PACKET CAPTURE ANALYSIS REPORT: - DANIEL LODI

BACKGROUND:

Suspicious network activity has been detected coming from a user on the ANZ network.

A laptop had been flagged up on our security systems due to suspicious internet traffic, and the company needed to investigate the network traffic in order to establish what the user accessed and downloaded.

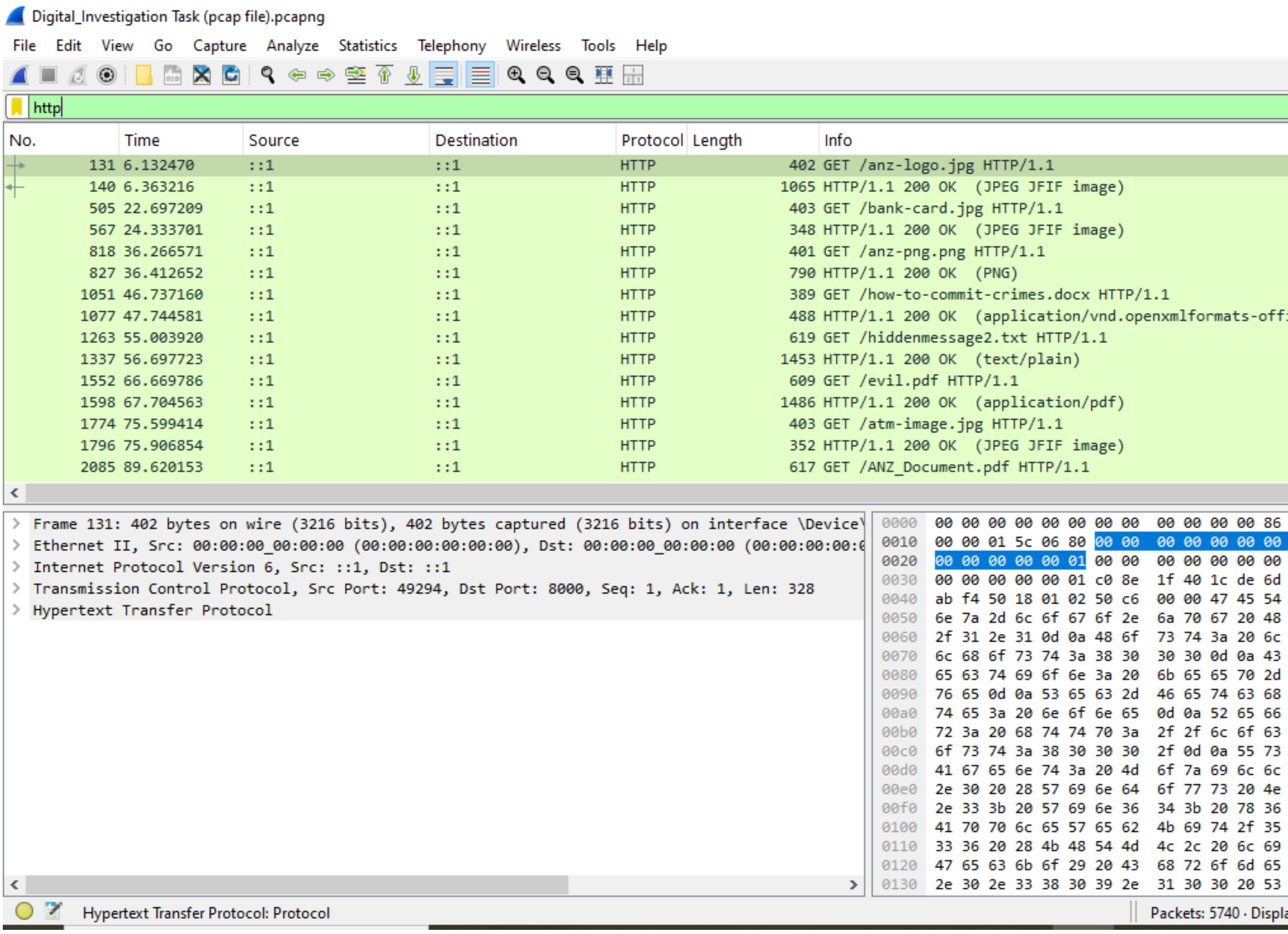
My task was to examine their network activity and gather whatever information I could on what images they viewed and what files they accessed.

