

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

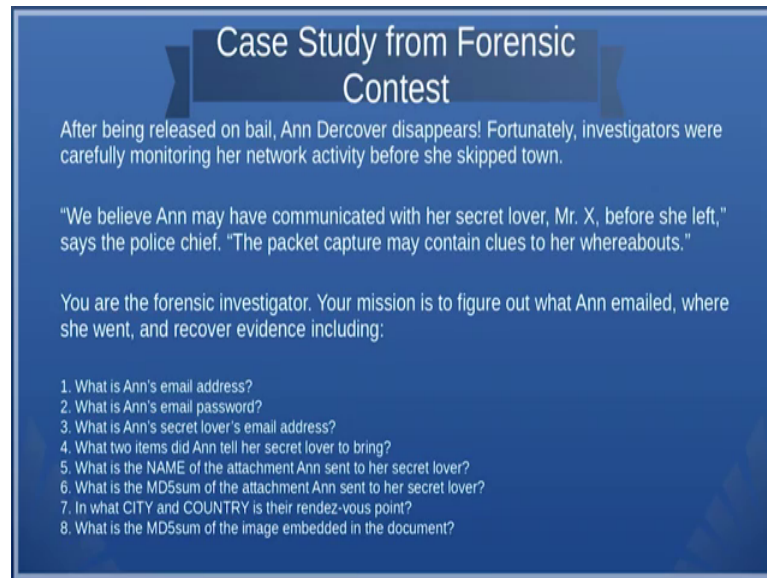
**Lecture – 46**  
**Case Study 2 - Use of Tools**

Hi, welcome to this session on network security and forensics. We had been discussing about evidence capture, we have been discussing about evidence capturing in wired networks and wireless networks. We also saw one case study of how one could go ahead and use command line in Linux to identify the attacker or to identify any suspicious activity that occurs in the network we were making use of Wireshark mostly and the related tools like TShark. What we will do now is we will now see, how it is beneficial to actually use some of the existing tools or to write scripts. So, what as a network forensic person, there are some repeated activity that we will like to do.

So, what we could do is we could write our own software using many of these tools like TShark and we could put it in a very nice framework in this session, we will just discuss about one such particular tool called Network Miner. This is actually one part of it is freely available as freely available to you, the other part; you have to buy ok, but since its freely available, we will use make use of the freely available part and then we will demo how this tool can reduce the workload of a forensic person.

So, what we are going to do is we are going to go ahead and have another case study ok.

(Refer Slide Time: 02:02)



**Case Study from Forensic Contest**

After being released on bail, Ann Dercover disappears! Fortunately, investigators were carefully monitoring her network activity before she skipped town.

"We believe Ann may have communicated with her secret lover, Mr. X, before she left," says the police chief. "The packet capture may contain clues to her whereabouts."

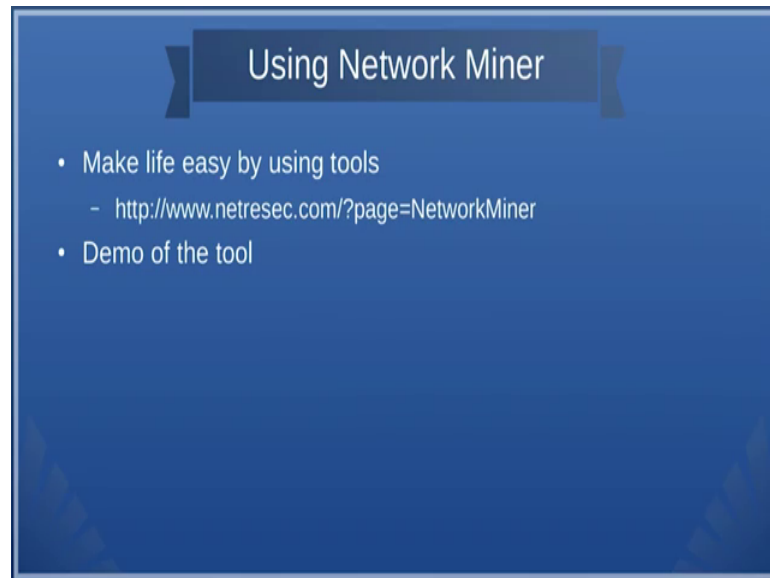
You are the forensic investigator. Your mission is to figure out what Ann emailed, where she went, and recover evidence including:

