

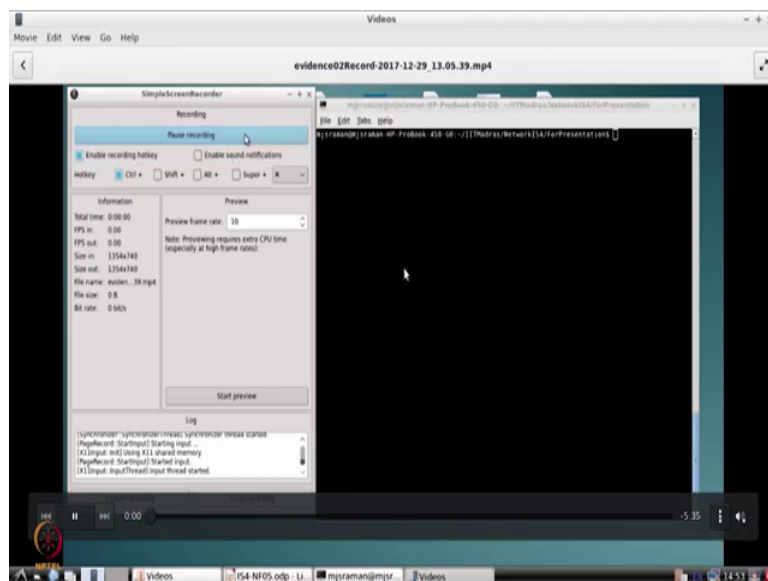
**Information security - IV**  
**Prof. M J Shankar Raman**  
**Department of Computer Science and Engineering**  
**Indian Institute of Technology, Madras**

**Lecture - 42**  
**Case study : Ann's Bad AIM Part II**

Hi, welcome to this session on the case study, where we were discussing how one could do forensic network forensic on a captured file. We saw that we could use wire shark and other tools and go through a tedious process of looking at each and every data; obviously, I mean you have to look at each and every data and then slowly form the case on what has happened ok.

So, in this section, we will find out and understand that it is not only I mean the whole tedious process good as well be automated, and you could get a much more elegant solution ok. Obviously then you are to do lot of work to get this elegant solution, but then in this by automatic the process you should be able to get more and more tools. So, what could happen is that; you could start accumulating these tools at one point in time and then this could itself from a kind of weight forensic tool to quickly get the evidences ok.

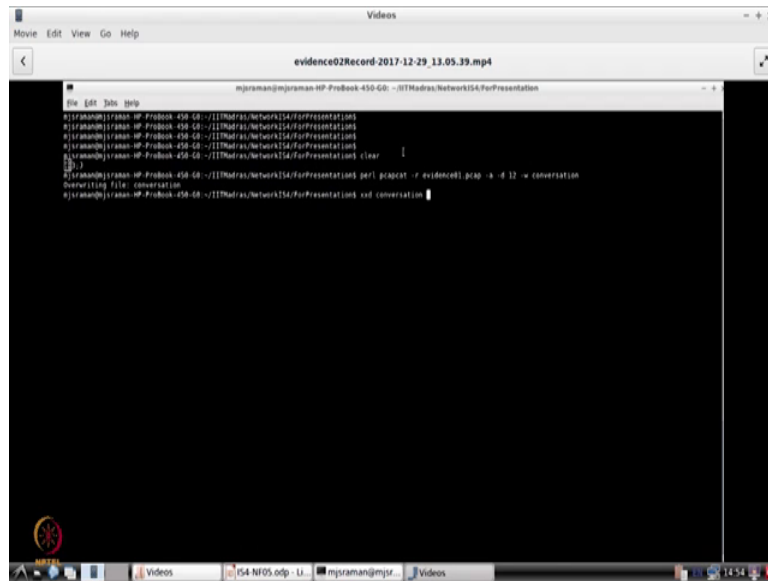
(Refer Slide Time: 01:30)



So, let us take a look at, how you could use the command lines or programming language to quicken up the whole job ok. So, in this case what we are going to discuss is a solution

that has provided for this for this problem and which one of the best price ok. So, what will; so what this authorized done is written some 2 or 3 scripts ok, using pearl and he has also looked into the protocol ok, he has reverse engineate the protocol; so that it is able to dump the packets in the protocols and you are able to identify all the packets very quickly etcetera ok.

