

## Forensics: Eat\_pcap

### Description

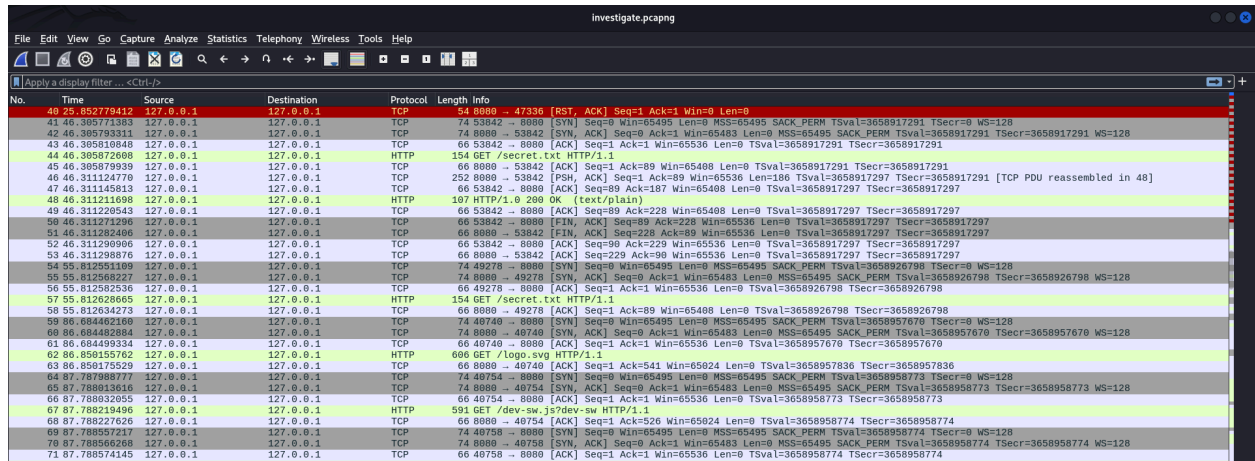
My Teacher told me https is more secure than http traffic. Thank you sir!!!