1. What is Ann's email address?
2. What is Ann's email password?
3. What is Ann's secret lover's email address?
4. What two items did Ann tell her secret lover to bring?
5. What is the NAME of the attachment Ann sent to her secret lover?
6. What is the MD5sum of the attachment Ann sent to her secret lover?
7. In what CITY and COUNTRY is their rendez-vous point?
8. What is the MD5sum of the image embedded in the document?

So, this case study goes something like this in the first case study, we saw that this person called Ann Dercover was trying to send a recipe to a particular person ok. So, the this person gets caught because we did some forensic analysis and what happens is this person is being after being released on bail, this person disappears ok, but it looks like the forensic investigators were actually monitoring our network activity before she left the town. So, what they did was they actually where were found out, they actually found out that she was communicating with her secret lover ok, before she left the town ok.

So, what we could do now is how could one use this packet capture; captured packets and identify what has happened with this person ok. So, as a forensic investigator you will be very very happy to find out what is Ann's email address which she has been using right now what is her password and what is her lover's email address and what is the what did what are the two things that this person had told her lover, etcetera. So, what we could do is and you could capture the packets and use a forensic tool and identify what has gone wrong now we could see that if you can using such kind of tools life becomes extremely easy ok, but definitely as a forensic investigator life is not easy, but well such tools can reduce your load on finding out what this happened.

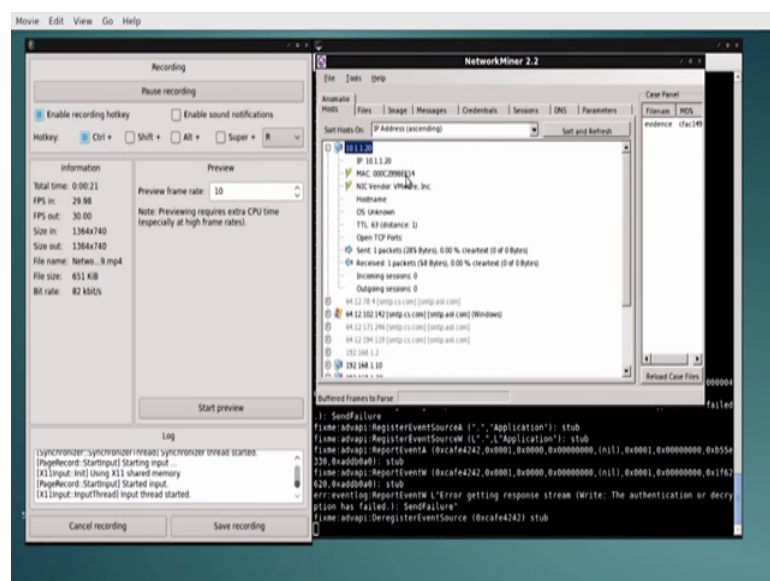
(Refer Slide Time: 03:49)



So, what we could use is we will use a tool called network miner and we will just look at a demo of a tool on how to identify, I mean or how to answer all these questions that are posed please understand that the same work can even be done with t current command line tools like TCP, dump tshark, etcetera, but then having a framework like this or having a tool like this actually helps.

So, we will now look into the demo of the tool ok.

(Refer Slide Time: 04:15)



So, here actually this tool called network miner is available in windows version you could actually use wine and then start running it in on Linux. So, in our case we have used wine to run this windows version of the tool and once you open the tool you see that it has three tabs one is known as a file the tools and the help and then it has a lot of other tabs that you can use like holes files image message credential session DNS parameter keyboard anomaly, etcetera and on the right hand side you see something known as a case panel and what we could do now is we will take the evidence file and make this network miner read the evidence file. So, I will open the file and then I read the evidence file and once I open the evidence file you see this tool actually reads the evidence file and splits the data from the evident file into the different tabs.