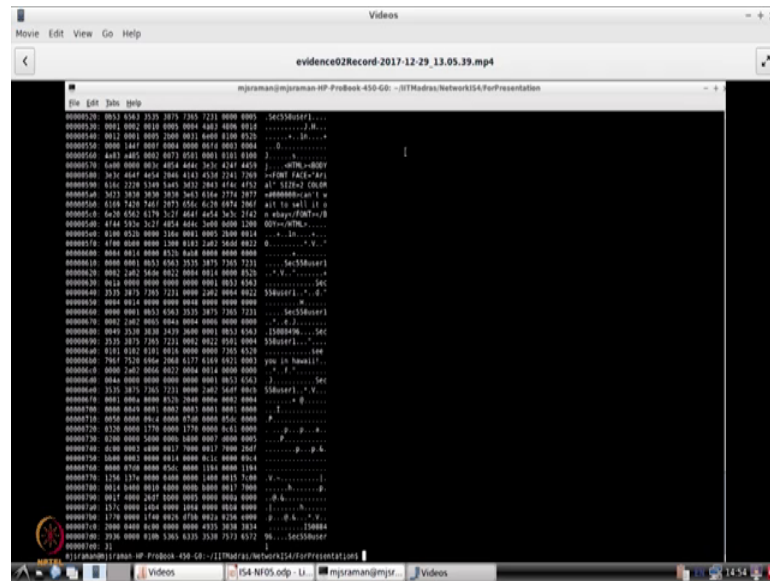
(Refer Slide Time: 02:11)



```
File Edit View Go Help
evidence02Record-2017-12-29_13.05.39.mp4
mjraman@mjraman-HP-ProBook-450-G6-...ITMadras:NetworkISA:ForPresentation
[mjraman@mjraman-HP-ProBook-450-G6-...ITMadras:NetworkISA:ForPresentation]
[mjraman@mjraman-HP-ProBook-450-G6-...ITMadras:NetworkISA:ForPresentation]
[mjraman@mjraman-HP-ProBook-450-G6-...ITMadras:NetworkISA:ForPresentation]
[mjraman@mjraman-HP-ProBook-450-G6-...ITMadras:NetworkISA:ForPresentation] clear
[mjraman@mjraman-HP-ProBook-450-G6-...ITMadras:NetworkISA:ForPresentation] perl pcapcat / evidence01.pcap -s 4 12 -w conversation
Overwritting file: conversation
[mjraman@mjraman-HP-ProBook-450-G6-...ITMadras:NetworkISA:ForPresentation] xcd conversation
```

So, let us see how this person is done this ok. So what has happened is that; you can actually take the evidence file and then pcapcat can be used; and then what he does is? He is actually extracting the conversation that is happened; and you could go to his to the solution website and identify the actually the source the source code for these files ok.

(Refer Slide Time: 02:49)

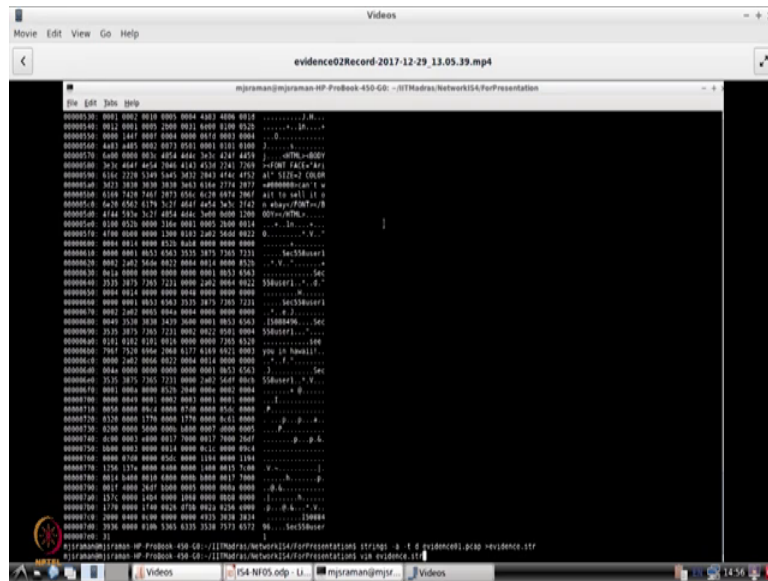


And what has happened is; once he identifies the conversation file, he goes ahead; and then and you can go out and look at this you can use the x x d which is the x editor or view the look view the file in a hex format and you can just go ahead and take and then go through this file and which will also give the similar letters to what we did last time I mean using our wire shark ok.

