GHARDA FOUNDATION

GHARDA INSTITUTE OF TECHNOLOGY, LAVEL

Department of Computer Engineering

Evaluation Sheet

Class: TE-Computer Engineering Sem: V

Subject: **Computer Networks**

Experiment No: 7

Title of Experiment: Study of Packets Capturing using Wireshark

Name of Student: Harvande Sanket Chandrashekhar Roll No: 19

Sr. No.	Evaluation Criteria	Max Marks	Marks Obtained
1	Practical Performance	8	
2	Oral	5	
3	Timely Submission	2	
	Total	15	

Signature of Subject Teacher
(Mr. S. S. Tathare)

Aim: To study the packets capturing using Wireshark.

Apparatus: Wireshark software
Procedure:

Step1: Install Wireshark & Select the interface on which packets will be captured

Step2: Start capturing and check for the fields viewed: Time(packet was received/sent;view-time display format), Source Ip, Destination IP, Protocol, Length, Information

Step3: Click on any TCP packet from your IP to other and check the frame info, ethernet info, IP(src and destn addr), TCP info(src port(temp),destn port no, seq no and ack no)

Step4: Click on capture again and continue without saving

Step5: Open GIT website on browser and now stop capturing packets on packet tracer and then check for http GET packet; you can see large packets captured in seconds

Step6: We can use filter and type HTTP and open the http packet and you will see the http section below TCP, which u can explore and see the 1) host as the website name visited 2)User-agent as Windows 10 and Chrome

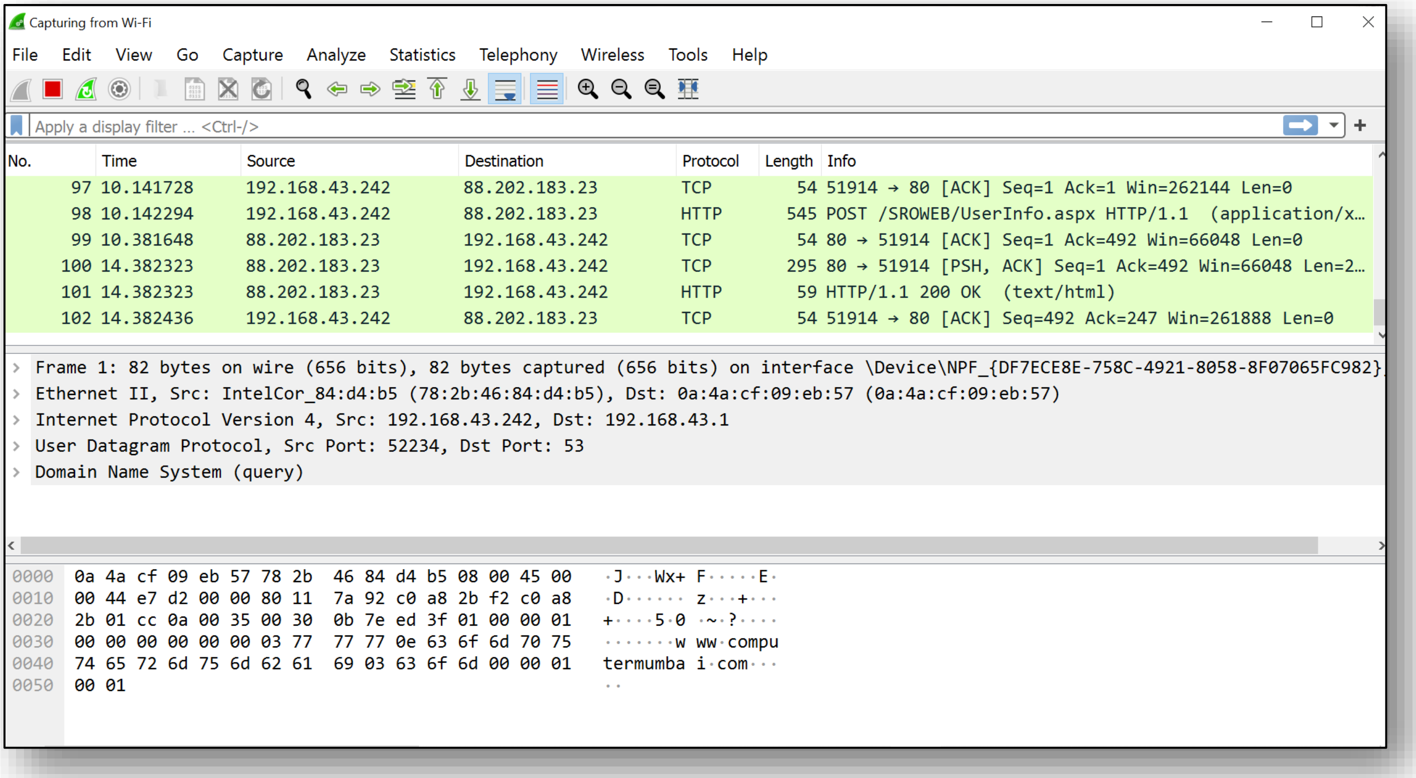
Step 7: If you want to check for the packets from certain source IP, click on that IP, right click and click on Apply as Filter and selected; "and selected" is for the filter to be applied for the given source IP along-with http

