VIT®

Vellore Institute of Technology

(Deemed to be University under section 3 of UGC Act, 1956)

School of Computer Science and Engineering (SCOPE)

Name : Yash Phatak

RegNo : 21BCT0288

Subject : Information Security Management

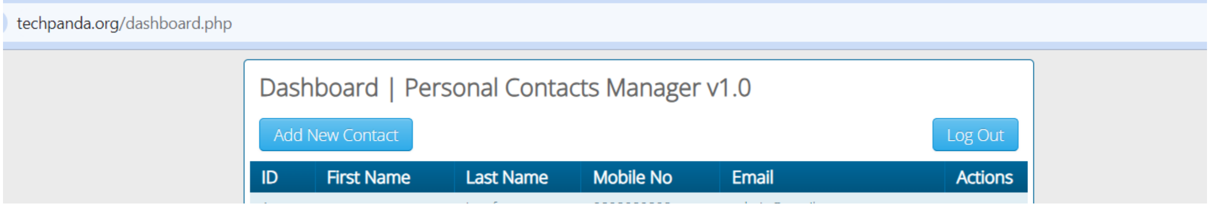
LAB Digital ASSESSMENT 1

Winter Semester 2023-24

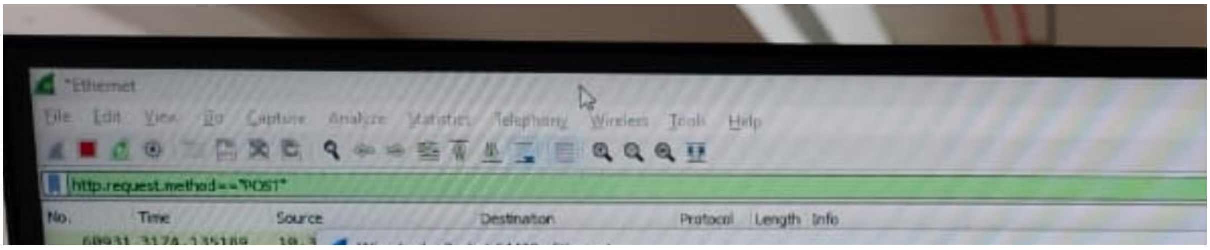
BCSE354E - Information Security Management Lab

Q1. Retrieve the Login ID and Password of a Website using WireShark.

1. Logging into the http://www.techpanda.org/ using a given username.

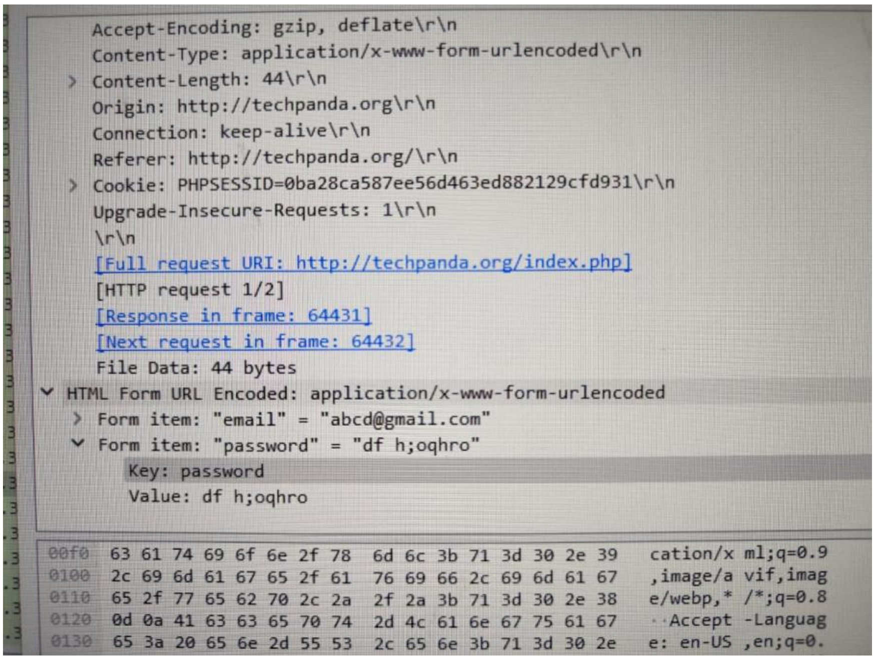

techpanda.org/dashboard.php
Dashboard | Personal Contacts Manager v1.0
Add New Contact
Log Out
ID
First Name
Last Name
Mobile No
Email
Actions

