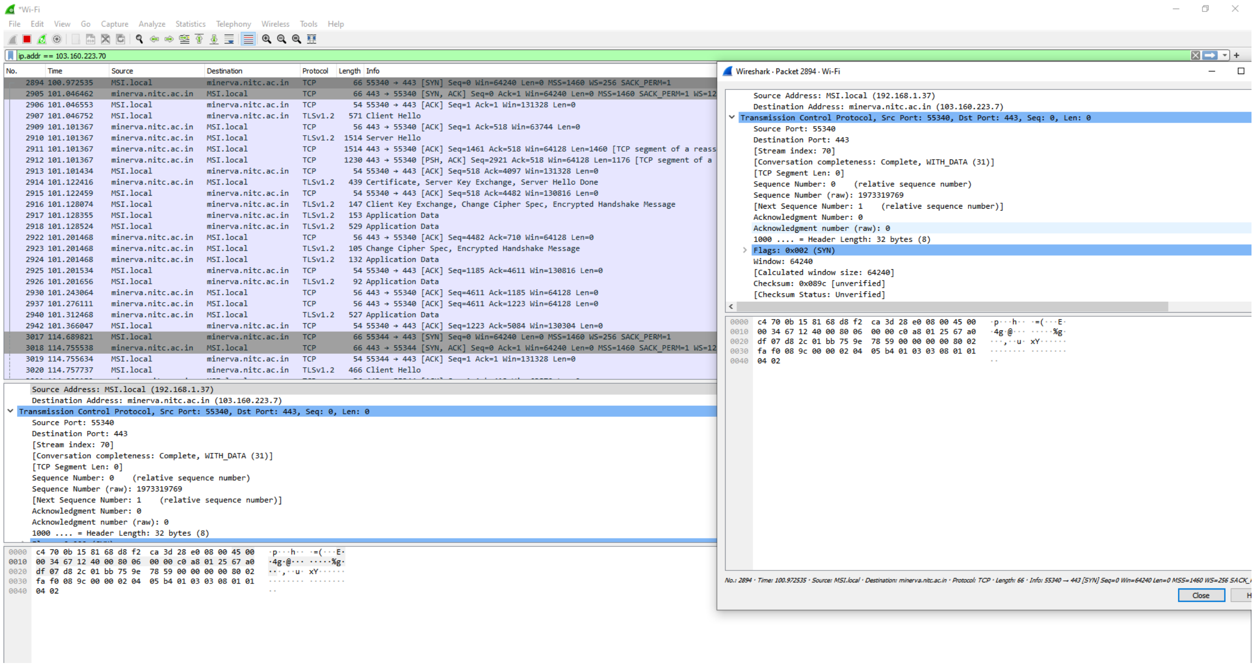
NETWORKS LAB
CS3093D
ASSIGNMENT 2

Submitted by,
Indrajith T S
B180486CS
S8 - Btech

1. Running wireshark in paralle with the wget command on the given link(https://minerva.nitc.ac.in/sites/default/files/attachments/news/TT_Winter2021-2022%20%281%29.pdf).



