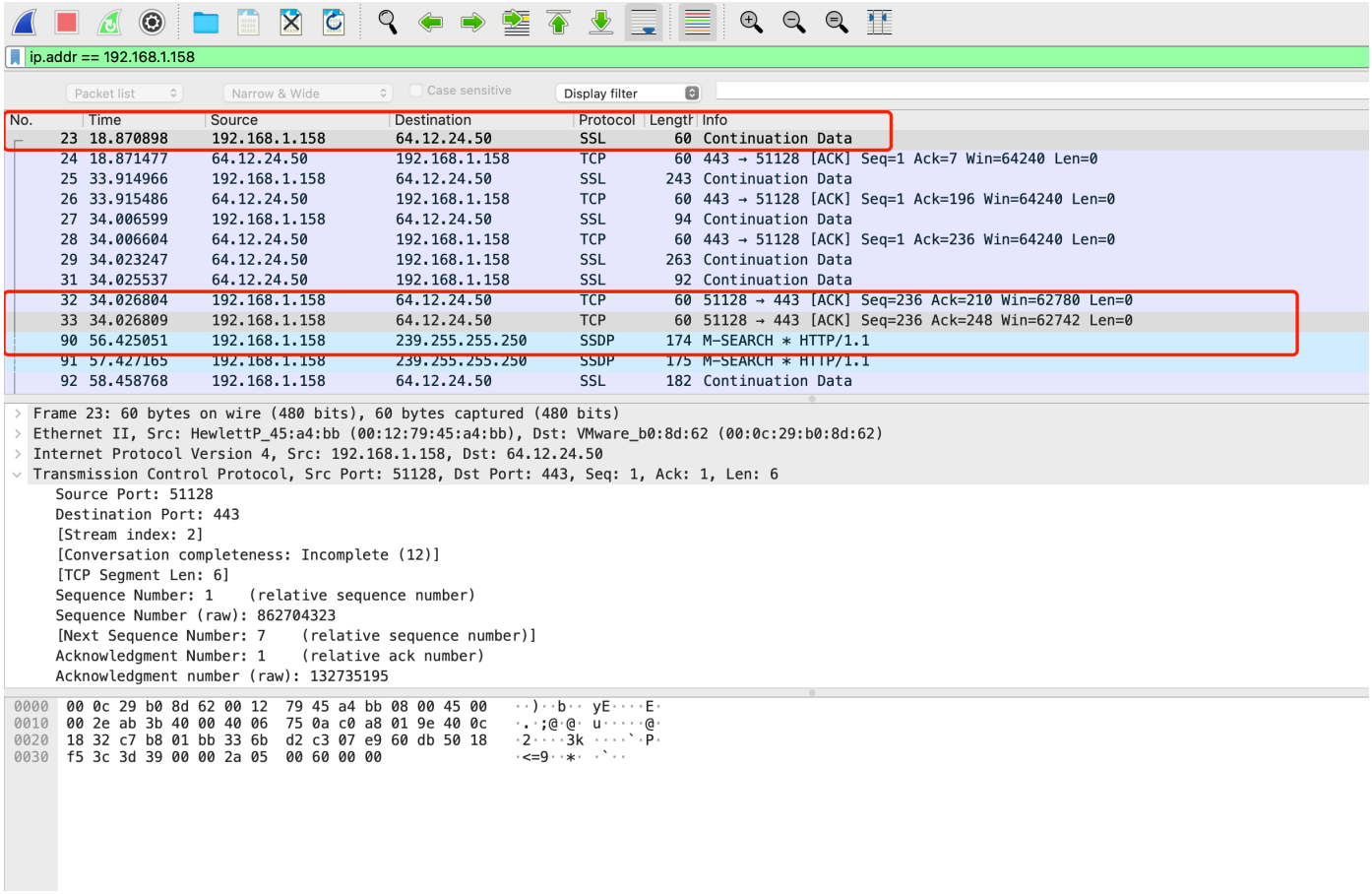
IERG 5320

Name：Lin Youguang

SID : 1155169171

We know that Ann's IP is 192.168.1.158, so first use the display filter: ip.addr == 192.168.1.158

```
ip.addr == 192.168.1.158
```



We found that the destination is 64.12.24.50.

We searched this ip on google, we found that it came from American.

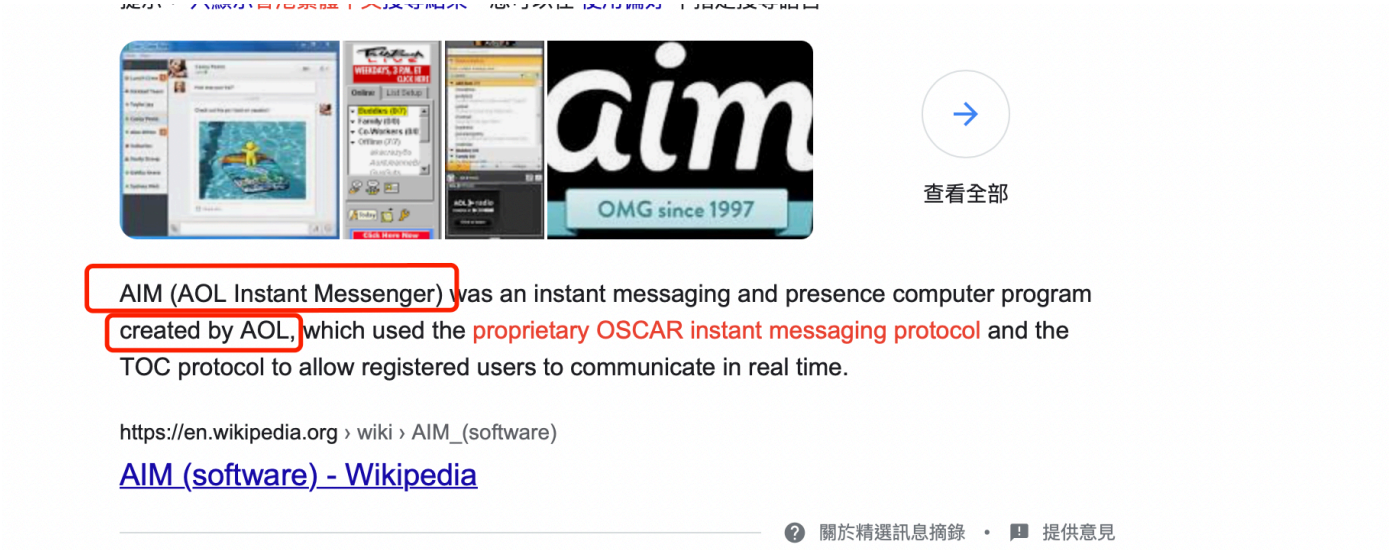
輸入 IP 或 Domain： 64.12.24.50 查詢

查詢結果

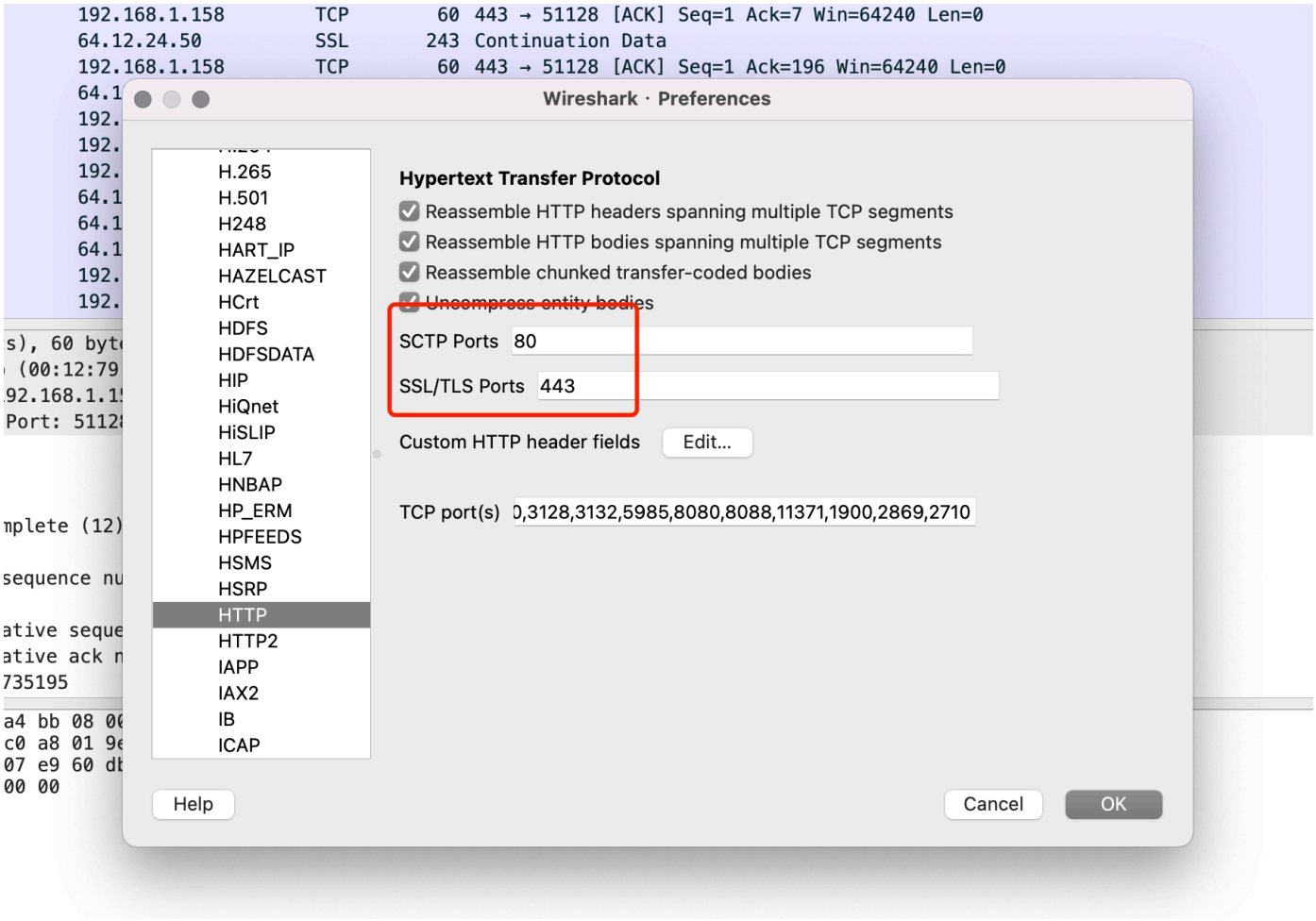
主機名稱：	-
國家名稱：	NA - North America (北美洲) US - United States (美國)
經度緯度：	經度：-97.822　緯度：37.751
電訊名稱：	Oath Holdings
單位名稱：	Oath Holdings
網域名稱：	aol.com
時區單位：	America/Chicago (UTC -06:00)

By checking the domain name, we know that he is from the American company Aol.

