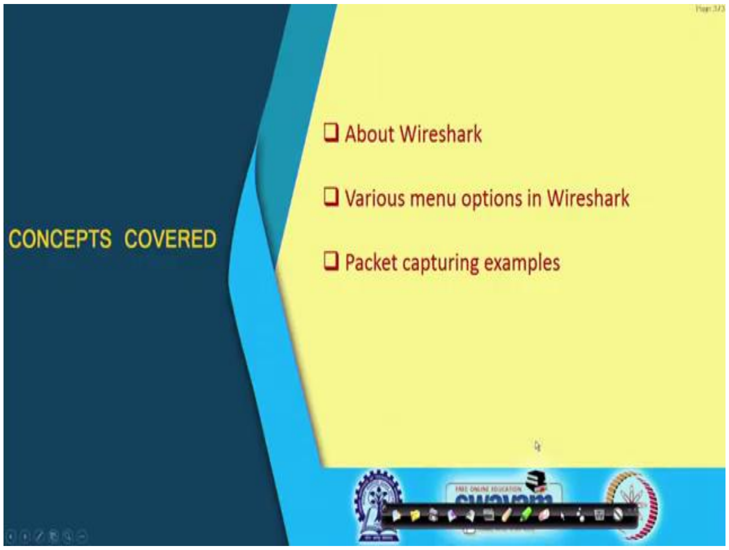
Ethical Hacking
Prof. Indranil Sengupta
Department of Computer Science and Engineering
Indian Institute of Technology, Kharagpur

Lecture – 59
Network Analysis Using Wireshark

So, in this lecture we shall be taking you through a quick tour of the Wireshark tool which you already know is very useful when you talk about capturing packets and analyzing network traffic. So, the topic of this lecture is Network Analysis using Wireshark.

(Refer Slide Time: 00:36)

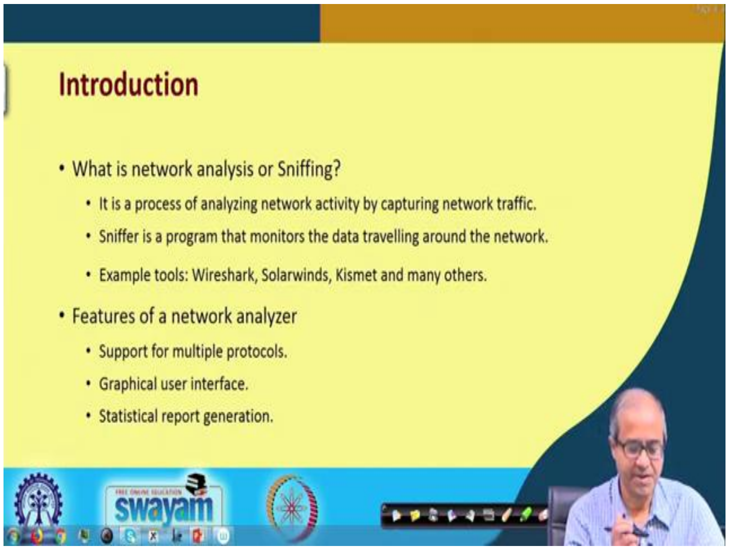


CONCEPTS COVERED

- ❑ About Wireshark
- ❑ Various menu options in Wireshark
- ❑ Packet capturing examples

Now, in this lecture we shall be basically talking about the Wireshark tool; what are the various options which are available in Wireshack under the menu options and lastly we shall be looking at a few examples.

(Refer Slide Time: 00:50)



Introduction

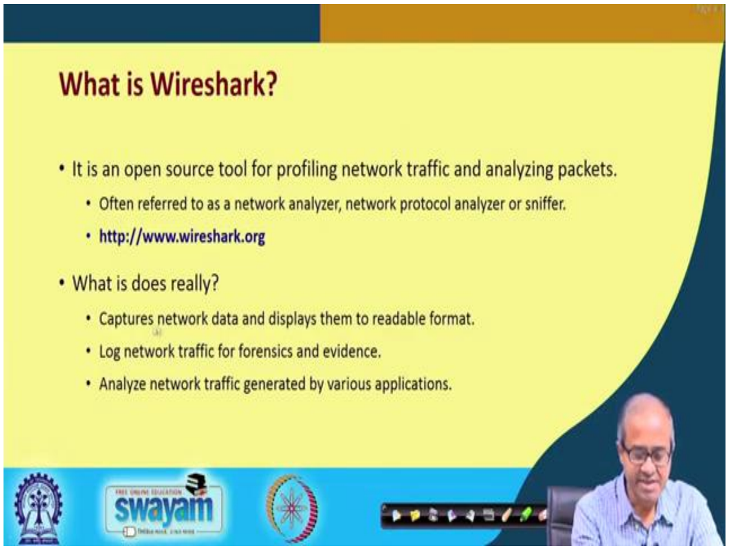
- What is network analysis or Sniffing?
  - It is a process of analyzing network activity by capturing network traffic.
  - Sniffer is a program that monitors the data travelling around the network.
  - Example tools: Wireshark, Solarwinds, Kismet and many others.
- Features of a network analyzer
  - Support for multiple protocols.
  - Graphical user interface.
  - Statistical report generation.

Well talking about the Wireshark tool, it is a kind of network analysis or you can say packet sniffing tool. So, what is it actually? Network analysis or packet sniffing when you talk about, it is basically a process of analyzing the network activity with respect to some network interface. I have a computer; it is connected to a network; I want to see, what is the traffic, what kind of traffic is flowing across the network interface at that point of the network ok. This is what packet capturing or packet sniffing is all about.

Sniffer, well Wireshark is an example of a sniffer program. It is a program actually, which monitors the data which means the packets which are flowing at a particular network interface through the network, around the network. Well, other than Wireshark there are many other tools available for this packet capture or sniffing; like, Solarwinds, Kismet and there are many others ok.

This Wireshark is one of the more popular tools; because it is quite powerful and also it is freely available ok. Well, any of the network analyzers or packet capturing, sniffing tool that we use, they will be having some common features; like, they will have support for multiple protocols to become useful. They should be having a proper user interface so that you can view or visualize the traffic in various different graphical ways. And of course, finally you need some mechanism for statistical report generation which is also important.

(Refer Slide Time: 02:41)



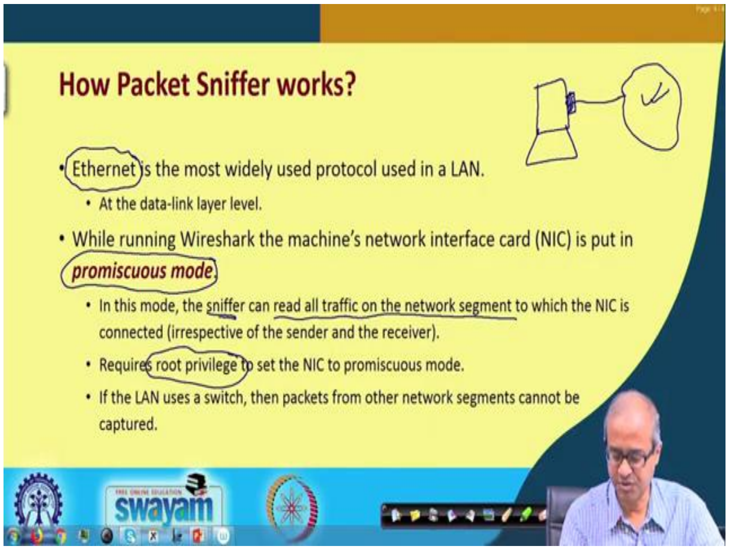
What is Wireshark?

- It is an open source tool for profiling network traffic and analyzing packets.
  - Often referred to as a network analyzer, network protocol analyzer or sniffer.
  - http://www.wireshark.org
- What is does really?
  - Captures network data and displays them to readable format.
  - Log network traffic for forensics and evidence.
  - Analyze network traffic generated by various applications.

Now, Wireshark as it said, is a, it is an open source tool; it is freely available this is used for profiling network traffic. Once you capture the network packets, the data packets, you can analyze them to find out what is going on. This kind of a tool is sometimes referred to as network analyzer, network protocol analyzer or simply a sniffer or packet sniffer. This Wireshark can be downloaded from this website, ok. This Wireshark, basically it captures network packets, network data and displays them in some format so that the user of the tool can visualize it in a proper format.

And this capturing of the network data which we call as logging, this is very useful for forensics and evidence. For example, some attack has happened; we can capture the network data and analyze it later on that what and how the attack did took place; what are the kind of packet exchanges that took place in the network for mounting that particular attack. Well, and we can analyze network traffic generated with respect to various kinds of applications ok.

(Refer Slide Time: 04:03)



How Packet Sniffer works?

- Ethernet is the most widely used protocol used in a LAN.
  - At the data-link layer level.
- While running Wireshark the machine's network interface card (NIC) is put in promiscuous mode.
  - In this mode, the sniffer can read all traffic on the network segment to which the NIC is connected (irrespective of the sender and the receiver).
  - Requires root privilege to set the NIC to promiscuous mode.
  - If the LAN uses a switch, then packets from other network segments cannot be captured.

Now, basically this packet sniffing tools, the way they work is, they sniff packet at some network interface. Now, in most of the networks where you use, where you have our computers in, we normally use the Ethernet protocol at the data link layer level; that is the most widely used and prevalent protocol that we use. And the point is that suppose, I have a computer here; this computer is connected to a network; this is our network and this is my network interface; there is a network interface card.

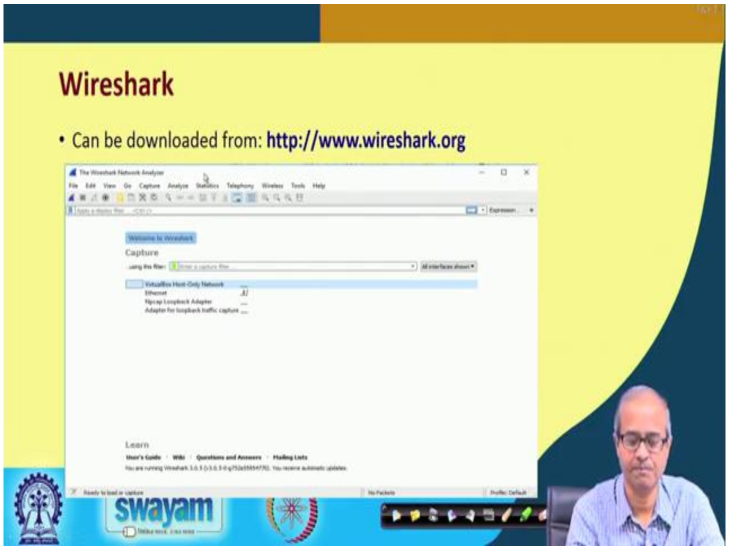
Now, the point is that in order to capture all packets that are flowing through the interface, I must initialize or program the Network Interface or NIC in something called promiscuous mode. Well, when it is set in the promiscuous mode, it will capture not only the packets which are meant for my machine, but all other packets; may be the destination is some other machine, but still I can capture them; I can view them ok.

So, it is important; I have to initialize the interface in the promiscuous mode and for initializing the promiscuous mode we need root privilege. So, the point is that for running this kind of packet capturing tool you need supervisory or root privilege; otherwise you cannot initialize the interface in the promiscuous mode ok.

So, once you set it in this mode; this sniffing tool can read all traffic on the network segment; this particular network segment to which the network interface is connected to ok. Now, the point to note is that if your computer is connected via a switch, say a layer to switch our bridge, the switch essentially partitions a LAN into several different LANs;

then you may be prevented from viewing the traffic that is flowing through the other LANs. So, it depends on the environment. So, if you are able to sniff in the proper position, proper location, then you can see or visualize many traffics or many packets that are flowing through the network ok.

(Refer Slide Time: 06:26)



Wireshark

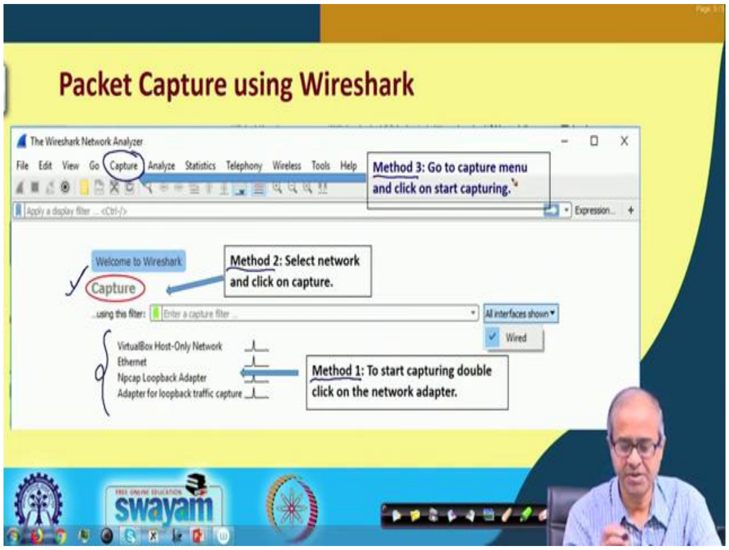
- Can be downloaded from: **http://www.wireshark.org**

The Wireshark Network Analyzer
File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help
Apply a display filter ... <Ctrl-/>
Expression...
Welcome to Wireshark
Capture
...using this filter:
Enter a capture filter ...
All interfaces shown
VirtualBox Host-Only Network
Ethernet
Npcap Loopback Adapter
Adapter for loopback traffic capture
Learn
User's Guide · Wiki · Questions and Answers · Mailing Lists
Ready to load or capture
No Packets
Profile: Default
swayam

You are running Wireshark 3.0.5 (v3.0.5-0-g752a85954770). You receive automatic updates.

So, when you start Wireshark, as I said you can download the tool from **www.wireshark.org**. So, this is the opening screen; the way it looks like. So, you see, capture, there is a apply a display filter and there are a number of menu options on the top; as you can see file, edit, view, captured, analyze, statistics and so on. Let us look into this one by one.

(Refer Slide Time: 06:57)



Packet Capture using Wireshark

Method 3: Go to capture menu and click on start capturing.

Method 2: Select network and click on capture.

