minimum/optimal): 512 bytes / 512 bytes  
Disklabel type: dos  
Disk identifier: 0x92fdbaf8  


| Device    | Boot | Start   | End      | Sectors  | Size  | Id | Type      |
|-----------|------|---------|----------|----------|-------|----|-----------|
| /dev/sda1 | *    | 2048    | 1050623  | 1048576  | 512M  | b  | W95 FAT32 |
| /dev/sda2 |      | 1052670 | 41940991 | 40888322 | 19.5G | 5  | Extended  |
| /dev/sda5 |      | 1052672 | 41940991 | 40888320 | 19.5G | 83 | Linux     |

  
Command (m for help): 1  
Unknown command  
Command (m for help):  
Command (m for help): p  
Disk /dev/sda: 20 GB, 21474836480 bytes, 41943040 sectors  
Disk model: VMware Virtual S  
Units: sectors of 1 * 512 = 512 bytes  
Sector size (logical/physical): 512 bytes / 512 bytes  
I/O size (minimum/optimal): 512 bytes / 512 bytes  
Disklabel type: dos  
Disk identifier: 0x92fdbaf8  


| Device    | Boot | Start | End     | Sectors | Size | Id | Type      |
|-----------|------|-------|---------|---------|------|----|-----------|
| /dev/sda1 | *    | 2048  | 1050623 | 1048576 | 512M | b  | W95 FAT32 |


```

- 12 To change the newly created partition to the Windows 95 FAT32 file system, first type t and press Enter,

```
Command (m for help): t  
Partition number (1,2,5, default 5): 1  
Hex code (type L to list all codes): L  


| Code | System          |
|------|-----------------|
| 0    | Empty           |
| 1    | FAT12           |
| 2    | XENIX root      |
| 3    | XENIX usr       |
| 4    | FAT16 <32M      |
| 5    | Extended        |
| 6    | FAT16           |
| 7    | HPFS/NTFS/exFAT |
| 8    | AIX             |
| 9    | AIX bootable    |
| a    | OS/2 Boot Manag |
| b    | W95 FAT32       |
| c    | W95 FAT32 (LBA) |
| e    | W95 FAT16 (LBA) |
| f    | W95 Ext'd (LBA) |
| 10   | OPUS            |
| 11   | Hidden FAT32    |
| 12   | Compaq diagnost |
| 14   | Hidden FAT16 <3 |
| 16   | Hidden FAT16    |
| 17   | Hidden HPFS/NTF |
| 18   | AST SmartSleep  |
| 1b   | Hidden W95 FAT3 |
| 1c   | Hidden W95 FAT3 |
| 1e   | Hidden W95 FAT1 |
| 1f   | Hidden W95 FAT1 |

  
Hex code (type L to list all codes): 1  
Changed type of partition 'W95 FAT32' to 'FAT12'.
```

- 13 List available file systems and their code values by typing l and pressing Enter.

Violations of academic honesty represent a serious breach of discipline and may be considered grounds for disciplinary action, including dismissal from the University. The University requires that all assignments submitted to faculty members by students be the work of the individual student submitting the work. An exception would be group projects assigned by the instructor. (Source: SEMO website)


```
Command (m for help): t
Partition number (1,2,5, default 5): 1
Hex code (type L to list all codes): L

0 Empty                24 NEC DOS                81 Minix / old Lin bf Solaris
1 FAT12                27 Hidden NTFS Win 82 Linux swap / So c1 DRDOS/sec (FAT-
2 XENIX root           39 Plan 9                 83 Linux          c4 DRDOS/sec (FAT-
3 XENIX usr            3c PartitionMagic         84 OS/2 hidden or c5 DRDOS/sec (FAT-
4 FAT16 <32M          40 Venix 80286            85 Linux extended c7 Syrix
5 Extended             41 PPC PReP Boot         86 NTFS volume set da Non-FS data
6 FAT16               42 SFS                   87 NTFS volume set db CP/M / CTOS / .
7 HPFS/NTFS/exFAT     4d QNX4.x                88 Linux plaintext de Dell Utility
8 AIX                 4e QNX4.x 2nd part 8e Linux LVM          df BootIt
9 AIX bootable        4f QNX4.x 3rd part 93 Amoeba          e1 DOS access
a OS/2 Boot Manag    50 OnTrack DM            94 Amoeba BBT        e3 DOS R/O
b W95 FAT32           51 OnTrack DM6 Aux 9f  BSD/OS          e4 Speedstor
c W95 FAT32 (LBA)     52 CP/M                  a0 IBM Thinkpad hl ea Rufus alignment
e W95 FAT16 (LBA)     53 OnTrack DM6 Aux a5 FreeBSD          eb BeOS fs
f W95 Ext'd (LBA)     54 OnTrackDM6            a6 OpenBSD          ee GPT
10 OPUS              55 Ez-Drive              a7 NextSTEP          ef EFI (FAT-12/16/
11 Hidden FAT12       56 Golden Bow           a8 Darwin UFS        f0 Linux/PA-RISC b
12 Compaq diagnost    5c PrLan Edisk           a9 NetBSD            f1 Speedstor
14 Hidden FAT16 <3    61 Speedstor            ab Darwin boot       f4 Speedstor
16 Hidden FAT16       63 GNU HURD or Sys af  HFS+ / HFS+         f2 DOS secondary
17 Hidden HPFS/NTFS   64 Novell Network       b7 BSDI fs           fb VMware VMFS
18 AST SmartSleep     65 Novell Network       b8 BSDI swap          fc VMware VMKCORE
1b Hidden W95 FAT17   70 DiskSecure Multi     bb Boot Wizard hid  fd Linux raid auto
1c Hidden W95 FAT17   75 PC/IX                 bc Acronis FAT32 L  fe LANstep
1e Hidden W95 FAT18   80 Old Minix             be Solaris boot       ff BBT

Hex code (type L to list all codes): 1

Changed type of partition 'W95 FAT32' to 'FAT12'.

Command (m for help): c
DOS Compatibility flag is set (DEPRECATED)

Command (m for help): p
Disk /dev/sda: 20 GiB, 21474836480 bytes, 41943040 sectors
Disk model: VMware Virtual S
```

14 Change the newly created partition to the Windows 95 FAT32 file system, type c

```
Hex code (type L to list all codes): 1

Changed type of partition 'W95 FAT32' to 'FAT12'.

Command (m for help): c
DOS Compatibility flag is set (DEPRECATED)

Command (m for help): p
Disk /dev/sda: 20 GiB, 21474836480 bytes, 41943040 sectors
Disk model: VMware Virtual S
```

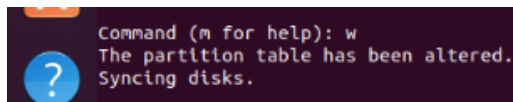
15 To display partitions of the newly changed drive, type p and press Enter, which produces the following output:

```
Command (m for help): c
DOS Compatibility flag is set (DEPRECATED!)

Command (m for help): p
Disk /dev/sda: 10 GiB, 10737418240 bytes, 20971520 sectors
Disk model: VBOX HARDDISK
Geometry: 255 heads, 2 sectors/track, 1305 cylinders
Units: sectors of 1 * 512 = 512 bytes
Sector size (logical/physical): 512 bytes / 512 bytes
I/O size (minimum/optimal): 512 bytes / 512 bytes
Disklabel type: dos
Disk identifier: 0x43cea034

Device      Boot    Start        End    Sectors    Size Id Type
/dev/sda1   *         2048     1050623     1048576    512M  b W95 FAT32
/dev/sda2             1052670    20969471    19916802     9.5G  5 Extended
/dev/sda5             1052672    20969471    19916800     9.5G  83 Linux
```

16 Write the newly created partition to the /dev/sda drive by typing w



- 17 Show the known drives connected to your computer by typing `fdisk -l` and pressing Enter, which produces the following output:

```
root@safal-VirtualBox:/home/safal/Desktop# fdisk -l
Disk /dev/loop0: 55.51 MiB, 58191872 bytes, 113656 sectors
Units: sectors of 1 * 512 = 512 bytes
Sector size (logical/physical): 512 bytes / 512 bytes
I/O size (minimum/optimal): 512 bytes / 512 bytes

Disk /dev/loop1: 4 KiB, 4096 bytes, 8 sectors
Units: sectors of 1 * 512 = 512 bytes
Sector size (logical/physical): 512 bytes / 512 bytes
I/O size (minimum/optimal): 512 bytes / 512 bytes

Disk /dev/loop2: 65.1 MiB, 68259840 bytes, 133320 sectors
Units: sectors of 1 * 512 = 512 bytes
Sector size (logical/physical): 512 bytes / 512 bytes
I/O size (minimum/optimal): 512 bytes / 512 bytes
```

```
Disk /dev/loop8: 65.22 MiB, 68378624 bytes, 133552 sectors
Units: sectors of 1 * 512 = 512 bytes
Sector size (logical/physical): 512 bytes / 512 bytes
I/O size (minimum/optimal): 512 bytes / 512 bytes

Disk /dev/loop9: 55.52 MiB, 58204160 bytes, 113680 sectors
Units: sectors of 1 * 512 = 512 bytes
Sector size (logical/physical): 512 bytes / 512 bytes
I/O size (minimum/optimal): 512 bytes / 512 bytes

Disk /dev/loop10: 43.44 MiB, 45543424 bytes, 88952 sectors
Units: sectors of 1 * 512 = 512 bytes
Sector size (logical/physical): 512 bytes / 512 bytes
I/O size (minimum/optimal): 512 bytes / 512 bytes

Disk /dev/loop11: 247.93 MiB, 259948544 bytes, 507712 sectors
Units: sectors of 1 * 512 = 512 bytes
Sector size (logical/physical): 512 bytes / 512 bytes
I/O size (minimum/optimal): 512 bytes / 512 bytes
```

Violations of academic honesty represent a serious breach of discipline and may be considered grounds for disciplinary action, including dismissal from the University. The University requires that all assignments submitted to faculty members by students be the work of the individual student submitting the work. An exception would be group projects assigned by the instructor. (Source: SEMO website)

- 18 To format a FAT file system from Linux, type `mkfs.msdos -vF32 /dev/sda1` and press Enter, which produces the following output:

```
root@safal-VirtualBox:/home/safal/Desktop# mkfs.msdos -vF32 /dev/sda1
mkfs.fat 4.1 (2017-01-24)
mkfs.msdos: /dev/sda1 contains a mounted filesystem.
```

- 19 Close the shell window for this session by typing `exit` and pressing Enter. This drive can now be mounted and used to receive an image of a suspect drive. Later in this section, you learn how to mount and write to this Microsoft FAT target drive.