Then we google Aol,

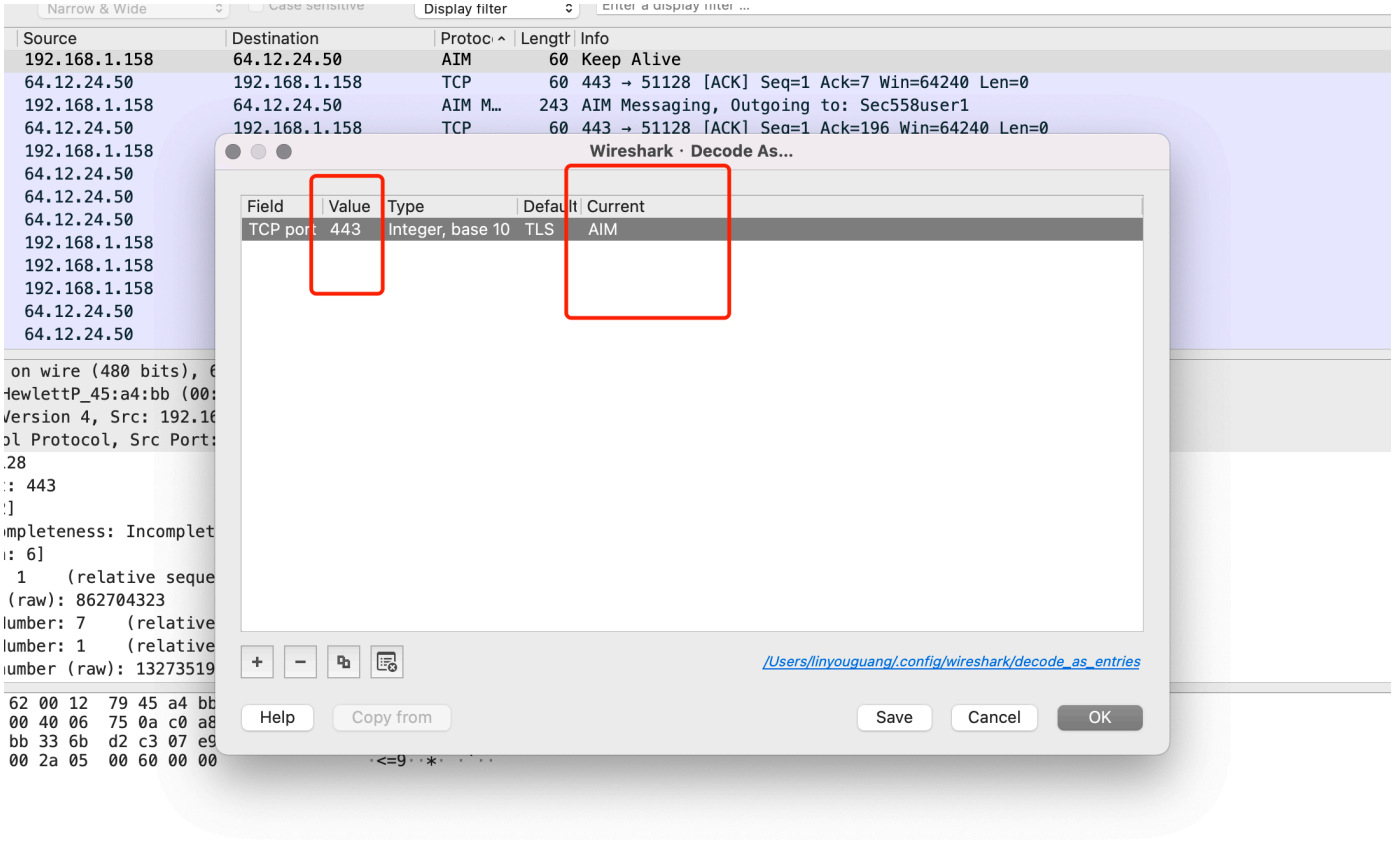


AOL Instant Messenger (AOL Instant Messenger) is abbreviated as AIM. As a communication service, AOL should have its own communication protocol (for example, the communication protocol of QQ is OICQ), and the port is 443.

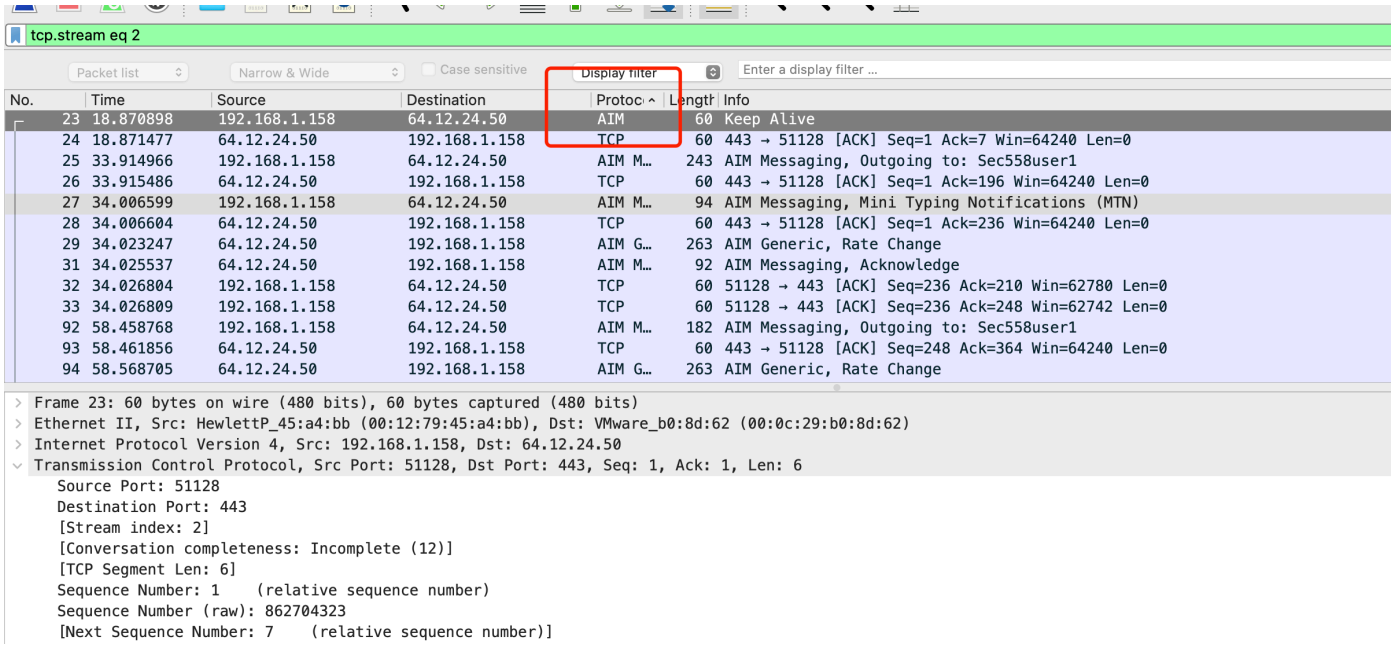


Since the Wireshark resolution protocol is based on the port, and the communication port displayed in the settings is 443, it will naturally be resolved to SSL. Therefore, when we see SSL or TLS, it may be communication encryption, or it may be a parsing error.

Since we know that the other party of Ann's communication is AOL's server, it is likely that they communicated using the AOL and AIM protocol. So we try to decode. We changed its port 443 and used AIM protocol.

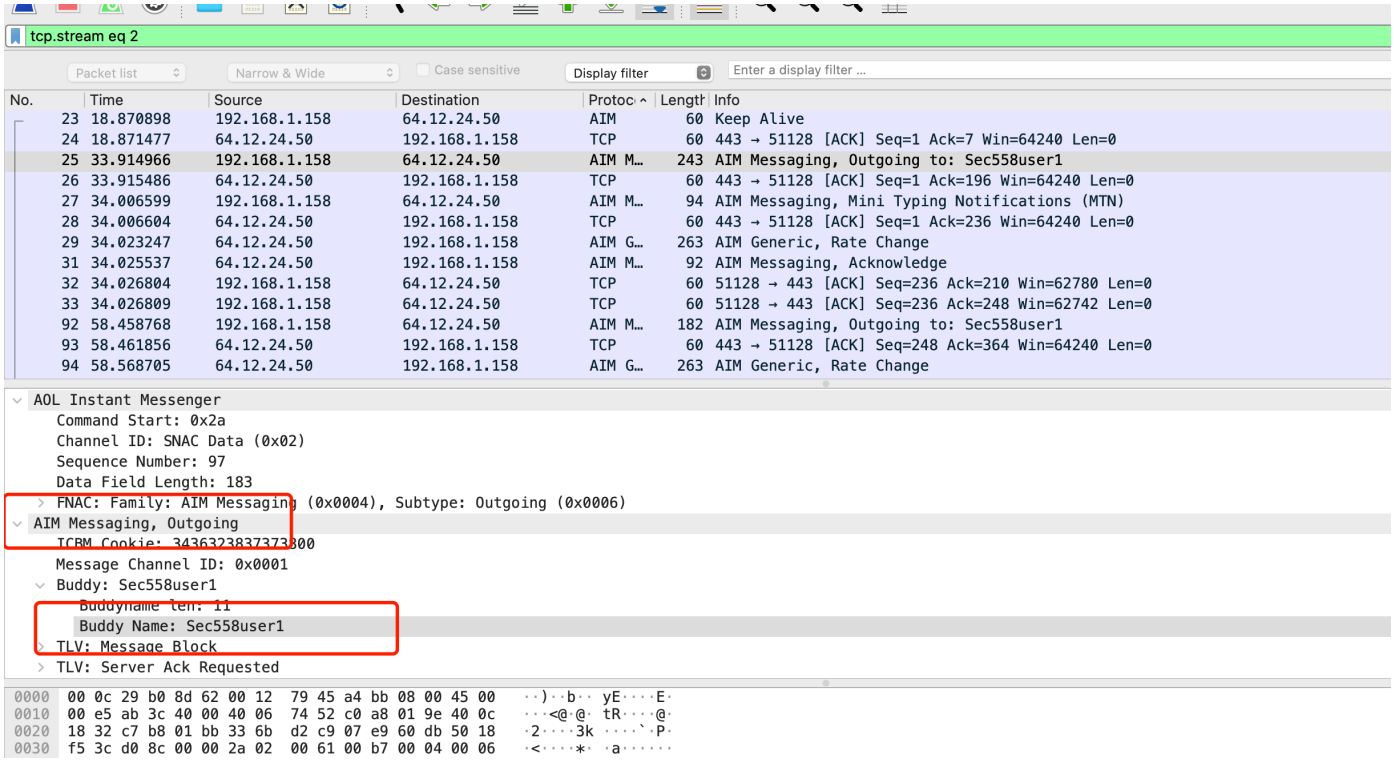


We found that the analysis was successful! Now, its protocol became AIM.



