



SRI LANKA INSTITUTE OF INFORMATION TECHNOLOGY

**Information Systems Security Audit & Control**

**4<sup>th</sup> Year 2<sup>nd</sup> Semester 2016**

Name: Harshanath W.W.D.K

SLIIT ID: IT13069032

Practical Session: WE Friday

Practical Number: Lab 4

Date of Evaluation : \_\_\_\_\_

Evaluators Signature : \_\_\_\_\_

# Wireshark

Wireshark is the world's foremost network protocol analyzer. It lets you see what's happening on your network at a microscopic level. It is the de facto (and often de jure) standard across many industries and educational institutions.

Wireshark development thrives thanks to the contributions of networking experts across the globe. It is the continuation of a project that started in 1998.

## Wireshark Filters

### Display Filters

Wireshark uses display filters for general packet filtering while viewing and for its ColoringRules.

The basics and the syntax of the display filters are described in the User's Guide.

The master list of display filter protocol fields can be found in the display filter reference.

If you need a display filter for a specific protocol, have a look for it at the ProtocolReference.

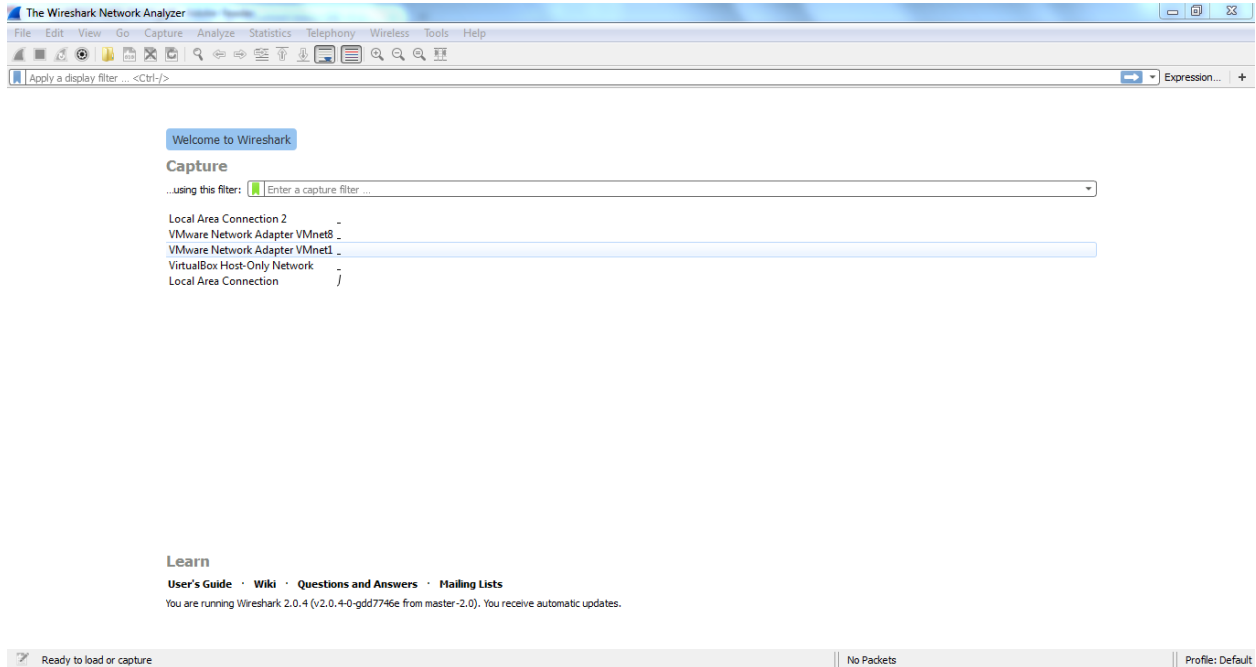
### Capture Filters

An overview of the capture filter syntax can be found in the User's Guide. A complete reference can be found in the expression section of the tcpdump manual page.

