

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

No.	Time	Source	Destination	Protocol	Length	Info
23	18.870898	192.168.1.158	64.12.24.50	SSL	60	Continuation Data
24	18.871477	64.12.24.50	192.168.1.158	TCP	60	443 → 51128 [ACK] Seq=1 Ack=7 Win=64240 Len=0
25	33.914966	192.168.1.158	64.12.24.50	SSL	243	Continuation Data
26	33.915486	64.12.24.50	192.168.1.158	TCP	60	443 → 51128 [ACK] Seq=1 Ack=196 Win=64240 Len=0
27	34.006599	192.168.1.158	64.12.24.50	SSL	94	Continuation Data
28	34.006604	64.12.24.50	192.168.1.158	TCP	60	443 → 51128 [ACK] Seq=1 Ack=236 Win=64240 Len=0
29	34.023247	64.12.24.50	192.168.1.158	SSL	263	Continuation Data
31	34.025537	64.12.24.50	192.168.1.158	SSL	92	Continuation Data
32	34.026804	192.168.1.158	64.12.24.50	TCP	60	51128 → 443 [ACK] Seq=236 Ack=210 Win=62780 Len=0
33	34.026809	192.168.1.158	64.12.24.50	TCP	60	51128 → 443 [ACK] Seq=236 Ack=248 Win=62742 Len=0
90	56.425051	192.168.1.158	239.255.255.250	SSDP	174	M-SEARCH * HTTP/1.1
91	57.42/165	192.168.1.158	239.255.255.250	SSDP	175	M-SEARCH * HTTP/1.1
92	58.458768	192.168.1.158	64.12.24.50	SSL	182	Continuation Data

> Frame 23: 60 bytes on wire (480 bits), 60 bytes captured (480 bits)
> Ethernet II, Src: HewlettP_45:a4:bb (00:12:79:a4:bb), Dst: VMware_b0:8d:62 (00:0c:29:b0:8d:62)
> Internet Protocol Version 4, Src: 192.168.1.158, Dst: 64.12.24.50
✓ Transmission Control Protocol, Src Port: 51128, Dst Port: 443, Seq: 1, Ack: 1, Len: 6
Source Port: 51128
Destination Port: 443
[Stream index: 2]
[Conversation completeness: Incomplete (12)]
[TCP Segment Len: 6]
Sequence Number: 1 (relative sequence number)
Sequence Number (raw): 862704323
[Next Sequence Number: 7 (relative sequence number)]
Acknowledgment Number: 1 (relative ack number)
Acknowledgment number (raw): 132735195

0000	00 0c 29 b0 8d 62 00 12	79 45 a4 bb 08 00 45 00	... b yE E
0010	00 2e ab 3b 40 06	75 0a c0 a8 01 9e 40 0c	.. ;@ u .. @
0020	18 32 c7 b8 01 bb 33 6b	d2 c3 07 e9 60 db 50 18	2 3k .. P
0030	f5 3c 3d 39 00 00 2a 05	00 60 00 00	<=9 * ..

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 (AIM) was an instant messaging and presence computer program created by AOL, which used the proprietary OSCAR instant messaging protocol and the TOC protocol to allow registered users to communicate in real time.