I have been provided with a packet capture file (pcap) containing all their recent network activity. There may be a number of artifacts contained within the packet capture file, and I was expected to identify and report as many as possible.

SUBTASK 1:

Investigating the images

To find the images the user accessed called **anz-logo.jpg** and **bank-card.jpg** I followed the following process for both images:


Digital_Investigation Task (pcap file).pcapng
File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help

```
http
```

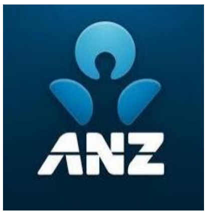
```
No.       Time        Source     Destination  Protocol Length  Info
    131 6.132470     ::1         ::1          HTTP        402 GET /anz-logo.jpg HTTP/1.1
    140 6.363216     ::1         ::1          HTTP       1065 HTTP/1.1 200 OK  (JPEG JFIF image)
    505 22.697209    ::1         ::1          HTTP        403 GET /bank-card.jpg HTTP/1.1
    567 24.333701    ::1         ::1          HTTP        348 HTTP/1.1 200 OK  (JPEG JFIF image)
    818 36.266571    ::1         ::1          HTTP        401 GET /anz-png.png HTTP/1.1
    827 36.412652    ::1         ::1          HTTP        790 HTTP/1.1 200 OK  (PNG)
   1051 46.737160    ::1         ::1          HTTP        389 GET /how-to-commit-crimes.docx HTTP/1.1
   1077 47.744581    ::1         ::1          HTTP        488 HTTP/1.1 200 OK  (application/vnd.openxmlformats-offi
   1263 55.003920    ::1         ::1          HTTP        619 GET /hiddenmessage2.txt HTTP/1.1
   1337 56.697723    ::1         ::1          HTTP       1453 HTTP/1.1 200 OK  (text/plain)
   1552 66.669786    ::1         ::1          HTTP        609 GET /evil.pdf HTTP/1.1
   1598 67.704563    ::1         ::1          HTTP       1486 HTTP/1.1 200 OK  (application/pdf)
   1774 75.599414    ::1         ::1          HTTP        403 GET /atm-image.jpg HTTP/1.1
   1796 75.906854    ::1         ::1          HTTP        352 HTTP/1.1 200 OK  (JPEG JFIF image)
   2085 89.620153    ::1         ::1          HTTP        617 GET /ANZ_Document.pdf HTTP/1.1
```

```
> Frame 131: 402 bytes on wire (3216 bits), 402 bytes captured (3216 bits) on interface \Device\
> Ethernet II, Src: 00:00:00_00:00:00 (00:00:00:00:00:00), Dst: 00:00:00_00:00:00 (00:00:00:00:0
> Internet Protocol Version 6, Src: ::1, Dst: ::1
> Transmission Control Protocol, Src Port: 49294, Dst Port: 8000, Seq: 1, Ack: 1, Len: 328
> Hypertext Transfer Protocol
```

```
0000  00 00 00 00 00 00 00 00  00 00 00 00 86
0010  00 00 01 5c 06 80 00 00  00 00 00 00 00
0020  00 00 00 00 00 01 00 00  00 00 00 00 00
0030  00 00 00 00 00 01 c0 8e  1f 40 1c de 6d
0040  ab f4 50 18 01 02 50 c6  00 00 47 45 54
0050  6e 7a 2d 6c 6f 67 6f 2e  6a 70 67 20 48
0060  2f 31 2e 31 0d 0a 48 6f  73 74 3a 20 6c
0070  6c 68 6f 73 74 3a 38 30  30 30 0d 0a 43
0080  65 63 74 69 6f 6e 3a 20  6b 65 65 70 2d
0090  76 65 0d 0a 53 65 63 2d  46 65 74 63 68
00a0  74 65 3a 20 6e 6f 6e 65  0d 0a 52 65 66
00b0  72 3a 20 68 74 74 70 3a  2f 2f 6c 6f 63
00c0  6f 73 74 3a 38 30 30 30  2f 0d 0a 55 73
00d0  41 67 65 6e 74 3a 20 4d  6f 7a 69 6c 6c
00e0  2e 30 20 28 57 69 6e 64  6f 77 73 20 4e
00f0  2e 33 3b 20 57 69 6e 36  34 3b 20 78 36
0100  41 70 70 6c 65 57 65 62  4b 69 74 2f 35
0110  33 36 20 28 4b 48 54 4d  4c 2c 20 6c 69
0120  47 65 63 6b 6f 29 20 43  68 72 6f 6d 65
0130  2e 30 2e 33 38 30 39 2e  31 30 30 20 53
```

