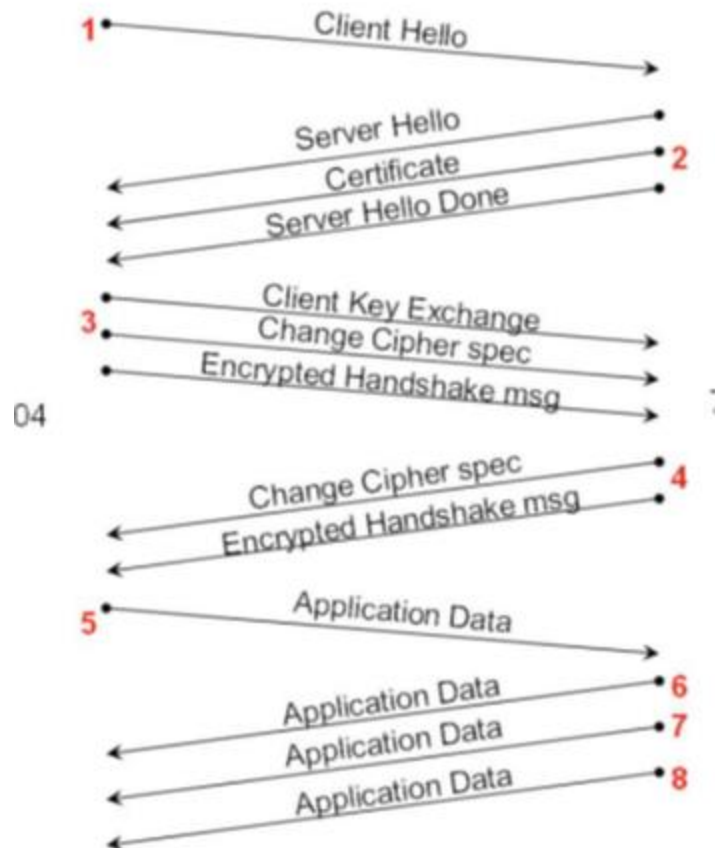


LAB-9

1. Visit your bank website or some of your favorite purchase website for capturing SSL. Be sure to exit without any 'dangerous' transaction
2. Locate the below messages for your SSL transaction by filtering for SSL transactions and categorize them from 1-8 as per below figure



Captured the packets from Amazon using Wireshark.

668	9.121014	52.85.232.220	192.168.0.7	TLSv1...	1067 Application Data	
669	9.121014	52.85.232.220	192.168.0.7	TLSv1...	85 Application Data	
754	9.457065	192.168.0.7	52.114.128.70	TLSv1...	282 Client Hello	(1)
893	9.744372	52.114.128.70	192.168.0.7	TLSv1...	1400 Server Hello, Certificate, Server Key Exchange, Server Hello Done	(2)
896	9.758601	192.168.0.7	52.114.128.70	TLSv1...	212 Client Key Exchange, Change Cipher Spec, Encrypted Handshake Message	(3)
912	10.034133	52.114.128.70	192.168.0.7	TLSv1...	105 Change Cipher Spec, Encrypted Handshake Message	(4)
914	10.035828	192.168.0.7	52.114.128.70	TLSv1...	994 Application Data	
915	10.036068	192.168.0.7	52.114.128.70	TLSv1...	1176 Application Data	(5)
939	10.199185	192.168.0.7	23.45.162.131	TLSv1...	147 Application Data	
947	10.315674	52.114.128.70	192.168.0.7	TLSv1...	411 Application Data	(6)(7)(8)
949	10.318010	192.168.0.7	52.114.128.70	TLSv1...	993 Application Data	
950	10.318565	192.168.0.7	52.114.128.70	TLSv1...	668 Application Data	

Transmission Control Protocol, Src Port: 13875, Dst Port: 443, Seq: 1, Ack: 1, Len: 228					
Transport Layer Security					
TLSv1.2 Record Layer: Handshake Protocol: Client Hello					
Content Type: Handshake (22)					
Version: TLS 1.2 (0x0303)					
Length: 223					
Handshake Protocol: Client Hello					

0030	04 00 76 66 00 00 16 03 03 00 df 01 00 00 db 03	..vf....
0040	03 5f ce 7c b1 d0 8c de e7 20 11 2d 33 0e 22 11	.._-3..."
0050	5f 9e b3 e5 b1 fa 6a 0e 61 36 49 0e eb 7e 76 cfj.	a6I...~v.
0060	c5 20 92 1d 00 00 4a 59 56 79 a1 2d e6 43 ad 84JY Vy...	C..
0070	a1 af b2 7a 60 97 59 e9 f4 26 bf a4 5c 72 63 a6	...z`Y.	&...rc.
0080	a2 f3 00 26 c0 2c c0 2b c0 30 c0 2f c0 24 c0 23	...&,+.	0\$/.\$.#
0090	c0 28 c0 27 c0 0a c0 09 c0 14 c0 13 00 9d 00 9c	(.'....
00a0	00 3d 00 3c 00 35 00 2f 00 0a 01 00 00 6c 00 00	=<.5./l.
00b0	00 22 00 20 00 00 1d 76 32 30 2e 65 76 65 6e 74	""....v	20.event
00c0	73 2e 64 61 74 61 2e 6d 69 63 72 6f 73 6f 66 74	s.data.m	icrosoft