So, if you look at this you are able to see, what is the username? So here is a secret recipe, I just downloaded from the file server just copy to thumb drive and you are good to go and then it I mean; so and then there is this recipe dot doc hex etcetera; all these things. And we saw that the user was scc 55-58 user one ok; and you can see all the information that is there ok. So, the recipe was dot and then here this person says see you in Hawaii and all those things.

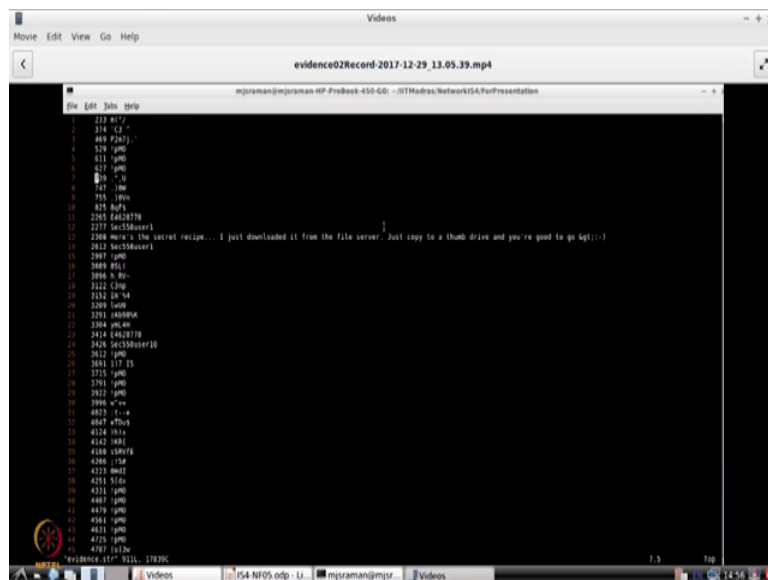
So, the same thing with what we did with wire shark we could also do with this command line ok. Then what we could do is; we can use the string command and go ahead and get all the strings that had happened in the conversation.

(Refer Slide Time: 03:58)



So, this is another way without using wire shark; we can just use this command line and then identify what are all the strings that are used. So, let us identify a storing it in a file called evidence dot str.

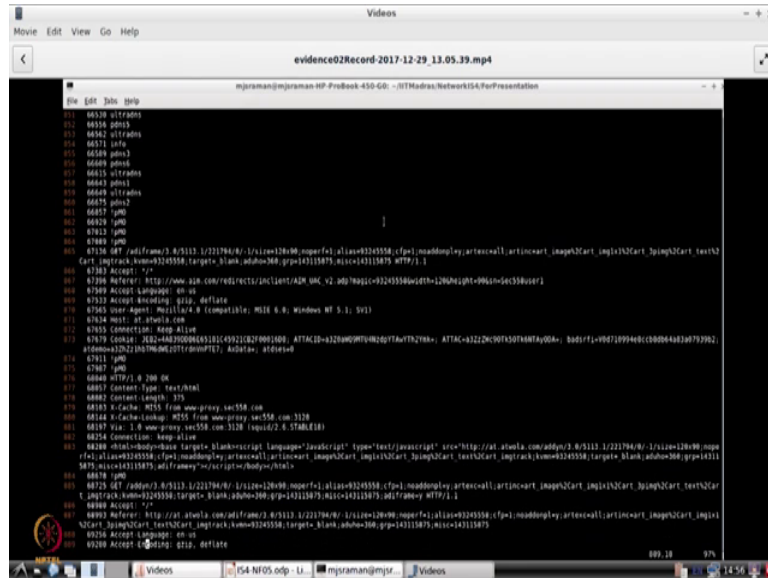
(Refer Slide Time: 04:27)



And once you look into the file ok, so it lists all the strings that are there. So, and this is much more readable for us ok. So, we can go through it obviously, it is a big huge file and we have looked at whether the any HTTP messages, and in the HTTP message we are particularly interested in establishing that the name of this person ok. So, if you look

at s n parameter. So we will search for the s n parameter ok, which will tell what is the login name of this person? Who is having a chat with the other person ok?

