

- The first thing that happened was the 3 way handshake that always happens. This is them establishing communication

No.	Time	Source	Destination	Protocol	Length	Info
1	0.000000000	192.168.64.2	172.233.221.124	TCP	74	58318 → 80 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 SACK_PERM TS...
2	0.000000000	192.168.64.2	172.233.221.124	TCP	74	58334 → 80 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 SACK_PERM TS...
3	0.018048495	172.233.221.124	192.168.64.2	TCP	66	80 → 58318 [SYN, ACK] Seq=0 Ack=1 Win=64240 Len=0 MSS=1382 SA...
4	0.018048829	172.233.221.124	192.168.64.2	TCP	66	80 → 58334 [SYN, ACK] Seq=0 Ack=1 Win=64240 Len=0 MSS=1382 SA...
5	0.018128497	192.168.64.2	172.233.221.124	TCP	54	58318 → 80 [ACK] Seq=1 Ack=1 Win=64256 Len=0
6	0.018147247	192.168.64.2	172.233.221.124	TCP	54	58334 → 80 [ACK] Seq=1 Ack=1 Win=64256 Len=0

- Next got a GET/basicauth/HTTP/1.1 which I am assuming is http using the get call to pull up the username and password login for the person

7	0.018430502	192.168.64.2	172.233.221.124	HTTP	404	GET /basicauth/ HTTP/1.1
8	0.037189594	172.233.221.124	192.168.64.2	TCP	54	80 → 58334 [ACK] Seq=1 Ack=351 Win=64128 Len=0
9	0.037189927	172.233.221.124	192.168.64.2	HTTP	457	HTTP/1.1 401 Unauthorized (text/html)
10	0.037245512	192.168.64.2	172.233.221.124	TCP	54	58334 → 80 [ACK] Seq=351 Ack=404 Win=64128 Len=0
11	5.189477616	192.168.64.2	172.233.221.124	TCP	54	58318 → 80 [FIN, ACK] Seq=1 Ack=1 Win=64256 Len=0

- I am also getting communication Like TCP KEEP Alive which I am assuming is TCP saying not to close the communication

14	40.893294037	192.168.64.2	172.233.221.124	TCP	54	[TCP Keep-Alive] 56020 → 80 [ACK] Seq=370 Ack=404 Win=64128 Len=0
15	40.911603196	172.233.221.124	192.168.64.2	TCP	54	[TCP Keep-Alive ACK] 80 → 56020 [ACK] Seq=404 Ack=370 Win=64128 Len=0
16	51.134575467	192.168.64.2	172.233.221.124	TCP	54	[TCP Keep-Alive] 56020 → 80 [ACK] Seq=370 Ack=404 Win=64128 Len=0
17	51.305486577	172.233.221.124	192.168.64.2	TCP	54	[TCP Keep-Alive ACK] 80 → 56020 [ACK] Seq=404 Ack=370 Win=64128 Len=0
18	61.373883343	192.168.64.2	172.233.221.124	TCP	54	[TCP Keep-Alive] 56020 → 80 [ACK] Seq=370 Ack=404 Win=64128 Len=0
19	61.393197734	172.233.221.124	192.168.64.2	TCP	54	[TCP Keep-Alive ACK] 80 → 56020 [ACK] Seq=404 Ack=370 Win=64128 Len=0
20	71.613903796	192.168.64.2	172.233.221.124	TCP	54	[TCP Keep-Alive] 56020 → 80 [ACK] Seq=370 Ack=404 Win=64128 Len=0
21	71.753731345	172.233.221.124	192.168.64.2	TCP	54	[TCP Keep-Alive ACK] 80 → 56020 [ACK] Seq=404 Ack=370 Win=64128 Len=0
22	75.093557917	172.233.221.124	192.168.64.2	TCP	54	80 → 56020 [FIN, ACK] Seq=404 Ack=371 Win=64128 Len=0
23	75.095032241	192.168.64.2	172.233.221.124	TCP	54	56020 → 80 [FIN, ACK] Seq=371 Ack=405 Win=64128 Len=0
24	75.113502864	172.233.221.124	192.168.64.2	TCP	54	80 → 56020 [ACK] Seq=405 Ack=372 Win=64128 Len=0

- I noticed that from the second I put in the password a line showed up next to all the frames after that and when I clicked on the line it said that it was Transmission Control Protocol