```
root@ubuntu:/home# fdisk -l
Disk /dev/sdb: 2 GiB, 2147483648 bytes, 4194304 sectors
Disk model: VMware Virtual S
Units: sectors of 1 * 512 = 512 bytes
Sector size (logical/physical): 512 bytes / 512 bytes
I/O size (minimum/optimal): 512 bytes / 512 bytes

Disk /dev/sda: 20 GiB, 21474836480 bytes, 41943040 sectors
Disk model: VMware Virtual S
Units: sectors of 1 * 512 = 512 bytes
Sector size (logical/physical): 512 bytes / 512 bytes
I/O size (minimum/optimal): 512 bytes / 512 bytes
Disklabel type: dos
Disk identifier: 0x5dd4e7a1

Device Boot      Start         End      Sectors  Size Id Type
/dev/sda1 *        2048     1050623     1048576    512M  b W95 FAT32
/dev/sda2           1052670  41940991  40888322   19.5G  5 Extended
/dev/sda5           1052672  41940991  40888320   19.5G  83 Linux

root@ubuntu:/home#
```

```
root@ubuntu:/home# fdisk -l
Disk /dev/sdb: 2 GiB, 2147483648 bytes, 4194304 sectors
Disk model: VMware Virtual S
Units: sectors of 1 * 512 = 512 bytes
Sector size (logical/physical): 512 bytes / 512 bytes
I/O size (minimum/optimal): 512 bytes / 512 bytes

Disk /dev/sda: 20 GiB, 21474836480 bytes, 41943040 sectors
Disk model: VMware Virtual S
Units: sectors of 1 * 512 = 512 bytes
Sector size (logical/physical): 512 bytes / 512 bytes
I/O size (minimum/optimal): 512 bytes / 512 bytes
Disklabel type: dos
Disk identifier: 0x5dd4e7a1

Device Boot      Start         End      Sectors  Size Id Type
/dev/sda1 *        2048     1050623     1048576    512M  b W95 FAT32
/dev/sda2           1052670  41940991  40888322   19.5G  5 Extended
/dev/sda5           1052672  41940991  40888320   19.5G  83 Linux

root@ubuntu:/home#
```

Hands on Project 3-2:

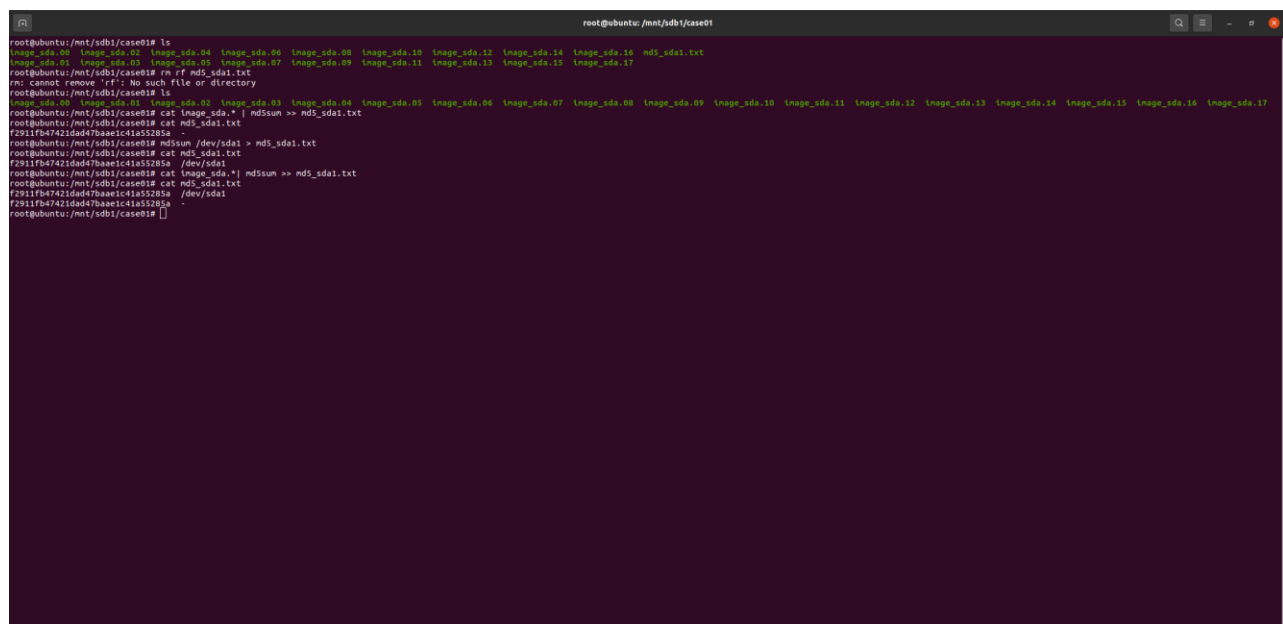
A method of connecting the FAT32 drive, and the drive created in Hands-On Project 3-1 to your workstation, such as USB, FireWire, external SATA, or internal connections, such as PATA or SATA

Violations of academic honesty represent a serious breach of discipline and may be considered grounds for disciplinary action, including dismissal from the University. The University requires that all assignments submitted to faculty members by students be the work of the individual student submitting the work. An exception would be group projects assigned by the instructor. (Source: SEMO website)

• A review of the “Acquiring Data with dd in Linux” and “Validating dd-Acquired Data” sections Follow these steps:

1. Make sure you’ve connected the drive you prepared in Hands-On Project 3-1 to your Linux workstation.
2. Start your workstation, if necessary, and log on to Linux or boot the Linux Live CD.
3. Reboot the Linux system, and make the dd acquisition, following the steps in “Acquiring Data with dd in Linux.” For the split -b command, make the segmented size 30m, and use the -d switch to create numeric extensions for each segmented file.
4. When the acquisition is finished, do a validation of the suspect drive and the acquired image files.

Follow the steps in the “Validating dd-Acquired Data” section. When you’re finished, keep the terminal window open, and keep Linux running for the next project.



```
root@ubuntu:/mnt/sdb1/case01# ls
image_sda.00 image_sda.01 image_sda.02 image_sda.03 image_sda.04 image_sda.05 image_sda.06 image_sda.07 image_sda.08 image_sda.09 image_sda.10 image_sda.11 image_sda.12 image_sda.13 image_sda.14 image_sda.15 md5_sda1.txt
image_sda.16 image_sda.17
root@ubuntu:/mnt/sdb1/case01# rm rf md5_sda1.txt
rm: cannot remove 'rf': No such file or directory
root@ubuntu:/mnt/sdb1/case01# ls
image_sda.00 image_sda.01 image_sda.02 image_sda.03 image_sda.04 image_sda.05 image_sda.06 image_sda.07 image_sda.08 image_sda.09 image_sda.10 image_sda.11 image_sda.12 image_sda.13 image_sda.14 image_sda.15 image_sda.16 image_sda.17
root@ubuntu:/mnt/sdb1/case01# cat image_sda.* | md5sum > md5_sda1.txt
root@ubuntu:/mnt/sdb1/case01# cat md5_sda1.txt
f2911fb47421dad47baae1c41a55285a  -
root@ubuntu:/mnt/sdb1/case01# md5sum /dev/sda1 > md5_sda1.txt
root@ubuntu:/mnt/sdb1/case01# cat md5_sda1.txt
f2911fb47421dad47baae1c41a55285a  /dev/sda1
root@ubuntu:/mnt/sdb1/case01# cat image_sda.* | md5sum > md5_sda1.txt
root@ubuntu:/mnt/sdb1/case01# cat md5_sda1.txt
f2911fb47421dad47baae1c41a55285a  /dev/sda1
root@ubuntu:/mnt/sdb1/case01#
```

