> DATA IS THE NEW CURRENCY

BY: ES
DIFFICULTY: EASY
CATEGORY: FORENSICS
SOLVES: SOME, A FEW, NONE, ON PART II

DESCRIPTION:
Corrupt government officials are offering the voter information as a service for a profit. You have been tasked with uncovering this hidden service. Hint: The 2 types of crypto used are AES CBC and RSA

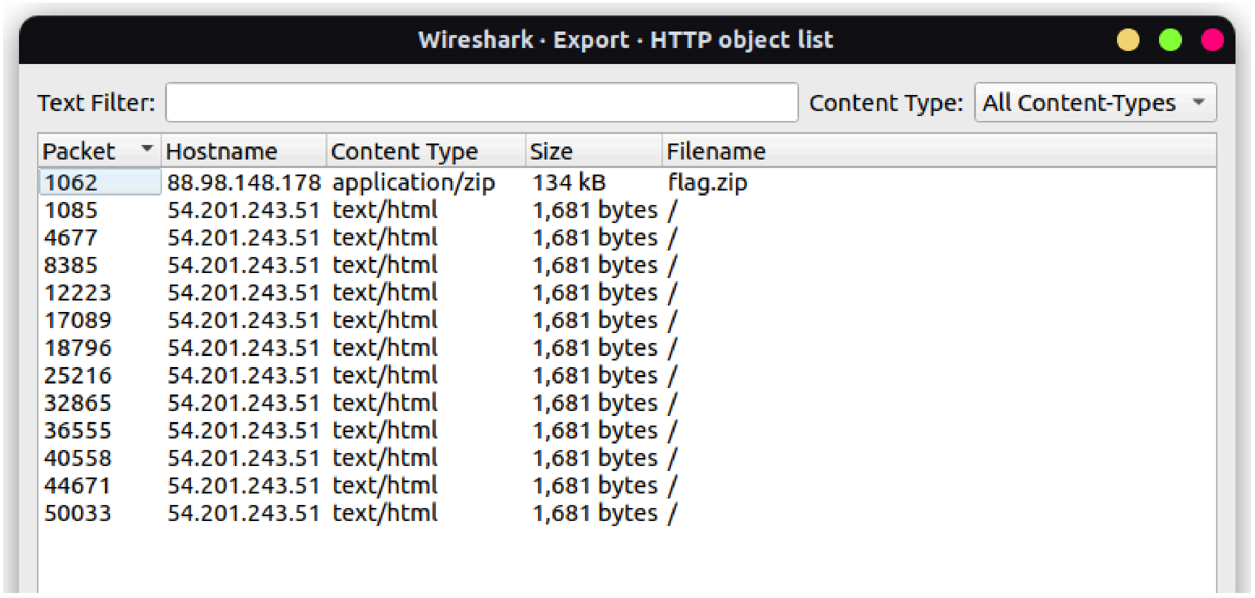
ARTIFACTS: ARTIFACT.PCAP

SOLUTION:

PART 1:

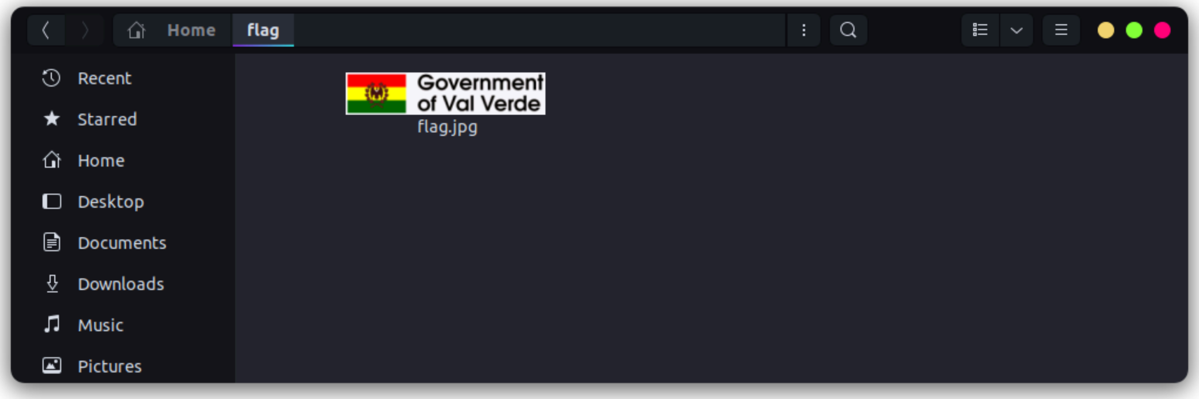
What file is sent to the customer, who just purchased access to the voter information service? (Answer Format is the full path)

We are given a pcap, let's open it with wireshark.
First an aside. There is a flag.zip in the HTTP traffic:


Wireshark · Export · HTTP object list
Text Filter:
Content Type: All Content-Types

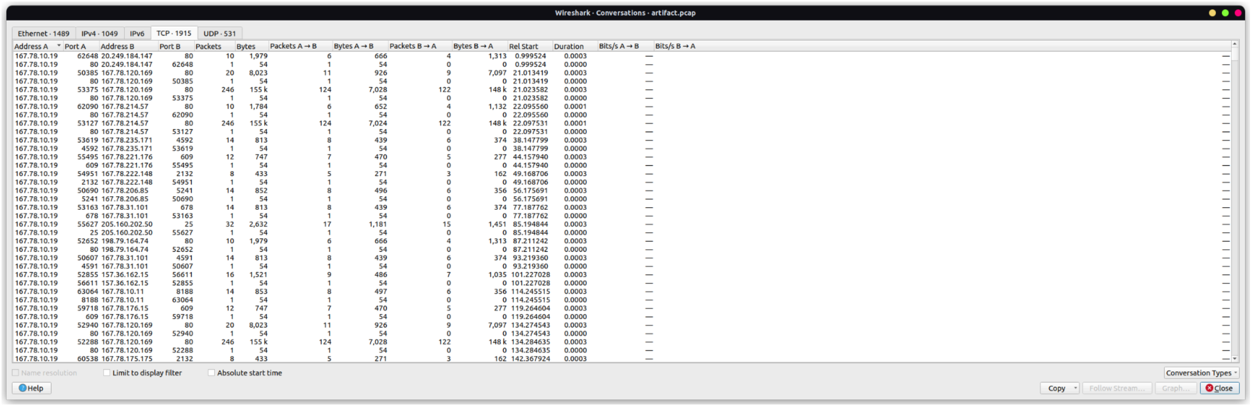
Packet	Hostname	Content Type	Size	Filename
1062	88.98.148.178	application/zip	134 kB	flag.zip
1085	54.201.243.51	text/html	1,681 bytes	/
4677	54.201.243.51	text/html	1,681 bytes	/
8385	54.201.243.51	text/html	1,681 bytes	/
12223	54.201.243.51	text/html	1,681 bytes	/
17089	54.201.243.51	text/html	1,681 bytes	/
18796	54.201.243.51	text/html	1,681 bytes	/
25216	54.201.243.51	text/html	1,681 bytes	/
32865	54.201.243.51	text/html	1,681 bytes	/
36555	54.201.243.51	text/html	1,681 bytes	/
40558	54.201.243.51	text/html	1,681 bytes	/
44671	54.201.243.51	text/html	1,681 bytes	/
50033	54.201.243.51	text/html	1,681 bytes	/

If you export the HTTP object and extract it, you get the image file flag.jpg:



This is just the Val Verde flag, there is nothing hidden inside of it. Its a red herring. I didn't expect people to try to analyze the image.

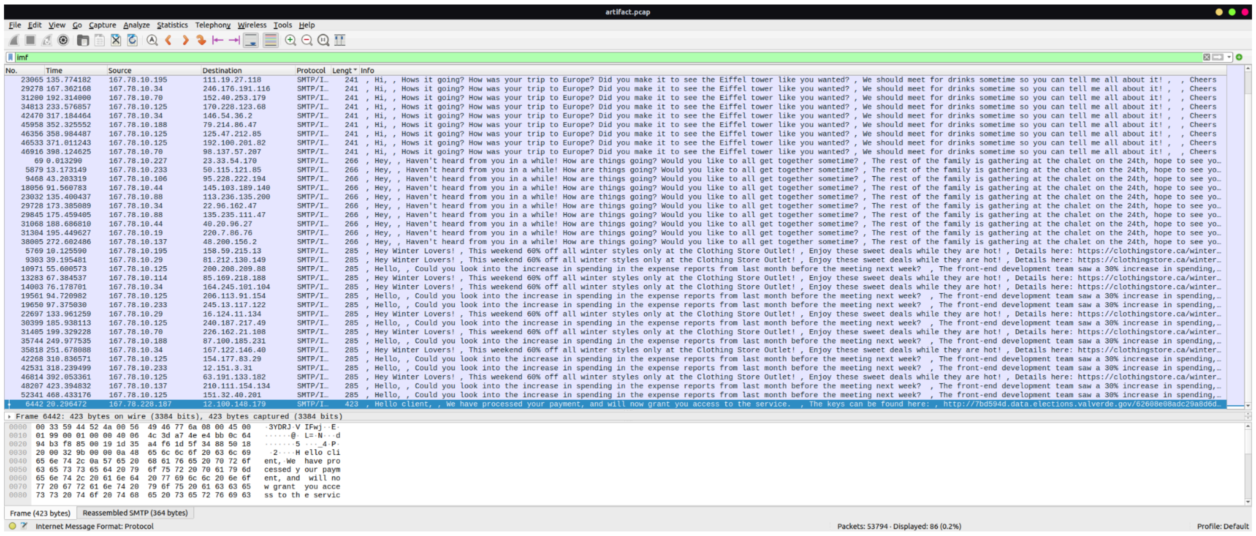
If we look at the conversation statistics, there are too many conversations to search manually, we must think about what protocols could be used to send a message, and obvious candidate is SMTP (ie. email).