First I filtered the packet capture for **http** traffic and looked through the remaining packets for the **GET request** that downloaded the image. I then **right clicked the image and followed its TCP stream**. In the TCP stream I saw what looked like image data. In order to view the data in hex format, I changed the **view to 'raw'**, and then searched the hex data for **a jpeg's file signature**. After finding the file signature **"FFD8"** the top, and the file footer **"FFD9"** at the bottom, I copied everything between those two points into the **hex editor HxD** and saved it as a jpg image. This was the image I found for

anz-logo.jpg:



bank-card.jpg:

SUB-TASK 2:

Finding Documents and text file the user viewed and downloaded.

In order to find the contents of the document, I had to view the TCP stream of the http get request for the file. The documents contents were visible in the ascii view.

The full document contained the message:

- Step 1: Find target
- Step 2: Hack them This is a suspicious document.

SUBTASK 3:

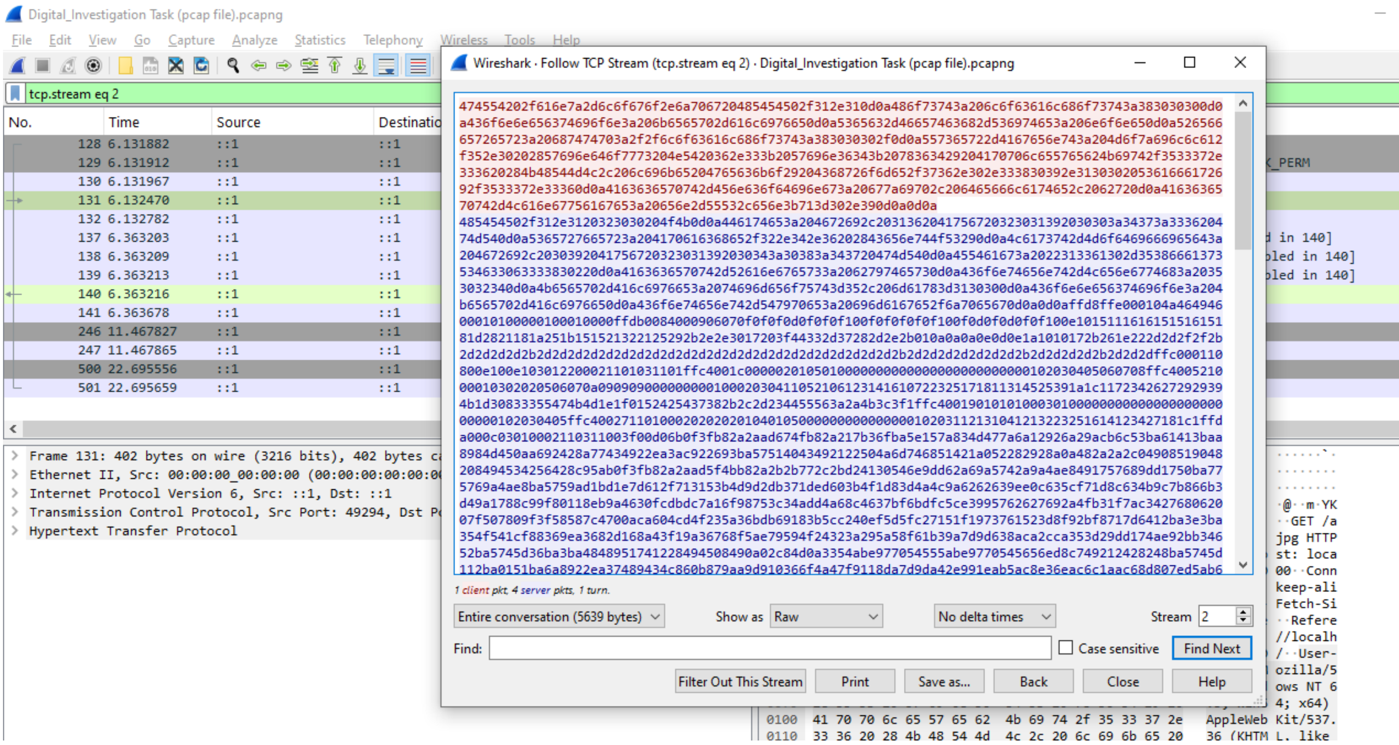
Investigating the PDFs

In order to view these PDF's I viewed the TCP stream as usual, and found the file signature for a PDF, which was the hex data "25 50 44 46". I noticed in the ascii view that the PDF data went until the very end of the TCP stream, so I copied all the hex date from the file signature onwards into HxD and saved it as a pdf file. The same process worked for all three files:

- ✓ Document.pdf
- ✓ Document2.pdf
- ✓ Securepdf.pdf

Screenshots:

1. Following TCP Stream



Digital_Investigation Task (pcap file).pcapng

File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help

tcp.stream eq 2

```
No.  Time       Source  Destinatio
128 6.131882    ::1     ::1
129 6.131912    ::1     ::1
130 6.131967    ::1     ::1
131 6.132470    ::1     ::1
132 6.132782    ::1     ::1
137 6.363203    ::1     ::1
138 6.363209    ::1     ::1
139 6.363213    ::1     ::1
140 6.363216    ::1     ::1
141 6.363678    ::1     ::1
246 11.467827   ::1     ::1
247 11.467865   ::1     ::1
500 22.695556   ::1     ::1
501 22.695659   ::1     ::1
```

```
> Frame 131: 402 bytes on wire (3216 bits), 402 bytes ca
> Ethernet II, Src: 00:00:00_00:00:00 (00:00:00:00:00:0
> Internet Protocol Version 6, Src: ::1, Dst: ::1
> Transmission Control Protocol, Src Port: 49294, Dst Po
> Hypertext Transfer Protocol
```

```
K_PERM
d in 140]
bled in 140]
bled in 140]
```

```
......`.
........
........
.@..m.YK
..GET /a
jpg HTTP
st: loca
00..Conn
keep-ali
Fetch-Si
..Refere
//localh
/..User-
ozilla/5
ows NT 6
4; x64)
0100  41 70 70 6c 65 57 65 62  4b 69 74 2f 35 33 37 2e   AppleWeb Kit/537.
0110  33 36 20 28 4b 48 54 4d  4c 2c 20 6c 69 6b 65 20   36 (KHTM L, like
```

Wireshark · Follow TCP Stream (tcp.stream eq 2) · Digital_Investigation Task (pcap file).pcapng