Question 1.1

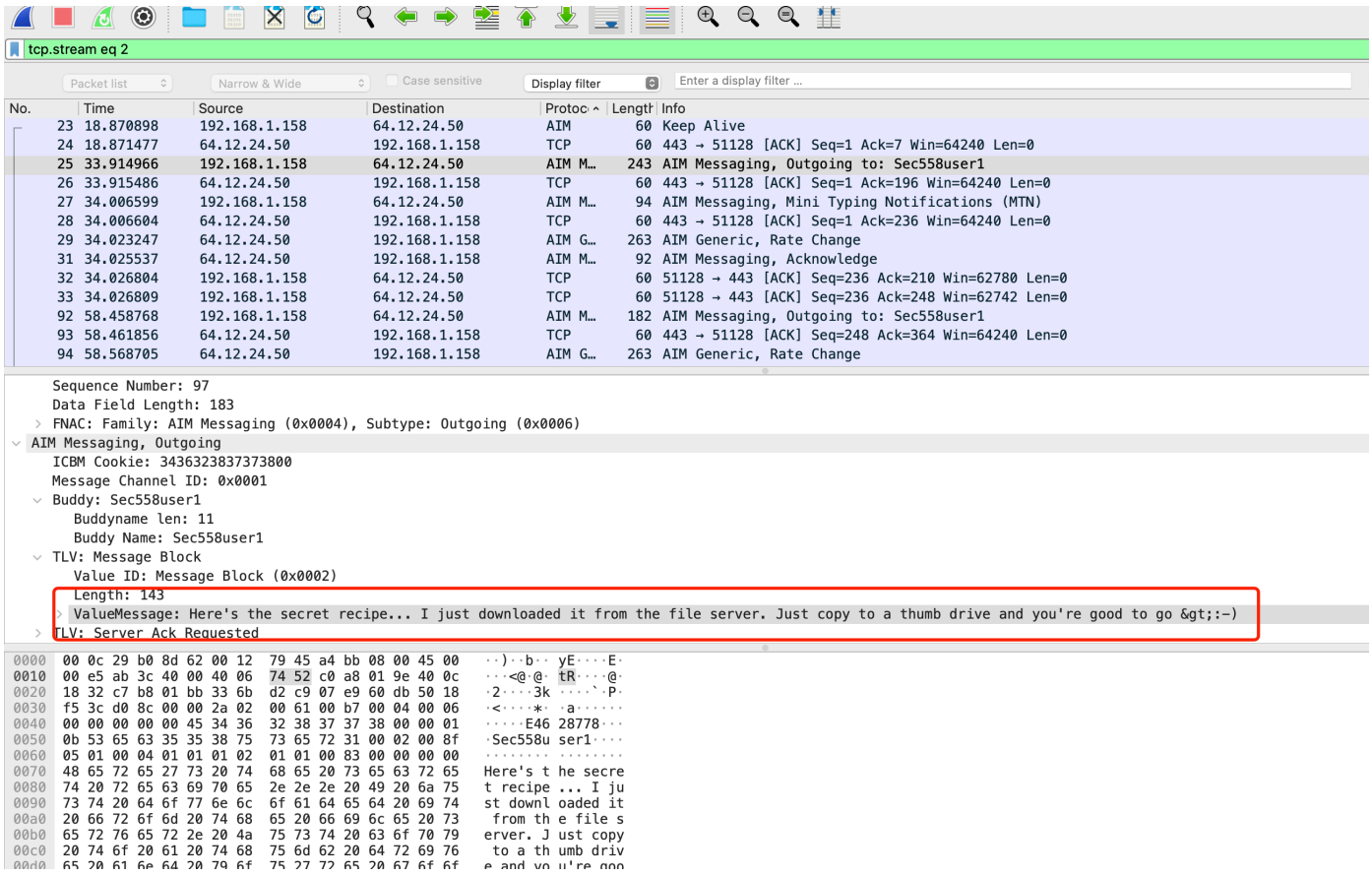
Then, we found in the No.25 in transmission layer , it has Ann's IM buddy name: "Sec558user1".



Question 1.2

The first comment in the captured IM conversation:

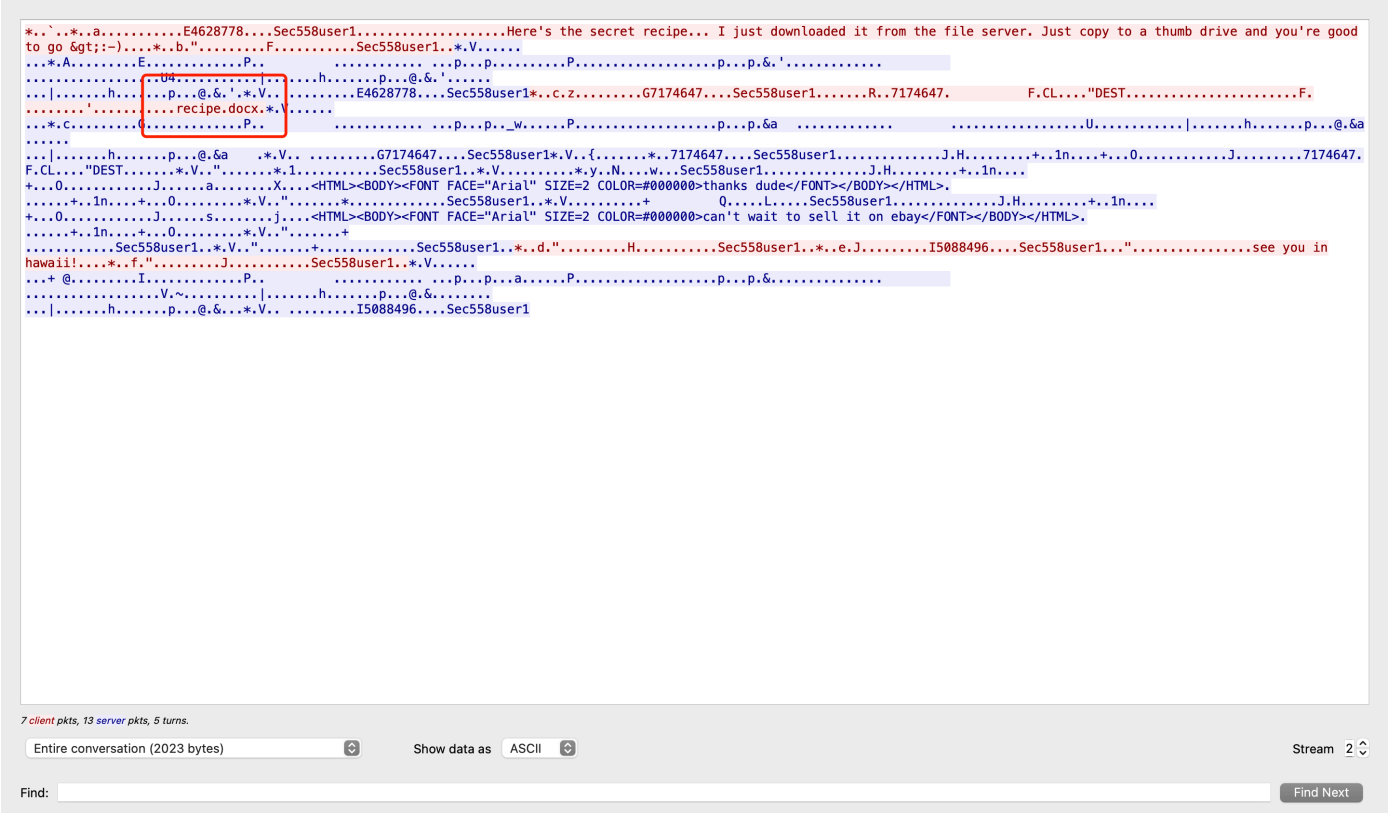
```
ValueMessage: Here's the secret recipe... I just downloaded it from the file server.
Just copy to a thumb drive and you're good to go &gt;:-)
```



Question 1.3

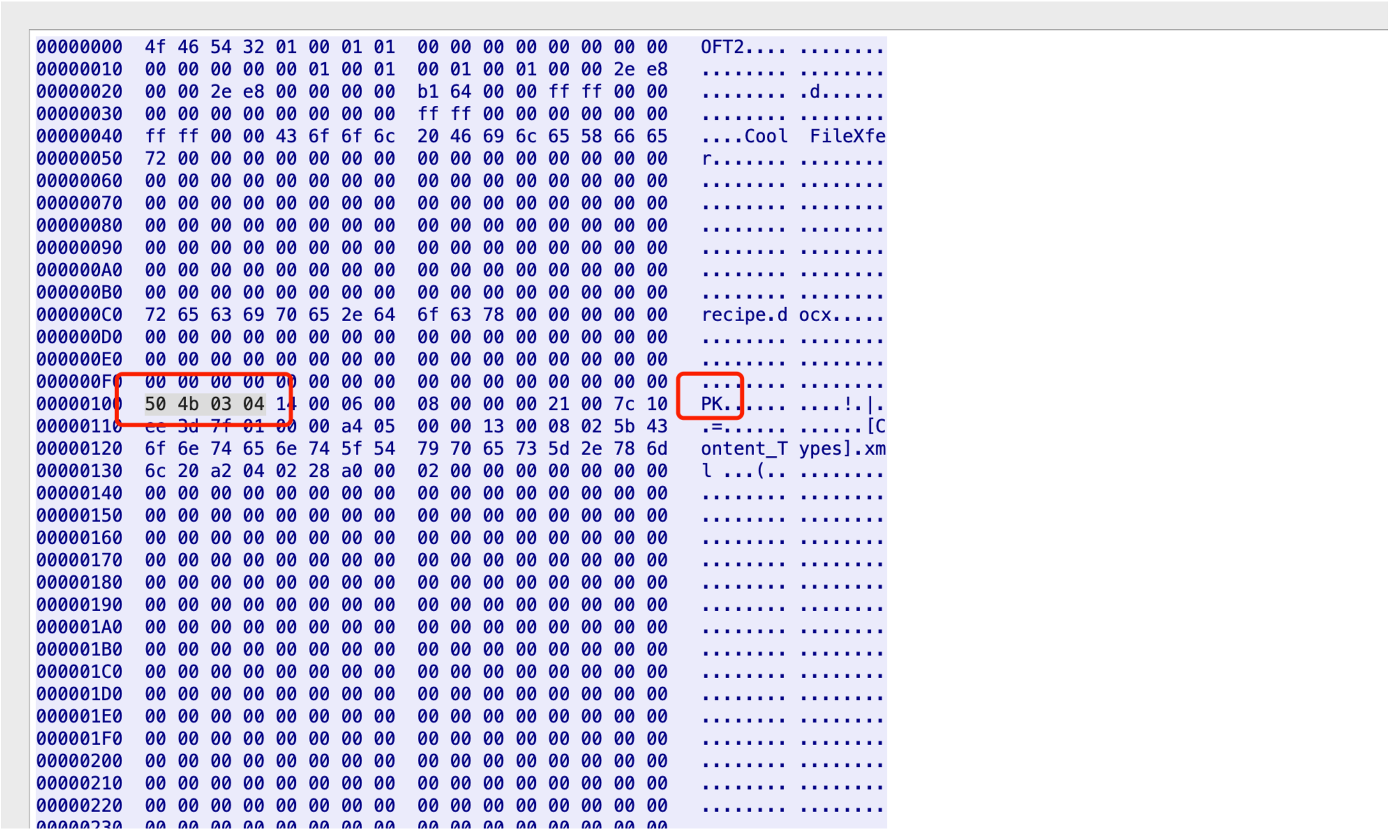
In order to see the communication between the two hosts, we right-click -> Trace Flow -> TCP Flow.

