ASSIGNMENT 4

Purva Naresh Rumde

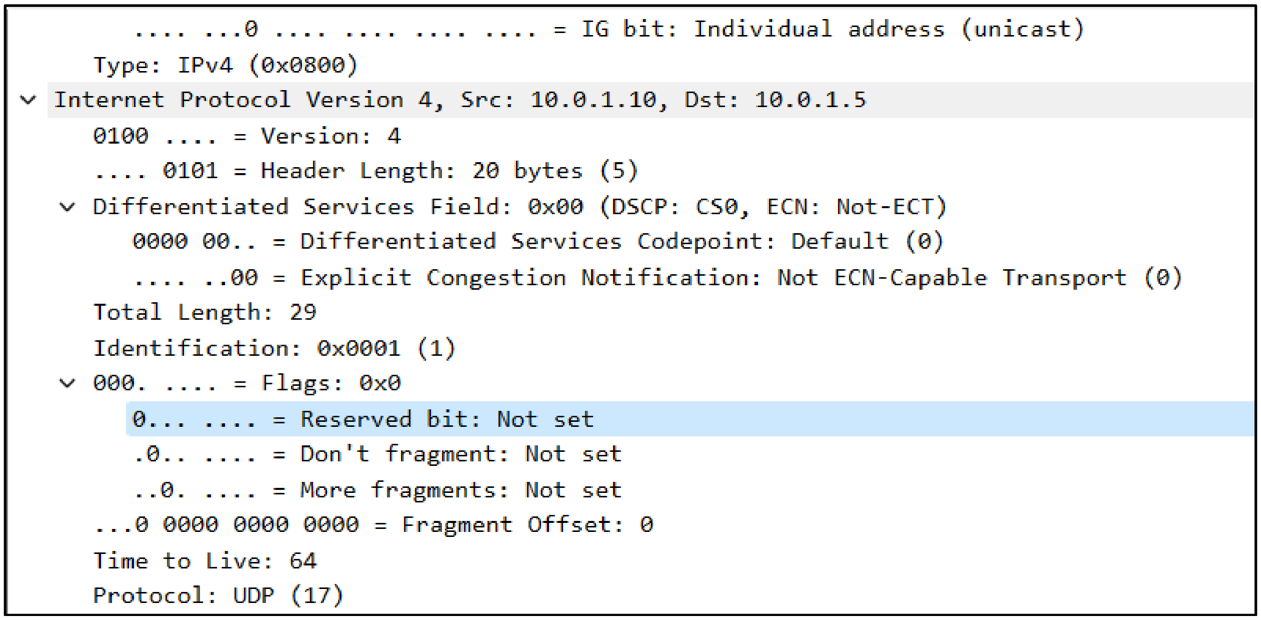
Problem ID	Captured Flag	Steps
P1	flag{3V1L_817_3xf1l7R4710N_4_7H3_W1N_51D43c8000034d0c}	Open the pcap file in Wireshark. Apply a filter to display only packets with the reserved bit set to 0. Examine each filtered packet and record the last character from each packet, as it represents part of the flag.
P2	flag{74573_Y0u_c4N_533}	Open the file in Wireshark. Apply a filter to display traffic with the specified source and destination IP addresses. Locate and extract the 6th stream. Use CyberChef to decode the contents and obtain an image. Convert the image from hexadecimal format to retrieve the flag.
P3	flag{9ebd4718347e389aaa2a3241624a 15}	Mount the disk image. List all hidden files. Locate the .docx file and open it in CyberChef. Extract all contents from the .docx file. Utilize the image containing a QR code and input the extracted text into CyberChef. Decode the text from base64 and hexadecimal to obtain the flag.
P4		

Detailed Explanations (Including Screenshots)

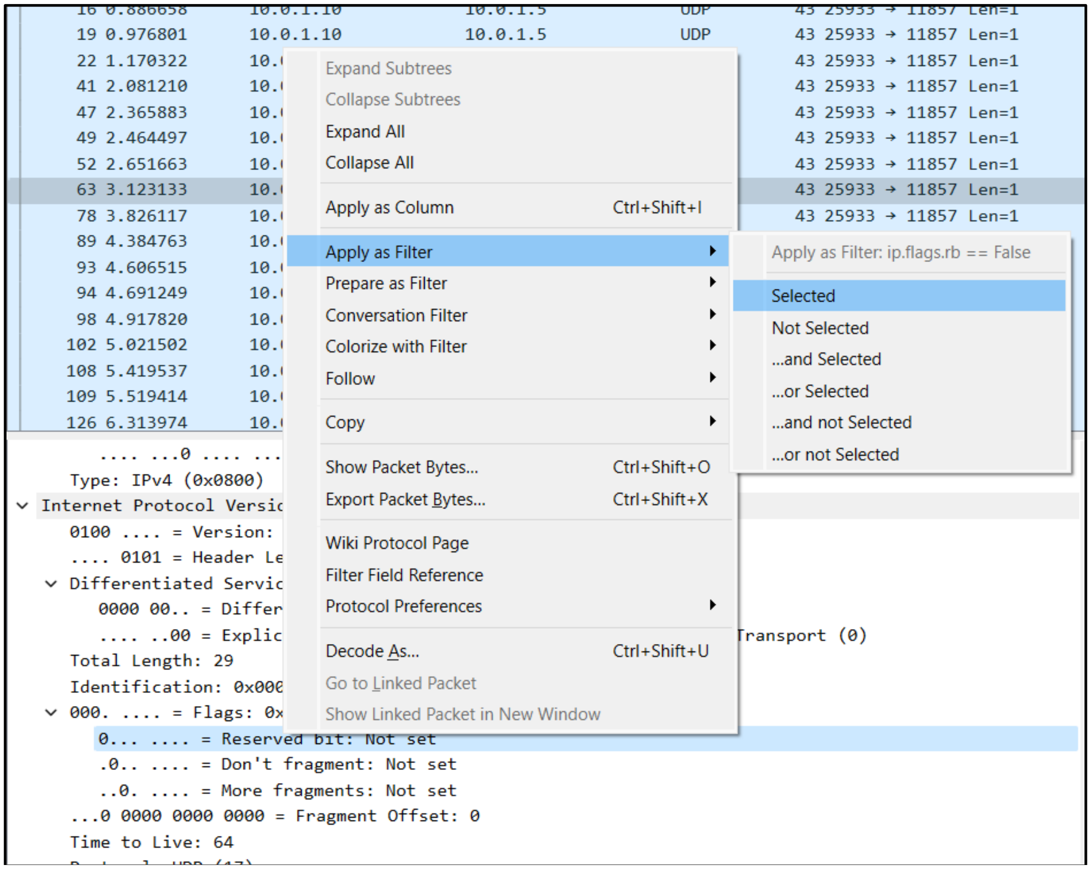
Q1.