(Refer Slide Time: 04:38)



So, we will have to go through this file and then we will search for sec 558 user one, which is supposed to be a login could be the login name ok. And if you look at this; we will go ahead and find out now, remember this is a prompt that you will usually get in a protocol I mean; so what you will do is and; so if you look at this line it clearly says that this s n ok, so this person has tried to login into America online web server.

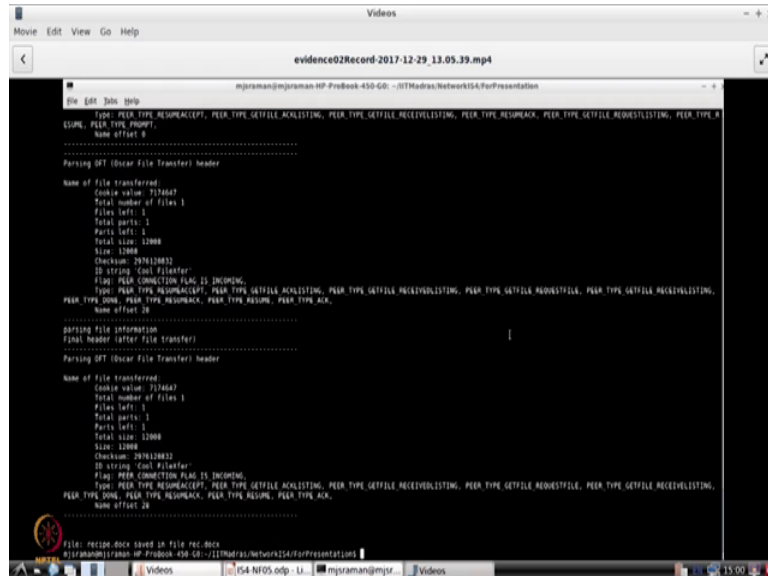
So, this is establishes that, this person who are it is sec 55-58 user one it could be the same person or could be different person, but we at least know the this is the login id of the person. So, this person as the one who has had a conversation with the other person and we got what the conversation is all about. Then what we will do is? We will now go ahead having established this; we will now go ahead and write and use one more script command line script.

Now, this will identify what are all the conversations that as happened between the particular machine and the other machine from the evidence that p p cap file. So, what will do now; is we will try to find out what are all the conversations that as happened between these two people ok.



tells you that from this o f t cat extract this recipe dot doc file, how do we extract recipe dot doc file?