Step 8: Check for the http packets captured intended to us from webserver to us, which shows text/html OR text/css, and we can also see the corresponding html code.

Step 9: Check for the ARP packet which is used to check for the MAC address at the initial stage, till it gets discovered, which can also be shown.

Step 10: Check for the Port no 53 for DNS by filtering the corresponding packet.

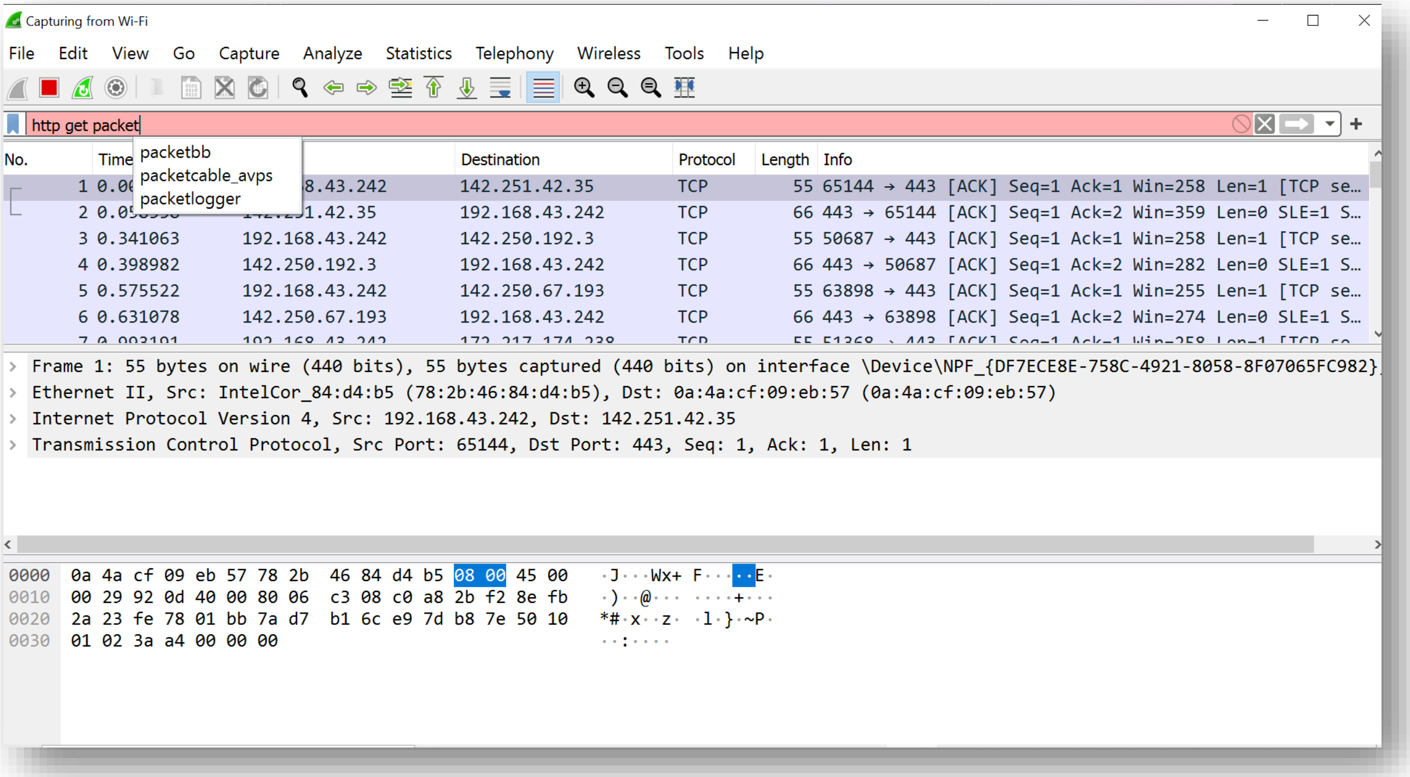
Screenshots:


Capturing from Wi-Fi
File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help
Apply a display filter … <Ctrl-/>

```
No.   Time       Source          Destination     Protocol Length Info
 97 10.141728  192.168.43.242  88.202.183.23   TCP       54 51914 → 80 [ACK] Seq=1 Ack=1 Win=262144 Len=0
 98 10.142294  192.168.43.242  88.202.183.23   HTTP     545 POST /SROWEB/UserInfo.aspx HTTP/1.1  (application/x…
 99 10.381648  88.202.183.23   192.168.43.242  TCP       54 80 → 51914 [ACK] Seq=1 Ack=492 Win=66048 Len=0
100 14.382323  88.202.183.23   192.168.43.242  TCP      295 80 → 51914 [PSH, ACK] Seq=1 Ack=492 Win=66048 Len=2…
101 14.382323  88.202.183.23   192.168.43.242  HTTP      59 HTTP/1.1 200 OK  (text/html)
102 14.382436  192.168.43.242  88.202.183.23   TCP       54 51914 → 80 [ACK] Seq=492 Ack=247 Win=261888 Len=0
```

```
> Frame 1: 82 bytes on wire (656 bits), 82 bytes captured (656 bits) on interface \Device\NPF_{DF7ECE8E-758C-4921-8058-8F07065FC982}
> Ethernet II, Src: IntelCor_84:d4:b5 (78:2b:46:84:d4:b5), Dst: 0a:4a:cf:09:eb:57 (0a:4a:cf:09:eb:57)
> Internet Protocol Version 4, Src: 192.168.43.242, Dst: 192.168.43.1
> User Datagram Protocol, Src Port: 52234, Dst Port: 53
> Domain Name System (query)
```

```
0000  0a 4a cf 09 eb 57 78 2b  46 84 d4 b5 08 00 45 00   ·J···Wx+ F·····E·
0010  00 44 e7 d2 00 00 80 11  7a 92 c0 a8 2b f2 c0 a8   ·D······ z···+···
0020  2b 01 cc 0a 00 35 00 30  0b 7e ed 3f 01 00 00 01   +····5·0 ·~·?····
0030  00 00 00 00 00 00 03 77  77 77 0e 63 6f 6d 70 75   ·······w ww·compu
0040  74 65 72 6d 75 6d 62 61  69 03 63 6f 6d 00 00 01   termumba i·com···
0050  00 01                                              ··
```