ip.addr == 103.160.223.70

```
No.   Time        Source              Destination         Protocol  Length Info
 2894 100.972535  MSI.local           minerva.nitc.ac.in  TCP         66 55340 → 443 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 WS=256 SACK_PERM=1
 2905 101.046462  minerva.nitc.ac.in  MSI.local           TCP         66 443 → 55340 [SYN, ACK] Seq=0 Ack=1 Win=64240 Len=0 MSS=1460 SACK_PERM=1 WS=12
 2906 101.046553  MSI.local           minerva.nitc.ac.in  TCP         54 55340 → 443 [ACK] Seq=1 Ack=1 Win=131328 Len=0
 2907 101.046752  MSI.local           minerva.nitc.ac.in  TLSv1.2    571 Client Hello
 2909 101.101367  minerva.nitc.ac.in  MSI.local           TCP         56 443 → 55340 [ACK] Seq=1 Ack=518 Win=63744 Len=0
 2910 101.101367  minerva.nitc.ac.in  MSI.local           TLSv1.2   1514 Server Hello
 2911 101.101367  minerva.nitc.ac.in  MSI.local           TCP       1514 443 → 55340 [ACK] Seq=1461 Ack=518 Win=64128 Len=1460 [TCP segment of a reass
 2912 101.101367  minerva.nitc.ac.in  MSI.local           TCP       1230 443 → 55340 [PSH, ACK] Seq=2921 Ack=518 Win=64128 Len=1176 [TCP segment of a
 2913 101.101434  MSI.local           minerva.nitc.ac.in  TCP         54 55340 → 443 [ACK] Seq=518 Ack=4097 Win=131328 Len=0
 2914 101.122416  minerva.nitc.ac.in  MSI.local           TLSv1.2    439 Certificate, Server Key Exchange, Server Hello Done
 2915 101.122459  MSI.local           minerva.nitc.ac.in  TCP         54 55340 → 443 [ACK] Seq=518 Ack=4482 Win=130816 Len=0
 2916 101.128074  MSI.local           minerva.nitc.ac.in  TLSv1.2    147 Client Key Exchange, Change Cipher Spec, Encrypted Handshake Message
 2917 101.128355  MSI.local           minerva.nitc.ac.in  TLSv1.2    153 Application Data
 2918 101.128524  MSI.local           minerva.nitc.ac.in  TLSv1.2    529 Application Data
 2922 101.201468  minerva.nitc.ac.in  MSI.local           TCP         56 443 → 55340 [ACK] Seq=4482 Ack=710 Win=64128 Len=0
 2923 101.201468  minerva.nitc.ac.in  MSI.local           TLSv1.2    105 Change Cipher Spec, Encrypted Handshake Message
 2924 101.201468  minerva.nitc.ac.in  MSI.local           TLSv1.2    132 Application Data
 2925 101.201534  MSI.local           minerva.nitc.ac.in  TCP         54 55340 → 443 [ACK] Seq=1185 Ack=4611 Win=130816 Len=0
 2926 101.201656  MSI.local           minerva.nitc.ac.in  TLSv1.2     92 Application Data
 2930 101.243064  minerva.nitc.ac.in  MSI.local           TCP         56 443 → 55340 [ACK] Seq=4611 Ack=1185 Win=64128 Len=0
 2937 101.276111  minerva.nitc.ac.in  MSI.local           TCP         56 443 → 55340 [ACK] Seq=4611 Ack=1223 Win=64128 Len=0
 2940 101.312468  minerva.nitc.ac.in  MSI.local           TLSv1.2    527 Application Data
 2942 101.366047  MSI.local           minerva.nitc.ac.in  TCP         54 55340 → 443 [ACK] Seq=1223 Ack=5084 Win=130304 Len=0
 3017 114.689821  MSI.local           minerva.nitc.ac.in  TCP         66 55344 → 443 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 WS=256 SACK_PERM=1
 3018 114.755538  minerva.nitc.ac.in  MSI.local           TCP         66 443 → 55344 [SYN, ACK] Seq=0 Ack=1 Win=64240 Len=0 MSS=1460 SACK_PERM=1 WS=12
 3019 114.755634  MSI.local           minerva.nitc.ac.in  TCP         54 55344 → 443 [ACK] Seq=1 Ack=1 Win=131328 Len=0
 3020 114.757737  MSI.local           minerva.nitc.ac.in  TLSv1.2    466 Client Hello
```

```
    Source Address: MSI.local (192.168.1.37)
    Destination Address: minerva.nitc.ac.in (103.160.223.7)
v Transmission Control Protocol, Src Port: 55340, Dst Port: 443, Seq: 0, Len: 0
    Source Port: 55340
    Destination Port: 443
    [Stream index: 70]
    [Conversation completeness: Complete, WITH_DATA (31)]
    [TCP Segment Len: 0]
    Sequence Number: 0    (relative sequence number)
    Sequence Number (raw): 1973319769
    [Next Sequence Number: 1    (relative sequence number)]
    Acknowledgment Number: 0
    Acknowledgment number (raw): 0
    1000 .... = Header Length: 32 bytes (8)
```

```
0000  c4 70 0b 15 81 68 d8 f2  ca 3d 28 e0 08 00 45 00   ·p···h·· ·=(···E·
0010  00 34 67 12 40 00 80 06  00 00 c0 a8 01 25 67 a0   ·4g·@··· ·····%g·
0020  df 07 d8 2c 01 bb 75 9e  78 59 00 00 00 00 80 02   ···,··u· xY······
0030  fa f0 08 9c 00 00 02 04  05 b4 01 03 03 08 01 01   ········ ········
0040  04 02                                              ··
```

