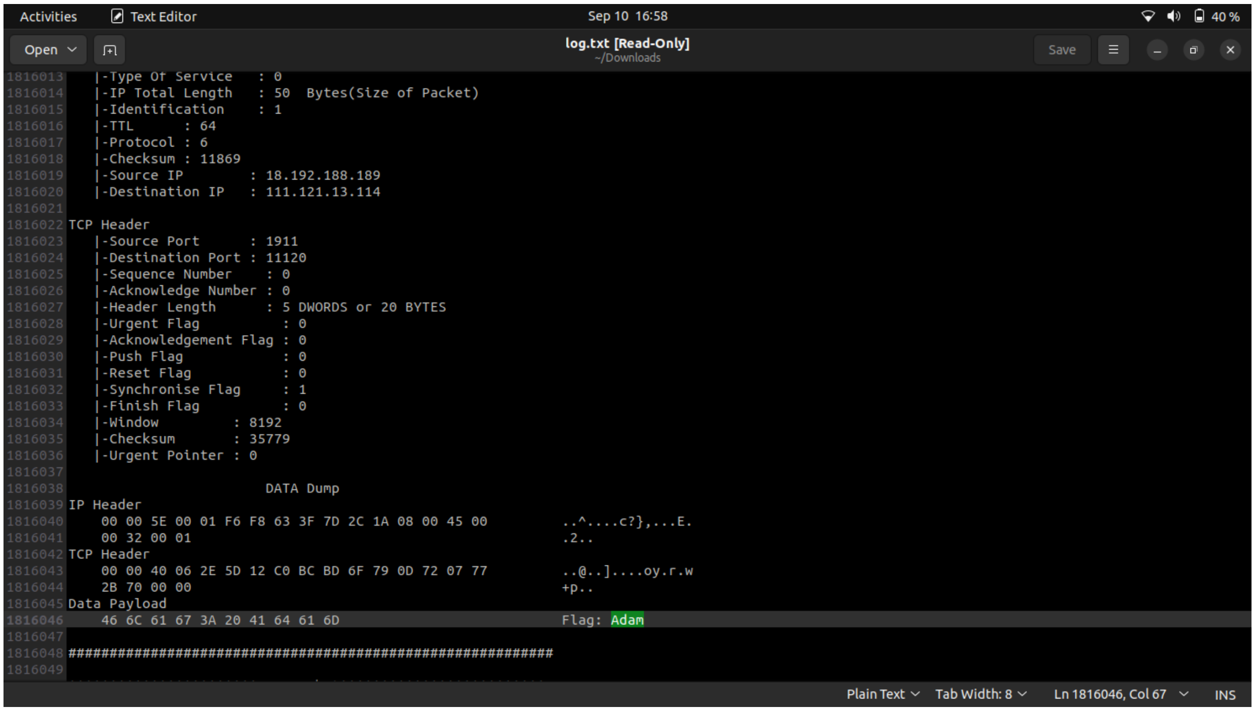
CTF Questions

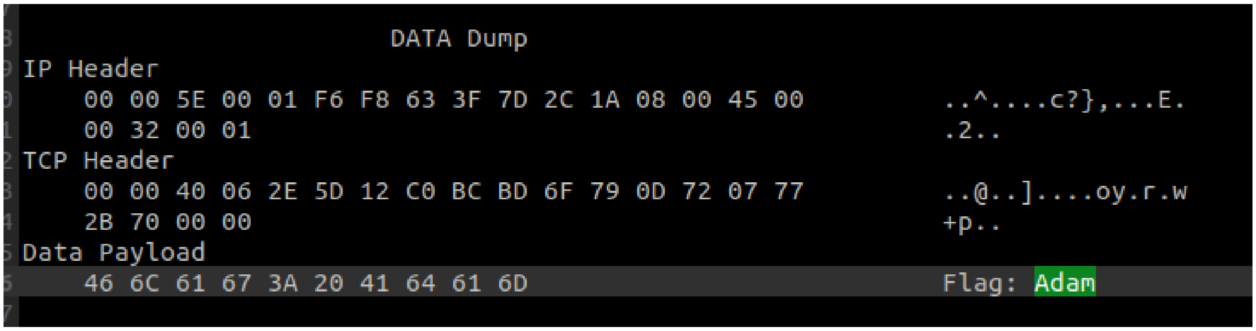
1.