1. Open the pcap file in Wireshark.
2. Apply a filter to display only packets with the reserved bit set to 0.
3. Examine each filtered packet and record the last character from each packet, as it represents part of the flag.
4. After loading the PCAP file into Wireshark, I examined several packets and identified a distinct pattern in the reserve bit for a specific set of packets.
5. I discovered that certain packets had their reserve bit set to zero, while others had different values. Using Wireshark's filter option, I isolated packets with the reserve bit set to zero.
6. Once filtered, I observed that the last byte in the hexadecimal dump indicated a flag.

7. By systematically analyzing each filtered packet and recording the last characters, I compiled the following sequence of characters on my notepad.

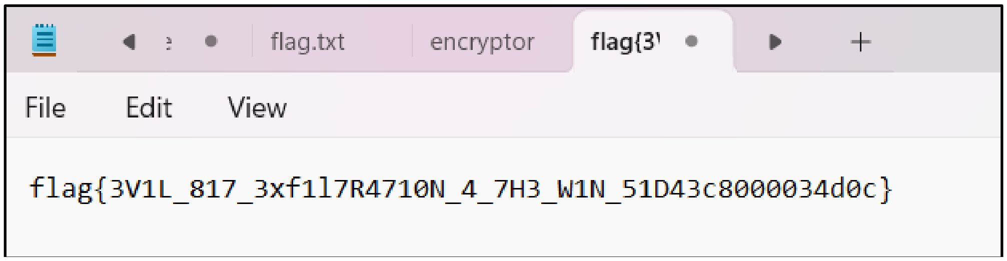


```
      .... ...0 .... .... .... .... = IG bit: Individual address (unicast)
    Type: IPv4 (0x0800)
⌄ Internet Protocol Version 4, Src: 10.0.1.10, Dst: 10.0.1.5
    0100 .... = Version: 4
    .... 0101 = Header Length: 20 bytes (5)
  ⌄ Differentiated Services Field: 0x00 (DSCP: CS0, ECN: Not-ECT)
      0000 00.. = Differentiated Services Codepoint: Default (0)
      .... ..00 = Explicit Congestion Notification: Not ECN-Capable Transport (0)
    Total Length: 29
    Identification: 0x0001 (1)
  ⌄ 000. .... = Flags: 0x0
      0... .... = Reserved bit: Not set
      .0.. .... = Don't fragment: Not set
      ..0. .... = More fragments: Not set
    ...0 0000 0000 0000 = Fragment Offset: 0
    Time to Live: 64
    Protocol: UDP (17)
```



```
 16 0.886658   10.0.1.10    10.0.1.5    UDP    43 25933 → 11857 Len=1
 19 0.976801   10.0.1.10    10.0.1.5    UDP    43 25933 → 11857 Len=1
 22 1.170322   10.                             43 25933 → 11857 Len=1
 41 2.081210   10.                             43 25933 → 11857 Len=1
 47 2.365883   10.                             43 25933 → 11857 Len=1
 49 2.464497   10.                             43 25933 → 11857 Len=1
 52 2.651663   10.                             43 25933 → 11857 Len=1
 63 3.123133   10.                             43 25933 → 11857 Len=1
 78 3.826117   10.                             43 25933 → 11857 Len=1
 89 4.384763   10.
 93 4.606515   10.
 94 4.691249   10.
 98 4.917820   10.
102 5.021502   10.
108 5.419537   10.
109 5.519414   10.
126 6.313974   10.
```

```
      .... ...0 .... ...
    Type: IPv4 (0x0800)
⌄ Internet Protocol Versio
    0100 .... = Version:
    .... 0101 = Header Le
  ⌄ Differentiated Servic
      0000 00.. = Differ
      .... ..00 = Explic                                 Transport (0)
    Total Length: 29
    Identification: 0x000
  ⌄ 000. .... = Flags: 0x
      0... .... = Reserved bit: Not set
      .0.. .... = Don't fragment: Not set
      ..0. .... = More fragments: Not set
    ...0 0000 0000 0000 = Fragment Offset: 0
    Time to Live: 64
```



```
flag{3V1L_817_3xf1l7R4710N_4_7H3_W1N_51D43c8000034d0c}
```

Q2.

1. Open the file in Wireshark.
2. Apply a filter to display traffic with the specified source and destination IP addresses.
3. Locate and extract the 6th stream.
4. Use CyberChef to decode the contents and obtain an image.
5. Convert the image from hexadecimal format to retrieve the flag.

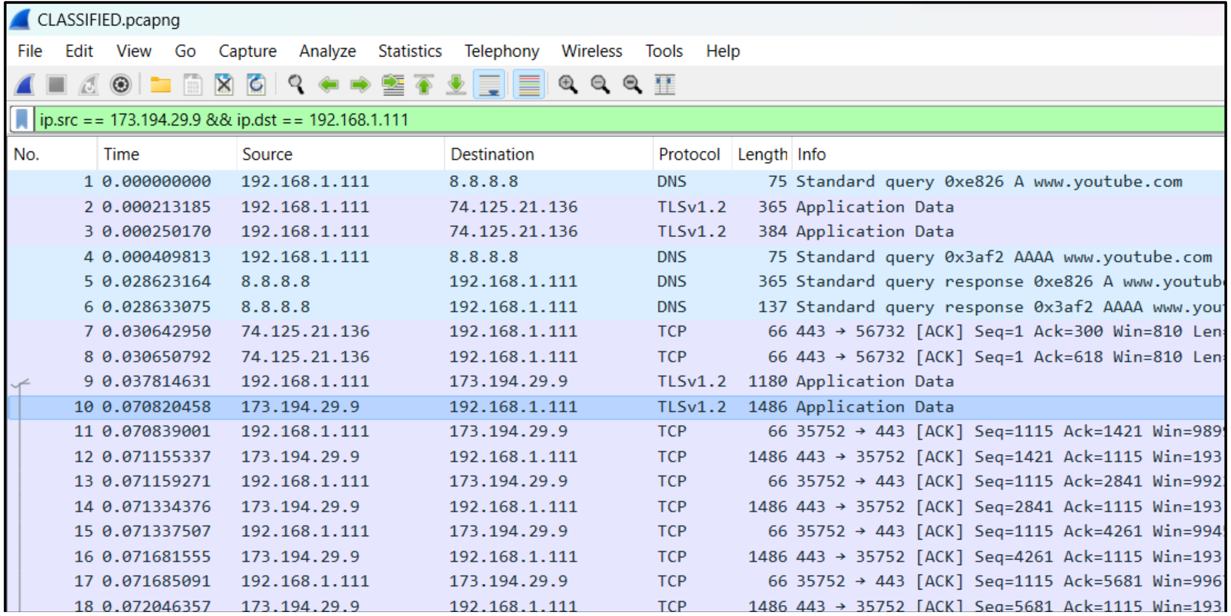
I analyzed the file in Wireshark to examine the generated packets, particularly focusing on those originating from 173.194.29.9 and destined for 192.168.1.111, which appeared to be repeated multiple times and part of internal traffic.