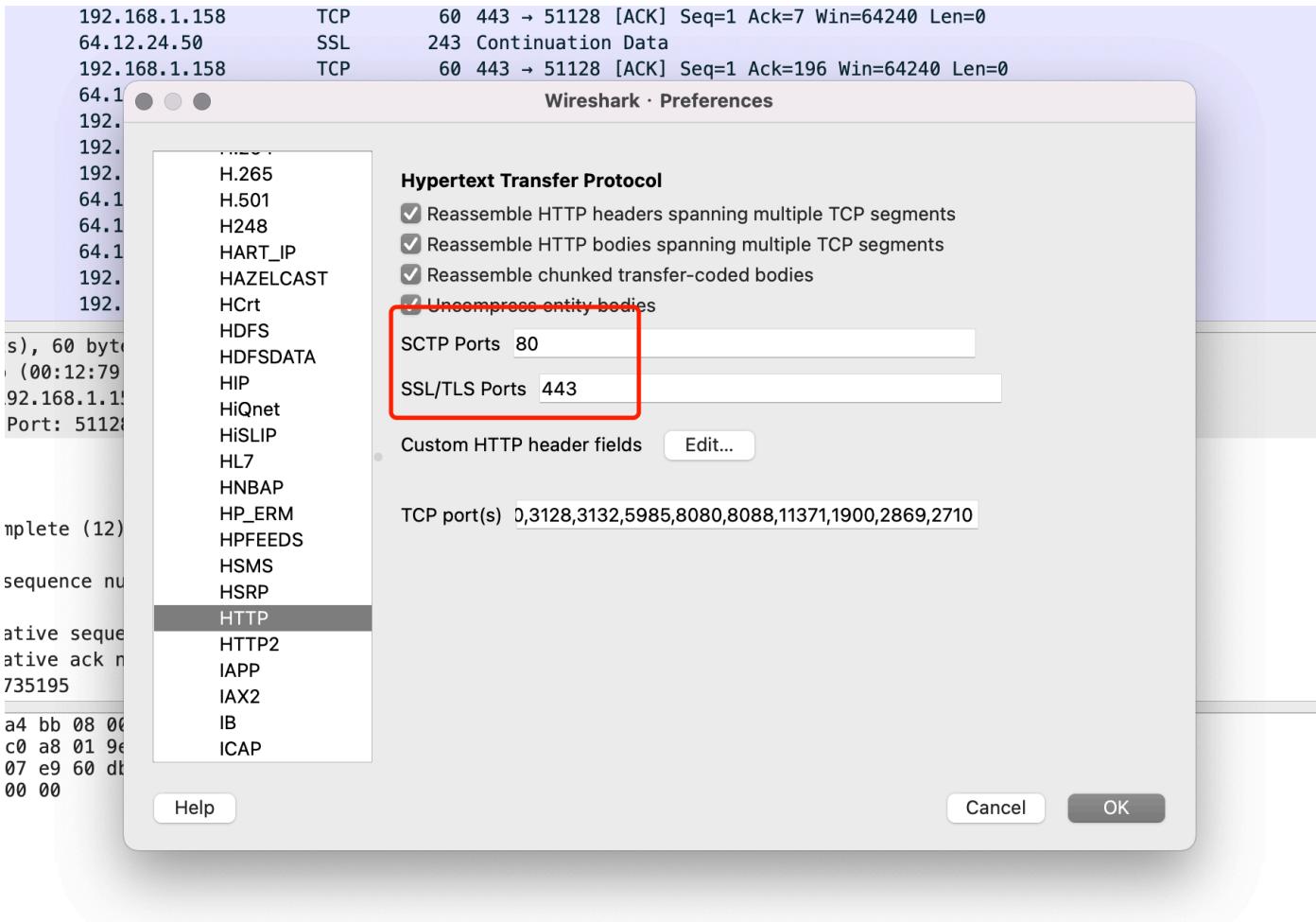
AIM (AOL Instant Messenger) was an instant messaging and presence computer program created by AOL, which used the proprietary OSCAR instant messaging protocol and the TOC protocol to allow registered users to communicate in real time.

[https://en.wikipedia.org/wiki/AIM_\(software\)](https://en.wikipedia.org/wiki/AIM_(software))

[AIM \(software\) - Wikipedia](#)

關於精選訊息摘錄 · 提供意見

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.

The screenshot shows the Wireshark interface with a context menu open over a selected AIM protocol entry. A sub-menu window titled 'Wireshark · Decode As...' is displayed, containing a table with one row. The table has columns for Field, Value, Type, Default, and Current. The 'Value' and 'Current' columns are both highlighted with red boxes. The 'Value' cell contains '443' and the 'Current' cell contains 'AIM'. Below the table are buttons for '+', '−', 'Copy from', 'Save', 'Cancel', and 'OK'. The path to the configuration file is shown as '/Users/linyouguang/config/wireshark/decode_as_entries'.

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

The screenshot shows the Wireshark packet list for stream 2. The AIM protocol is now correctly identified for all relevant packets. The first few entries are:

No.	Time	Source	Destination	Protocol	Length	Info
23	18.870898	192.168.1.158	64.12.24.50	AIM	60	Keep Alive
24	18.871477	64.12.24.50	192.168.1.158	TCP	60	443 → 51128 [ACK] Seq=1 Ack=7 Win=64240 Len=0
25	33.914966	192.168.1.158	64.12.24.50	AIM M...	243	AIM Messaging, Outgoing to: Sec558user1

Below the table, the analysis pane shows details for the selected AIM message, including source and destination ports, sequence numbers, and acknowledgment information.