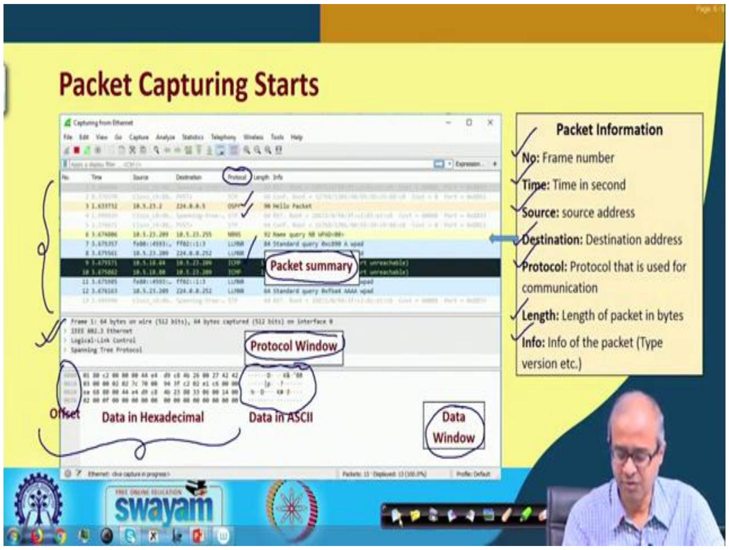
Method 1: To start capturing double click on the network adapter.

The Wireshark Network Analyzer
File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help
Apply a display filter ... <Ctrl-/>
Expression...
Welcome to Wireshark
Capture
...using this filter:
Enter a capture filter ...
All interfaces shown
Wired
VirtualBox Host-Only Network
Ethernet
Npcap Loopback Adapter
Adapter for loopback traffic capture
swayam

So, when we are trying to do packet capturing using Wireshark, so what we actually do is? So, we have to somehow specify from where to capture and we have to say that yes, now start the capture. You see here on one side is displayed all the network interfaces where you can possibly capture the packets from. The first thing, the first method is you can start capturing by double clicking on the proper network interface directly here. This is one method or you just select by single click, then you click on this capture, capture button; this is your method 2.

Or thirdly, you can see there is a capture menu option also available here in the top, in the top menu bar. You can directly go to the capture menu and you can specify that you want to capture and how you want to capture. These are the different ways you can specify that we want to capture packets from the network interface.

(Refer Slide Time: 08:08)



Packet Capturing Starts

Capturing from Ethernet
File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help
No. Time Source Destination Protocol Length Info
Packet summary
Protocol Window
Offset
Data in Hexadecimal
Data in ASCII
Data Window
swayam

Frame 1: 64 bytes on wire (512 bits), 64 bytes captured (512 bits) on interface 0

Packet Information

- No: Frame number
- Time: Time in second
- Source: source address
- Destination: Destination address
- Protocol: Protocol that is used for communication
- Length: Length of packet in bytes
- Info: Info of the packet (Type version etc.)

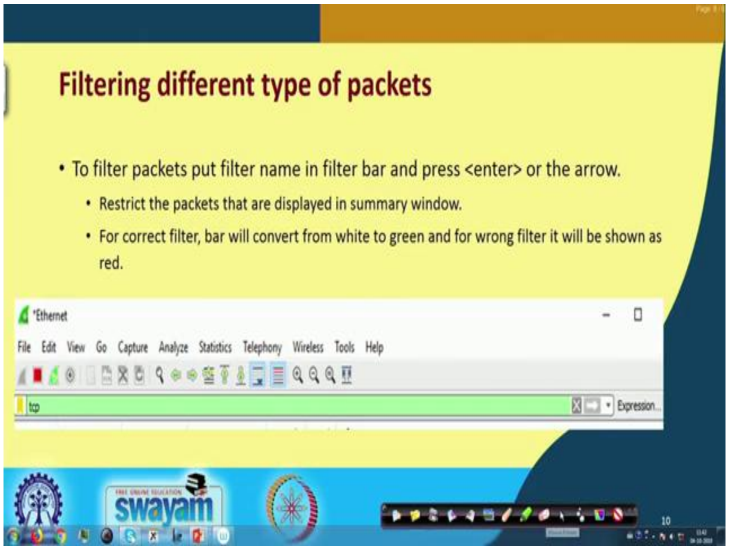
Now, once the packet capturing starts, the window looks like this. So, you can see a lot of information that gets displayed on the window. There are broadly 3 windows that come by default; the one on the top is packet summary. Here you can see a list of all the packets and this list will go on scrolling as the packets come. So, every row here indicates one packet that has been captured ok.

Now, here you can see there are a lot of columns. So, the columns are mentioned here; it specifies the frame number, the time; so, when this packet was captured; what is the source IP address, destination IP address; what protocol was used? You see the protocol here; you can say OSPF, STP, there are, there are a lot, ICMP, there are lot of different protocols you can see. Length is the number of bytes in the packet and lastly, in the last column some information about the packet; what is it type, the version and so on. So, this is with respect to packet summary.

Then, there is a protocol window. Well once you select one of these packets, you click on one of the rows, that row gets highlighted and you can see some details in this window. So, you can see that what is the frame containing; what type of packet is; some details are shown and if you want to see the contents of the packet in hexadecimal or in ASCII, it is the third window which is the data window that shows you that. On the left the data gets displayed in hexadecimal, the contents of the packet. Ultimately the data is going in binary; here you have a hexadecimal view of the data as you can see.

So, the first it shows the offset, the address and the contents of the packet and on the right side some of the data may be going in clear text, ASCII. So, the same thing is also displayed in ASCII; in case you want to visualize the text part of the packet, if there is something going in clear text ok. So, this is how the overall window of the Wireshark looks like once it starts capturing the packets. Then you can apply a lot of filters; because you will be seeing or visualizing a large number of packets coming; I may not be wanting to see all the packets.

(Refer Slide Time: 10:53)

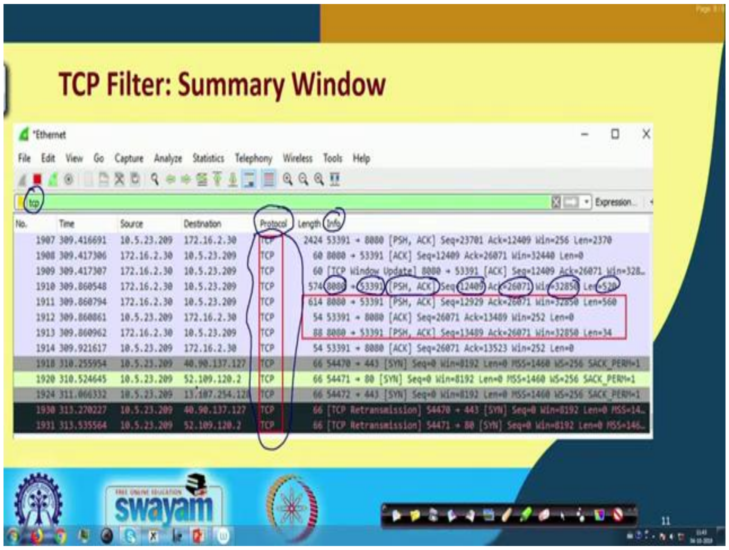


Filtering different type of packets

- To filter packets put filter name in filter bar and press <enter> or the arrow.
  - Restrict the packets that are displayed in summary window.
  - For correct filter, bar will convert from white to green and for wrong filter it will be shown as red.

So, you can apply some filters. So, when you want to apply filters, you see, there is a filter bar in the top of the window; here this is the first one. Here you can specify the type of filter; like, here I am specifying TCP for instance; then you can either press enter or you can click on this arrow on the right; if you can see this arrow on the right, you can click here. So, once you set it, only packets of these particular types will get displayed on the window ok. So, you can actually display the packets in a filtered form.

(Refer Slide Time: 11:32)



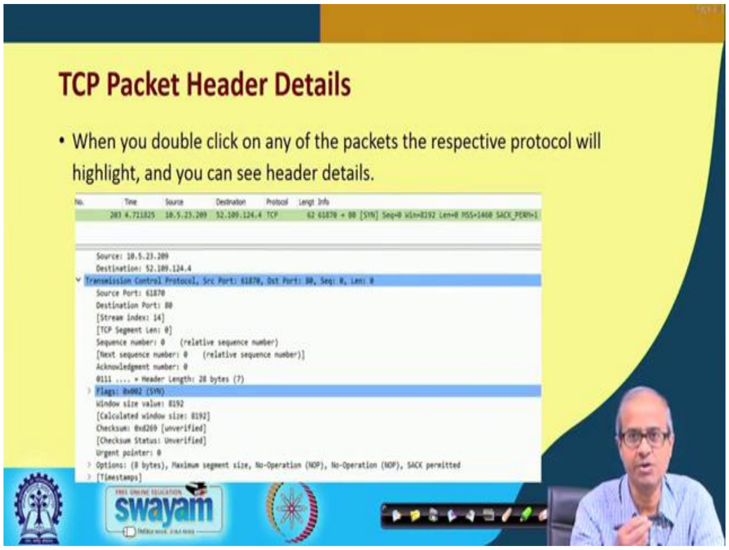
TCP Filter: Summary Window

*Ethernet
File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help
tcp
Expression...

No.	Time	Source	Destination	Protocol	Length	Info
1907	309.416691	10.5.23.209	172.16.2.30	TCP	2424	53391 → 8080 [PSH, ACK] Seq=23701 Ack=12409 Win=256 Len=2370
1908	309.417306	172.16.2.30	10.5.23.209	TCP	60	8080 → 53391 [ACK] Seq=12409 Ack=26071 Win=32440 Len=0
1909	309.417307	172.16.2.30	10.5.23.209	TCP	60	[TCP Window Update] 8080 → 53391 [ACK] Seq=12409 Ack=26071 Win=328…
1910	309.860548	172.16.2.30	10.5.23.209	TCP	574	8080 → 53391 [PSH, ACK] Seq=12409 Ack=26071 Win=32850 Len=520
1911	309.860794	172.16.2.30	10.5.23.209	TCP	614	8080 → 53391 [PSH, ACK] Seq=12929 Ack=26071 Win=32850 Len=560
1912	309.860861	10.5.23.209	172.16.2.30	TCP	54	53391 → 8080 [ACK] Seq=26071 Ack=13489 Win=252 Len=0
1913	309.860962	172.16.2.30	10.5.23.209	TCP	88	8080 → 53391 [PSH, ACK] Seq=13489 Ack=26071 Win=32850 Len=34
1914	309.921617	10.5.23.209	172.16.2.30	TCP	54	53391 → 8080 [ACK] Seq=26071 Ack=13523 Win=252 Len=0
1918	310.255954	10.5.23.209	40.90.137.127	TCP	66	54470 → 443 [SYN] Seq=0 Win=8192 Len=0 MSS=1460 WS=256 SACK_PERM=1
1920	310.524645	10.5.23.209	52.109.120.2	TCP	66	54471 → 80 [SYN] Seq=0 Win=8192 Len=0 MSS=1460 WS=256 SACK_PERM=1
1924	311.066332	10.5.23.209	13.107.254.12	TCP	66	54472 → 443 [SYN] Seq=0 Win=8192 Len=0 MSS=1460 WS=256 SACK_PERM=1
1930	313.270227	10.5.23.209	40.90.137.127	TCP	66	[TCP Retransmission] 54470 → 443 [SYN] Seq=0 Win=8192 Len=0 MSS=14…
1931	313.535564	10.5.23.209	52.109.120.2	TCP	66	[TCP Retransmission] 54471 → 80 [SYN] Seq=0 Win=8192 Len=0 MSS=146…

Let us take some examples. So, here we have selected a filtered TCP. So, you can see, all packets that are displayed are having protocol all TCP; all TCP packets are getting displayed ok. And in the information part, the last column you see all relevant information about TCP packets are shown; like, what is the source port number, destination port number, what are the flags which are active, sequence number, acknowledgement number, window, length of the packet and so on ok; So, you can create a filter like this and you can only view the respective kind of packet you want to look at ok.

(Refer Slide Time: 12:25)



TCP Packet Header Details

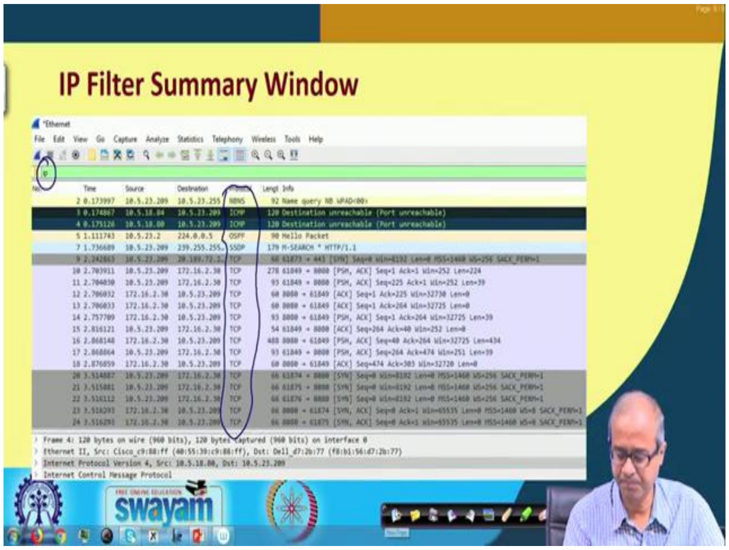
- When you double click on any of the packets the respective protocol will highlight, and you can see header details.

No.	Time	Source	Destination	Protocol	Lengt	Info
203	4.711825	10.5.23.209	52.109.124.4	TCP	62	61870 → 80 [SYN] Seq=0 Win=8192 Len=0 MSS=1460 SACK_PERM=1

```
    Source: 10.5.23.209
    Destination: 52.109.124.4
v Transmission Control Protocol, Src Port: 61870, Dst Port: 80, Seq: 0, Len: 0
    Source Port: 61870
    Destination Port: 80
    [Stream index: 14]
    [TCP Segment Len: 0]
    Sequence number: 0    (relative sequence number)
    [Next sequence number: 0    (relative sequence number)]
    Acknowledgment number: 0
    0111 .... = Header Length: 28 bytes (7)
  > Flags: 0x002 (SYN)
    Window size value: 8192
    [Calculated window size: 8192]
    Checksum: 0xd269 [unverified]
    [Checksum Status: Unverified]
    Urgent pointer: 0
  > Options: (8 bytes), Maximum segment size, No-Operation (NOP), No-Operation (NOP), SACK permitted
  > [Timestamps]
```

Now, suppose if you go back previously, suppose you have all the packets; if you click on one of the rows, suppose I want to see the detail of one of the rows; if you click on it, then you will see details of that particular packet. You see I have clicked on one of the rows; that row is showing on top and you can see the details of the TCP packet. The contents of the headers are shown in detail; what is the source port, destination port, TCP segment length, sequence number, acknowledgement number and so on and so forth; what are the contents of the flags, checksum everything; you can see the whole contents of the packet ok.