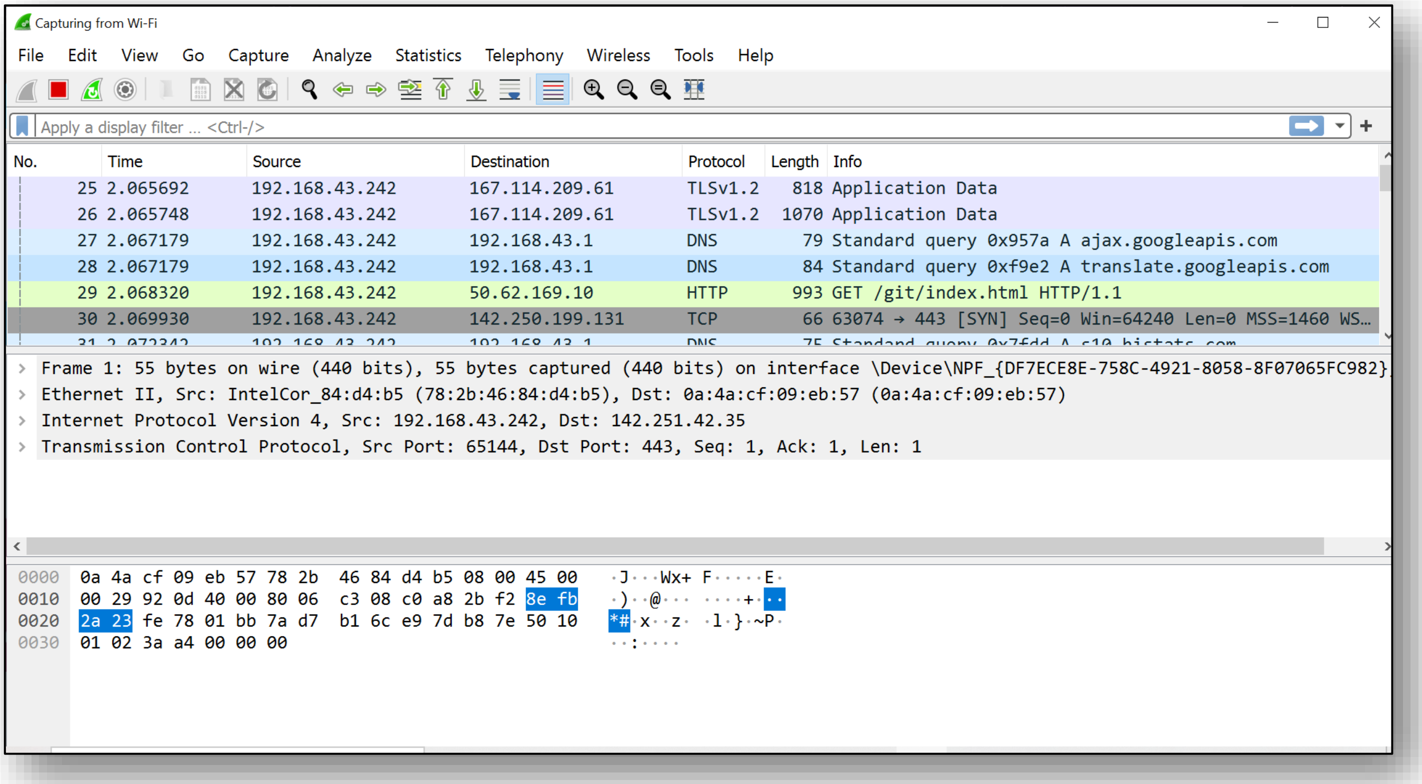

Capturing from Wi-Fi
File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help
packetbb
packetcable_avps
packetlogger