Say for example, the hosts tab which we are going to see right now actually use it tells you what are all the hosts that were involved in the transaction ok. So, you could see that there is a host called ten dot one dot one dot twenty and then it has sent one packet it has received another packet that is not of much interest to us then there is this sixty four dot twelve dot seventy eight dot four.

So, you if you remember you can use who is to find out who are these sixty dot twelve dot addresses and all that. So, in this case for example, it tells you that there is a windows machine and remember this tool makes use of lot of others tools that you had learnt in the previous question like nmap. So, it does a port scanning it trusts, fingerprinting, etcetera all these activities is does. So, it is not just one it you make use of tshark alone we are also using other tools that were used in when you are talking about the os security course ok.

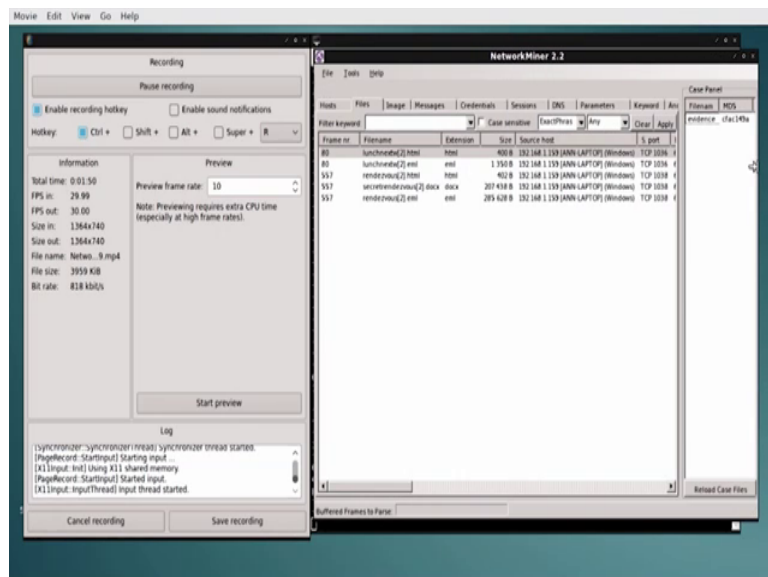
So, it use makes use of all the tools and then finally, maps the computers the it maps the oss, it maps the ports, etcetera. So, you could see that there are many machines that are involved, for example, it is able to identify a windows machine which are sent 255 packets and received 235 packets and then it has identified another public address machine. So, likewise it is identified many machines the using which communication has taken place and you could also see that different machines that send different number of packets, etcetera.

So, in this way we are able to first find out who are all the hosts that were involved in the transactions and one of the stuff that if you see that 192 168 at 1 dot 159 was Ann's

laptop. So, this is the name of the laptop, I mean she usually do device name or something. So, it just tells you that Ann was using this laptop and it has sent about 254 packets and received about 256 package and it had had a outgoing session to one of the server which is an SMTP server which essentially tells you that this person was involved in sending out some sort of an email.

So, now you are very curious about what is the email who to whom to whom she sent this email what is the content of the email etcetera and that is exactly what this software can identify.

(Refer Slide Time: 07:42)



So, let us look at what is the host and what is the SMTP. So, if you go to files ok. Now, this tells you what are all the files that were exchanged between these two people. So, there is there is something like. So, if you look there are some html files, then eml is email files and then docx files documents and then there is a secret render wood document file, etcetera.