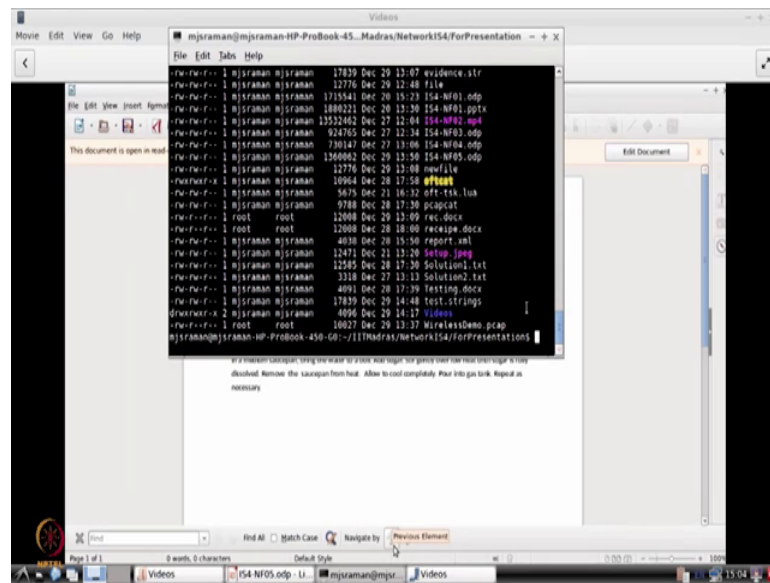
(Refer Slide Time: 08:44)



```
File Edit View Go Help
evidence02Record 2017-12-29_13.05.39.mp4
mjr@man@mjrman-HP-ProBook-450-G0: ~/ITMadras/Network154/ForPresentation
File: recipe.docx saved as file rec.docx
Type: PEER TYPE RESUMACEPT, PEER TYPE GETFILE_RECEIVELISTING, PEER TYPE GETFILE_RECEIVEFILE, PEER TYPE GETFILE_RECEIVELISTING, PEER TYPE X
ESUME, PEER TYPE POWER,
Name offset 8
-----
Parsing OFT (Oscar File Transfer) header
Name of file transferred
Cookie value: 7176d47
Total number of files: 1
Files left: 1
Total parts: 1
Parts left: 1
Total size: 12000
Size: 12000
Checksum: 2976126833
ID string: Cool FileTransfer
Flag: PEER CONNECTION FLAG IS INCOMING,
Type: PEER TYPE RESUMACEPT, PEER TYPE GETFILE_RECEIVELISTING, PEER TYPE GETFILE_RECEIVEFILE, PEER TYPE GETFILE_RECEIVELISTING,
PEER TYPE DONE, PEER TYPE RESUMACK, PEER TYPE RESUME, PEER TYPE ACK,
Name offset 20
-----
Parsing file information
Final header (after file transfer)
Parsing OFT (Oscar File Transfer) header
Name of file transferred
Cookie value: 7176d47
Total number of files: 1
Files left: 1
Total parts: 1
Parts left: 1
Total size: 12000
Size: 12000
Checksum: 2976126833
ID string: Cool FileTransfer
Flag: PEER CONNECTION FLAG IS INCOMING,
Type: PEER TYPE RESUMACEPT, PEER TYPE GETFILE_RECEIVELISTING, PEER TYPE GETFILE_RECEIVEFILE, PEER TYPE GETFILE_RECEIVELISTING,
PEER TYPE DONE, PEER TYPE RESUMACK, PEER TYPE RESUME, PEER TYPE ACK,
Name offset 20
```

You first identify the fingerprint that you have at the top and then the start of the file marker and the end of the file market. So if you look at this he has written a script which actually takes the Oscar file transfer protocol and then deciphers this protocol. And then collects the data packets from this. So, this is so in this case as told you should understand, what is protocol is? And then once he finds out how this protocol works, then he is actually takes the file recipe dot doc hex and sales it as our file recipe rec dot x.

(Refer Slide Time: 09:16)