Wireshark · Packet 2894 · Wi-Fi

```
    Source Address: MSI.local (192.168.1.37)
    Destination Address: minerva.nitc.ac.in (103.160.223.7)
v Transmission Control Protocol, Src Port: 55340, Dst Port: 443, Seq: 0, Len: 0
    Source Port: 55340
    Destination Port: 443
    [Stream index: 70]
    [Conversation completeness: Complete, WITH_DATA (31)]
    [TCP Segment Len: 0]
    Sequence Number: 0    (relative sequence number)
    Sequence Number (raw): 1973319769
    [Next Sequence Number: 1    (relative sequence number)]
    Acknowledgment Number: 0
    Acknowledgment number (raw): 0
    1000 .... = Header Length: 32 bytes (8)
```

```
  > Flags: 0x002 (SYN)
    Window: 64240
    [Calculated window size: 64240]
    Checksum: 0x089c [unverified]
    [Checksum Status: Unverified]
```

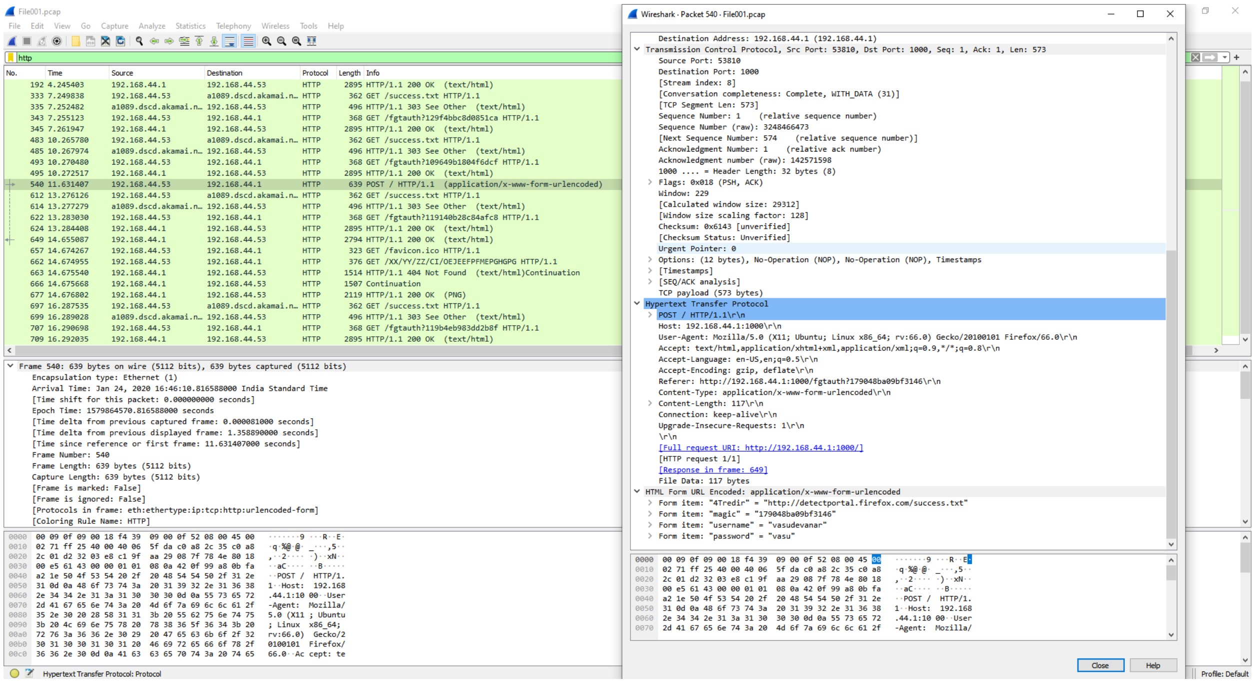
```
0000  c4 70 0b 15 81 68 d8 f2  ca 3d 28 e0 08 00 45 00   ·p···h·· ·=(···E·
0010  00 34 67 12 40 00 80 06  00 00 c0 a8 01 25 67 a0   ·4g·@··· ·····%g·
0020  df 07 d8 2c 01 bb 75 9e  78 59 00 00 00 00 80 02   ···,··u· xY······
0030  fa f0 08 9c 00 00 02 04  05 b4 01 03 03 08 01 01   ········ ········
0040  04 02                                              ··
```