By applying a filter to isolate packets with the specified source and destination addresses, I refined my analysis to focus solely on relevant packets.

Upon inspecting the packet streams, I identified the sixth stream as containing substantial content. Notably, at the end of this packet's content, there was a string ending with an equals sign, indicative of a base64 representation.

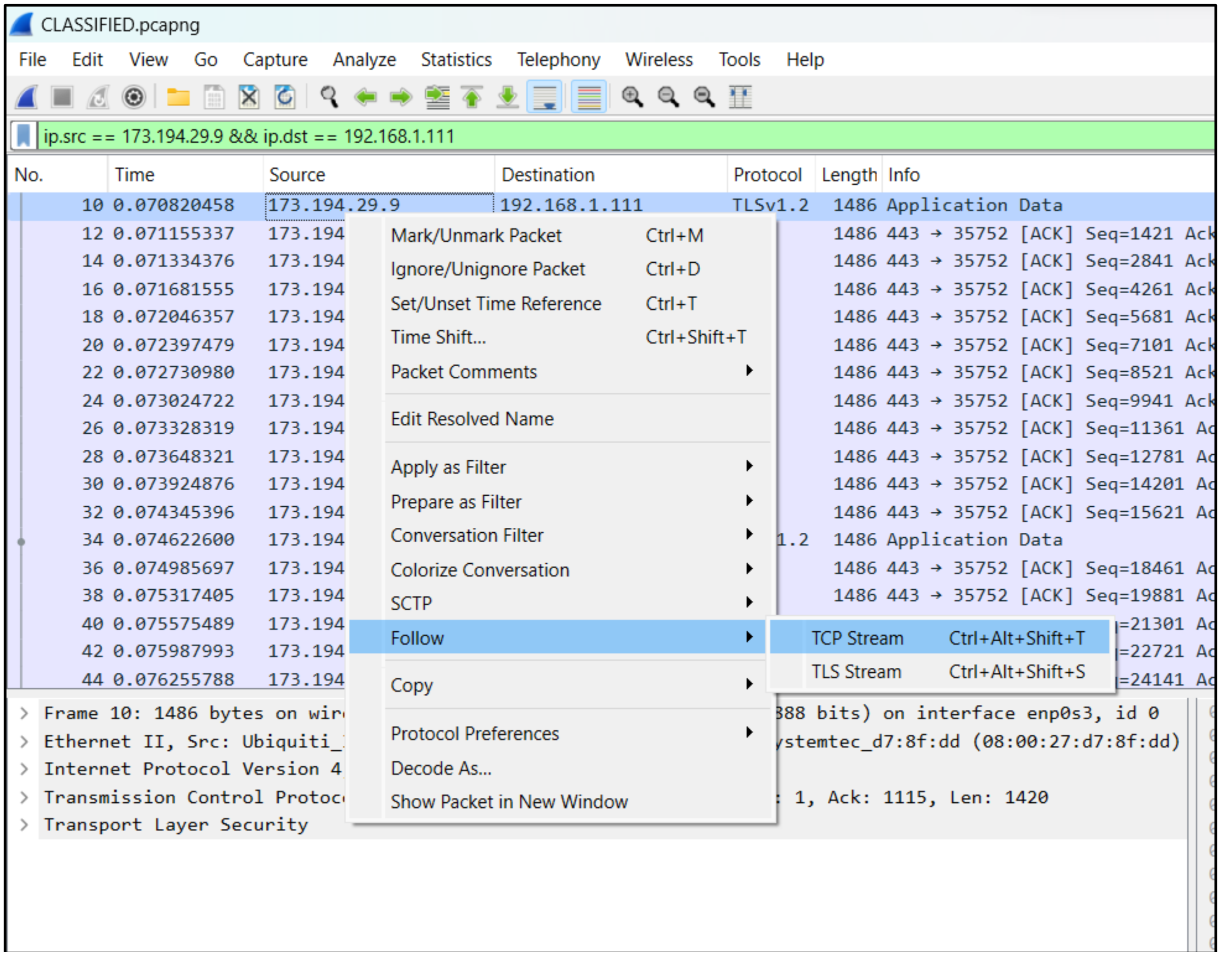
Using CyberChef, I decoded the base64-encoded string and discovered the presence of a JFIF file signature, signaling an image file. Consequently, I utilized text-to-image translation to obtain the image.

Despite considerable efforts to decode the image using techniques like steganography, no meaningful information was revealed. However, further experimentation in CyberChef revealed that decoding from hexadecimal produced the flag.