3.pcap

1. There is a Flag in a TCP Packet. Identify the flag. (Hint: Search for the keyword Flag)

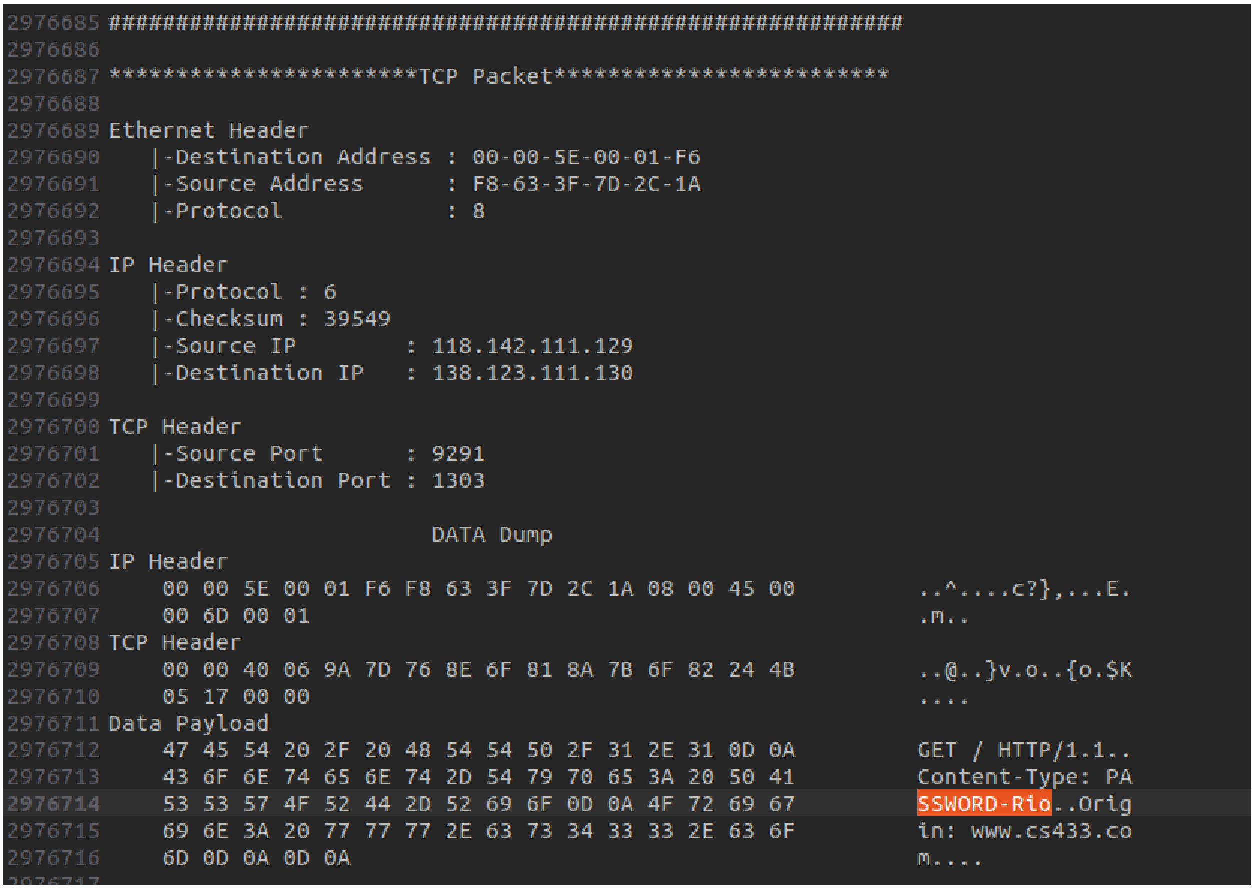


```
   |-Type Of Service   : 0
   |-IP Total Length   : 50  Bytes(Size of Packet)
   |-Identification    : 1
   |-TTL      : 64
   |-Protocol : 6
   |-Checksum : 11869
   |-Source IP        : 18.192.188.189
   |-Destination IP   : 111.121.13.114

TCP Header
   |-Source Port      : 1911
   |-Destination Port : 11120
   |-Sequence Number    : 0
   |-Acknowledge Number : 0
   |-Header Length      : 5 DWORDS or 20 BYTES
   |-Urgent Flag          : 0
   |-Acknowledgement Flag : 0
   |-Push Flag            : 0
   |-Reset Flag           : 0
   |-Synchronise Flag     : 1
   |-Finish Flag          : 0
   |-Window         : 8192
   |-Checksum       : 35779
   |-Urgent Pointer : 0

                        DATA Dump
IP Header
    00 00 5E 00 01 F6 F8 63 3F 7D 2C 1A 08 00 45 00         ..^....c?},...E.
    00 32 00 01                                             .2..
TCP Header
    00 00 40 06 2E 5D 12 C0 BC BD 6F 79 0D 72 07 77         ..@..]....oy.r.w
    2B 70 00 00                                             +p..
Data Payload
    46 6C 61 67 3A 20 41 64 61 6D                           Flag: Adam

############################################################
```



