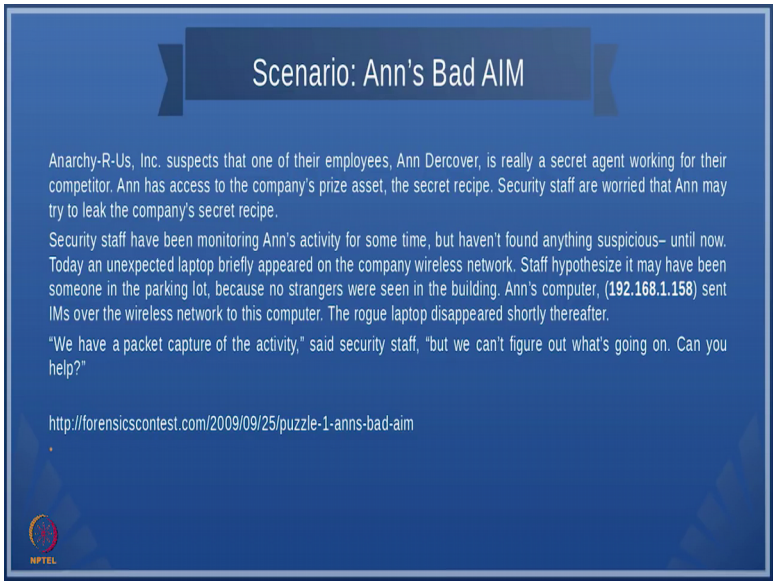
Information security - IV
Prof. M J Shankar Raman
Department of Computer Science and Engineering
Indian Institute of Technology, Madras

Lecture - 41
Case study : Ann's Bad AIM Part I

Welcome to this session on Network Security and Forensics. In the past few modules we had seen how to capture packets, and what are all the types of analysis that one can do after capturing the packets. What you are going to do right now is to look at a case study and see how forensics can be approached after we capture the data packets.

Now there are many ways to solve the problem. So, what we will do is that we are not going to look into details of all the ways, but overall let us tell how some cases are investigated. Now there is actually a very good website which is called Forensic contest dot com, I suggest that you participate in many of the forensic contest that these people are providing. If possible actually take the cases that are already existing and see how people are solve the problems.

(Refer Slide Time: 01:27)



Now we will take one such problem and then we will analyze what has happened using the evidence file that is being given in that website. Now, of course these problems are just toy problems, the real analysis will involve much more aspects but then for this

course we will essentially look at how the problems are approached. Ok after that finally, it depends on your intelligence and your skill on how to solve the problems.

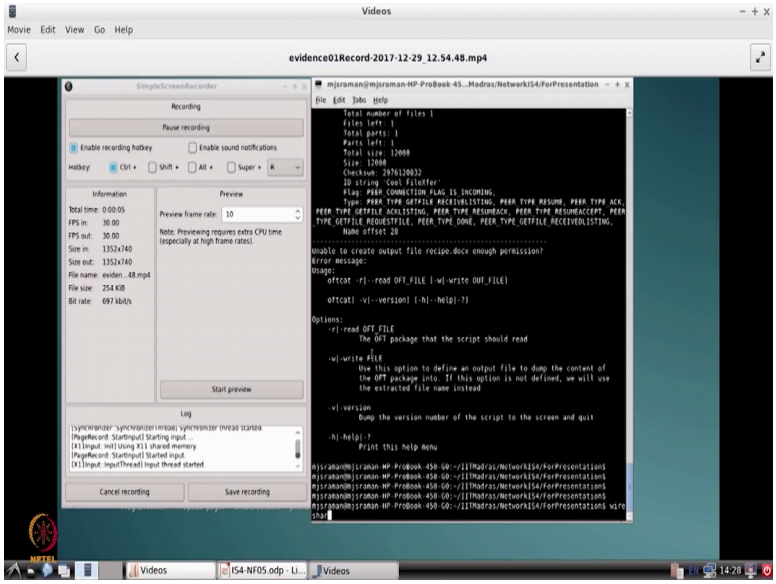
Now we will be discussing two ways to solve the problem one is using Wireshark, the other is given in that website, puzzle website where they are developed tools to understand protocols and then extract information based on the tools. You have to install some of those tools because in the demo that we are going to show we have already install those tools, so it should straight away work. But in general sometimes these tools may not be available. So, you might out install them separately that itself is a separate task, but then I would suggest that you go ahead and practice installing the tools also ok.

So, let us come to the case study. There is a company which suspects that one of his employees is a secret agent working for the competitor. And this company does some food items ok. So, there is a secret recipe that the company is worried might have exchanged hands. So, what has happened is some security staff have actually found out that there could be some suspicious activity and the particular employ could have sent the data out to it is competitor.