Question 1.1

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

No.	Time	Source	Destination	Protocol	Length	Info
23	18.870898	192.168.1.158	64.12.24.50	AIM	60	Keep Alive
24	18.871477	64.12.24.50	192.168.1.158	TCP	60	443 → 51128 [ACK] Seq=1 Ack=7 Win=64240 Len=0
25	33.914966	192.168.1.158	64.12.24.50	AIM M...	243	AIM Messaging, Outgoing to: Sec558user1
26	33.915486	64.12.24.50	192.168.1.158	TCP	60	443 → 51128 [ACK] Seq=1 Ack=196 Win=64240 Len=0
27	34.006599	192.168.1.158	64.12.24.50	AIM M...	94	AIM Messaging, Mini Typing Notifications (MTN)
28	34.006604	64.12.24.50	192.168.1.158	TCP	60	443 → 51128 [ACK] Seq=1 Ack=236 Win=64240 Len=0
29	34.023247	64.12.24.50	192.168.1.158	AIM G...	263	AIM Generic, Rate Change
31	34.025537	64.12.24.50	192.168.1.158	AIM M...	92	AIM Messaging, Acknowledge
32	34.026804	192.168.1.158	64.12.24.50	TCP	60	51128 → 443 [ACK] Seq=236 Ack=210 Win=62780 Len=0
33	34.026809	192.168.1.158	64.12.24.50	TCP	60	51128 → 443 [ACK] Seq=236 Ack=248 Win=62742 Len=0
92	58.458768	192.168.1.158	64.12.24.50	AIM M...	182	AIM Messaging, Outgoing to: Sec558user1
93	58.461856	64.12.24.50	192.168.1.158	TCP	60	443 → 51128 [ACK] Seq=248 Ack=364 Win=64240 Len=0
94	58.568705	64.12.24.50	192.168.1.158	AIM G...	263	AIM Generic, Rate Change

✓ AOL Instant Messenger
 Command Start: 0x2a
 Channel ID: SNAC Data (0x02)
 Sequence Number: 97
 Data Field Length: 183

- > FNAC: Family: AIM Messaging (0x0004), Subtype: Outgoing (0x0006)
- ✓ AIM Messaging, Outgoing
 ICBM Cookie: 3436323837373800
 Message Channel ID: 0x0001
- ✓ Buddy: Sec558user1
 - Buddyname len: 11
 - Buddy Name: Sec558user1
- ✓ TLV: Message Block
- > TLV: Server Ack Requested

```

0000 00 0c 29 b0 8d 62 00 12 79 45 a4 bb 08 00 45 00  ... ) b... yE...E...
0010 00 e5 ab 3c 40 00 40 06 74 52 c0 a8 01 9e 40 0c  ...<@ @. tR...@.
0020 18 32 c7 b8 01 bb 33 6b d2 c9 07 e9 60 db 50 18  .2...3k ...P...
0030 f5 3c d0 8c 00 00 2a 02 00 61 00 b7 00 04 00 06  <...* a.....

```

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 >:-)

No.	Time	Source	Destination	Protocol	Length	Info
23	18.870898	192.168.1.158	64.12.24.50	AIM	60	Keep Alive
24	18.871477	64.12.24.50	192.168.1.158	TCP	60	443 → 51128 [ACK] Seq=1 Ack=7 Win=64240 Len=0
25	33.914966	192.168.1.158	64.12.24.50	AIM M...	243	AIM Messaging, Outgoing to: Sec558user1
26	33.915486	64.12.24.50	192.168.1.158	TCP	60	443 → 51128 [ACK] Seq=1 Ack=196 Win=64240 Len=0
27	34.006599	192.168.1.158	64.12.24.50	AIM M...	94	AIM Messaging, Mini Typing Notifications (MTN)
28	34.006604	64.12.24.50	192.168.1.158	TCP	60	443 → 51128 [ACK] Seq=1 Ack=236 Win=64240 Len=0
29	34.023247	64.12.24.50	192.168.1.158	AIM G...	263	AIM Generic, Rate Change
31	34.025537	64.12.24.50	192.168.1.158	AIM M...	92	AIM Messaging, Acknowledge
32	34.026804	192.168.1.158	64.12.24.50	TCP	60	51128 → 443 [ACK] Seq=236 Ack=210 Win=62780 Len=0
33	34.026809	192.168.1.158	64.12.24.50	TCP	60	51128 → 443 [ACK] Seq=236 Ack=248 Win=62742 Len=0
92	58.458768	192.168.1.158	64.12.24.50	AIM M...	182	AIM Messaging, Outgoing to: Sec558user1
93	58.461856	64.12.24.50	192.168.1.158	TCP	60	443 → 51128 [ACK] Seq=248 Ack=364 Win=64240 Len=0
94	58.568705	64.12.24.50	192.168.1.158	AIM G...	263	AIM Generic, Rate Change

Sequence Number: 97
 Data Field Length: 183

> FNAC: Family: AIM Messaging (0x0004), Subtype: Outgoing (0x0006)

✓ AIM Messaging, Outgoing
 ICBM Cookie: 3436323837373800
 Message Channel ID: 0x0001