Address A	Port A	Address B	Port B	Packets	Bytes	Packets A → B	Bytes A → B	Packets B → A	Bytes B → A	Rel Start	Duration	Bits/s A → B	Bits/s B → A
167.78.10.19	62648	20.249.184.147	80	10	1,979	6	666	4	1,313	0.999524	0.0003	—	—
167.78.10.19	80	20.249.184.147	62648	1	54	1	54	0	0	0.999524	0.0000	—	—
167.78.10.19	50385	167.78.120.169	80	20	8,023	11	926	9	7,097	21.013419	0.0003	—	—
167.78.10.19	80	167.78.120.169	50385	1	54	1	54	0	0	21.013419	0.0000	—	—
167.78.10.19	53375	167.78.120.169	80	246	155 k	124	7,028	122	148 k	21.023582	0.0003	—	—
167.78.10.19	80	167.78.120.169	53375	1	54	1	54	0	0	21.023582	0.0000	—	—
167.78.10.19	62090	167.78.214.57	80	10	1,784	6	652	4	1,132	22.095560	0.0001	—	—
167.78.10.19	80	167.78.214.57	62090	1	54	1	54	0	0	22.095560	0.0000	—	—
167.78.10.19	53127	167.78.214.57	80	246	155 k	124	7,024	122	148 k	22.097531	0.0001	—	—
167.78.10.19	80	167.78.214.57	53127	1	54	1	54	0	0	22.097531	0.0000	—	—
167.78.10.19	53619	167.78.235.171	4592	14	813	8	439	6	374	38.147799	0.0003	—	—
167.78.10.19	4592	167.78.235.171	53619	1	54	1	54	0	0	38.147799	0.0000	—	—
167.78.10.19	55495	167.78.221.176	609	12	747	7	470	5	277	44.157940	0.0003	—	—
167.78.10.19	609	167.78.221.176	55495	1	54	1	54	0	0	44.157940	0.0000	—	—
167.78.10.19	54951	167.78.222.148	2132	8	433	5	271	3	162	49.168706	0.0003	—	—
167.78.10.19	2132	167.78.222.148	54951	1	54	1	54	0	0	49.168706	0.0000	—	—
167.78.10.19	50690	167.78.206.85	5241	14	852	8	496	6	356	56.175691	0.0003	—	—
167.78.10.19	5241	167.78.206.85	50690	1	54	1	54	0	0	56.175691	0.0000	—	—
167.78.10.19	53163	167.78.31.101	678	14	813	8	439	6	374	77.187762	0.0003	—	—
167.78.10.19	678	167.78.31.101	53163	1	54	1	54	0	0	77.187762	0.0000	—	—
167.78.10.19	55627	205.160.202.50	25	32	2,632	17	1,181	15	1,451	85.194844	0.0003	—	—
167.78.10.19	25	205.160.202.50	55627	1	54	1	54	0	0	85.194844	0.0000	—	—
167.78.10.19	52652	198.79.164.74	80	10	1,979	6	666	4	1,313	87.211242	0.0003	—	—
167.78.10.19	80	198.79.164.74	52652	1	54	1	54	0	0	87.211242	0.0000	—	—
167.78.10.19	50607	167.78.31.101	4591	14	813	8	439	6	374	93.219360	0.0003	—	—
167.78.10.19	4591	167.78.31.101	50607	1	54	1	54	0	0	93.219360	0.0000	—	—
167.78.10.19	52855	157.36.162.15	56611	16	1,521	9	486	7	1,035	101.227028	0.0003	—	—
167.78.10.19	56611	157.36.162.15	52855	1	54	1	54	0	0	101.227028	0.0000	—	—
167.78.10.19	63064	167.78.10.11	8188	14	853	8	497	6	356	114.245515	0.0003	—	—
167.78.10.19	8188	167.78.10.11	63064	1	54	1	54	0	0	114.245515	0.0000	—	—
167.78.10.19	59718	167.78.176.15	609	12	747	7	470	5	277	119.264604	0.0003	—	—
167.78.10.19	609	167.78.176.15	59718	1	54	1	54	0	0	119.264604	0.0000	—	—
167.78.10.19	52940	167.78.120.169	80	20	8,023	11	926	9	7,097	134.274543	0.0003	—	—
167.78.10.19	80	167.78.120.169	52940	1	54	1	54	0	0	134.274543	0.0000	—	—
167.78.10.19	52288	167.78.120.169	80	246	155 k	124	7,028	122	148 k	134.284635	0.0003	—	—
167.78.10.19	80	167.78.120.169	52288	1	54	1	54	0	0	134.284635	0.0000	—	—
167.78.10.19	60538	167.78.175.175	2132	8	433	5	271	3	162	142.367924	0.0003	—	—

Lets try and filter on that.
Additionally, we can see alot of repetition in the traffic, we are essentially looking for anomalies.

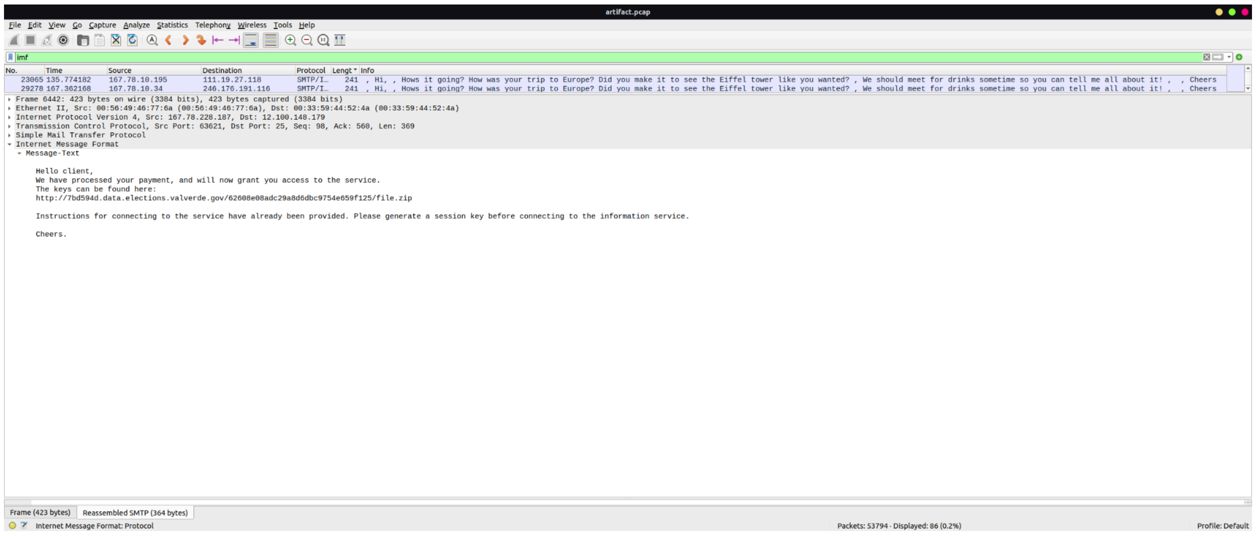
Filter on imf (Internet Message Format), and sort by message length:


artifact.pcap
File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help
imf

```
No.   Time           Source            Destination        Protocol  Lengt  Info
23065 135.774182     167.78.10.195     111.19.27.118      SMTP/I…   241    , Hi, , Hows it going? How was your trip to Europe? Did you make it to see the Eiffel tower like you wanted? , We should meet for drinks sometime so you can tell me all about it! ,  , Cheers
29278 167.362168     167.78.10.34      246.176.191.116    SMTP/I…   241    , Hi, , Hows it going? How was your trip to Europe? Did you make it to see the Eiffel tower like you wanted? , We should meet for drinks sometime so you can tell me all about it! ,  , Cheers
31200 192.314000     167.78.10.70      152.40.253.179     SMTP/I…   241    , Hi, , Hows it going? How was your trip to Europe? Did you make it to see the Eiffel tower like you wanted? , We should meet for drinks sometime so you can tell me all about it! ,  , Cheers
34813 233.576857     167.78.10.125     170.228.123.68     SMTP/I…   241    , Hi, , Hows it going? How was your trip to Europe? Did you make it to see the Eiffel tower like you wanted? , We should meet for drinks sometime so you can tell me all about it! ,  , Cheers
42470 317.184464     167.78.10.34      146.54.36.2        SMTP/I…   241    , Hi, , Hows it going? How was your trip to Europe? Did you make it to see the Eiffel tower like you wanted? , We should meet for drinks sometime so you can tell me all about it! ,  , Cheers
45958 352.325552     167.78.10.188     79.214.86.47       SMTP/I…   241    , Hi, , Hows it going? How was your trip to Europe? Did you make it to see the Eiffel tower like you wanted? , We should meet for drinks sometime so you can tell me all about it! ,  , Cheers
46356 358.984487     167.78.10.125     125.47.212.85      SMTP/I…   241    , Hi, , Hows it going? How was your trip to Europe? Did you make it to see the Eiffel tower like you wanted? , We should meet for drinks sometime so you can tell me all about it! ,  , Cheers
46533 371.011243     167.78.10.125     192.100.201.82     SMTP/I…   241    , Hi, , Hows it going? How was your trip to Europe? Did you make it to see the Eiffel tower like you wanted? , We should meet for drinks sometime so you can tell me all about it! ,  , Cheers
46916 398.124625     167.78.10.70      98.137.57.207      SMTP/I…   241    , Hi, , Hows it going? How was your trip to Europe? Did you make it to see the Eiffel tower like you wanted? , We should meet for drinks sometime so you can tell me all about it! ,  , Cheers
   69 0.013290       167.78.10.227     23.33.54.170       SMTP/I…   266    , Hey, , Haven't heard from you in a while! How are things going? Would you like to all get together sometime? , The rest of the family is gathering at the chalet on the 24th, hope to see yo…
 5879 13.173149      167.78.10.233     50.115.121.85      SMTP/I…   266    , Hey, , Haven't heard from you in a while! How are things going? Would you like to all get together sometime? , The rest of the family is gathering at the chalet on the 24th, hope to see yo…
 9468 43.203319      167.78.10.106     95.228.222.194     SMTP/I…   266    , Hey, , Haven't heard from you in a while! How are things going? Would you like to all get together sometime? , The rest of the family is gathering at the chalet on the 24th, hope to see yo…
18056 91.560783      167.78.10.44      145.103.189.140    SMTP/I…   266    , Hey, , Haven't heard from you in a while! How are things going? Would you like to all get together sometime? , The rest of the family is gathering at the chalet on the 24th, hope to see yo…
23032 135.400437     167.78.10.88      113.236.135.200    SMTP/I…   266    , Hey, , Haven't heard from you in a while! How are things going? Would you like to all get together sometime? , The rest of the family is gathering at the chalet on the 24th, hope to see yo…
29728 173.385089     167.78.10.34      22.96.162.47       SMTP/I…   266    , Hey, , Haven't heard from you in a while! How are things going? Would you like to all get together sometime? , The rest of the family is gathering at the chalet on the 24th, hope to see yo…
29845 175.459405     167.78.10.88      135.235.111.47     SMTP/I…   266    , Hey, , Haven't heard from you in a while! How are things going? Would you like to all get together sometime? , The rest of the family is gathering at the chalet on the 24th, hope to see yo…
31068 188.686810     167.78.10.44      40.20.96.27        SMTP/I…   266    , Hey, , Haven't heard from you in a while! How are things going? Would you like to all get together sometime? , The rest of the family is gathering at the chalet on the 24th, hope to see yo…
31304 195.449627     167.78.10.19      220.7.86.76        SMTP/I…   266    , Hey, , Haven't heard from you in a while! How are things going? Would you like to all get together sometime? , The rest of the family is gathering at the chalet on the 24th, hope to see yo…
38005 272.602486     167.78.10.137     48.200.156.2       SMTP/I…   266    , Hey, , Haven't heard from you in a while! How are things going? Would you like to all get together sometime? , The rest of the family is gathering at the chalet on the 24th, hope to see yo…
 5769 10.125590      167.78.10.195     158.59.215.13      SMTP/I…   285    , Hey Winter Lovers! , This weekend 60% off all winter styles only at the Clothing Store Outlet! , Enjoy these sweet deals while they are hot! , Details here: https://clothingstore.ca/winter…
 9303 39.195481      167.78.10.29      81.212.130.149     SMTP/I…   285    , Hey Winter Lovers! , This weekend 60% off all winter styles only at the Clothing Store Outlet! , Enjoy these sweet deals while they are hot! , Details here: https://clothingstore.ca/winter…
10971 55.600573      167.78.10.125     200.208.209.88     SMTP/I…   285    , Hello, , Could you look into the increase in spending in the expense reports from last month before the meeting next week?  , The front-end development team saw a 30% increase in spending,…
13283 67.384537      167.78.10.114     85.169.218.188     SMTP/I…   285    , Hey Winter Lovers! , This weekend 60% off all winter styles only at the Clothing Store Outlet! , Enjoy these sweet deals while they are hot! , Details here: https://clothingstore.ca/winter…
14003 76.178701      167.78.10.34      164.245.101.104    SMTP/I…   285    , Hey Winter Lovers! , This weekend 60% off all winter styles only at the Clothing Store Outlet! , Enjoy these sweet deals while they are hot! , Details here: https://clothingstore.ca/winter…
19561 94.720982      167.78.10.125     206.113.91.154     SMTP/I…   285    , Hello, , Could you look into the increase in spending in the expense reports from last month before the meeting next week?  , The front-end development team saw a 30% increase in spending,…
19650 97.375030      167.78.10.233     245.13.117.122     SMTP/I…   285    , Hello, , Could you look into the increase in spending in the expense reports from last month before the meeting next week?  , The front-end development team saw a 30% increase in spending,…
22697 133.961259     167.78.10.29      16.124.11.134      SMTP/I…   285    , Hey Winter Lovers! , This weekend 60% off all winter styles only at the Clothing Store Outlet! , Enjoy these sweet deals while they are hot! , Details here: https://clothingstore.ca/winter…
30399 185.938113     167.78.10.125     240.187.217.49     SMTP/I…   285    , Hello, , Could you look into the increase in spending in the expense reports from last month before the meeting next week?  , The front-end development team saw a 30% increase in spending,…
31405 199.329228     167.78.10.70      226.162.21.108     SMTP/I…   285    , Hey Winter Lovers! , This weekend 60% off all winter styles only at the Clothing Store Outlet! , Enjoy these sweet deals while they are hot! , Details here: https://clothingstore.ca/winter…
35744 249.977535     167.78.10.188     87.100.185.231     SMTP/I…   285    , Hello, , Could you look into the increase in spending in the expense reports from last month before the meeting next week?  , The front-end development team saw a 30% increase in spending,…
35818 251.678088     167.78.10.34      167.122.146.40     SMTP/I…   285    , Hey Winter Lovers! , This weekend 60% off all winter styles only at the Clothing Store Outlet! , Enjoy these sweet deals while they are hot! , Details here: https://clothingstore.ca/winter…
42268 310.836571     167.78.10.125     154.177.83.29      SMTP/I…   285    , Hello, , Could you look into the increase in spending in the expense reports from last month before the meeting next week?  , The front-end development team saw a 30% increase in spending,…
42531 318.239499     167.78.10.233     12.151.3.31        SMTP/I…   285    , Hello, , Could you look into the increase in spending in the expense reports from last month before the meeting next week?  , The front-end development team saw a 30% increase in spending,…
46814 392.053361     167.78.10.125     63.191.133.182     SMTP/I…   285    , Hey Winter Lovers! , This weekend 60% off all winter styles only at the Clothing Store Outlet! , Enjoy these sweet deals while they are hot! , Details here: https://clothingstore.ca/winter…
48207 423.394832     167.78.10.137     210.111.154.134    SMTP/I…   285    , Hello, , Could you look into the increase in spending in the expense reports from last month before the meeting next week?  , The front-end development team saw a 30% increase in spending,…
52341 468.433176     167.78.10.125     151.32.40.201      SMTP/I…   285    , Hello, , Could you look into the increase in spending in the expense reports from last month before the meeting next week?  , The front-end development team saw a 30% increase in spending,…
 6442 20.296472      167.78.228.187    12.100.148.179     SMTP/I…   423    , Hello client, , We have processed your payment, and will now grant you access to the service.  , The keys can be found here: , http://7bd594d.data.elections.valverde.gov/62608e08adc29a8d6d…

› Frame 6442: 423 bytes on wire (3384 bits), 423 bytes captured (3384 bits)
0000  00 33 59 44 52 4a 00 56  49 46 77 6a 08 00 45 00   ·3YDRJ·V IFwj··E·
0010  01 99 00 01 00 00 40 06  4c 3d a7 4e e4 bb 0c 64   ······@· L=·N···d
0020  94 b3 f8 85 00 19 1d 35  a4 f6 1d 5f 34 88 50 18   ·······5 ···_4·P·
0030  20 00 32 9b 00 00 0a 48  65 6c 6c 6f 20 63 6c 69    ·2····H ello cli
0040  65 6e 74 2c 0a 57 65 20  68 61 76 65 20 70 72 6f   ent,·We  have pro
0050  63 65 73 73 65 64 20 79  6f 75 72 20 70 61 79 6d   cessed y our paym
0060  65 6e 74 2c 20 61 6e 64  20 77 69 6c 6c 20 6e 6f   ent, and  will no
0070  77 20 67 72 61 6e 74 20  79 6f 75 20 61 63 63 65   w grant  you acce
0080  73 73 20 74 6f 20 74 68  65 20 73 65 72 76 69 63   ss to th e servic
```

