SRI LANKA INSTITUTE OF INFORMATION TECHNOLOGY

Information Systems Security Audit & Control

4th Year 2nd 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.

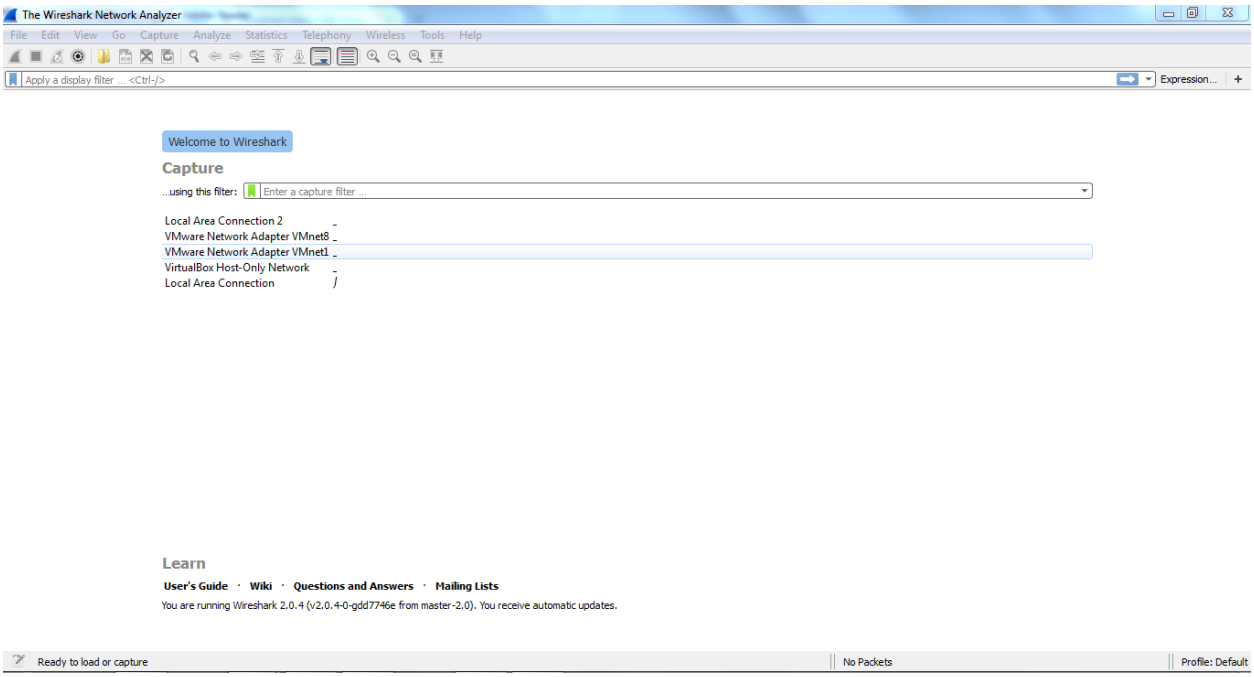
Capture Filters

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.

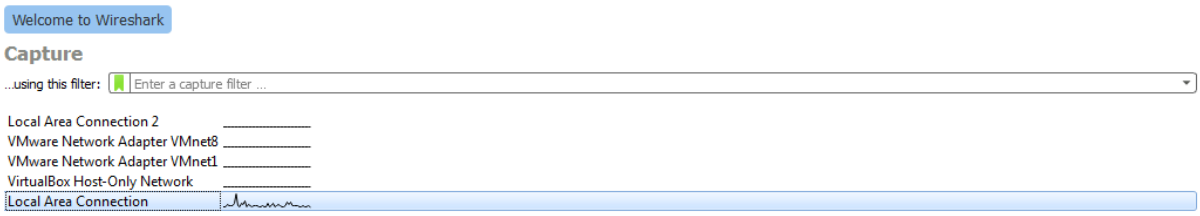
Wireshark uses the same syntax for capture filters as tcpdump, WinDump, Analyzer, and any other program that uses the libpcap/WinPcap library.