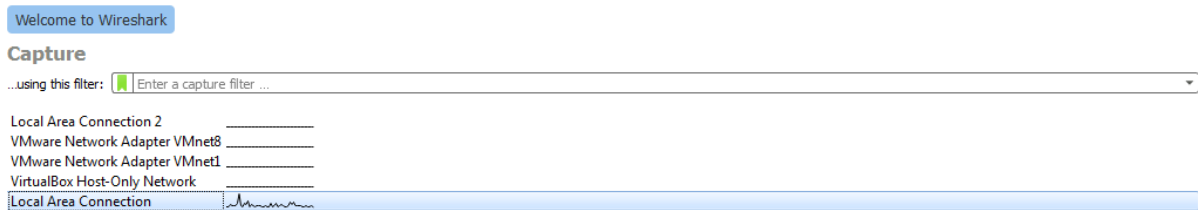
Wireshark uses the same syntax for capture filters as tcpdump, WinDump, Analyzer, and any other program that uses the libpcap/WinPcap library.

If you need a capture filter for a specific protocol, have a look for it at the ProtocolReference.

## Step 01: Open Wireshark software



## Step 02: Select internet connection (Ethernet, LAN or wireless)



## Step 03: Start capturing from Local Area Connection

The image shows the Wireshark network protocol analyzer interface. The top menu bar includes File, Edit, View, Go, Capture, Analyze, Statistics, Telephony, Wireless, Tools, and Help. Below the menu is a toolbar with various icons for file operations, capture control, and analysis. The main window is divided into three panes:

- Packet List:** Displays a list of captured packets. The selected packet is 21, a TCP RST, ACK packet from 192.168.10.110 to 52.32.185.255.
- Packet Details:** Shows the hierarchical structure of the selected packet. It includes Ethernet II, Internet Protocol Version 4, and User Datagram Protocol.
- Packet Bytes:** Displays the raw packet data in hexadecimal and ASCII.

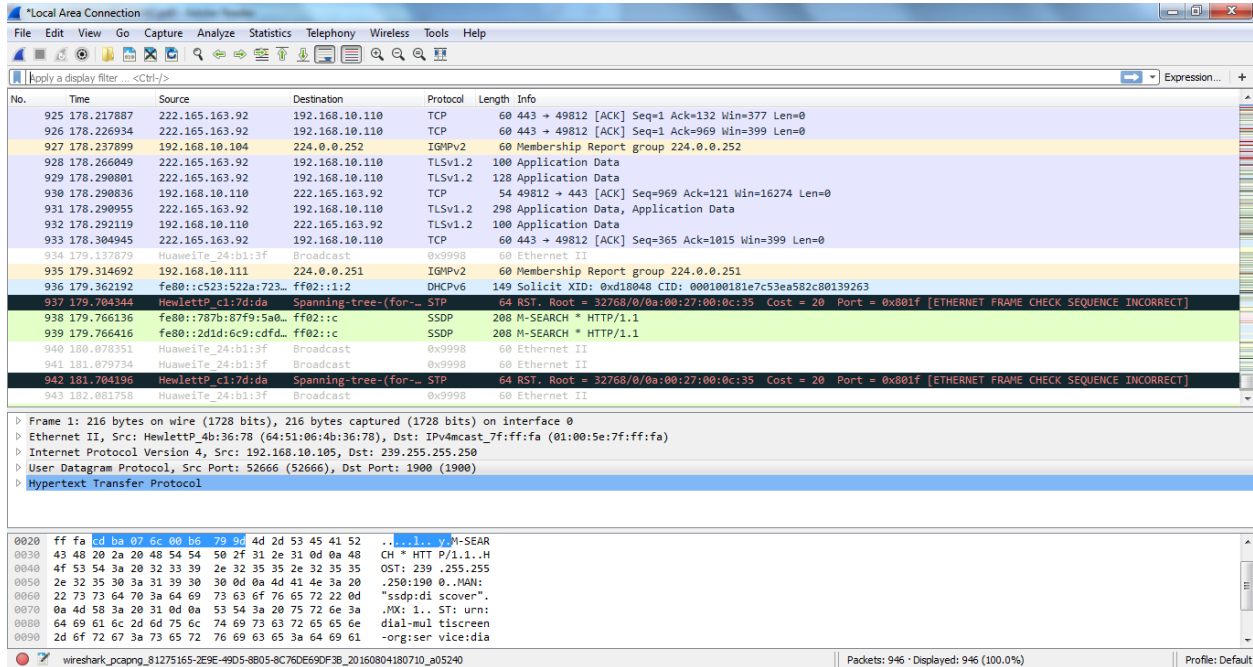
The status bar at the bottom indicates "Local Area Connection: <live capture in progress>" and "Packets: 44 · Displayed: 44 (100.0%)".