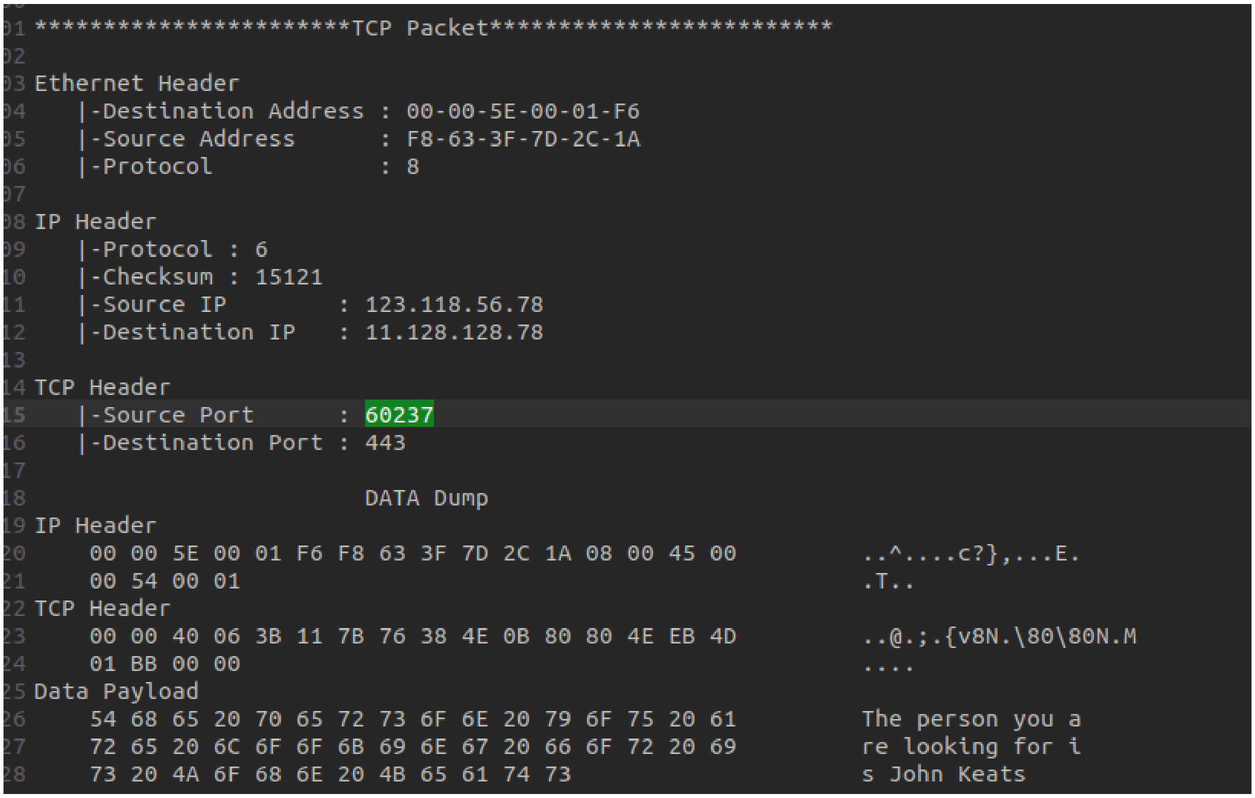
```
                        DATA Dump
IP Header
    00 00 5E 00 01 F6 F8 63 3F 7D 2C 1A 08 00 45 00         ..^....c?},...E.
    00 32 00 01                                             .2..
TCP Header
    00 00 40 06 2E 5D 12 C0 BC BD 6F 79 0D 72 07 77         ..@..]....oy.r.w
    2B 70 00 00                                             +p..
Data Payload
    46 6C 61 67 3A 20 41 64 61 6D                           Flag: Adam
```