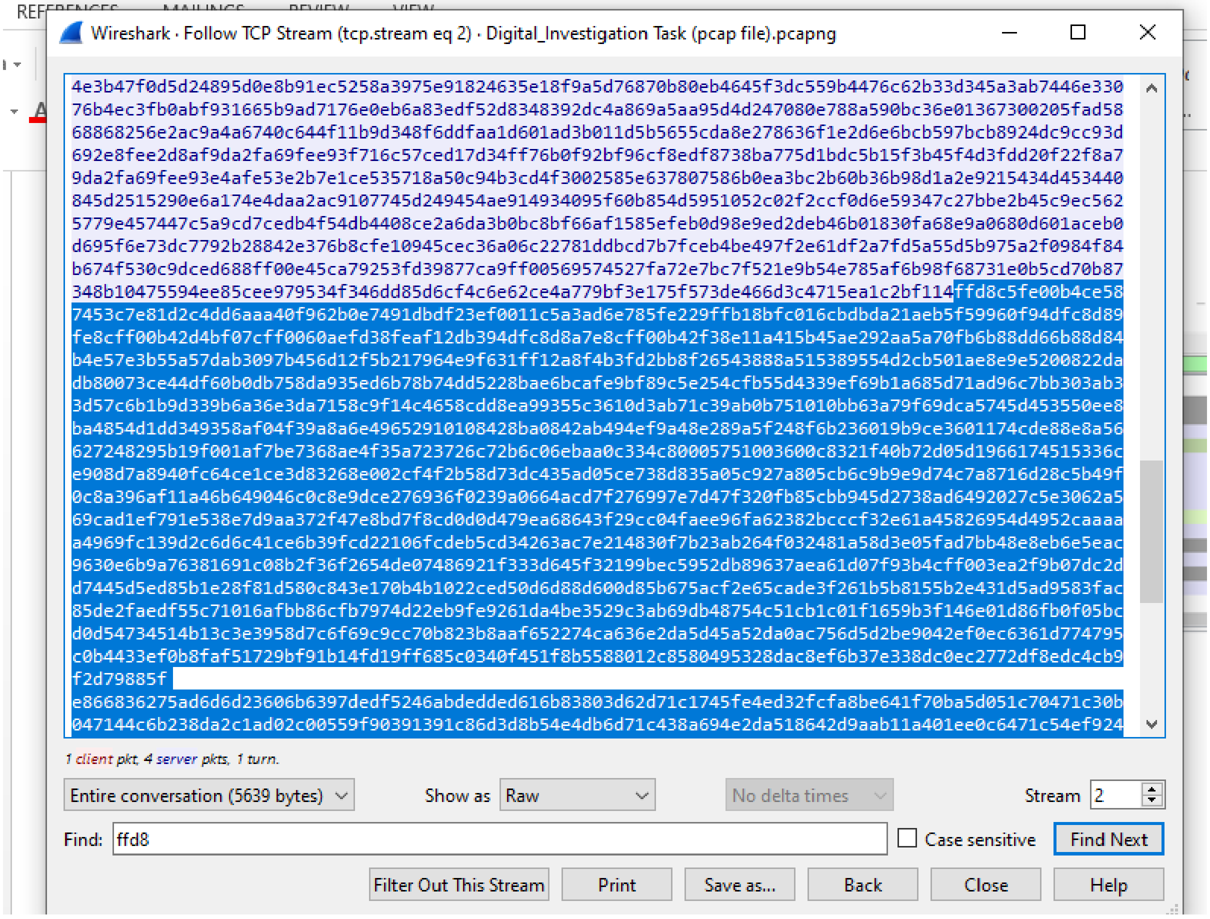
```
474554202f616e7a2d6c6f676f2e6a706720485454502f312e310d0a486f73743a206c6f63616c686f73743a383030300d0
a436f6e6e656374696f6e3a206b6565702d616c6976650d0a5365632d46657463682d536974653a206e6f6e650d0a526566
657265723a20687474703a2f2f6c6f63616c686f73743a383030302f0d0a557365722d4167656e743a204d6f7a696c6c612
f352e30202857696e646f7773204e5420362e333b2057696e36343b207836342920417070c655765624b69742f3533372e
33362028284b48544d4c2c206c696b65204765636b6f29204368726f6d652f37362e302e333830392e31303205361666172
692f3533372e33360d0a4163636570742d456e636f64696e673a20677a69702c206465666c6174652c2062720d0a41636365
70742d4c616e67756167653a20656e2d55532c656e3b713d302e390d0a0d0a
485454502f312e3120323030204f4b0d0a446174653a204672692c2031362041756720323031392030303a34373a3336204
74d540d0a5365727665723a204170616368652f322e342e3620284656e744f53290d0a4c6173742d4d6f64696669656643a
204672692c203039204175672032303139203030343a30383a343720474d540d0a455461673a202231361302d3538666137
3534633063333830220d0a4163636570742d52616e6765733a2062797465730d0a436f6e74656e742d4c656e6774683a2035
3032340d0a4b6565702d416c6976653a2074696d656f75743d352c206d61783d3130300d0a436f6e6e656374696f6e3a204
b6565702d416c6976650d0a436f6e74656e742d547970653a20696d6167652f6a7065670d0a0d0affd8ffe000104a464946
00010100000100010000ffdb0084000906070f0f0f0d0f0f0f100f0f0f0f0f100f0d0f0d0f0f100e101511161615151516151
81d2821181a251b151521322125292b2e2e3017203f44332d37282d2e2b010a0a0a0e0d0e1a1010172b261e222d2d2f2f2b
