Information security - IV

Prof. M J Shankar Raman
Department of Computer Science and Engineering
Indian Institute of Technology, Madras

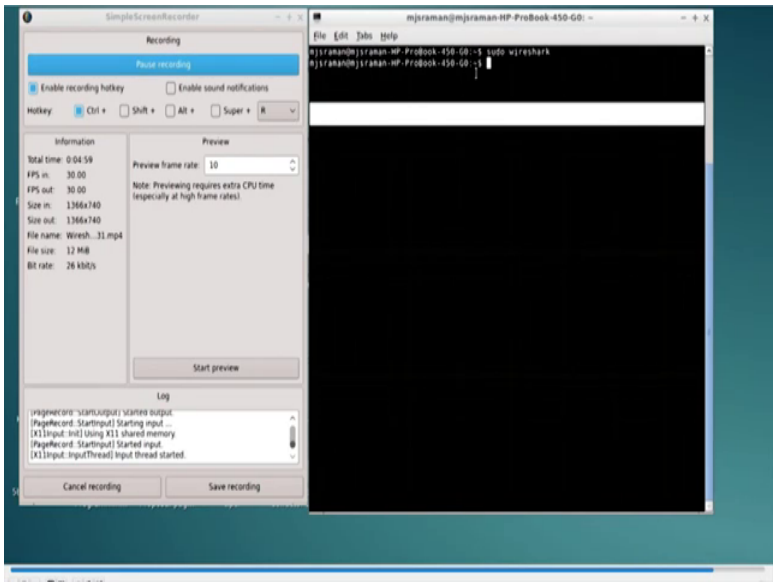
Lecture – 38
Wireshark Introduction

Welcome to this session on network security and forensics. Until now we have been talking about how to collect evidence. We saw that we might have to attach ourselves physically to the network, to collect evidence and if the evidences collected live; it is active evidence. If the evidences collected and stored or you take it from some storage medium, it is passive we can call it as a static or a passive kind of evidence.

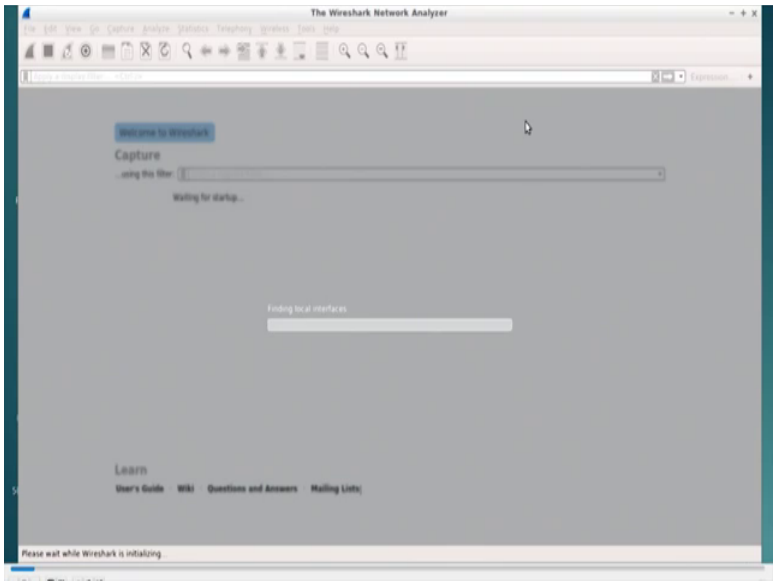
Essentially we will look at one tool which is wireshark, which can be used to collect data packets, and if you remember the process what we have tried to do was that, we want to collect whatever is the data packet that is flowing in the network to which we are connected and then start gathering evidences. So this was one of our aims in this network forensics course.

So, what we will do now is, we will take a look at wireshark which is used for capturing the packets. This will a sort of hands on, so we are going to only give an introduction for about 15 to 20 minutes about this wireshark tool, so you need to work much more on various problems of how to collect data, how to collect series of data, how to identify the flows using wireshark. There are also other tools that such as tshark, but we will be mostly concentrating on wireshark because it is slightly easier to explain wireshark since it consist of a nice graphical user interface. This wireshark tool is actually found in Kali Linux which probably you are very familiar with and which you have been using. So, you need not separately install this and if you have Kali Linux you can start using wireshark. You can invoke wireshark by doing the following operation, you can do a pseudo command and then invoke wireshark.