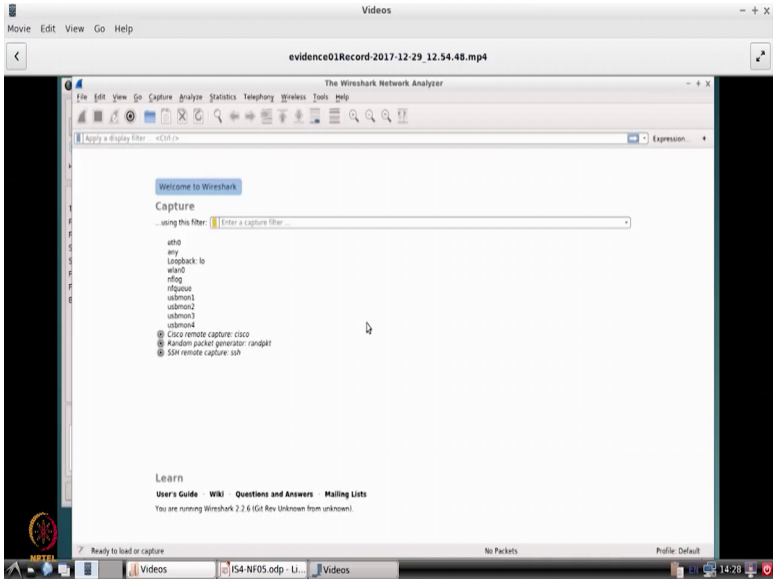
So, what they do is they just have captured the data that has traversed over a medium probably a wireless network and they know the IP address of the computer, in which this person has worked ok. So, there are question is we have a packet capture of the activity, but we cannot figure out what is going on, so can you help. So, this is a puzzle and you can see similar kinds of puzzles in this website. So, this is one of the puzzles, but there are about 7 or 8 puzzles they have given and there are more than one solution or more than one approach for solving the problem.

So, you would suggest that you go through this whole website and see how people have solved the problems. So, how do we solve this problem ok? So, let us workout by some ways. So the first information that we have is the machines IP address, and the second information that we are given is the p cap packet capture ok. And using these too let us see how this problem is solved.

(Refer Slide Time: 04:35)

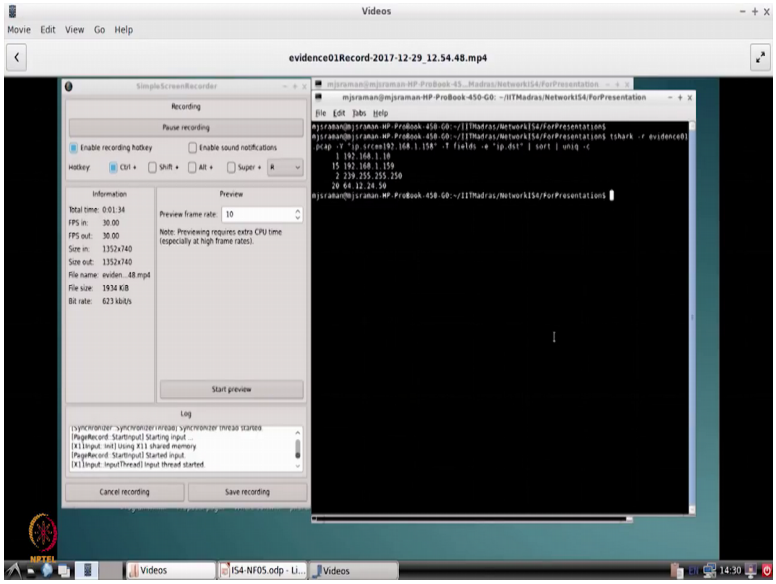


(Refer Slide Time: 04:37)



So, therefore, what we do is we just invoke wireshark and then we actually find out the evidence file ok. So, this evidence file is actually given in the website, so you could download this evidence file and then you can use wireshark and open this evidence file after you are downloaded it ok, I think we discussed it in one of the previous sessions and how to do it. So, please go at file and then open it and once you open you get these screens.

(Refer Slide Time: 05:23)



Now the first thing that we can do is that we have got the IP address of the employee or the suspected employee. So one of the things that we can do is that so as I told you can use either wireshark or T shark to find out what has going on ok. So, here is an example ok. So, we are using t shark what we are trying to do is that we are trying to find out the data that has gone from the source address 192 168 dot 1 dot 58 ok, 158 ok.

So, then what we are trying to see is we are trying to identify to which are all the destinations to which this person has connected ok. So it will just tell you that to which destination this person has connected and how many packets to that particular destination. And if you will remember in information security three course, we had talked about this command call sort, and this command called unique and minus is the count.