Frame (423 bytes)
Reassembled SMTP (364 bytes)
Internet Message Format: Protocol
Packets: 53794 · Displayed: 86 (0.2%)
Profile: Default

Viewing the message itself we get the flag:


artifact.pcap
File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help
imf

```
No.   Time           Source            Destination        Protocol  Lengt  Info
23065 135.774182     167.78.10.195     111.19.27.118      SMTP/I…   241    , Hi, , Hows it going? How was your trip to Europe? Did you make it to see the Eiffel tower like you wanted? , We should meet for drinks sometime so you can tell me all about it! ,  , Cheers
29278 167.362168     167.78.10.34      246.176.191.116    SMTP/I…   241    , Hi, , Hows it going? How was your trip to Europe? Did you make it to see the Eiffel tower like you wanted? , We should meet for drinks sometime so you can tell me all about it! ,  , Cheers

› Frame 6442: 423 bytes on wire (3384 bits), 423 bytes captured (3384 bits)
› Ethernet II, Src: 00:56:49:46:77:6a (00:56:49:46:77:6a), Dst: 00:33:59:44:52:4a (00:33:59:44:52:4a)
› Internet Protocol Version 4, Src: 167.78.228.187, Dst: 12.100.148.179
› Transmission Control Protocol, Src Port: 63621, Dst Port: 25, Seq: 98, Ack: 560, Len: 369
› Simple Mail Transfer Protocol
⌄ Internet Message Format
  ⌄ Message-Text

      Hello client,
      We have processed your payment, and will now grant you access to the service.
      The keys can be found here:
      http://7bd594d.data.elections.valverde.gov/62608e08adc29a8d6dbc9754e659f125/file.zip

      Instructions for connecting to the service have already been provided. Please generate a session key before connecting to the information service.

      Cheers.
```

Frame (423 bytes)
Reassembled SMTP (364 bytes)
Internet Message Format: Protocol
Packets: 53794 · Displayed: 86 (0.2%)
Profile: Default

Flag: /62608e08adc29a8d6dbc9754e659f125/file.zip

PART 2:

What is the occupation of Tatiana Castro?

There are some hints in the message from the previous part:

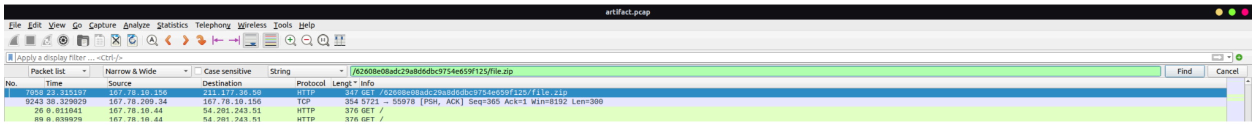
```
Hello client,
We have processed your payment, and will now grant you access to
the service.
The keys can be found here:
```

```
http://7bd594d.data.elections.valverde.gov/62608e08adc29a8d6dbc9754
e659f125/file.zip

Instructions for connecting to the service have already been
provided. Please generate a session key before connecting to the
information service.

Cheers.
```

Tatiana's occupation can likely be found as part of the information service, as as stated in the challenge description: You have been tasked with uncovering this (voter information) hidden service.

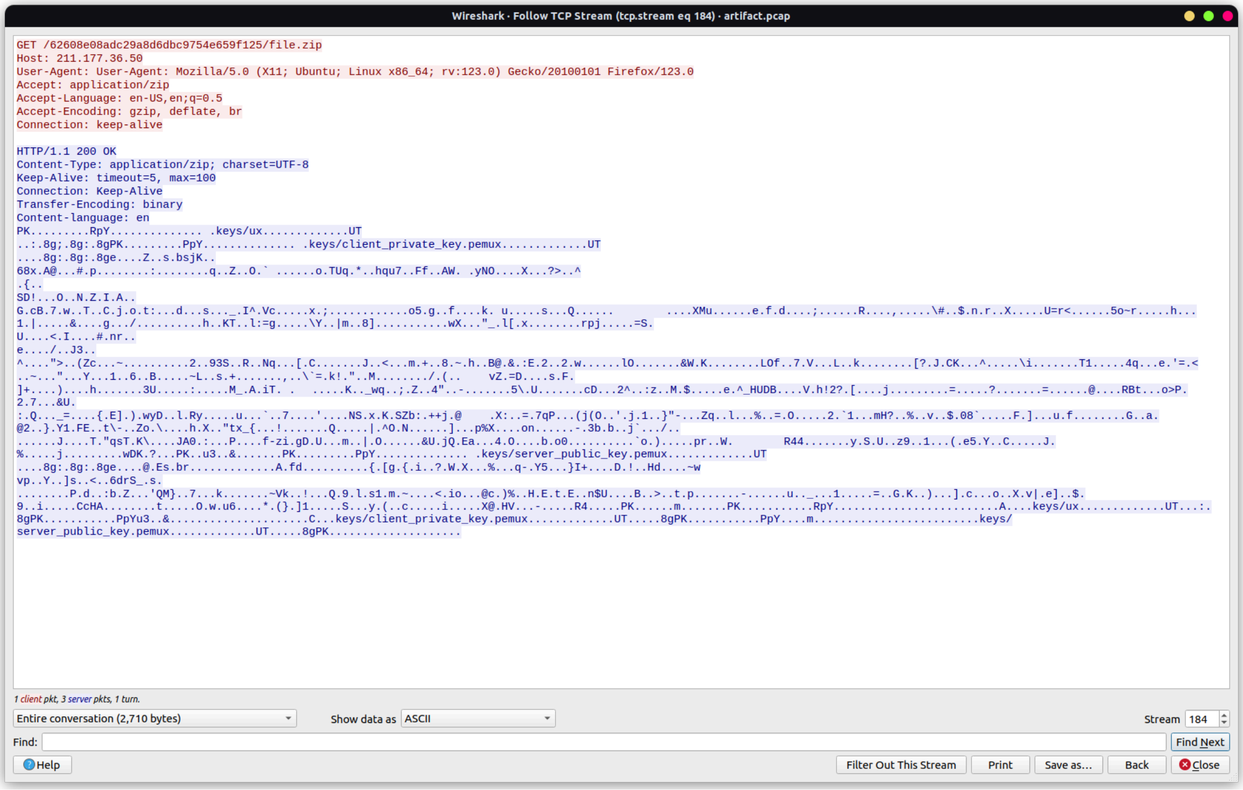
In the message it says: *`Please generate a session key before connecting to the information service`*, and provides a path to a file containing keys. Lets start by downloading this file .

We can find it by filtering on the file path:



```
Search: /62608e08adc29a8d6dbc9754e659f125/file.zip
No.   Time       Source          Destination     Protocol Lengt Info
 7058 23.315197  167.78.10.156   211.177.36.50   HTTP     347 GET /62608e08adc29a8d6dbc9754e659f125/file.zip
 9243 38.329029  167.78.209.34   167.78.10.156   TCP      354 5721 → 55978 [PSH, ACK] Seq=365 Ack=1 Win=8192 Len=300
   26 0.011041   167.78.10.44    54.201.243.51   HTTP     376 GET /
   89 0.039929   167.78.10.44    54.201.243.51   HTTP     376 GET /
```

Extract the bytes in the HTTP response to get a zip file:


Wireshark · Follow TCP Stream (tcp.stream eq 184) · artifact.pcap
Help
Filter Out This Stream
Print
Save as…
Back
Close
Find Next