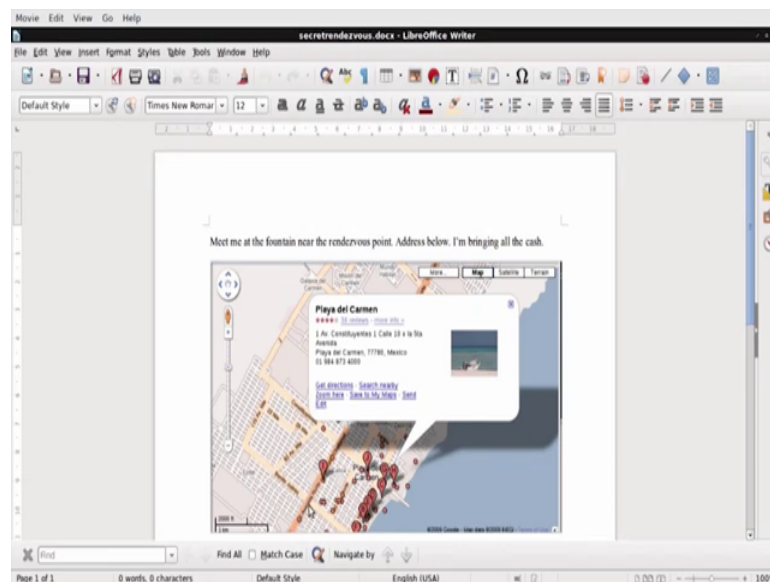
So, it also finds us now we can actually go and edit these files I mean if you remember, how we had captured this docx file in the last, it had something known as fingerprinting there was a fingerprinting kind of stuff for adder, then there is a fingerprinting for a tail and between these two the document was stuff. So, similarly you can identify the documents and this tool actually identifies it and what we can do is you can actually look into the html file ok, you just have to click the file and right click and then you can

actually open the file, let me give some time to open because the very first time its opening a browser. So, the meantime, let us adjust the screen. So, that comes out. So, so once the html file is up you will be able to view the contents of the html.

So, let us see. So, there it is the contents of the html says it sorry I cannot do lunch next week, after all heading out of town another time. So, that was one email that was sent and this is the email file ok, you can even open the email, sometimes if you have it if you do not have the corresponding program to open it, it will just say success and it does not do anything ok. Similarly, you can look at another html file called rendezvous dot html, let us open it now hopefully.

So, it says as we taught bringing fake passport on business, you would at address attached. So, you can see that there is a secret communication that was going on and they are also given some kind of address that has been given as attachment and this is actually the emails that have got exchanged we will also see the emails, but since there is not associated tool to open this it just say success and then it comes out now yes we can now find out the docx file.

(Refer Slide Time: 09:48)

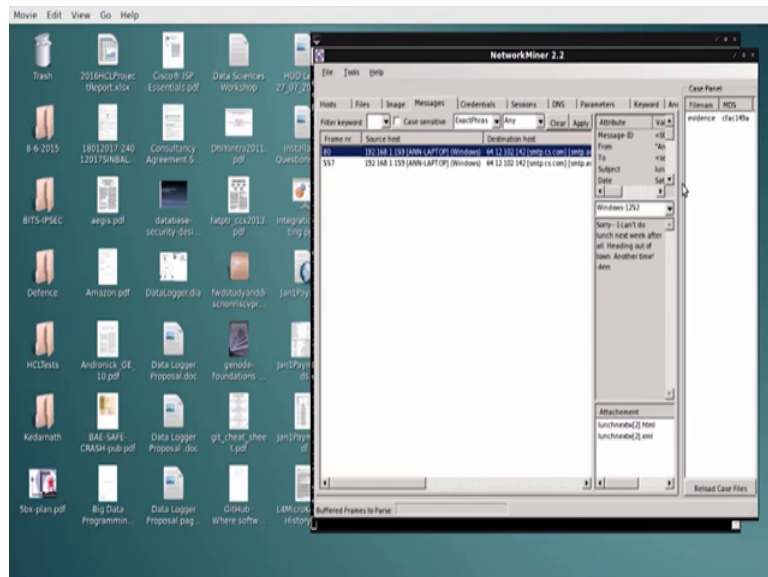


So, let us go and take out the docx file. So, here is the docx file. So, it just tells you that this person has sent a docx file along with the location where they were planning to meet. So, it just says that meet me at the fountain near the rendezvous point address below I am bringing all cash.