2. My username is secret, Identify my secret.
3. I have a TCP checksum “0x46a4”. I have instructions in my path.



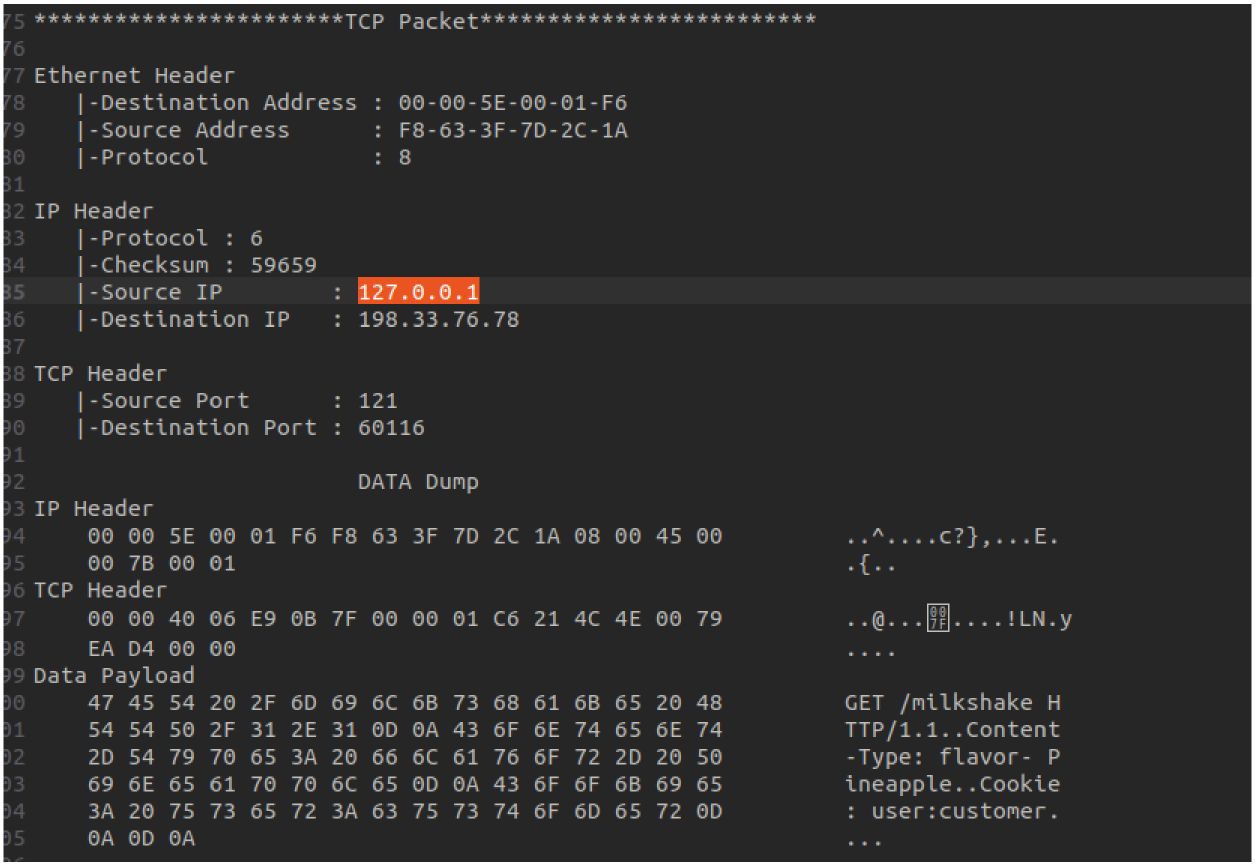
```
############################################################

***********************TCP Packet*************************

Ethernet Header
   |-Destination Address : 00-00-5E-00-01-F6
   |-Source Address      : F8-63-3F-7D-2C-1A
   |-Protocol            : 8

IP Header
   |-Protocol : 6
   |-Checksum : 39549
   |-Source IP        : 118.142.111.129
   |-Destination IP   : 138.123.111.130

TCP Header
   |-Source Port      : 9291
   |-Destination Port : 1303

                        DATA Dump
IP Header
    00 00 5E 00 01 F6 F8 63 3F 7D 2C 1A 08 00 45 00         ..^....c?},....E.
    00 6D 00 01                                             .m..
TCP Header
    00 00 40 06 9A 7D 76 8E 6F 81 8A 7B 6F 82 24 4B         ..@..}v.o..{o.$K
    05 17 00 00                                             ....
Data Payload
    47 45 54 20 2F 20 48 54 54 50 2F 31 2E 31 0D 0A         GET / HTTP/1.1..
    43 6F 6E 74 65 6E 74 2D 54 79 70 65 3A 20 50 41         Content-Type: PA
    53 53 57 4F 52 44 2D 52 69 6F 0D 0A 4F 72 69 67         SSWORD-Rio..Orig
    69 6E 3A 20 77 77 77 2E 63 73 34 33 33 2E 63 6F         in: www.cs433.co
    6D 0D 0A 0D 0A                                          m....
```