(Refer Slide Time: 13:07)



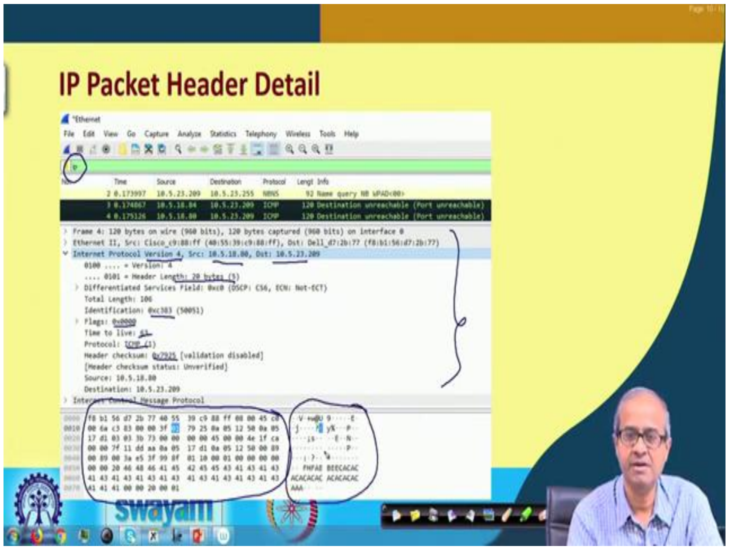
IP Filter Summary Window

*Ethernet
File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help
ip

```
No.  Time        Source        Destination     Protocol Lengt Info
   2 0.173997    10.5.23.209   10.5.23.255     NBNS      92 Name query NB WPAD<00>
   3 0.174867    10.5.18.84    10.5.23.209     ICMP     120 Destination unreachable (Port unreachable)
   4 0.175126    10.5.18.80    10.5.23.209     ICMP     120 Destination unreachable (Port unreachable)
   5 1.111743    10.5.23.2     224.0.0.5       OSPF      90 Hello Packet
   7 1.736689    10.5.23.209   239.255.255...  SSDP     179 M-SEARCH * HTTP/1.1
   9 2.242863    10.5.23.209   20.189.72.2...  TCP       66 61873 → 443 [SYN] Seq=0 Win=8192 Len=0 MSS=1460 WS=256 SACK_PERM=1
  10 2.703911    10.5.23.209   172.16.2.30     TCP      278 61849 → 8080 [PSH, ACK] Seq=1 Ack=1 Win=252 Len=224
  11 2.704030    10.5.23.209   172.16.2.30     TCP       93 61849 → 8080 [PSH, ACK] Seq=225 Ack=1 Win=252 Len=39
  12 2.706032    172.16.2.30   10.5.23.209     TCP       60 8080 → 61849 [ACK] Seq=1 Ack=225 Win=32730 Len=0
  13 2.706033    172.16.2.30   10.5.23.209     TCP       60 8080 → 61849 [ACK] Seq=1 Ack=264 Win=32725 Len=0
  14 2.757709    172.16.2.30   10.5.23.209     TCP       93 8080 → 61849 [PSH, ACK] Seq=1 Ack=264 Win=32725 Len=39
  15 2.816121    10.5.23.209   172.16.2.30     TCP       54 61849 → 8080 [ACK] Seq=264 Ack=40 Win=252 Len=0
  16 2.868148    172.16.2.30   10.5.23.209     TCP      488 8080 → 61849 [PSH, ACK] Seq=40 Ack=264 Win=32725 Len=434
  17 2.868864    10.5.23.209   172.16.2.30     TCP       93 61849 → 8080 [PSH, ACK] Seq=264 Ack=474 Win=251 Len=39
  18 2.876859    172.16.2.30   10.5.23.209     TCP       60 8080 → 61849 [ACK] Seq=474 Ack=303 Win=32720 Len=0
  20 3.514887    10.5.23.209   172.16.2.30     TCP       66 61874 → 8080 [SYN] Seq=0 Win=8192 Len=0 MSS=1460 WS=256 SACK_PERM=1
  21 3.515881    10.5.23.209   172.16.2.30     TCP       66 61875 → 8080 [SYN] Seq=0 Win=8192 Len=0 MSS=1460 WS=256 SACK_PERM=1
  22 3.516112    10.5.23.209   172.16.2.30     TCP       66 61876 → 8080 [SYN] Seq=0 Win=8192 Len=0 MSS=1460 WS=256 SACK_PERM=1
  23 3.516293    172.16.2.30   10.5.23.209     TCP       66 8080 → 61874 [SYN, ACK] Seq=0 Ack=1 Win=65535 Len=0 MSS=1400 WS=8 SACK_PERM=1
  24 3.516293    172.16.2.30   10.5.23.209     TCP       66 8080 → 61875 [SYN, ACK] Seq=0 Ack=1 Win=65535 Len=0 MSS=1400 WS=8 SACK_PERM=1

> Frame 4: 120 bytes on wire (960 bits), 120 bytes captured (960 bits) on interface 0
> Ethernet II, Src: Cisco_c9:88:ff (40:55:39:c9:88:ff), Dst: Dell_d7:2b:77 (f8:b1:56:d7:2b:77)
> Internet Protocol Version 4, Src: 10.5.18.80, Dst: 10.5.23.209
> Internet Control Message Protocol
```

Now, here I am showing that instead of TCP, suppose I have applied a filter IP. So, I want to capture all IP packets. So, now, you see in the protocol and not only TCP, the other packets which run on top of IP are also getting captured; well TCP runs on top of IP. So, by default TCP will get captured; but you can see other types NBNS, ICMP, OSPF and so on; these packets are also getting captured ok. So, here the details of the packets are very similar. So, you can create filters like this, different types of filters as you want.

(Refer Slide Time: 13:51)


*Ethernet
File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help
ip
swayam

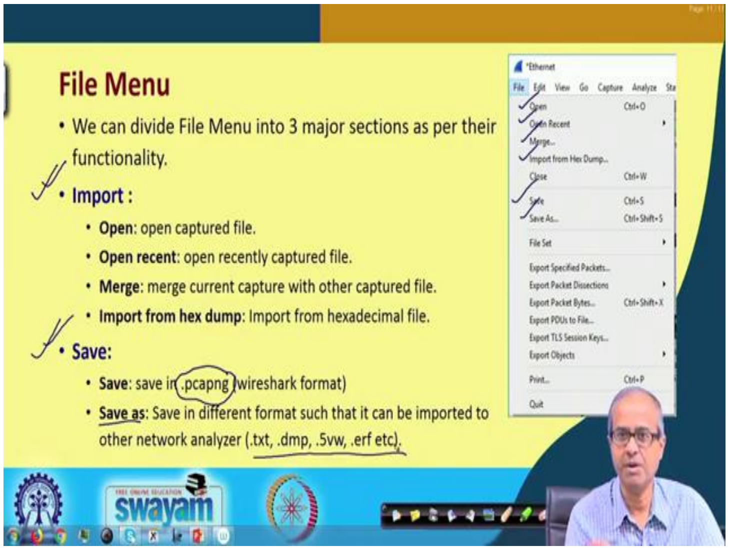
IP Packet Header Detail

```
No.  Time      Source       Destination  Protocol Lengt Info
   2 0.173997  10.5.23.209  10.5.23.255  NBNS      92 Name query NB WPAD<00>
   3 0.174067  10.5.18.84   10.5.23.209  ICMP     120 Destination unreachable (Port unreachable)
   4 0.175126  10.5.18.80   10.5.23.209  ICMP     120 Destination unreachable (Port unreachable)

> Frame 4: 120 bytes on wire (960 bits), 120 bytes captured (960 bits) on interface 0
> Ethernet II, Src: Cisco_c9:88:ff (40:55:39:c9:88:ff), Dst: Dell_d7:2b:77 (f8:b1:56:d7:2b:77)
v Internet Protocol Version 4, Src: 10.5.18.80, Dst: 10.5.23.209
    0100 .... = Version: 4
    .... 0101 = Header Length: 20 bytes (5)
  > Differentiated Services Field: 0xc0 (DSCP: CS6, ECN: Not-ECT)
    Total Length: 106
    Identification: 0xc383 (50051)
  > Flags: 0x0000
    Time to live: 63
    Protocol: ICMP (1)
    Header checksum: 0x7925 [validation disabled]
    [Header checksum status: Unverified]
    Source: 10.5.18.80
    Destination: 10.5.23.209
> Internet Control Message Protocol

0000  f8 b1 56 d7 2b 77 40 55  39 c9 88 ff 08 00 45 c0   ..V.+w@U 9.....E.
0010  00 6a c3 83 00 00 3f 01  79 25 0a 05 12 50 0a 05   .j....?. y%...P..
0020  17 d1 03 03 3b 73 00 00  00 00 45 00 00 4e 1f ca   ....;s.. ..E..N..
0030  00 00 7f 11 dd aa 0a 05  17 d1 0a 05 12 50 00 89   ........ .....P..
0040  00 89 00 3a e5 3f 99 8f  01 10 00 01 00 00 00 00   ...:.?.. ........
0050  00 00 20 46 48 46 41 45  42 45 45 43 41 43 41 43   .. FHFAE BEECACAC
0060  41 43 41 43 41 43 41 43  41 43 41 43 41 43 41 43   ACACACAC ACACACAC
0070  41 41 41 00 00 20 00 01                            AAA.. ..
```

Now, if you click on one of these packets, let us say, if I click on 1 of these packets, I can see the IP packet header detail, if I am selecting IP; see in the earlier case, previous example, I was selecting TCP here; that is why the detail was, that was getting, was the relevant TCP header details; but here I have selected IP and I have clicked on a packet; I will be getting the corresponding headers of the IP protocol. You see, these are all familiar things protocol version number, then source IP address, destination IP address, then you can say header length, Id, flags, time to live, protocol, header checksum.

So, all the fields in the IP header are being showed here. These are shown in a textual form and the entire content of the packet is also displayed in hexadecimal in the bottom and on the right, you can also see the same thing in ASCII form right. So, you can visualize the entire contents of the IP packet. Now, let us look at the different menu options; what are the different settings that you can have in Wireshark to use it in the way you want to.

(Refer Slide Time: 15:15)



File Menu

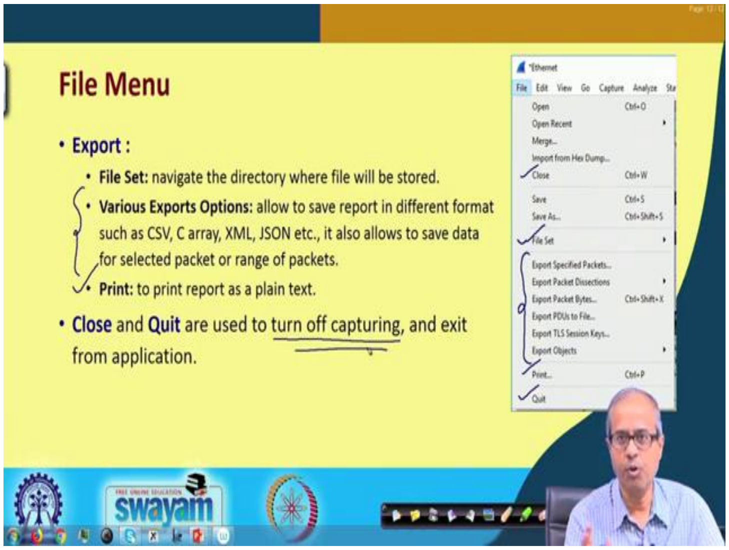
- We can divide File Menu into 3 major sections as per their functionality.
- **Import :**
  - **Open:** open captured file.
  - **Open recent:** open recently captured file.
  - **Merge:** merge current capture with other captured file.
  - **Import from hex dump:** Import from hexadecimal file.
- **Save:**
  - **Save:** save in .pcapng wireshark format)
  - **Save as:** Save in different format such that it can be imported to other network analyzer (.txt, .dmp, .5vw, .erf etc).

First comes the file menu. Well in the file menu, broadly you can divide it into 3 different sections. One is the import section, where you want to read some new thing. You see here, there are different options like open, open recent, merge, import from hex dump; there are 4 options here under this category.

So, you can open a file which was already captured earlier. You can open the most recently captured file or you can merge the most current capture with an existing file which was captured earlier or you might have created a hex dump earlier that was an option also to say. So, you can import from a hex file from a hex dump file.

Similarly, there are some save options; you can see save, save as. So, you can save in particular Wireshark format; Wireshark uses some special formats for saving or you can you save as, there are multiple formats; you can select which format you want to save the data in, the capture data.

(Refer Slide Time: 16:32)



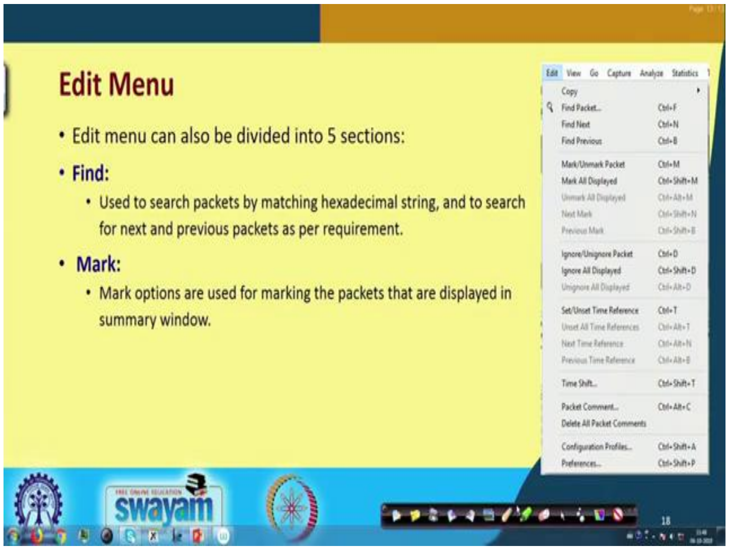
File Menu

- **Export :**
  - **File Set:** navigate the directory where file will be stored.
  - **Various Exports Options:** allow to save report in different format such as CSV, C array, XML, JSON etc., it also allows to save data for selected packet or range of packets.
  - **Print:** to print report as a plain text.
- **Close** and **Quit** are used to turn off capturing, and exit from application.

Import, save and the third one is export. So, under export you can see there are a host number of export options. So, export specifies first is the, there is a file set where you specify in which folder you want to export your captured data into; where the file will be stored and there are various export options you can specify.

So, whatever report you are generating from the packet capture, you can specify various different kinds of reports and you can save it in various different formats or even you can print; if you want a print, you can also print the report ok. And finally, there is close or quit, where you can close a window or you can quit the entire tool which will turn off the capturing and also pause or exit the application; this is about the file menu.