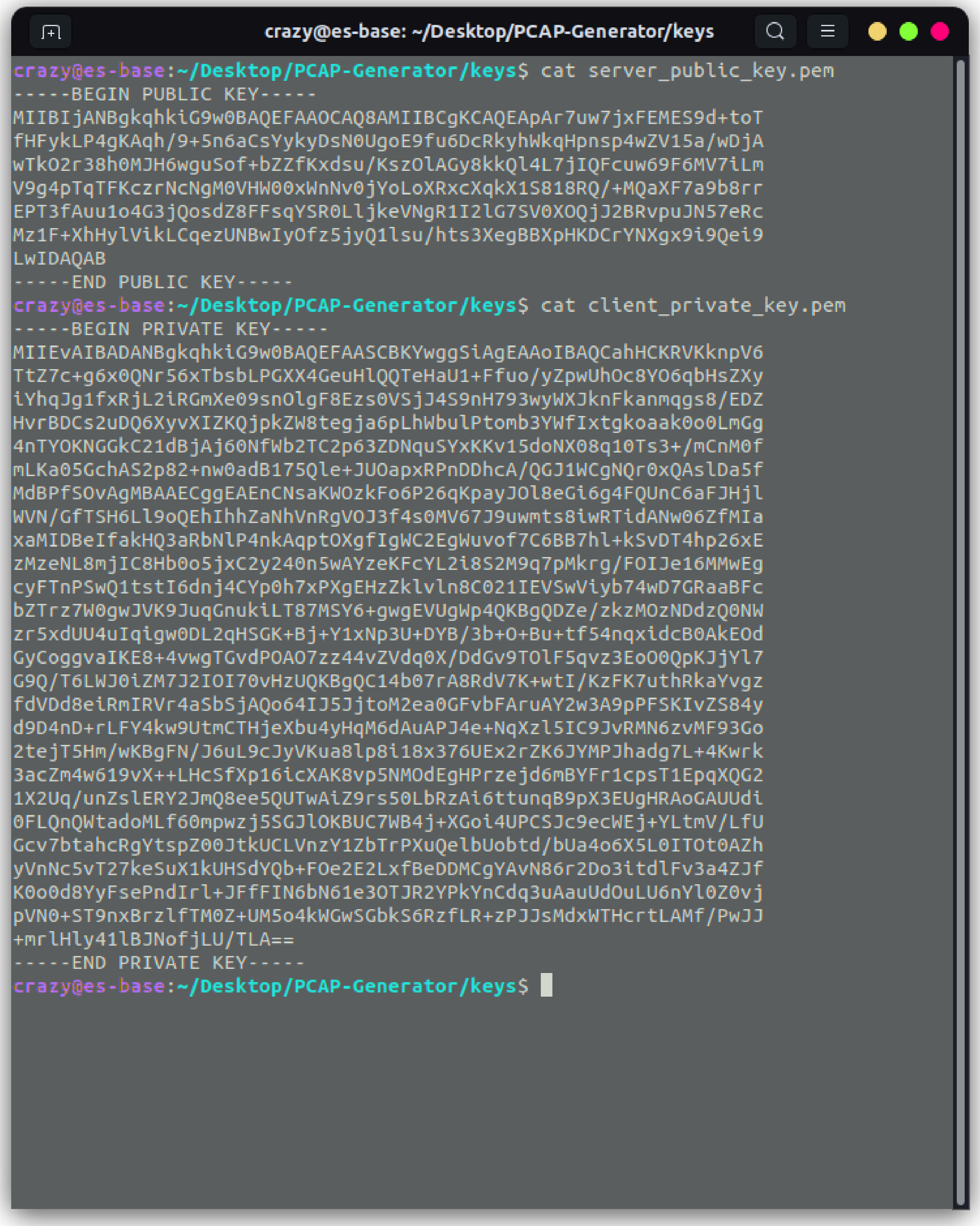
```
GET /62608e08adc29a8d6dbc9754e659f125/file.zip
Host: 211.177.36.50
User-Agent: User-Agent: Mozilla/5.0 (X11; Ubuntu; Linux x86_64; rv:123.0) Gecko/20100101 Firefox/123.0
Accept: application/zip
Accept-Language: en-US,en;q=0.5
Accept-Encoding: gzip, deflate, br
Connection: keep-alive

HTTP/1.1 200 OK
Content-Type: application/zip; charset=UTF-8
Keep-Alive: timeout=5, max=100
Connection: Keep-Alive
Transfer-Encoding: binary
Content-language: en
PK.........RpY.............. .keys/ux.............UT
..:.8g;.8g:.8gPK.........PpY.............. .keys/client_private_key.pemux............UT
....8g:.8g:.8ge....Z..s.bsjK..
68x.A@...#.p........:........q..Z..O.` ......o.TUq.*..hqu7..Ff..AW. .yNO....X...?>..^
.{..
SD!...O..N.Z.I.A..
G.cB.7.w..T..C.j.o.t:...d...s..._.I^.Vc.....x.;............o5.g..f....k. u.....s...Q......        ....XMu......e.f.d....;......R....,.....\#..$.n.r..X.....U=r<......5o~r.....h...
1.|.....&....g.../..........h..KT..l:=g.....\Y..|m..8]...........wX..."_.l[.x........rpj.....=S.
U....<.I....#.nr..
e..../..J3..
^....">..(Zc...~..........2..93S..R..Nq...[.C.......J..<...m.+..8.~.h..B@.&.:E.2..2.w......lO.......&W.K........LOf..7.V...L..k........[?.J.CK...^.....\i.......T1.....4q...e.'=.<
..~..."...Y...1..6..B.....~L..s.+.......,..\`=.k!."..M......../.(..    vZ.=D....s.F.
]+....)....h.......3U.....:.....M_.A.iT. .   .....K.._wq..;.Z..4"..-.......5\.U.......cD...2^..:z..M.$.....e.^_HUDB....V.h!2?.[....j.........=.....?.......=......@....RBt...o>P.
2.7...&U.
:.Q..._=....{.E].).wyD..l.Ry.....u...`..7....'....NS.x.K.SZb:.++j.@    .X:..=.7qP...(j(O..'.j.1..}"-...Zq..l...%..=.O.....2.`1...mH?..%..v..$.08`.....F.]...u.f........G..a.
@2..}.Y1.FE..t\-..Zo.\....h.X.."tx_{...!.......Q.....|.^O.N......]...p%X....on......-.3b.b..j`.../..
......J....T."qsT.K\....JA0.:...P....f-zi.gD.U...m..|.O......&U.jQ.Ea...4.O....b.o0..........`o.).....pr..W.        R44.......y.S.U..z9..1...(.e5.Y..C.....J.
%.....j.........wDK.?...PK..u3..&.......PK.........PpY.............. .keys/server_public_key.pemux............UT
....8g:.8g:.8ge....@.Es.br.............A.fd..........{.[g.{.i..?.W.X...%...q-.Y5...}I+....D.!..Hd....~w
vp..Y..]s..<..6drS_.s.
........P.d..:b.Z...'QM}..7...k.......~Vk..!...Q.9.l.s1.m.~....<.io...@c.)%..H.E.t.E..n$U....B..>..t.p.......-......u.._...1.....=..G.K..)...].c...o..X.v|.e]..$.
9..i.....CcHA........t.....O.w.u6....*.(}.]1.....S...y.(..c.....i.....X@.HV...-.....R4.....PK......m.......PK...........RpY.........................A....keys/ux.............UT...:.
8gPK...........PpYu3..&.....................C...keys/client_private_key.pemux............UT.....8gPK...........PpY....m..........................keys/
server_public_key.pemux............UT.....8gPK...................
```

1 client pkt, 3 server pkts, 1 turn.

Entire conversation (2,710 bytes)   Show data as ASCII   Stream 184

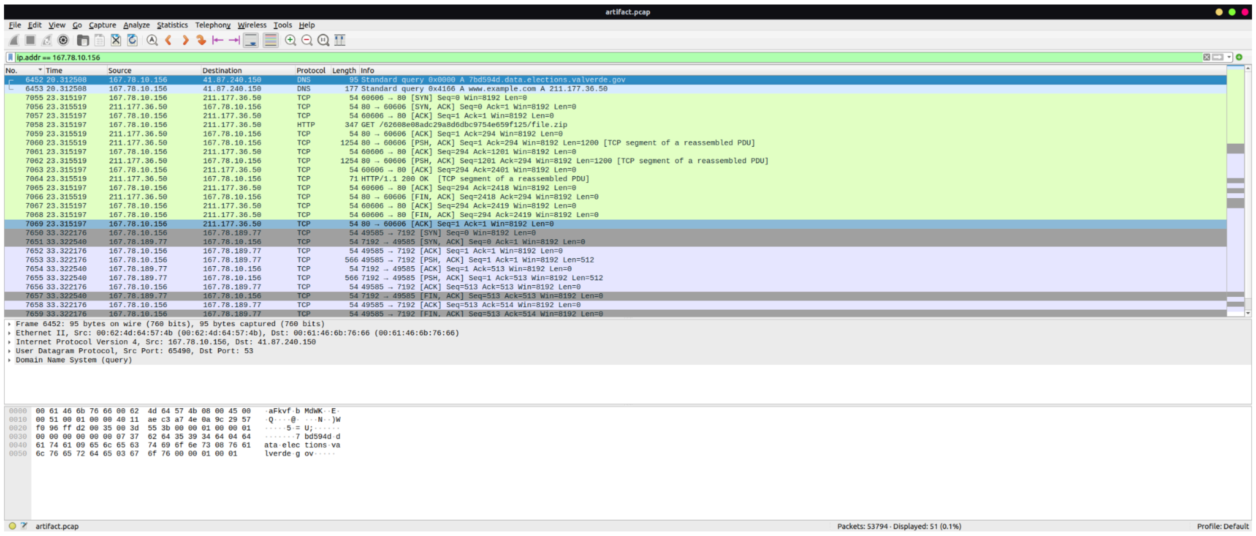
Find:

We get the private key of the server, and the public key of the client:



```
crazy@es-base: ~/Desktop/PCAP-Generator/keys
crazy@es-base:~/Desktop/PCAP-Generator/keys$ cat server_public_key.pem
-----BEGIN PUBLIC KEY-----
MIIBIjANBgkqhkiG9w0BAQEFAAOCAQ8AMIIBCgKCAQEApAr7uw7jxFEMES9d+toT
fHFykLP4gKAqh/9+5n6aCsYykyDsN0UgoE9fu6DcRkyhWkqHpnsp4wZV15a/wDjA
wTkO2r38h0MJH6wguSof+bZZfKxdsu/KszOlAGy8kkQl4L7jIQFcuw69F6MV7iLm
V9g4pTqTFKczrNcNgM0VHW00xWnNv0jYoLoXRxcXqkX1S818RQ/+MQaXF7a9b8rr
EPT3fAuu1o4G3jQosdZ8FFsqYSR0LljkeVNgR1I2lG7SV0XOQjJ2BRvpuJN57eRc
Mz1F+XhHylVikLCqezUNBwIyOfz5jyQ1lsu/hts3XegBBXpHKDCrYNXgx9i9Qei9
LwIDAQAB
-----END PUBLIC KEY-----
crazy@es-base:~/Desktop/PCAP-Generator/keys$ cat client_private_key.pem
-----BEGIN PRIVATE KEY-----
MIIEvAIBADANBgkqhkiG9w0BAQEFAASCBKYwggSiAgEAAoIBAQCahHCKRVKknpV6
TtZ7c+g6x0QNr56xTbsbLPGXX4GeuHlQQTeHaU1+Ffuo/yZpwUhOc8YO6qbHsZXy
iYhqJg1fxRjL2iRGmXe09snOlgF8Ezs0VSjJ4S9nH793wyWXJknFkanmqgs8/EDZ
HvrBDCs2uDQ6XyvXIZKQjpkZW8tegja6pLhWbulPtomb3YWfIxtgkoaak0o0LmGg
4nTYOKNGGkC21dBjAj60NfWb2TC2p63ZDNquSYxKKv15doNX08q10Ts3+/mCnM0f
mLKa05GchAS2p82+nw0adB175Qle+JUOapxRPnDDhcA/QGJ1WCgNQr0xQAslDa5f
MdBPfSOvAgMBAAECggEAEnCNsaKWOzkFo6P26qKpayJOl8eGi6g4FQUnC6aFJHjl
WVN/GfTSH6Ll9oQEhIhhZaNhVnRgVOJ3f4s0MV67J9uwmts8iwRTidANw06ZfMIa
xaMIDBeIfakHQ3aRbNlP4nkAqptOXgfIgWC2EgWuvof7C6BB7hl+kSvDT4hp26xE
zMzeNL8mjIC8Hb0o5jxC2y240n5wAYzeKFcYL2i8S2M9q7pMkrg/FOIJe16MMwEg
cyFTnPSwQ1tstI6dnj4CYp0h7xPXgEHzZklvln8C021IEVSwViyb74wD7GRaaBFc
bZTrz7W0gwJVK9JuqGnukiLT87MSY6+gwgEVUgWp4QKBgQDZe/zkzMOzNDdzQ0NW
zr5xdUU4uIqigw0DL2qHSGK+Bj+Y1xNp3U+DYB/3b+O+Bu+tf54nqxidcB0AkEOd
GyCoggvaIKE8+4vwgTGvdPOAO7zz44vZVdq0X/DdGv9TOlF5qvz3EoO0QpKJjYl7
G9Q/T6LWJ0iZM7J2IOI70vHzUQKBgQC14b07rA8RdV7K+wtI/KzFK7uthRkaYvgz
fdVDd8eiRmIRVr4aSbSjAQo64IJ5JjtoM2ea0GFvbFAruAY2w3A9pPFSKIvZS84y
d9D4nD+rLFY4kw9UtmCTHjeXbu4yHqM6dAuAPJ4e+NqXzl5IC9JvRMN6zvMF93Go
2tejT5Hm/wKBgFN/J6uL9cJyVKua8lp8i18x376UEx2rZK6JYMPJhadg7L+4Kwrk
3acZm4w619vX++LHcSfXp16icXAK8vp5NMOdEgHPrzejd6mBYFr1cpsT1EpqXQG2
1X2Uq/unZslERY2JmQ8ee5QUTwAiZ9rs50LbRzAi6ttunqB9pX3EUgHRAoGAUUdi
0FLQnQWtadoMLf60mpwzj5SGJlOKBUC7WB4j+XGoi4UPCSJc9ecWEj+YLtmV/LfU
Gcv7btahcRgYtspZ00JtkUCLVnzY1ZbTrPXuQelbUobtd/bUa4o6X5L0ITOt0AZh
yVnNc5vT27keSuX1kUHSdYQb+FOe2E2LxfBeDDMCgYAvN86r2Do3itdlFv3a4ZJf
K0o0d8YyFsePndIrl+JFfFIN6bN61e3OTJR2YPkYnCdq3uAauUdOuLU6nYl0Z0vj
pVN0+ST9nxBrzlfTM0Z+UM5o4kWGwSGbkS6RzfLR+zPJJsMdxWTHcrtLAMf/PwJJ
+mrlHly41lBJNofjLU/TLA==
-----END PRIVATE KEY-----
crazy@es-base:~/Desktop/PCAP-Generator/keys$
```

Based on the information in the email, you have to figure out that there is a key generation service. To find it filter on IP of client fetching the zip file.zip mentioned in the email, 167.78.10.156


artifact.pcap
File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help

```
ip.addr == 167.78.10.156
```

```
No.     Time      Source         Destination    Protocol Length Info
  6452 20.312508  167.78.10.156  41.87.240.150  DNS        95 Standard query 0x0000 A 7bd594d.data.elections.valverde.gov
  6453 20.312508  167.78.10.156  41.87.240.150  DNS       177 Standard query 0x4166 A www.example.com A 211.177.36.50
  7055 23.315197  167.78.10.156  211.177.36.50  TCP        54 60606 → 80 [SYN] Seq=0 Win=8192 Len=0
  7056 23.315519  211.177.36.50  167.78.10.156  TCP        54 80 → 60606 [SYN, ACK] Seq=0 Ack=1 Win=8192 Len=0
  7057 23.315197  167.78.10.156  211.177.36.50  TCP        54 60606 → 80 [ACK] Seq=1 Ack=1 Win=8192 Len=0
  7058 23.315197  167.78.10.156  211.177.36.50  HTTP      347 GET /62608e08adc29a8d6dbc9754e659f125/file.zip
  7059 23.315519  211.177.36.50  167.78.10.156  TCP        54 80 → 60606 [ACK] Seq=1 Ack=294 Win=8192 Len=0
  7060 23.315519  211.177.36.50  167.78.10.156  TCP      1254 80 → 60606 [PSH, ACK] Seq=1 Ack=294 Win=8192 Len=1200 [TCP segment of a reassembled PDU]
  7061 23.315197  167.78.10.156  211.177.36.50  TCP        54 60606 → 80 [ACK] Seq=294 Ack=1201 Win=8192 Len=0
  7062 23.315519  211.177.36.50  167.78.10.156  TCP      1254 80 → 60606 [PSH, ACK] Seq=1201 Ack=294 Win=8192 Len=1200 [TCP segment of a reassembled PDU]
  7063 23.315197  167.78.10.156  211.177.36.50  TCP        54 60606 → 80 [ACK] Seq=294 Ack=2401 Win=8192 Len=0
  7064 23.315519  211.177.36.50  167.78.10.156  TCP        71 HTTP/1.1 200 OK  [TCP segment of a reassembled PDU]
  7065 23.315197  167.78.10.156  211.177.36.50  TCP        54 60606 → 80 [ACK] Seq=294 Ack=2418 Win=8192 Len=0
  7066 23.315519  211.177.36.50  167.78.10.156  TCP        54 80 → 60606 [FIN, ACK] Seq=2418 Ack=294 Win=8192 Len=0
  7067 23.315197  167.78.10.156  211.177.36.50  TCP        54 60606 → 80 [ACK] Seq=294 Ack=2419 Win=8192 Len=0
  7068 23.315197  167.78.10.156  211.177.36.50  TCP        54 60606 → 80 [FIN, ACK] Seq=294 Ack=2419 Win=8192 Len=0
  7069 23.315197  167.78.10.156  211.177.36.50  TCP        54 80 → 60606 [ACK] Seq=1 Ack=1 Win=8192 Len=0
  7650 33.322176  167.78.10.156  167.78.189.77  TCP        54 49585 → 7192 [SYN] Seq=0 Win=8192 Len=0
  7651 33.322540  167.78.189.77  167.78.10.156  TCP        54 7192 → 49585 [SYN, ACK] Seq=0 Ack=1 Win=8192 Len=0
  7652 33.322176  167.78.10.156  167.78.189.77  TCP        54 49585 → 7192 [ACK] Seq=1 Ack=1 Win=8192 Len=0
  7653 33.322176  167.78.10.156  167.78.189.77  TCP       566 49585 → 7192 [PSH, ACK] Seq=1 Ack=1 Win=8192 Len=512
  7654 33.322540  167.78.189.77  167.78.10.156  TCP        54 7192 → 49585 [ACK] Seq=1 Ack=513 Win=8192 Len=0
  7655 33.322540  167.78.189.77  167.78.10.156  TCP       566 7192 → 49585 [PSH, ACK] Seq=1 Ack=513 Win=8192 Len=512
  7656 33.322176  167.78.10.156  167.78.189.77  TCP        54 49585 → 7192 [ACK] Seq=513 Ack=513 Win=8192 Len=0
  7657 33.322540  167.78.189.77  167.78.10.156  TCP        54 7192 → 49585 [FIN, ACK] Seq=513 Ack=513 Win=8192 Len=0
  7658 33.322176  167.78.10.156  167.78.189.77  TCP        54 49585 → 7192 [ACK] Seq=513 Ack=514 Win=8192 Len=0
  7659 33.322176  167.78.10.156  167.78.189.77  TCP        54 49585 → 7192 [FIN, ACK] Seq=513 Ack=514 Win=8192 Len=0
```

```
› Frame 6452: 95 bytes on wire (760 bits), 95 bytes captured (760 bits)
› Ethernet II, Src: 00:62:4d:64:57:4b (00:62:4d:64:57:4b), Dst: 00:61:46:6b:76:66 (00:61:46:6b:76:66)
› Internet Protocol Version 4, Src: 167.78.10.156, Dst: 41.87.240.150
› User Datagram Protocol, Src Port: 65490, Dst Port: 53
› Domain Name System (query)
```

```
0000  00 61 46 6b 76 66 00 62  4d 64 57 4b 08 00 45 00   ·aFkvf·b MdWK··E·
0010  00 51 00 01 00 00 40 11  ae c3 a7 4e 0a 9c 29 57   ·Q····@· ···N··)W
0020  f0 96 ff d2 00 35 00 3d  55 3b 00 00 01 00 00 01   ·····5·= U;······
0030  00 00 00 00 00 00 07 37  62 64 35 39 34 64 04 64   ·······7 bd594d·d
0040  61 74 61 09 65 6c 65 63  74 69 6f 6e 73 08 76 61   ata·elec tions·va
0050  6c 76 65 72 64 65 03 67  6f 76 00 00 01 00 01      lverde·g ov·····
```

```
artifact.pcap                                   Packets: 53794 · Displayed: 51 (0.1%)                    Profile: Default
```