4. My device has an IP Address “131.144.126.118”. Sum of my connection ports will lead you to a person.



```
**********************TCP Packet*************************

Ethernet Header
   |-Destination Address : 00-00-5E-00-01-F6
   |-Source Address      : F8-63-3F-7D-2C-1A
   |-Protocol            : 8

IP Header
   |-Protocol : 6
   |-Checksum : 15121
   |-Source IP        : 123.118.56.78
   |-Destination IP   : 11.128.128.78

TCP Header
   |-Source Port      : 60237
   |-Destination Port : 443

                        DATA Dump
IP Header
    00 00 5E 00 01 F6 F8 63 3F 7D 2C 1A 08 00 45 00         ..^....c?},...E.
    00 54 00 01                                             .T..
TCP Header
    00 00 40 06 3B 11 7B 76 38 4E 0B 80 80 4E EB 4D         ..@.;.{v8N.\80\80N.M
    01 BB 00 00                                             ....
Data Payload
    54 68 65 20 70 65 72 73 6F 6E 20 79 6F 75 20 61         The person you a
    72 65 20 6C 6F 6F 6B 69 6E 67 20 66 6F 72 20 69         re looking for i
    73 20 4A 6F 68 6E 20 4B 65 61 74 73                     s John Keats
```

5. I come from localhost, I requested a milkshake. Find my flavour.



```
***********************TCP Packet*************************

Ethernet Header
   |-Destination Address : 00-00-5E-00-01-F6
   |-Source Address      : F8-63-3F-7D-2C-1A
   |-Protocol            : 8

IP Header
   |-Protocol : 6
   |-Checksum : 59659
   |-Source IP        : 127.0.0.1
   |-Destination IP   : 198.33.76.78

TCP Header
   |-Source Port      : 121
   |-Destination Port : 60116

                        DATA Dump
IP Header
    00 00 5E 00 01 F6 F8 63 3F 7D 2C 1A 08 00 45 00         ..^....c?},...E.
    00 7B 00 01                                             .{..
TCP Header
    00 00 40 06 E9 0B 7F 00 00 01 C6 21 4C 4E 00 79         ..@...␡....!LN.y
    EA D4 00 00                                             ....
Data Payload
    47 45 54 20 2F 6D 69 6C 6B 73 68 61 6B 65 20 48         GET /milkshake H
    54 54 50 2F 31 2E 31 0D 0A 43 6F 6E 74 65 6E 74         TTP/1.1..Content
    2D 54 79 70 65 3A 20 66 6C 61 76 6F 72 2D 20 50         -Type: flavor- P
    69 6E 65 61 70 70 6C 65 0D 0A 43 6F 6F 6B 69 65         ineapple..Cookie
    3A 20 75 73 65 72 3A 63 75 73 74 6F 6D 65 72 0D         : user:customer.
    0A 0D 0A                                                ...
```