✓ Buddy: Sec558user1

- Buddyname len: 11
- Buddy Name: Sec558user1

✓ TLV: Message Block

- Value ID: Message Block (0x0002)
- Length: 143

> 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 >:-)

✓ TLV: Server Ack Requested

```

0000 00 00 29 b0 8d 62 00 12 79 45 a4 bb 08 00 45 00  ... ) b... yE...E...
0010 00 e5 ab 3c 40 00 40 06 74 52 c0 a8 01 9e 40 0c  ...<@ @. tR...@.
0020 18 32 c7 b8 01 bb 33 6b d2 c9 07 e9 60 db 50 18  .2...3k ...P...
0030 f5 3c d0 8c 00 00 2a 02 00 61 00 b7 00 04 00 06  <...* a.....
0040 00 00 00 00 00 45 34 36 32 38 37 37 38 00 00 01  ....E46 28778...
0050 0b 53 63 35 35 38 75 73 65 72 31 00 02 00 8f  .Sec558user1...
0060 05 01 00 04 01 01 02 01 01 00 83 00 00 00 00  .....
0070 48 65 72 65 27 73 20 74 68 65 20 73 65 63 72 65  Here's t he secre
0080 74 20 72 65 63 69 70 65 2e 2e 20 49 20 6a 75  t recipe ... I ju
0090 73 74 20 64 6f 77 6e 6c 6f 61 64 65 64 20 69 74  st downl oaded it
00a0 20 66 72 65 6d 20 74 68 65 20 66 69 6c 65 20 73  from th e file s
00b0 65 72 76 65 72 2e 20 4a 75 73 74 20 63 6f 70 79  erver. J ust copy
00c0 20 74 6f 20 61 20 74 68 75 6d 62 20 64 72 69 76  to a th umb driv
00d0 65 20 61 6a 64 20 79 6f 75 27 77 65 20 67 6f 6f  e and vo u're goo

```

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



The screenshot shows a NetworkMiner capture window. The main pane displays a sequence of network packets. A red box highlights the word 'recipe.docx' in the payload of a packet from host Sec558user1 to host F.CL. The packet number is 104. The payload contains HTML code related to a secret recipe download. Below the main pane, there are several status and control buttons: 'client pkts, 13 server pkts, 5 turns.', 'Entire conversation (2023 bytes)', 'Show data as ASCII', 'Stream 2', 'Find Next', and a 'Find' input field.

Question 1.4

Docx Magic number is 50 4B 03 04.

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

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
Postscript 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

The screenshot shows the Wireshark interface with a context menu open over a selected packet. A red box highlights the "Save Stream Content As..." option, which has brought up a save dialog window. The dialog window has the following fields:

- Save As:** recipe.bin
- Tags:** (empty)
- Where:** Desktop
- Buttons:** Cancel and Save

The background of the Wireshark window shows a large amount of captured data, including XML fragments and binary file contents. The XML includes elements like `fontTable.xml`, `wordSettings.xml`, and `docProps/app.xml`. The binary content appears as a series of hex and ASCII characters.

Storing the file in the local storage.

Recipe for Disaster:

1 serving

Ingredients:

4 cups sugar

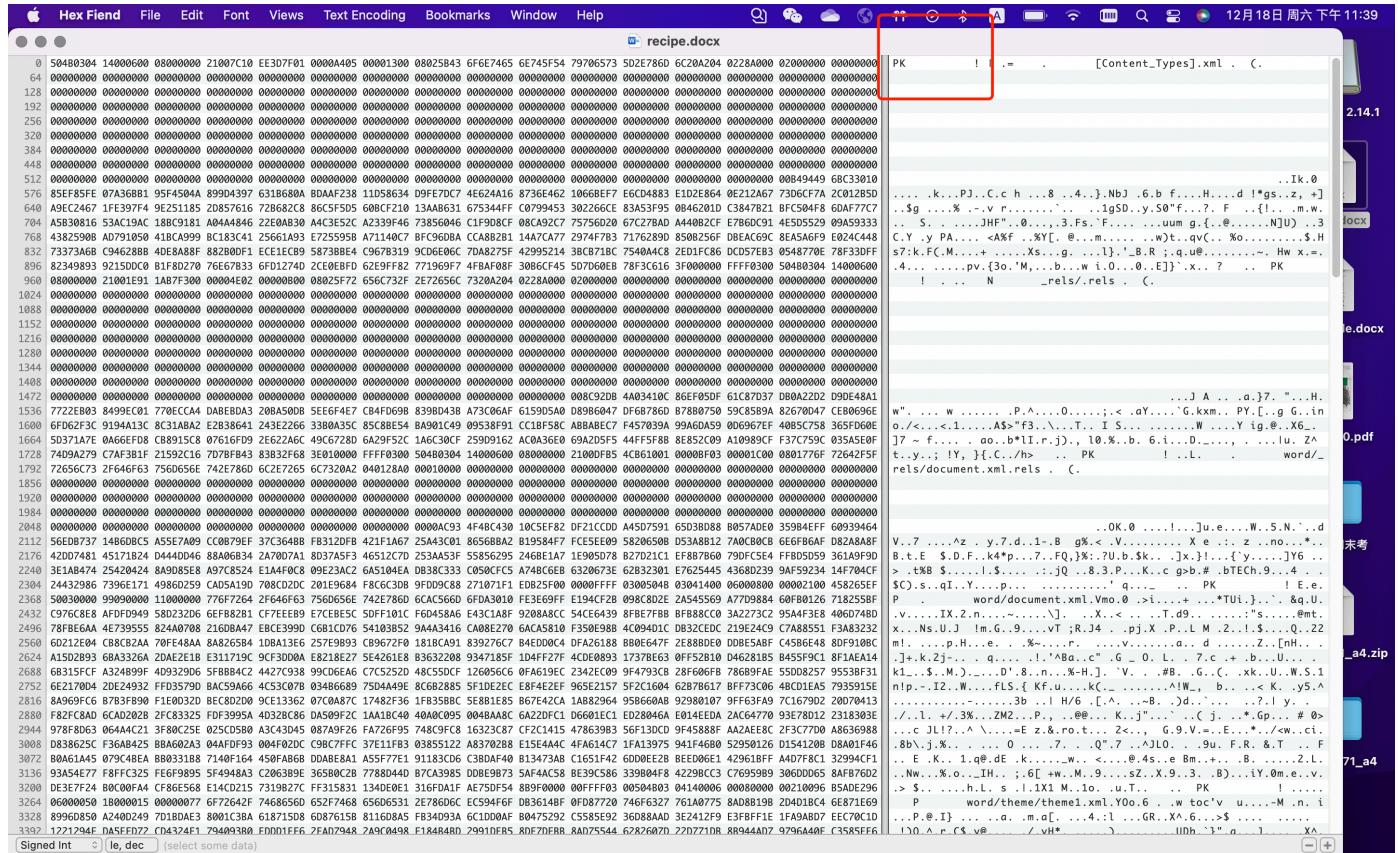
2 cups water

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.

```

1155169171_04      5520 页 科
1155169171_a4.zip  5709 课件+笔记
5320 Pre           5710sample.docx
5320打印          5820 Project
5320论文          5830作业