## Step 04: Observe used protocols and details

The image shows the "Packet Details" pane in Wireshark, displaying the protocol stack for the selected packet. The protocols are listed in a tree view:

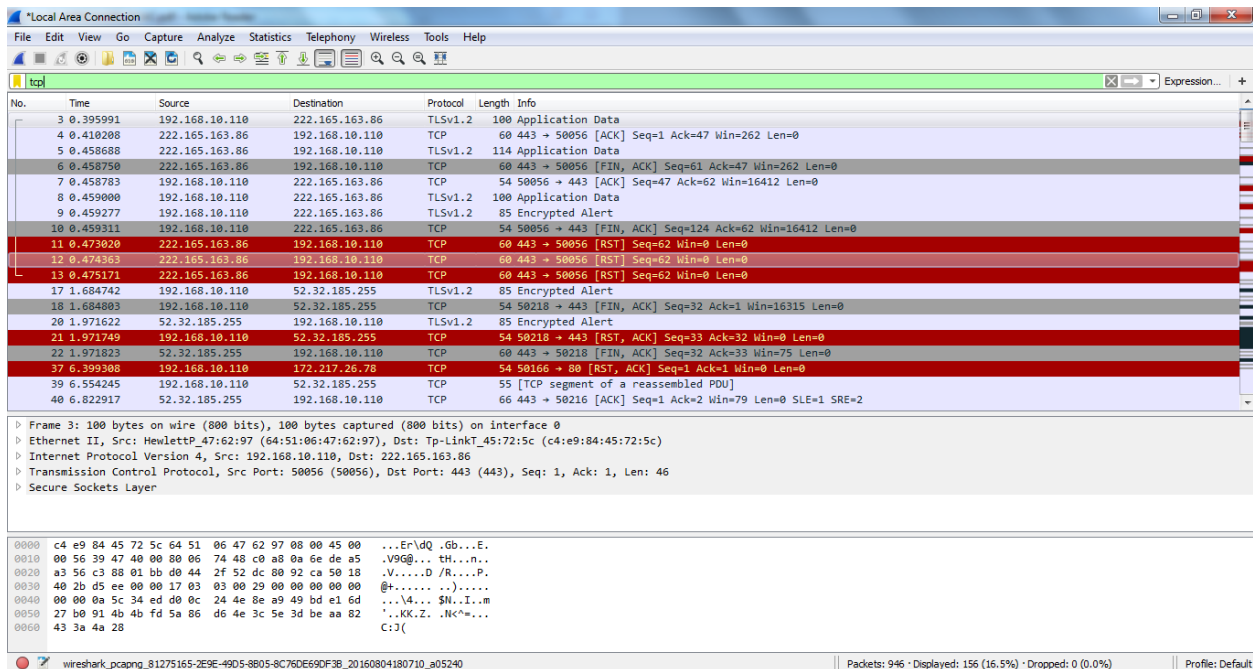
- Frame 1: 216 bytes on wire (1728 bits), 216 bytes captured (1728 bits) on interface 0
- Ethernet II, Src: HewlettP\_4b:36:78 (64:51:06:4b:36:78), Dst: IPv4mcast\_7f:ff:fa (01:00:5e:7f:ff:fa)
- Internet Protocol Version 4, Src: 192.168.10.105, Dst: 239.255.255.250
- User Datagram Protocol, Src Port: 52666 (52666), Dst Port: 1900 (1900)
- Hypertext Transfer Protocol