(Refer Slide Time: 02:22)

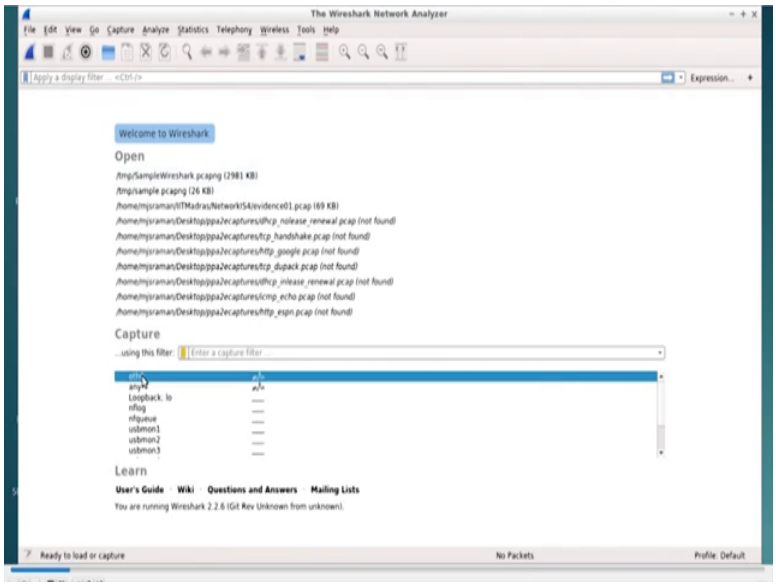


(Refer Slide Time: 02:23)



So, this is in Ubuntu systems for other systems find you have to become a super user you become a super user and try to invoke wireshark. Otherwise what you can do is, you can get necessary permissions to access the Ethernet interface and then use wireshark. So once you invoke wireshark you get a nice GUI something like this.

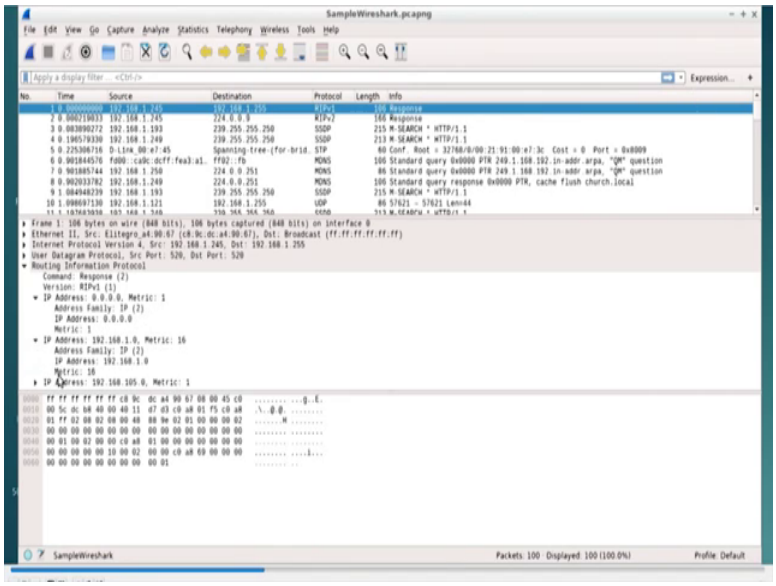
(Refer Slide Time: 02:41)



So, if you look at this it says that error during loading and it says do file has been disabled due to wireshark running as super user ok. You can just ignore it for the time being; if you want to find out what this is this messages is just go to the web and check. Now our idea here is to capture the evidence so we are not bother about all these messages. So, what we will go do is, we will once we will just press and then once we go here; you see this is the main screen of wireshark and it might vary depending on what version of wireshark you use, but in general wireshark you will have these kind of screens, where you can just open the previously captured packet or you can capture the packets live ok.

So, in this case for example, we are using wireshark 2 dot 2 dot 6 probably you could get some other version of wireshark which is in your Kali Linux. Now the idea is we want to capture the data from Ethernet interface ok. So in at least in this case; if you have a wireless interface you could that wireless interface will also be shown here. So the idea is that we will go ahead and capture data; so what I do what we will do is, we will just go ahead and then double click on this eth 0 to capture the data. So here we are double clicked it. And once you are double clicked it you see that wireshark has started to capture the data packets.

(Refer Slide Time: 04:01)



Now if you look at this, the wireshark actually I mean it divides I mean one of the things that you should be careful is that whether I will get all these three partitions of the screens etcetera it depends on what is the configuration you are going to do for wireshark, we will look into it shortly.