(base) linyouguang@linyouguangdeMacBook-Air Desktop % cd De
cd: no such file or directory: De
(base) linyouguang@linyouguangdeMacBook-Air Desktop % md5 recipe.docx
MD5 (recipe.docx) = 8350582774e1d4dbe1d61d64c89e0ea1
(base) linyouguang@linyouguangdeMacBook-Air Desktop %

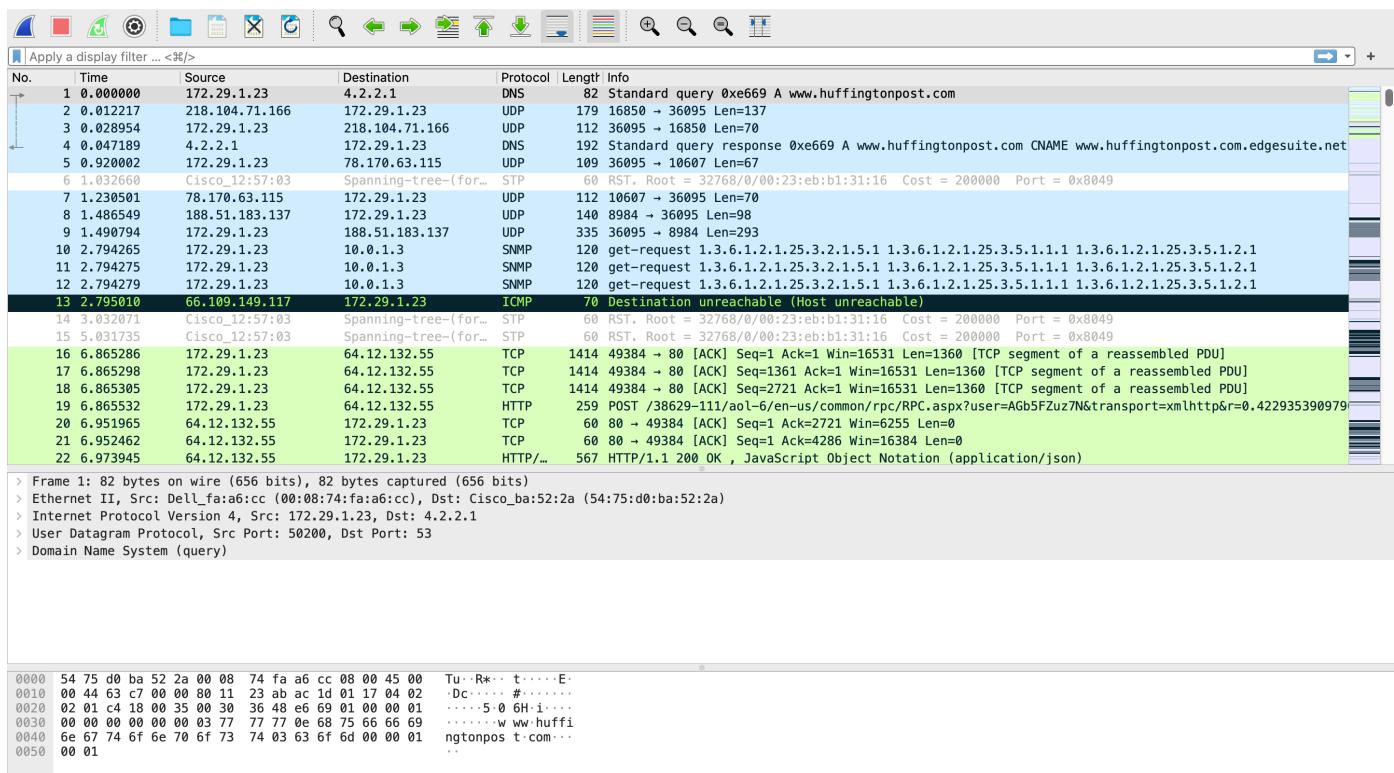
```