## Step 05: Stop capturing from Local Area Connection



## Step 06: Wireshark Display Filter Results

### I) Filter results by protocol



## II) Filter results by port

Wireshark capture showing a filtered packet list for 'tcp.port eq 80'. The packet list shows a single packet (No. 37) from 192.168.10.110 to 172.217.26.78, protocol TCP, length 54 bytes. The packet details pane shows the frame structure: Ethernet II, Internet Protocol Version 4, and Transmission Control Protocol (Seq=1, Ack=1, Win=0, Len=0). The packet bytes pane shows the raw data in hexadecimal and ASCII.

## III) Filter results based on multiple conditions

Wireshark capture showing a filtered packet list for 'tcp or dns'. The packet list shows multiple packets (Nos. 3, 4, 5, 6, 7, 8, 9, 10, 11, 12, 13, 17, 18, 20, 21, 22, 37, 39, 40) from 192.168.10.110 to various destinations, including 222.165.163.86, 52.32.185.255, and 172.217.26.78. The packet details pane shows the frame structure: Ethernet II, Internet Protocol Version 4, and Transmission Control Protocol (Seq=1, Ack=1, Win=0, Len=0). The packet bytes pane shows the raw data in hexadecimal and ASCII.

Local Area Connection

File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help

udp and http

No.	Time	Source	Destination	Protocol	Length	Info
1	0.000000	192.168.10.105	239.255.255.250	SSDP	216	M-SEARCH * HTTP/1.1
14	0.483474	192.168.10.105	239.255.255.250	SSDP	175	M-SEARCH * HTTP/1.1
15	1.013875	192.168.10.105	239.255.255.250	SSDP	216	M-SEARCH * HTTP/1.1
24	2.754190	fe80::787b:87f9:5a0...	ff02::c	SSDP	208	M-SEARCH * HTTP/1.1
25	2.754368	fe80::2d1d:6c9:cdfd...	ff02::c	SSDP	208	M-SEARCH * HTTP/1.1
28	3.502172	192.168.10.105	239.255.255.250	SSDP	175	M-SEARCH * HTTP/1.1
34	5.754314	fe80::787b:87f9:5a0...	ff02::c	SSDP	208	M-SEARCH * HTTP/1.1
35	5.754494	fe80::2d1d:6c9:cdfd...	ff02::c	SSDP	208	M-SEARCH * HTTP/1.1
38	6.495311	192.168.10.105	239.255.255.250	SSDP	175	M-SEARCH * HTTP/1.1
46	9.495454	192.168.10.105	239.255.255.250	SSDP	175	M-SEARCH * HTTP/1.1
48	9.754276	fe80::787b:87f9:5a0...	ff02::c	SSDP	208	M-SEARCH * HTTP/1.1
49	9.754462	fe80::2d1d:6c9:cdfd...	ff02::c	SSDP	208	M-SEARCH * HTTP/1.1
56	12.754311	fe80::787b:87f9:5a0...	ff02::c	SSDP	208	M-SEARCH * HTTP/1.1
57	12.754493	fe80::2d1d:6c9:cdfd...	ff02::c	SSDP	208	M-SEARCH * HTTP/1.1
88	15.754299	fe80::787b:87f9:5a0...	ff02::c	SSDP	208	M-SEARCH * HTTP/1.1
89	15.754477	fe80::2d1d:6c9:cdfd...	ff02::c	SSDP	208	M-SEARCH * HTTP/1.1
100	19.754582	fe80::787b:87f9:5a0...	ff02::c	SSDP	208	M-SEARCH * HTTP/1.1
101	19.754760	fe80::2d1d:6c9:cdfd...	ff02::c	SSDP	208	M-SEARCH * HTTP/1.1
133	22.755392	fe80::787b:87f9:5a0...	ff02::c	SSDP	208	M-SEARCH * HTTP/1.1