```
root@ubuntu:/mnt/sdb1/case01# ls
image_sda.00 image_sda.02 image_sda.04 image_sda.06 image_sda.08 image_sda.10 image_sda.12 image_sda.14 image_sda.16 md5_sdai.txt
image_sda.01 image_sda.03 image_sda.05 image_sda.07 image_sda.09 image_sda.11 image_sda.13 image_sda.15 image_sda.17
root@ubuntu:/mnt/sdb1/case01# rm rf md5_sdai.txt
rm: cannot remove 'rf': No such file or directory
root@ubuntu:/mnt/sdb1/case01# ls
image_sda.00 image_sda.02 image_sda.03 image_sda.04 image_sda.05 image_sda.06 image_sda.07 image_sda.08 image_sda.09 image_sda.10 image_sda.11 image_sda.12 image_sda.13 image_sda.14 image_sda.15 image_sda.16 image_sda.17
root@ubuntu:/mnt/sdb1/case01# cat image_sda.* | md5sum >> md5_sdai.txt
root@ubuntu:/mnt/sdb1/case01# cat md5_sdai.txt
f2911fb47421dad47baae1c41a55285a  -
root@ubuntu:/mnt/sdb1/case01# md5sum /dev/sda > md5_sdai.txt
root@ubuntu:/mnt/sdb1/case01# cat md5_sdai.txt
f2911fb47421dad47baae1c41a55285a  /dev/sda
root@ubuntu:/mnt/sdb1/case01# cat image_sda.* | md5sum >> md5_sdai.txt
root@ubuntu:/mnt/sdb1/case01# cat md5_sdai.txt
f2911fb47421dad47baae1c41a55285a  /dev/sda
f2911fb47421dad47baae1c41a55285a  /dev/sda
f2911fb47421dad47baae1c41a55285a  -
root@ubuntu:/mnt/sdb1/case01#
```

```
root@ubuntu:/mnt/sdb1/case01#
Disk /dev/sda: 20 GiB, 21474836480 bytes, 41943040 sectors
Disk model: VMware Virtual S
Units: sectors of 1 * 512 = 512 bytes
Sector size (logical/physical): 512 bytes / 512 bytes
I/O size (minimum/optimal): 512 bytes / 512 bytes
Disklabel type: dos
Disk identifier: 0x5d5de7a1

Device Boot      Start         End      Sectors  Size Id Type
/dev/sda1 *       2048      1050623     1048576    512M b W95 FAT32
/dev/sda2          1050700  41940991  40888322  19.5G 5 extended
/dev/sda5          1052072  41940991  40888320  19.5G 83 Linux

root@ubuntu:/home# mdfix_mdos -vf32 /dev/sdb1
mfixfat v1.1 (2017-01-24)
/dev/sdb1 has 255 heads and 63 sectors per track,
1 hidden sectors (63880),
logical sector size is 512,
using bdrv media descriptor, with 4192256 sectors;
drive number 8380;
filesystem has 2 32-bit FATs and 8 sectors per cluster.
FAT size is 4088 sectors, and provides 523880 clusters.
There are 32 reserved sectors.
Volume ID is 559c940b, no volume label.
root@ubuntu:/home# mdfix /mnt/sdb1
root@ubuntu:/home# mount -t vfat /dev/sdb1 /mnt/sdb1/
root@ubuntu:/home# cd /mnt/sdb1/
root@ubuntu:/mnt/sdb1# mdfix_case01
root@ubuntu:/mnt/sdb1# cd case01/
root@ubuntu:/mnt/sdb1/case01# dd if=/dev/sda1 | split -d -b 30m - image_sda.
1048576+0 records in
1048576+0 records out
53687040 bytes (53.7 MB, 512 MiB) copied, 14.1903 s, 3.73 MB/s
root@ubuntu:/mnt/sdb1/case01# ls -la
total 32436
drwxr-xr-x 2 root root  4096 Feb  7 20:51 .
drwxr-xr-x 3 root root  4096 Dec 31 1969 ..
-rwxr-xr-x 1 root root 31457280 Feb  7 20:50 image_sda.00
-rwxr-xr-x 1 root root 31457280 Feb  7 20:50 image_sda.01
-rwxr-xr-x 1 root root 31457280 Feb  7 20:50 image_sda.02
-rwxr-xr-x 1 root root 31457280 Feb  7 20:50 image_sda.03
-rwxr-xr-x 1 root root 31457280 Feb  7 20:50 image_sda.04
-rwxr-xr-x 1 root root 31457280 Feb  7 20:50 image_sda.05
-rwxr-xr-x 1 root root 31457280 Feb  7 20:50 image_sda.06
-rwxr-xr-x 1 root root 31457280 Feb  7 20:50 image_sda.07
-rwxr-xr-x 1 root root 31457280 Feb  7 20:50 image_sda.08
-rwxr-xr-x 1 root root 31457280 Feb  7 20:50 image_sda.09
-rwxr-xr-x 1 root root 31457280 Feb  7 20:50 image_sda.10
-rwxr-xr-x 1 root root 31457280 Feb  7 20:51 image_sda.11
-rwxr-xr-x 1 root root 31457280 Feb  7 20:51 image_sda.12
-rwxr-xr-x 1 root root 31457280 Feb  7 20:51 image_sda.13
-rwxr-xr-x 1 root root 31457280 Feb  7 20:51 image_sda.14
-rwxr-xr-x 1 root root 31457280 Feb  7 20:51 image_sda.15
-rwxr-xr-x 1 root root 31457280 Feb  7 20:51 image_sda.16
-rwxr-xr-x 1 root root 2097152 Feb  7 20:51 image_sda.17
root@ubuntu:/mnt/sdb1/case01#
```

Violations of academic honesty represent a serious breach of discipline and may be considered grounds for disciplinary action, including dismissal from the University. The University requires that all assignments submitted to faculty members by students be the work of the individual student submitting the work. An exception would be group projects assigned by the instructor. (Source: SEMO website)


```
root@ubuntu:/mnt/sdb1/case01
Syncing disks.

root@ubuntu/home# fdisk -l

Command 'fdisk' not found, did you mean:
  command 'fdisk' from deb fdisk (2.34-0.1ubuntu9.1)

Try: apt install <deb name>

root@ubuntu/home# fdisk -l
Disk /dev/sdb: 2 GiB, 2147483648 bytes, 4194304 sectors
Disk model: VMware Virtual S
Units: sectors of 1 * 512 = 512 bytes
Sector size (logical/physical): 512 bytes / 512 bytes
I/O size (minimum/optimal): 512 bytes / 512 bytes
Disklabel type: dos
Disk identifier: 0x839762f7

Device      Boot  Start        End  Sectors  Size Id Type
/dev/sdb1                2048 4194303 4192256   2G c W95 FAT32 (LBA)

Disk /dev/sda: 20 GiB, 21474836480 bytes, 41943040 sectors
Disk model: VMware Virtual S
Units: sectors of 1 * 512 = 512 bytes
Sector size (logical/physical): 512 bytes / 512 bytes
I/O size (minimum/optimal): 512 bytes / 512 bytes
Disklabel type: dos
Disk identifier: 0x5d64e7a1

Device      Boot  Start        End  Sectors  Size Id Type
/dev/sda1 *      2048 1050623 1048576 512M b W95 FAT32
/dev/sda2      1052670 41940991 40888322 19.5G 5 Extended
/dev/sda3      1052672 41940991 40888320 19.5G 83 Linux

root@ubuntu/home# mkfs.msdos -vF32 /dev/sdb1
mkfs.fat 4.1 (2017-01-24)
/dev/sdb1 has 255 heads and 63 sectors per track,
hidden sectors 0x0000;
logical sector size is 512,
using 0xf1 media descriptor, with 4192256 sectors;
drive number 0x00;
Filesystem has 2 32-bit FATs and 8 sectors per cluster.
FAT size is 4088 sectors, and provides 523006 clusters.
There are 32 reserved sectors.
Volume ID is 556c4e6b, no volume label.
root@ubuntu/home# mkdir /mnt/sdb1
root@ubuntu/home# mount -t vfat /dev/sdb1 /mnt/sdb1/
root@ubuntu/home# cd /mnt/sdb1/
root@ubuntu/mnt/sdb1# mkdir case01
root@ubuntu/mnt/sdb1# cd case01/
root@ubuntu/mnt/sdb1/case01# dd if=/dev/sda1 | split -d -b 30m - image_sde.
10485760 records in
10485760 records out
536879012 bytes (537 MB, 512 MiB) copied, 14.3963 s, 37.3 MB/s
root@ubuntu/mnt/sdb1/case01#

root@ubuntu:/mnt/sdb1/case01
Command (m for help): w
The partition table has been altered.
Calling ioctl() to re-read partition table.
Syncing disks.

root@ubuntu/home# fdisk -l

Command 'fdisk' not found, did you mean:
  command 'fdisk' from deb fdisk (2.34-0.1ubuntu9.1)

Try: apt install <deb name>

root@ubuntu/home# fdisk -l
Disk /dev/sdb: 2 GiB, 2147483648 bytes, 4194304 sectors
Disk model: VMware Virtual S
Units: sectors of 1 * 512 = 512 bytes
Sector size (logical/physical): 512 bytes / 512 bytes
I/O size (minimum/optimal): 512 bytes / 512 bytes
Disklabel type: dos
Disk identifier: 0x839762f7

Device      Boot  Start        End  Sectors  Size Id Type
/dev/sdb1                2048 4194303 4192256   2G c W95 FAT32 (LBA)