(Refer Slide Time: 17:33)



Edit Menu

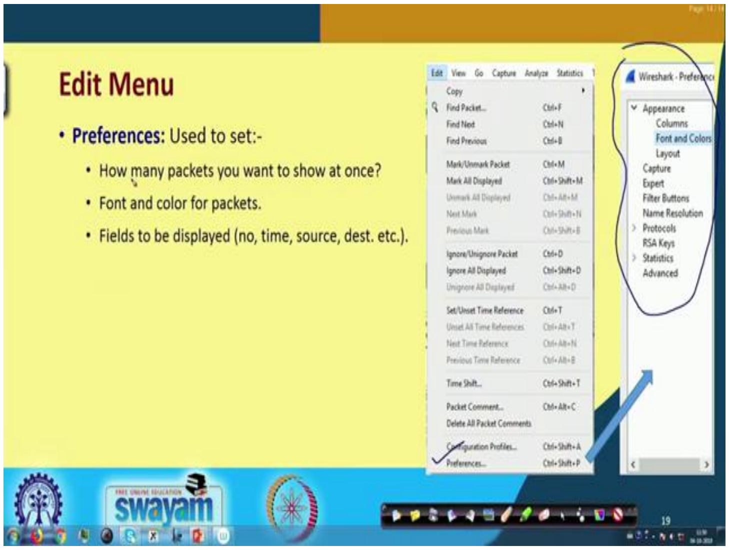
- Edit menu can also be divided into 5 sections:
- **Find:**
  - Used to search packets by matching hexadecimal string, and to search for next and previous packets as per requirement.
- **Mark:**
  - Mark options are used for marking the packets that are displayed in summary window.

Edit View Go Capture Analyze Statistics
Copy
Find Packet... Ctrl+F
Find Next Ctrl+N
Find Previous Ctrl+B
Mark/Unmark Packet Ctrl+M
Mark All Displayed Ctrl+Shift+M
Unmark All Displayed Ctrl+Alt+M
Next Mark Ctrl+Shift+N
Previous Mark Ctrl+Shift+B
Ignore/Unignore Packet Ctrl+D
Ignore All Displayed Ctrl+Shift+D
Unignore All Displayed Ctrl+Alt+D
Set/Unset Time Reference Ctrl+T
Unset All Time References Ctrl+Alt+T
Next Time Reference Ctrl+Alt+N
Previous Time Reference Ctrl+Alt+B
Time Shift... Ctrl+Shift+T
Packet Comment... Ctrl+Alt+C
Delete All Packet Comments
Configuration Profiles... Ctrl+Shift+A
Preferences... Ctrl+Shift+P
swayam
18

Now, let us come to the edit menu. So, if you click on edit on the top, so, here again you will see that there are so many menu options. So, broadly you can divide it up to 5 sections. First is the class of find; so you are trying to search for a packet. So, under find you can search packets by specifying some hexadecimal string; it will match whether that string is present in any of the packets; wherever there is a match, only those packets will be displayed.

Then you have some mark; well you can mark some of the packets that are displayed on the screen so that you can analyze them later; you can selectively mark some of the packets; this will be under the mark option.

(Refer Slide Time: 18:33)



Edit Menu

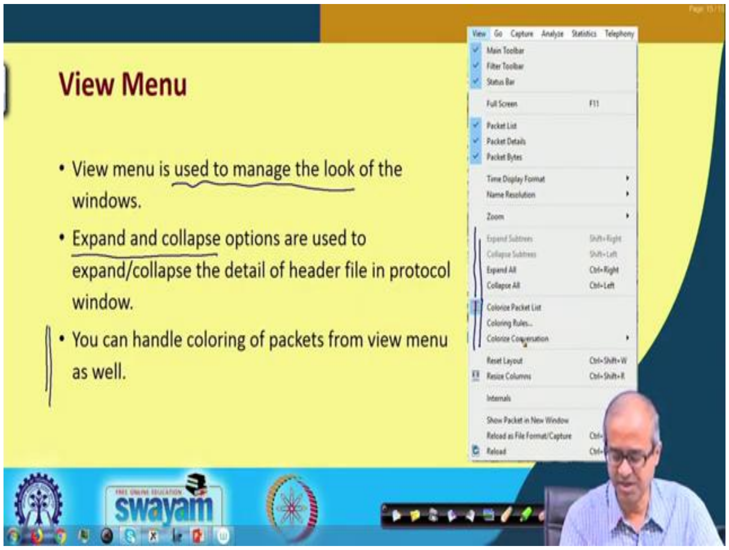
- Preferences: Used to set:-
  - How many packets you want to show at once?
  - Font and color for packets.
  - Fields to be displayed (no, time, source, dest. etc.).

Edit View Go Capture Analyze Statistics
Copy
Find Packet... Ctrl+F
Find Next Ctrl+N
Find Previous Ctrl+B
Mark/Unmark Packet Ctrl+M
Mark All Displayed Ctrl+Shift+M
Unmark All Displayed Ctrl+Alt+M
Next Mark Ctrl+Shift+N
Previous Mark Ctrl+Shift+B
Ignore/Unignore Packet Ctrl+D
Ignore All Displayed Ctrl+Shift+D
Unignore All Displayed Ctrl+Alt+D
Set/Unset Time Reference Ctrl+T
Unset All Time References Ctrl+Alt+T
Next Time Reference Ctrl+Alt+N
Previous Time Reference Ctrl+Alt+B
Time Shift... Ctrl+Shift+T
Packet Comment... Ctrl+Alt+C
Delete All Packet Comments
Configuration Profiles... Ctrl+Shift+A
Preferences... Ctrl+Shift+P
Wireshark · Preferences
Appearance
Columns
Font and Colors
Layout
Capture
Expert
Filter Buttons
Name Resolution
Protocols
RSA Keys
Statistics
Advanced
swayam
19

Then you can specify some preferences well. The preference option comes at the end; you see, at the very bottom you have preferences here and if you click on preferences, another window comes up. Here some specific things are mentioned as you can see font, colour and so on. Like can you specify among other things; that how many packets you want to display at once on the screen; you can change it in the preference 10, 20 or more.

So, what font type and what color you can use for the different types of packets; you can specify that and also what are the fields you want to display. By default Wireshark displays certain fields; but in the preference you can, if you want, you can hide some of the fields or some of the columns ok. So, under the preferences you can specify how you want your window or the packet display to look like.

(Refer Slide Time: 19:39)



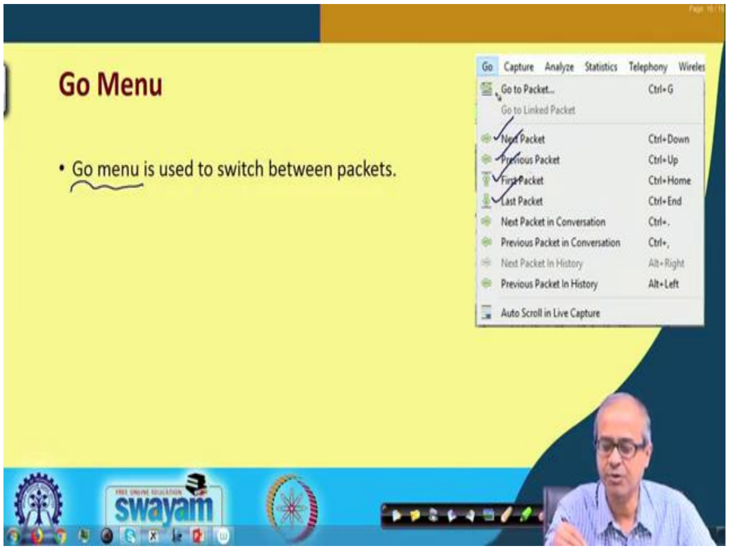
View Menu

- View menu is used to manage the look of the windows.
- Expand and collapse options are used to expand/collapse the detail of header file in protocol window.
- You can handle coloring of packets from view menu as well.

Then comes the view menu; there are other options also in view menu; some of them I mentioned. Next in the view menu, well here you can manage the look of the windows; how the windows will look like; then you can expand and collapse. You see, there are expand and collapse options here. So, some of the details of the header file you can show in detail or you can collapse them if you want or you can also select colouring of the different packets; these options are also available ok.

With this, if we explore with this, you will see a lot of different options are there; you can colour them in various ways so that when the packets are getting displayed, it will be easier for you to locate specific types of packets. So, here I am not going into all the details of these menu options; but these are broadly the types of options or commands you can give.

(Refer Slide Time: 20:52)



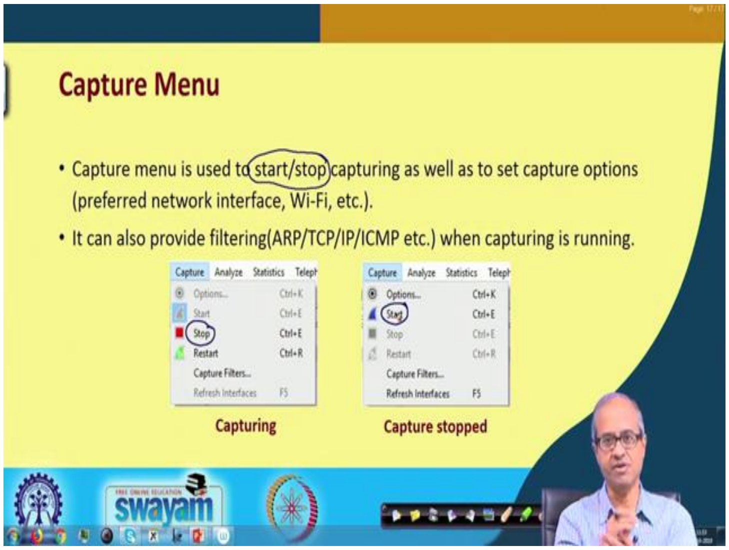
Go Menu

- Go menu is used to switch between packets.

Then there is a menu called go where you can go to some specific packet; like you are displaying a packet, current packet; you can either go to the next packet, previous packet or you can jump to some other specific packet. So, there are a number of so called go options; these are all under Go menu; you can see. Next packet, previous packet, you can go to the first packet, last packet; you to go to a particular packet ok.

Now, with respect to a conversation that is going on, you can go to the next packet; some transaction is going on, next packet within that conversation or previous packet in that conversation. In terms of history, if you have saved a number of packets, viewed a number of packets, they will be kept in the history; you can move along in the history, also browse the history. So, there are various ways you can go from one packet to another depending on which packet you want to view next ok, fine.

(Refer Slide Time: 22:00)

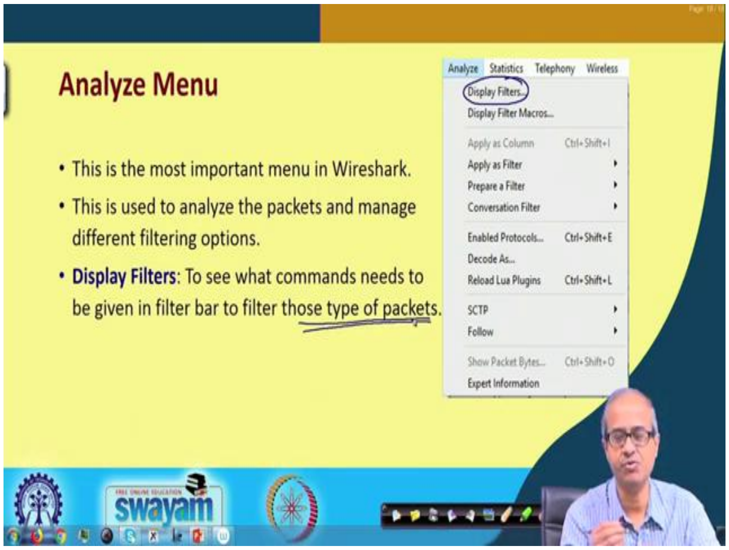


Capture Menu

- Capture menu is used to start/stop capturing as well as to set capture options (preferred network interface, Wi-Fi, etc.).
- It can also provide filtering(ARP/TCP/IP/ICMP etc.) when capturing is running.

Then comes the capture menu. Now, in the capture menu, here you basically specify that you want to start the capturing process or stop the capturing process. You see, when capturing is going on, you see this start option is disabled, but this stop option is enabled; you can click on this stop. But when capturing is not going on, capture is stopped, it is the other way around; you see stop option is disabled, but the start option is enabled; you can click it. So, just under the capture menu, you can go, you can either start capture or you can stop capture whenever you want.

(Refer Slide Time: 22:45)



Analyze Menu

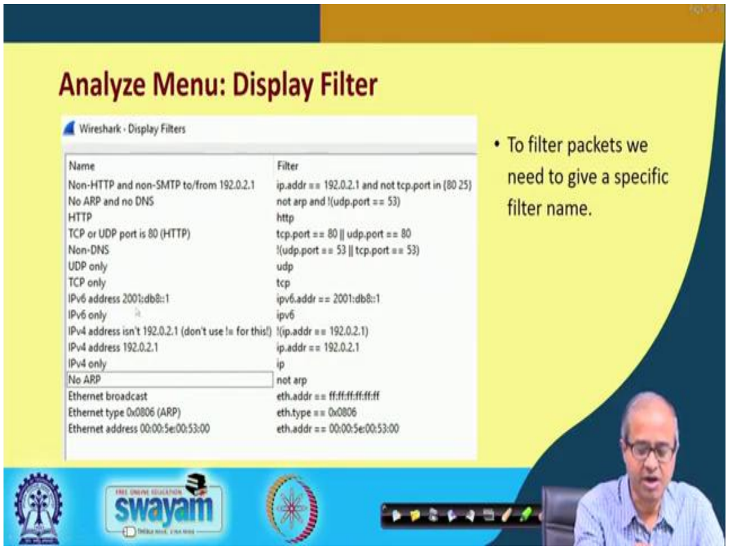
- This is the most important menu in Wireshark.
- This is used to analyze the packets and manage different filtering options.
- **Display Filters**: To see what commands needs to be given in filter bar to filter those type of packets.

Analyze Statistics Telephony Wireless
Display Filters...
Display Filter Macros...
Apply as Column Ctrl+Shift+I
Apply as Filter
Prepare a Filter
Conversation Filter
Enabled Protocols... Ctrl+Shift+E
Decode As...
Reload Lua Plugins Ctrl+Shift+L
SCTP
Follow
Show Packet Bytes... Ctrl+Shift+O
Expert Information
swayam

Then comes the analyze menu; well analyze is one of the most important menus in Wireshark; because here you can specify the different kinds of filters and analysis methods that you want to operate on the packets that you have captured ok. So, you see the different options in the analyse thing display filter, then apply some filter, then enabled protocol, which are the protocols which are enabled, follow; these are some of the important menu options here.

Display filters, the first option as you can see display filters here. Here you can just specify the filters that what types of packets will be captured and displayed on the screen; you can specify this with respect to a detailed list.