So, essentially what has happened is. So, this tells you that what is the email that was sent remember the email had an embedded document and then the email also had an image of the location where they are trying to meet and this tool is able to detect what are all the communication that has happened and where they are planning to meet etcetera ok. So, this is they are sent it in the form of a word document. So, you might ask I mean. So, should we not send word doc ones anymore should we send it in other format no as I told you, it is a question of having a fingerprints.

So, even pdf has got a fingerprinting mechanism. So, if you have this kind of fingerprint or signature whatever you call it signature for particular documents, then you will be able to access those documents.

(Refer Slide Time: 10:48)



So, this in this way you are able to identify what are all the communication that has happened then if there are any image files that they had exchanged ok, you could see that in the image you can also look at the messages that they had communicated. So, this is actually what it is trying to do is trying to capture the email communication that was sent between these two people. So, here is some email communication you see this that sorry I cannot do lunch next you see whatever we had seen that eml that is now getting captured here and the advantage of many with this screen is that if you look at it just lets open this ok.

So, you see what is the message to what is the subject line and all that. So, if you look at this it tells you; what is the email of Ann Dercover ok. So, it says that it is sneaky g three g thirty three at k at aol dot com. So, if you look at this then there is another email address something it tells you at what time this email was sent. So, you could actually now find out ok. So, as you say it says it is sent on Saturday, the 10th October, 2009 at 7:38. So, here it is you are actually establishing a time line you are also establishing, what is the message that has been sent you are also telling from which computer the message was sent and from where they are planning to meet and hopefully, if no one leaks out these news, you will be able to capture this person when they are departing for a particular place or you could capture them at the particular place ok.

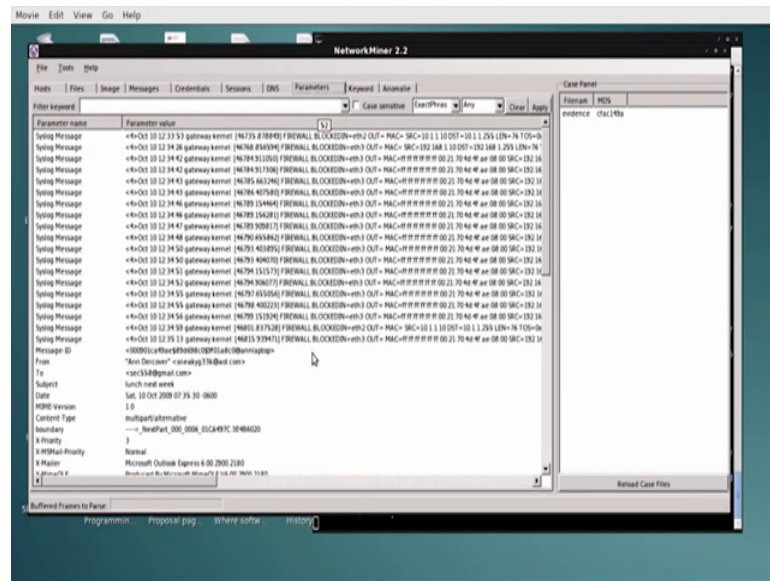
So, there are a lot of such information that is given and then it also talks about the credentials. So, the whole point about the credentials is; what is the username and the password of this person and recover ok. So, if you look at this, it is a sneaky yg thirty three k at aol dot com is the username you see on the right hand side username and then there is this password. So, you were able to see both the username and the password of this person. So, you can actually copy the username and password and actually I mean once you know the username password and cracking someone's email box is very easy ok.

So, in this way; so, it also tells you when the person had logged in ok. So, it is I mean even though it says that the valid login or things is unknown, but the end of the day you get the username the password the email when it was sent on the plan the place where they are trying to meet and I think I mean this is good enough evidence for someone to act upon ok.

So, this is the advantage of the of using such a tool ok, it is I mean we are not endorsing that you must use this, but we are just saying that such tools we are taking this as an example and we can the idea is that people are put in lot of effort. So, here is it.