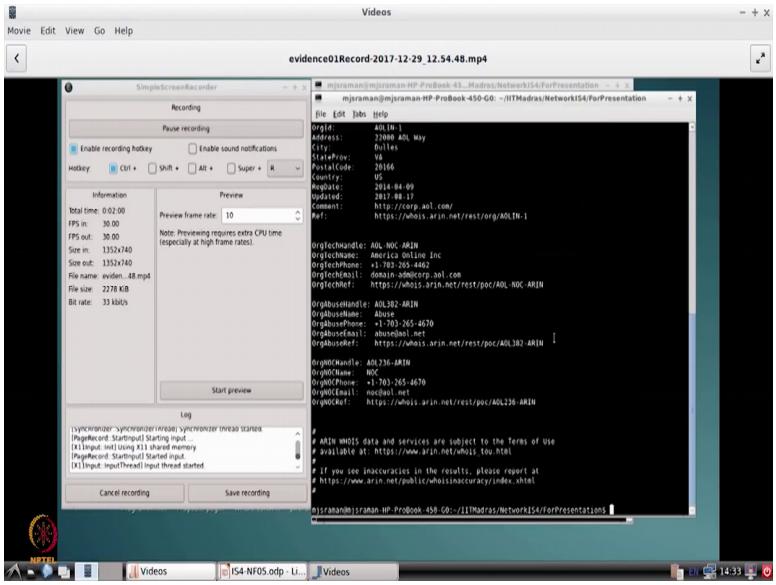
So, what did does use that, you would have lot of data that has come out of 192 dot 168 1 dot 158, but then what we do is we try to filter out what is the unique places to which this communication has taken place. And you see that with 192 168 dot 1 dot 10 there is only one packet that had gone through, but what is of interest is 192 168 dot 1 dot 159 and 64 dot 12 dot 24 dot 50.

What are the things that you can see is that the highest information has our data exchanges happened between 64 dot 12 dot 24 dot 50 and they the user 182 dot 168 dot 1 dot 158. Now one of the things we can try to do is you see that it is actually seems to be

an external IP address ok. Because the local IP address was somewhere around 192 168 and something like that and above 220, above this I mean this the second was some multi cast address.

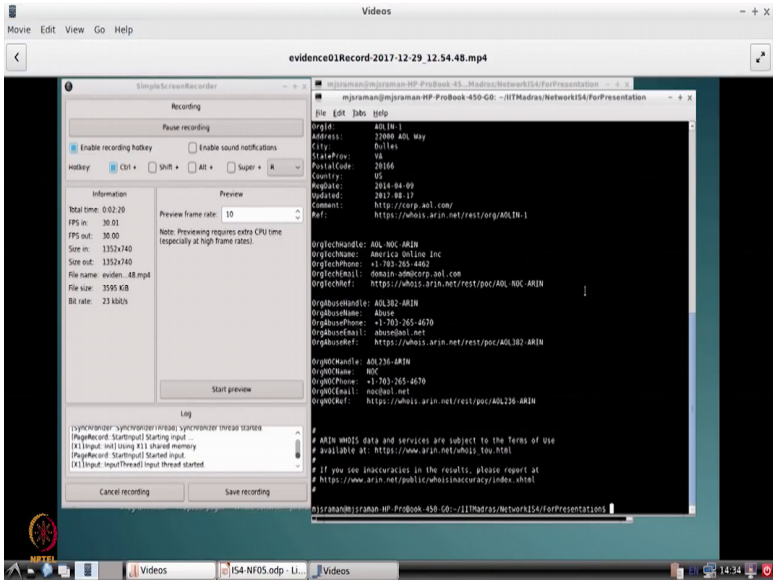
So, therefore, what we can look at is that fine, there seems to be one suspicious activity for which there is lot of data that has gone through ok. So, what we do right now is we try to identify who this 64 dot 12 dot 24 dot 50 is. So, there are many tools we can use to find out who is this external IP address. So, for example, in this case we know that it is 64 dot 12 dot 24 dot 50. And what we can do is that we can actually use ns lookup, or we can use a command called hooeys. So, let us take a look at the usage of the command hooeys and then with hooeys we are going to type 64 dot 12 dot 24 dot 50.

(Refer Slide Time: 07:30)



Now, you see that it tries to tell you who is the person or the institution which has this address ok. And we are able to see that this belong this belongs to AOL that is America online. So, one thing is now clear this person has tried to contact an external location, and done some activity; so that is what we can understand from these two tools ok.