2. Tracking the username and password using Wireshark using Filter.



http.request.method=="POST"

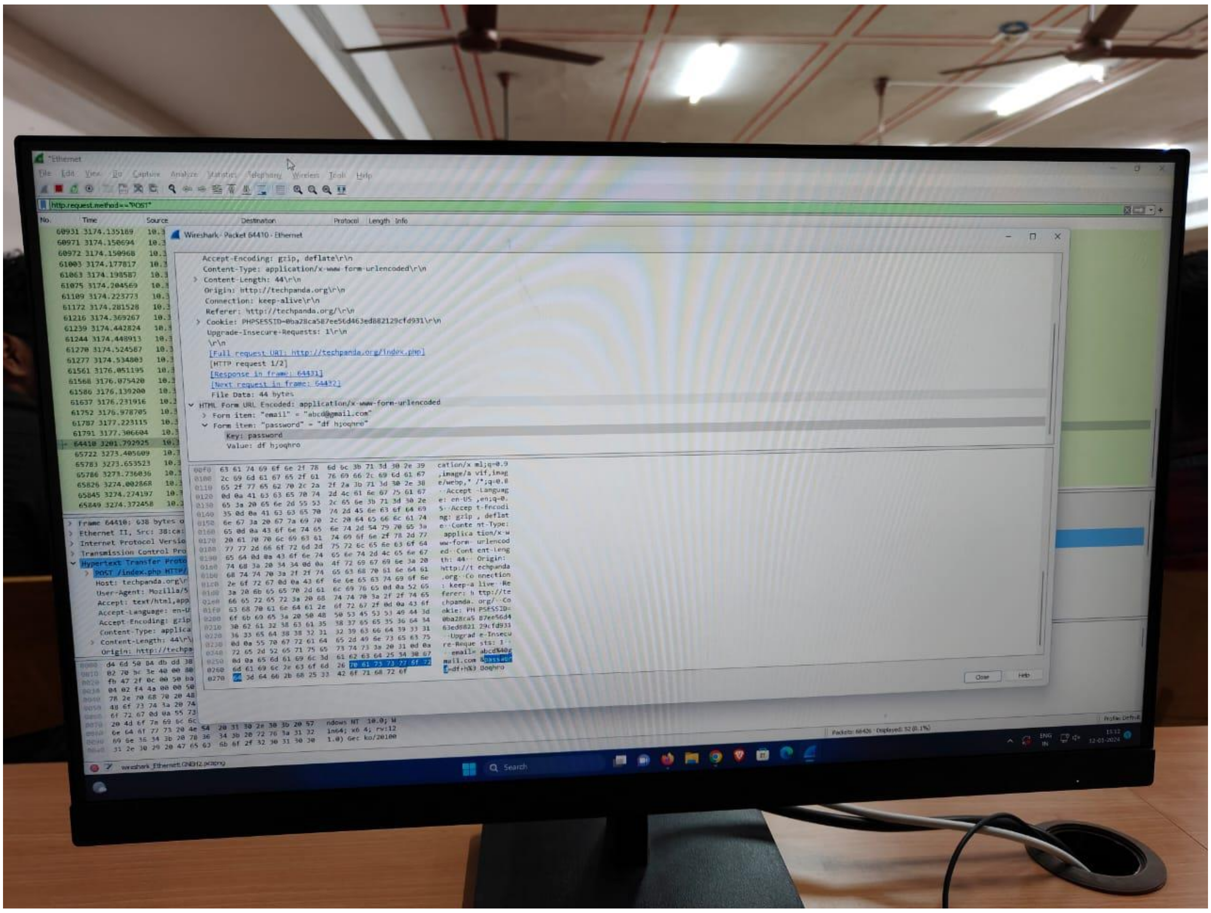
3. Screenshots of the Output File.



```
    Accept-Encoding: gzip, deflate\r\n
    Content-Type: application/x-www-form-urlencoded\r\n
  > Content-Length: 44\r\n
    Origin: http://techpanda.org\r\n
    Connection: keep-alive\r\n
    Referer: http://techpanda.org/\r\n
  > Cookie: PHPSESSID=0ba28ca587ee56d463ed882129cfd931\r\n
    Upgrade-Insecure-Requests: 1\r\n
    \r\n
    [Full request URI: http://techpanda.org/index.php]
    [HTTP request 1/2]
    [Response in frame: 64431]
    [Next request in frame: 64432]
    File Data: 44 bytes
v HTML Form URL Encoded: application/x-www-form-urlencoded
  > Form item: "email" = "abcd@gmail.com"
  v Form item: "password" = "df h;oqhro"
      Key: password
      Value: df h;oqhro

00f0  63 61 74 69 6f 6e 2f 78  6d 6c 3b 71 3d 30 2e 39   cation/x ml;q=0.9
0100  2c 69 6d 61 67 65 2f 61  76 69 66 2c 69 6d 61 67   ,image/a vif,imag
0110  65 2f 77 65 62 70 2c 2a  2f 2a 3b 71 3d 30 2e 38   e/webp,* /*;q=0.8
0120  0d 0a 41 63 63 65 70 74  2d 4c 61 6e 67 75 61 67   ··Accept -Languag
0130  65 3a 20 65 6e 2d 55 53  2c 65 6e 3b 71 3d 30 2e   e: en-US ,en;q=0.
```