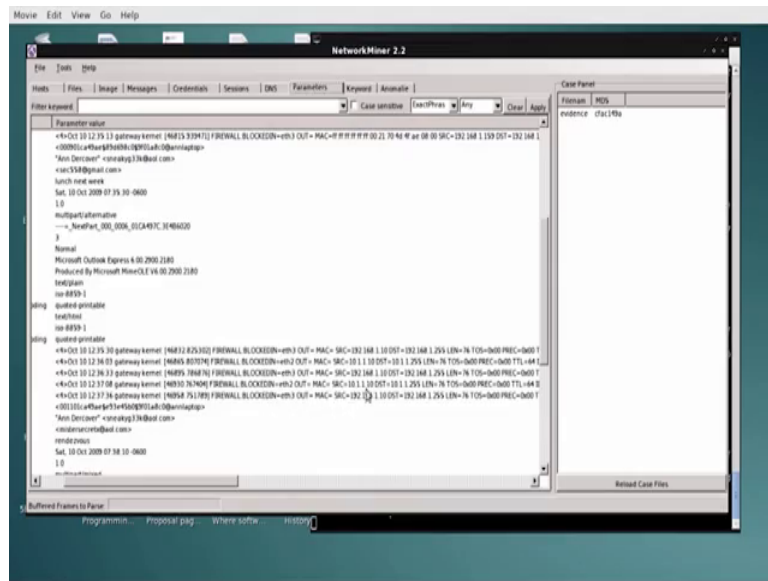
(Refer Slide Time: 13:56)



It also talks about the dns remember we were looking at what are the domains it contacted and then what is the dns server, it contacted and then you also have got to establish what is the ip address which is easily you can get easily and so, all these things can be got from this kind of a tool it also tells you the parameters now this is very interesting. So, it has captured the firewall and the syslog messages. So, you will be able to go through this I mean and derive much more information so.

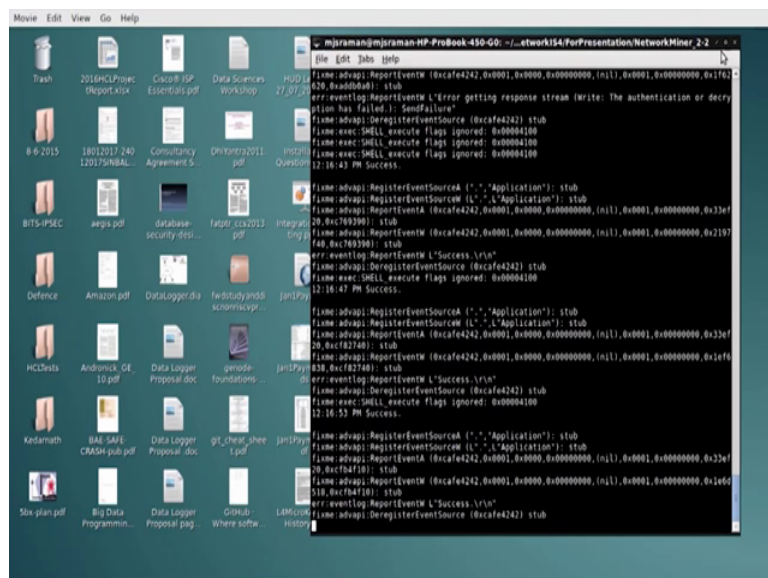
So, establishing that something has happened in a fool proof manner you could use all these information. So, it has almost all the information what does the firewall blocked and can you guess the name of the person on the other side you it was there in one of the screens ok.

(Refer Slide Time: 14:30).



So, anyway the secret x his name was there in one of the screens. So, in this way you would be able to identify what has exactly happened and how the name of the person is mr secret x at aol dot com. So, this is the other person with whom she has tried to communicate. So, using this kind of tool you are able to actually capture the data and you can actually clear and then load another file, etcetera. So, this is the way this tool works and what we have been telling you is that ok.

(Refer Slide Time: 15:06)



So, you should be able to use such kind of tools, we just showed an example of one of the tools to use such tools and then do the forensic analysis much quicker ok.

Thank you very much.