Disk /dev/sda: 20 GiB, 21474836480 bytes, 41943040 sectors
Disk model: VMware Virtual S
Units: sectors of 1 * 512 = 512 bytes
Sector size (logical/physical): 512 bytes / 512 bytes
I/O size (minimum/optimal): 512 bytes / 512 bytes
Disklabel type: dos
Disk identifier: 0x5d64e7a1

Device      Boot  Start        End  Sectors  Size Id Type
/dev/sda1 *      2048 1050623 1048576 512M b W95 FAT32
/dev/sda2      1052670 41940991 40888322 19.5G 5 Extended
/dev/sda3      1052672 41940991 40888320 19.5G 83 Linux

root@ubuntu/home# mkfs.msdos -vF32 /dev/sdb1
mkfs.fat 4.1 (2017-01-24)
/dev/sdb1 has 255 heads and 63 sectors per track,
hidden sectors 0x0000;
logical sector size is 512,
using 0xf1 media descriptor, with 4192256 sectors;
drive number 0x00;
Filesystem has 2 32-bit FATs and 8 sectors per cluster.
FAT size is 4088 sectors, and provides 523006 clusters.
There are 32 reserved sectors.
Volume ID is 556c4e6b, no volume label.
root@ubuntu/home# mkdir /mnt/sdb1
root@ubuntu/home# mount -t vfat /dev/sdb1 /mnt/sdb1/
root@ubuntu/home# cd /mnt/sdb1/
root@ubuntu/mnt/sdb1# mkdir case01
root@ubuntu/mnt/sdb1# cd case01/
root@ubuntu/mnt/sdb1/case01# dd if=/dev/sda1 | split -d -b 30m - image_sde.
10485760 records in
10485760 records out
536879012 bytes (537 MB, 512 MiB) copied, 14.3963 s, 37.3 MB/s
root@ubuntu/mnt/sdb1/case01#
```

Violations of academic honesty represent a serious breach of discipline and may be considered grounds for disciplinary action, including dismissal from the University. The University requires that all assignments submitted to faculty members by students be the work of the individual student submitting the work. An exception would be group projects assigned by the instructor. (Source: SEMO website)

```
root@ubuntu:/home
Disklabel type: dos
Disk identifier: 0x039702f7

Device      Boot Start      End Sectors Size Id Type
/dev/sdb1    2048 4194303 4192256  2G c W95 FAT32 (LBA)

Command (m for help): w
The partition table has been altered.
Calling ioctl() to re-read partition table.
Syncing disks.

root@ubuntu:/home# fdisk -l

Command 'fdisk' not found, did you mean:
  command 'fdisk' from deb fdisk (2.34-0.1ubuntu9.1)

Try: apt install <deb name>

root@ubuntu:/home# fdisk -l
Disk /dev/sdb: 2 GiB, 2147483648 bytes, 4194304 sectors
Disk model: VMware Virtual S
Units: sectors of 1 * 512 = 512 bytes
Sector size (logical/physical): 512 bytes / 512 bytes
I/O size (minimum/optimal): 512 bytes / 512 bytes
Disklabel type: dos
Disk identifier: 0x039702f7

Device      Boot Start      End Sectors Size Id Type
/dev/sdb1    2048 4194303 4192256  2G c W95 FAT32 (LBA)

Disk /dev/sda: 20 GiB, 21474836480 bytes, 41943040 sectors
Disk model: VMware Virtual S
Units: sectors of 1 * 512 = 512 bytes
Sector size (logical/physical): 512 bytes / 512 bytes
I/O size (minimum/optimal): 512 bytes / 512 bytes
Disklabel type: dos
Disk identifier: 0x3d64e7a1

Device      Boot Start      End Sectors Size Id Type
/dev/sda1    * 2048 1050623 1048576 512M b W95 FAT32
/dev/sda2    1052070 41940991 40888322 19.3G s Extended
/dev/sda5    1052072 41940991 40888320 19.3G 83 Linux

root@ubuntu:/home# mke2fs.mke2fs -v -f32 /dev/sdb1
mke2fs 1.41 (2017-08-24)
/dev/sdb1 has 255 heads and 63 sectors per track,
1 hidden sectors (0x0000);
logical sector size is 512,
using 0x00 media descriptor, with 4192256 sectors;
drive number 0x00;
Filesystem has 2 32-bit FATs and 8 sectors per cluster.
FAT size is 4088 sectors, and provides 520800 clusters.
There are 32 reserved sectors.
Volume ID is 559c94d0, no volume label.
root@ubuntu:/home#

root@ubuntu:/home
ic Hidden W95 FAT3 75 PC/IX      hc Acronis FAT32 L fe LBAstep
ie Hidden W95 FAT1 80 Old Minix  be Solaris boot  ff BBT
hex code (type L to list all codes): c
changed type of partition 'Linux' to 'W95 FAT32 (LBA)'.

Command (m for help): p
Disk /dev/sdb: 2 GiB, 2147483648 bytes, 4194304 sectors
Disk model: VMware Virtual S
Units: sectors of 1 * 512 = 512 bytes
Sector size (logical/physical): 512 bytes / 512 bytes
I/O size (minimum/optimal): 512 bytes / 512 bytes
Disklabel type: dos
Disk identifier: 0x039702f7

Device      Boot Start      End Sectors Size Id Type
/dev/sdb1    2048 4194303 4192256  2G c W95 FAT32 (LBA)

Command (m for help): w
The partition table has been altered.
Calling ioctl() to re-read partition table.
Syncing disks.

root@ubuntu:/home# fdisk -l

Command 'fdisk' not found, did you mean:
  command 'fdisk' from deb fdisk (2.34-0.1ubuntu9.1)

Try: apt install <deb name>

root@ubuntu:/home# fdisk -l
Disk /dev/sdb: 2 GiB, 2147483648 bytes, 4194304 sectors
Disk model: VMware Virtual S
Units: sectors of 1 * 512 = 512 bytes
Sector size (logical/physical): 512 bytes / 512 bytes
I/O size (minimum/optimal): 512 bytes / 512 bytes
Disklabel type: dos
Disk identifier: 0x039702f7

Device      Boot Start      End Sectors Size Id Type
/dev/sdb1    2048 4194303 4192256  2G c W95 FAT32 (LBA)

Disk /dev/sda: 20 GiB, 21474836480 bytes, 41943040 sectors
Disk model: VMware Virtual S
Units: sectors of 1 * 512 = 512 bytes
Sector size (logical/physical): 512 bytes / 512 bytes
I/O size (minimum/optimal): 512 bytes / 512 bytes
Disklabel type: dos
Disk identifier: 0x3d64e7a1

Device      Boot Start      End Sectors Size Id Type
/dev/sda1    * 2048 1050623 1048576 512M b W95 FAT32
/dev/sda2    1052070 41940991 40888322 19.3G s Extended
/dev/sda5    1052072 41940991 40888320 19.3G 83 Linux

root@ubuntu:/home#
```

Violations of academic honesty represent a serious breach of discipline and may be considered grounds for disciplinary action, including dismissal from the University. The University requires that all assignments submitted to faculty members by students be the work of the individual student submitting the work. An exception would be group projects assigned by the instructor. (Source: SEMO website)

```
root@ubuntu:/home

Sector size (logical/physical): 512 bytes / 512 bytes
I/O size (minimum/optimal): 512 bytes / 512 bytes
Disklabel type: dos
Disk identifier: 0x839762f7

Device      Boot Start    End Sectors Size Id Type
/dev/sdb1   2048 4194303 4192256 2G 83 Linux

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

 0 Empty                24 NEC DOS                81 Mlnix / old Lin bf Solaris
 1 FAT12                27 Hidden NTFS Win 82 Linux swap / So c1 DRDOS/sec (FAT-
 2 XENIX root           39 Plan 9                  83 Linux          c4 DRDOS/sec (FAT-
 3 XENIX usr             3c PartitionMagic         84 OS/2 hidden or c6 DRDOS/sec (FAT-
 4 FAT16 <32M           40 Venix 80286             85 Linux extended c7 Syrix
 5 Extended             41 PPC PReP Boot          86 NTFS volume set da Non-FS data
 6 FAT16                42 SFS                    87 NTFS volume set db CP/M / CTOS / .
 7 HPFS/NTFS/exFAT      4d QNX4.x                  88 Linux plaintext de Dell Utility
 8 AIX                  4e QNX4.x 2nd part 8e Linux LVM          df BootIt
 9 AIX bootable         4f QNX4.x 3rd part 93 Amosha          e1 DOS access
 a OS/2 boot Manag     50 OnTrack DM             94 Amosha BBT          e3 DOS R/O
 b W95 FAT32           51 OnTrack DMS Aux 9f BSD/OS          e4 SpeedStor
 c W95 FAT32 (LBA)     52 CP/M                   a0 IBM Thinkpad hi ea Rufus alignment
 d W95 FAT16 (LBA)     53 OnTrack DMS Aux a5 FreeBSD          eb BeOS fs
 f W95 Ext'd (LBA)     54 OnTrackDMG             as OpenBSD          ee GPT
10 GPT                 55 EZ-Drive              a7 NEXTSTEP          ef EFI (FAT-12/16/
11 Hidden FAT12        56 Golden Bow           a8 Darwin UFS         f0 Linux/PA-RISC b
12 Compaq diagnot 5c Priam Edisk           a9 NetBSD             f1 SpeedStor
14 Hidden FAT16 <3 61 SpeedStor    ab Darwin boot        fa SpeedStor
16 Hidden FAT16        63 GNU HURD or Sys af HFS / HFS+         fb VMware VMFS
17 Hidden HPFS/NTF 64 Novell Netware        b7 BSDI fs            fd VMware VMFS
18 AST SmartSleep 65 Novell Netware        bb BSDL swap          fc VMware VMCORE
1b Hidden W95 FAT3 70 DiskSecure Mult bb Root Wizard hid fd Linux raid auto
1c Hidden W95 FAT3 75 PC/IX       bc Acronis FAT32 L fe LANtsep
1e Hidden W95 FAT1 88 Old Minix    be Solaris boot       ff BBT

Hex code (type L to list all codes): c
changed type of partition 'Linux' to 'W95 FAT32 (LBA)'.