No.	Time	Source	Destination	Protocol	Length	Info
22	75.093557917	172.233.221.124	192.168.64.2	TCP	54	80 → 56020 [FIN, ACK] Seq=404 Ack=371 Win=64128 Len=0
23	75.095032241	192.168.64.2	172.233.221.124	TCP	54	56020 → 80 [FIN, ACK] Seq=371 Ack=405 Win=64128 Len=0
24	75.113502864	172.233.221.124	192.168.64.2	TCP	54	80 → 56020 [ACK] Seq=405 Ack=372 Win=64128 Len=0
25	125.555322498	192.168.64.2	172.233.221.124	TCP	74	55528 → 80 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 SACK_PERM TS...
26	125.573217360	172.233.221.124	192.168.64.2	TCP	66	80 → 55528 [SYN, ACK] Seq=0 Ack=1 Win=64240 Len=0 MSS=1382 SA...
27	125.573305111	192.168.64.2	172.233.221.124	TCP	54	55528 → 80 [ACK] Seq=1 Ack=1 Win=64256 Len=0
28	125.573666911	192.168.64.2	172.233.221.124	HTTP	467	GET /basicauth/ HTTP/1.1
29	125.744455552	172.233.221.124	192.168.64.2	TCP	54	80 → 55528 [ACK] Seq=1 Ack=414 Win=64128 Len=0
30	125.744456010	172.233.221.124	192.168.64.2	HTTP	458	HTTP/1.1 200 OK (text/html)
31	125.744517803	192.168.64.2	172.233.221.124	TCP	54	55528 → 80 [ACK] Seq=414 Ack=405 Win=64128 Len=0
32	125.871176658	192.168.64.2	172.233.221.124	HTTP	447	GET /favicon.ico HTTP/1.1
33	125.893456285	172.233.221.124	192.168.64.2	HTTP	383	HTTP/1.1 404 Not Found (text/html)
34	125.893500578	192.168.64.2	172.233.221.124	TCP	54	55528 → 80 [ACK] Seq=807 Ack=734 Win=64128 Len=0
35	135.902162257	192.168.64.2	172.233.221.124	TCP	54	[TCP Keep-Alive] 55528 → 80 [ACK] Seq=806 Ack=734 Win=64128 Len=0
36	135.920290207	172.233.221.124	192.168.64.2	TCP	54	[TCP Keep-Alive ACK] 80 → 55528 [ACK] Seq=734 Ack=806 Win=64128 Len=0
37	146.109836985	192.168.64.2	172.233.221.124	TCP	54	[TCP Keep-Alive] 55528 → 80 [ACK] Seq=806 Ack=734 Win=64128 Len=0
38	146.208707051	172.233.221.124	192.168.64.2	TCP	54	[TCP Keep-Alive ACK] 80 → 55528 [ACK] Seq=734 Ack=806 Win=64128 Len=0

- I could not see the password and user name being exchanged
- When I opened the first link on the page it jump multiple frames and these black frames showed up

No.	Time	Source	Destination	Protocol	Length	Info
861	405.445483215	192.168.64.2	172.233.221.124	TCP	54	38944 → 80 [ACK] Seq=396 Ack=576295 Win=1044608 Len=
862	405.445495132	172.233.221.124	192.168.64.2	TCP	13874	80 → 38944 [PSH, ACK] Seq=576295 Ack=396 Win=64128 Len=
863	405.445505966	192.168.64.2	172.233.221.124	TCP	54	38944 → 80 [ACK] Seq=396 Ack=590115 Win=1072256 Len=
864	405.445510049	172.233.221.124	192.168.64.2	TCP	1436	[TCP Previous segment not captured] 80 → 38944 [ACK]
865	405.445510091	172.233.221.124	192.168.64.2	TCP	1436	[TCP Out-Of-Order] 80 → 38944 [ACK] Seq=590115 Ack=
866	405.445510132	172.233.221.124	192.168.64.2	TCP	8346	80 → 38944 [ACK] Seq=592879 Ack=396 Win=64128 Len=8
867	405.445517508	192.168.64.2	172.233.221.124	TCP	66	[TCP Dup ACK 863#1] 38944 → 80 [ACK] Seq=396 Ack=59
868	405.445519216	192.168.64.2	172.233.221.124	TCP	54	38944 → 80 [ACK] Seq=396 Ack=592879 Win=1078144 Len=
869	405.445520174	192.168.64.2	172.233.221.124	TCP	54	38944 → 80 [ACK] Seq=396 Ack=601171 Win=1094656 Len=
870	405.445528966	172.233.221.124	192.168.64.2	TCP	1436	[TCP Previous segment not captured] 80 → 38944 [ACK]
871	405.445529008	172.233.221.124	192.168.64.2	TCP	1436	[TCP Out-Of-Order] 80 → 38944 [ACK] Seq=601171 Ack=
872	405.445529050	172.233.221.124	192.168.64.2	TCP	2818	80 → 38944 [ACK] Seq=603935 Ack=396 Win=64128 Len=2
873	405.445529091	172.233.221.124	192.168.64.2	TCP	1436	[TCP Previous segment not captured] 80 → 38944 [ACK]
874	405.445529133	172.233.221.124	192.168.64.2	TCP	1436	[TCP Out-Of-Order] 80 → 38944 [ACK] Seq=606699 Ack=
875	405.445529175	172.233.221.124	192.168.64.2	TCP	1436	80 → 38944 [ACK] Seq=609463 Ack=396 Win=64128 Len=1
876	405.445529216	172.233.221.124	192.168.64.2	TCP	1436	[TCP Previous segment not captured] 80 → 38944 [ACK]
877	405.445536466	192.168.64.2	172.233.221.124	TCP	66	[TCP Dup ACK 869#1] 38944 → 80 [ACK] Seq=396 Ack=60

- These were also some frames that said out of order
- The black line also disappeared
- What does PSH means

916	405.449002296	172.233.221.124	192.168.64.2	TCP	15256	80 → 38944 [PSH, ACK] Seq=668889 Ack=396 Win=64128
917	405.449040505	192.168.64.2	172.233.221.124	TCP	54	38944 → 80 [ACK] Seq=396 Ack=668889 Win=1233152 Len=
918	405.449061297	192.168.64.2	172.233.221.124	TCP	54	38944 → 80 [ACK] Seq=396 Ack=684091 Win=1263488 Len=
919	405.449067714	172.233.221.124	192.168.64.2	TCP	11110	80 → 38944 [PSH, ACK] Seq=684091 Ack=396 Win=64128
920	405.449070631	192.168.64.2	172.233.221.124	TCP	54	38944 → 80 [ACK] Seq=396 Ack=695147 Win=1285632 Len=

- The amatures.txt did cause the that big of a jump which I assume is because it is just a text file with no HTML which the first link had pictures and fonts and everything else
- I was just a basic HTTP GET command
- I also tell me the type of text like (text/plain)
- The other 2 txt files had the same reaction nothing special about them
- The frames only really change the first time I open a new link but when I open it again it doesn't just frames