Frame 1: 216 bytes on wire (1728 bits), 216 bytes captured (1728 bits) on interface 0  
 Ethernet II, Src: HewlettP\_4b:36:78 (64:51:06:4b:36:78), Dst: IPv4mcast\_7f:ff:fa (01:00:5e:7f:ff:fa)  
 Internet Protocol Version 4, Src: 192.168.10.105, Dst: 239.255.255.250  
 User Datagram Protocol, Src Port: 52666 (52666), Dst Port: 1900 (1900)  
 Hypertext Transfer Protocol

0000 01 00 5e 7f ff fa 64 51 06 4b 36 78 00 00 45 00 ..^...dQ .K6x..E.  
 0010 00 ca 41 15 00 00 01 11 bd 02 c0 a8 0a 69 ef ff ..A....i..  
 0020 ff fa cd ba 07 6c 00 b6 79 9d 4d 2d 53 45 41 52 ....l..y.M-SEAR  
 0030 43 48 20 2a 20 48 54 54 50 2f 31 2e 31 0d 0a 48 CH \* HTTP/1.1..H  
 0040 4f 53 54 3a 20 32 33 39 2e 32 35 35 2e 32 35 35 OST: 239.255.255  
 0050 2e 32 35 30 3a 31 39 30 30 0d 0a 4d 41 4e 3a 20 .250:1900 0..HAN:  
 0060 22 73 73 64 70 3a 64 69 73 63 6f 76 65 72 2d 0d "ssdp:discover".  
 0070 0a 4d 58 3a 20 31 0d 0a 53 54 3a 20 75 72 6e 3a .MX: 1..ST: urn:

wireshark\_pcapng\_81275165-2E9E-49D5-8B05-8C76DE69DF36\_20160804180710\_a05240

Packets: 946 · Displayed: 157 (16.6%) · Dropped: 0 (0.0%) Profile: Default

## IV) Filter results by IP addresses

### 01. Find my IP address

```
Microsoft Windows [Version 6.1.7600]
Copyright (c) 2009 Microsoft Corporation. All rights reserved.

C:\Users\ISSAC>ipconfig

Windows IP Configuration

Ethernet adapter Local Area Connection 2:

    Connection-specific DNS Suffix  . : 
    Link-local IPv6 Address . . . . . : fe80::b583:582e:1dac:6117%41
    IPv4 Address. . . . . : 169.254.123.186
    Subnet Mask . . . . . : 255.255.0.0
    Default Gateway . . . . . : 

Ethernet adapter Local Area Connection:

    Connection-specific DNS Suffix  . : 
    Link-local IPv6 Address . . . . . : fe80::b542:a3d9:b24:5737%11
    IPv4 Address. . . . . : 192.168.10.110
    Subnet Mask . . . . . : 255.255.255.0
    Default Gateway . . . . . : 192.168.10.1
```

## 02. Filter results by my IP address

The screenshot shows the Wireshark interface with the filter `ip.src==192.168.10.110` applied. The packet list displays various protocols including TLSv1.2, TCP, and QUIC. The packet details pane shows the structure of a QUIC packet (Frame 82), including Ethernet II, Internet Protocol Version 4, User Datagram Protocol, and QUIC (Quick UDP Internet Connections) fields. The packet bytes pane shows the raw data in hexadecimal and ASCII.