(Refer Slide Time: 23:45)



Analyze Menu: Display Filter

Wireshark · Display Filters

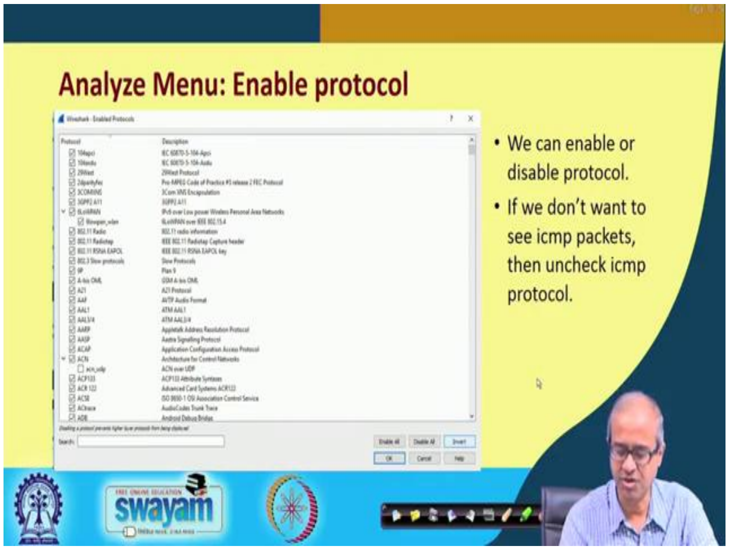
Name	Filter
Non-HTTP and non-SMTP to/from 192.0.2.1	ip.addr == 192.0.2.1 and not tcp.port in {80 25}
No ARP and no DNS	not arp and !(udp.port == 53)
HTTP	http
TCP or UDP port is 80 (HTTP)	tcp.port == 80 || udp.port == 80
Non-DNS	!(udp.port == 53 || tcp.port == 53)
UDP only	udp
TCP only	tcp
IPv6 address 2001:db8::1	ipv6.addr == 2001:db8::1
IPv6 only	ipv6
IPv4 address isn't 192.0.2.1 (don't use != for this!)	!(ip.addr == 192.0.2.1)
IPv4 address 192.0.2.1	ip.addr == 192.0.2.1
IPv4 only	ip
No ARP	not arp
Ethernet broadcast	eth.addr == ff:ff:ff:ff:ff:ff
Ethernet type 0x0806 (ARP)	eth.type == 0x0806
Ethernet address 00:00:5e:00:53:00	eth.addr == 00:00:5e:00:53:00

- To filter packets we need to give a specific filter name.

So, let us see some of these. Display filter if you select, so I am showing a part of the window; this is a large doc, means document; you can scroll up and down; you can see some of these. Some of the filter non-HTTP and non-SMTP, no ARP, no DNS, TCP only, UDP only, IPv6 only; there are many kind of filters available; you select which filter is relevant to; what you are trying to see or view; you click on that.

On the right side the explanation of the filters is also mentioned in some language which is easy to understand that how it is checked non-HTTP, non-SMTP to or from this IP address which means IP address should be equal to this and not TCP port in 80 or 25. The port number should not be 20 or 25 or 80, SMTP or HTTP like this. So, you can specify a specific filter name to start filtering the packets.

(Refer Slide Time: 26:53)



Analyze Menu: Enable protocol

Wireshark · Enabled Protocols

Protocol	Description
☑ 104apci	IEC 60870-5-104-Apci
☑ 104asdu	IEC 60870-5-104-Asdu
☑ 29West	29West Protocol
☑ 2dparityfec	Pro-MPEG Code of Practice #3 release 2 FEC Protocol
☑ 3COMXNS	3Com XNS Encapsulation
☑ 3GPP2 A11	3GPP2 A11
☑ 6LoWPAN	IPv6 over Low power Wireless Personal Area Networks
☑ 6lowpan_wlan	6LoWPAN over IEEE 802.15.4
☑ 802.11 Radio	802.11 radio information
☑ 802.11 Radiotap	IEEE 802.11 Radiotap Capture header
☑ 802.11 RSNA EAPOL	IEEE 802.11 RSNA EAPOL key
☑ 802.3 Slow protocols	Slow Protocols
☑ 9P	Plan 9
☑ A-bis OML	GSM A-bis OML
☑ A21	A21 Protocol
☑ AAF	AVTP Audio Format
☑ AAL1	ATM AAL1
☑ AAL3/4	ATM AAL3/4
☑ AARP	Appletalk Address Resolution Protocol
☑ AASP	Aastra Signalling Protocol
☑ ACAP	Application Configuration Access Protocol
☑ ACN	Architecture for Control Networks
□ acn_udp	ACN over UDP
☑ ACP133	ACP133 Attribute Syntaxes
☑ ACR 122	Advanced Card Systems ACR122
☑ ACSE	ISO 8650-1 OSI Association Control Service
☑ ACtrace	AudioCodes Trunk Trace
☑ ADB	Android Debug Bridge

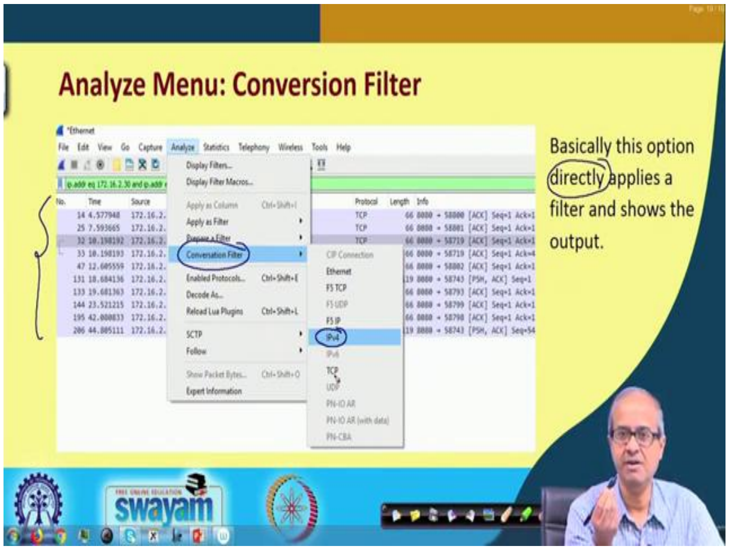
Disabling a protocol prevents higher layer protocols from being displayed

Search:

- We can enable or disable protocol.
- If we don't want to see icmp packets, then uncheck icmp protocol.

Then there is an enable protocol option under the analyze menu. So, here again you will get a big list of the protocols. So, these are all check boxes; you can check or uncheck some of the options. Suppose you do not want to see the ICMP packets; you will have to uncheck the box that corresponds to ICMP; well in this window you cannot see ICMP; it is down below; you will have to scroll up to see ICMP. But you will be seeing a large list of protocols which are all supported by Wireshark and these are used in some network or the other. So, you can, you can enable some of the protocols or disable some of them as you want.

(Refer Slide Time: 25:38)



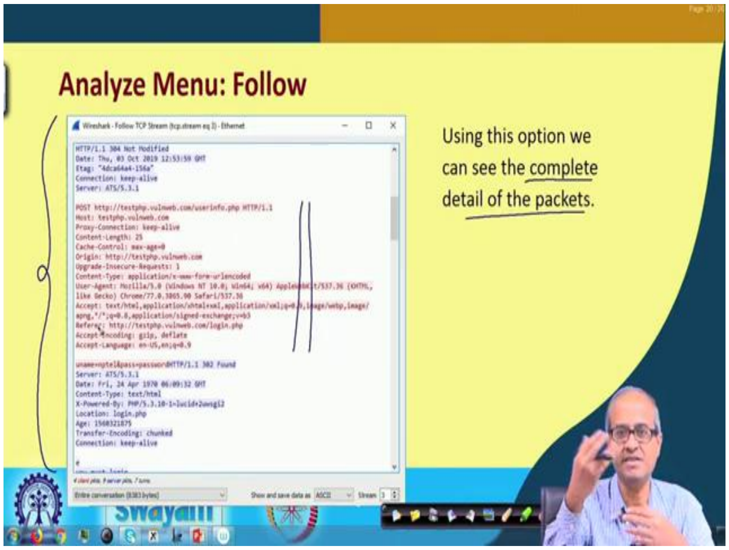
Analyze Menu: Conversion Filter

```
ip.addr eq 172.16.2.30 and ip.addr

No.  Time        Source      Protocol  Length  Info
 14  4.577948    172.16.2.   TCP           66  8080 → 58800 [ACK] Seq=1 Ack=1
 25  7.593665    172.16.2.   TCP           66  8080 → 58801 [ACK] Seq=1 Ack=1
 32  10.198192   172.16.2.   TCP           66  8080 → 58719 [ACK] Seq=1 Ack=1
 33  10.198193   172.16.2.                 66  8080 → 58719 [ACK] Seq=1 Ack=4
 47  12.605559   172.16.2.                 66  8080 → 58802 [ACK] Seq=1 Ack=1
131  18.684136   172.16.2.                119  8080 → 58743 [PSH, ACK] Seq=1
133  19.681363   172.16.2.                 66  8080 → 58793 [ACK] Seq=1 Ack=1
144  23.521215   172.16.2.                 66  8080 → 58799 [ACK] Seq=1 Ack=1
195  42.000833   172.16.2.                 66  8080 → 58798 [ACK] Seq=1 Ack=1
206  44.005111   172.16.2.                119  8080 → 58743 [PSH, ACK] Seq=54
```

Basically this option directly applies a filter and shows the output.

Then you can have something called conversion filter. The conversion filter is something like you are applying a filter directly. You directly apply a filter and see the output. This is like a quick shortcut option; you can say. You can directly go to under analyse; you can go to this conversation filter; you will get a list; you can directly specify say, for example, IP version 4. So, if I click IPv4, then only IPv4 packets will get displayed. So, I can very quickly select what I want to see ok. So, this is like a shortcut option to select specific things.

(Refer Slide Time: 26:24)



Analyze Menu: Follow

Wireshark - Follow TCP Stream (tcp.stream eq 1) - Ethernet

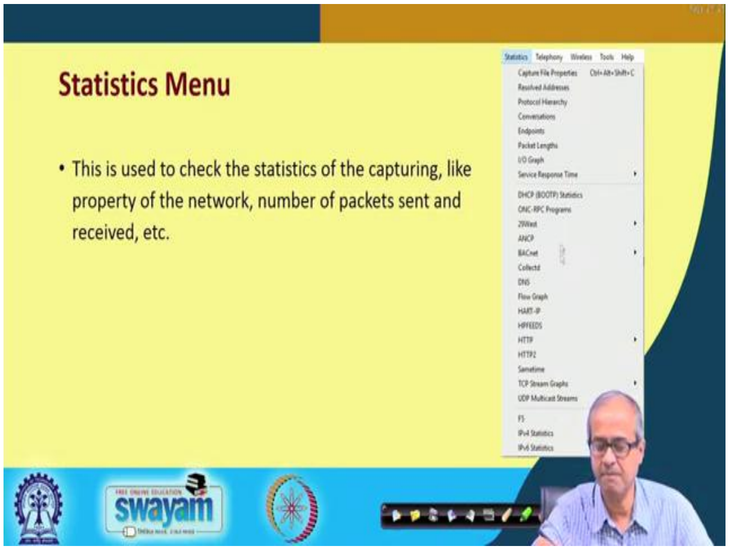
```
HTTP/1.1 304 Not Modified
Date: Thu, 03 Oct 2019 12:53:59 GMT
Etag: "4dca64a4-156a"
Connection: keep-alive
Server: ATS/5.3.1

POST http://testphp.vulnweb.com/userinfo.php HTTP/1.1
Host: testphp.vulnweb.com
Proxy-Connection: keep-alive
Content-Length: 25
Cache-Control: max-age=0
Origin: http://testphp.vulnweb.com
Upgrade-Insecure-Requests: 1
Content-Type: application/x-www-form-urlencoded
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML,
like Gecko) Chrome/77.0.3865.90 Safari/537.36
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,image/
apng,*/*;q=0.8,application/signed-exchange;v=b3
Referer: http://testphp.vulnweb.com/login.php
Accept-Encoding: gzip, deflate
Accept-Language: en-US,en;q=0.9

uname=nptel&pass=passwordHTTP/1.1 302 Found
Server: ATS/5.3.1
Date: Fri, 24 Apr 1970 06:09:32 GMT
Content-Type: text/html
X-Powered-By: PHP/5.3.10-1~lucid+2uwsgi2
Location: login.php
Age: 1568321875
Transfer-Encoding: chunked
Connection: keep-alive
```

4 client pkts, 8 server pkts, 7 turns
Entire conversation (8383 bytes)
Show and save data as ASCII
Stream 1

Using this option we can see the complete detail of the packets.

Then follow well, if I select, I mean, after selecting a packet if I click on the follow option under analyze, then I can see the complete detail of the packet. Here for example, there was one HTTP request packet which was selected and this follow option was there and you can see the entire detail of the HTTP response is shown here. These are the HTTP commands; you can see here completely ok; post, host, proxy connection, keep alive, these are all HTTP commands that goes between a client and a web server. The client sends a request; web server sends back a response right. So, this is how you can see them.

(Refer Slide Time: 27:21)

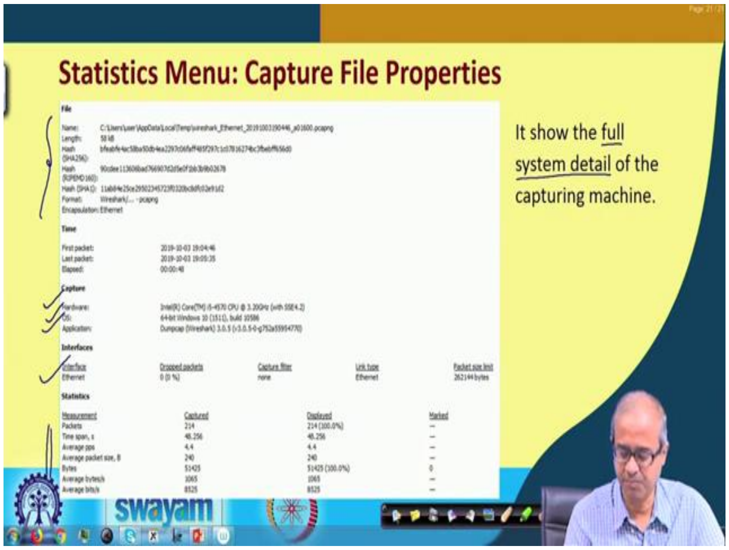


Statistics Menu

- This is used to check the statistics of the capturing, like property of the network, number of packets sent and received, etc.

Then there are a number of statistics menus; these are also interesting; you may be interested to look at various kinds of statistics. So, you can see, under statistics there are so many options available ok; I am just showing you a few of them.