We found the a file named recipe.docx



Question 1.4

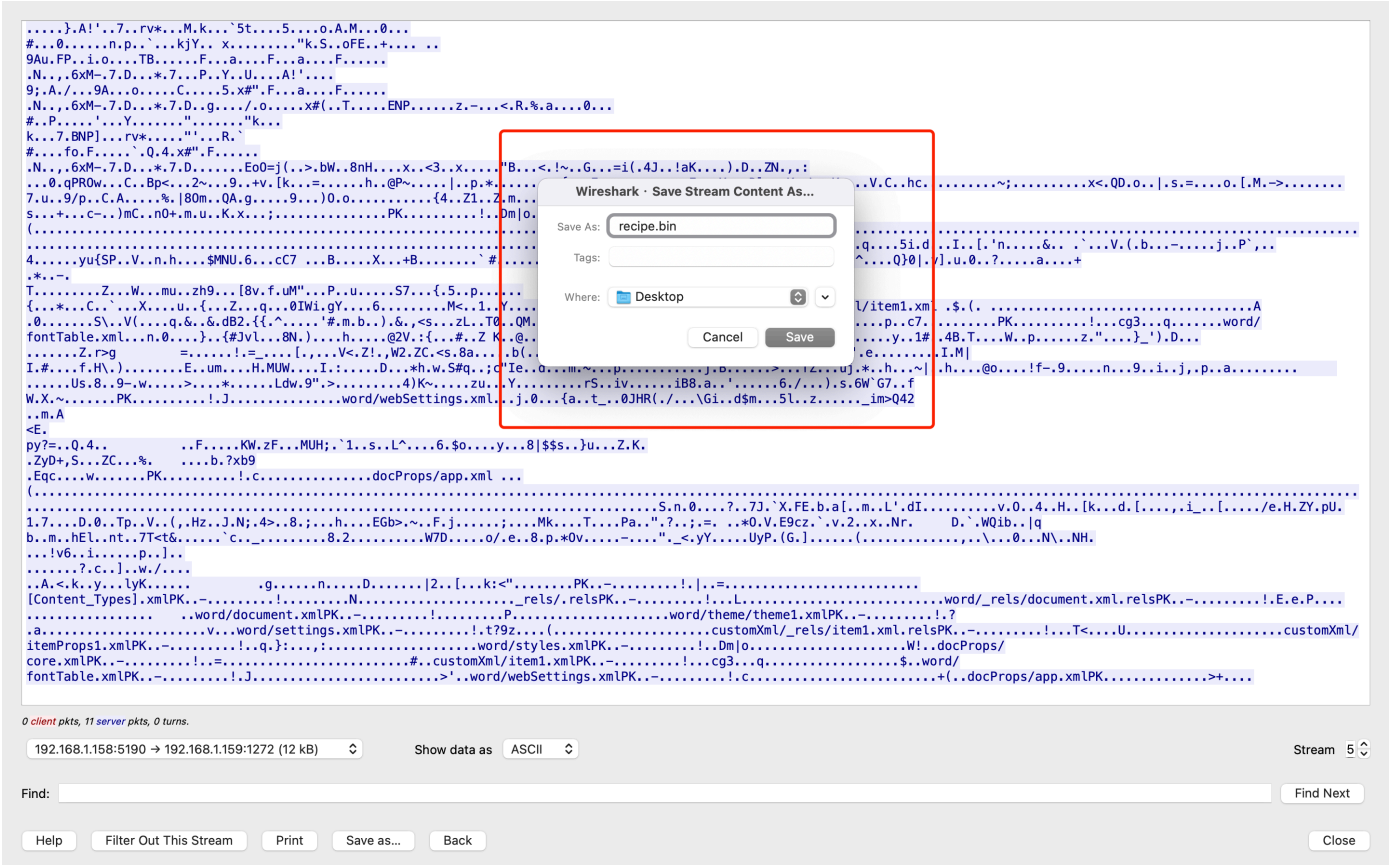
Docx Magic number is 50 4B 03 04.


00000000 4f 46 54 32 01 00 01 01 00 00 00 00 00 00 00 00 OFT2.... ....
00000010 00 00 00 00 00 01 00 01 00 01 00 01 00 00 2e e8 ....
00000020 00 00 2e e8 00 00 00 00 b1 64 00 00 ff ff 00 00 .... .d......
00000030 00 00 00 00 00 00 00 00 ff ff 00 00 00 00 00 00 ....
00000040 ff ff 00 00 43 6f 6f 6c 20 46 69 6c 65 58 66 65 ....Cool FileXfe
00000050 72 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 r....... ....
000000C0 72 65 63 69 70 65 2e 64 6f 63 78 00 00 00 00 00 recipe.d ocx.....
000000F0 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 ....
00000100 50 4b 03 04 14 00 06 00 08 00 00 00 21 00 7c 10 PK...... ....!.|.
00000120 6f 6e 74 65 6e 74 5f 54 79 70 65 73 5d 2e 78 6d ontent_T ypes].xm
00000130 6c 20 a2 04 02 28 a0 00 02 00 00 00 00 00 00 00 l ...(.. ....


Packet 119. 0 client pkts, 11 server pkts, 0 turns. Click to select.
192.168.1.158:5190 → 192.168.1.159:1272 (12 kB)
Show data as
Raw
Stream 5
Find:
Find Next

Help file	.hlp	3F 5F 03 00 [?_..]
VMWare Disk file	.vmdk	4B 44 4D 56 [KDMV]
Outlook Post Office file	.pst	21 42 44 4E 42 [!BDNB]
PDF Document	.pdf	25 50 44 46 [%PDF]
Word Document	.doc	D0 CF 11 E0 A1 B1 1A E1
RTF Document	.rtf	7B 5C 72 74 66 31 [{ tf1]
Excel Document	.xls	D0 CF 11 E0 A1 B1 1A E1
PowerPoint Document	.ppt	D0 CF 11 E0 A1 B1 1A E1
Visio Document	.vsd	D0 CF 11 E0 A1 B1 1A E1
DOCX (Office 2010)	.docx	50 4B 03 04 [PK]
XLSX (Office 2010)	.xlsx	50 4B 03 04 [PK]
PPTX (Office 2010)	.pptx	50 4B 03 04 [PK]
Microsoft Database	.mdb	53 74 61 6E 64 61 72 64 20 4A 65 74
Postcript File	.ps	25 21 [%!]
Outlook Message File	.msg	D0 CF 11 E0 A1 B1 1A E1
EPS File	.eps	25 21 50 53 2D 41 64 6F 62 65 2D 33 2E 30 20 45 50 53 46 2D 33 20 30
Jar File	.jar	50 4B 03 04 14 00 08 00 08 00

Question 1.5



Storing the file in the local storage.

Recipe for Disaster:

1 serving

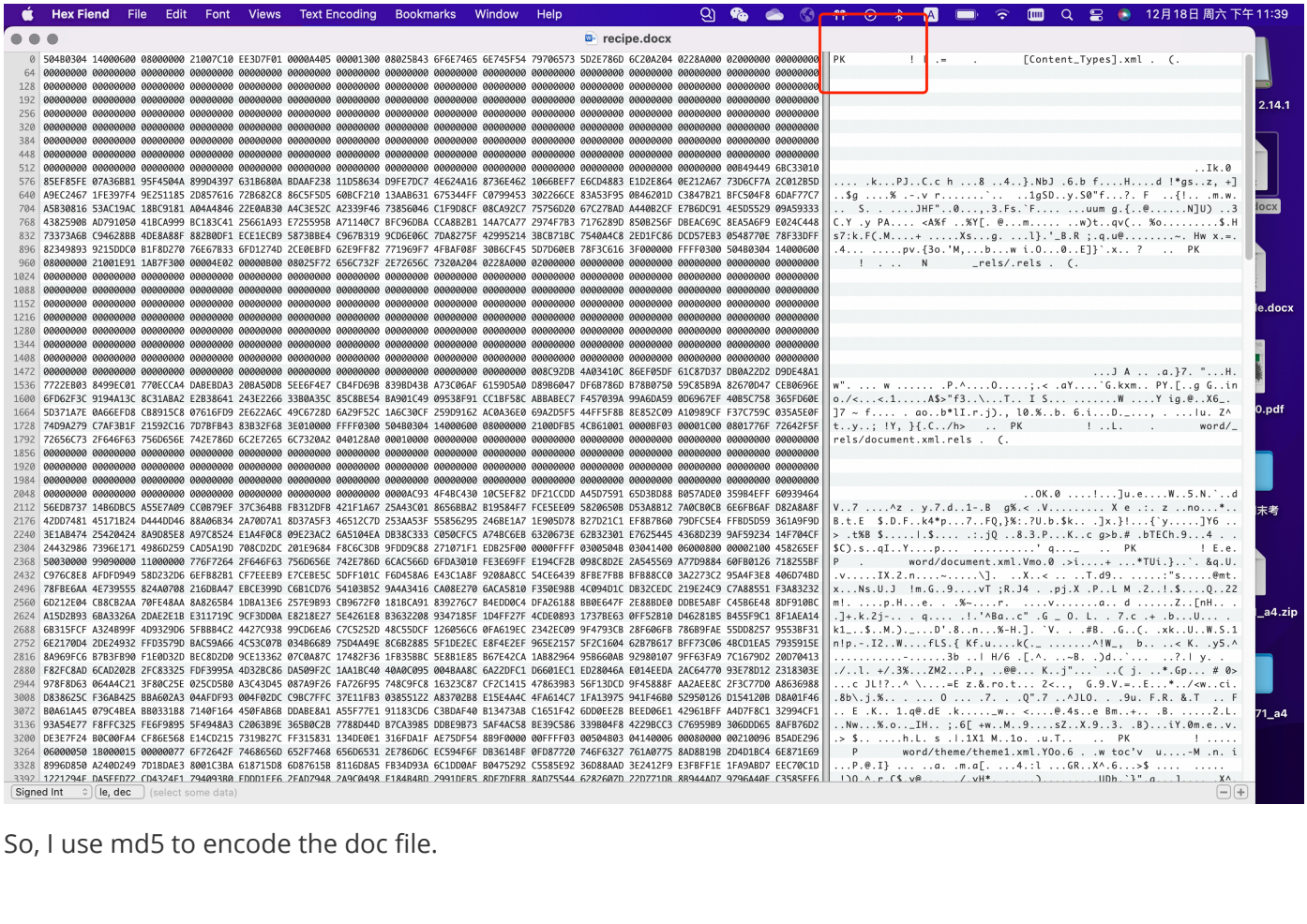
Ingredients:

4 cups sugar

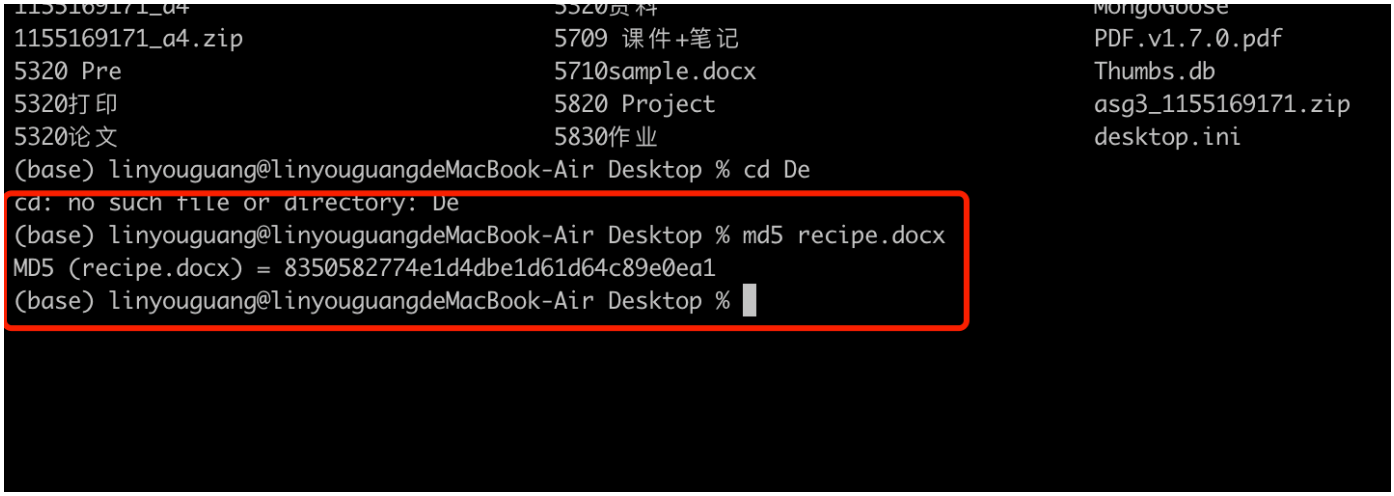
2 cups water

In a medium saucepan, bring the water to a boil. Add sugar. Stir gently over low heat until sugar is fully dissolved. Remove the saucepan from heat. Allow to cool completely. Pour into gas tank. Repeat as necessary.

Then, I deleted the content before the "PK" in recipe.docx



So, I use md5 to encode the doc file.

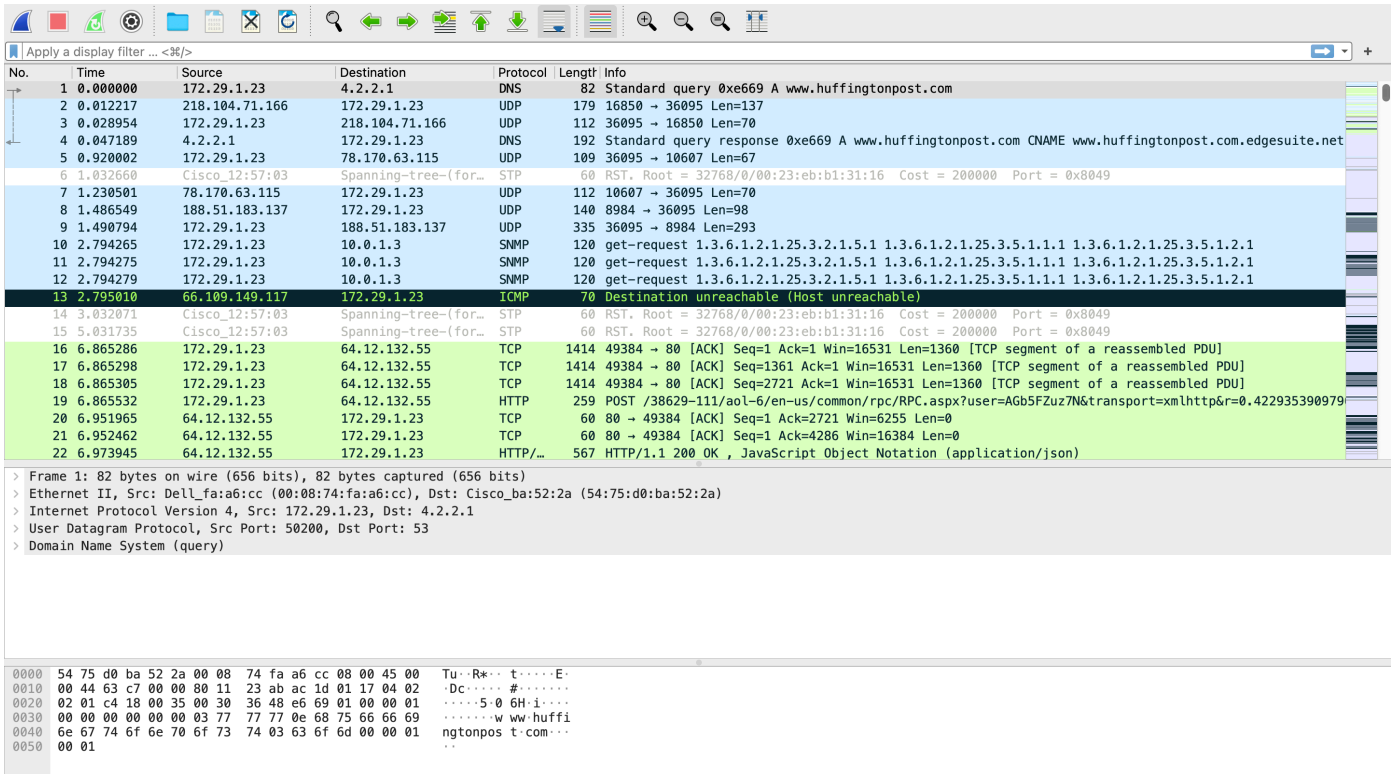


So, my md5 is

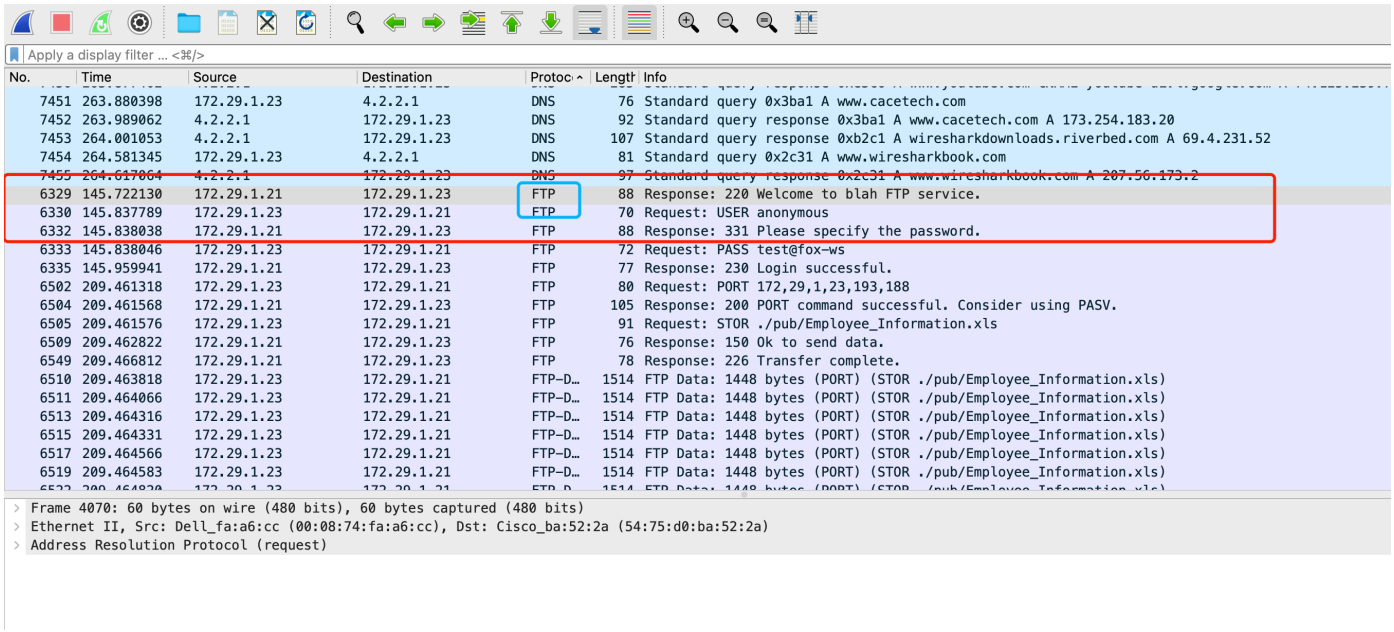
```
MD5 (recipe.docx) = 8350582774e1d4dbe1d61d64c89e0ea1
```

Question 2.1

Firtly, use WireShark open the problem_2.pcap.



Because the file is stolen through network, so I found the protocol about FTP started at No 6329.