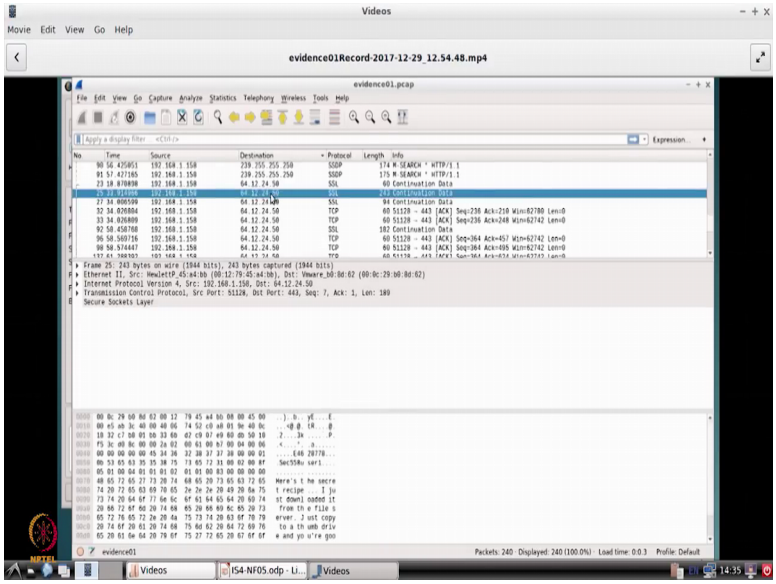
(Refer Slide Time: 09:03)



So, if you remember the first time that we did was we actually use this t shark and then identify whatever the packets and second we found out that there are one suspicious IP address that was not that of the institute or the current company. Therefore, we looked at what that IP address is, and it seems to be an American online ok.

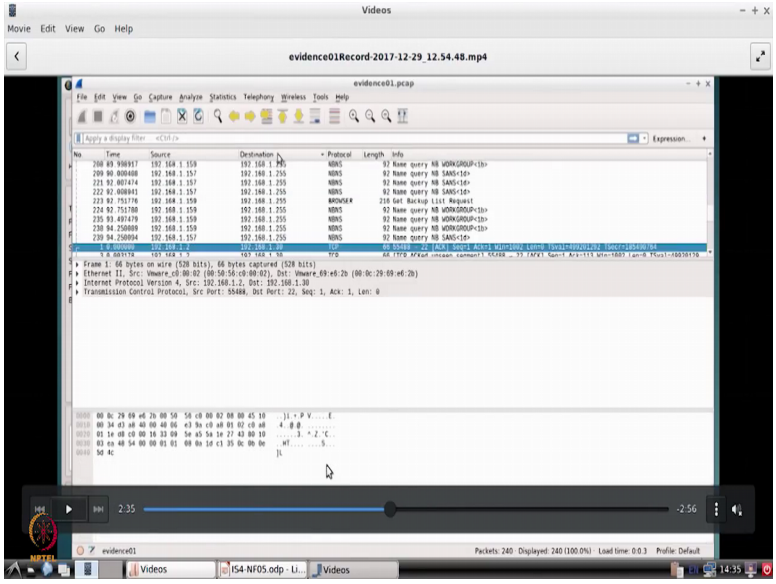
Now we will come back to wireshark and what we can do is you could actually sort according to destination or sort according to source I think we have seen all those things. So, what we will do is we will go ahead and use wireshark and then try to see some of the suspicious packets that are got transferred between these two people ok. So, we will sort according to destination, and then we will see that will try to find out where this particular destination is so which was the 64 dot 12 dot 24 dot 50 address.

(Refer Slide Time: 10:07)



And then once we go into this it is it is we when we seem to be very lucky here. So, what has happened is that if you look at packet number 25 and then you just press this ok and there is something interesting that has come here. So, if you look at this.

(Refer Slide Time: 10:27)



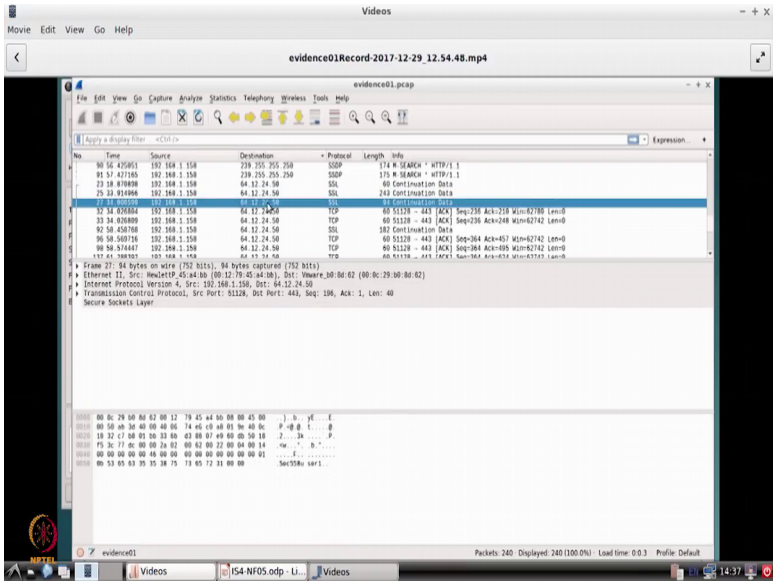
So, it tells you that there is some data that has there ok. So, if you look at this so what we are seeing is that we are able to see if you if you actually take the packets from 192 168 1 dot 158 to 64 12 24 50. And especially if you are able to track this SSL data you are able to see something very fishy ok. So, you see that there is a string parses here is the secret

recipe, I just downloaded it from the files; file server just copy to a thumb drive and you are good to go ok.