http get packet

```
No.   Time      Source          Destination      Protocol Length Info
  1 0.00       8.43.242        142.251.42.35    TCP       55 65144 → 443 [ACK] Seq=1 Ack=1 Win=258 Len=1 [TCP se…
  2 0.05       1.42.35         192.168.43.242   TCP       66 443 → 65144 [ACK] Seq=1 Ack=2 Win=359 Len=0 SLE=1 S…
  3 0.341063  192.168.43.242  142.250.192.3    TCP       55 50687 → 443 [ACK] Seq=1 Ack=1 Win=258 Len=1 [TCP se…
  4 0.398982  142.250.192.3   192.168.43.242   TCP       66 443 → 50687 [ACK] Seq=1 Ack=2 Win=282 Len=0 SLE=1 S…
  5 0.575522  192.168.43.242  142.250.67.193   TCP       55 63898 → 443 [ACK] Seq=1 Ack=1 Win=255 Len=1 [TCP se…
  6 0.631078  142.250.67.193  192.168.43.242   TCP       66 443 → 63898 [ACK] Seq=1 Ack=2 Win=274 Len=0 SLE=1 S…
  7 0.993101  192.168.43.242  172.217.174.238  TCP       55 51368 → 443 [ACK] Seq=1 Ack=1 Win=258 Len=1 [TCP se…
```

```
> Frame 1: 55 bytes on wire (440 bits), 55 bytes captured (440 bits) on interface \Device\NPF_{DF7ECE8E-758C-4921-8058-8F07065FC982}
> Ethernet II, Src: IntelCor_84:d4:b5 (78:2b:46:84:d4:b5), Dst: 0a:4a:cf:09:eb:57 (0a:4a:cf:09:eb:57)
> Internet Protocol Version 4, Src: 192.168.43.242, Dst: 142.251.42.35
> Transmission Control Protocol, Src Port: 65144, Dst Port: 443, Seq: 1, Ack: 1, Len: 1
```

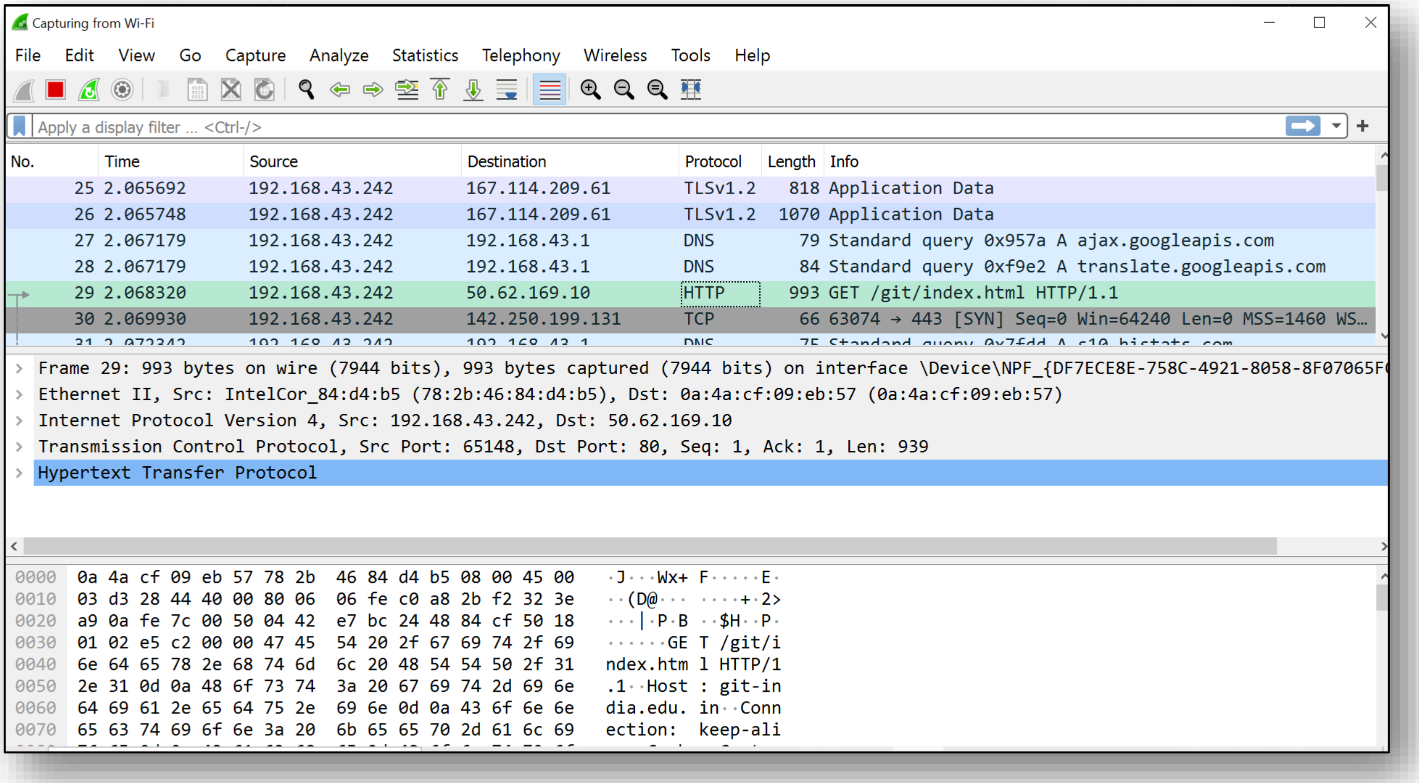
```
0000  0a 4a cf 09 eb 57 78 2b  46 84 d4 b5 08 00 45 00   ·J···Wx+ F·····E·
0010  00 29 92 0d 40 00 80 06  c3 08 c0 a8 2b f2 8e fb   ·)··@··· ····+···
0020  2a 23 fe 78 01 bb 7a d7  b1 6c e9 7d b8 7e 50 10   *#·x··z· ·l·}·~P·
0030  01 02 3a a4 00 00 00                               ··:····
```