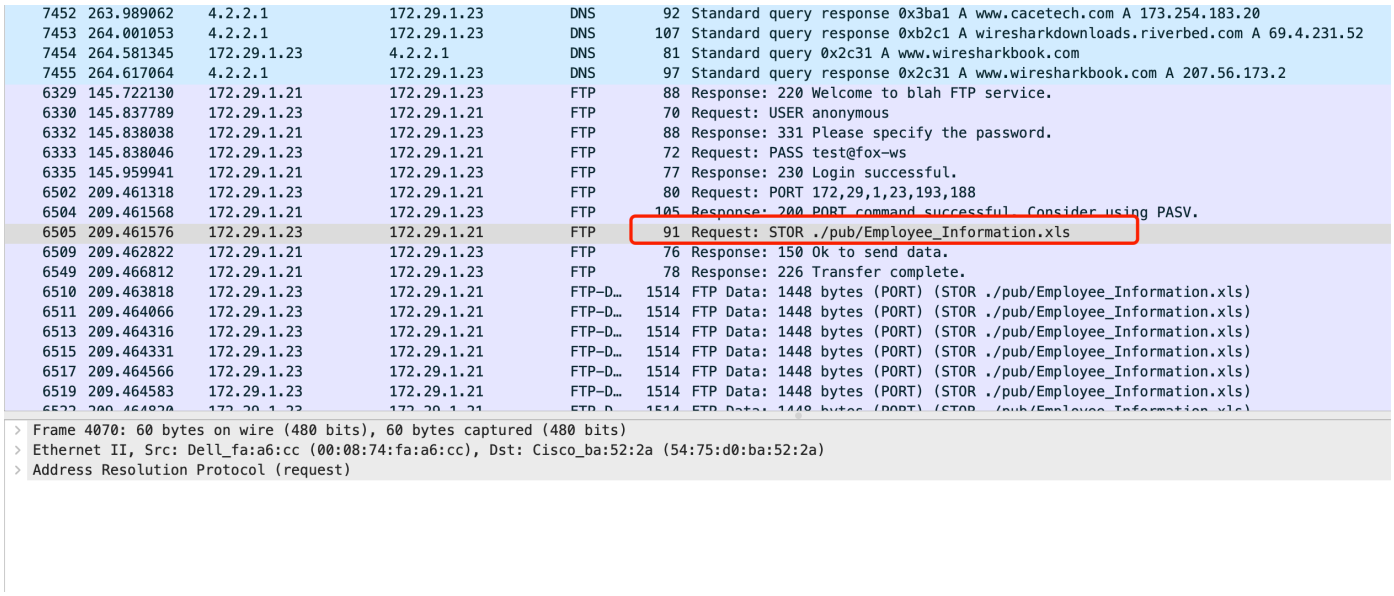


Apply a display filter ... <⌘/>

No.	Time	Source	Destination	Protoc	Length	Info
7451	263.880398	172.29.1.23	4.2.2.1	DNS	76	Standard query 0x3ba1 A www.cacetech.com
7452	263.989062	4.2.2.1	172.29.1.23	DNS	92	Standard query response 0x3ba1 A www.cacetech.com A 173.254.183.20
7453	264.001053	4.2.2.1	172.29.1.23	DNS	107	Standard query response 0xb2c1 A wiresharkdownloads.riverbed.com A 69.4.231.52
7454	264.581345	172.29.1.23	4.2.2.1	DNS	81	Standard query 0x2c31 A www.wiresharkbook.com
7455	264.617064	4.2.2.1	172.29.1.23	DNS	97	Standard query response 0x2c31 A www.wiresharkbook.com A 207.56.173.2
6329	145.722130	172.29.1.21	172.29.1.23	FTP	88	Response: 220 Welcome to blah FTP service.
6330	145.837789	172.29.1.23	172.29.1.21	FTP	70	Request: USER anonymous
6332	145.838038	172.29.1.21	172.29.1.23	FTP	88	Response: 331 Please specify the password.
6333	145.838046	172.29.1.23	172.29.1.21	FTP	72	Request: PASS test@fox-ws
6335	145.959941	172.29.1.21	172.29.1.23	FTP	77	Response: 230 Login successful.
6502	209.461318	172.29.1.23	172.29.1.21	FTP	80	Request: PORT 172,29,1,23,193,188
6504	209.461568	172.29.1.21	172.29.1.23	FTP	105	Response: 200 PORT command successful. Consider using PASV.
6505	209.461576	172.29.1.23	172.29.1.21	FTP	91	Request: STOR ./pub/Employee_Information.xls
6509	209.462822	172.29.1.21	172.29.1.23	FTP	76	Response: 150 Ok to send data.
6549	209.466812	172.29.1.21	172.29.1.23	FTP	78	Response: 226 Transfer complete.
6510	209.463818	172.29.1.23	172.29.1.21	FTP-D…	1514	FTP Data: 1448 bytes (PORT) (STOR ./pub/Employee_Information.xls)
6511	209.464066	172.29.1.23	172.29.1.21	FTP-D…	1514	FTP Data: 1448 bytes (PORT) (STOR ./pub/Employee_Information.xls)
6513	209.464316	172.29.1.23	172.29.1.21	FTP-D…	1514	FTP Data: 1448 bytes (PORT) (STOR ./pub/Employee_Information.xls)
6515	209.464331	172.29.1.23	172.29.1.21	FTP-D…	1514	FTP Data: 1448 bytes (PORT) (STOR ./pub/Employee_Information.xls)
6517	209.464566	172.29.1.23	172.29.1.21	FTP-D…	1514	FTP Data: 1448 bytes (PORT) (STOR ./pub/Employee_Information.xls)
6519	209.464583	172.29.1.23	172.29.1.21	FTP-D…	1514	FTP Data: 1448 bytes (PORT) (STOR ./pub/Employee_Information.xls)

> Frame 4070: 60 bytes on wire (480 bits), 60 bytes captured (480 bits)
> Ethernet II, Src: Dell_fa:a6:cc (00:08:74:fa:a6:cc), Dst: Cisco_ba:52:2a (54:75:d0:ba:52:2a)
> Address Resolution Protocol (request)

I found a info in these actions to store "./pub/Employee_Information.xls" at No.6505.

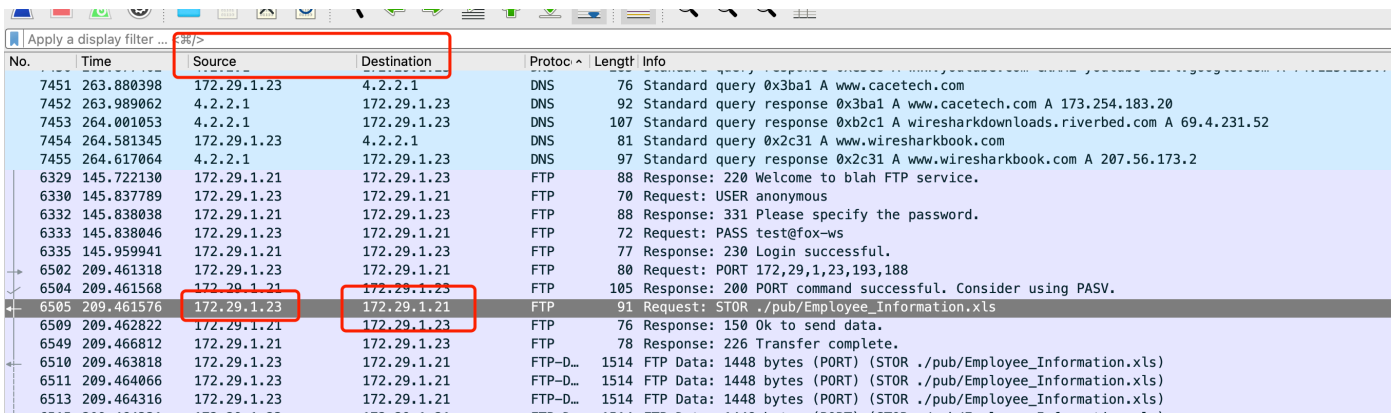


7452	263.989062	4.2.2.1	172.29.1.23	DNS	92	Standard query response 0x3ba1 A www.cacetech.com A 173.254.183.20
7453	264.001053	4.2.2.1	172.29.1.23	DNS	107	Standard query response 0xb2c1 A wiresharkdownloads.riverbed.com A 69.4.231.52
7454	264.581345	172.29.1.23	4.2.2.1	DNS	81	Standard query 0x2c31 A www.wiresharkbook.com
7455	264.617064	4.2.2.1	172.29.1.23	DNS	97	Standard query response 0x2c31 A www.wiresharkbook.com A 207.56.173.2
6329	145.722130	172.29.1.21	172.29.1.23	FTP	88	Response: 220 Welcome to blah FTP service.
6330	145.837789	172.29.1.23	172.29.1.21	FTP	70	Request: USER anonymous
6332	145.838038	172.29.1.21	172.29.1.23	FTP	88	Response: 331 Please specify the password.
6333	145.838046	172.29.1.23	172.29.1.21	FTP	72	Request: PASS test@fox-ws
6335	145.959941	172.29.1.21	172.29.1.23	FTP	77	Response: 230 Login successful.
6502	209.461318	172.29.1.23	172.29.1.21	FTP	80	Request: PORT 172,29,1,23,193,188
6504	209.461568	172.29.1.21	172.29.1.23	FTP	105	Response: 200 PORT command successful. Consider using PASV.
6505	209.461576	172.29.1.23	172.29.1.21	FTP	91	Request: STOR ./pub/Employee_Information.xls
6509	209.462822	172.29.1.21	172.29.1.23	FTP	76	Response: 150 Ok to send data.
6549	209.466812	172.29.1.21	172.29.1.23	FTP	78	Response: 226 Transfer complete.
6510	209.463818	172.29.1.23	172.29.1.21	FTP-D…	1514	FTP Data: 1448 bytes (PORT) (STOR ./pub/Employee_Information.xls)
6511	209.464066	172.29.1.23	172.29.1.21	FTP-D…	1514	FTP Data: 1448 bytes (PORT) (STOR ./pub/Employee_Information.xls)
6513	209.464316	172.29.1.23	172.29.1.21	FTP-D…	1514	FTP Data: 1448 bytes (PORT) (STOR ./pub/Employee_Information.xls)
6515	209.464331	172.29.1.23	172.29.1.21	FTP-D…	1514	FTP Data: 1448 bytes (PORT) (STOR ./pub/Employee_Information.xls)
6517	209.464566	172.29.1.23	172.29.1.21	FTP-D…	1514	FTP Data: 1448 bytes (PORT) (STOR ./pub/Employee_Information.xls)
6519	209.464583	172.29.1.23	172.29.1.21	FTP-D…	1514	FTP Data: 1448 bytes (PORT) (STOR ./pub/Employee_Information.xls)

> Frame 4070: 60 bytes on wire (480 bits), 60 bytes captured (480 bits)
> Ethernet II, Src: Dell_fa:a6:cc (00:08:74:fa:a6:cc), Dst: Cisco_ba:52:2a (54:75:d0:ba:52:2a)
> Address Resolution Protocol (request)

From this action, we can see the file is sent to destination of IP "172.29.1.21" With this information, we can assume that this address belongs to the attacker or, at the very least, to the server on which the attacker is storing stolen information.

Therefore, it can be inferred that the attacker's IP may be 172.29.1.21.