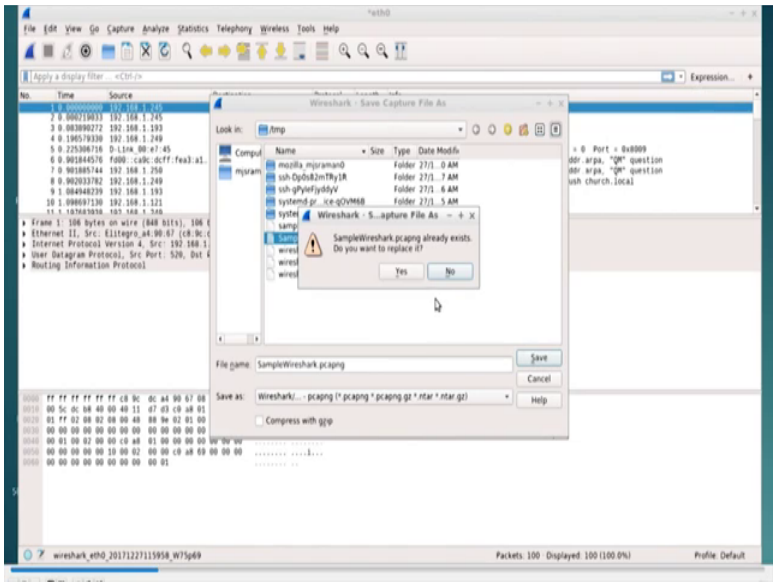
But then in general; once you open wireshark, it will have three partitions the first partitions shows the packets, the second partition shows each of the packets and the third partition shows the values in hex. So if you look at this part, you see that its displays the number of packets that are collected; so and the number of packets that are displayed. So if you look at this since its live, you see that the packets are increasing will collect about 100 packets and then stop. So we can go ahead and stop wireshark after collecting about 100 packets.

So, now we have stopped wireshark and once we have stopped capturing ok; so this gives you if you look at this, we have different so it starts the packet numbers are sequence something like this, that is the sequence number 1, 2, 3, 4 5, 6, 7, 8, 9, 10 etcetera. This is the packets, the independent packets that are flowing and get captured by wireshark. The second one is its shows the time; time stats in the current time.

So, these 0th pack I mean the first packet is cart at the 0th time, I mean this can be changed so we will see how this can be changed; then it talks about the source address, the destination address, the protocol, what is the kind of protocol that it has captured,

then its finds out the length of the packet and then what is the info that it can decipher. See many a time we might have to do this hard work of inferring what is there inside the packet, but to some extent this wireshark provides you some basic information about the packets that it tries to interpret ok.

(Refer Slide Time: 06:13)



Now moving on, so if you look at this you have various options you can open files you can save as file so what we are going to do right now is, we just have to whatever packets that we have captured, we have captured about 100 packets. We will just store it in the slash tmp directory ok. So just I mean this just a experiment purposes.

So, this is how you actually acquire the data. So what we are doing right now is, there are various formats you can even zip it etcetera, but we will for the time being we will just capture it in p cap n g format. So I am just over writing a file, if you want I can create a new file or you can over write file. So in this case for example, I am over writing sample wireshark p cap n g So, I am just replacing that file and the data gets saved. So, what I can do right now is that, I can actually having saved the data, I can now remember we have told you that we should always work on a copy of the data and not on the real data, that is why we are actually storing the data.

So, then this is these are all the packets that this guy captured. So as I told there is time field, source filed, destination protocol, length and info etcetera ok. The protocols so one of the things that you should be aware is that as network forensic expert, we should be

aware of many of the protocols that are there in internet. We will tell you I mean where this information of the protocols can be found. One of the advantages of using wireshark is that, you can actually if for example, the protocol is not a standard protocol; that is proposed by intent engineering task force and it is a proprietary protocol. If you get information about this proprietary protocol, you can actually writes scripts in a language called lu a; Lua and then you can actually integrated with wireshark.

So, many a time you might have to do this, because while doing forensic you might have to do lot of scripting and that is one of the reasons in the previous course we thought about one scripting language, which is the shell scripts. You might have to writes code in python or ruby or I mean the Lua programming language anything I mean you might have to be familiar with at least one of these programming languages. So that you can write your own protocol interpreter and integrated with wireshark ok. We will see how these things are done, but not in detail, but we will be doing some case studies and we will we shows how this things are done ok.

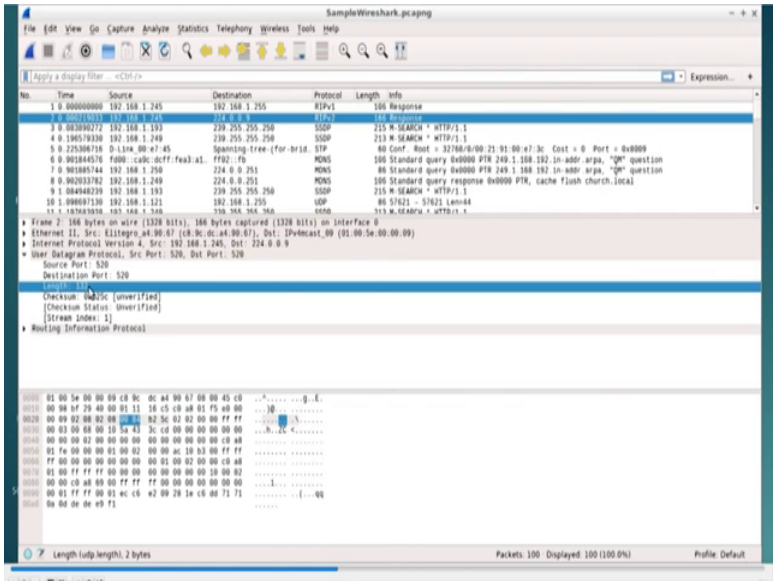
Now, what is tells you that, you should be aware of the almost all the protocols that are there in the internet and which is quite impossible. So you should have the ability to understand the protocol and then try to write scripts, whereby the protocols can be interpreted ok; that is more important.