So, if you look at this just by now we do not have any idea of who has send this, but we just know that this machine; from machine 192 168 1 dot 158 and 64 12 24 50 ok, the data has gone ok, but one of the things you should know is I could always argue that I did not send the secret data ok. So, I was just having chat and this is something else.

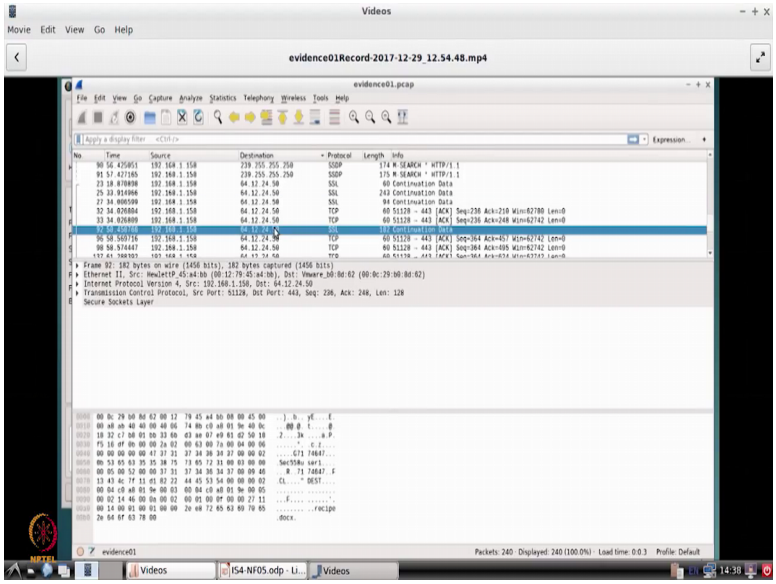
So, in order to give a full proof solution what you are supposed to do is you are suppose to analyze, establish what protocols these people have used, establish the chat session, and then establish whether a file transfer has happened and establish whether the other personal acknowledge. So, all these activities have to be done in case of forensics. Of course, we will not look at all these activities we will just give you a brief of how these activities are done. So, in this case for example, what I can do is I can always that looking at SSL and then continuation data.

(Refer Slide Time: 12:13)



So, let me now go ahead and do this I have look at SSL and continues data and there is something that that occurs again and again and again which is SCC 55 8 U SCR 1 ok. So, if you look at the continuation data I just go on look at the continuation data even here you have this SCC 55 8 U SCR 1 ok, even here you are able to see this ok. Of course, there are other junk information, we will look at what are the information we want. So, we are going packet by packet ok.

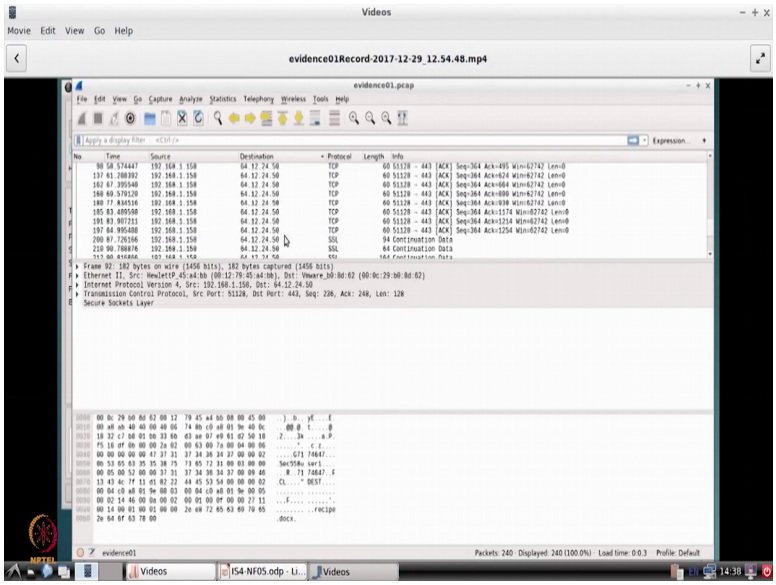
(Refer Slide Time: 12:47)



So, and this is very interesting. So, it tells you that there is SCC 55 558 U S C R 1 and then there is something called as recipe dot doc. So, if you look at the last line you see that there is a recipe called doc x that has come in between the conversation. We still do not know whether it was from the other side or this side.