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.

No.	Time	Source	Destination	Protocol	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)
6522	209.464920	172.29.1.23	172.29.1.21	FTP-D...	1514	FTP Data: 1448 bytes (PORT) (STOR ./pub/Employee_Information.xls)

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	172.29.1.23	172.29.1.21	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)
6522	209.464920	172.29.1.23	172.29.1.21	FTP-D...	1514	FTP Data: 1448 bytes (PORT) (STOR ./pub/Employee_Information.xls)

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.

No.	Time	Source	Destination	Protocol	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	172.29.1.23	172.29.1.21	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)

Question 2.2

We use TCP stream to get the transmitted Information.

The screenshot shows a Wireshark interface with a list of captured packets on the left and detailed packet information on the right. A context menu is open over a selected packet, specifically over the 'Follow' option in the list of protocols. The 'TCP Stream' option is highlighted. The right pane shows the raw bytes of the selected packet.

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

The screenshot shows the 'Save Stream Content As...' dialog in Wireshark. The 'Save As:' field is set to '1.xls'. The 'Where:' dropdown shows 'Downloads'. The 'Save' button is highlighted. The background shows the raw hex dump of the selected TCP stream.

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

	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S
Client	Address	City	Region	Credit #															
1 Melodie T. McConnell	Ap #329-451 Est St.	Banff	Alberta	4929 975 18 8059															
2 Jim V. Hopkins	983-2950 Nullam Avenue	Haguenau	Alsace	4716 971 91 3455027															
3 Ivan Z. Rhodes	P.O. Box 896, 3615 Netus St.	Málaga	Andalucía	4532 944 53 5093															
4 Isela D. Herman	P.O. Box 552, 710 Sodales Ave	Mérignac	Aquitaine	4477 587 16 4993															
5 Quintessa Z. Davis	618-7141 Eget, Road	Huesca	Aragón	4532 068 58 9699219															
6 Issim X. Herring	429-446 Vulputate Street	Phoenix	Arizona	4716 219 24 6243															
7 Dell C. Peters	777-3414 Donec St.	Fayetteville	Arkansas	4749 577 70 2416															
8 Eaton U. Little	4654 Natoque Avenue	Palma de Mallorca	BA	4.7162E+12															
9 Naomi H. Fischer	224-9491 Pellentesque Road	Terrance	BC	4556 329 42 0794847															
10 Jili H. Rivera	4424 Tortor, Av.	Berlin	BE	4556 273 50 0632073															
11 Anna X. Fleming	702 Nec, Rd.	Berlin	BE	4.06451E+15															
12 Theodore I. Norton	P.O. Box 381, 9032 Nulla. St.	Berlin	BE	4024 007 15 4696586															
13 Ioper I. Stevenson	903-911 Duis Rd.	Berlin	BE	4929 845 15 8918878															
14 Cecilia Q. Wilson	628 Leo. Av.	Sorbo Serpico	CA	4.53994E+15															
15 Gabriel C. Nash	Ap #55-2624 Nunc Rd.	Santa Coloma de Gramenet	CA	4539 417 03 3589															
16 Leslie J. Mullins	Ap #284-217 Felis, Ave	Telde	Canarias	4024 007 18 2201136															
17 Taryam E. Holland	Ap #462-9726 Quam Rd.	Carmen	Cartago	4.71694E+12															
18 Irak P. Gay	Ap #647-2122 Sodales Street	Albacete	Castilla - La Mancha	4913 999 45 3823487															
19 Isaac J. Riggs	P.O. Box 643, 8485 Et, Rd.	Guadalajara	Castilla - La Mancha	4.71605E+12															
20 Jasmine U. Baker	P.O. Box 841, 454 Tellus, Street	Zamora	Castilla y León	4556 031 62 7213957															
21 Juri V. Greer	3712 Mauris Avenue	Palencia	Castilla y León	4.53927E+12															
22 Anna P. Owen	Ap #184-6007 Magnis Ave	Maracanáú	Ceará	4.9167E+12															
23 Hollie F. Rogers	2013 Risus. Avenue	Wallasey	Cheshire	4485 922 48 3515															
24 Anthus W. Wiggins	Ap #487-8136 Sem, St.	Bilaspur	Chhattisgarh	4.71674E+12															
25 Amerian Z. Gardner	Ap #207-3332 Pede Rd.	Bear	Delaware	4539 700 74 7002															

```
Last login: Sun Dec 19 00:41:57 on ttys001
(base) linyouguang@linyouguangdeMacBook-Air ~ % cd Desktop
(base) linyouguang@linyouguangdeMacBook-Air Desktop % md5 1.xls
MD5 (1.xls) = da50fdf0e278c8df24b8a48e630b8445
(base) linyouguang@linyouguangdeMacBook-Air Desktop %
```

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.

No.	Time	Source	Destination	Protocol	Length	Info
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-DATA	1514	FTP Data: 1448 bytes (PORT) (STOR ./pub/Employee_Information.xls)
6511	209.464066	172.29.1.23	172.29.1.21	FTP-DATA	1514	FTP Data: 1448 bytes (PORT) (STOR ./pub/Employee_Information.xls)
6513	209.464316	172.29.1.23	172.29.1.21	FTP-DATA	1514	FTP Data: 1448 bytes (PORT) (STOR ./pub/Employee_Information.xls)
6515	209.464331	172.29.1.23	172.29.1.21	FTP-DATA	1514	FTP Data: 1448 bytes (PORT) (STOR ./pub/Employee_Information.xls)
6517	209.464566	172.29.1.23	172.29.1.21	FTP-DATA	1514	FTP Data: 1448 bytes (PORT) (STOR ./pub/Employee_Information.xls)
6519	209.464583	172.29.1.23	172.29.1.21	FTP-DATA	1514	FTP Data: 1448 bytes (PORT) (STOR ./pub/Employee_Information.xls)
6522	209.464820	172.29.1.23	172.29.1.21	FTP-DATA	1514	FTP Data: 1448 bytes (PORT) (STOR ./pub/Employee_Information.xls)
6525	209.464842	172.29.1.23	172.29.1.21	FTP-DATA	1514	FTP Data: 1448 bytes (PORT) (STOR ./pub/Employee_Information.xls)
6527	209.465067	172.29.1.23	172.29.1.21	FTP-DATA	1514	FTP Data: 1448 bytes (PORT) (STOR ./pub/Employee_Information.xls)
6529	209.465317	172.29.1.23	172.29.1.21	FTP-DATA	1514	FTP Data: 1448 bytes (PORT) (STOR ./pub/Employee_Information.xls)
6531	209.465322	172.29.1.23	172.29.1.21	FTP-DATA	1514	FTP Data: 1448 bytes (PORT) (STOR ./pub/Employee_Information.xls)

Frame 6510: 1514 bytes on wire (12112 bits), 1514 bytes captured (12112 bits)

Encapsulation type: Ethernet (1)

Arrival Time: Jul 15, 2014 04:27:51.424337000 HKT

[Time shift for this packet: 0.000000000 seconds]

Epoch Time: 1405369671.424337000 seconds

[Time delta from previous captured frame: 0.000096000 seconds]

[Time delta from previous displayed frame: 0.000096000 seconds]

[Time since reference or first frame: 209.463818000 seconds]

Frame Number: 6510

Frame Length: 1514 bytes (12112 bits)

