

Practical 5

Aim:- Use Wireshark (Sniffer) to capture network traffic and analyse

Code & Output:-

The screenshot displays two windows. The top window is a web browser showing the 'TRASH MAIL' website. The page has a blue header with 'TRASH MAIL' and 'INBOX' below it. There are navigation links: 'Inbox', 'To write', 'New address', and 'Help'. A message prompt says 'Please enter your email address in the field below (including your password if required). Do you need help?'. Below this is a social media promotion: 'Do you like trash mail? Tell your friends!' with Facebook, Twitter, and Google+ icons. The login form includes an 'E-mail address' field with 'onkar15' and a domain dropdown set to 'opentrash.com'. The 'password' field contains masked characters '.....'. A 'fetch emails' button is at the bottom.

The bottom window is 'The Wireshark Network Analyzer'. It shows the 'Capture' panel with a list of network interfaces. 'Wi-Fi' is selected, and a 'Start capture' button is visible. The main packet list shows several captured packets. The selected packet (No. 488) is a TCP packet from 192.168.0.113 to 23.212.253.224, port 443. The packet details pane shows the structure of the packet: Ethernet II, Internet Protocol Version 4, User Datagram Protocol, and Data (33 bytes). The packet bytes pane shows the raw data in hexadecimal and ASCII.

No.	Time	Source	Destination	Protocol	Length	Info
483	45.339393	192.168.0.113	23.212.253.224	TLSv1.3	69	Application Data
484	45.345470	23.212.253.224	192.168.0.113	TCP	85	[TCP Spurious Retransmission] 443 → 50245 [PSH, ACK] Seq=1132 Ack=3239 Win=64128 Len=31
485	45.345513	192.168.0.113	23.212.253.224	TCP	66	[TCP Dup ACK 482#1] 50245 → 443 [ACK] Seq=3274 Ack=1163 Win=131072 Len=0 SLE=1132 SRE=1163
486	45.382559	23.212.253.224	192.168.0.113	TCP	54	443 → 50245 [ACK] Seq=1163 Ack=3274 Win=64128 Len=0
487	46.183637	Tp-LinkT_aa:17:82	Broadcast	ARP	42	Who has 192.168.0.100? Tell 192.168.0.1
488	46.491836	192.168.0.113	72.52.251.71	TCP	54	[TCP Retransmission] 50243 → 80 [FIN, ACK] Seq=514 Ack=1104 Win=131328 Len=0
489	46.778595	72.52.251.71	192.168.0.113	TCP	54	80 → 50244 [FIN, ACK] Seq=3180 Ack=1310 Win=32256 Len=0
490	46.778641	192.168.0.113	72.52.251.71	TCP	54	50244 → 80 [ACK] Seq=1310 Ack=3181 Win=132352 Len=0
491	46.901133	Tp-LinkT_aa:17:82	Broadcast	ARP	42	Who has 192.168.0.105? Tell 192.168.0.1
492	47.207753	Tp-LinkT_aa:17:82	Broadcast	ARP	42	Who has 192.168.0.100? Tell 192.168.0.1
493	47.209311	Tp-LinkT_aa:17:82	Broadcast	ARP	42	Who has 192.168.0.100? Tell 192.168.0.1
494	47.508662	Tp-LinkT_aa:17:82	Broadcast	ARP	42	Who has 192.168.0.100? Tell 192.168.0.1
495	48.228303	Tp-LinkT_aa:17:82	Broadcast	ARP	42	Who has 192.168.0.109? Tell 192.168.0.1
496	48.234121	Tp-LinkT_aa:17:82	Broadcast	ARP	42	Who has 192.168.0.100? Tell 192.168.0.1
497	49.046905	Tp-LinkT_aa:17:82	Broadcast	ARP	42	Who has 192.168.0.100? Tell 192.168.0.1
498	49.148153	Tp-LinkT_aa:17:82	Broadcast	ARP	42	Who has 192.168.0.109? Tell 192.168.0.1
499	49.149330	Tp-LinkT_aa:17:82	Broadcast	ARP	42	Who has 192.168.0.100? Tell 192.168.0.1

Frame 1: 75 bytes on wire (600 bits), 75 bytes captured (600 bits) on interface \Device\NPF_{...} (84:d8:1b:aa:17:82)
> Ethernet II, Src: ChiconyE_45:1d:e4 (4c:bb:58:45:1d:e4), Dst: Tp-LinkT_aa:17:82 (84:d8:1b:aa:17:82)
> Internet Protocol Version 4, Src: 192.168.0.113, Dst: 172.217.166.42
> User Datagram Protocol, Src Port: 54522, Dst Port: 443
> Data (33 bytes)