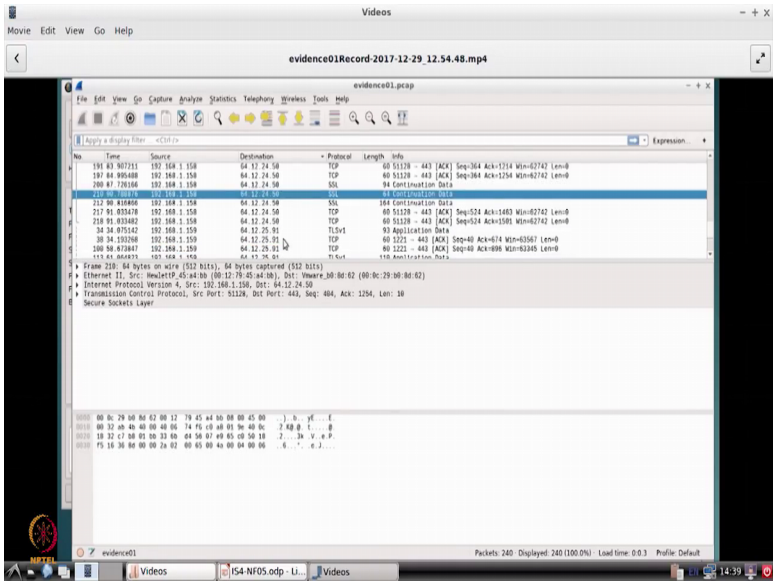
So, one or things you could guesses that it is once 192 168 1 dot 158 to 64 12 24 dot 50, that data has gone from here to there, so that is the guess correct guess that we can do right now ok. So, let us look at some more packets.

(Refer Slide Time: 13:33)



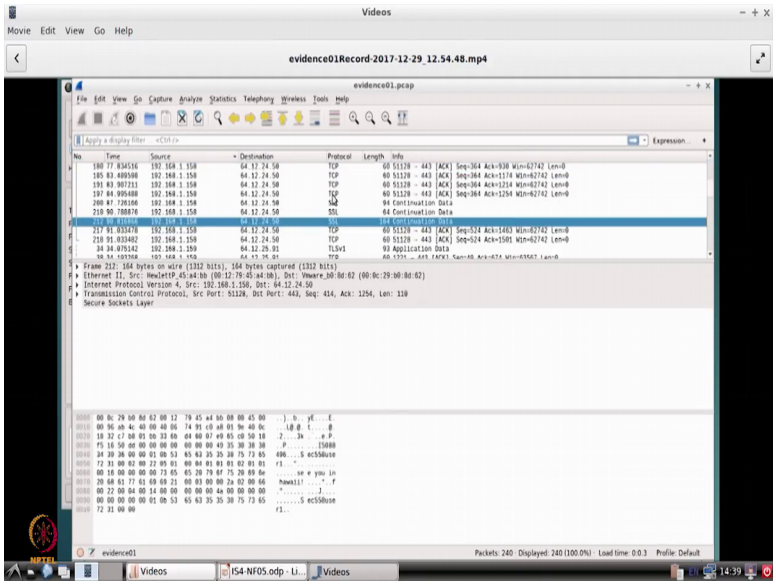
So we will just go one by one I mean we will just move around those packets. And then continuation data will see whether anything else interesting comes to us.

(Refer Slide Time: 13:37)



And here is something much more interesting. So, here it is says see you in Hawaii ok, so this is something much more one more clue that we are getting. So, one over things that we can understand from here this if you can capture this SSL based data we could be able to we could find out what is the conversation that has happened between these two people, so that is one clue that we have right now.

(Refer Slide Time: 14:13)



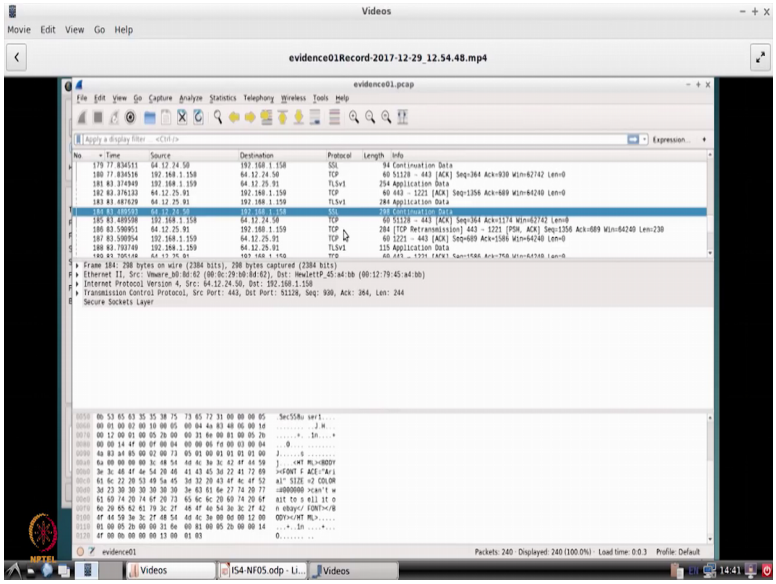
So, we look at other application data also ok. So, one of the things that you can do is see with wireshark you could also trace conversations ok, you can trace TCP conversations, you can say SSL conversations in this you can analyze the floors ok. So, you can follow the flows I think we saw examples of that in the previous session on wireshark ok.