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

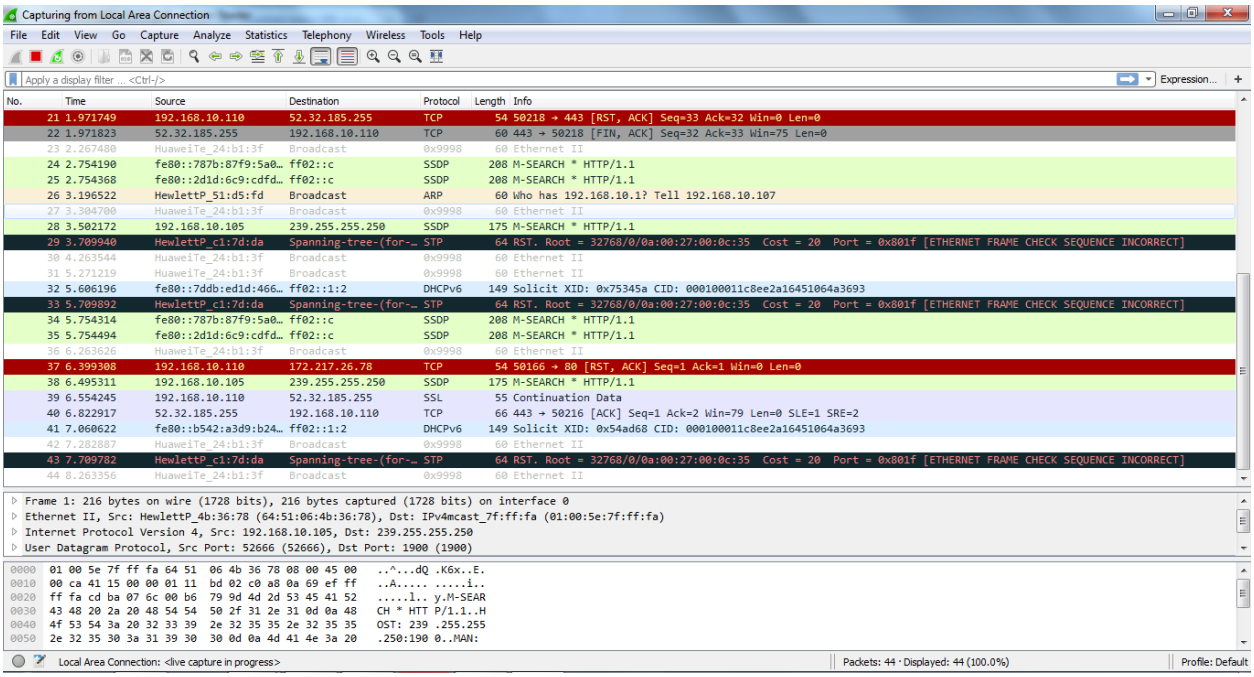
Step 01: Open Wireshark software



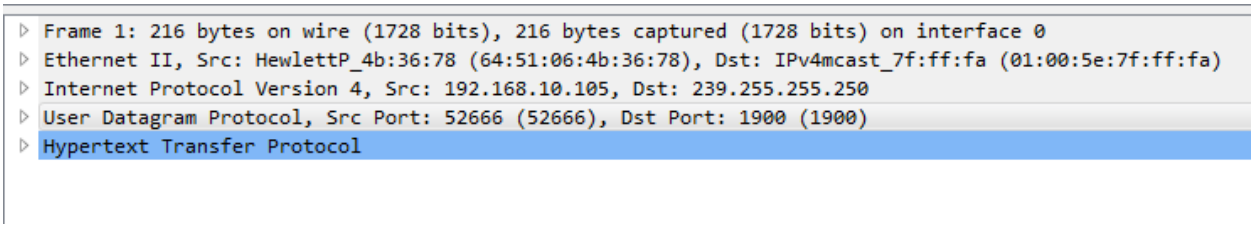
Step 02: Select internet connection (Ethernet, LAN or wireless)