No.: 2894 · Time: 100.972535 · Source: MSI.local · Destination: minerva.nitc.ac.in · Protocol: TCP · Length: 66 · Info: 55340 → 443 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 WS=256 SACK_

After sniffing the packet in the wifi interface while running the above results were obtained and then a filter with the ip of minerva.nitc.ac.in is applied to the result. Some observations made were :-

- The communication starts with the three-way handshake for the tcp protocol.
- Source ip is 192.168.1.37 destination ip is 103.160.223.7
- Browser program in port 55340 destination server port in 443.
- Sequence number is the last sequence no plus the size of the window while the acknowledge number is the next sequence number of the other machine.
- Application data is set through multiple packets using encryption of data with http-over-tls protocol.
- Connection was reseted using RST flag and then re established.

2. The pcap file was analysed and following conclusions were obtained.


File001.pcap
File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help
http
Wireshark · Packet 540 · File001.pcap
Close
Help
Hypertext Transfer Protocol: Protocol
Profile: Default

```
No.  Time       Source               Destination          Protocol Length Info
 192 4.245403   192.168.44.1         192.168.44.53        HTTP     2895 HTTP/1.1 200 OK  (text/html)
 333 7.249838   192.168.44.53        a1089.dscd.akamai.n… HTTP      362 GET /success.txt HTTP/1.1
 335 7.252482   a1089.dscd.akamai.n… 192.168.44.53        HTTP      496 HTTP/1.1 303 See Other  (text/html)
 343 7.255123   192.168.44.53        192.168.44.1         HTTP      368 GET /fgtauth?129f4bbc8d0851ca HTTP/1.1
 345 7.261947   192.168.44.1         192.168.44.53        HTTP     2895 HTTP/1.1 200 OK  (text/html)
 483 10.265780  192.168.44.53        a1089.dscd.akamai.n… HTTP      362 GET /success.txt HTTP/1.1
 485 10.267974  a1089.dscd.akamai.n… 192.168.44.53        HTTP      496 HTTP/1.1 303 See Other  (text/html)
 493 10.270480  192.168.44.53        192.168.44.1         HTTP      368 GET /fgtauth?109649b1804f6dcf HTTP/1.1
 495 10.272517  192.168.44.1         192.168.44.53        HTTP     2895 HTTP/1.1 200 OK  (text/html)
 540 11.631407  192.168.44.53        192.168.44.1         HTTP      639 POST / HTTP/1.1  (application/x-www-form-urlencoded)
 612 13.276126  192.168.44.53        a1089.dscd.akamai.n… HTTP      362 GET /success.txt HTTP/1.1
 614 13.277279  a1089.dscd.akamai.n… 192.168.44.53        HTTP      496 HTTP/1.1 303 See Other  (text/html)
 622 13.283030  192.168.44.53        192.168.44.1         HTTP      368 GET /fgtauth?119140b28c84afc8 HTTP/1.1
 624 13.284408  192.168.44.1         192.168.44.53        HTTP     2895 HTTP/1.1 200 OK  (text/html)
 649 14.655087  192.168.44.1         192.168.44.53        HTTP     2794 HTTP/1.1 200 OK  (text/html)
 657 14.674267  192.168.44.53        192.168.44.1         HTTP      323 GET /favicon.ico HTTP/1.1
 662 14.674955  192.168.44.53        192.168.44.1         HTTP      376 GET /XX/YY/ZZ/CI/OEJEEFPFMEPGHGPG HTTP/1.1
 663 14.675540  192.168.44.1         192.168.44.53        HTTP     1514 HTTP/1.1 404 Not Found  (text/html)Continuation
 666 14.675668  192.168.44.1         192.168.44.53        HTTP     1507 Continuation
 677 14.676802  192.168.44.1         192.168.44.53        HTTP     2119 HTTP/1.1 200 OK  (PNG)
 697 16.287535  192.168.44.53        a1089.dscd.akamai.n… HTTP      362 GET /success.txt HTTP/1.1
 699 16.289028  a1089.dscd.akamai.n… 192.168.44.53        HTTP      496 HTTP/1.1 303 See Other  (text/html)
 707 16.290698  192.168.44.53        192.168.44.1         HTTP      368 GET /fgtauth?119b4eb983dd2b8f HTTP/1.1