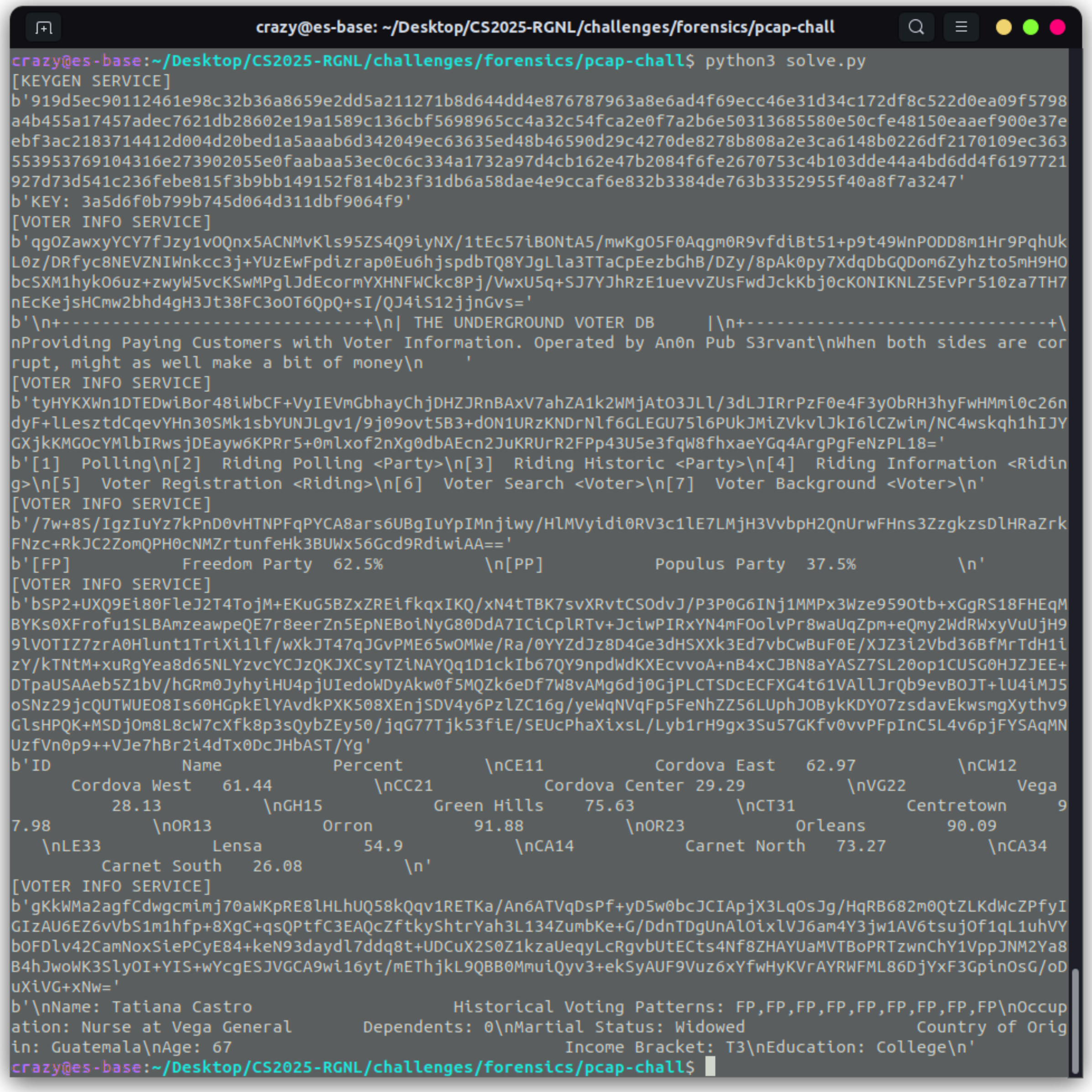
They have much less traffic. They fetch file.zip, and connect to two other services, one on port 7192, and the other on port 5721.

Because they need to generate a session key before they can connect to the voter information service, we can assume the first service is a key gen service, and the second is the voter information service. Let's write a script to extract the traffic, passing the session key obtained from the first service to decrypt the traffic from the second.
The decrypt functions are implemented based on the crypto algorithms given in the hint, and were the first results on google. It may take a few tries to get the right one.

```python
from scapy.all import *
from cryptography.hazmat.primitives import hashes
from cryptography.hazmat.primitives.asymmetric import rsa, padding
from cryptography.hazmat.primitives import serialization
import base64
from Cryptodome.Cipher import AES
from Cryptodome.Hash import SHA256
from Cryptodome import Random
from pathlib import Path

r = rdpcap("artifact.pcap")

n = len(r)
client_ip = "167.78.10.156"

keygen_service_port = 7192
voter_info_service_port = 5721

```

```
def decrypt(message_encrypted, private_key):
  try:
      message_decrypted = private_key.decrypt(
          message_encrypted,
          padding.OAEP(
              mgf=padding.MGF1(algorithm=hashes.SHA256()),
              algorithm=hashes.SHA256(),
              label=None
          )
      )
      return message_decrypted
  except ValueError:
      return "Failed to Decrypt"

def decrypt0(key, source, decode=True):
   if decode:
       source = base64.b64decode(source)
   key = SHA256.new(key).digest()  # use SHA-256 over our key to get a
proper-sized AES key
   IV = source[:AES.block_size]  # extract the IV from the beginning
   decryptor = AES.new(key, AES.MODE_CBC, IV)
   data = decryptor.decrypt(source[AES.block_size:])  # decrypt
   padding = data[-1]  # pick the padding value from the end; Python 2.x:
ord(data[-1])
   if data[-padding:] != bytes([padding]) * padding:  # Python 2.x:
chr(padding) * padding
       raise ValueError("Invalid padding...")
   return data[:-padding]  # remove the padding


private_pem_bytes = Path("keys/client_private_key.pem").read_bytes()
client_priv = serialization.load_pem_private_key(private_pem_bytes,
password=None)

key = b""
for i in range(n):
   pkt = r[i]
   is_tcp = pkt.haslayer(TCP)
   if Raw in pkt and r[i].haslayer(TCP) and pkt[TCP].sport ==
keygen_service_port and pkt[IP].dst == client_ip:
       print(pkt[TCP].load)
       resp = pkt[TCP].load
       resp = resp.decode()
       resp = bytes.fromhex(resp)
       msg = decrypt(resp, client_priv)
       print(msg)
       msg = msg.decode()
       key = msg.replace("KEY: ", "").encode()
   if Raw in pkt and r[i].haslayer(TCP) and pkt[TCP].sport ==
voter_info_service_port and pkt[IP].dst == client_ip:
       if key == b"":
           print('ERROR!')
       else:
           print(pkt[TCP].load)
           resp = pkt[TCP].load
           msg = decrypt0(key, resp)
           print(msg)
```