Final Output :



Wireshark · Packet 64410 · Ethernet

```
Accept-Encoding: gzip, deflate\r\n
Content-Type: application/x-www-form-urlencoded\r\n
> Content-Length: 44\r\n
Origin: http://techpanda.org\r\n
Connection: keep-alive\r\n
Referer: http://techpanda.org/\r\n
> Cookie: PHPSESSID=0ba28ca587ee56d463ed882129cfd931\r\n
Upgrade-Insecure-Requests: 1\r\n
\r\n
[Full request URI: http://techpanda.org/index.php]
[HTTP request 1/2]
[Response in frame: 64431]
[Next request in frame: 64432]
File Data: 44 bytes
v HTML Form URL Encoded: application/x-www-form-urlencoded
  > Form item: "email" = "abcd@gmail.com"
  v Form item: "password" = "df h;oqhro"
      Key: password
      Value: df h;oqhro
```

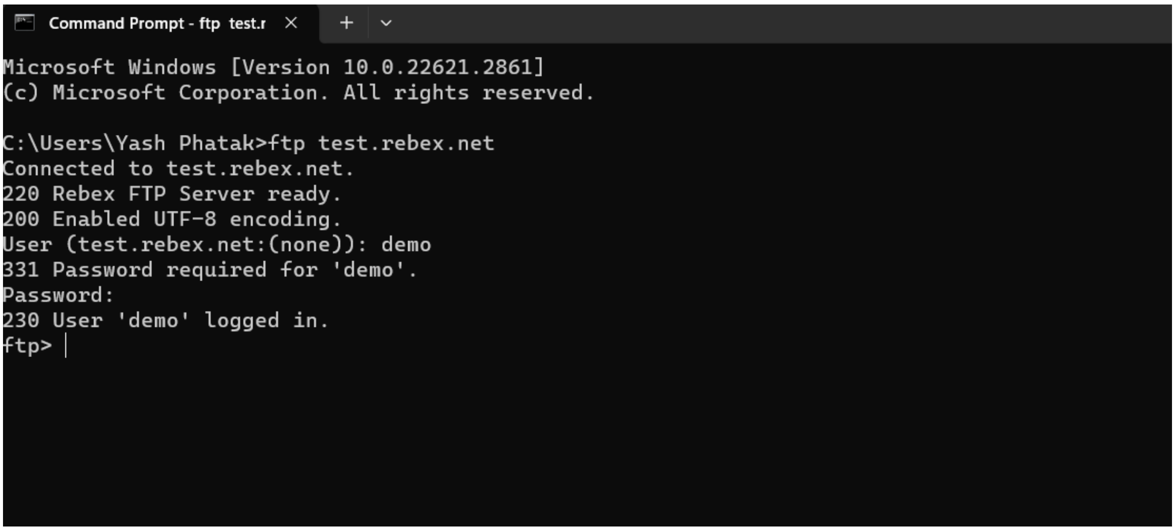
4. a. Name of the Filter : http.request.method == “POST”

   The request method accesses a property of the request object, which holds information about the current HTTP request from the user's browser.