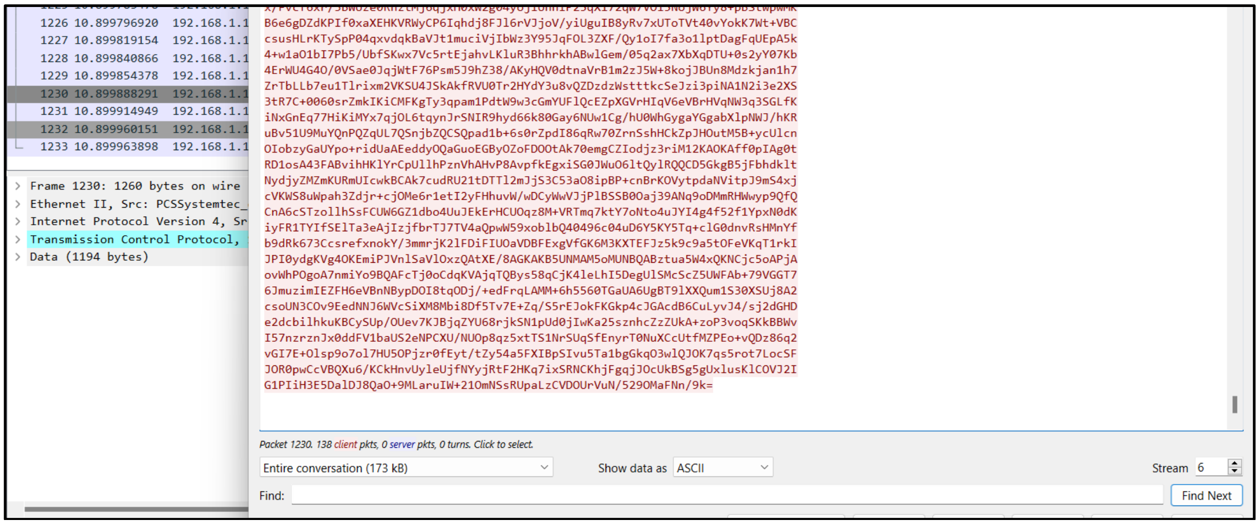
CLASSIFIED.pcapng
File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help

```
ip.src == 173.194.29.9 && ip.dst == 192.168.1.111

No.   Time          Source          Destination     Protocol  Length Info
    1 0.000000000   192.168.1.111   8.8.8.8         DNS         75 Standard query 0xe826 A www.youtube.com
    2 0.000213185   192.168.1.111   74.125.21.136   TLSv1.2    365 Application Data
    3 0.000250170   192.168.1.111   74.125.21.136   TLSv1.2    384 Application Data
    4 0.000409813   192.168.1.111   8.8.8.8         DNS         75 Standard query 0x3af2 AAAA www.youtube.com
    5 0.028623164   8.8.8.8         192.168.1.111   DNS        365 Standard query response 0xe826 A www.youtub
    6 0.028633075   8.8.8.8         192.168.1.111   DNS        137 Standard query response 0x3af2 AAAA www.you
    7 0.030642950   74.125.21.136   192.168.1.111   TCP         66 443 → 56732 [ACK] Seq=1 Ack=300 Win=810 Len
    8 0.030650792   74.125.21.136   192.168.1.111   TCP         66 443 → 56732 [ACK] Seq=1 Ack=618 Win=810 Len
    9 0.037814631   192.168.1.111   173.194.29.9    TLSv1.2   1180 Application Data
   10 0.070820458   173.194.29.9    192.168.1.111   TLSv1.2   1486 Application Data
   11 0.070839001   192.168.1.111   173.194.29.9    TCP         66 35752 → 443 [ACK] Seq=1115 Ack=1421 Win=989
   12 0.071155337   173.194.29.9    192.168.1.111   TCP       1486 443 → 35752 [ACK] Seq=1421 Ack=1115 Win=193
   13 0.071159271   192.168.1.111   173.194.29.9    TCP         66 35752 → 443 [ACK] Seq=1115 Ack=2841 Win=992
   14 0.071334376   173.194.29.9    192.168.1.111   TCP       1486 443 → 35752 [ACK] Seq=2841 Ack=1115 Win=193
   15 0.071337507   192.168.1.111   173.194.29.9    TCP         66 35752 → 443 [ACK] Seq=1115 Ack=4261 Win=994
   16 0.071681555   173.194.29.9    192.168.1.111   TCP       1486 443 → 35752 [ACK] Seq=4261 Ack=1115 Win=193
   17 0.071685091   192.168.1.111   173.194.29.9    TCP         66 35752 → 443 [ACK] Seq=1115 Ack=5681 Win=996
   18 0.072046357   173.194.29.9    192.168.1.111   TCP       1486 443 → 35752 [ACK] Seq=5681 Ack=1115 Win=193
```