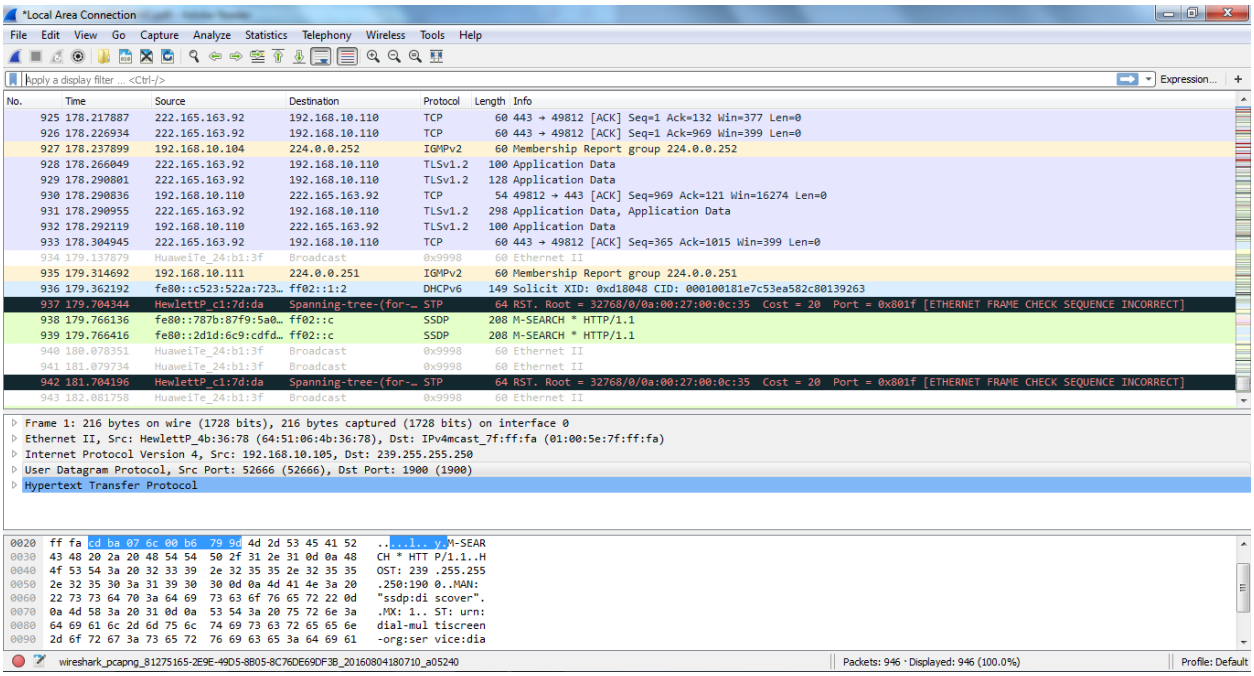
Step 03: Start capturing from Local Area Connection