No.	Time	Source	Destination	Protocol	Length	Info
3	0.395991	192.168.10.110	222.165.163.86	TLSv1.2	100	Application Data
7	0.458783	192.168.10.110	222.165.163.86	TCP	54	50056 → 443 [ACK] Seq=47 Ack=62 Win=16412 Len=0
8	0.459000	192.168.10.110	222.165.163.86	TLSv1.2	100	Application Data
9	0.459277	192.168.10.110	222.165.163.86	TLSv1.2	85	Encrypted Alert
10	0.459311	192.168.10.110	222.165.163.86	TCP	54	50056 → 443 [FIN, ACK] Seq=124 Ack=62 Win=16412 Len=0
17	1.684742	192.168.10.110	52.32.185.255	TLSv1.2	85	Encrypted Alert
18	1.684803	192.168.10.110	52.32.185.255	TCP	54	50218 → 443 [FIN, ACK] Seq=32 Ack=1 Win=16315 Len=0
21	1.971749	192.168.10.110	52.32.185.255	TCP	54	50218 → 443 [RST, ACK] Seq=33 Ack=32 Win=0 Len=0
37	6.399308	192.168.10.110	172.217.26.78	TCP	54	50166 → 80 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0
39	6.554245	192.168.10.110	52.32.185.255	TCP	55	[TCP segment of a reassembled PDU]
52	10.366193	192.168.10.110	74.125.68.189	QUIC	82	Payload (Encrypted), CID: 5680295283317698357, Seq: 161
73	14.398532	192.168.10.110	222.165.163.119	TLSv1.2	100	Application Data
77	14.659225	192.168.10.110	222.165.163.119	TCP	54	50106 → 443 [ACK] Seq=47 Ack=62 Win=16450 Len=0
78	14.659318	192.168.10.110	222.165.163.119	TLSv1.2	100	Application Data
79	14.659428	192.168.10.110	222.165.163.119	TLSv1.2	85	Encrypted Alert
80	14.659438	192.168.10.110	222.165.163.119	TCP	54	50106 → 443 [FIN, ACK] Seq=124 Ack=62 Win=16450 Len=0
91	16.822889	192.168.10.110	52.32.185.255	TCP	55	[TCP Keep-Alive] 50216 → 443 [ACK] Seq=1 Ack=1 Win=16450 Len=1
112	22.400274	192.168.10.110	192.0.77.32	TLSv1.2	100	Application Data
113	22.400370	192.168.10.110	74.125.200.95	TLSv1.2	100	Application Data

Frame 82: 82 bytes on wire (656 bits), 82 bytes captured (656 bits) on interface 0  
Ethernet II, Src: HewlettP\_47:62:97 (64:51:06:47:62:97), Dst: Tp-LinkT\_45:72:5c (c4:e9:84:45:72:5c)  
Internet Protocol Version 4, Src: 192.168.10.110, Dst: 74.125.68.189  
User Datagram Protocol, Src Port: 60195 (60195), Dst Port: 443 (443)  
QUIC (Quick UDP Internet Connections)

0000 c4 e9 84 45 72 5c 64 51 06 47 62 97 08 00 45 00 ...Er\dq .Gb...E.  
0010 00 44 39 51 00 00 08 11 a7 07 c0 a8 0a 0e 4a 7d .DQ....nJ  
0020 44 bd eb 23 01 bb 00 30 a0 43 0c 35 6f 7a f5 76 D,\*.0.C50z.v  
0030 76 d4 4e a1 54 40 7d 3e f5 90 d9 ba 50 00 64 dc v.N.T@>...P.d.  
0040 8c f8 34 f0 ac 6f f5 32 3d cc f9 fa 71 6e c5 79 ..4..o.2=...qn.y  
0050 b9 9c ..

wireshark\_pcapng\_81275165-2E9E-49D5-8B05-8C76D6E9DF3B\_20160804180710\_a05240

Packets: 946 · Displayed: 108 (11.4%) · Dropped: 0 (0.0%)

Profile: Default

## Step 07: Packet colorization

The screenshot shows the Wireshark interface with the filter `tcp.analysis.flags` applied. The packet list displays various TCP Keep-Alive packets. The packet details pane shows the structure of a TCP packet (Frame 91), including Interface id, Encapsulation type, Arrival Time, Epoch Time, Frame Number, Frame Length, Capture Length, and Protocols in frame.