Command (m for help): p
Disk /dev/sdb: 2 GiB, 2147483648 bytes, 4194304 sectors
Disk model: VMware Virtual S
Units: sectors of 1 * 512 = 512 bytes
Sector size (logical/physical): 512 bytes / 512 bytes
I/O size (minimum/optimal): 512 bytes / 512 bytes
Disklabel type: dos
Disk identifier: 0x839762f7

Device      Boot Start    End Sectors Size Id Type
/dev/sdb1   2048 4194303 4192256 2G c W95 FAT32 (LBA)

Command (m for help): w
The partition table has been altered.
Calling ioctl() to re-read partition table.
Syncing disks.

root@ubuntu:/home

Disk identifier: 0x839762f7

Command (m for help): n
Partition type:
  p   primary (0 primary, 0 extended, 4 free)
  e   extended (container for logical partitions)
Select (default p): p
Partition number (1-4, default 1):
First sector (2048-4194303, default 2048):
Last sector, +/-sectors or +/-size[K,M,G,T,P] (2048-4194303, default 4194303):

Created a new partition 1 of type 'Linux' and of size 2 GiB.

Command (m for help): p
Disk /dev/sdb: 2 GiB, 2147483648 bytes, 4194304 sectors
Disk model: VMware Virtual S
Units: sectors of 1 * 512 = 512 bytes
Sector size (logical/physical): 512 bytes / 512 bytes
I/O size (minimum/optimal): 512 bytes / 512 bytes
Disklabel type: dos
Disk identifier: 0x839762f7

Device      Boot Start    End Sectors Size Id Type
/dev/sdb1   2048 4194303 4192256 2G 83 Linux

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

 0 Empty                24 NEC DOS                81 Mlnix / old Lin bf Solaris
 1 FAT12                27 Hidden NTFS Win 82 Linux swap / So c1 DRDOS/sec (FAT-
 2 XENIX root           39 Plan 9                  83 Linux          c4 DRDOS/sec (FAT-
 3 XENIX usr             3c PartitionMagic         84 OS/2 hidden or c6 DRDOS/sec (FAT-
 4 FAT16 <32M           40 Venix 80286             85 Linux extended c7 Syrix
 5 Extended             41 PPC PReP Boot          86 NTFS volume set da Non-FS data
 6 FAT16                42 SFS                    87 NTFS volume set db CP/M / CTOS / .
 7 HPFS/NTFS/exFAT      4d QNX4.x                  88 Linux plaintext de Dell Utility
 8 AIX                  4e QNX4.x 2nd part 8e Linux LVM          df BootIt
 9 AIX bootable         4f QNX4.x 3rd part 93 Amosha          e1 DOS access
 a OS/2 boot Manag     50 OnTrack DM             94 Amosha BBT          e3 DOS R/O
 b W95 FAT32           51 OnTrack DMS Aux 9f BSD/OS          e4 SpeedStor
 c W95 FAT32 (LBA)     52 CP/M                   a0 IBM Thinkpad hi ea Rufus alignment
 d W95 FAT16 (LBA)     53 OnTrack DMS Aux a5 FreeBSD          eb BeOS fs
 f W95 Ext'd (LBA)     54 OnTrackDMG             as OpenBSD          ee GPT
10 GPT                 55 EZ-Drive              a7 NEXTSTEP          ef EFI (FAT-12/16/
11 Hidden FAT12        56 Golden Bow           a8 Darwin UFS         f0 Linux/PA-RISC b
12 Compaq diagnot 5c Priam Edisk           a9 NetBSD             f1 SpeedStor
14 Hidden FAT16 <3 61 SpeedStor    ab Darwin boot        fa SpeedStor
16 Hidden FAT16        63 GNU HURD or Sys af HFS / HFS+         fb VMware VMFS
17 Hidden HPFS/NTF 64 Novell Netware        b7 BSDI fs            fd VMware VMFS
18 AST SmartSleep 65 Novell Netware        bb BSDL swap          fc VMware VMCORE
1b Hidden W95 FAT3 70 DiskSecure Mult bb Root Wizard hid fd Linux raid auto
1c Hidden W95 FAT3 75 PC/IX       bc Acronis FAT32 L fe LANtsep
1e Hidden W95 FAT1 88 Old Minix    be Solaris boot       ff BBT

Hex code (type L to list all codes): c
Changed type of partition 'Linux' to 'W95 FAT32 (LBA)'.

Command (m for help):
```

Violations of academic honesty represent a serious breach of discipline and may be considered grounds for disciplinary action, including dismissal from the University. The University requires that all assignments submitted to faculty members by students be the work of the individual student submitting the work. An exception would be group projects assigned by the instructor. (Source: SEMO website)


```
root@ubuntu: /home

Disk /dev/sda: 20 GiB, 21474836480 bytes, 4194304 sectors
Disk model: VMware Virtual S
Units: sectors of 1 * 512 = 512 bytes
Sector size (logical/physical): 512 bytes / 512 bytes
I/O size (minimum/optimal): 512 bytes / 512 bytes
Disklabel type: dos
Disk identifier: 0x6d4de7a1

Device      Boot  Start      End  Sectors  Size Id Type
/dev/sda1   *    2048    105623    104576  512M  b W95 FAT32
/dev/sda2           105623  4194091  4088322  19.5G  5 Extended
/dev/sda5           4088322  4194091    105670  536K  83 Linux

root@ubuntu:/home# fdisk /dev/sdb

Welcome to fdisk (util-linux 2.34)
Changes will remain in memory only, until you decide to write them.
Be careful before using the write command.

Device does not contain a recognized partition table.
Created a new DOS disklabel with disk identifier 0xb39762f7.

Command (m for help): p
Disk /dev/sdb: 2 GiB, 2147483648 bytes, 4194304 sectors
Disk model: VMware Virtual S
Units: sectors of 1 * 512 = 512 bytes
Sector size (logical/physical): 512 bytes / 512 bytes
I/O size (minimum/optimal): 512 bytes / 512 bytes
Disklabel type: dos
Disk identifier: 0xb39762f7

Command (m for help): n
Partition type
  p primary (0 primary, 0 extended, 4 free)
  e extended (container for logical partitions)
Select (default p): p
Partition number (1-4, default 1):
First sector (2048-4194303, default 2048):
Last sector, +/-sectors or +/-size[K,M,G,T,P] (2048-4194303, default 4194303):
Created a new partition 1 of type 'Linux' and of size 2 GiB.

Command (m for help): p
Disk /dev/sdb: 2 GiB, 2147483648 bytes, 4194304 sectors
Disk model: VMware Virtual S
Units: sectors of 1 * 512 = 512 bytes
Sector size (logical/physical): 512 bytes / 512 bytes
I/O size (minimum/optimal): 512 bytes / 512 bytes
Disklabel type: dos
Disk identifier: 0xb39762f7

Device      Boot  Start      End  Sectors  Size Id Type
/dev/sdb1           2048  4194303  4192256  2G 83 Linux

Command (m for help):

root@ubuntu:/home# fdisk /dev/sdb

Welcome to fdisk (util-linux 2.34)
Changes will remain in memory only, until you decide to write them.
Be careful before using the write command.

Device does not contain a recognized partition table.
Created a new DOS disklabel with disk identifier 0xab5b58c6.

Command (m for help): m

Help:

DOS (MBR)
  a toggle a bootable flag
  b edit nested bsd disklabel
  c toggle the dos compatibility flag

Generic
  d delete a partition
  f list free unpartitioned space
  l list known partition types
  n add a new partition
  p print the partition table
  t change a partition type
  v verify the partition table
  l print information about a partition

Misc
  m print this menu
  u change display/entry units
  x extra functionality (experts only)

Script
  i load disk layout from sfdisk script file
  o dump disk layout to sfdisk script file

Save & Exit
  w write table to disk and exit
  q quit without saving changes

Create a new label
  g create a new empty GPT partition table
  G create a new empty GUID (UEFI) partition table
  o create a new empty DOS partition table
  s create a new empty Sun partition table

Command (m for help): p
Disk /dev/sdb: 2 GiB, 2147483648 bytes, 4194304 sectors
Disk model: VMware Virtual S
Units: sectors of 1 * 512 = 512 bytes
Sector size (logical/physical): 512 bytes / 512 bytes
I/O size (minimum/optimal): 512 bytes / 512 bytes
Disklabel type: dos
Disk identifier: 0xab5b58c6

Command (m for help):
```

Violations of academic honesty represent a serious breach of discipline and may be considered grounds for disciplinary action, including dismissal from the University. The University requires that all assignments submitted to faculty members by students be the work of the individual student submitting the work. An exception would be group projects assigned by the instructor. (Source: SEMO website)

```
root@ubuntu: /home
Disklabel type: dos
Disk identifier: 0x5d64e7a1

Device Boot Start End Sectors Size Id Type
/dev/sda1 * 2048 1050623 1048576 512M b W95 FAT32
/dev/sda2 1052070 41940991 40888322 19.3G 5 Extended
/dev/sda5 1052072 41940991 40888320 19.3G 83 Linux

root@ubuntu:/home# fdisk /dev/sdb

Welcome to fdisk (util-linux 2.34).
Changes will remain in memory only, until you decide to write them.
Be careful before using the write command.