So, in this case for example, we can see a RIP version 1 protocol and RIP version 2 protocol and as I told you this the second window here, the second partition here actually shows what is being carried by this packet. So if you look at this it has a Ethernet frame, and it has a so it has a internet protocol version 4. So IP is being used and if you see this is the broadcast address for the subnet. So there is the router that is broadcasting its routes and it uses the use UDP and it uses the routing information protocol. One of the things that you should note in this is that if for example, I just open this routing information protocol; now I can go on expanding this routing information protocol. So if you look one of the ways to find out how this correlates with the RIP protocol is that if you go to the corresponding RFC which that the current RFC numbers usually changes as they make updates to protocols.

So, you can just go to IETF website and then check what is the current RFC for this. Now in that they would have given a packet format for RIP. So, this so RIP requires and

then there is a response and things like that; so this is RIP version 1 and then it tells you what are all the IP addresses that it is carrying essentially the routing table that it is carrying or the routes that are reachable. So you will gets this kind of format and wireshark helps you identify read this things in a much better way by interpreting it with the standard diagrams that is given in the RFC s ok.

(Refer Slide Time: 10:57)



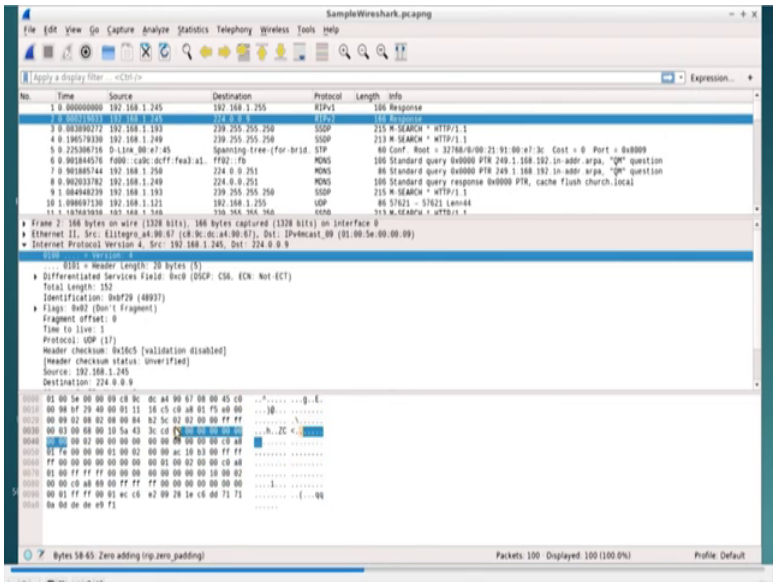
So here we are talking about the route matrix and if you click on one of this route matrix for example, that will actually go ahead and for example, I mean if you look at this we are looking at the RIP v 2 packet now; the RIP v 2 packet has more information than the RIP v 1 packet essentially I mean it has more information and what we do is now if you just click on one of the one of the what should I say the fields ok.

For example we are clicking on source port field 520. Now once you click on this field look at this here ok. So there is a blue color that is so he tells you that this hex value corresponds to this source port field. So either you can click on the values here, then the values will be highlighted or if click on the values here the values will be highlighted.

So, this tells you that in the packet, this field corresponds to the source port. Similarly I can identify other stuff for example, the destination port is also identified 0208 and then if you look at this I mean remember this is in hex, so 84 is 16 into 8 plus 4 that is so 132 so that is 128 plus 4 that is 132. So these are all hex numbers whereas, this guys clearly for easy readability it is printing it in decimal format. Of course, hex numbers are printed