Step 04: Observe used protocols and details

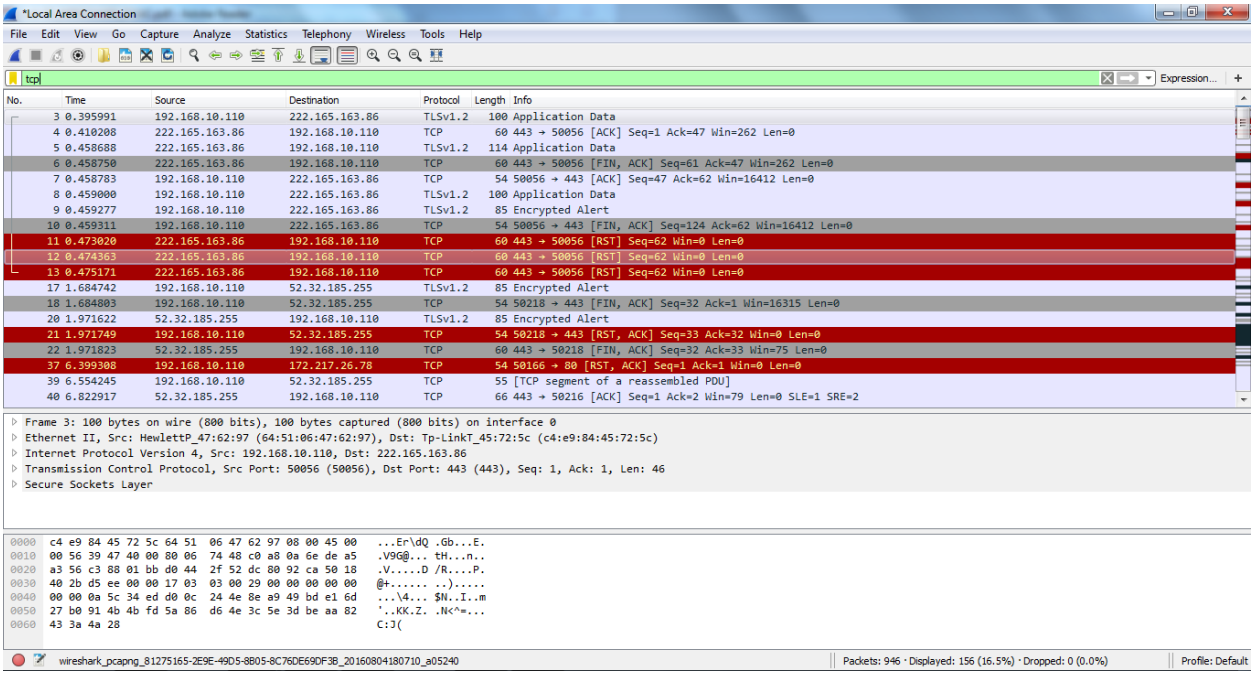


Step 05: Stop capturing from Local Area Connection