Device does not contain a recognized partition table.
Created a new DOS disklabel with disk identifier 0x8db58c8d.

Command (n for help): n

Help:
DOS (MBR)
n toggle a bootable flag
b write nested BIOS disklabel
c toggle the dos compatibility flag

Generic
d delete a partition
l list known partition types
n add a new partition
p print the partition table
t change a partition type
v verify the partition table
i print information about a partition

Misc
m print this menu
u change display/entry units
x extra functionality (experts only)

Script
I load disk layout from sfdisk script file
O dump disk layout to sfdisk script file

Save & Exit
w write table to disk and exit
q quit without saving changes

Create a new label
g create a new empty GPT partition table
G create a new empty GUID (UEFI) partition table
o create a new empty DOS partition table
s create a new empty Sun partition table

Command (n for help):
```

```
root@ubuntu:~# cd /home/
root@ubuntu:/home# ls
root@ubuntu:/home# fdisk -l
Disk /dev/sdb: 2 GiB, 2147483648 bytes, 4194304 sectors
Disk model: VMware Virtual S
Units: sectors of 1 * 512 = 512 bytes
Sector size (logical/physical): 512 bytes / 512 bytes
I/O size (minimum/optimal): 512 bytes / 512 bytes

Disk /dev/sda: 20 GiB, 21474836480 bytes, 41943040 sectors
Disk model: VMware Virtual S
Units: sectors of 1 * 512 = 512 bytes
Sector size (logical/physical): 512 bytes / 512 bytes
I/O size (minimum/optimal): 512 bytes / 512 bytes
Disklabel type: dos
Disk identifier: 0x5d64e7a1

Device Boot Start End Sectors Size Id Type
/dev/sda1 * 2048 1050623 1048576 512M b W95 FAT32
/dev/sda2 1052070 41940991 40888322 19.3G 5 Extended
/dev/sda5 1052072 41940991 40888320 19.3G 83 Linux

root@ubuntu:/home# fdisk /dev/sdb

Welcome to fdisk (util-linux 2.34).
Changes will remain in memory only, until you decide to write them.
Be careful before using the write command.

Device does not contain a recognized partition table.
Created a new DOS disklabel with disk identifier 0x8db58c8d.