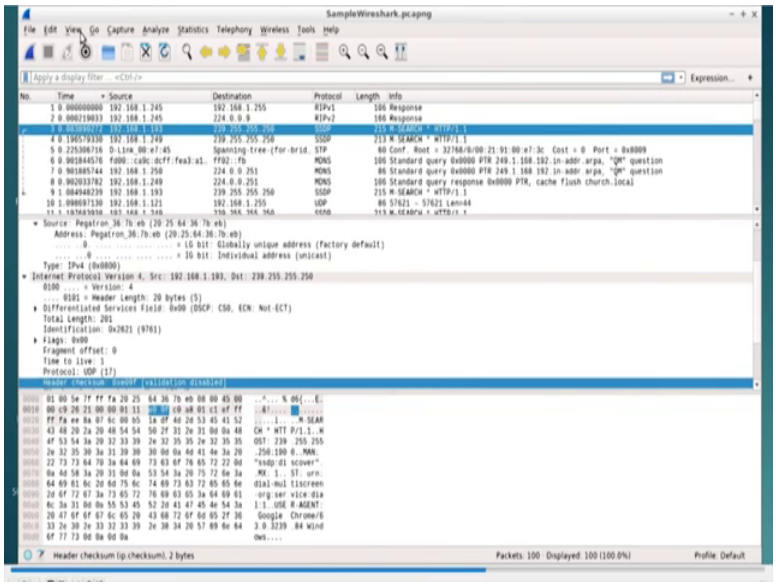
as 0 x, so if you look at this the checksum is this and the checksum it says is unverified which is so similarly you can identify for internet protocol internet protocol we are using IPv 4 and looking at the IP address, we can say IPv 4 this is an IPv 6 packets ok.

(Refer Slide Time: 12:29)



So, we can identify what type of protocol that we have captured. So it also tells you that there is a spanning tree, so there is dealing link switches actually getting a spanning tree protocol STP trying to identify the spanning tree in order to avoid cycles etcetera. So, in this way you will be able to interpret many of the fields, but for this you might have to have your RFC next to you to understand what this field means and all those specific details ok. Now why are these specific details needed because you might have to present a report and in the report you might have to underline what are these fields and why this fields correlate as evidence ok.

(Refer Slide Time: 13:24)



So, similarly I mean like what we have done this can be done for each of the protocol that it carries. So in this case for example, if we I mean if we can identify we can just press our button on some particular hex value then we will able to see what that value is for example, 11 is actually 17 so it tells you that the IP is carrying a UDP protocol on top of it.

So, in this way we will be identify we will be able to each packet can be analyzed. Now let us try to see how this analysis can be done for example, let us say that I want to track what are all the data packets that are emanating from one machine particular machine. So in this case I can actually do a sorting based on the machine id. So if you look at this what I have done right now is I have just click on the source tab and its source according to the IP addresses. So in this way I will be able to capture what are all the data packets that are gone from a particulars source machine. Now similarly I can do it so if you look this here you see that 192 dot 168 dot 1 dot 245 has communicated with 192 and sent a broadcaster request and it is also sent request to a RIPv 2 request to 224 dot 0 dot 0 dot 9 and so on.

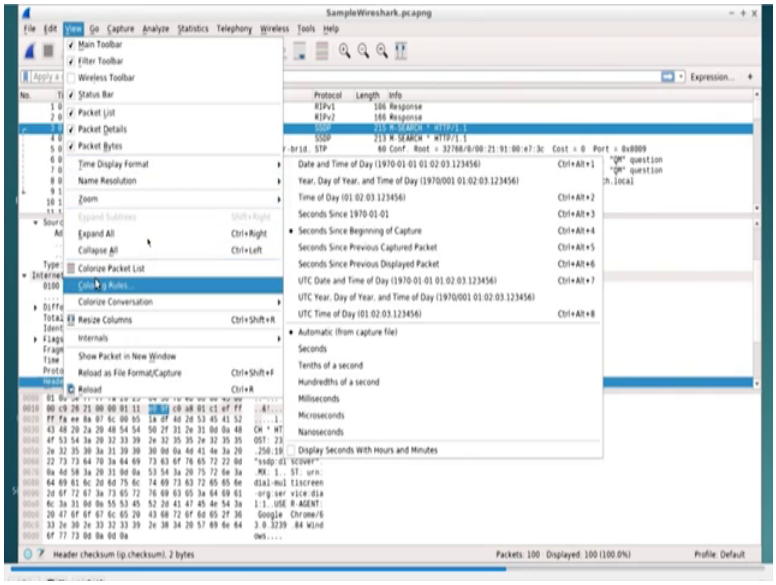
So, in this way I will be so 249 is talked with so many other routers ok; now remember all these data can actually be presented in the form of graph and then we can later go on find out the connectivity of the network; who are all the people that I have try to contact and all those things. So this actually spans I mean this goes into something known as

network discovery part. So, each data that is available here can be used for very many purposes, but we just wanted to present you that what is the kind of information that wireshark provides you.