No.	Time	Source	Destination	Protocol	Length	Info
92	17.091357	52.32.185.255	192.168.10.110	TCP	66	[TCP Keep-Alive ACK] 443 → 50216 [ACK] Seq=1 Ack=2 Win=79 Len=0 SLE=1 SRE=2
200	27.083293	192.168.10.110	52.32.185.255	TCP	55	[TCP Keep-Alive] 50216 → 443 [ACK] Seq=1 Ack=1 Win=16450 Len=1
202	27.352136	52.32.185.255	192.168.10.110	TCP	66	[TCP Keep-Alive ACK] 443 → 50216 [ACK] Seq=1 Ack=2 Win=79 Len=0 SLE=1 SRE=2
246	37.344953	192.168.10.110	52.32.185.255	TCP	55	[TCP Keep-Alive] 50216 → 443 [ACK] Seq=1 Ack=1 Win=16450 Len=1
247	37.614476	52.32.185.255	192.168.10.110	TCP	66	[TCP Keep-Alive ACK] 443 → 50216 [ACK] Seq=1 Ack=2 Win=79 Len=0 SLE=1 SRE=2
285	47.614357	192.168.10.110	52.32.185.255	TCP	55	[TCP Keep-Alive] 50216 → 443 [ACK] Seq=1 Ack=1 Win=16450 Len=1
287	47.882889	52.32.185.255	192.168.10.110	TCP	66	[TCP Keep-Alive ACK] 443 → 50216 [ACK] Seq=1 Ack=2 Win=79 Len=0 SLE=1 SRE=2
374	70.776079	192.168.10.110	74.125.200.19	TCP	55	[TCP Keep-Alive] 50184 → 443 [ACK] Seq=1 Ack=1 Win=16484 Len=1
375	71.029658	74.125.200.19	192.168.10.110	TCP	66	[TCP Keep-Alive ACK] 443 → 50184 [ACK] Seq=1 Ack=2 Win=351 Len=0 SLE=1 SRE=2
426	88.346474	192.168.10.110	222.165.163.92	TCP	55	[TCP Keep-Alive] 49812 → 443 [ACK] Seq=1 Ack=1 Win=16304 Len=1
427	88.359489	222.165.163.92	192.168.10.110	TCP	66	[TCP Keep-Alive ACK] 443 → 49812 [ACK] Seq=1 Ack=2 Win=377 Len=0 SLE=1 SRE=2
431	89.712931	192.168.10.110	222.165.163.119	TCP	55	[TCP Keep-Alive] 50170 → 443 [ACK] Seq=1 Ack=1 Win=16375 Len=1
432	89.726376	222.165.163.119	192.168.10.110	TCP	66	[TCP Keep-Alive ACK] 443 → 50170 [ACK] Seq=1 Ack=2 Win=237 Len=0 SLE=1 SRE=2
557	116.024984	192.168.10.110	74.125.200.19	TCP	55	[TCP Keep-Alive] 50184 → 443 [ACK] Seq=1 Ack=1 Win=16484 Len=1
559	116.278219	74.125.200.19	192.168.10.110	TCP	66	[TCP Keep-Alive ACK] 443 → 50184 [ACK] Seq=1 Ack=2 Win=351 Len=0 SLE=1 SRE=2
616	133.356898	192.168.10.110	222.165.163.92	TCP	55	[TCP Keep-Alive] 49812 → 443 [ACK] Seq=1 Ack=1 Win=16304 Len=1