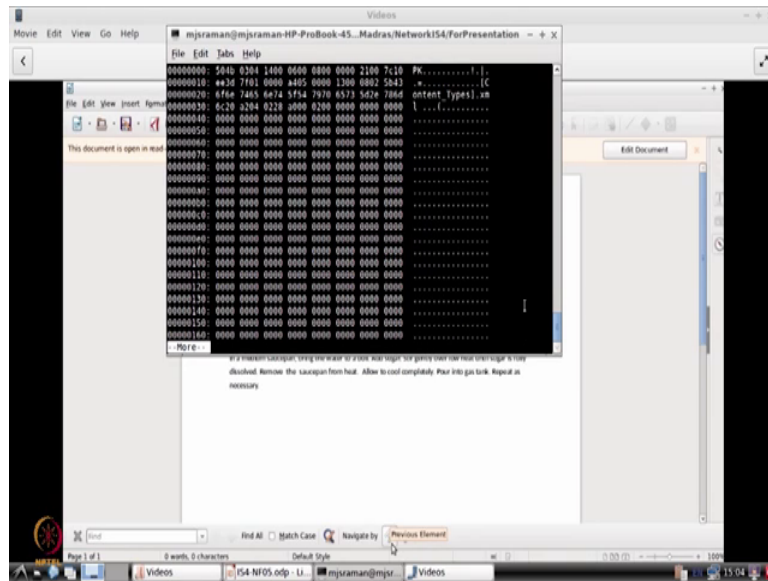
```
shcher@x:~$ ls -l
total 12
drwxr-xr-x 1 mjstraman mjstraman 17839 Dec 29 13:07 evidence_str
drwxr-xr-x 1 mjstraman mjstraman 12776 Dec 29 12:40 file
drwxr-xr-x 1 mjstraman mjstraman 1715561 Dec 20 15:29 IS4-NF01.odp
drwxr-xr-x 1 mjstraman mjstraman 1880221 Dec 20 13:30 IS4-NF01.pptx
drwxr-xr-x 1 mjstraman mjstraman 13532462 Dec 27 12:04 IS4-NF02.apk
drwxr-xr-x 1 mjstraman mjstraman 928765 Dec 27 12:34 IS4-NF03.odp
drwxr-xr-x 1 mjstraman mjstraman 730163 Dec 27 13:06 IS4-NF04.odp
drwxr-xr-x 1 mjstraman mjstraman 1360062 Dec 29 13:50 IS4-NF05.odp
drwxr-xr-x 1 mjstraman mjstraman 12776 Dec 29 13:08 newfile
drwxr-xr-x 1 mjstraman mjstraman 10964 Dec 28 17:50 #?#?#?#?
drwxr-xr-x 1 mjstraman mjstraman 5633 Dec 21 16:32 opt-test.lua
drwxr-xr-x 1 mjstraman mjstraman 9788 Dec 28 17:30 pcapcat
drwxr-xr-x 1 root root 12008 Dec 29 13:09 rec.docx
drwxr-xr-x 1 root root 12008 Dec 28 18:00 recipe.docx
drwxr-xr-x 1 mjstraman mjstraman 4038 Dec 28 15:50 report.nsl
drwxr-xr-x 1 mjstraman mjstraman 12471 Dec 21 13:20 Setup_jmgg
drwxr-xr-x 1 mjstraman mjstraman 12585 Dec 28 17:30 Solution1.txt
drwxr-xr-x 1 mjstraman mjstraman 3318 Dec 27 13:12 Solution2.txt
drwxr-xr-x 1 mjstraman mjstraman 4061 Dec 28 17:30 Testing.docx
drwxr-xr-x 1 mjstraman mjstraman 17839 Dec 29 14:48 test-strings
drwxr-xr-x 2 mjstraman mjstraman 4096 Dec 29 14:17 videos
drwxr-xr-x 1 root root 10027 Dec 29 13:37 WirelessDemo.pcap
mjstraman@mjstraman-HP-ProBook-450-G6-.../11Madras/Network154/ForPresentation
```

So, how do we know that this is a doc x file ok. One you are able to guess that the person see said that recipe dot doc x. So, that is one, but that mean I could actually send it has even as a text file, and then say that it is a doc x files. So, usually people do it when Gmail says that such executable file cannot be sent people usually converted as txt and then send it and Gmail accepts it; I do not know why, but it accepts it ok.

So, so similarly ok; so how does; so someone could cheat that is; so what we do is; all these kind of files have some sort of a signature I think we discussed it in the last module. So, what we will do is? We will try to see what is the signature of a doc x file. So, we have got a r e c dot doc x. So, what we will do is we will do a hex dump of r e c dot doc x and then send it to more ok.