Now, so you can sort according to the source address or you can sort according to the destination address or the protocol. So if you look at this we have this many types of SNMP protocols; so it SNMP protocol there is 0 dot 10 has generated lot of traps so and it also tells you at what time the straps are generated and so on.

So, and you can even sort according to the length of the packets; so it provides you huge amount of search opportunities sorting opportunities etcetera I mean the idea is that by see if you just put the data in a different format you may come to a as different conclusion ok. So this so because of this distance provides you all the facilities that are needed ok.

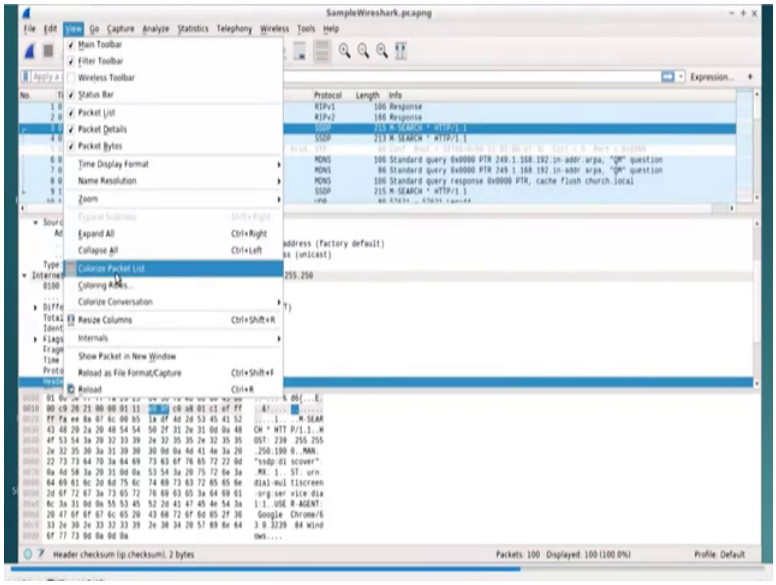
(Refer Slide Time: 16:10)



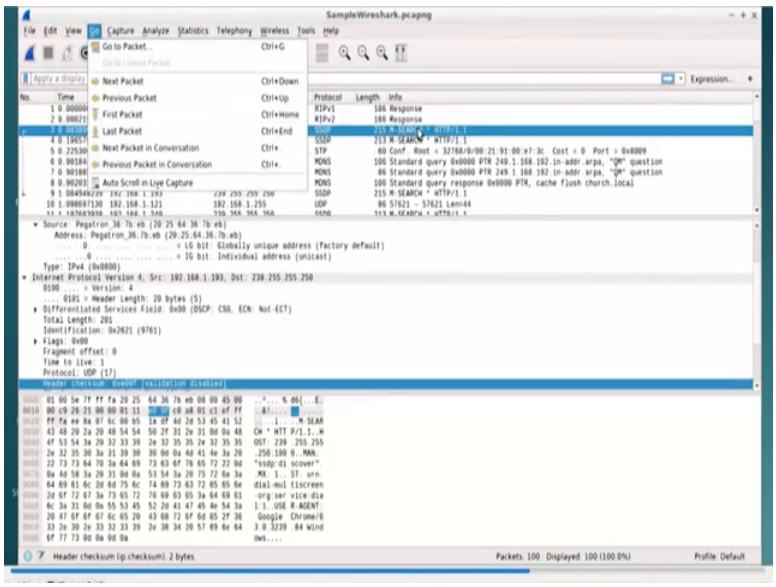
Now, what are the other things that this tools; so if you got each one of the tab that is given so if you look at this you see that there is a packet list, there is a packet details and packet bytes; now this correspond to packet list, this corresponds to packet details and this corresponds to packet bytes. So, in this way so you can enable or disable whatever you want so and if you look at the time field I set the field started with 0, but actually what you can do is if you go to this time display format then give this gives u lot of ways see what we have done a second since beginning of capture that is what we have done.

So, what you can do is we can even do with time of the day date and time of the day etcetera. So this provides you lot of facilities you can even do 10s of a sectioned 100s of a second and milliseconds and etcetera ok. So if you look at I mean please go through all these tabs and then try to find out you can see for easy readability this also you can also color the packets; so if you look at this we have just pressed on this tab to color the packets and you can also remove the coloring by clicking on it ok. So, now the colors have been improved.