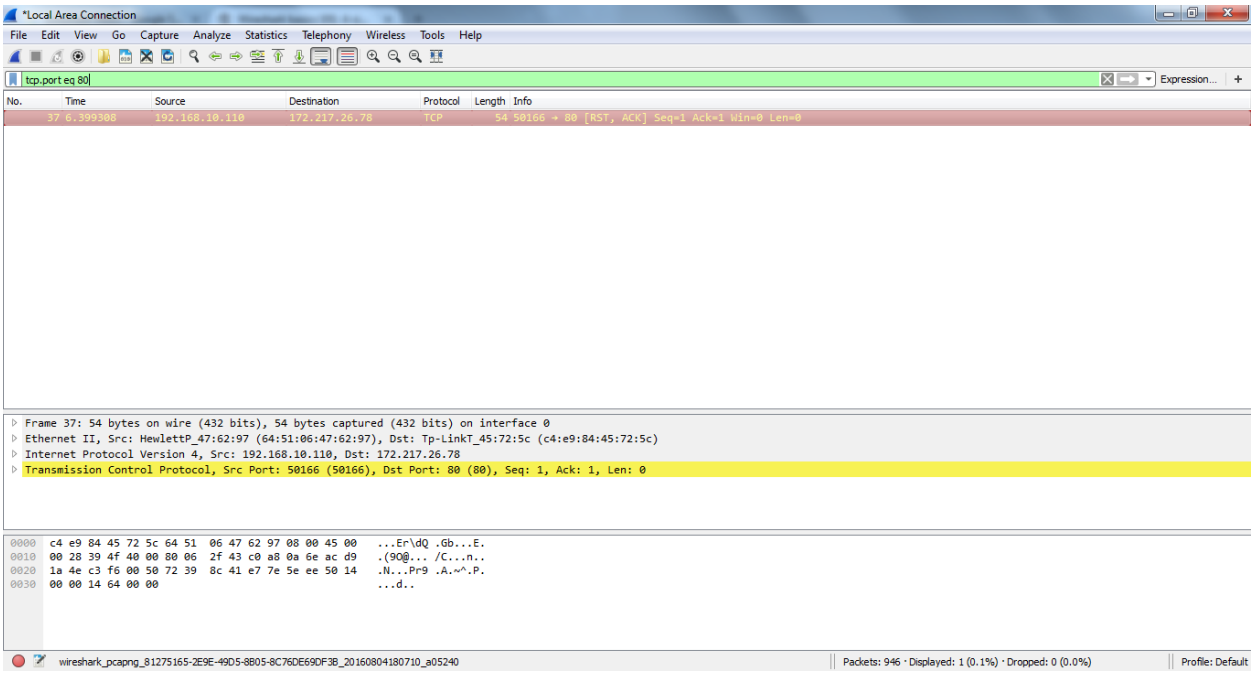


Step 06: Wireshark Display Filter Results

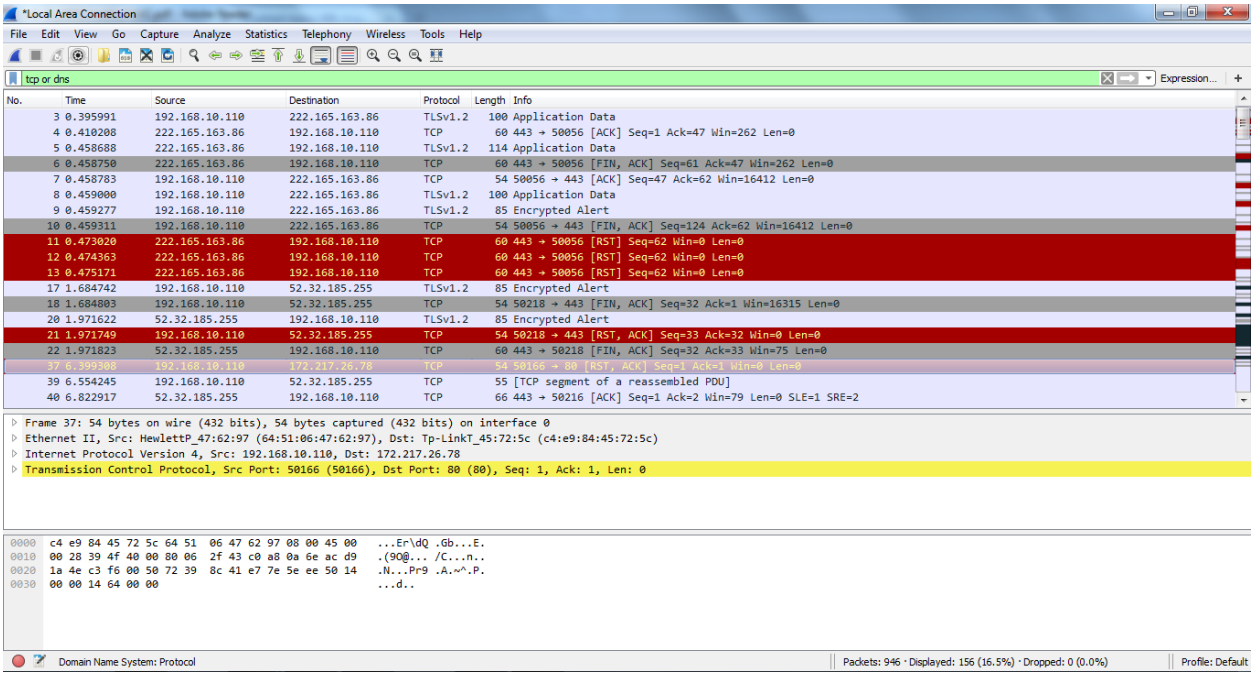
I) Filter results by protocol