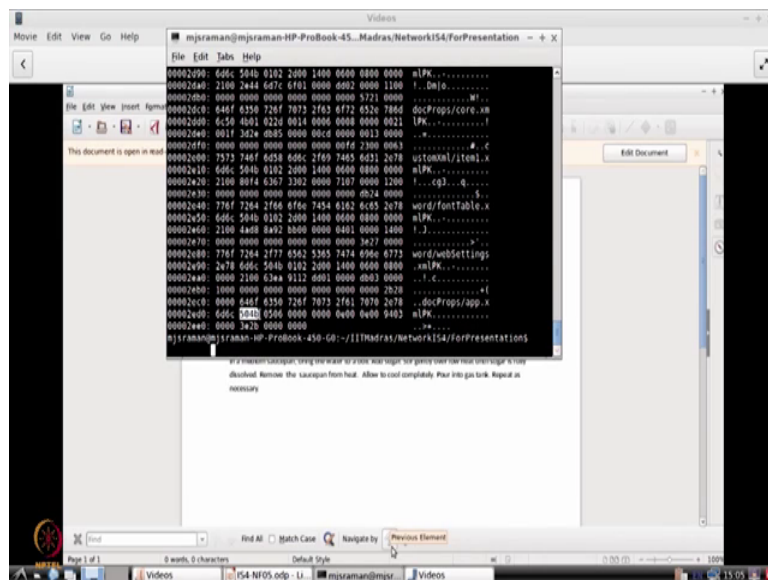


(Refer Slide Time: 10:12)



And if you look at this if you look at the very first byte it is 504b; almost all doc x files have this keyword ok. So, if you look let us take some other doc x file ok. So, let us say testing the doc x ok.

(Refer Slide Time: 10:40)



So, hopefully that is a doc x file. So, this is also start with a 504b you can use the tail command also. If you want let us go to the end and you see something like 504b appears here again ok. And there is a 3e2b ok, let us see which one is a signature here. So, here it

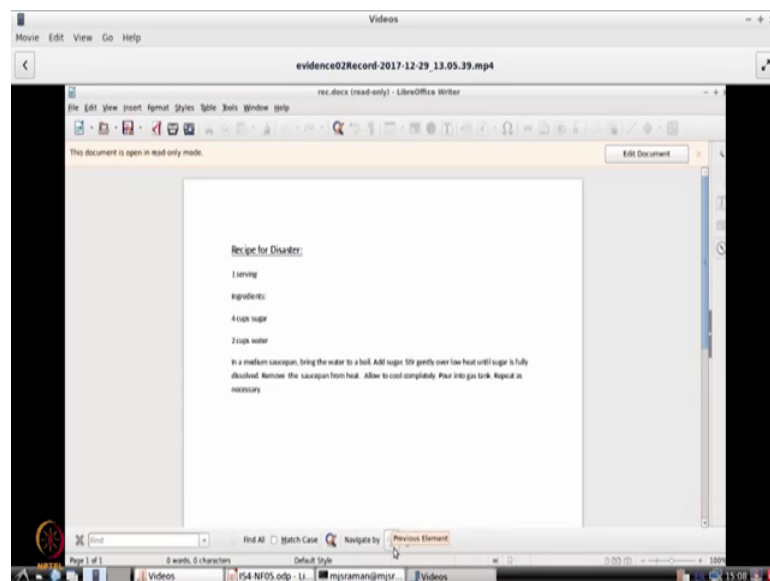
is 504b and this is the end of the file. So, this 3e2b actually makes the marker as the end of the file.

So, based on this 3e2b you actually know that this file starts with the one that we saw here ok. So, between these two files are the markers for your doc x. So, in this way I will be able to identify ok, what is the extract the contents of the file and in our case for example, we found out that this is a doc x file therefore, these are all the two boundaries, so you cut the hex and then make it as a file together, and then you just display it ok.

So, this process has been automated in the script it is given there. So, in this way; so let us look at the learning's from this kind of forensic analysis. The first thing that we should do is that; yes there is going to be huge amount of data and every data is important ok. The second one is that you might have to first get a overall picture of what has happened; so what that what you do is? You do some kind of a flow you take the flow; so you can do a packet analysis, then you have to do a flow analysis, then you can do a protocol analysis once you do all three then you have to do data carving and extraction.

So, the last step was data carving and extraction, where we use the oft call file the o f t call program and before that we were trying to identify. So for example, the command like strings and all that were trying to get an idea of what has happened?

(Refer Slide Time: 12:31)



So, this is in short a small case study on, how to go ahead and do forensic activity. So, we are seen the theory before and in this case study you have just briefly covered ok. How to do this activity? But there are lot more details, so our suggestion is that you go to that forensic contacts dot com website. And then take this case and then read almost all the solutions that others have come up with, say because different people have come up with different solutions.

And what we are seen is two such solutions there are many other solutions that are there in the website, please go ahead and review some of those solutions and see how people have worked on getting the data out.

Thank you very much.