Output:



```
crazy@es-base: ~/Desktop/CS2025-RGNL/challenges/forensics/pcap-chall
crazy@es-base:~/Desktop/CS2025-RGNL/challenges/forensics/pcap-chall$ python3 solve.py
[KEYGEN SERVICE]
b'919d5ec90112461e98c32b36a8659e2dd5a211271b8d644dd4e876787963a8e6ad4f69ecc46e31d34c172df8c522d0ea09f5798
a4b455a17457adec7621db28602e19a1589c136cbf5698965cc4a32c54fca2e0f7a2b6e50313685580e50cfe48150eaaef900e37e
ebf3ac2183714412d004d20bed1a5aaab6d342049ec63635ed48b46590d29c4270de8278b808a2e3ca6148b0226df2170109ec363
553953769104316e273902055e0faabaa53ec0c6c334a1732a97d4cb162e47b2084f6fe2670753c4b103dde44a4bd6dd4f6197721
927d73d541c236febe815f3b9bb149152f814b23f31db6a58dae4e9ccaf6e832b3384de763b3352955f40a8f7a3247'
b'KEY: 3a5d6f0b799b745d064d311dbf9064f9'
[VOTER INFO SERVICE]
b'qgOZawxyYCY7fJzy1vOQnx5ACNMvKls95ZS4Q9iyNX/1tEc57iBONtA5/mwKgO5F0Aqgm0R9vfdiBt51+p9t49WnPODD8m1Hr9PqhUk
L0z/DRfyc8NEVZNIWnkcc3j+YUzEwFpdizrap0Eu6hjspdbTQ8YJgLla3TTaCpEezbGhB/DZy/8pAk0py7XdqDbGQDom6Zyhzto5mH9HO
bcSXM1hykO6uz+zwyW5vcKSwMPglJdEcormYXHNFWCkc8Pj/VwxU5q+SJ7YJhRzE1uevvZUsFwdJckKbj0cKONIKNLZ5EvPr510za7TH7
nEcKejsHCmw2bhd4gH3Jt38FC3oOT6QpQ+sI/QJ4iS12jjnGvs='
b'\n+------------------------------+\n| THE UNDERGROUND VOTER DB      |\n+------------------------------+\
nProviding Paying Customers with Voter Information. Operated by An0n Pub S3rvant\nWhen both sides are cor
rupt, might as well make a bit of money\n    '
[VOTER INFO SERVICE]
b'tyHYKXWn1DTEDwiBor48iWbCF+VyIEVmGbhayChjDHZJRnBAxV7ahZA1k2WMjAtO3JLl/3dLJIRrPzF0e4F3yObRH3hyFwHMmi0c26n
dyF+lLesztdCqevYHn30SMk1sbYUNJLgv1/9j09ovt5B3+dON1URzKNDrNlf6GLEGU75l6PUkJMiZVkvlJkI6lCZwim/NC4wskqh1hIJY
GXjkKMGOcYMlbIRwsjDEayw6KPRr5+0mlxof2nXg0dbAEcn2JuKRUrR2FPp43U5e3fqW8fhxaeYGq4ArgPgFeNzPL18='
b'[1]  Polling\n[2]  Riding Polling <Party>\n[3]  Riding Historic <Party>\n[4]  Riding Information <Ridin
g>\n[5]  Voter Registration <Riding>\n[6]  Voter Search <Voter>\n[7]  Voter Background <Voter>\n'
[VOTER INFO SERVICE]
b'/7w+8S/IgzIuYz7kPnD0vHTNPFqPYCA8ars6UBgIuYpIMnjiwy/HlMVyidi0RV3c1lE7LMjH3VvbpH2QnUrwFHns3ZzgkzsDlHRaZrk
FNzc+RkJC2ZomQPH0cNMZrtunfeHk3BUWx56Gcd9RdiwiAA=='
b'[FP]          Freedom Party  62.5%          \n[PP]          Populus Party  37.5%          \n'
[VOTER INFO SERVICE]
b'bSP2+UXQ9Ei80FleJ2T4TojM+EKuG5BZxZREifkqxIKQ/xN4tTBK7svXRvtCSOdvJ/P3P0G6INj1MMPx3Wze959Otb+xGgRS18FHEqM
BYKs0XFrofu1SLBAmzeawpeQE7r8eerZn5EpNEBoiNyG80DdA7ICiCplRTv+JciwPIRxYN4mFOolvPr8waUqZpm+eQmy2WdRWxyVuUjH9
9lVOTIZ7zrA0Hlunt1TriXi1lf/wXkJT47qJGvPME65wOMWe/Ra/0YYZdJz8D4Ge3dHSXXk3Ed7vbCwBuF0E/XJZ3i2Vbd36BfMrTdH1i
zY/kTNtM+xuRgYea8d65NLYzvcYCJzQKJXCsyTZiNAYQq1D1ckIb67QY9npdWdKXEcvvoA+nB4xCJBN8aYASZ7SL20op1CU5G0HJZJEE+
DTpaUSAAeb5Z1bV/hGRm0JyhyiHU4pjUIedoWDyAkw0f5MQZk6eDf7W8vAMg6dj0GjPLCTSDcECFXG4t61VAllJrQb9evBOJT+lU4iMJ5
oSNz29jcQUTWUEO8Is60HGpkElYAvdkPXK508XEnjSDV4y6PzlZC16g/yeWqNVqFp5FeNhZZ56LUphJOBykKDYO7zsdavEkwsmgXythv9
GlsHPQK+MSDjOm8L8cW7cXfk8p3sQybZEy50/jqG77Tjk53fiE/SEUcPhaXixsL/Lyb1rH9gx3Su57GKfv0vvPFpInC5L4v6pjFYSAqMN
UzfVn0p9++VJe7hBr2i4dTx0DcJHbAST/Yg'
b'ID           Name           Percent          \nCE11           Cordova East   62.97          \nCW12
      Cordova West   61.44          \nCC21           Cordova Center 29.29          \nVG22           Vega
        28.13          \nGH15           Green Hills    75.63          \nCT31           Centretown     9
7.98          \nOR13           Orron          91.88          \nOR23           Orleans        90.09
   \nLE33           Lensa          54.9           \nCA14           Carnet North   73.27          \nCA34
         Carnet South   26.08          \n'
[VOTER INFO SERVICE]
b'gKkWMa2agfCdwgcmimj70aWKpRE8lHLhUQ58kQqv1RETKa/An6ATVqDsPf+yD5w0bcJCIApjX3LqOsJg/HqRB682m0QtZLKdWcZPfyI
GIzAU6EZ6vVbS1m1hfp+8XgC+qsQPtfC3EAQcZftkyShtrYah3L134ZumbKe+G/DdnTDgUnAlOixlVJ6am4Y3jw1AV6tsujOf1qL1uhVY
bOFDlv42CamNoxSiePCyE84+keN93daydl7ddq8t+UDCuX2S0Z1kzaUeqyLcRgvbUtECts4Nf8ZHAYUaMVTBoPRTzwnChY1VppJNM2Ya8
B4hJwoWK3SlyOI+YIS+wYcgESJVGCA9wi16yt/mEThjkL9QBB0MmuiQyv3+ekSyAUF9Vuz6xYfwHyKVrAYRWFML86DjYxF3GpinOsG/oD
uXiVG+xNw='
b'\nName: Tatiana Castro                    Historical Voting Patterns: FP,FP,FP,FP,FP,FP,FP,FP,FP\nOccup
ation: Nurse at Vega General       Dependents: 0\nMartial Status: Widowed                 Country of Orig
in: Guatemala\nAge: 67                              Income Bracket: T3\nEducation: College\n'
crazy@es-base:~/Desktop/CS2025-RGNL/challenges/forensics/pcap-chall$ 
```

And we can see the profession of Tatiana Castro in the output.
Flag: `Nurse at Vega General`

<u>A mistake I made:</u>
I used b"3a5d6f0b799b745d064d311dbf9064f9" instead of the actual byte values as the key when encrypting with AES, and it confused a lot of people. Its still something that could happen, but its unexpected.

DONE!
FEEDBACK IS WELCOME :)