 709 16.292035  192.168.44.1         192.168.44.53        HTTP     2895 HTTP/1.1 200 OK  (text/html)
```

```
Frame 540: 639 bytes on wire (5112 bits), 639 bytes captured (5112 bits)
    Encapsulation type: Ethernet (1)
    Arrival Time: Jan 24, 2020 16:46:10.816588000 India Standard Time
    [Time shift for this packet: 0.000000000 seconds]
    Epoch Time: 1579864570.816588000 seconds
    [Time delta from previous captured frame: 0.000081000 seconds]
    [Time delta from previous displayed frame: 1.358890000 seconds]
    [Time since reference or first frame: 11.631407000 seconds]
    Frame Number: 540
    Frame Length: 639 bytes (5112 bits)
    Capture Length: 639 bytes (5112 bits)
    [Frame is marked: False]
    [Frame is ignored: False]
    [Protocols in frame: eth:ethertype:ip:tcp:http:urlencoded-form]
    [Coloring Rule Name: HTTP]
```

```
0000  00 09 0f 09 00 18 f4 39  09 00 0f 52 08 00 45 00   ·······9 ···R··E·
0010  02 71 ff 25 40 00 40 06  5f da c0 a8 2c 35 c0 a8   ·q·%@·@· _···,5··
0020  2c 01 d2 32 03 e8 c1 9f  aa 29 08 7f 78 4e 80 18   ,··2···· ·)··xN··
0030  00 e5 61 43 00 00 01 01  08 0a 42 0f 99 a8 0b fa   ··aC···· ··B·····
0040  a2 1e 50 4f 53 54 20 2f  20 48 54 54 50 2f 31 2e   ··POST /  HTTP/1.
0050  31 0d 0a 48 6f 73 74 3a  20 31 39 32 2e 31 36 38   1··Host:  192.168
0060  2e 34 34 2e 31 3a 31 30  30 30 0d 0a 55 73 65 72   .44.1:10 00··User
0070  2d 41 67 65 6e 74 3a 20  4d 6f 7a 69 6c 6c 61 2f   -Agent:  Mozilla/
0080  35 2e 30 20 28 58 31 31  3b 20 55 62 75 6e 74 75   5.0 (X11 ; Ubuntu
0090  3b 20 4c 69 6e 75 78 20  78 38 36 5f 36 34 3b 20   ; Linux  x86_64;
00a0  72 76 3a 36 36 2e 30 29  20 47 65 63 6b 6f 2f 32   rv:66.0)  Gecko/2
00b0  30 31 30 30 31 30 31 20  46 69 72 65 66 6f 78 2f   0100101  Firefox/
00c0  36 36 2e 30 0d 0a 41 63  63 65 70 74 3a 20 74 65   66.0··Ac cept: te
```

```
    Destination Address: 192.168.44.1 (192.168.44.1)
Transmission Control Protocol, Src Port: 53810, Dst Port: 1000, Seq: 1, Ack: 1, Len: 573
    Source Port: 53810
    Destination Port: 1000
    [Stream index: 8]
    [Conversation completeness: Complete, WITH_DATA (31)]
    [TCP Segment Len: 573]
    Sequence Number: 1    (relative sequence number)
    Sequence Number (raw): 3248466473
    [Next Sequence Number: 574    (relative sequence number)]
    Acknowledgment Number: 1    (relative ack number)
    Acknowledgment number (raw): 142571598
    1000 .... = Header Length: 32 bytes (8)
  > Flags: 0x018 (PSH, ACK)
    Window: 229
    [Calculated window size: 29312]
    [Window size scaling factor: 128]
    Checksum: 0x6143 [unverified]
    [Checksum Status: Unverified]
    Urgent Pointer: 0
  > Options: (12 bytes), No-Operation (NOP), No-Operation (NOP), Timestamps
  > [Timestamps]
  > [SEQ/ACK analysis]
    TCP payload (573 bytes)
Hypertext Transfer Protocol
  > POST / HTTP/1.1\r\n
    Host: 192.168.44.1:1000\r\n
    User-Agent: Mozilla/5.0 (X11; Ubuntu; Linux x86_64; rv:66.0) Gecko/20100101 Firefox/66.0\r\n
    Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8\r\n
    Accept-Language: en-US,en;q=0.5\r\n
    Accept-Encoding: gzip, deflate\r\n
    Referer: http://192.168.44.1:1000/fgtauth?179048ba09bf3146\r\n
    Content-Type: application/x-www-form-urlencoded\r\n
  > Content-Length: 117\r\n
    Connection: keep-alive\r\n
    Upgrade-Insecure-Requests: 1\r\n
    \r\n
    [Full request URI: http://192.168.44.1:1000/]
    [HTTP request 1/1]
    [Response in frame: 649]
    File Data: 117 bytes
HTML Form URL Encoded: application/x-www-form-urlencoded
  > Form item: "4Tredir" = "http://detectportal.firefox.com/success.txt"
  > Form item: "magic" = "179048ba09bf3146"
  > Form item: "username" = "vasudevanar"
  > Form item: "password" = "vasu"
```