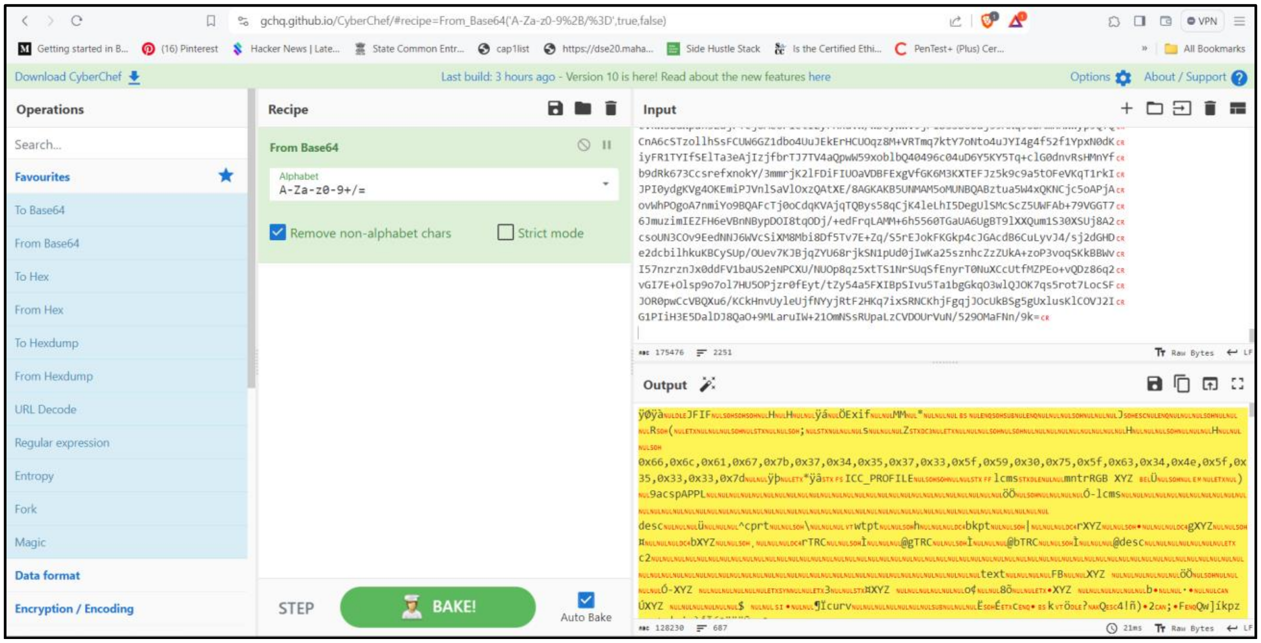
CLASSIFIED.pcapng
File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help
Mark/Unmark Packet Ctrl+M
Ignore/Unignore Packet Ctrl+D
Set/Unset Time Reference Ctrl+T
Time Shift... Ctrl+Shift+T
Packet Comments
Edit Resolved Name
Apply as Filter
Prepare as Filter
Conversation Filter
Colorize Conversation
SCTP
Follow
Copy
Protocol Preferences
Decode As...
Show Packet in New Window
TCP Stream Ctrl+Alt+Shift+T
TLS Stream Ctrl+Alt+Shift+S

```
ip.src == 173.194.29.9 && ip.dst == 192.168.1.111

No.   Time          Source          Destination     Protocol  Length Info
   10 0.070820458   173.194.29.9    192.168.1.111   TLSv1.2   1486 Application Data
   12 0.071155337   173.194                                   1486 443 → 35752 [ACK] Seq=1421 Ack
   14 0.071334376   173.194                                   1486 443 → 35752 [ACK] Seq=2841 Ack
   16 0.071681555   173.194                                   1486 443 → 35752 [ACK] Seq=4261 Ack
   18 0.072046357   173.194                                   1486 443 → 35752 [ACK] Seq=5681 Ack
   20 0.072397479   173.194                                   1486 443 → 35752 [ACK] Seq=7101 Ack
   22 0.072730980   173.194                                   1486 443 → 35752 [ACK] Seq=8521 Ack
   24 0.073024722   173.194                                   1486 443 → 35752 [ACK] Seq=9941 Ack
   26 0.073328319   173.194                                   1486 443 → 35752 [ACK] Seq=11361 Ac
   28 0.073648321   173.194                                   1486 443 → 35752 [ACK] Seq=12781 Ac
   30 0.073924876   173.194                                   1486 443 → 35752 [ACK] Seq=14201 Ac
   32 0.074345396   173.194                                   1486 443 → 35752 [ACK] Seq=15621 Ac
   34 0.074622600   173.194                            1.2    1486 Application Data
   36 0.074985697   173.194                                   1486 443 → 35752 [ACK] Seq=18461 Ac
   38 0.075317405   173.194                                   1486 443 → 35752 [ACK] Seq=19881 Ac
   40 0.075575489   173.194                                                            =21301 Ac
   42 0.075987993   173.194                                                            =22721 Ac
   44 0.076255788   173.194                                                            =24141 Ac

> Frame 10: 1486 bytes on wir                          388 bits) on interface enp0s3, id 0
> Ethernet II, Src: Ubiquiti_                          ystemtec_d7:8f:dd (08:00:27:d7:8f:dd)
> Internet Protocol Version 4
> Transmission Control Protoc                          : 1, Ack: 1115, Len: 1420
> Transport Layer Security
```



```
1226 10.899796920  192.168.1.1
1227 10.899819154  192.168.1.1
1228 10.899840866  192.168.1.1
1229 10.899854378  192.168.1.1
1230 10.899888291  192.168.1.1
1231 10.899914949  192.168.1.1
1232 10.899960151  192.168.1.1
1233 10.899963898  192.168.1.1

> Frame 1230: 1260 bytes on wire
> Ethernet II, Src: PCSSystemtec_
> Internet Protocol Version 4, Sr
> Transmission Control Protocol,
> Data (1194 bytes)
```

```
B6e6gDZdKPIf0xaXEHKVRWyCP6Iqhdj8FJl6rVJjoV/yiUguIB8yRv7xUToTVt40vYokK7Wt+VBC
csusHLrKTySpP04qxvdqkBaVJt1muciVjIbWz3Y95JqFOL3ZXF/Qy1oI7fa3o1lptDagFqUEpA5k
4+w1aO1bI7Pb5/UbfSKwx7Vc5rtEjahvLKluR3BhhrkhABwlGem/05q2ax7XbXqDTU+0s2yY07Kb
4ErWU4G4O/0VSae0JqjWtF76Psm5J9hZ38/AKyHQV0dtnaVrB1m2zJ5W+8kojJBUn8Mdzkjan1h7
ZrTbLLb7eu1Tlrixm2VKSU4JSkAkfRVU0Tr2HYdY3u8vQZDzdzWstttkcSeJzi3piNA1N2i3e2XS
3tR7C+0060srZmkIKiCMFKgTy3qpam1PdtW9w3cGmYUFlQcEZpXGVrHIqV6eVBrHVqNW3q3SGLfK
iNxGnEq77HiKiMYx7qjOL6tqynJrSNIR9hyd66k80Gay6NUw1Cg/hU0WhGygaYGgabXlpNWJ/hKR
uBv51U9MuYQnPQZqUL7QSnjbZQCSQpad1b+6s0rZpdI86qRw70ZrnSshHCkZpJHOutM5B+ycUlcn
OIobzyGaUYpo+ridUaAEeddyOQaGuoEGByOZoFDOOtAk70emgCZIodjz3riM12KAOKAff0pIAg0t
RD1osA43FABvihHKlYrCpUllhPznVhAHvP8AvpfkEgxiSG0JWuO6ltQylRQQCD5GkgB5jFbhdklt
NydjyZMZmKURmUIcwkBCAk7cudRU21tDTTl2mJjS3C53aO8ipBP+cnBrKOVytpdaNVitpJ9mS4xj
cVKWS8uWpah3Zdjr+cjOMe6r1etI2yFHhuvW/wDCyWwVJjPlBSSB0Oaj39ANq9oDMmRHWwyp9QfQ
CnA6cSTzollhSsFCUW6GZ1dbo4UuJEkErHCUOqz8M+VRTmq7ktY7oNto4uJYI4g4f52f1YpxN0dK
iyFR1TYIfSElTa3eAjIzjfbrTJ7TV4aQpwW59xoblbQ40496c04uD6Y5KY5Tq+clG0dnvRsHMnYf
b9dRk673CcsrefxnokY/3mmrjK2lFDiFIUOaVDBFExgVfGK6M3KXTEFJz5k9c9a5tOFeVKqT1rkI
JPI0ydgKVg4OKEmiPJVnlSaVlOxzQAtXE/8AGKAKB5UNMAM5oMUNBQABztua5W4xQKNCjc5oAPjA
ovWhPOgoA7nmiYo9BQAFcTj0oCdqKVAjqTQBys58qCjK4leLhI5DegUlSMcScZ5UWFAb+79VGGT7
6JmuzimIEZFH6eVBnNBypDOI8tqODj/+edFrqLAMM+6h5560TGaUA6UgBT9lXXQum1S30XSUj8A2
csoUN3COv9EedNNJ6WVcSiXM8Mbi8Df5Tv7E+Zq/S5rEJokFKGkp4cJGAcdB6CuLyvJ4/sj2dGHD
e2dcbilhkuKBCySUp/OUev7KJBjqZYU68rjkSN1pUd0jIwKa25sznhcZzZUkA+zoP3voqSKkBBWv
I57nzrznJx0ddFV1baUS2eNPCXU/NUOp8qz5xtTS1NrSUqSfEnyrT0NuXCcUtfMZPEo+vQDz86q2
vGI7E+Olsp9o7ol7HU5OPjzr0fEyt/tZy54a5FXIBpSIvu5Ta1bgGkqO3wlQJOK7qs5rot7LocSF
JOR0pwCcVBQXu6/KCkHnvUyleUjfNYyjRtF2HKq7ixSRNCKhjFgqjJOcUkBSg5gUxlusKlCOVJ2I
G1PIiH3E5DalDJ8QaO+9MLaruIW+21OmNSsRUpaLzCVDOUrVuN/529OMaFNn/9k=

Packet 1230. 138 client pkts, 0 server pkts, 0 turns. Click to select.
Entire conversation (173 kB)   Show data as ASCII   Stream 6
Find:                                                Find Next
```



```
gchq.github.io/CyberChef/#recipe=From_Base64('A-Za-z0-9%2B/%3D',true,false)
```