Frame 91: 55 bytes on wire (440 bits), 55 bytes captured (440 bits) on interface 0  
Interface id: 0 (\\Device\NPF\_{81275165-2E9E-49D5-8B05-8C76D6E9DF3B})  
Encapsulation type: Ethernet (1)  
Arrival Time: Aug 4, 2016 18:07:27.750974000 Sri Lanka Standard Time  
[Time shift for this packet: 0.000000000 seconds]  
Epoch Time: 1470314247.750974000 seconds  
[Time delta from previous captured frame: 0.569419000 seconds]  
[Time delta from previous displayed frame: 0.000000000 seconds]  
[Time since reference or first frame: 16.822889000 seconds]  
Frame Number: 91  
Frame Length: 55 bytes (440 bits)  
Capture Length: 55 bytes (440 bits)  
[Frame is marked: False]  
[Frame is ignored: False]  
[Protocols in frame: eth:ethertype:ip:tcp:data]  
[Coloring Rule Name: Bad TCP]  
[Coloring Rule String: tcp.analysis.flags && !tcp.analysis.window\_update]

Frame (frame), 55 bytes

Packets: 946 · Displayed: 22 (2.3%) · Dropped: 0 (0.0%)

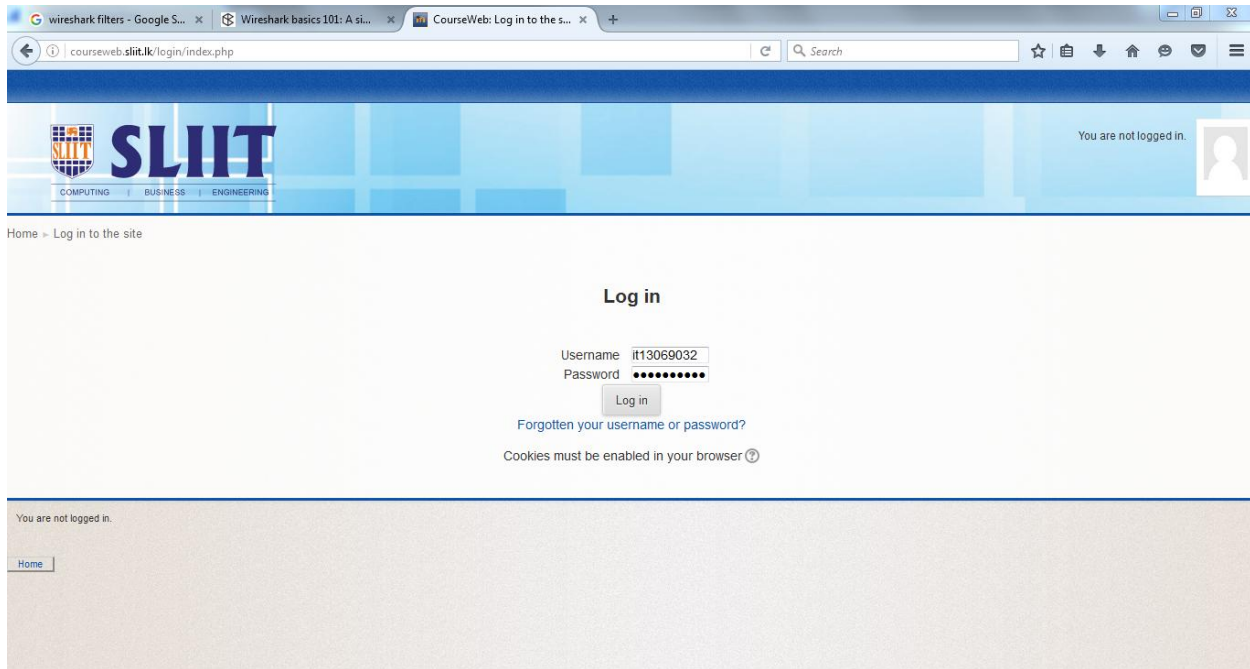
Profile: Default



## Step 08: Username and Password tracking

### I) Login to http website

E.g.: <http://courseweb.sliit.lk/>



### II) Track Username and Password using corresponding filters after the capturing process