   b. IP Address is 72.52.251.71

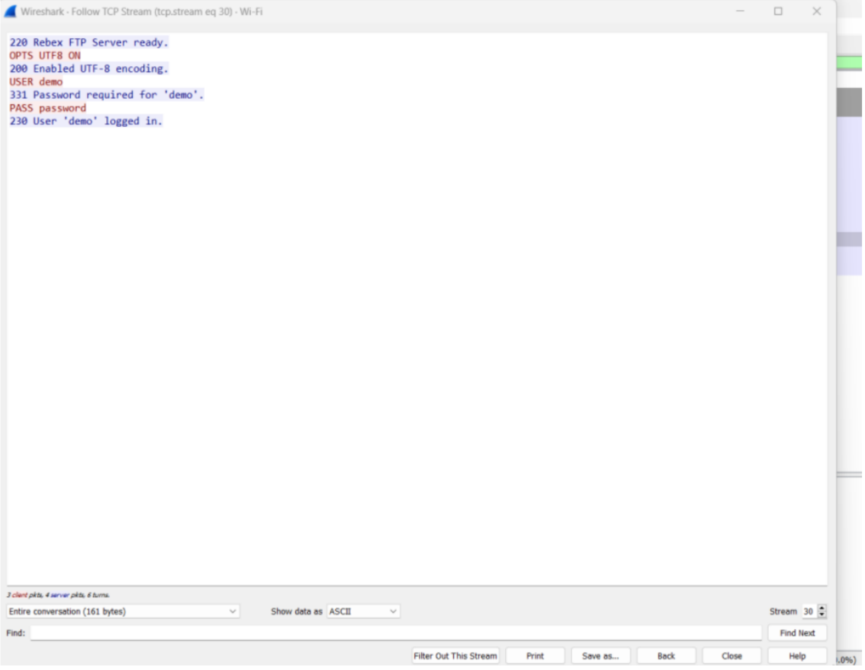
Q2. Crack the FTP user_ID and Password using WireShark.

1. Login to Host FTP using Command Prompt



```
Microsoft Windows [Version 10.0.22621.2861]
(c) Microsoft Corporation. All rights reserved.

C:\Users\Yash Phatak>ftp test.rebex.net
Connected to test.rebex.net.
220 Rebex FTP Server ready.
200 Enabled UTF-8 encoding.
User (test.rebex.net:(none)): demo
331 Password required for 'demo'.
Password:
230 User 'demo' logged in.
ftp>
```

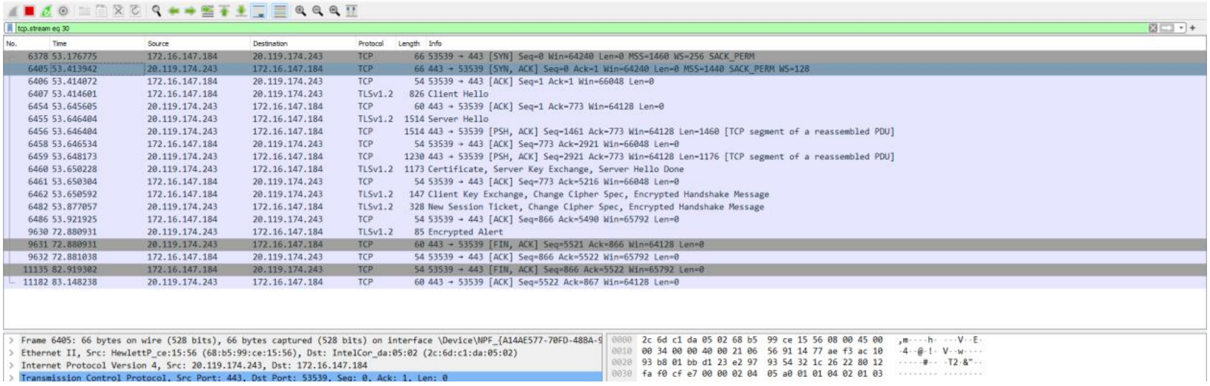


```
220 Rebex FTP Server ready.
OPTS UTF8 ON
200 Enabled UTF-8 encoding.
USER demo
331 Password required for 'demo'.
PASS password
230 User 'demo' logged in.
```

3 client pkts, 4 server pkts, 6 turns.