### Approach

This is the pcap file investigation challenge

#### Step 1:

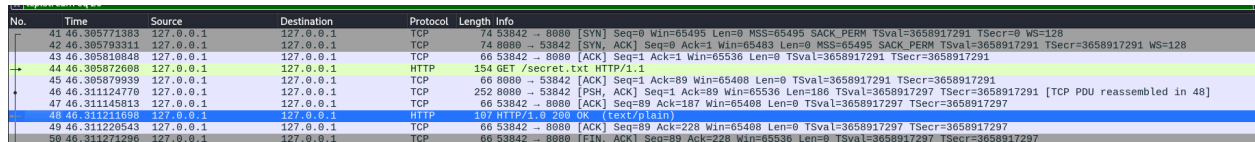
Open the given Pcap file in wireshark



No.	Time	Source	Destination	Protocol	Length	Info
40	25.852779412	127.0.0.1	127.0.0.1	TCP	54	8080 → 47336 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0
41	46.305771383	127.0.0.1	127.0.0.1	TCP	74	53842 → 8080 [SYN] Seq=0 Win=65495 Len=0 MSS=65495 SACK_PERM TSval=3658917291 TSecr=0 WS=128
42	46.3057793311	127.0.0.1	127.0.0.1	TCP	74	8080 → 53842 [SYN, ACK] Seq=0 Ack=1 Win=65483 Len=0 MSS=65495 SACK_PERM TSval=3658917291 TSecr=3658917291 WS=128
43	46.305810848	127.0.0.1	127.0.0.1	TCP	66	53842 → 8080 [ACK] Seq=1 Ack=1 Win=65536 Len=0 TSval=3658917291 TSecr=3658917291
44	46.305872608	127.0.0.1	127.0.0.1	HTTP	154	GET /secret.txt HTTP/1.1
45	46.305879939	127.0.0.1	127.0.0.1	TCP	66	8080 → 53842 [ACK] Seq=1 Ack=89 Win=65408 Len=0 TSval=3658917291 TSecr=3658917291
46	46.31124770	127.0.0.1	127.0.0.1	TCP	252	8080 → 53842 [PSH, ACK] Seq=1 Ack=89 Win=65536 Len=186 TSval=3658917297 TSecr=3658917291 [TCP PDU reassembled in 48]
47	46.311145813	127.0.0.1	127.0.0.1	TCP	66	53842 → 8080 [ACK] Seq=89 Ack=187 Win=65408 Len=0 TSval=3658917297 TSecr=3658917297
48	46.311211698	127.0.0.1	127.0.0.1	HTTP	197	HTTP/1.0 200 OK (text/plain)
49	46.311225543	127.0.0.1	127.0.0.1	TCP	66	53842 → 8080 [ACK] Seq=89 Ack=228 Win=65408 Len=0 TSval=3658917297 TSecr=3658917297
50	46.311271296	127.0.0.1	127.0.0.1	TCP	66	53842 → 8080 [FIN, ACK] Seq=89 Ack=228 Win=65536 Len=0 TSval=3658917297 TSecr=3658917297
51	46.311282486	127.0.0.1	127.0.0.1	TCP	66	8080 → 53842 [FIN, ACK] Seq=228 Ack=89 Win=65536 Len=0 TSval=3658917297 TSecr=3658917297
52	46.311290960	127.0.0.1	127.0.0.1	TCP	66	53842 → 8080 [ACK] Seq=90 Ack=229 Win=65536 Len=0 TSval=3658917297 TSecr=3658917297
53	46.311298876	127.0.0.1	127.0.0.1	TCP	66	8080 → 53842 [ACK] Seq=229 Ack=90 Win=65536 Len=0 TSval=3658917297 TSecr=3658917297
54	55.812551109	127.0.0.1	127.0.0.1	TCP	74	49278 → 8080 [SYN] Seq=0 Win=65495 Len=0 MSS=65495 SACK_PERM TSval=3658926798 TSecr=0 WS=128
55	55.812568227	127.0.0.1	127.0.0.1	TCP	74	8080 → 49278 [SYN, ACK] Seq=0 Ack=1 Win=65483 Len=0 MSS=65495 SACK_PERM TSval=3658926798 TSecr=3658926798 WS=128
56	55.812582536	127.0.0.1	127.0.0.1	TCP	66	49278 → 8080 [ACK] Seq=1 Ack=1 Win=65536 Len=0 TSval=3658926798 TSecr=3658926798
57	55.812628665	127.0.0.1	127.0.0.1	HTTP	154	GET /secret.txt HTTP/1.1
58	55.812634273	127.0.0.1	127.0.0.1	TCP	66	8080 → 49278 [ACK] Seq=1 Ack=89 Win=65408 Len=0 TSval=3658926798 TSecr=3658926798
59	86.684462160	127.0.0.1	127.0.0.1	TCP	74	48740 → 8080 [SYN] Seq=0 Win=65495 Len=0 MSS=65495 SACK_PERM TSval=3658957678 TSecr=0 WS=128
60	86.684499334	127.0.0.1	127.0.0.1	TCP	74	8080 → 48740 [SYN, ACK] Seq=0 Ack=1 Win=65483 Len=0 MSS=65495 SACK_PERM TSval=3658957678 TSecr=3658957678 WS=128
61	86.684499334	127.0.0.1	127.0.0.1	TCP	66	48740 → 8080 [ACK] Seq=1 Ack=1 Win=65536 Len=0 TSval=3658957678 TSecr=3658957678
62	86.858155762	127.0.0.1	127.0.0.1	HTTP	606	GET /logo.svg HTTP/1.1
63	86.858175529	127.0.0.1	127.0.0.1	TCP	66	8080 → 48740 [ACK] Seq=1 Ack=541 Win=65824 Len=0 TSval=3658957836 TSecr=3658957836
64	87.788798877	127.0.0.1	127.0.0.1	TCP	74	48754 → 8080 [SYN] Seq=0 Win=65495 Len=0 MSS=65495 SACK_PERM TSval=3658958773 TSecr=0 WS=128
65	87.788813616	127.0.0.1	127.0.0.1	TCP	74	8080 → 48754 [SYN, ACK] Seq=0 Ack=1 Win=65483 Len=0 MSS=65495 SACK_PERM TSval=3658958773 TSecr=3658958773 WS=128
66	87.788829555	127.0.0.1	127.0.0.1	TCP	66	48754 → 8080 [ACK] Seq=1 Ack=1 Win=65536 Len=0 TSval=3658958773 TSecr=3658958773
67	87.788219496	127.0.0.1	127.0.0.1	HTTP	591	GET /dev-sw.js?dev-sw HTTP/1.1
68	87.788227626	127.0.0.1	127.0.0.1	TCP	66	8080 → 48754 [ACK] Seq=1 Ack=526 Win=65824 Len=0 TSval=3658958774 TSecr=3658958774
69	87.788557217	127.0.0.1	127.0.0.1	TCP	74	48758 → 8080 [SYN] Seq=0 Win=65495 Len=0 MSS=65495 SACK_PERM TSval=3658958774 TSecr=0 WS=128
70	87.788566268	127.0.0.1	127.0.0.1	TCP	74	8080 → 48758 [SYN, ACK] Seq=1 Ack=1 Win=65483 Len=0 MSS=65495 SACK_PERM TSval=3658958774 TSecr=3658958774 WS=128
71	87.788574145	127.0.0.1	127.0.0.1	TCP	66	48758 → 8080 [ACK] Seq=1 Ack=1 Win=65536 Len=0 TSval=3658958774 TSecr=3658958774