(Refer Slide Time: 17:20)

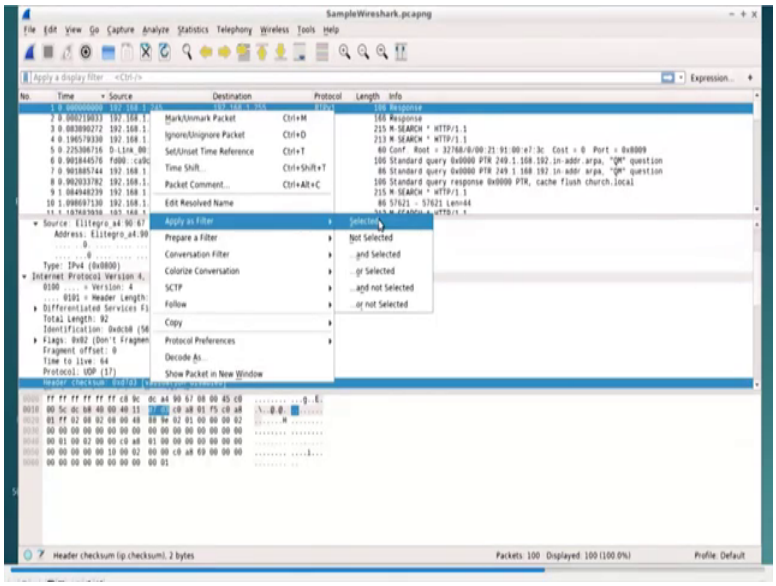


(Refer Slide Time: 17:25)



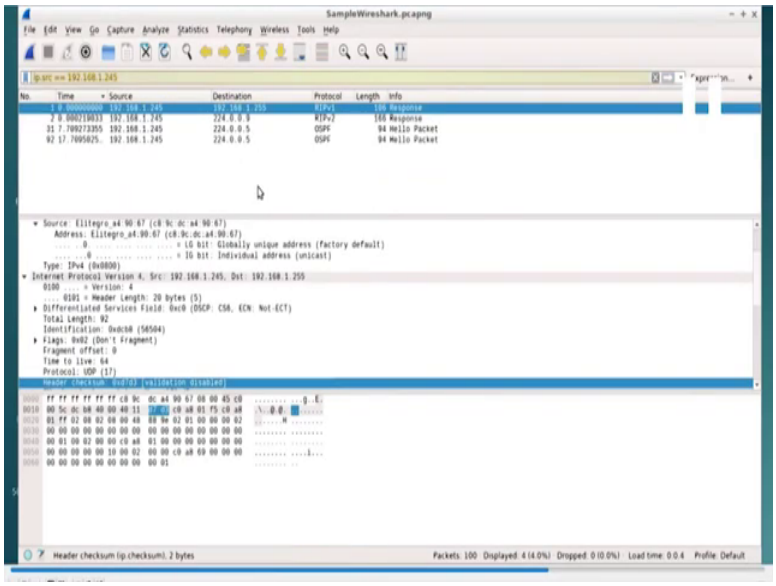
So now, you can also travels from one packet to another packet using the go tab or we can also do a filters ok; this is very important because this wireshark dumps lot of packets and we do not need all the packets I mean what if I am going to analyze who is a person who is talking to another person why do you need RIP packet? So in order to do this what we can do is we can apply filters ok. This filter just tells you that only those packets that satisfy the filter condition or displayed the rest of the packets are not shown.

(Refer Slide Time: 17:31)



So, there are many ways to apply filter; one is you can go and type in this apply a display filter column ok, or you what you can do is you can on a selected packet you can just apply a filter, and in which case you see this it just tells you all the routing protocols like RIPv 1 and RIPv 2.

(Refer Slide Time: 18:10)

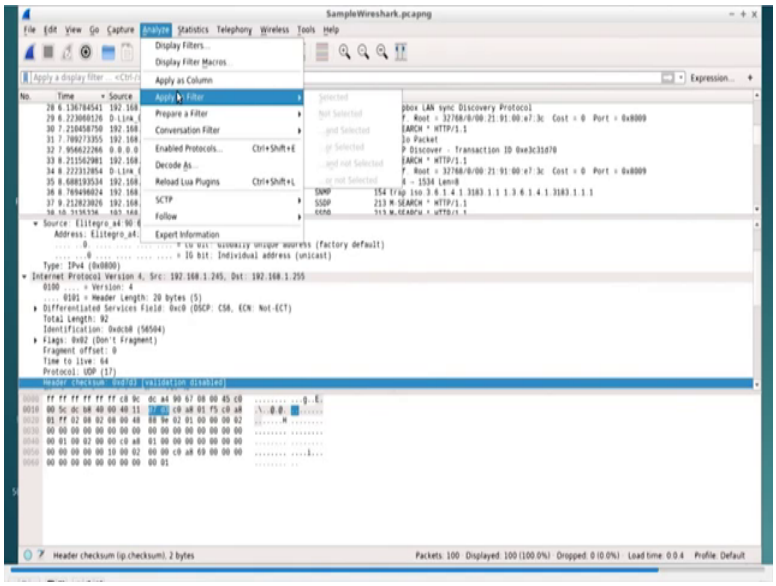


So, what we are saying in these cases if whatever is if the IP source address is 192 dot 168 dot 1 dot 245 just display those packets.