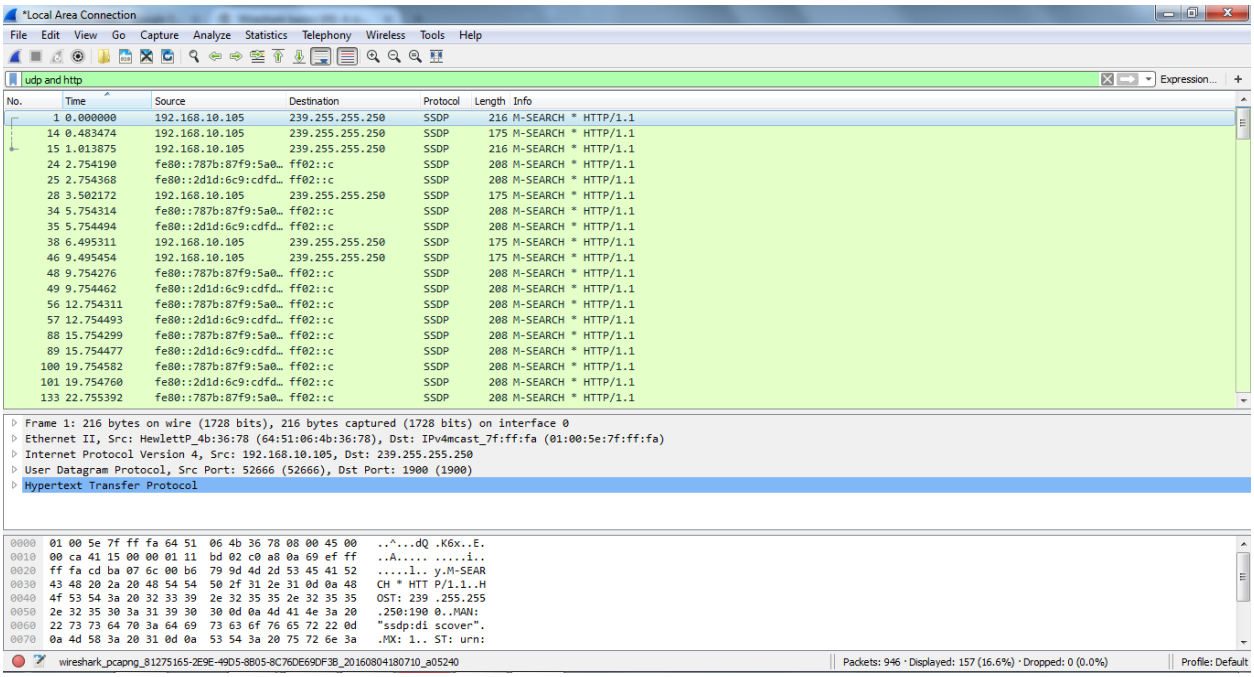


II) Filter results by port



III) Filter results based on multiple conditions



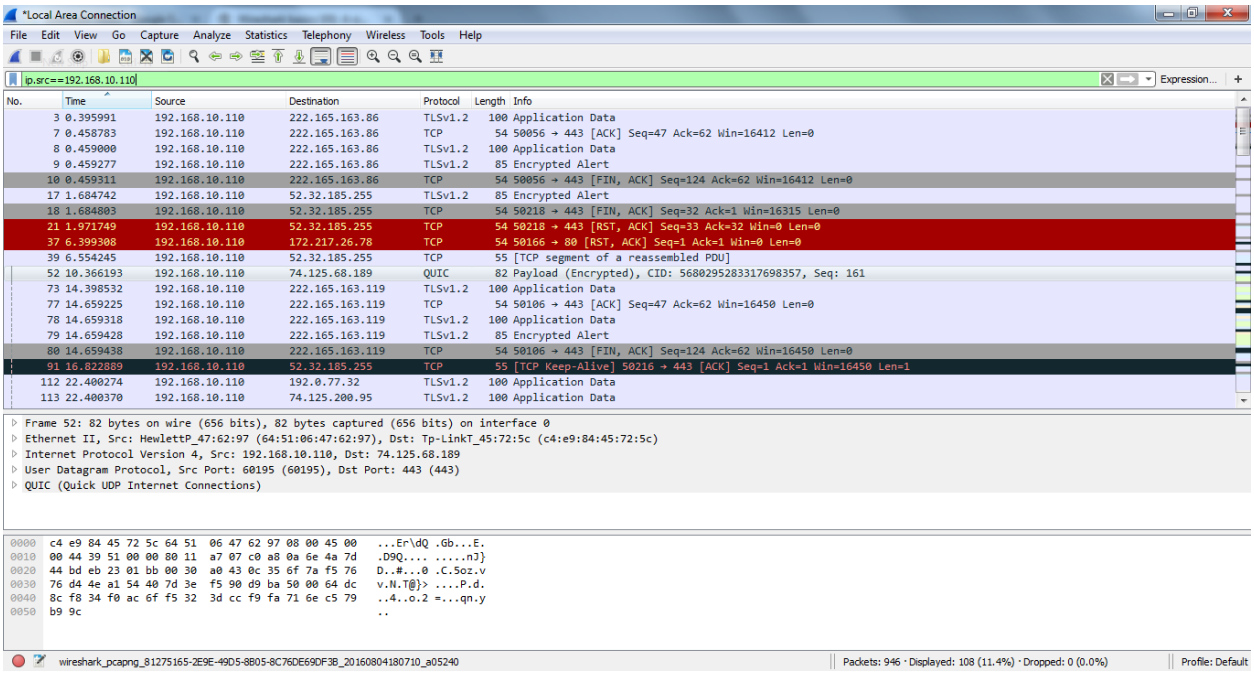