#### Step2

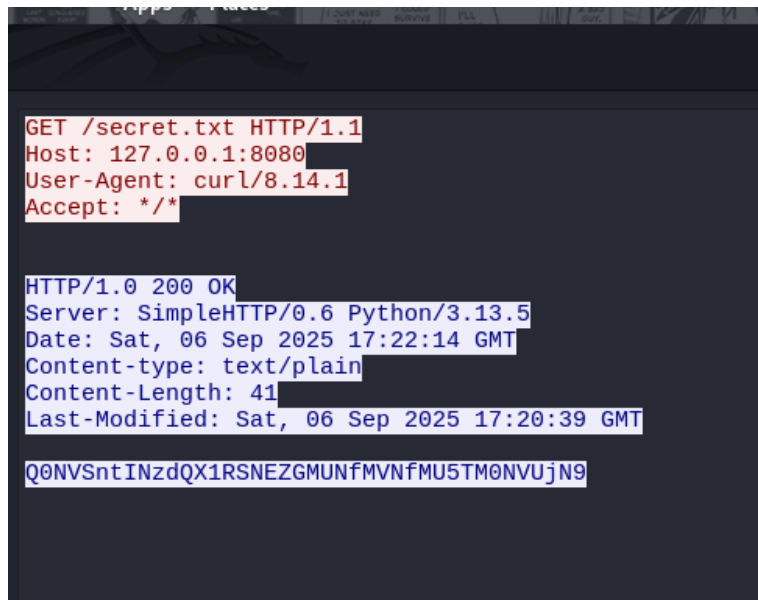
Search for any http or FTP traffic



No.	Time	Source	Destination	Protocol	Length	Info
41	46.305771383	127.0.0.1	127.0.0.1	TCP	74	53842 → 8080 [SYN] Seq=0 Win=65495 Len=0 MSS=65495 SACK_PERM TSval=3658917291 TSecr=0 WS=128
42	46.305793311	127.0.0.1	127.0.0.1	TCP	74	8080 → 53842 [SYN, ACK] Seq=0 Ack=1 Win=65483 Len=0 MSS=65495 SACK_PERM TSval=3658917291 TSecr=3658917291 WS=128
43	46.305810848	127.0.0.1	127.0.0.1	TCP	66	53842 → 8080 [ACK] Seq=1 Ack=1 Win=65536 Len=0 TSval=3658917291 TSecr=3658917291
44	46.305872608	127.0.0.1	127.0.0.1	HTTP	154	GET /secret.txt HTTP/1.1
45	46.305879939	127.0.0.1	127.0.0.1	TCP	66	8080 → 53842 [ACK] Seq=1 Ack=89 Win=65408 Len=0 TSval=3658917291 TSecr=3658917291
46	46.31124770	127.0.0.1	127.0.0.1	TCP	252	8080 → 53842 [PSH, ACK] Seq=1 Ack=89 Win=65536 Len=186 TSval=3658917297 TSecr=3658917291 [TCP PDU reassembled in 48]
47	46.311145813	127.0.0.1	127.0.0.1	TCP	66	53842 → 8080 [ACK] Seq=89 Ack=187 Win=65408 Len=0 TSval=3658917297 TSecr=3658917297
48	46.311211698	127.0.0.1	127.0.0.1	HTTP	197	HTTP/1.0 200 OK (text/plain)
49	46.311225543	127.0.0.1	127.0.0.1	TCP	66	53842 → 8080 [ACK] Seq=89 Ack=228 Win=65408 Len=0 TSval=3658917297 TSecr=3658917297
50	46.311271296	127.0.0.1	127.0.0.1	TCP	66	53842 → 8080 [FIN, ACK] Seq=89 Ack=228 Win=65536 Len=0 TSval=3658917297 TSecr=3658917297

#### Step 3:

Found a secret.txt file in the http request



Step 4:

the file contain a string value most probably base64 So, encode it

```
$ echo -n 'Q0NVSntINzdQX1RSNEZGMUNfMVNfMU5TM0NVUjN9' | base64 -d  
CCUJ{H77P_TR4FF1C_1S_1NS3CUR3}
```

Flag: CCUJ{H77P\_TR4FF1C\_1S\_1NS3CUR3}