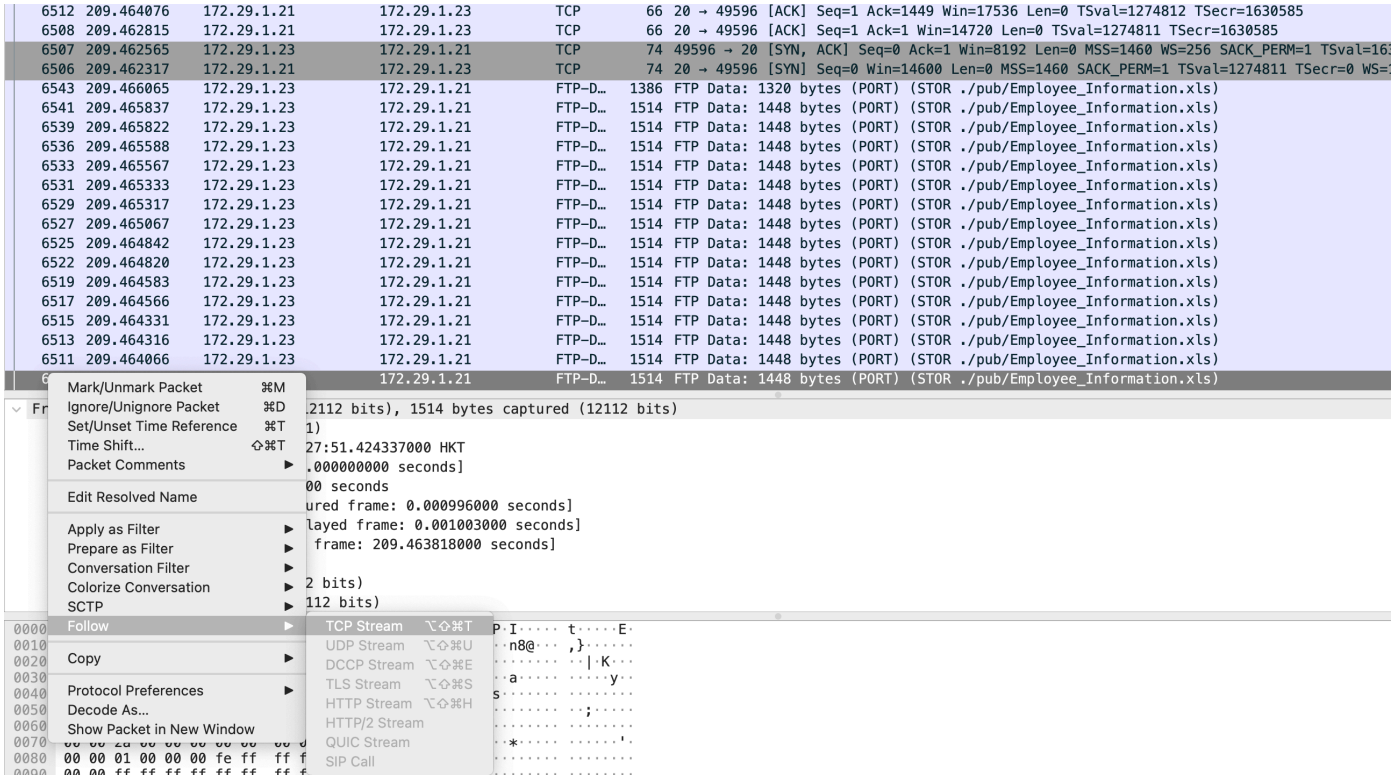


Apply a display filter ... <⌘/>

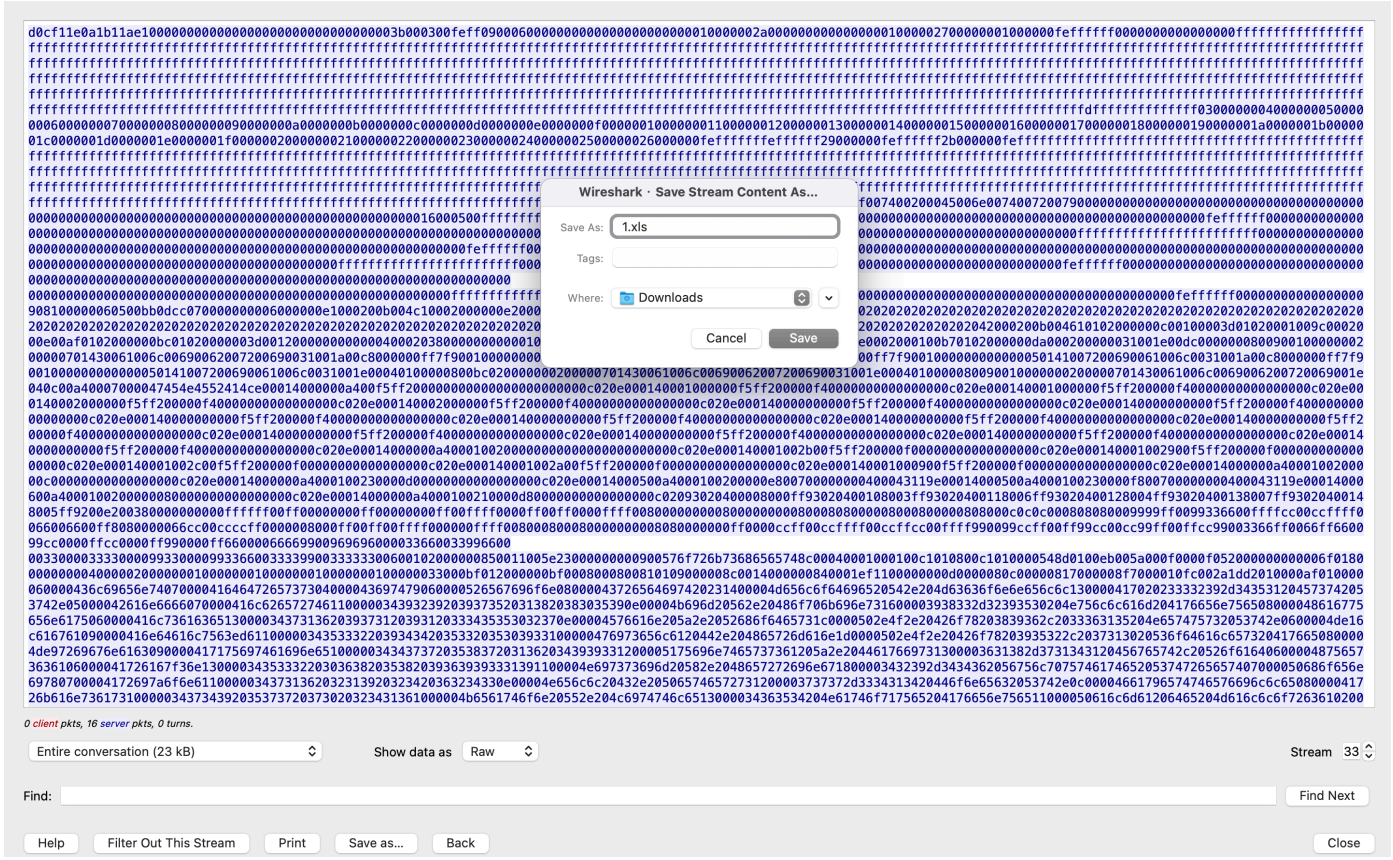
No.	Time	Source	Destination	Protoc	Length	Info
7451	263.880398	172.29.1.23	4.2.2.1	DNS	76	Standard query 0x3ba1 A www.cacetech.com
7452	263.989062	4.2.2.1	172.29.1.23	DNS	92	Standard query response 0x3ba1 A www.cacetech.com A 173.254.183.20
7453	264.001053	4.2.2.1	172.29.1.23	DNS	107	Standard query response 0xb2c1 A wiresharkdownloads.riverbed.com A 69.4.231.52
7454	264.581345	172.29.1.23	4.2.2.1	DNS	81	Standard query 0x2c31 A www.wiresharkbook.com
7455	264.617064	4.2.2.1	172.29.1.23	DNS	97	Standard query response 0x2c31 A www.wiresharkbook.com A 207.56.173.2
6329	145.722130	172.29.1.21	172.29.1.23	FTP	88	Response: 220 Welcome to blah FTP service.
6330	145.837789	172.29.1.23	172.29.1.21	FTP	70	Request: USER anonymous
6332	145.838038	172.29.1.21	172.29.1.23	FTP	88	Response: 331 Please specify the password.
6333	145.838046	172.29.1.23	172.29.1.21	FTP	72	Request: PASS test@fox-ws
6335	145.959941	172.29.1.21	172.29.1.23	FTP	77	Response: 230 Login successful.
6502	209.461318	172.29.1.23	172.29.1.21	FTP	80	Request: PORT 172,29,1,23,193,188
6504	209.461568	172.29.1.21	172.29.1.23	FTP	105	Response: 200 PORT command successful. Consider using PASV.
6505	209.461576	172.29.1.23	172.29.1.21	FTP	91	Request: STOR ./pub/Employee_Information.xls
6509	209.462822	172.29.1.21	172.29.1.23	FTP	76	Response: 150 Ok to send data.
6549	209.466812	172.29.1.21	172.29.1.23	FTP	78	Response: 226 Transfer complete.
6510	209.463818	172.29.1.23	172.29.1.21	FTP-D…	1514	FTP Data: 1448 bytes (PORT) (STOR ./pub/Employee_Information.xls)
6511	209.464066	172.29.1.23	172.29.1.21	FTP-D…	1514	FTP Data: 1448 bytes (PORT) (STOR ./pub/Employee_Information.xls)
6513	209.464316	172.29.1.23	172.29.1.21	FTP-D…	1514	FTP Data: 1448 bytes (PORT) (STOR ./pub/Employee_Information.xls)