Capture Length: 1514 bytes (12112 bits)

```
0000  50 e5 49 e4 8b d3 00 08  74 fa a6 cc 08 00 45 00  P·I..... t.....E·
0010  05 dc 6e 38 40 00 80 06  2c 7d ac 1d 01 17 ac 1d  ..n@... ,} ,|K...
0020  01 15 c1 bc 00 14 dd b3  9a fc 7c d0 4b b1 80 10  ..a..... ..y...
0030  01 04 61 ed 00 00 01 01  08 0a 00 18 e1 79 00 13  s..... .
0040  73 bb d0 cf 11 e0 a1 b1  1a c1 00 00 00 00 00 00 00  ..;....;
0050  00 00 00 00 00 00 00 00  00 00 3b 00 03 00 fe ff  ....;....;
0060  09 00 06 00 00 00 00 00  00 00 00 00 00 00 01 00  ....;....;
0070  00 00 2a 00 00 00 00 00  00 00 00 10 00 00 27 00  ....;....;
0080  00 00 01 00 00 00 00 fe ff ff ff 00 00 00 00 00 00 00  ....;....;
```

We found the time in the content in Frame 6510

No.	Time	Source	Destination	Protocol	Length	Info
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-DATA	1514	FTP Data: 1448 bytes (PORT) (STOR ./pub/Employee_Information.xls)
6511	209.464066	172.29.1.23	172.29.1.21	FTP-DATA	1514	FTP Data: 1448 bytes (PORT) (STOR ./pub/Employee_Information.xls)
6513	209.464316	172.29.1.23	172.29.1.21	FTP-DATA	1514	FTP Data: 1448 bytes (PORT) (STOR ./pub/Employee_Information.xls)
6515	209.464331	172.29.1.23	172.29.1.21	FTP-DATA	1514	FTP Data: 1448 bytes (PORT) (STOR ./pub/Employee_Information.xls)
6517	209.464566	172.29.1.23	172.29.1.21	FTP-DATA	1514	FTP Data: 1448 bytes (PORT) (STOR ./pub/Employee_Information.xls)
6519	209.464583	172.29.1.23	172.29.1.21	FTP-DATA	1514	FTP Data: 1448 bytes (PORT) (STOR ./pub/Employee_Information.xls)
6522	209.464820	172.29.1.23	172.29.1.21	FTP-DATA	1514	FTP Data: 1448 bytes (PORT) (STOR ./pub/Employee_Information.xls)
6525	209.464842	172.29.1.23	172.29.1.21	FTP-DATA	1514	FTP Data: 1448 bytes (PORT) (STOR ./pub/Employee_Information.xls)
6527	209.465067	172.29.1.23	172.29.1.21	FTP-DATA	1514	FTP Data: 1448 bytes (PORT) (STOR ./pub/Employee_Information.xls)
6529	209.465317	172.29.1.23	172.29.1.21	FTP-DATA	1514	FTP Data: 1448 bytes (PORT) (STOR ./pub/Employee_Information.xls)
6531	209.465322	172.29.1.23	172.29.1.21	FTP-DATA	1514	FTP Data: 1448 bytes (PORT) (STOR ./pub/Employee_Information.xls)

Frame 6510: 1514 bytes on wire (12112 bits), 1514 bytes captured (12112 bits)

Encapsulation type: Ethernet (1)

Arrival Time: Jul 15, 2014 04:27:51.424337000 HKT

[Time shift for this packet: 0.000000000 seconds]

Epoch Time: 1405369671.424337000 seconds

[Time delta from previous captured frame: 0.000096000 seconds]

[Time delta from previous displayed frame: 0.000096000 seconds]

[Time since reference or first frame: 209.463818000 seconds]

Frame Number: 6510

Frame Length: 1514 bytes (12112 bits)

Capture Length: 1514 bytes (12112 bits)

```
0000  50 e5 49 e4 8b d3 00 08  74 fa a6 cc 08 00 45 00  P·I..... t.....E·
0010  05 dc 6e 38 40 00 80 06  2c 7d ac 1d 01 17 ac 1d  ..n@... ,} ,|K...
0020  01 15 c1 bc 00 14 dd b3  9a fc 7c d0 4b b1 80 10  ..a..... ..y...
0030  01 04 61 ed 00 00 01 01  08 0a 00 18 e1 79 00 13  s..... .
0040  73 bb d0 cf 11 e0 a1 b1  1a c1 00 00 00 00 00 00 00 00  ..;....;
0050  00 00 00 00 00 00 00 00  00 00 3b 00 03 00 fe ff  ....;....;
0060  09 00 06 00 00 00 00 00  00 00 00 00 00 00 00 01 00  ....;....;
```

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