0000 84 d8 1b aa 17 82 4c bb 58 45 1d e4 08 00 45 00L. XE...E-
0010 00 3d 24 72 40 00 00 11 c2 20 c0 a8 00 71 ac d9 ..=r@... ..q..
0020 a6 2a d4 fa 01 bb 00 29 20 d6 5e f0 d6 5c 01 2c\..\.
0030 b6 c7 dc 74 1e e4 3f a5 f9 84 df 7d e9 57 5a da?.....uZ
0040 00 89 a3 fd a3 2f 17 e2 1a e5 c4

The image displays two screenshots of the Wireshark network traffic analysis tool. The top screenshot shows a list of captured packets, with packet 429 selected. The bottom screenshot shows the detailed view of packet 429, which is an HTTP POST request to /index.php.

Top Screenshot: Packet List

No.	Time	Source	Destination	Protocol	Length	Info
259	29.119353	192.168.0.113	72.52.251.71	HTTP	567	GET / HTTP/1.1
263	29.478267	72.52.251.71	192.168.0.113	HTTP	1156	HTTP/1.1 200 OK (text/html)
429	44.276536	192.168.0.113	72.52.251.71	HTTP	779	POST /index.php HTTP/1.1 (application/x-www-form-urlencoded)
431	44.522857	72.52.251.71	192.168.0.113	HTTP	1184	HTTP/1.1 302 Found (text/html)
432	44.529767	192.168.0.113	72.52.251.71	HTTP	638	GET /dashboard.php HTTP/1.1
435	44.779205	72.52.251.71	192.168.0.113	HTTP	663	HTTP/1.1 200 OK (text/html)

Bottom Screenshot: Packet Details

Frame 429: 779 bytes on wire (6232 bits), 779 bytes captured (6232 bits) on interface \Device\NPF_{07268189-4A4A-4097-A852-60A10200372A}, id 0

- Ethernet II, Src: ChiconyE_45:1d:e4 (4c:bb:58:45:1d:e4), Dst: Tp-LinkT_aa:17:82 (84:d8:1b:aa:17:82)
- Internet Protocol Version 4, Src: 192.168.0.113, Dst: 72.52.251.71
- Transmission Control Protocol, Src Port: 50244, Dst Port: 80, Seq: 1, Ack: 1, Len: 725
- Hypertext Transfer Protocol
- HTML Form URL Encoded: application/x-www-form-urlencoded
 - Form item: "email" = "onkar15@pentrash.com"
 - Form item: "password" = "789456"

Packet Bytes:

```
0210 2d 65 78 63 68 61 6e 67 65 3b 76 3d 62 33 3b 71 -exchang e;v=b3;q
0220 3d 30 2e 39 0d 0a 52 65 66 65 72 65 72 3a 20 68 =0.9 -Re ferer: h
0230 74 74 70 3a 2f 2f 74 65 63 68 70 61 6e 64 61 2e ttp://te chpanda.
0240 6f 72 67 2f 0d 0a 41 63 63 65 70 74 2d 45 6e 63 org/-/Ac cept-Enc
0250 6f 64 69 6e 67 3a 20 67 7a 69 70 2c 20 64 65 66 oding: g zip, def
0260 6c 61 74 65 0d 0a 41 63 63 65 70 74 2d 4c 61 6e late -Ac cept-Lan
0270 67 75 61 67 65 3a 20 65 6e 2d 49 4e 2c 65 6e 2d guage: e n-IN,en
0280 47 42 3b 71 3d 30 2e 39 2c 65 6e 2d 55 53 3b 71 GB;q=0.9 ,en-US;q
0290 3d 30 2e 38 2c 65 6e 3b 71 3d 30 2e 37 2c 68 69 =0.8,en; q=0.7,hi
02a0 3b 71 3d 30 2e 36 0d 0a 43 6f 6f 6b 69 65 3a 20 ;q=0.6 - Cookie:
02b0 50 48 50 53 45 53 45 49 44 3d 39 36 37 61 33 30 PHPSESS1 D=967a30
02c0 30 31 39 63 39 38 38 30 38 37 35 32 64 34 63 38 019c9808 8752d4c8
02d0 37 62 31 65 39 33 36 39 66 34 0d 0a 65 6d 7b1e9369 f4...m
02e0 61 69 6c 3d 6f 6e 6b 61 72 31 35 25 34 30 6f 70 all=onka r1540op
02f0 65 6e 74 72 61 73 68 2e 63 6f 6d 26 70 61 73 73 entresh. com&pass
0300 77 6f 72 64 3d 37 38 39 34 35 3d word=789 456
```