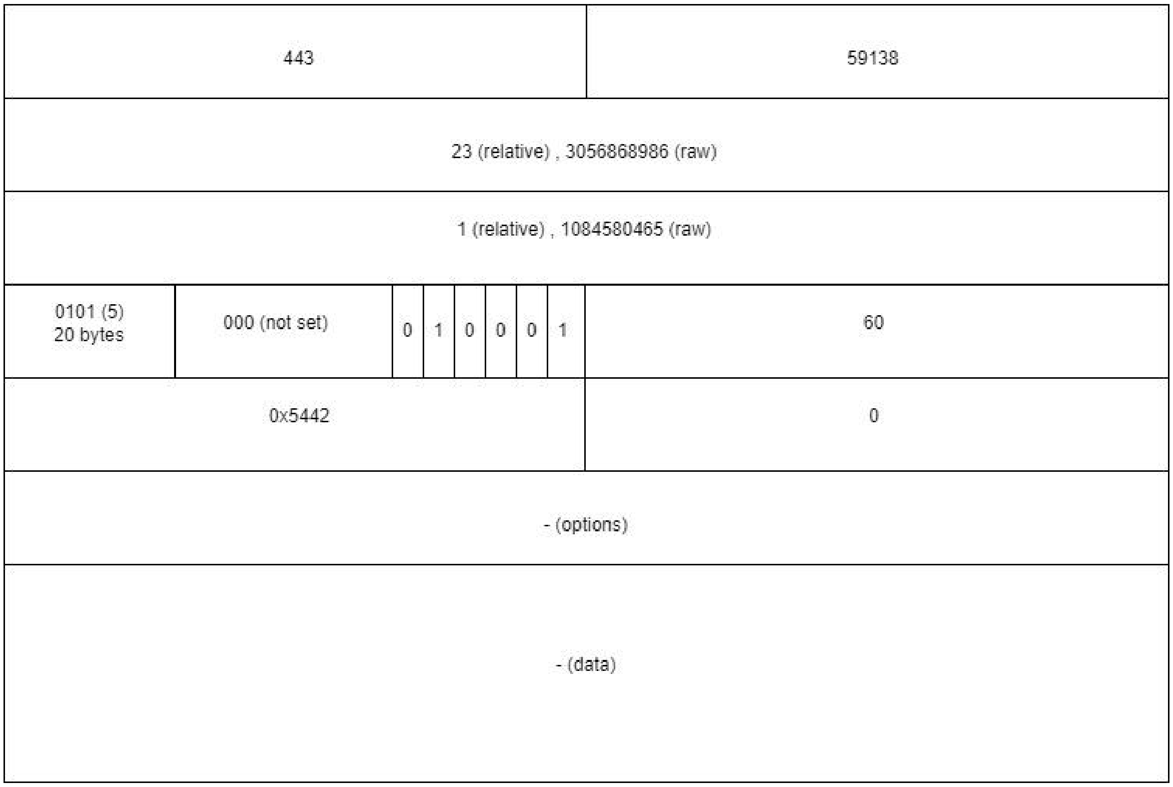
```
0000  00 09 0f 09 00 18 f4 39  09 00 0f 52 08 00 45 00   ·······9 ···R··E·
0010  02 71 ff 25 40 00 40 06  5f da c0 a8 2c 35 c0 a8   ·q·%@·@· _···,5··
0020  2c 01 d2 32 03 e8 c1 9f  aa 29 08 7f 78 4e 80 18   ,··2···· ·)··xN··
0030  00 e5 61 43 00 00 01 01  08 0a 42 0f 99 a8 0b fa   ··aC···· ··B·····
0040  a2 1e 50 4f 53 54 20 2f  20 48 54 54 50 2f 31 2e   ··POST /  HTTP/1.
0050  31 0d 0a 48 6f 73 74 3a  20 31 39 32 2e 31 36 38   1··Host:  192.168
0060  2e 34 34 2e 31 3a 31 30  30 30 0d 0a 55 73 65 72   .44.1:10 00··User
0070  2d 41 67 65 6e 74 3a 20  4d 6f 7a 69 6c 6c 61 2f   -Agent:  Mozilla/
```