So, one of the things that we can now frame I mean so if you look at this we can get some more anxious from whatever we have seen ok. So, one this person has said that we can see you in Hawaii and here is a something that I have sent and then there is a document that was gone. So, in this so now slowly you are putting forth what are the things that has happened ok.

And one of the things is one of the things if you look at this in one of the continuation data we can also see that cannot wait to sell it in eBay. So this is the next one that we have shown. So, slowly if you look at this we are trying to converge on what has happened. So that is the idea by doing this kind as we can do a packet analysis, we can do a flow analysis.

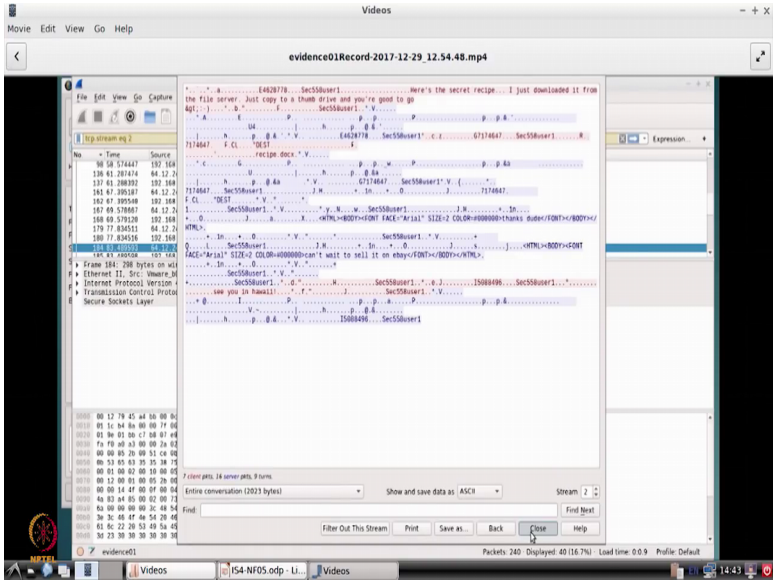
And probably if you if you had established this is the conversation that has happened you are also got to do protocol analysis. So, here what we are now and this protocol maybe a known protocol or an unknown protocol. So, if it is known protocol then there should be support in wireshark so that we can trace the conversations and get the protocol. If not probably we will have to apply I mean read the protocol, write some scripts etcetera and then go ahead and find out what has exactly happened.

(Refer Slide Time: 15:58)



So, it is a long driven process it is not going to be easy I mean even for the simple problem if you look at this solution you would have to work for more than 2 or 3 days to identify all these data together. Since it is part of a lecture we are moving quite fast on that this is thing can be done that can be done etcetera anyways. So, now let us look at how we can follow the streams.

(Refer Slide Time: 16:29)

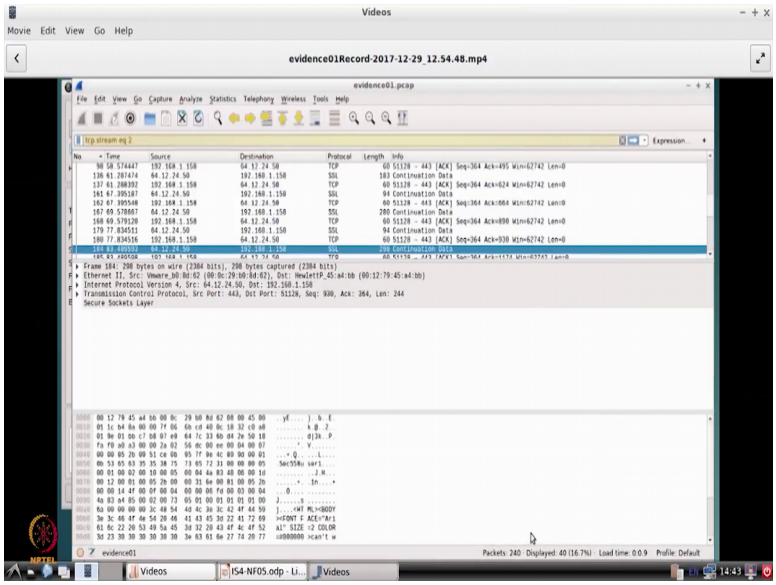


So, if you look at this one of the things that we are done is we are taken one packet SSL packet and said that we will follow the stream; that means, it will try to capture all the

related packets and here is something good that we are come across. So, here it says here is the secret recipe I just downloaded it from the file server just copy it thumb ray and your good to go ok. And then there after this there is something like a recipe dot doc x you see and then there is another thing that come.