Capturing from Wi-Fi
File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help
Apply a display filter ... <Ctrl-/>

```
No.   Time       Source          Destination      Protocol  Length Info
   25 2.065692   192.168.43.242  167.114.209.61   TLSv1.2    818 Application Data
   26 2.065748   192.168.43.242  167.114.209.61   TLSv1.2   1070 Application Data
   27 2.067179   192.168.43.242  192.168.43.1     DNS         79 Standard query 0x957a A ajax.googleapis.com
   28 2.067179   192.168.43.242  192.168.43.1     DNS         84 Standard query 0xf9e2 A translate.googleapis.com
   29 2.068320   192.168.43.242  50.62.169.10     HTTP       993 GET /git/index.html HTTP/1.1
   30 2.069930   192.168.43.242  142.250.199.131  TCP         66 63074 → 443 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 WS…
   31 2.072342   192.168.43.242  192.168.43.1     DNS         75 Standard query 0x7fdd A c10.histats.com
```

```
> Frame 1: 55 bytes on wire (440 bits), 55 bytes captured (440 bits) on interface \Device\NPF_{DF7ECE8E-758C-4921-8058-8F07065FC982}
> Ethernet II, Src: IntelCor_84:d4:b5 (78:2b:46:84:d4:b5), Dst: 0a:4a:cf:09:eb:57 (0a:4a:cf:09:eb:57)
> Internet Protocol Version 4, Src: 192.168.43.242, Dst: 142.251.42.35
> Transmission Control Protocol, Src Port: 65144, Dst Port: 443, Seq: 1, Ack: 1, Len: 1
```