a. Details of login credentials are found on packet 540.
Source ip = 192.168.44.53
Source port = 53810
Destination ip = 192.168.44.1
Destination port = 1000

b. These login credentials are sent over http protocol.
These are sent as plain text without any encryption.

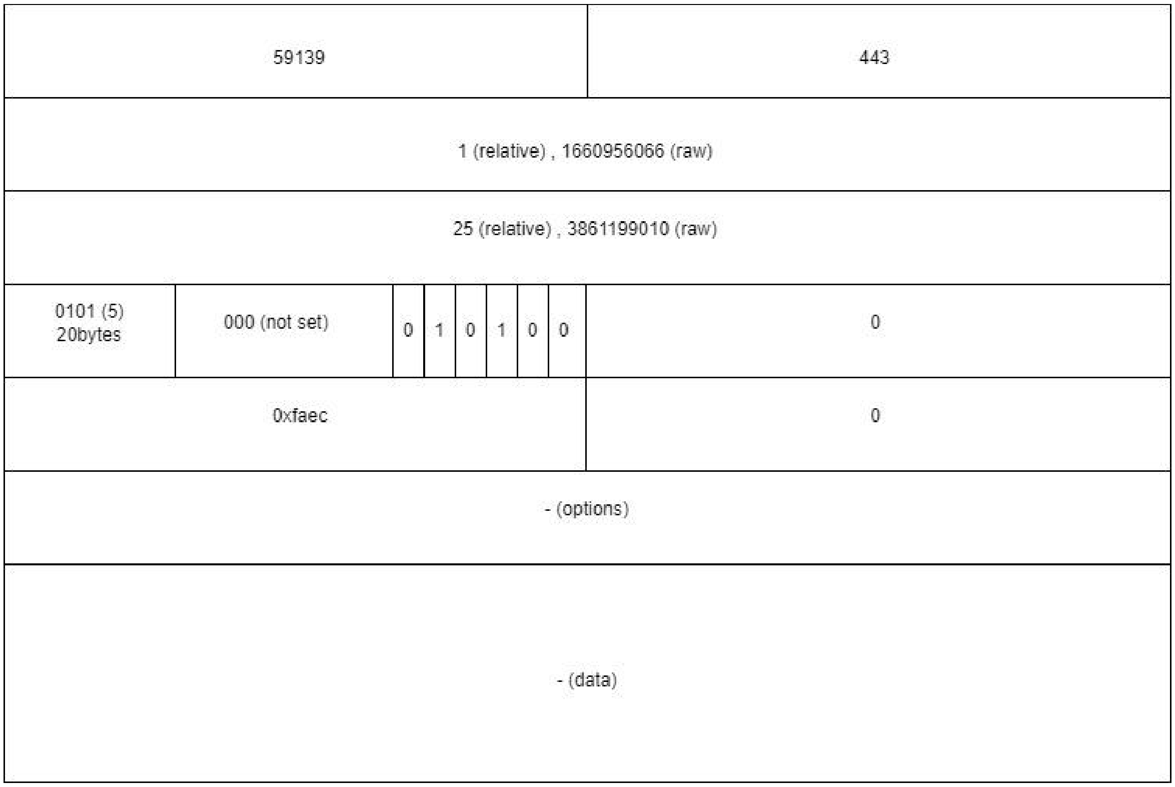
c. Login credentials:
“username” = “vasudevanar”
“password” = “vasu”

3. For packet 27 TCP header filled is as given below



443								59138
23 (relative) , 3056868986 (raw)								
1 (relative) , 1084580465 (raw)								
0101 (5) 20 bytes	000 (not set)	0	1	0	0	0	1	60
0x5442								0
- (options)								
- (data)								

For packet 32 is given below



59139								443
1 (relative) , 1660956066 (raw)								
25 (relative) , 3861199010 (raw)								
0101 (5) 20bytes	000 (not set)	0	1	0	1	0	0	0
0xfaec								0
- (options)								
- (data)								