Command (n for help):
```

Case Project 3-1

Your supervisor has asked you to research current acquisition tools. Using your preferred Internet search engine and the vendors listed in this chapter, prepare a report containing the following information for each tool and stating which tool you would prefer to use:

- Forensics vendor name
- Acquisition tool name and latest version number
- Features of the vendor's product

Violations of academic honesty represent a serious breach of discipline and may be considered grounds for disciplinary action, including dismissal from the University. The University requires that all assignments submitted to faculty members by students be the work of the individual student submitting the work. An exception would be group projects assigned by the instructor. (Source: SEMO website)

With this data collected, prepare a spreadsheet listing vendor in the rows. For the column headings, list the following features:

- Raw format
- Proprietary format
- AFF format
- Other proprietary formats the tool can read
- Compression of image files
- Remote network acquisition capabilities
- Method used to validate (MD5, SHA-1, and so on)

Solution:

Computer forensics involves the digital evidence in support of crime, or administrative cases to be used as evidence. The evidence obtained should be legal, authentic, and admissible.

It is different from data recovery, work forensics and disaster recovery in many aspects. In computer forensic we search for an unknown data which was hidden by the suspect or user which can be used as a valid proof against the suspect

➔The utilization of electronic forensics or administrative records as evidence for digital evidence supporting the crime is required. Legally valid, authentic, and admissible evidence is required. Data recovery, forensics, and catastrophe recovery are just a few examples. We hunt for identifying details hidden by the individual or the user in computer forensics, which can be used as legitimate evidence against the defendant.

When evaluating evidence in a device, computer forensics tools are used for a variety of purposes. Some are used to retrieve data, while others are used to create photographs and still others are used to store computer files. Depending on the investigative demands, it is not required to apply all approaches in a particular case. Because of the numerous applications of the tens of thousands of tools generated.

Acquisition tool name and latest version number:

1. EnCase: the guide software forensic tool, the new edition 20.4. This method is used for different purposes, including procurement, research, and reporting.
2. Forensic Toolkit: Developed by Access Data, the most recent version of this tool is 7.1.0. Since it is a multifunctional tool that is mostly used to index the media acquired. This tool performs challenging tasks.

Violations of academic honesty represent a serious breach of discipline and may be considered grounds for disciplinary action, including dismissal from the University. The University requires that all assignments submitted to faculty members by students be the work of the individual student submitting the work. An exception would be group projects assigned by the instructor. (Source: SEMO website)

3. PTK Forensics: The newest version of the program developed by DF Labs Inc. These tools act as Sleuth Kt's GUI.

4. ProDiscover: the technology pathways tool is developed, and the most recent version is 8.2.0.5. This tool is designed to convert a raw image to a VMWare bootable disk.

5. X-Ways Forensics 16.4 X-Tensions API: is the machine forensic software. It provides cloning and imagery features. It can read files in raw format. It supports various file structure types.

Spreadsheet of tools:-

Vendor	Raw Format	Proprietary Format	AFF format	proprietary formats the tool can read	Compression of image files	Remote network acquisition capabilities	Method used to validate
ProDiscover	.pds	-	-	-	yes	yes	SHA-1, MD5, CRC-12
FTK Imager	dd	.e01,.s01	-	-	yes	yes	SHA-1, MD5, CRC-12
X-Way Forensic	dd	.e01	-	-	yes	no	SHA-1, MD5
X-Way Forensic	dd	.e01	-	-	yes	yes	SHA-1, MD5
Access data FTK	dd	.e01	-	-	yes	no	SHA-1, MD5

Case Project 3-2

At a murder scene, you have started making an image of a computer's drive. You're in the back bedroom of the house, and a small fire has started in the kitchen. If the fire can't be extinguished, you have only a few minutes to acquire data from a 10 GB hard disk. Write one to two pages outlining your options for preserving the data.

Solution: -

Violations of academic honesty represent a serious breach of discipline and may be considered grounds for disciplinary action, including dismissal from the University. The University requires that all assignments submitted to faculty members by students be the work of the individual student submitting the work. An exception would be group projects assigned by the instructor. (Source: SEMO website)

Case description

A person was killed when he was in the back room of his residence. Because the investigating agency knew when they entered the crime scene, the house caught fire. It was impossible to put out the fire since it was so hot. Now the investigator only has a short time to acquire data that is 10 GB in size and kept in the system at the criminal site. Offenders may also employ techniques to gather information before the fire spreads across the building.

Methods of Data Acquisition

Data collection means data collected for solving a case from a crime scene. There are two forms static collection and direct collection which is required for data collection.

When retrieving data takes a long time, static collection is employed. Prosecutor required less time than a difficult-to-extinguish fire. The data collecting method in this scenario is static collection. The primary goal of static data collecting is to save data proof that can be used in future claims. Researchers only have one opportunity to create a copy or save a file to disk. As a result, the enumerator has less time to acquire data in this scenario. In these types of circumstances, static collection is commonly utilized in digital evidence because once data is lost, it can never be recovered.

Tools used in investigation

When prosecuting a case, prosecutors take every measure to preserve the facts that will be used to bring the perpetrator to justice. Evidence storage plans have been put in place to ensure that no evidence is lost or tainted. Most investigators do not copy duplicate image files due to a lack of time. Distinct forensic firms have developed different purchasing tools, such as ProDiscover, EnCase, and FTK Imager, which can be used to make purchases.

1.FTK: FTK imager is a data collection windows application. It required license package for copying Access Data Forensic. FTK is developed to blend proof, and it generates disk and picture files from proprietary file formats. In its installed partition, this software displays an image file or a disk partition.

2. EnCase: EnCase is the device used to procure remotely. The Instruction program is designed to create the first remote forensic acquisition tool. It contains several functions such as:

- a) Data from any device's media or RAM can be received at the remote site.
- b) Data can be compiled from a variety of sources.
- b) An understanding of the framework for deciding whether to intervene further.
- d) RAID support in both hardware and software.
- e) It works with a variety of file formats, including NTFS, FAT, FFS, LVM8, DVD, Palm, UDF, and others.

Violations of academic honesty represent a serious breach of discipline and may be considered grounds for disciplinary action, including dismissal from the University. The University requires that all assignments submitted to faculty members by students be the work of the individual student submitting the work. An exception would be group projects assigned by the instructor. (Source: SEMO website)

f) Integrate methods for replicating the truth into the intrusion framework (IDS).

3. ProDiscover: The program ProDiscover is designed for remote data access. It has been developed in two versions:

1. Researcher of ProDiscover.
- 2 Incident Response ProDiscover.

When ProDiscover software is linked to the device remotely, the acquisition procedure is the same. The ProDiscover investigator is a live acquisition of suspicious folks from the device that collects data as the user runs q. For accessing data at the distant site, the ProDiscover program operates as the PDServer agent. The PDServer on the suspect's device must be enhanced till ProDiscover response and the ProDiscover investigator can use it. Prodiscover investigator links to the examiner device are encrypted using a 256-bit advanced encryption standard. All PDServer-Investigator-Computer communication is encrypted in ProDiscover Investigator. In this case, ProDiacover Basic is applied.

Procedure to collect data from ProDiscover

ProDiscover is a technology pathway tool, and the most current version is 7.04. These instruments have been used to transform a raw picture to a bootable VMware computer from one disk.

The picture of the suspected file is made with this program. A multitude of purchasing functions are automated by ProDiscover. The USB drives are usually smaller than the disk so they can be segmented without. Use a write-blocker system or write security method for USB drives before you acquire the data from your suspicious drive with ProDiscover Simple. With an extension, ProDiscover generates the image file. A log file provides a list of errors that occurred when data was obtained. It also includes a special inventory file that provides ProDiscover with information on segmented quantities. ProDiscover makes four files. nvo of them are the parts of the spited image of the disk of suspected person and third is the log file and the next one is .psd file. A larger drive would have more than two segmented volumes. The extension of the segmented volumes is. eve and for other volumes the extensions are suffix —Split1, —Split2, —Split3, and so on with the. eve extension file. During the extraction of the files, it may be possible that the data get altered to solve this problem hardware writeblocker device is used with the ProDiscover. You extract the hash value using the hacking algorithm, then search the file and finally when the proof in the short hash value is matched. The data are not updated if the hash values are the same.

CASE PROJECT 3-3

You need to acquire an image of a disk on a computer that can't be removed from the scene, and you discover that it's a Linux computer. What are your options for acquiring the image? Write a brief paper specifying the hardware and software you would use.

Violations of academic honesty represent a serious breach of discipline and may be considered grounds for disciplinary action, including dismissal from the University. The University requires that all assignments submitted to faculty members by students be the work of the individual student submitting the work. An exception would be group projects assigned by the instructor. (Source: SEMO website)

Solution: -

Description of the Linux OS and commands used for acquisition. Linux is the operating system with different forensic tools pre-defined functions applicable for the retrieval of records. The Linux property is that the drive not installed may be ars-A44.

Physical disk control can be used to read data from hard drives, USB drives, and other storage devices. The Linux base acquisition technology is utilized to collect data from the accused device in the instance of Linux.

The Linux base acquisition technology is utilized to collect data from the accused device in the instance of Linux. The ability to read and install various disks is a unique feature of the Linux Live CD. To collect data, only a few tools are required:

1. Live CD Aforensic.
2. Cable-based USB, SATAe idernal drives.
3. Information to change the Linux Live CD from the suspect computer's BIOS.
4. Information of the data collection shell command.

Commands used for data aquation

The data acquisition order is dd. The term dd' here reflects dumping info. This command has a variety of functions and switches to write the data from a data file and media system for reading. The dd command doesn't depend on the file's physical structure. The dd command creates a raw format for data collecting that can be read by most forensic applications. Because the dd control has flaws, researchers can get data via dcfldd. The dd order has arrived! Hue is used to gather information but not to obtain forensic information. The new command, which contains more features like The DD Command, was created by Nicolas Habour due to the kind coming:

- a) Choose a pattern or hexadecimal text to wipe.
- b) Errors in the output log, which provide the specifics of all errors that can be handled and evaluated afterwards.
- c) Using SHA-1, MD5, SHA-256, SHA-384, and SHA-512 for logging.
- d) It possesses characteristics that indicate the process' precise progression.
- e) At the completion of the investigation, the acquired data was compared to the original disk. It aids in determining whether the information obtained is correct.
- f) Break into different portions, and then render a copy for obtaining results. Each segment is allocated a number. As a result, the Linux operating system provides two choices for data gathering. The dd and dcfldd instructions are the same.

These commands are used for the appropriate instruments.

Violations of academic honesty represent a serious breach of discipline and may be considered grounds for disciplinary action, including dismissal from the University. The University requires that all assignments submitted to faculty members by students be the work of the individual student submitting the work. An exception would be group projects assigned by the instructor. (Source: SEMO website)

Case Project 3-4

A bank has hired your firm to investigate employee fraud. The bank uses four 20 TB machines on a LAN. You're permitted to talk to the network administrator, who is familiar with where the data is stored. What diplomatic strategies should you use? Which acquisition method should you use? Write a two-page report outlining the problems you expect to encounter, explaining how to rectify them, and describing your solution. Be sure to address any customer privacy issues.

Solution: -

Case Description

The focus of the investigation is on the firm employee who has the potential to be complicit in the scam. It is also recognized. The server has a total capacity of 20 TB, and the survey will provide server information. To collect data for all server files, the Investigator must first gain the server's password and login in order to obtain information for all company files. In these types of investigations, planning is critical for extracting the facts.

Data acquisition methods

When an investigator obtains information, he or she tries to transfer the file onto a suspect machine or create a picture of the lie. The file is usually quite large, thus copying the lie takes a long time. The first is a rational acquisition, while the second is a scant acquisition.

1. Logical procurement:

Two logical acquisition acquisition methodologies and sparse acquisition technologies are used to save investigator time. The investigator only documents files that are relevant to the case or files of a specific type in a logical order. A sensible acquisition occurs in the email inquiry. Researchers only need to look at .psd or .ost files to find out more. On the other side of the investigation, the investigator gets extensive records from the RAID server. If the user has processed the Terabyte of data, the logical approach is the sole way to acquire speaker data.

2. Sparse acquisition:

If the amount of data is large, the researcher will employ sparse acquisition. It's the same logical H operation as before, but it also gathers unassigned Hong data with the file type on a storage drive or computer suspicious. If the researcher does not need to examine the full disk, this method of acquisition is used.

Data acquisition tools

The employee, who must be the employee, conducts the survey. Only files that are required for a given employee's operation are erased from the server. Other individuals associated