2d2d2d2d2b2d2d2d2d2d2d2d2d2d2d2d2d2d2d2d2d2d2d2d2d2d2d2d2d2d2d2d2d2b2d2d2d2d2d2d2d2b2d2d2d2d2b2d2d2dffc000110
800e100e1030122000211010311011ffc4001c00000201050100000000000000000000000102030405060708ffc4005210
00010302020506070a09090900000000010002030411052106123141610722325171811314525391a1c117234262729293
94b1d3083355474b4d1e1f0152425437382b2c2d234455563a2a4b3c3f1ffc40019010101000301000000000000000000
00000102030405ffc4002711010002020202010401050000000000000000102031121310412132232516141234271181c1ffd
a000c03010002110311003f00d06b0f3fb82a2aad674fb82a217b36fba5e157a834d477a6a12926a29acb6c53ba61413baa
8984d450aa692428a77434922ea3ac922693ba57514043492122504a6d746851421a052282928a0a482a2a2c049085190048
208494534256428c95ab0f3fb82a2aad5f4bb82a2b2b772c2bd24130546e9dd62a69a5742a9a4ae8491757689dd1750ba77
5769a4ae8ba5759ad1bd1e7d612f713153b4d9d2db371ded603b4f1d83d4a4c9a6262639ee0c635cf71d8c634b9c7b866b3
d49a1788c99f80118eb9a4630fcdbdc7a16f98753c34add4a68c4637bf6bdfc5ce3995762627692a4fb31f7ac3427680620
07f507809f3f58587c4700aca604cd4f235a36bdb69183b5cc240ef5d5fc27151f1973761523d8f92bf8717d6412ba3e3ba
354f541cf88369ea3682d168a43f19a36768f5ae79594f24323a295a58f61b39a7d9d638aca2cca353d29dd174ae92bb346
52ba5745d36ba3ba48489517412284945084 90a02c84d0a3354abe977054555abe9770545656ed8c749212428248ba5745d
112ba0151ba6a8922ea37489434c860b879aa9d910366f4a47f9118da7d9da42e991eab5ac8e36eac6c1aac68d807ed5ab6
```