From Base64

Alphabet
A-Za-z0-9+/=

☑ Remove non-alphabet chars ☐ Strict mode

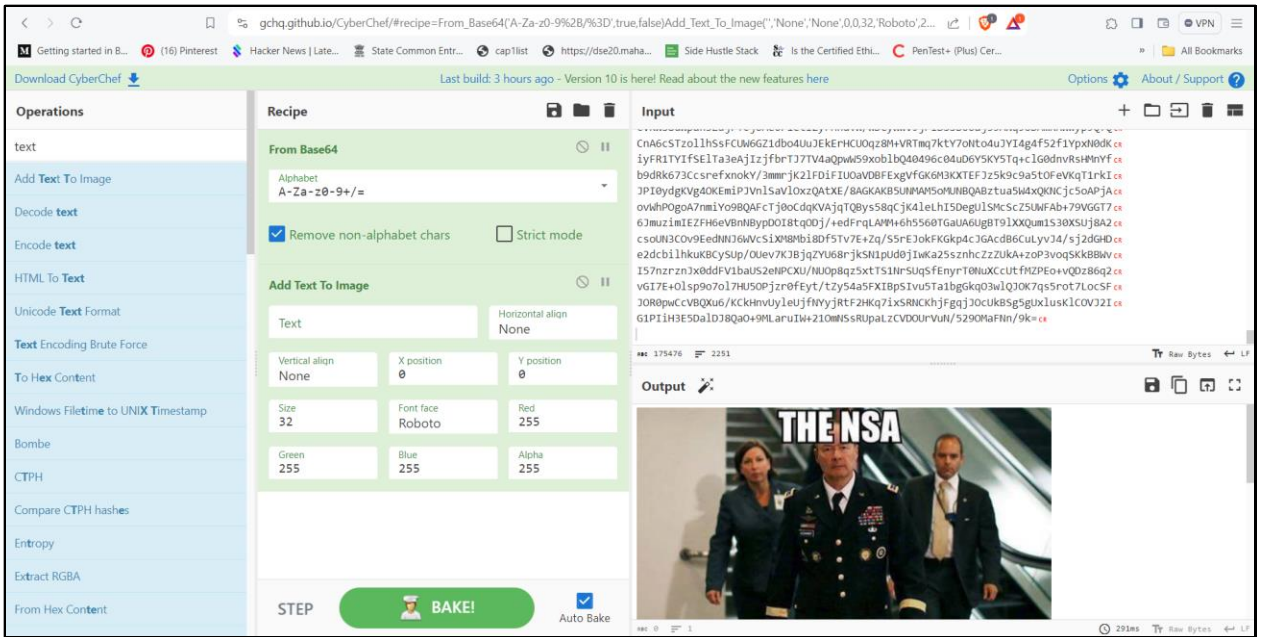
☑ Auto Bake

```
CnA6cSTzollhSsFCUW6GZ1dbo4UuJEkErHCUOqz8M+VRTmq7ktY7oNto4uJYI4g4f52f1YpxN0dK
iyFR1TYIfSElTa3eAjIzjfbrTJ7TV4aQpwW59xoblbQ40496c04uD6Y5KY5Tq+clG0dnvRsHMnYf
b9dRk673CcsrefxnokY/3mmrjK2lFDiFIUOaVDBFExgVfGK6M3KXTEFJz5k9c9a5tOFeVKqT1rkI
JPI0ydgKVg4OKEmiPJVnlSaVlOxzQAtXE/8AGKAKB5UNMAM5oMUNBQABztua5W4xQKNCjc5oAPjA
ovWhPOgoA7nmiYo9BQAFcTj0oCdqKVAjqTQBys58qCjK4leLhI5DegUlSMcScZ5UWFAb+79VGGT7
6JmuzimIEZFH6eVBnNBypDOI8tqODj/+edFrqLAMM+6h5560TGaUA6UgBT9lXXQum1S30XSUj8A2
csoUN3COv9EedNNJ6WVcSiXM8Mbi8Df5Tv7E+Zq/S5rEJokFKGkp4cJGAcdB6CuLyvJ4/sj2dGHD
e2dcbilhkuKBCySUp/OUev7KJBjqZYU68rjkSN1pUd0jIwKa25sznhcZzZUkA+zoP3voqSKkBBWv
I57nzrznJx0ddFV1baUS2eNPCXU/NUOp8qz5xtTS1NrSUqSfEnyrT0NuXCcUtfMZPEo+vQDz86q2
vGI7E+Olsp9o7ol7HU5OPjzr0fEyt/tZy54a5FXIBpSIvu5Ta1bgGkqO3wlQJOK7qs5rot7LocSF
JOR0pwCcVBQXu6/KCkHnvUyleUjfNYyjRtF2HKq7ixSRNCKhjFgqjJOcUkBSg5gUxlusKlCOVJ2I
G1PIiH3E5DalDJ8QaO+9MLaruIW+21OmNSsRUpaLzCVDOUrVuN/529OMaFNn/9k=
```

```
175476   2251                                   Raw Bytes   LF
```

```
ÿØÿàJFIFHHÿáÖExifMM*JRS(;SZHH
0x66,0x6c,0x61,0x67,0x7b,0x37,0x34,0x35,0x37,0x33,0x5f,0x59,0x30,0x75,0x5f,0x63,0x34,0x4e,0x5f,0x
35,0x33,0x33,0x7dÿþ*ÿâICC_PROFILElcmsmntrRGB XYZ ÜE)
9acspAPPLöÖÓ-lcms
descü^cprt\wtpthbkpt|rXYZgXYZ
¤bXYZrTRCÌ@gTRCÌ@bTRCÌ@desc
c2
textFBXYZ öÖ
Ó-XYZ 3¤XYZ o¢8õXYZ b
ÚXYZ $ ¶Ïcurv ËÉCkÖ?Q4!ñ)2;FQw]íkpz
```

```
128230   687                          21ms   Raw Bytes   LF
```



gchq.github.io/CyberChef/#recipe=From_Base64('A-Za-z0-9%2B/%3D',true,false)Add_Text_To_Image('','None','None',0,0,32,'Roboto',2...