Violations of academic honesty represent a serious breach of discipline and may be considered grounds for disciplinary action, including dismissal from the University. The University requires that all assignments submitted to faculty members by students be the work of the individual student submitting the work. An exception would be group projects assigned by the instructor. (Source: SEMO website)

to the perpetrator's information is also provided, including the files of the employees participating in the scam. To retrieve the data from the server where the data is physically stored, we can utilize a variety of acquisition methods. In order to obtain information from the server, some of the applications include ProDiscover Basic, EnCase, and FTK Imager..

1. FTK: For copying Access, FTK imager is a windows application that requires a license package. It creates other proprietary file formats for disks and disk-to-image files, and Data Forensic is designed to fuse evidence. In its installed partition, this software displays an image file or a disk partition.

2. EnCase: EnCase is the device used to procure remotely. The Guidance program is designed to create the first remote forensic acquisition tool. It contains several functions such as:

- a) Data from the media or RAM of any device can be accessed from a remote locator.
- b) It is possible to build data from various systems.
- c) An insight into the framework for the further action decision.
- d) Both hardware and software support for RAID.
- e) It supports a wide variety of file formats, including NTFS, FAT, FFS, LVMB, DVD, Palm and UDF, among others.
- f) In integration with IDS software for replicating intrusion detection systems (IDS).

3. ProDiscover: the program ProDiscover is designed for remote data access. It has been developed in two versions:

1. Researcher

2 of ProDiscover. Incident Response ProDiscover. The method of the acquisition is the same when ProDiscover software is linked to the device remotely. The ProDiscover investigator is a live acquisition of suspicious folks from the device that collects data as the user runs q. For accessing data at the distant site, the ProDiscover program operates as the PDServer agent. The PDServer on the suspect's device must be enhanced till ProDiscover response and the ProDiscover investigator can use it. ProDiscover investigator links to the examiner device are encrypted using a 256-bit advanced encryption standard. All PDServer-Investigator-Computer communication is encrypted in ProDiscover Investigator. In this case, ProDiscover Basic is applied.

Procedure to collect data from ProDiscover

The most recent version of ProDiscover, a technology pathway tool, is 7.04. These tools were used to convert a raw image into a bootable VMware PC from a single disk. This application is used to create an image of the suspected file. ProDiscover automates a wide range of purchasing functions. Because USB drives are typically smaller than hard disks, they do not need to be partitioned. Before you use ProDiscover Simple to get the data from your suspected USB device, use a write-blocker system or a write security approach.

ProDiscover creates the image file using an extension. A log file contains a list of errors that occurred throughout the data collection process. It also comes with a special inventory file that gives ProDiscover data on segmented quantities. ProDiscover creates four different files. The components of the corrupted image of the suspected person's disk, the log file, and the.psd file are the first three. There would be more than two segmented volumes on a bigger drive. The segmented volumes have the.eve extension, while other volumes have the suffix —Split1, —Split2, —Split3, and so on with the.eve extension file. The data may be altered during the extraction of the files, so a hardware writeblocker device is used with the ProDiscover to solve this problem. You extract the hash value using the hacking algorithm, then search the file and finally when the proof in the short hash value is matched. The data are not updated if the hash values are the same. As this case relates to fraud by a single employee of the bank in his office, only the employee supposed to be part of the fraud is being investigated. Therefore, the rule of privacy is breached because the company is entitled to prosecute the crime in case of fraud.

CASE PROJECT 3-5

You're investigating a case involving a 2 GB drive that you need to copy at the scene. Write one to two pages describing the three types of acquisitions—physical, logical, and sparse— you can use to copy the drive accurately. Be sure to include your software and media choices.

Solution: -

First of all I would acquire the data from the place of crime to solve the case. Data acquisition takes place in 4 methods:

- Create disk to image file
- Disk-to- disk copy
- Logical disk to disk or disk to data file
- Creating a sparse copy of a folder

Disk imaging: we will use the **Forensic Imager** that will acquire a sector copy of a drive into one of the following common forensic file format.

- DD/ RAW ("Drive Dump")
- AFF
- E01(EnCase)

Running forensic imager:

It is run by selecting the " Disk Image" option. There will be 3 options:

Acquire: to axtract copy of the target into an image file

Convert: to copy an existing image file from 1 to another; EG: DD to E01

Violations of academic honesty represent a serious breach of discipline and may be considered grounds for disciplinary action, including dismissal from the University. The University requires that all assignments submitted to faculty members by students be the work of the individual student submitting the work. An exception would be group projects assigned by the instructor. (Source: SEMO website)

Hash or verify:

Case Description

The case consists of a 2 GB disk drive and the data from the disk drive is to be copied on the scene of the crime. To obtain a rapid and reliable copy of the data, the investigator shall apply the best data acquisition technique.

Data Acquisition techniques

The investigator attempts to copy the file on the computer of the suspects during the acquisition of data or to photograph the filing. Often the files are very huge, and copying the file takes a long time. The investigator must decide first of all about the type of data acquisition he is going to undertake. The acquisition of information is divided into two types: the one logical and the other sparse.

1. Logical acquisition:

Investigators use two logical purchaser acquisition procedures and sparse purchaser technology if the duration is constrained. During the logical acquisition, the investigator only documents files that are relevant to the cases or specific sorts of files. The logical acquisition takes place in the email investigator. All that is required of the inquirer is a file search. .ost or.psd During another type of investigation, the investigator obtains unique records from the RAID server. The logical technique is the only way to get the specified data if the user has stored the data in terabytes.

2. Sparse acquisition:

The researcher will employ the sparse purchaser if the data is extremely large. It's similar to the logical technique, but it collects unallocated (deleted) data fragments in addition to the specific file type on the disc or device. If the investigator does not need to inspect the entire disk, this method of purchase is used.

Tools for gathering data from the drive of the suspect

For the data acquirer from the suspect machine different types of tools are created.

1. **ProDiscover Basic:** ProDiscover is the technology pathways tool, and its latest version is 7.04, which transforms a raw image of a disk to a VMware bootable computer. ProDiscover Basic.
This program takes a photo of the file of the suspect. A lot of acquisition functions are automated by ProDiscover. Usually, USB drives are smaller than the drives so that they

Violations of academic honesty represent a serious breach of discipline and may be considered grounds for disciplinary action, including dismissal from the University. The University requires that all assignments submitted to faculty members by students be the work of the individual student submitting the work. An exception would be group projects assigned by the instructor. (Source: SEMO website)

can be without segmented. Use a write-blocker system or write protection method for usb-connected drives until you acquire data from the suspected drive with ProDiscover Simple. ProDiscover generates a .eve extension image file. When data is obtained, a log file contains a list of errors. It also includes a one-of-a-kind inventory file that provides ProDiscover with information on the divided volumes. ProDiscover generates four files. The first two are spun image bits from a suspect's disk, the third is a log file, and the fourth is a psd file. There would be a greater push if there were more than two segmented volumes. Four files are created by ProDiscover. The first two are spun image bits from a suspect's disk, the third is a log file, and the fourth is a psd file. More than two segmented volumes would have a wider push. The extension file for extended segmented volumes is .eve, and the extensions for other volumes are -split2, -split3, and so on for the .eve extension file.

2. FTK Imager:

FTK Imager is a data collection tool for Windows. It's utilized to transfer the data to the suspect's computer. This program can be used with either USB or Ice via a parallel port. The FTK imager is an application that allows you to see proprietary disk and disk-to-image data. The Suspect Machine may use the FTK Imager to make copies of files, allowing the Investigator to physically copy the data. The writeblocking or USB writer-protection functionality on the data collection drive between the workstation and the proof drive can be enabled with this software, which is built for Windows. Within the protected area, FTK is unable to access data. The file format AccessData (.ad1), SMART (.s01), Expert Witness (e01) and raw formats can be read by the FTK Imager.

3. NT1-SafeBack: is an MS-DOS data acquisition tool that calculates SHA-256 in order to protect data integrity during an investigation. It also creates a log file that records all completed transactions. The remark block in this analysis tool gives context for the transaction and aids in finding the full details. It has different characteristics:

- a) Create picture files.
- b) Copy from the suspected drive to the destination drive.
- c) Copies the score to a picture.
- d) To reduce your disk size, compress the image file.
- e) Copies suspicious drive to the target drive photo.

CASE PROJECT 3-6

Your supervisor has asked you to list the acquisition tools available on a forensic Linux Live CD. Download the current ISO version of Deft (www.deftlinux.net), CAINE (www.caine-live.net), Kali Linux (www.kali.org), or Penguin Sleuth (www.linux-forensics.com), and then create a

Violations of academic honesty represent a serious breach of discipline and may be considered grounds for disciplinary action, including dismissal from the University. The University requires that all assignments submitted to faculty members by students be the work of the individual student submitting the work. An exception would be group projects assigned by the instructor. (Source: SEMO website)

bootable CD or DVD of it. Start it on your workstation and survey its tools. Then write a one to two-page report containing a brief description of each acquisition utility on the CD or DVD.

Solution: -

These tools/utilities can be stored in cd for kali linux:

1. Binwalk tool:

Binwalk is a forensic tool in Kali that looks for executable code and files in a binary image. It recognizes all of the files contained within any firmware image. It makes use of the "libmagic" library, which sorts out magic signatures in Unix file utilities.

2. Bulk extractor tool:

Credit card numbers, URL links, and email addresses are extracted in bulk and utilized as digital proof. Malware and intrusion attacks, identity investigations, cyber vulnerabilities, and password cracking are all possible with this program. This program is unique in that it not only works with conventional data, but it also works with compressed and incomplete data.

3. HashDeep tool:

The hash depth tool is a modified version of the dc3dd hash tool for digital forensics. This tool includes the automated hashing of data, i.e. sha-1, sha-256 and 512. Automatically writes an error log file. Each performance generates progress reports.

4. Magical rescue tool:

Magic rescue is a forensic technique that performs blocked device scanning. Using magic bytes, this utility pulls all known file kinds from the system. This illustrates the ability to repair lost or corrupt files by opening scanning and reading devices for file kinds. It will work with any filesystem.

5. Scalpel tool:

This forensic method produces and indexes the entire collection of files that run on Linux and Windows. The scalpel tool makes multithreading of multiple core systems simple. File carving occurs in small chunks, such as regular or binary expressions. The Scrounge-NTFS program is a forensic tool that aids in recovering data from corrupted NTFS disks or partitions. It recovers data from a corrupted filesystem and saves it to a fresh functional filesystem.

6. Guymager tool:

This forensic software is used to obtain media and a graphical user interface for forensic imagery. It is a very fast tool because of its multi-threaded data processing and compression. Cloning supports this method as well. It produces flat images, AFF, and the EWF. The UI can be used easily.

Violations of academic honesty represent a serious breach of discipline and may be considered grounds for disciplinary action, including dismissal from the University. The University requires that all assignments submitted to faculty members by students be the work of the individual student submitting the work. An exception would be group projects assigned by the instructor. (Source: SEMO website)

7. Pdftid tool:

This forensic procedure is utilized in pdf files. When you open a pdf file, the tool searches for specific keywords to find executable code. This utility fixes the most common issues with pdf files. The questionable files are next evaluated using the pdfparser program.

8. pdf-parser tool:

This is one of the most important forensics tools for pdf files. The pdf-parser technique scans a pdf document and distinguishes the important parts utilized in its analysis, but it does not render the page. Peepdf tool: A way for analyzing pdf documents in order to determine whether they are safe or dangerous. It contains all of the components needed to do pdf analysis in a single package. It shows suspicious entities and offers a variety of encryption and filtering options. You can also examine documents that have been encrypted.

9. Autopsy tool:

One forensic method for efficiently recovering and filtering data is an autopsy. With PhotoRec, you can create unallocated files and media. It is also possible to extract the EXIF multimedia extension. The STIX library's compromise predictor is based on autopsy scans. Both the command line and the graphical user interface are available.

10. img cat tool:

Image file output content is provided by the img cat tool. Because the recovered image files contain meta-data and embedded data, they can be converted to raw data. By executing the output on this raw data, the MD5 hash may be calculated.

11. ICAT tool:

ICAT is a TSK tool that generates a file output based on its inode number or identifier. ICAT generates a file output. It opens and copies the named file images to a standard output with a specific inode number. This forensic software is lightning fast. An inode is a Linux device data structure that stores data and data from a Linux file, such as ownership, file size, and typing, writing, and reading rights..

12. Srch strings tool:

This tool looks for feasible ASCII and Unicode strings in binary data and publishes the offset string that it finds. The tool srch strings removes and restores strings from a file, as well as sending offset bites if required.