



Name Sonia

Assignment 1

ID 24109119

Assignment:

Make the USB drive protected, create a DD Image, and extract data through Autopsy.

Subject: Digital Forensics

Professor: Muhammad Waqar

Task 1: USB Protected Read only mode:

```
Administrator: Command Prompt - diskpart
Microsoft DiskPart version 10.0.26100.1150

Copyright (C) Microsoft Corporation.
On computer: DESKTOP-8BL3MIG

DISKPART> list disk

Disk ###  Status        Size      Free      Dyn  Gpt
-----  -
Disk 0    Online        238 GB    2048 KB    *
Disk 1    Online        29 GB     0 B

DISKPART> select disk 1

Disk 1 is now the selected disk.

DISKPART> attributes disk
Current Read-only State : No
Read-only               : No
Boot Disk               : No
Pagefile Disk           : No
Hibernation File Disk   : No
Crashdump Disk          : No
Clustered Disk          : No

DISKPART> attributes disk set readonly

Disk attributes set successfully.

DISKPART>
```

Task 2: Create DD Image:

```
C:\Users\PMLS\Desktop\2nd semester\Digital Forensic\dd-0.6beta3>dd --list
rawwrite dd for windows version 0.6beta3.
Written by John Newbigin <jn@it.swin.edu.au>
This program is covered by terms of the GPL Version 2.
```

Win32 Available Volume Information

```
\\.\Volume{e56d3d1d-9853-4f4b-9adf-d8111f39fe06}\
  link to \\?\Device\HarddiskVolume3
  fixed media
  Mounted on \\.\c:
```

```
\\.\Volume{a278889d-b082-4e69-a581-9fea86a35bf9}\
  link to \\?\Device\HarddiskVolume4
  fixed media
  Not mounted
```

```
\\.\Volume{9149033a-2681-11f0-b5d7-04e8b90a8308}\
  link to \\?\Device\HarddiskVolume7
  removeable media
  Mounted on \\.\d:
```

```
\\.\Volume{7f63c9cc-2b56-4766-86a7-011543d72d65}\
  link to \\?\Device\HarddiskVolume1
  fixed media
  Not mounted
```

```
\\.\Volume{91490566-2681-11f0-b5d7-04e8b90a8308}\
  link to \\?\Device\Volume{a4970278-c791-3e24-a0ee-12244993264d}
  fixed media
  Mounted on \\.\g:
```

```
C:\Windows\System32\cmd.e x + v
link to \\?\Device\HarddiskVolume1
fixed media
Not mounted

\\.\Volume{91490566-2681-11f0-b5d7-04e8b90a8308}\
link to \\?\Device\Volume{a4970278-c791-3e24-a0ee-12244993264d}\
fixed media
Mounted on \\.\g:

NT Block Device Objects

Virtual input devices
/dev/zero (null data)
/dev/random (pseudo-random data)
- (standard input)

Virtual output devices
- (standard output)
/dev/null (discard the data)

C:\Users\PMLS\Desktop\2nd semester\Digital Forensic\dd-0.6beta3>dd if=\\.\D: of="C:\Users\PMLS\Desktop\2nd semester\Digital Forensic
usb_partition_image.dd" bs=1M --progress
rawwrite dd for windows version 0.6beta3.
Written by John Newbigin <jn@it.swin.edu.au>
This program is covered by terms of the GPL Version 2.

30,016M
30016+1 records in
30016+1 records out

C:\Users\PMLS\Desktop\2nd semester\Digital Forensic\dd-0.6beta3>
C:\Users\PMLS\Desktop\2nd semester\Digital Forensic\dd-0.6beta3>
```

Task 3 Autopsy:

The screenshot shows the Autopsy 4.22.1 interface. The left sidebar displays a tree view of data sources and file types. The main window shows a table of 10 results, which are files from a USB partition image. The table includes columns for Source Name, S, C, O, Version, Date Created, Date Modified, Data Source, and Description. The selected file is 'A systematic literature review of methods and data'. The bottom pane shows the metadata for this file, including Name, Type, MIME Type, Size, File Name Allocation, Metadata Allocation, Modified, Accessed, Created, Changed, MD5, and SHA-256 hashes.

Source Name	S	C	O	Version	Date Created	Date Modified	Data Source	Descr
DrHusnainAli_3805_21633_1_3-How to read a pape				1.6	2013-08-02 18:23:46 PKT	2017-06-13 15:22:41 PKT	usb_partition_image.dd	
A hybrid deep learning model for efficient intrusi				1.7	2019-12-13 05:13:25 PKT	2019-12-13 05:13:55 PKT	usb_partition_image.dd	A hyb
A systematic literature review of methods and data				1.7	2022-11-09 08:38:25 PKT	2022-11-09 08:39:06 PKT	usb_partition_image.dd	A syst
Attack classification of an intrusion detection syste				1.7	2021-04-19 17:11:25 PKT	2021-04-19 17:14:05 PKT	usb_partition_image.dd	Attack
Critical review.pdf				1.3	2021-02-18 15:21:13 PKT	2021-03-08 10:25:57 PKT	usb_partition_image.dd	A criti
Deep Learning-Based Intrusion Detection Systems				1.4	2021-07-22 06:06:02 PKT	2021-07-22 23:27:22 PKT	usb_partition_image.dd	Deep
Design and development of a deep learning-basec				1.4	2022-07-07 11:59:21 PKT	2022-07-07 20:47:45 PKT	usb_partition_image.dd	

Metadata

Name: /img_usb_partition_image.dd/RA/A systematic literature review of methods and datasets for anomaly-based network intrusion detection.pdf
Type: File System
MIME Type: application/pdf
Size: 2812154
File Name Allocation: Allocated
Metadata Allocation: Allocated
Modified: 2025-04-07 20:09:02 PKT
Accessed: 2025-04-27 00:00:00 PKT
Created: 2025-04-27 13:43:27 PKT
Changed: 0000-00-00 00:00:00
MD5: 750f83b6e3f4a6b7fd5898f7dfe2a16
SHA-256: ba4884650c682c07f2376ca59986a4fe97a88bc48ac370cb07c02530147f5f9