IV) Filter results by IP addresses

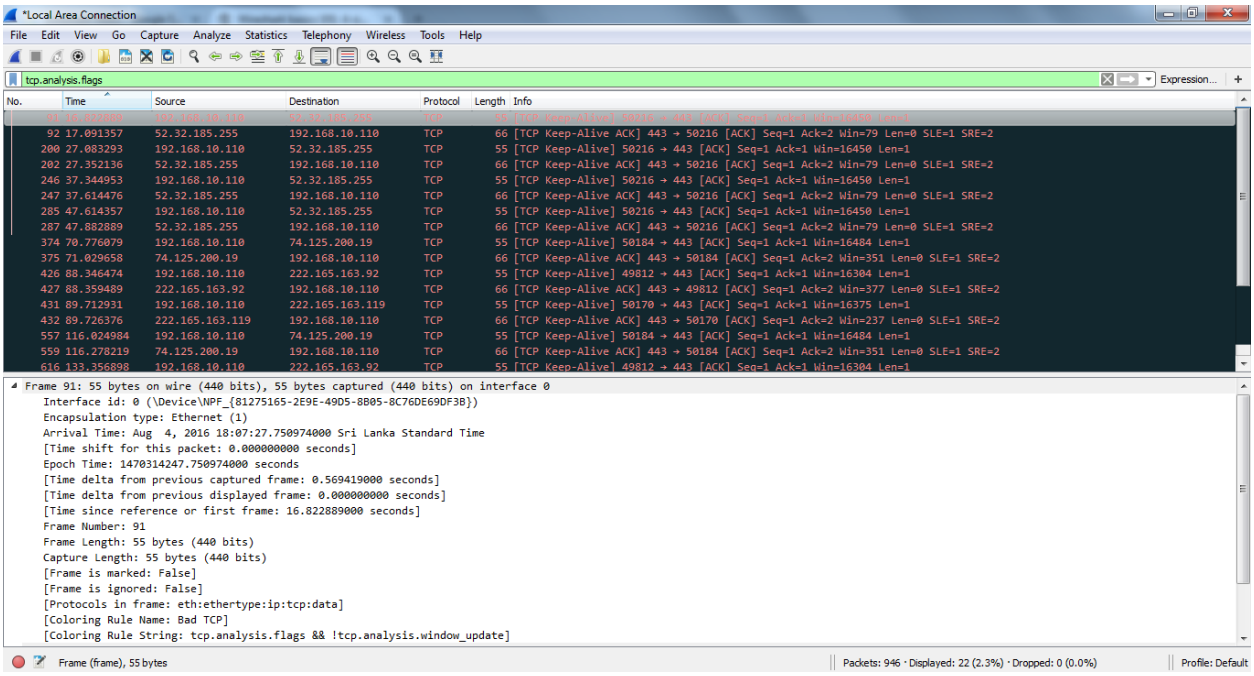
01. Find my IP address

```
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