1 client pkt, 4 server pkts, 1 turn.

Entire conversation (5639 bytes) | Show as: Raw | No delta times | Stream: 2

Find: □ Case sensitive

Carving out the image header and footer raw characters:



Wireshark · Follow TCP Stream (tcp.stream eq 2) · Digital_Investigation Task (pcap file).pcapng

```
4e3b47f0d5d24895d0e8b91ec5258a3975e91824635e18f9a5d76870b80eb4645f3dc559b4476c62b33d345a3ab7446e330
76b4ec3fb0abf931665b9ad7176e0eb6a83edf52d8348392dc4a869a5aa95d4d247080e788a590bc36e01367300205fad58
68868256e2ac9a4a6740c644f11b9d348f6ddfaa1d601ad3b011d5b5655cda8e278636f1e2d6e6bcb597bcb8924dc9cc93d
692e8fee2d8af9da2fa69fee93f716c57ced17d34ff76b0f92bf96cf8edf8738ba775d1bdc5b15f3b45f4d3fdd20f22f8a7
9da2fa69fee93e4afe53e2b7e1ce535718a50c94b3cd4f3002585e637807586b0ea3bc2b60b36b98d1a2e9215434d453440
845d2515290e6a174e4daa2ac9107745d249454ae914934095f60b854d5951052c02f2ccf0d6e59347c27bbe2b45c9ec562
5779e457447c5a9cd7cedb4f54db4408ce2a6da3b0bc8bf66af1585efeb0d98e9ed2deb46b01830fa68e9a0680d601aceb0
d695f6e73dc7792b28842e376b8cfe10945cec36a06c22781ddbcd7b7fceb4be497f2e61df2a7fd5a55d5b975a2f0984f84
b674f530c9dced688ff00e45ca79253fd39877ca9ff00569574527fa72e7bc7f521e9b54e785af6b98f68731e0b5cd70b87
348b10475594ee85cee979534f346dd85d6cf4c6e62ce4a779bf3e175f573de466d3c4715ea1c2bf114ffd8c5fe00b4ce58
7453c7e81d2c4dd6aaa40f962b0e7491dbdf23ef0011c5a3ad6e785fe229ffb18bfc016cbdbda21aeb5f59960f94dfc8d89
fe8cff00b42d4bf07cff0060aefd38feaf12db394dfc8d8a7e8cff00b42f38e11a415b45ae292aa5a70fb6b88dd66b88d84
b4e57e3b55a57dab3097b456d12f5b217964e9f631ff12a8f4b3fd2bb8f26543888a515389554d2cb501ae8e9e5200822da
db80073ce44df60b0db758da935ed6b78b74dd5228bae6bcafe9bf89c5e254cfb55d4339ef69b1a685d71ad96c7bb303ab3
3d57c6b1b9d339b6a36e3da7158c9f14c4658cdd8ea99355c3610d3ab71c39ab0b751010bb63a79f69dca5745d453550ee8
ba4854d1dd349358af04f39a8a6e49652910108428ba0842ab494ef9a48e289a5f248f6b236019b9ce3601174cde88e8a56
627248295b19f001af7be7368ae4f35a723726c72b6c06ebaa0c334c80005751003600c8321f40b72d05d1966174515336c
e908d7a8940fc64ce1ce3d83268e002cf4f2b58d73dc435ad05ce738d835a05c927a805cb6c9b9e9d74c7a8716d28c5b49f
0c8a396af11a46b649046c0c8e9dce276936f0239a0664acd7f276997e7d47f320fb85cbb945d2738ad6492027c5e3062a5
69cad1ef791e538e7d9aa372f47e8bd7f8cd0d0d479ea68643f29cc04faee96fa62382bcccf32e61a45826954d4952caaaa
a4969fc139d2c6d6c41ce6b39fcd22106fcdeb5cd34263ac7e214830f7b23ab264f032481a58d3e05fad7bb48e8eb6e5eac
9630e6b9a76381691c08b2f36f2654de07486921f333d645f32199bec5952db89637aea61d07f93b4cff003ea2f9b07dc2d
d7445d5ed85b1e28f81d580c843e170b4b1022ced50d6d88d600d85b675acf2e65cade3f261b5b8155b2e431d5ad9583fac
85de2faedf55c71016afbb86cfb7974d22eb9fe9261da4be3529c3ab69db48754c51cb1c01f1659b3f146e01d86fb0f05bc
d0d54734514b13c3e3958d7c6f69c9cc70b823b8aaf652274ca636e2da5d45a52da0ac756d5d2be9042ef0ec6361d774795
c0b4433ef0b8faf51729bf91b14fd19ff685c0340f451f8b5588012c8580495328dac8ef6b37e338dc0ec2772df8edc4cb9
f2d79885f
e866836275ad6d6d23606b6397dedf5246abdedded616b83803d62d71c1745fe4ed32fcfa8be641f70ba5d051c70471c30b
047144c6b238da2c1ad02c00559f90391391c86d3d8b54e4db6d71c438a694e2da518642d9aab11a401ee0c6471c54ef924
```

1 client pkt, 4 server pkts, 1 turn.

Entire conversation (5639 bytes) | Show as: Raw | No delta times | Stream: 2

Find: ffd8 □ Case sensitive