(Refer Slide Time: 27:39)



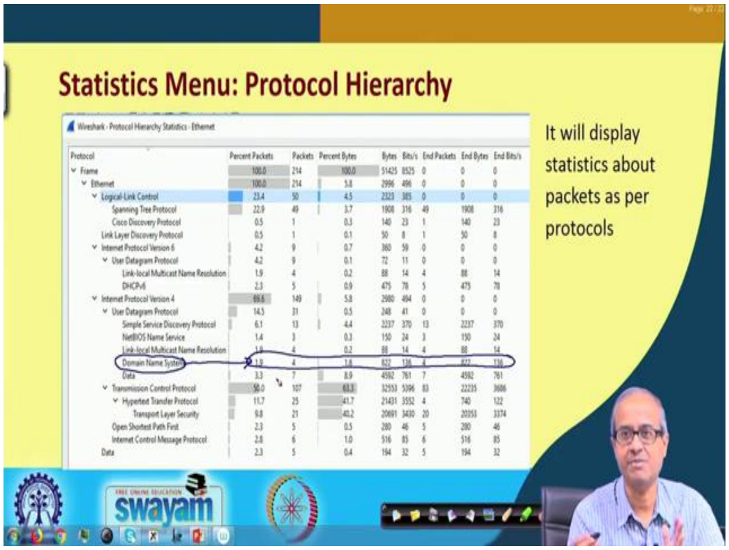
Statistics Menu: Capture File Properties

```
File

Name:           C:\Users\user\AppData\Local\Temp\wireshark_Ethernet_20191003190446_a01600.pcapng
Length:         50 kB
Hash            bfeabfe4ac58ba50db4ea2297c06faff485f297c1c0781627 4bc3fbebff656d0
(SHA256):
Hash            90cdee113606bad766907d2d5e0f1bb3b9b02678
(RIPEMD160):
Hash (SHA1):    11ab84e25ce29502345723f0320bcb8fc02e91d2
Format:         Wireshark/... - pcapng
Encapsulation:  Ethernet

Time

First packet:          2019-10-03 19:04:46
Last packet:           2019-10-03 19:05:35
Elapsed:               00:00:48

Capture

Hardware:              Intel(R) Core(TM) i5-4570 CPU @ 3.20GHz (with SSE4.2)
OS:                    64-bit Windows 10 (1511), build 10586
Application:           Dumpcap (Wireshark) 3.0.5 (v3.0.5-0-g752a55954770)

Interfaces

Interface              Dropped packets        Capture filter        Link type         Packet size limit
Ethernet               0 (0 %)                none                  Ethernet          262144 bytes

Statistics

Measurement               Captured               Displayed              Marked
Packets                   214                    214 (100.0%)           —
Time span, s              48.256                 48.256                 —
Average pps               4.4                    4.4                    —
Average packet size, B    240                    240                    —
Bytes                     51425                  51425 (100.0%)         0
Average bytes/s           1065                   1065                   —
Average bits/s            8525                   8525                   —
```

It show the full system detail of the capturing machine.

Like for example, capture file properties, if you select this, then it will show you full system detail of the capturing host. The host where you are carrying out the capture, it will specify not only the file, but also the hardware which hardware, which operating system, what application you are using, what kind of interface the packet capture is running on and how many captured packets, how many packets have been captured over how much time, everything. So, all the details are being shown, if you want to see them in a statistical and concise form.

(Refer Slide Time: 28:24)



Statistics Menu: Protocol Hierarchy

Wireshark · Protocol Hierarchy Statistics · Ethernet

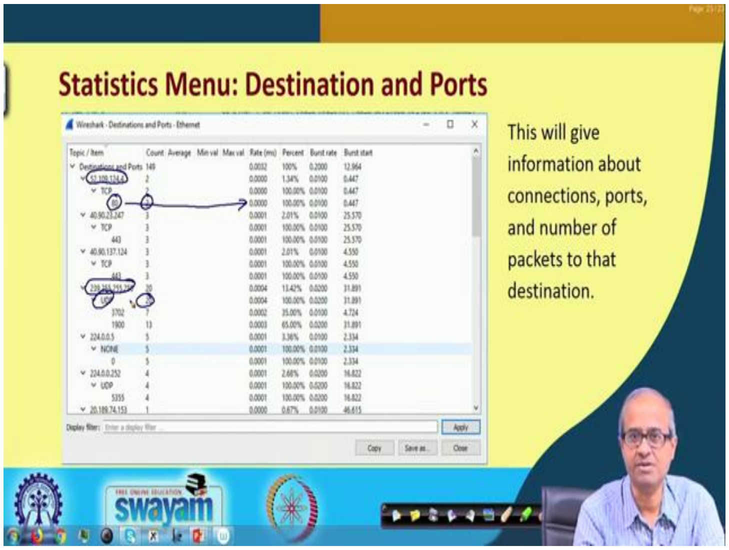
Protocol	Percent Packets	Packets	Percent Bytes	Bytes	Bits/s	End Packets	End Bytes	End Bits/s
˅ Frame	100.0	214	100.0	51425	8525	0	0	0
˅ Ethernet	100.0	214	5.8	2996	496	0	0	0
˅ Logical-Link Control	23.4	50	4.5	2323	385	0	0	0
Spanning Tree Protocol	22.9	49	3.7	1908	316	49	1908	316
Cisco Discovery Protocol	0.5	1	0.3	140	23	1	140	23
Link Layer Discovery Protocol	0.5	1	0.1	50	8	1	50	8
˅ Internet Protocol Version 6	4.2	9	0.7	360	59	0	0	0
˅ User Datagram Protocol	4.2	9	0.1	72	11	0	0	0
Link-local Multicast Name Resolution	1.9	4	0.2	88	14	4	88	14
DHCPv6	2.3	5	0.9	475	78	5	475	78
˅ Internet Protocol Version 4	69.6	149	5.8	2980	494	0	0	0
˅ User Datagram Protocol	14.5	31	0.5	248	41	0	0	0
Simple Service Discovery Protocol	6.1	13	4.4	2237	370	13	2237	370
NetBIOS Name Service	1.4	3	0.3	150	24	3	150	24
Link-local Multicast Name Resolution	1.9	4	0.2	88	14	4	88	14
Domain Name System	1.9	4	1.8	822	136	4	822	136
Data	3.3	7	8.9	4592	761	7	4592	761
˅ Transmission Control Protocol	50.0	107	63.3	32553	5396	83	22235	3686
˅ Hypertext Transfer Protocol	11.7	25	41.7	21431	3552	4	740	122
Transport Layer Security	9.8	21	40.2	20691	3430	20	20053	3374
Open Shortest Path First	2.3	5	0.5	280	46	5	280	46
Internet Control Message Protocol	2.8	6	1.0	516	85	6	516	85
Data	2.3	5	0.4	194	32	5	194	32

It will display statistics about packets as per protocols

Then you can look at protocol hierarchies; like you can see, if you select on protocols, so, protocol wise you can see statistics about the packets; like here, with respect to protocol you are viewing something like a statistical summary. Like for example, let us say under internet protocol version 4, UDP let us say, Domain Name System, DNS. So, you can see under DNS how many packets were sent. So, all those details you can see here ok. So, these details will be shown here, percentage packets, bytes, end packets and some information.

Similarly, the different kinds of packets, the protocols whatever was transferred, a breakup you can see, a summary kind of a report. So, actually you may try and find out what kind of packets are most frequently traversing the network; then you can try and find out the reason; why it is happening?

(Refer Slide Time: 39:32)



Statistics Menu: Destination and Ports

Wireshark · Destinations and Ports · Ethernet

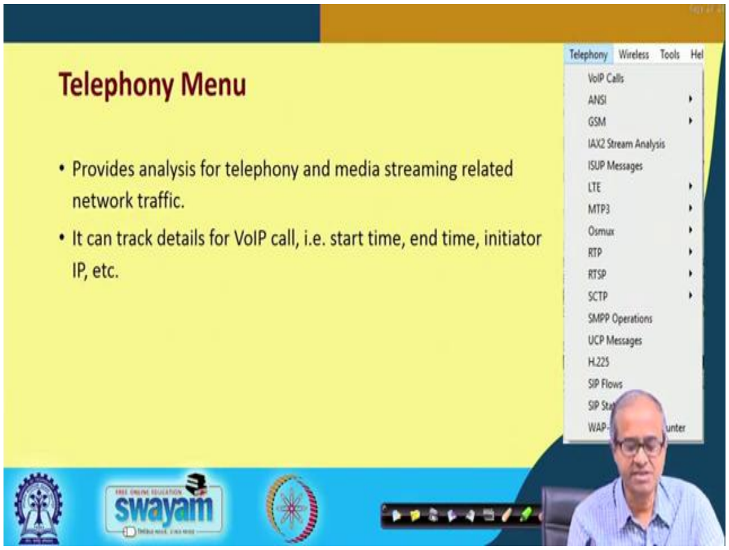
Topic / Item	Count	Average	Min val	Max val	Rate (ms)	Percent	Burst rate	Burst start
Destinations and Ports	149				0.0032	100%	0.2000	12.964
52.109.124.4	2				0.0000	1.34%	0.0100	0.447
TCP	2				0.0000	100.00%	0.0100	0.447
80	2				0.0000	100.00%	0.0100	0.447
40.90.23.247	3				0.0001	2.01%	0.0100	25.570
TCP	3				0.0001	100.00%	0.0100	25.570
443	3				0.0001	100.00%	0.0100	25.570
40.90.137.124	3				0.0001	2.01%	0.0100	4.550
TCP	3				0.0001	100.00%	0.0100	4.550
443	3				0.0001	100.00%	0.0100	4.550
239.255.255.250	20				0.0004	13.42%	0.0200	31.891
UDP	20				0.0004	100.00%	0.0200	31.891
3702	7				0.0002	35.00%	0.0100	4.724
1900	13				0.0003	65.00%	0.0200	31.891
224.0.0.5	5				0.0001	3.36%	0.0100	2.334
NONE	5				0.0001	100.00%	0.0100	2.334
0	5				0.0001	100.00%	0.0100	2.334
224.0.0.252	4				0.0001	2.68%	0.0200	16.822
UDP	4				0.0001	100.00%	0.0200	16.822
5355	4				0.0001	100.00%	0.0200	16.822
20.189.74.153	1				0.0000	0.67%	0.0100	46.615

Display filter: Enter a display filter ...

This will give information about connections, ports, and number of packets to that destination.

Similarly, with respect to destinations and ports you can obtain some statistics. Like for example, for a particular IP address destination, TCP port number 80 let us say. So, here you can say TCP port number 80, this is the so called information; there are 2 packets total and some information. Like for this particular host UDP packet, there were 20 UDP packets. So, like this, you can get statistics with respect to hosts and port numbers.

(Refer Slide Time: 30:15)



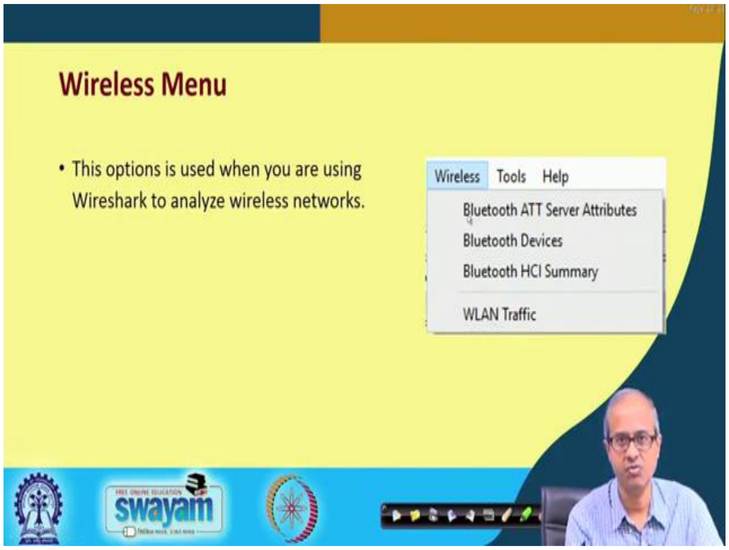
Telephony Menu

- Provides analysis for telephony and media streaming related network traffic.
- It can track details for VoIP call, i.e. start time, end time, initiator IP, etc.

Well how many packets were delivered to those destinations; well, then there are menus like telephony menu; well here I am not going into the detail of this. There are many cases or instances where you want to track details of voice over IP calls; you know when you use the voice over IP services, the voice that we generate, they are digitized and they are sent out as packets over a network, over a conventional network.

So, Wireshark can also capture voice over IP packets and you can visualize them; that whether any voice over IP communication is going on in the network right; start time, end time, initiator IP, lot of options are there under this. So, I am not going into detail of this.

(Refer Slide Time: 30:58)

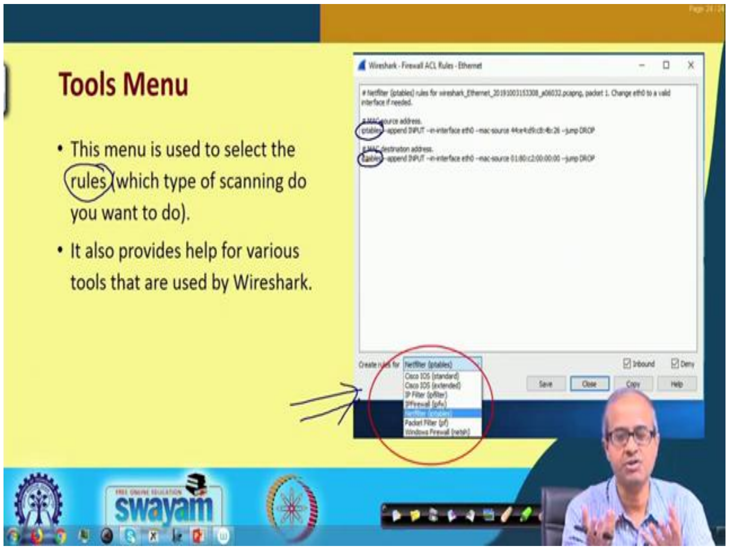


Wireless Menu

- This options is used when you are using Wireshark to analyze wireless networks.

Similarly, you have an wireless menu where you have specific options for capturing data from wireless networks like a wireless LAN or Bluetooth; these are the most widely used and commonly used type. So, here there are a number of options; you can start capturing from those wireless interfaces; instead of so called wide LAN you can capture, you can start your capture from a wireless LAN also.

(Refer Slide Time: 31:29)



Tools Menu

- This menu is used to select the rules (which type of scanning do you want to do).
- It also provides help for various tools that are used by Wireshark.