So, if you look at this I cannot wait it to sell in it eBay and then there is a CU in Hawaii. So, and if you look at the color code you can see that the red color is something that has happened between current person in 192 168 1 dot 158 to the person. Now so if you look at this now slowly we are trying to establish that there is a conversation that has happened between these two people and this conversation actually tells you that some file has got transferred.

(Refer Slide Time: 17:39)



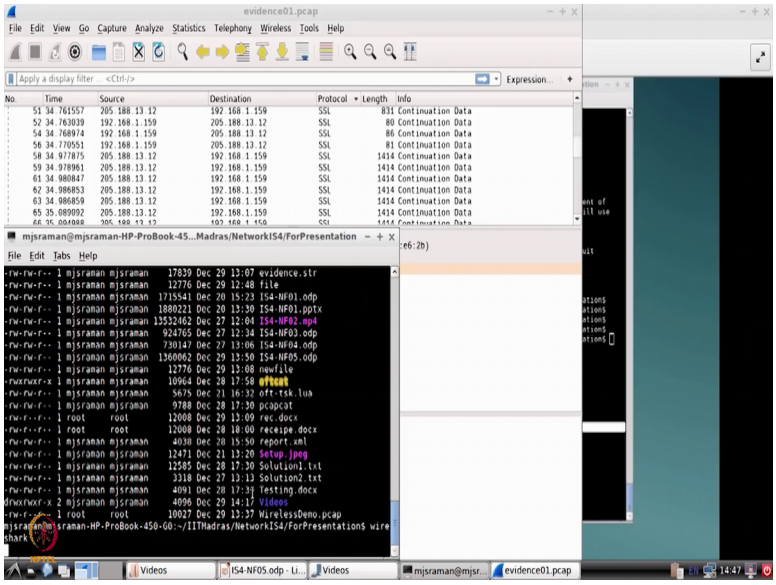
So, one or things that we could do right now is after identifying that yes some kind of conversation has happened now it is for us to establish that what is the document and what is the contents of the document. Because I could say yes I exchange the document that it was not this kind recipe. So, all these things can be done to avoid any legal hassle ok.

So therefore, what we will do is that we will see now for the time being we are just found out that we are able to identify that a conversation has happened and some document has got transferred, you know the name of the document and probably we will try to identify what type of document it is. So, every file has got a particular signature using which you

can identify what type of file it is? So, we will have to get this information from the current dump that we have ok.

So, what we could do is definitely the file would have got transferred from here to the other side ok. So, what I mean hopefully. So, what we will do is we will have to see whether such a file transfer is happened and if an in order to find out what the what is what file transfer has happened we need to identify what protocol it is using ok. Therefore, one of the suspect part is that yes have a used aim ok, AOL instant messenger for doing this conversation ok. So, how does one identify it?

(Refer Slide Time: 19:02)



So, if you look at this instead of going through wireshark also we can also look at strings command ok. So, what we can do is we can actually do a string, so one of the things that we can you see you could either go into wireshark and then try to identify what protocol they have used, or usually this OFT is protocol is used in America AOL instant messenger. Therefore, what we can do is we can actually going to the pickup file and then guess search for this OFT 2.

So, either you go through the data usually one by one or you write small shell script to identify what this protocol is. So, once I know that this OFT protocol yes then I know that yes this is a proprietary protocol and there are documentation on the web on how this protocol works. So, the other the one of the ways we can do it is now that I know

this is the protocol that is used, then I can go take the dump of the connection between the source and the destination.

So, this person would have said that here is a document. So, I would go and then type that enter press the document I mean press the enter key that document gets transmitted you find out this start point of the document you find the ends point of the document. Then what you do is you go ahead and cut this hex bytes and then dump it into a file and then open it accordingly. So, you will be able to get the information about the document ok.

So, what will do in the next session is that we will try to make use of I mean the solution next session the solution given by the person who won the first prize is very very elegant where he has written script using pearl ok, and yes actually decrypted the protocol and therefore, which just by using 5 or 6 commands is able to actually get back the file and actually print the file.

Now this process of using of going through wireshark, then cutting and then finding out the hex editor and then cutting and pasting from hex editor to a document etcetera and then changing the document and then getting it back and all those things it is a tedious process and the whole process has been automated and so that solution is very elegant will see that solution in the next module.

Thank you very much.