Entire conversation (161 bytes) Show data as ASCII Stream 30

Find:



tcp.stream eq 30

No.	Time	Source	Destination	Protocol	Length	Info
6378	53.176775	172.16.147.184	20.119.174.243	TCP	66	53539 → 443 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 WS=256 SACK_PERM
6405	53.413942	20.119.174.243	172.16.147.184	TCP	66	443 → 53539 [SYN, ACK] Seq=0 Ack=1 Win=64240 Len=0 MSS=1440 SACK_PERM WS=128
6406	53.414072	172.16.147.184	20.119.174.243	TCP	54	53539 → 443 [ACK] Seq=1 Ack=1 Win=66048 Len=0
6407	53.414601	172.16.147.184	20.119.174.243	TLSv1.2	826	Client Hello
6454	53.645605	20.119.174.243	172.16.147.184	TCP	60	443 → 53539 [ACK] Seq=1 Ack=773 Win=64128 Len=0
6455	53.646404	20.119.174.243	172.16.147.184	TLSv1.2	1514	Server Hello
6456	53.646404	20.119.174.243	172.16.147.184	TCP	1514	443 → 53539 [PSH, ACK] Seq=1461 Ack=773 Win=64128 Len=1460 [TCP segment of a reassembled PDU]
6458	53.646534	172.16.147.184	20.119.174.243	TCP	54	53539 → 443 [ACK] Seq=773 Ack=2921 Win=66048 Len=0
6459	53.648173	20.119.174.243	172.16.147.184	TCP	1230	443 → 53539 [PSH, ACK] Seq=2921 Ack=773 Win=64128 Len=1176 [TCP segment of a reassembled PDU]
6460	53.650228	20.119.174.243	172.16.147.184	TLSv1.2	1173	Certificate, Server Key Exchange, Server Hello Done
6461	53.650304	172.16.147.184	20.119.174.243	TCP	54	53539 → 443 [ACK] Seq=773 Ack=5216 Win=66048 Len=0
6462	53.650592	172.16.147.184	20.119.174.243	TLSv1.2	147	Client Key Exchange, Change Cipher Spec, Encrypted Handshake Message
6482	53.877057	20.119.174.243	172.16.147.184	TLSv1.2	328	New Session Ticket, Change Cipher Spec, Encrypted Handshake Message
6486	53.921925	172.16.147.184	20.119.174.243	TCP	54	53539 → 443 [ACK] Seq=866 Ack=5490 Win=65792 Len=0
9630	72.880931	20.119.174.243	172.16.147.184	TLSv1.2	85	Encrypted Alert
9631	72.880931	20.119.174.243	172.16.147.184	TCP	60	443 → 53539 [FIN, ACK] Seq=5521 Ack=866 Win=64128 Len=0
9632	72.881038	172.16.147.184	20.119.174.243	TCP	54	53539 → 443 [ACK] Seq=866 Ack=5522 Win=65792 Len=0
11135	82.919302	172.16.147.184	20.119.174.243	TCP	54	53539 → 443 [FIN, ACK] Seq=866 Ack=5522 Win=65792 Len=0
11182	83.148238	20.119.174.243	172.16.147.184	TCP	60	443 → 53539 [ACK] Seq=5522 Ack=867 Win=64128 Len=0

```
> Frame 6405: 66 bytes on wire (528 bits), 66 bytes captured (528 bits) on interface \Device\NPF_{A14AE577-70FD-48BA-9
> Ethernet II, Src: HewlettP_ce:15:56 (68:b5:99:ce:15:56), Dst: IntelCor_da:05:02 (2c:6d:c1:da:05:02)
> Internet Protocol Version 4, Src: 20.119.174.243, Dst: 172.16.147.184
> Transmission Control Protocol, Src Port: 443, Dst Port: 53539, Seq: 0, Ack: 1, Len: 0
```

```
0000  2c 6d c1 da 05 02 68 b5  99 ce 15 56 08 00 45 00   ,m····h· ···V··E·
0010  00 34 00 00 40 00 21 06  56 91 14 77 ae f3 ac 10   ·4··@·!· V··w····
0020  93 b8 01 bb d1 23 e2 97  93 54 32 1c 26 22 80 12   ·····#·· ·T2·&"··
0030  fa f0 cf e7 00 00 02 04  05 a0 01 01 04 02 01 03   ········ ········
```

Q. 1 -> Source IP is User and Destination is the FTP Server

Q.2 -> Source Port : 52508

Destination Port : 21