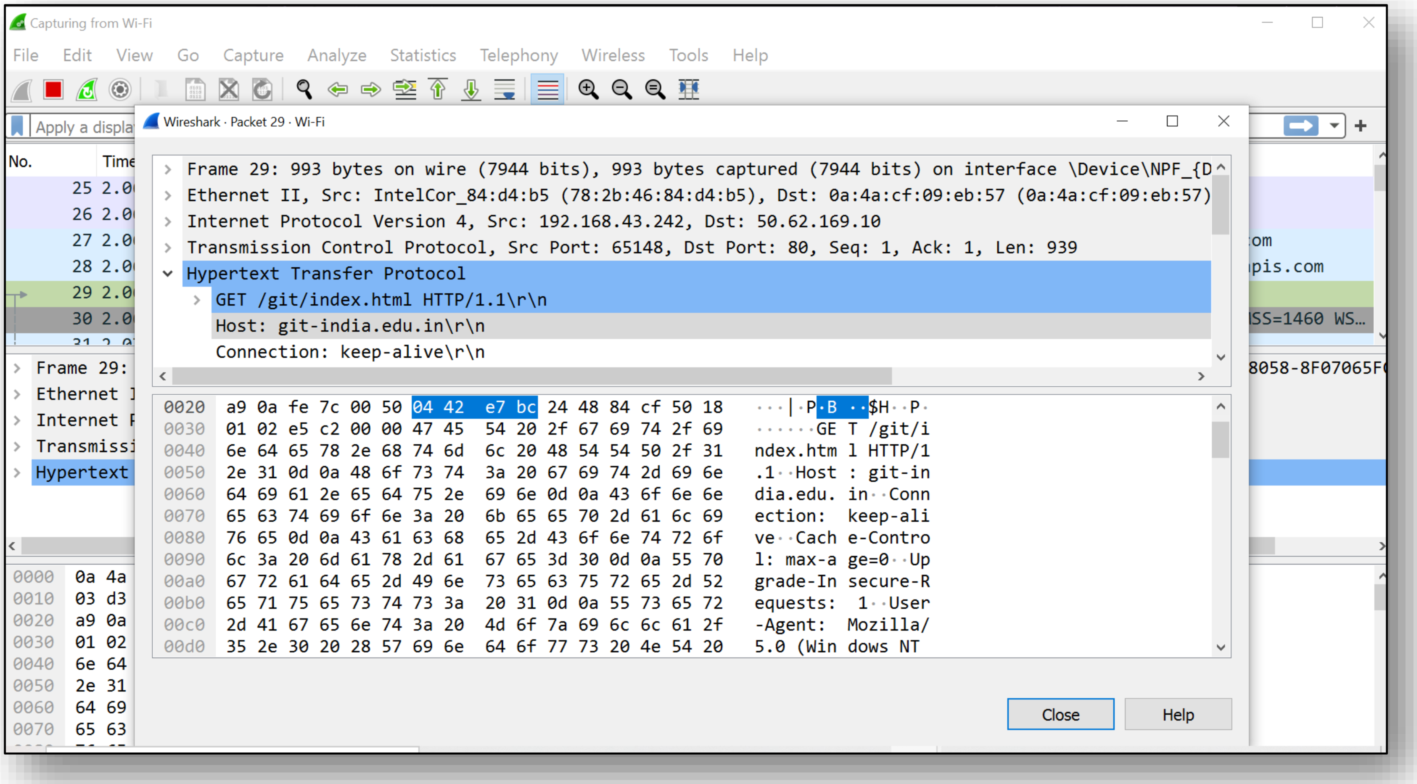
```
0000  0a 4a cf 09 eb 57 78 2b  46 84 d4 b5 08 00 45 00   ·J···Wx+ F·····E·
0010  00 29 92 0d 40 00 80 06  c3 08 c0 a8 2b f2 8e fb   ·)··@··· ····+···
0020  2a 23 fe 78 01 bb 7a d7  b1 6c e9 7d b8 7e 50 10   *#·x··z· ·l·}·~P·
0030  01 02 3a a4 00 00 00                               ··:····
```