Question 2.2

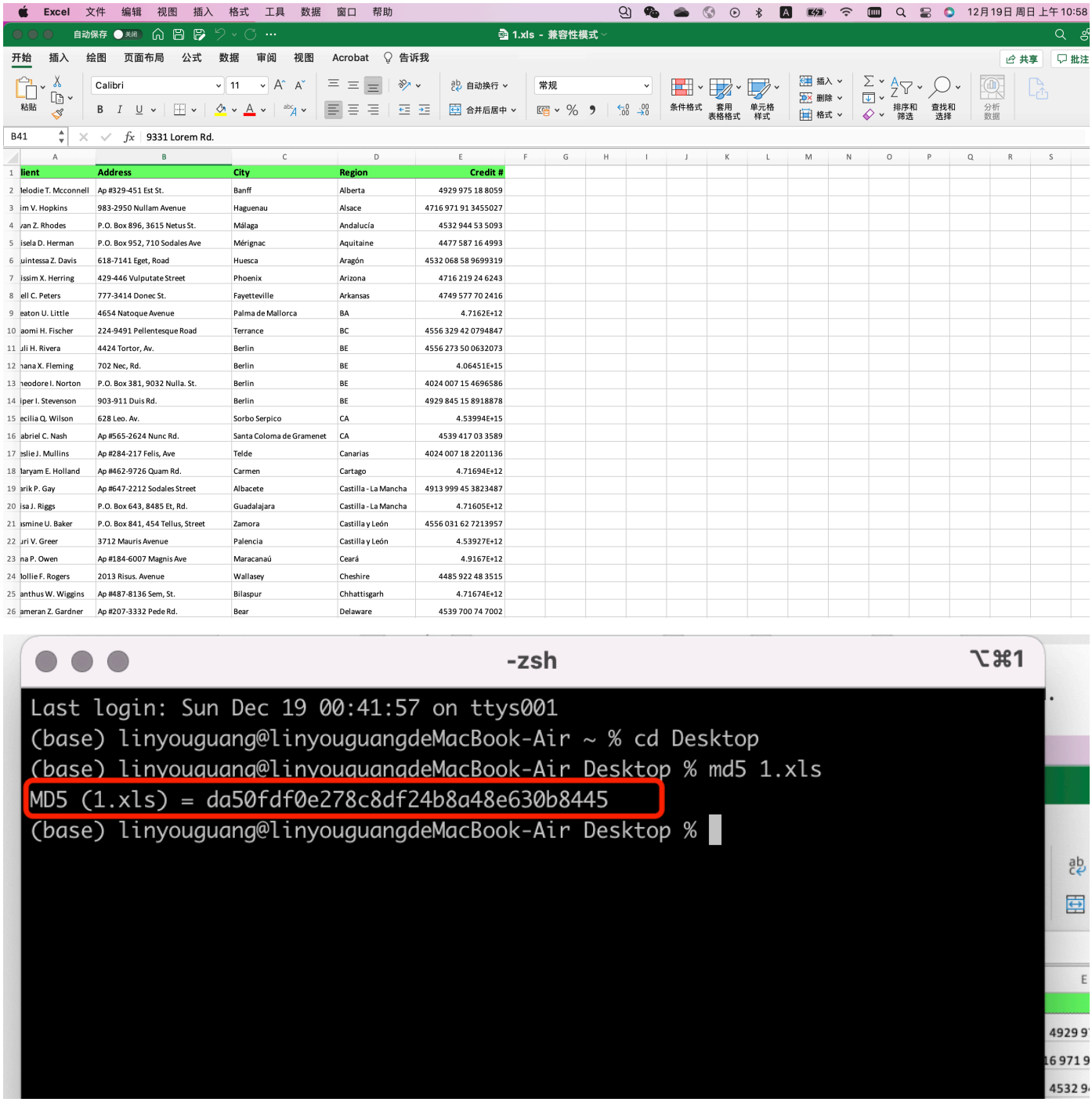
We use TCP stream to get the transmitted Information.



We save the raw stream as an Excel(.xls).



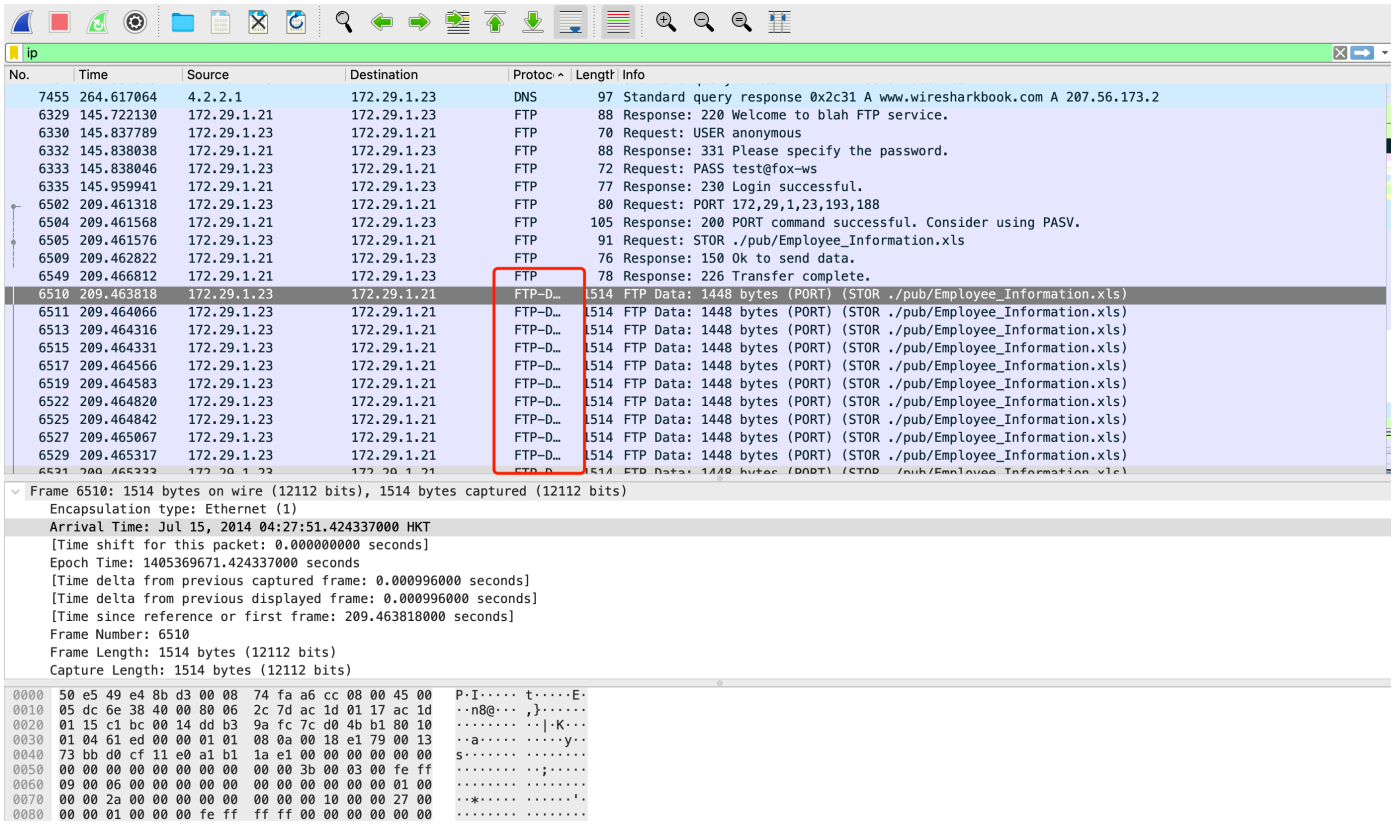
And then open it, we can see the stolen information.



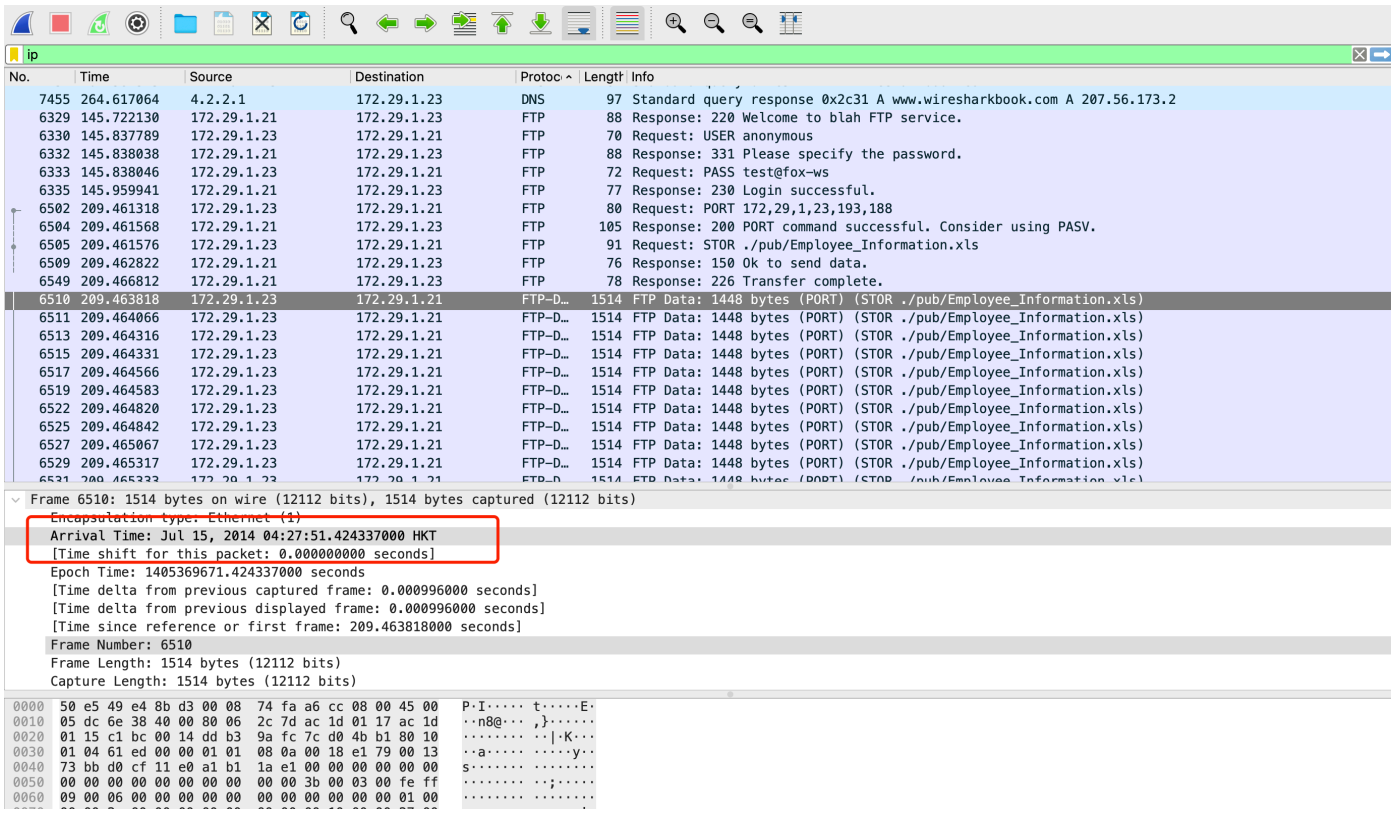
So the MD5 hash value of the stolen file is da50fdf0e278c8df24b8a48e630b8445.

Question 2.3

Next we go to find the when the file was stolen. The most straightforward is to find the time when the first file started to be transferred. Then, I found a set of FTP protocol actions just below the action.



We found the time in the content in Frame 6510



We found that the arrival time is July 15, 2014 04:27:51.424337000 HKT