Recipe

From Base64
Alphabet: A-Za-z0-9+/=
☑ Remove non-alphabet chars ☐ Strict mode

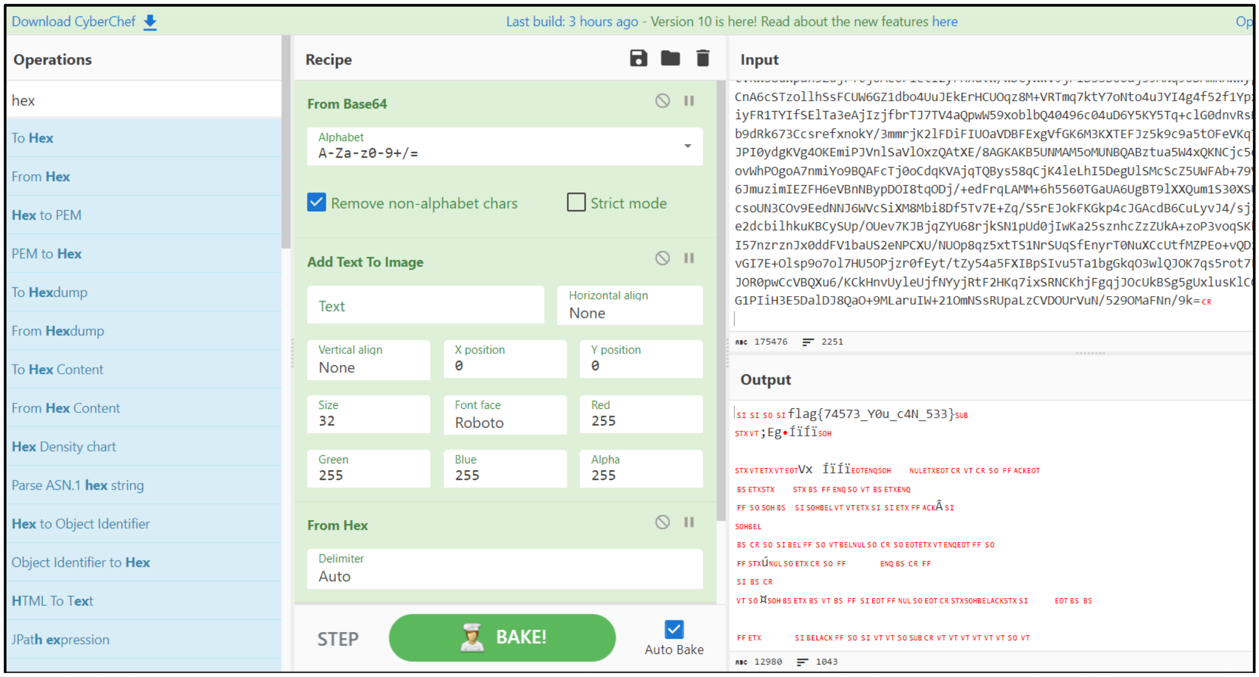
Add Text To Image
Text:
Horizontal align: None
Vertical align: None
X position: 0
Y position: 0
Size: 32
Font face: Roboto
Red: 255
Green: 255
Blue: 255
Alpha: 255

Input

```
CnA6cSTzollhSsFCUW6GZ1dbo4UuJEkErHCUOqz8M+VRTmq7ktY7oNto4uJYI4g4f52f1YpxN0dK
iyFR1TYIfSElTa3eAjIzjfbrTJ7TV4aQpwW59xoblbQ40496c04uD6Y5KY5Tq+clG0dnvRsHMnYf
b9dRk673CcsrefxnokY/3mmrjK2lFDiFIUOaVDBFExgVfGK6M3KXTEFJz5k9c9a5tOFeVKqT1rkI
JPI0ydgKVg4OKEmiPJVnlSaVlOxzQAtXE/8AGKAKB5UNMAM5oMUNBQABztua5W4xQKNCjc5oAPjA
ovWhPOgoA7nmiYo9BQAFcTj0oCdqKVAjqTQBys58qCjK4leLhI5DegUlSMcScZ5UWFAb+79VGGT7
6JmuzimIEZFH6eVBnNBypDOI8tqODj/+edFrqLAMM+6h556OTGaUA6UgBT9lXXQum1S30XSUj8A2
csoUN3COv9EedNNJ6WVcSiXM8Mbi8Df5Tv7E+Zq/S5rEJokFKGkp4cJGAcdB6CuLyvJ4/sj2dGHD
e2dcbilhkuKBCySUp/OUev7KJBjqZYU68rjkSN1pUd0jIwKa25sznhcZzZUkA+zoP3voqSKkBBWv
I57nzrznJx0ddFV1baUS2eNPCXU/NUOp8qz5xtTS1NrSUqSfEnyrT0NuXCcUtfMZPEo+vQDz86q2
vGI7E+Olsp9o7ol7HU5OPjzr0fEyt/tZy54a5FXIBpSIvu5Ta1bgGkqO3wlQJOK7qs5rot7LocSF
JOR0pwCcVBQXu6/KCkHnvUyleUjfNYyjRtF2HKq7ixSRNCKhjFgqjJOcUkBSg5gUxlusKlCOVJ2I
G1PIiH3E5DalDJ8QaO+9MLaruIW+21OmNSsRUpaLzCVDOUrVuN/529OMaFNn/9k=
```

Output

THE NSA



Download CyberChef

Last build: 3 hours ago - Version 10 is here! Read about the new features here

Recipe

From Base64
Alphabet: A-Za-z0-9+/=
☑ Remove non-alphabet chars ☐ Strict mode

Add Text To Image
Text:
Horizontal align: None
Vertical align: None
X position: 0
Y position: 0
Size: 32
Font face: Roboto
Red: 255
Green: 255
Blue: 255
Alpha: 255

From Hex
Delimiter: Auto

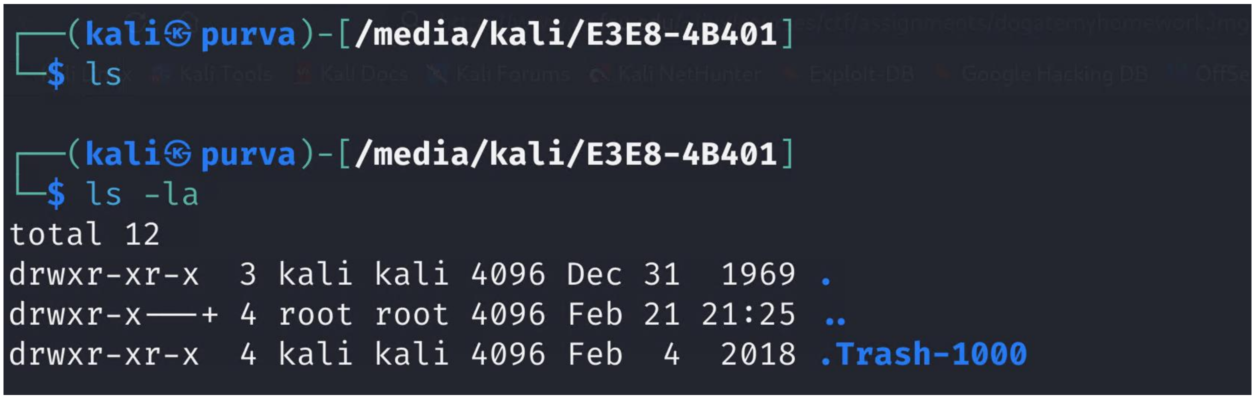
Output

```
SI SI SO SI flag{74573_Y0u_c4N_533}SUB
STX VT ;Eg•ÍïÍïSOH

STX VT ETX VT EOT Vx ÍïÍïEOT ENQ SOH    NUL ETX EOT CR VT CR SO FF ACK EOT
BS ETX STX    STX BS FF ENQ SO VT BS ETX ENQ
FF SO SOH BS   SI SOH BEL VT VT ETX SI SI ETX FF ACK Â SI
SOH BEL
BS CR SO SI BEL FF SO VT BEL NUL SO CR SO EOT ETX VT ENQ EOT FF SO
FF STX Ú NUL SO ETX CR SO FF       ENQ BS CR FF
SI BS CR
VT SO ¤SOH BS ETX BS VT BS FF SI EOT FF NUL SO EOT CR STX SOH BEL ACK STX SI      EOT BS BS

FF ETX       SI BEL ACK FF SO SI VT VT SO SUB CR VT VT VT VT VT VT SO VT
```

Q3.