Capturing from Wi-Fi
File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help
Apply a display filter ... <Ctrl-/>

```
No.   Time       Source          Destination      Protocol  Length Info
   25 2.065692   192.168.43.242  167.114.209.61   TLSv1.2    818 Application Data
   26 2.065748   192.168.43.242  167.114.209.61   TLSv1.2   1070 Application Data
   27 2.067179   192.168.43.242  192.168.43.1     DNS         79 Standard query 0x957a A ajax.googleapis.com
   28 2.067179   192.168.43.242  192.168.43.1     DNS         84 Standard query 0xf9e2 A translate.googleapis.com
   29 2.068320   192.168.43.242  50.62.169.10     HTTP       993 GET /git/index.html HTTP/1.1
   30 2.069930   192.168.43.242  142.250.199.131  TCP         66 63074 → 443 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 WS…
   31 2.072342   192.168.43.242  192.168.43.1     DNS         75 Standard query 0x7fdd A c10.histats.com
```

```
> Frame 29: 993 bytes on wire (7944 bits), 993 bytes captured (7944 bits) on interface \Device\NPF_{DF7ECE8E-758C-4921-8058-8F07065F
> Ethernet II, Src: IntelCor_84:d4:b5 (78:2b:46:84:d4:b5), Dst: 0a:4a:cf:09:eb:57 (0a:4a:cf:09:eb:57)
> Internet Protocol Version 4, Src: 192.168.43.242, Dst: 50.62.169.10
> Transmission Control Protocol, Src Port: 65148, Dst Port: 80, Seq: 1, Ack: 1, Len: 939
> Hypertext Transfer Protocol
```

```
0000  0a 4a cf 09 eb 57 78 2b  46 84 d4 b5 08 00 45 00   ·J···Wx+ F·····E·
0010  03 d3 28 44 40 00 80 06  06 fe c0 a8 2b f2 32 3e   ··(D@··· ····+·2>
0020  a9 0a fe 7c 00 50 04 42  e7 bc 24 48 84 cf 50 18   ···|·P·B ··$H··P·
0030  01 02 e5 c2 00 00 47 45  54 20 2f 67 69 74 2f 69   ······GE T /git/i
0040  6e 64 65 78 2e 68 74 6d  6c 20 48 54 54 50 2f 31   ndex.htm l HTTP/1
0050  2e 31 0d 0a 48 6f 73 74  3a 20 67 69 74 2d 69 6e   .1··Host : git-in
0060  64 69 61 2e 65 64 75 2e  69 6e 0d 0a 43 6f 6e 6e   dia.edu. in··Conn
0070  65 63 74 69 6f 6e 3a 20  6b 65 65 70 2d 61 6c 69   ection:  keep-ali
```



Capturing from Wi-Fi
File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help
Apply a displa
Wireshark · Packet 29 · Wi-Fi
Close
Help

```
> Frame 29: 993 bytes on wire (7944 bits), 993 bytes captured (7944 bits) on interface \Device\NPF_{D
> Ethernet II, Src: IntelCor_84:d4:b5 (78:2b:46:84:d4:b5), Dst: 0a:4a:cf:09:eb:57 (0a:4a:cf:09:eb:57)
> Internet Protocol Version 4, Src: 192.168.43.242, Dst: 50.62.169.10
> Transmission Control Protocol, Src Port: 65148, Dst Port: 80, Seq: 1, Ack: 1, Len: 939
v Hypertext Transfer Protocol
  > GET /git/index.html HTTP/1.1\r\n
    Host: git-india.edu.in\r\n
    Connection: keep-alive\r\n
```

```
0020  a9 0a fe 7c 00 50 04 42  e7 bc 24 48 84 cf 50 18   ···|·P·B ··$H··P·
0030  01 02 e5 c2 00 00 47 45  54 20 2f 67 69 74 2f 69   ······GE T /git/i
0040  6e 64 65 78 2e 68 74 6d  6c 20 48 54 54 50 2f 31   ndex.htm l HTTP/1
0050  2e 31 0d 0a 48 6f 73 74  3a 20 67 69 74 2d 69 6e   .1··Host : git-in
0060  64 69 61 2e 65 64 75 2e  69 6e 0d 0a 43 6f 6e 6e   dia.edu. in··Conn
0070  65 63 74 69 6f 6e 3a 20  6b 65 65 70 2d 61 6c 69   ection:  keep-ali
0080  76 65 0d 0a 43 61 63 68  65 2d 43 6f 6e 74 72 6f   ve··Cach e-Contro
0090  6c 3a 20 6d 61 78 2d 61  67 65 3d 30 0d 0a 55 70   l: max-a ge=0··Up
00a0  67 72 61 64 65 2d 49 6e  73 65 63 75 72 65 2d 52   grade-In secure-R
00b0  65 71 75 65 73 74 73 3a  20 31 0d 0a 55 73 65 72   equests:  1··User
00c0  2d 41 67 65 6e 74 3a 20  4d 6f 7a 69 6c 6c 61 2f   -Agent:  Mozilla/
00d0  35 2e 30 20 28 57 69 6e  64 6f 77 73 20 4e 54 20   5.0 (Win dows NT
```

Conclusion: Thus the study of packets capturing is done using Wireshark software.