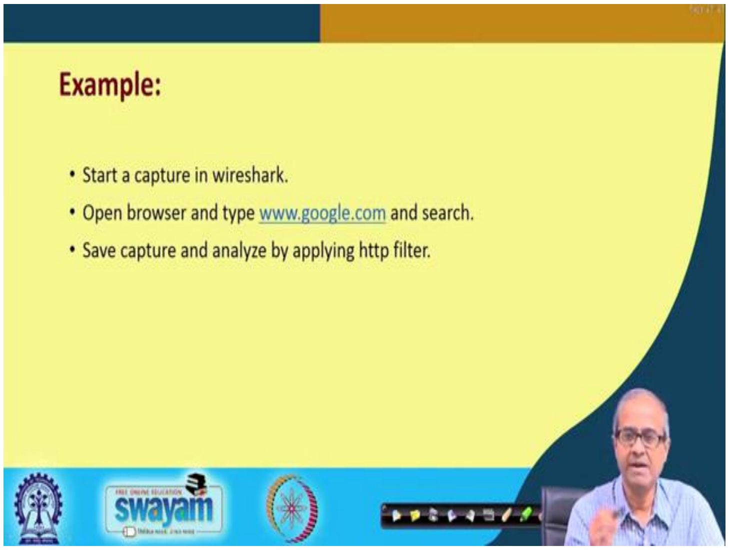
```
# Netfilter (iptables) rules for wireshark_Ethernet_20191003153308_a06032.pcapng, packet 1. Change eth0 to a valid interface if needed.

# MAC source address.
iptables --append INPUT --in-interface eth0 --mac-source 44:e4:d9:c8:4b:26 --jump DROP

# MAC destination address.
iptables --append INPUT --in-interface eth0 --mac-source 01:80:c2:00:00:00 --jump DROP
```

Create rules for: Netfilter (iptables)

Then there is a tools menu ok. Now, under tools menu, you can specify some scanning rules. Like here, you see a window like this comes up; down here you can see that you can create rules for different things, IP tables, packet filter, windows firewall. Suppose you want to filter some packets; you want to create your own firewall; you can specify some rules through this window ok. Well IP tables is an utility which is available under Linux; this is like a rudimentary firewall; you can configure IP tables and specify different rules; what do you want to stop; what do you want to filter out; what do you want to pass, ok.

So, this tools menu allows you to do all these things. Of course, I am not going into detail; because in order to understand this you have to have a very clear idea about how IP tables work; there is a tool that is available under Linux. Then let us look at some examples.

(Refer Slide Time: 32:48)

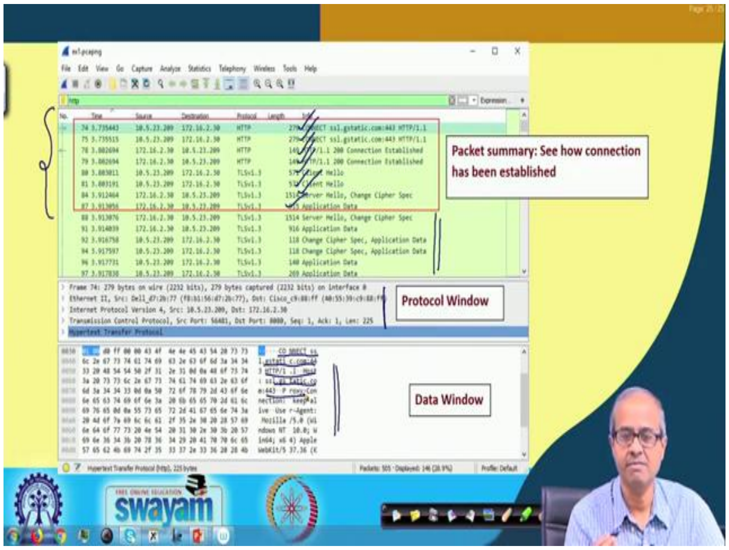


Example:

- Start a capture in wireshark.
- Open browser and type www.google.com and search.
- Save capture and analyze by applying http filter.

Let us say, we start with a very simple thing. We start capture in Wireshark, packet capturing and we open the browser **www.google.com** and we see what kind of packets are getting captured.

(Refer Slide Time: 33:05)



wl.pcapng
File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help
http
Expression...

```
No.  Time      Source       Destination  Protocol Length Info
74 3.735443   10.5.23.209  172.16.2.30  HTTP     279 CONNECT ssl.gstatic.com:443 HTTP/1.1
75 3.735515   10.5.23.209  172.16.2.30  HTTP     279 CONNECT ssl.gstatic.com:443 HTTP/1.1
78 3.882694   172.16.2.30  10.5.23.209  HTTP     140 HTTP/1.1 200 Connection Established
79 3.882694   172.16.2.30  10.5.23.209  HTTP     140 HTTP/1.1 200 Connection Established
80 3.883011   10.5.23.209  172.16.2.30  TLSv1.3  571 Client Hello
81 3.883191   10.5.23.209  172.16.2.30  TLSv1.3  53  Client Hello
84 3.912464   172.16.2.30  10.5.23.209  TLSv1.3  1514 Server Hello, Change Cipher Spec
87 3.913056   172.16.2.30  10.5.23.209  TLSv1.3  225 Application Data
88 3.913076   172.16.2.30  10.5.23.209  TLSv1.3  1514 Server Hello, Change Cipher Spec
91 3.914039   172.16.2.30  10.5.23.209  TLSv1.3  916 Application Data
92 3.916758   10.5.23.209  172.16.2.30  TLSv1.3  118 Change Cipher Spec, Application Data
94 3.917597   10.5.23.209  172.16.2.30  TLSv1.3  118 Change Cipher Spec, Application Data
96 3.917731   10.5.23.209  172.16.2.30  TLSv1.3  140 Application Data
97 3.917838   10.5.23.209  172.16.2.30  TLSv1.3  209 Application Data
```

Packet summary: See how connection has been established

```
> Frame 74: 279 bytes on wire (2232 bits), 279 bytes captured (2232 bits) on interface 0
> Ethernet II, Src: Dell_d7:2b:77 (f8:b1:56:d7:2b:77), Dst: Cisco_c9:88:ff (40:55:39:c9:88:ff)
> Internet Protocol Version 4, Src: 10.5.23.209, Dst: 172.16.2.30
> Transmission Control Protocol, Src Port: 56481, Dst Port: 8080, Seq: 1, Ack: 1, Len: 225
> Hypertext Transfer Protocol
```

Protocol Window

```
      d8 ff 00 00 43 4f  4e 4e 45 43 54 20 73 73     CO NNECT ss
6c 2e 67 73 74 61 74 69  63 2e 63 6f 6d 3a 34 34   l.gstati c.com:44
33 20 48 54 54 50 2f 31  2e 31 0d 0a 48 6f 73 74   3 HTTP/1 .1..Host
3a 20 73 73 6c 2e 67 73  74 61 74 69 63 2e 63 6f   : ssl.gs tatic.co
6d 3a 34 34 33 0d 0a 50  72 6f 78 79 2d 43 6f 6e   m:443..P roxy-Con
6e 65 63 74 69 6f 6e 3a  20 6b 65 65 70 2d 61 6c   nection:  keep-al
69 76 65 0d 0a 55 73 65  72 2d 41 67 65 6e 74 3a   ive..Use r-Agent:
20 4d 6f 7a 69 6c 6c 61  2f 35 2e 30 20 28 57 69    Mozilla /5.0 (Wi
6e 64 6f 77 73 20 4e 54  20 31 30 2e 30 3b 20 57   ndows NT  10.0; W
69 6e 36 34 3b 20 78 36  34 29 20 41 70 70 6c 65   in64; x6 4) Apple
57 65 62 4b 69 74 2f 35  33 37 2e 33 36 20 28 4b   WebKit/5 37.36 (K
```

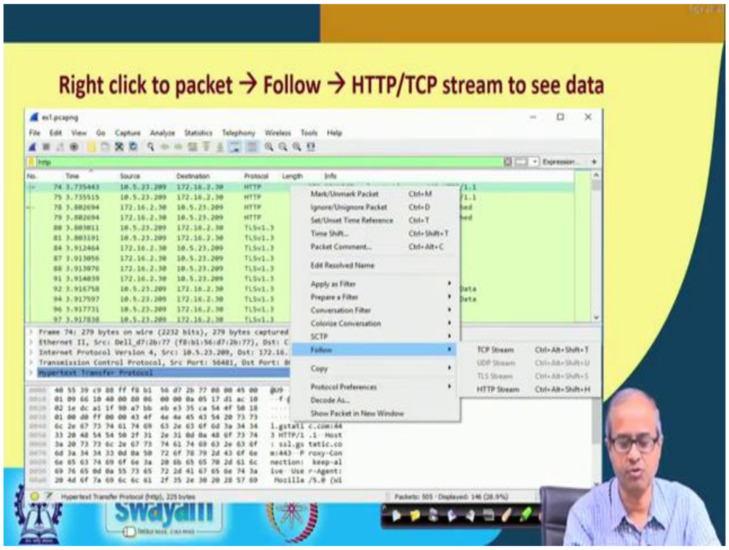
Data Window

Hypertext Transfer Protocol (http), 225 bytes
Packets: 505 · Displayed: 146 (28.9%)
Profile: Default

Well what we see is, the window will look something like this; where in the topmost window, the packet capture summary, you can see a number of packets; sorry, which are actually shown in this red rectangular box; these are the packets which are correspond, which correspond to this connection. So, when you connect to **google.com**, actually you are establishing an HTTP connection; say HTTP is a protocol running on top of TCP. So, you see, these are the so called HTTP connections, packets which are going; client sending Hello, server sending Hello, then the application data starts right.

So, there are a lot of things and because it is HTTPs, there are some other exchanges which are carrying out where the secret key and other things are shared, the protocols the cryptographic algorithm which is to be used that is shared so that secure data communication can take place and you can see the protocol window here and the data here. You say whatever connect ss1 data, you say these things are going in plaintext. So, you can see them in ASCII also right; these are not encrypted, the commands are not encrypted.

(Refer Slide Time: 34:33)



Right click to packet → Follow → HTTP/TCP stream to see data

ss1.pcapng
File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help
http
Expression...
Mark/Unmark Packet Ctrl+M
Ignore/Unignore Packet Ctrl+D
Set/Unset Time Reference Ctrl+T
Time Shift... Ctrl+Shift+T
Packet Comment... Ctrl+Alt+C
Edit Resolved Name
Apply as Filter
Prepare a Filter
Conversation Filter
Colorize Conversation
SCTP
Follow
Copy
Protocol Preferences
Decode As...
Show Packet in New Window
TCP Stream Ctrl+Alt+Shift+T
UDP Stream Ctrl+Alt+Shift+U
TLS Stream Ctrl+Alt+Shift+S
HTTP Stream Ctrl+Alt+Shift+H
swayam

```
No.  Time       Source        Destination   Protocol  Length  Info
  74 3.735443   10.5.23.209   172.16.2.30   HTTP                      /1.1
  75 3.735515   10.5.23.209   172.16.2.30   HTTP                      /1.1
  78 3.882694   172.16.2.30   10.5.23.209   HTTP                      hed
  79 3.882694   172.16.2.30   10.5.23.209   HTTP                      hed
  80 3.883011   10.5.23.209   172.16.2.30   TLSv1.3
  81 3.883191   10.5.23.209   172.16.2.30   TLSv1.3
  84 3.912464   172.16.2.30   10.5.23.209   TLSv1.3
  87 3.913056   172.16.2.30   10.5.23.209   TLSv1.3
  88 3.913076   172.16.2.30   10.5.23.209   TLSv1.3
  91 3.914039   172.16.2.30   10.5.23.209   TLSv1.3
  92 3.916758   10.5.23.209   172.16.2.30   TLSv1.3                   Data
  94 3.917597   10.5.23.209   172.16.2.30   TLSv1.3                   Data
  96 3.917731   10.5.23.209   172.16.2.30   TLSv1.3
  97 3.917838   10.5.23.209   172.16.2.30   TLSv1.3
```

```
> Frame 74: 279 bytes on wire (2232 bits), 279 bytes captured
> Ethernet II, Src: Dell_d7:2b:77 (f8:b1:56:d7:2b:77), Dst: C
> Internet Protocol Version 4, Src: 10.5.23.209, Dst: 172.16.
> Transmission Control Protocol, Src Port: 56481, Dst Port: 8
> Hypertext Transfer Protocol
```

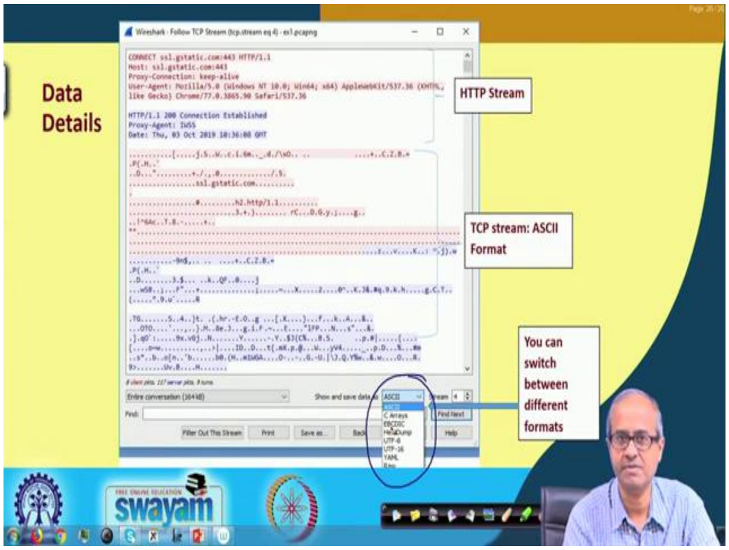
```
0000  40 55 39 c9 88 ff f8 b1  56 d7 2b 77 08 00 45 00   @U9·
0010  01 09 66 10 40 00 80 06  00 00 0a 05 17 d1 ac 10   ··f·
0020  02 1e dc a1 1f 90 a7 bb  eb e3 35 ca 54 4f 50 18
0030  01 00 d0 ff 00 00 43 4f  4e 4e 45 43 54 20 73 73
0040  6c 2e 67 73 74 61 74 69  63 2e 63 6f 6d 3a 34 34   l.gstati c.com:44
0050  33 20 48 54 54 50 2f 31  2e 31 0d 0a 48 6f 73 74   3 HTTP/1 .1··Host
0060  3a 20 73 73 6c 2e 67 73  74 61 74 69 63 2e 63 6f   : ssl.gs tatic.co
0070  6d 3a 34 34 33 0d 0a 50  72 6f 78 79 2d 43 6f 6e   m:443··P roxy-Con
0080  6e 65 63 74 69 6f 6e 3a  20 6b 65 65 70 2d 61 6c   nection:  keep-al
0090  69 76 65 0d 0a 55 73 65  72 2d 41 67 65 6e 74 3a   ive··Use r-Agent:
00a0  20 4d 6f 7a 69 6c 6c 61  2f 35 2e 30 20 28 57 69    Mozilla /5.0 (Wi
```

Hypertext Transfer Protocol (http), 225 bytes

Packets: 505 · Displayed: 146 (28.9%)

Then if you select on packet and then click on follow and then you select one of these streams let us say, HTTP or TCP stream, then you can see the corresponding detail of the packets. That suppose I want to look at HTTP streams only, then I will be seeing only the HTTP packets which are going; you see this HTTP, then transport layer security TLS; TLS is a security which is built on top of this HTTP runs along with that. So, all this packets you can see here.