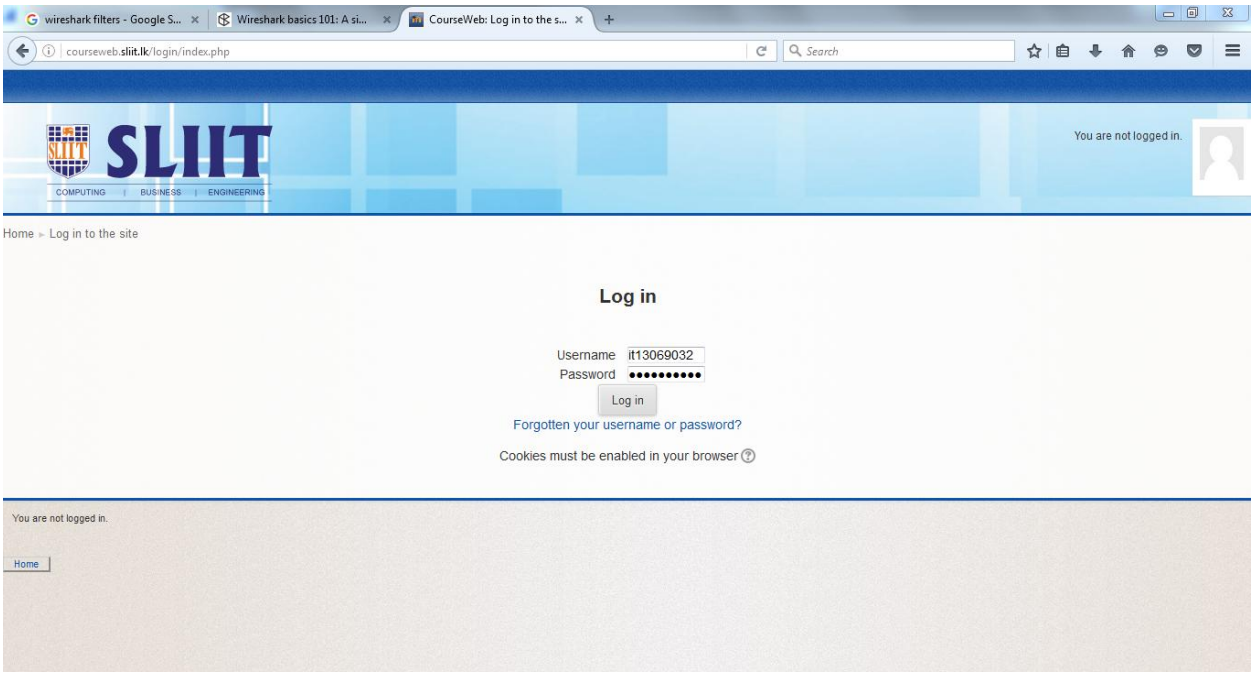
Step 07: Packet colorization



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