So, essentially we can know that this guy is a router and this is router trying to I mean people who are configured the router; now look at the information that we can get we can find out that the people have configurate both RIPv 1 and RIPv 2. I do not know for why they also done OSPF ok. So this tells you that this guy configured for OSPF and for example, if none of the other routers are there in OSP are used other using OSPF, you can actually disable this protocol otherwise this hello packets just occupy bandwidth. .

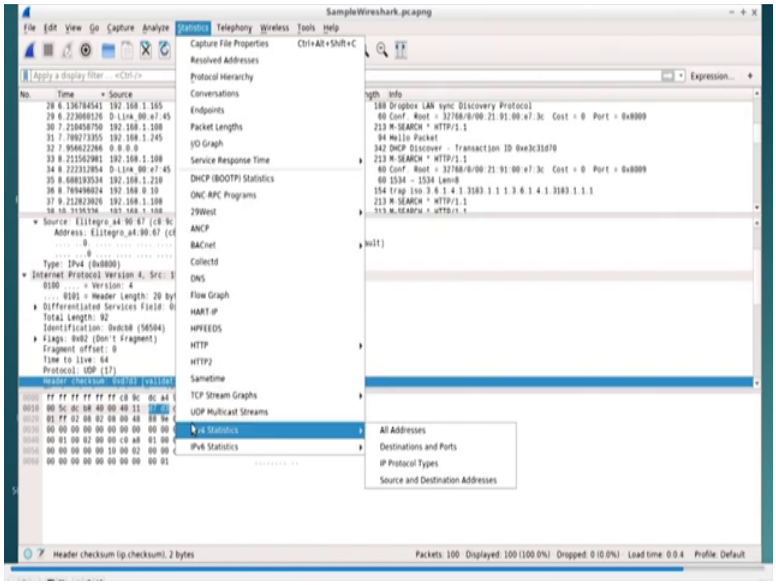
So, even some kind of performance optimization can if information can be obtained by using wireshark ok. This is very important tool that the network administrators used and it also used very largely by forensic experts and if you want to clear of just press that cross button. So it clears off and then it again stats is playing almost all the packets. So, this is one of the ways by which you can actually capture the packets that are flowing in the network.

(Refer Slide Time: 19:34)



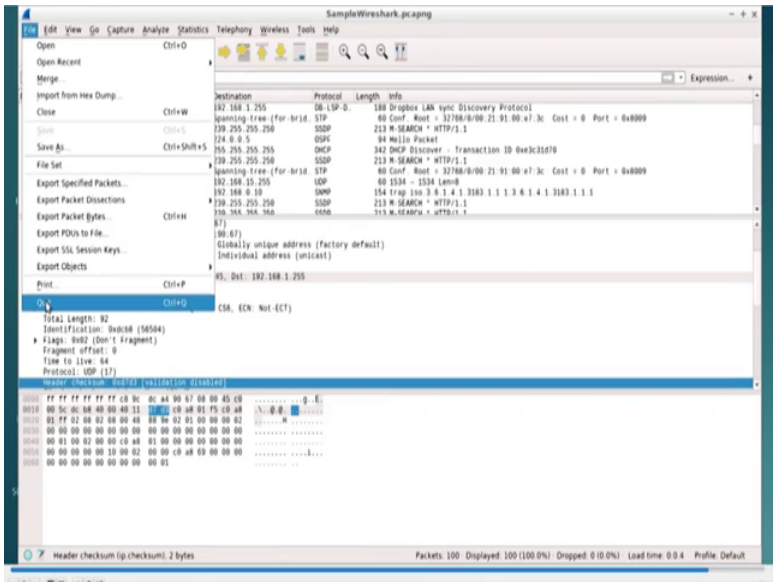
The next one, we can look at is so you can capture, you can do analysis, you can get some kind of statistics. And if you look at what is happening is that you can also look at for example telephony for telephony, what are all the certain kinds of protocols ok. So for telephony protocols you can actually specifically do the capture those particular packets ok.

(Refer Slide Time: 19:57)



You can do lot of statistics for example, I can find out the IPv 4 statistics for all address, then for telephony, then wireless, then you can have some ACL rules etcetera access control list etcetera.

(Refer Slide Time: 20:11)



As I told you one of the things and after that you can go ahead and quit it. Now if you remember we had actually stored the packet now we showed only the lives. Now we can go and store the packet and then we know we knew that, we are storing the packet as p cap and if you double click on that, so you are able to retrieve all those packets whatever you have stored in the previous sessions. So this gives you a very good interface for capturing packets.

Thank you very much.