(Refer Slide Time: 35:19)



Data Details

Wireshark · Follow TCP Stream (tcp.stream eq 4) · ex1.pcapng

```
CONNECT ssl.gstatic.com:443 HTTP/1.1
Host: ssl.gstatic.com:443
Proxy-Connection: keep-alive
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML,
like Gecko) Chrome/77.0.3865.90 Safari/537.36

HTTP/1.1 200 Connection Established
Proxy-Agent: IWSS
Date: Thu, 03 Oct 2019 10:36:08 GMT
```

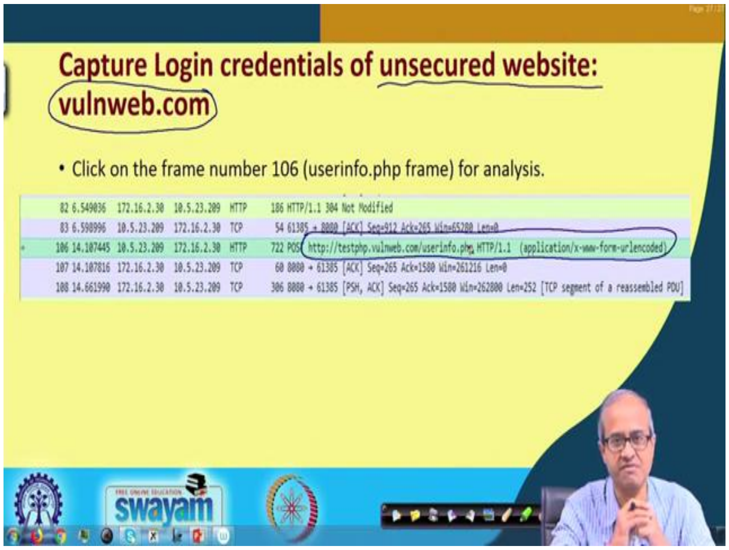
Entire conversation (164 kB)

Show and save data as: ASCII

Stream: 4

Now, if you click on this, one of them, some details you can see; you can see, means one particular packet which carries response from the server. So, you can see what text message you are send; these are something which in binary, which cannot be displayed in ASCII, HTP stream and you can switch between various display modes. So, here you can see in the bottom, there is a menu option here; by default we have selected ASCII, the thing is displayed in ASCII; but you can specify some other formats also, raw format or any other format; it will display in that that format.

(Refer Slide Time: 36:11)



Capture Login credentials of unsecured website: vulnweb.com

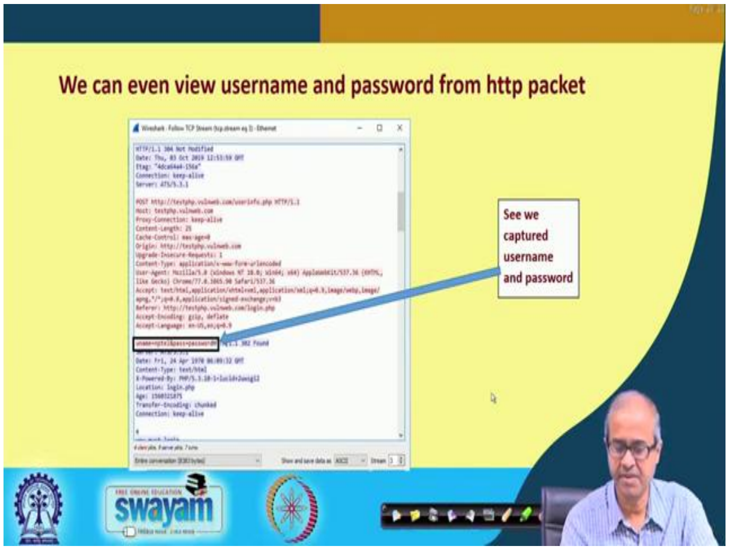
- Click on the frame number 106 (userinfo.php frame) for analysis.

```
 82 6.549036  172.16.2.30  10.5.23.209  HTTP   186 HTTP/1.1 304 Not Modified
 83 6.598996  10.5.23.209  172.16.2.30  TCP     54 61385 → 8080 [ACK] Seq=912 Ack=265 Win=65280 Len=0
106 14.107445 10.5.23.209  172.16.2.30  HTTP   722 POST http://testphp.vulnweb.com/userinfo.php HTTP/1.1  (application/x-www-form-urlencoded)
107 14.107816 172.16.2.30  10.5.23.209  TCP     60 8080 → 61385 [ACK] Seq=265 Ack=1580 Win=261216 Len=0
108 14.661990 172.16.2.30  10.5.23.209  TCP    306 8080 → 61385 [PSH, ACK] Seq=265 Ack=1580 Win=262800 Len=252 [TCP segment of a reassembled PDU]
```

Let us look at some other examples; you see there are some unsecured websites; well if you go to this vulnerable web dot com, **vulnweb.com**, you will see lot of information about these. So, here we are actually showing one such packet capturing with one of the web, with one of the means, IP addresses which are obtained from that website; that is supposed to be a vulnerable website ok.

So, we captured some of the packets while the website was opened and we select some of the, you see, some of the packets when the user authentication was carried out on that website; username, password was given ok.

(Refer Slide Time: 37:13)



We can even view username and password from http packet

Wireshark · Follow TCP Stream (tcp.stream eq 1) · Ethernet

```
HTTP/1.1 304 Not Modified
Date: Thu, 03 Oct 2019 12:53:59 GMT
Etag: "4dca64a4-156a"
Connection: keep-alive
Server: ATS/5.3.1

POST http://testphp.vulnweb.com/userinfo.php HTTP/1.1
Host: testphp.vulnweb.com
Proxy-Connection: keep-alive
Content-Length: 25
Cache-Control: max-age=0
Origin: http://testphp.vulnweb.com
Upgrade-Insecure-Requests: 1
Content-Type: application/x-www-form-urlencoded
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML,
like Gecko) Chrome/77.0.3865.90 Safari/537.36
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,image/
apng,*/*;q=0.8,application/signed-exchange;v=b3
Referer: http://testphp.vulnweb.com/login.php
Accept-Encoding: gzip, deflate
Accept-Language: en-US,en;q=0.9

uname=nptel&pass=passwordHTTP/1.1 302 Found
Date: Fri, 24 Apr 1970 06:09:32 GMT
Content-Type: text/html
X-Powered-By: PHP/5.3.10-1~lucid+2uwsgi2
Location: login.php
Age: 1568121875
Transfer-Encoding: chunked
Connection: keep-alive

0
```

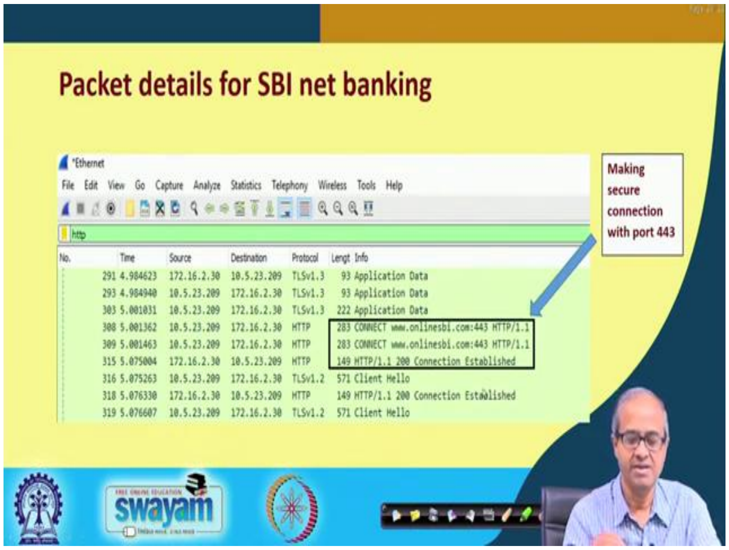
4 client pkts, 4 server pkts, 7 turns

Entire conversation (8383 bytes) · Show and save data as ASCII · Stream 1

See we captured username and password

So, what we find is that the detail of the packet looks like this, where you see that the username and password are available in clear text; they are not encrypted; that is why that site has been marked as vulnerable. Username is nptel; pass is password. So, user name, password can be captured by this kind of a simple packet capturing, if there is no encryption going on right.

(Refer Slide Time: 37:40)



Packet details for SBI net banking

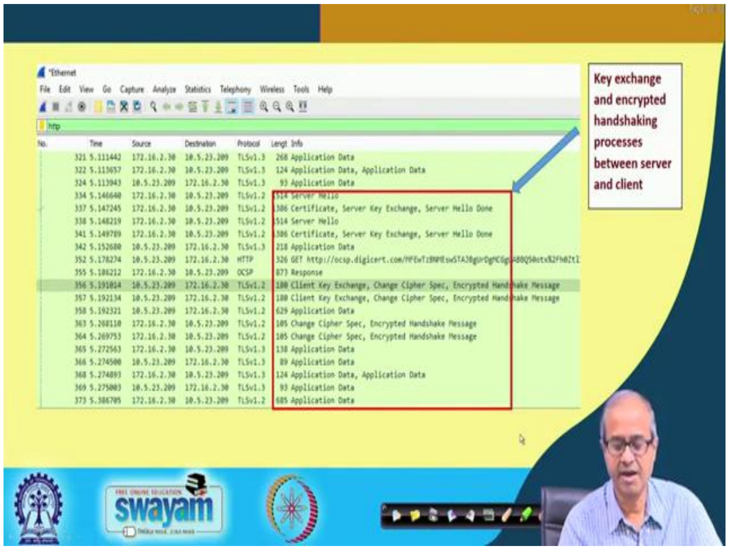
*Ethernet
File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help
http

```
No.      Time      Source        Destination   Protocol  Lengt Info
    291 4.984623  172.16.2.30   10.5.23.209   TLSv1.3    93 Application Data
    293 4.984940  10.5.23.209   172.16.2.30   TLSv1.3    93 Application Data
    303 5.001031  10.5.23.209   172.16.2.30   TLSv1.3   222 Application Data
    308 5.001362  10.5.23.209   172.16.2.30   HTTP      283 CONNECT www.onlinesbi.com:443 HTTP/1.1
    309 5.001463  10.5.23.209   172.16.2.30   HTTP      283 CONNECT www.onlinesbi.com:443 HTTP/1.1
    315 5.075004  172.16.2.30   10.5.23.209   HTTP      149 HTTP/1.1 200 Connection Established
    316 5.075263  10.5.23.209   172.16.2.30   TLSv1.2   571 Client Hello
    318 5.076330  172.16.2.30   10.5.23.209   HTTP      149 HTTP/1.1 200 Connection Established
    319 5.076607  10.5.23.209   172.16.2.30   TLSv1.2   571 Client Hello
```

Making secure connection with port 443

Similarly, another example I take; when you do SBI net banking, it is supposed to be a secure site. So, you see that when you doing the SBI net banking, we are in parallel doing a packet capture. If you see the packets, you will see that HTTP connect requests are going on, on port number 443 which is a secure connection, secure HTTP. So, everything will go on encrypted. So, this information verifies that fact; that we are establishing connection over port number 443 which is a secure layer connection.

(Refer Slide Time: 38:23)



*Ethernet
File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help
http

```
No.      Time      Source        Destination   Protocol  Lengt Info
    321 5.111442  172.16.2.30   10.5.23.209   TLSv1.3   268 Application Data
    322 5.113657  172.16.2.30   10.5.23.209   TLSv1.3   124 Application Data, Application Data
    324 5.113943  10.5.23.209   172.16.2.30   TLSv1.3    93 Application Data
    334 5.146640  172.16.2.30   10.5.23.209   TLSv1.2  1514 Server Hello
    337 5.147245  172.16.2.30   10.5.23.209   TLSv1.2  1306 Certificate, Server Key Exchange, Server Hello Done
    338 5.148219  172.16.2.30   10.5.23.209   TLSv1.2  1514 Server Hello
    341 5.149789  172.16.2.30   10.5.23.209   TLSv1.2  1306 Certificate, Server Key Exchange, Server Hello Done
    342 5.152680  10.5.23.209   172.16.2.30   TLSv1.3   218 Application Data
    352 5.178274  10.5.23.209   172.16.2.30   HTTP      326 GET http://ocsp.digicert.com/MFEwTzBNMEswSTAJBgUrDgMCGgUABBQS0otx%2Fh0Ztl
    355 5.186212  172.16.2.30   10.5.23.209   OCSP      873 Response
    356 5.191014  10.5.23.209   172.16.2.30   TLSv1.2   180 Client Key Exchange, Change Cipher Spec, Encrypted Handshake Message
    357 5.192134  10.5.23.209   172.16.2.30   TLSv1.2   180 Client Key Exchange, Change Cipher Spec, Encrypted Handshake Message
    358 5.192321  10.5.23.209   172.16.2.30   TLSv1.2   629 Application Data
    363 5.268110  172.16.2.30   10.5.23.209   TLSv1.2   105 Change Cipher Spec, Encrypted Handshake Message
    364 5.269753  172.16.2.30   10.5.23.209   TLSv1.2   105 Change Cipher Spec, Encrypted Handshake Message
    365 5.272563  172.16.2.30   10.5.23.209   TLSv1.3   138 Application Data
    366 5.274500  10.5.23.209   172.16.2.30   TLSv1.3    89 Application Data
    368 5.274893  172.16.2.30   10.5.23.209   TLSv1.3   124 Application Data, Application Data
    369 5.275003  10.5.23.209   172.16.2.30   TLSv1.3    93 Application Data
    373 5.306705  172.16.2.30   10.5.23.209   TLSv1.2   605 Application Data
```

Key exchange and encrypted handshaking processes between server and client

And means, when means, during the secure connection the transport layer security, TLS protocol starts running and you see there are lot of packet exchanges going on through TLS which exchanges the key, decides on the protocols and so on and so forth, which cryptographic protocol, encryption/decryption to use and so on ok. So, all these details you can see.

So, actually I have shown you just a few examples. There can be so many other examples; you can create a scenario; you can capture packets and try and analyze. So, this is the best way to learn what is going on in a network; create a scenario, capture the packets and analyze the packets and understand exactly what is going on; this is the best way to learn.

So, in this lecture we have very quickly gone through a short tutorial on the Wireshark tool and we argue to actually create this kind of scenarios, run Wireshark or any other kind of packet sniffer; capture the packets and try to analyze them. Only then you will be able to understand the process of networking; what actually goes on when some applications are run.

Thank you.