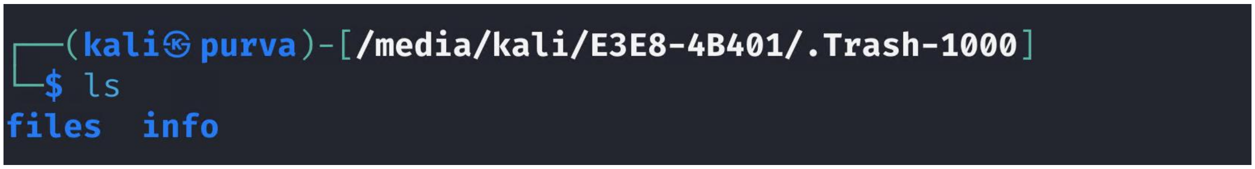
1. Mount the disk image.
2. List all hidden files.
3. Locate the .docx file and open it in CyberChef.
4. Extract all contents from the .docx file.
5. Utilize the image containing a QR code and input the extracted text into CyberChef.
6. Decode the text from base64 and hexadecimal to obtain the flag.
7. Question 3:

I mounted the file and ran the ls command to list all the files present in the folder. Since the contents were not visible, I ran the command with the -a option to print all the hidden files.



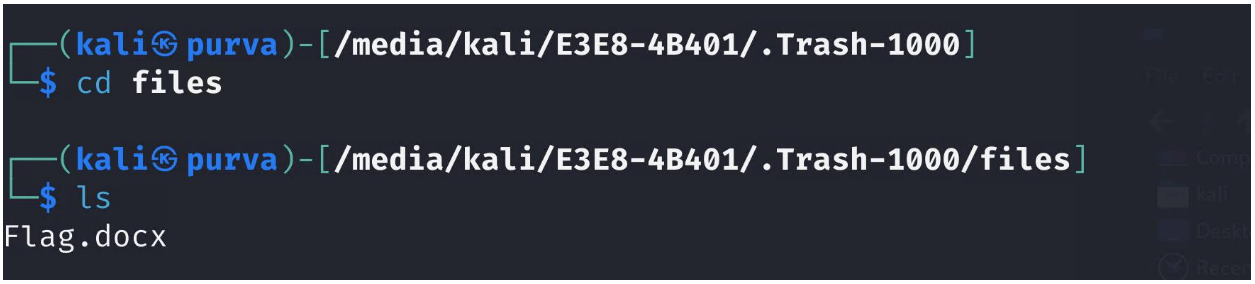
```
┌──(kali㉿purva)-[/media/kali/E3E8-4B401]
└─$ ls

┌──(kali㉿purva)-[/media/kali/E3E8-4B401]
└─$ ls -la
total 12
drwxr-xr-x  3 kali kali 4096 Dec 31  1969 .
drwxr-x───+ 4 root root 4096 Feb 21 21:25 ..
drwxr-xr-x  4 kali kali 4096 Feb  4  2018 .Trash-1000
```

I entered the Trash-1000 folder. Here, I was able to find two directories named files and info:



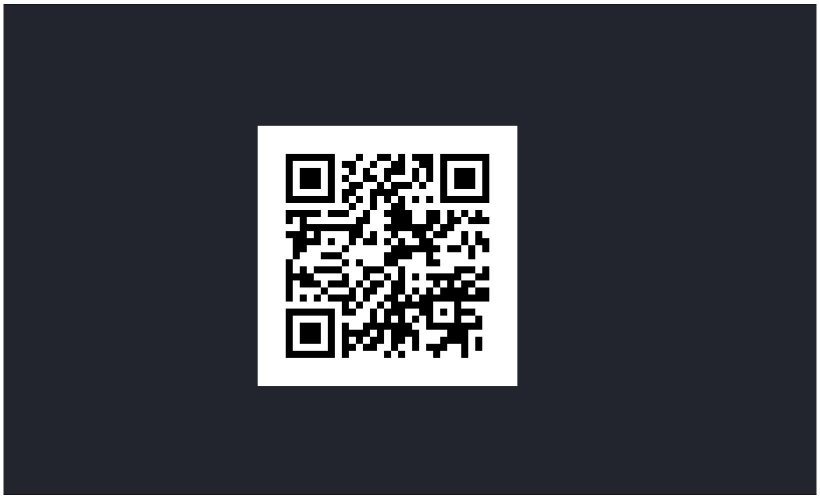
```
┌──(kali㉿purva)-[/media/kali/E3E8-4B401/.Trash-1000]
└─$ ls
files  info
```

Within the files folder, I found a document file name flag, hinting that this file relates to the flag:

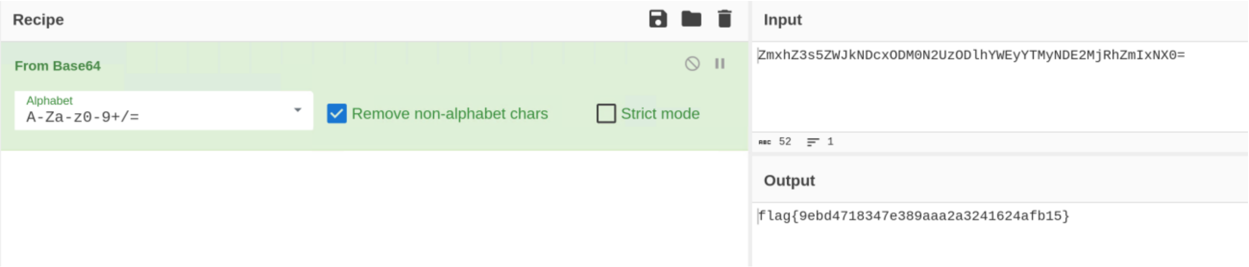


```
┌──(kali㉿purva)-[/media/kali/E3E8-4B401/.Trash-1000]
└─$ cd files

┌──(kali㉿purva)-[/media/kali/E3E8-4B401/.Trash-1000/files]
└─$ ls
Flag.docx
```

I opened the file in cyberchef and had to unzip it to reveal the contents. Within, I found a QR image. I got a piece of text when I scanned this code.



I was able to extract the flag by converting from base 64:



Alphabet: A-Za-z0-9+/=

☑ Remove non-alphabet chars

□ Strict mode

```
ZmxhZ3s5ZWJkNDcxODM0N2UzODlhYWEyYTMyNDE2MjRhZmIxNX0=
```

abc 52 ≡ 1

```
flag{9ebd4718347e389aaa2a3241624afb15}
```