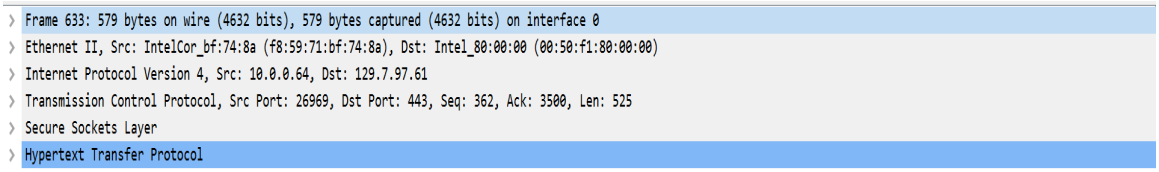
# *Homework 2: Logging and Decrypting TLS*

1. My packet trace consists of 1296 packets. There are different types of packets corresponding to different protocols like DNS,ARP,TCP,UDP,HTTP,TLS.

I observed the following things while inspecting my packet trace.

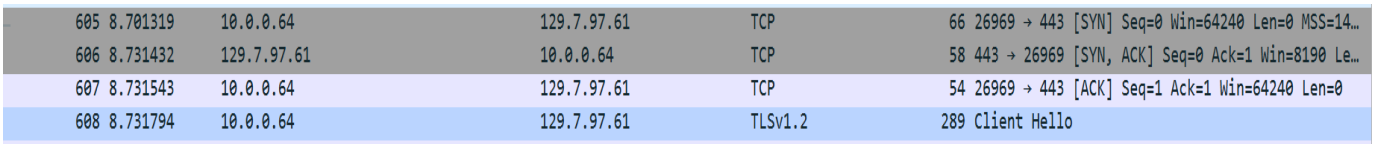
- Each packet has atmost 6 fields i.e.; Frame(physical layer),Ethernet(for datalink layer),Internet protocol(datagram for Network layer),Transmission control protocol(segment for Transport layer),Secure Sockets Layer,Hyper text transfer protocol(message for application layer).This demonstrates the encapsulation achieved for the internet protocol stack. All DNS query packets use UDP protocol.

Screenshot of for the above observation:




- Whenever my computer requests a TCP connection to a server inorder to request a http object, it performs a three way handshake of SYN,SYNACK,ACK packets. These packets are coded in grey color. Each TCP connection handles multiple request response messages. Once the connection is closed(indicated when the browser send ACK packet to the server indicating to close the connection) , the client i.e.; the browser again initiates a three way handshake .

Screenshot of for the above observation(for three way handshake):




- When the browser requests a website which requires authentication of the user, we can see the decrypted credentials in one of the http response packets. Thus, using wireshark we can sniff packets containing confidential information which is achieved by using SSL decryption.

```
> Frame 1602: 896 bytes on wire (7168 bits), 896 bytes captured (7168 bits) on interface 0
> Ethernet II, Src: IntelCor_bf:74:8a (f8:59:71:bf:74:8a), Dst: Intel_80:00:00 (00:50:f1:80:00:00)
> Internet Protocol Version 4, Src: 10.0.0.64, Dst: 129.7.97.61
> Transmission Control Protocol, Src Port: 16501, Dst Port: 443, Seq: 1299, Ack: 62215, Len: 842
> Secure Sockets Layer
> Hypertext Transfer Protocol
v HTML Form URL Encoded: application/x-www-form-urlencoded
  > Form item: "parama" = "[redacted]"
  > Form item: "paramb" = "[redacted]"
  > Form item: "popup" = "1"
  > Form item: "paramd" = "6ce9cf727a4115fa6b9d7bc33e186348"
  > Form item: "paramg" = "pslg"
  > Form item: "paramm" = "   Please enter PS ID"
```

(1) which website were you visiting and what action did you take to get the browser to generate packets with TLS.

- I accessed **access uh** website and logged into the website using my people soft credentials.

1. Opened the browser, searched for the website access uh, clicked on the access uh website link, and logged into people soft using my credentials.

(2) encrypted packet trace corresponding to that action.

```
0000  00 50 f1 80 00 00 f8 59  71 bf 74 8a 08 00 45 00   .P.....Y q.t...E.
0010  03 72 01 1d 40 00 80 06  09 e5 0a 00 00 40 81 07   .r..@... .....@..
0020  61 3d 40 75 01 bb a2 92  1d 69 af 1c b8 f4 50 18   a=@u.... .i....P.
0030  ff 00 8b ef 00 00 17 03  03 03 45 00 00 00 00 00   ........ ..E.....
0040  00 00 03 15 91 70 3b d4  aa 6d ef 99 20 68 53 9f   .....p;. .m.. hS.
0050  17 45 bd c7 58 f7 48 95  ba ab cb 98 e2 a0 8e 92   .E..X.H. ........
0060  74 67 a6 03 74 d6 0a 86  d9 66 91 25 a8 39 b2 b1   tg..t... .f.%.9..
0070  a6 fa 15 b7 30 04 4b 25  7f a3 26 2f 35 b7 df 4e   ....0.K% ..&/5..N
0080  16 fb 0b 3a f5 32 0f 95  76 d6 dd 84 af b2 3b 8d   ...:.2.. v.....;.
0090  d0 73 69 33 2d 5a 35 1d  30 5f 35 31 a6 f6 3a 94   .si3-Z5. 0_51..:.
00a0  51 4e f3 e9 32 ca e7 76  13 a2 c6 2e a1 31 0b 8d   QN..2..v .....1..
00b0  60 ac fb 42 23 ef f2 ae  1a 39 ea f7 95 fb eb 7b   `..B#... .9.....{
00c0  db 12 91 b2 64 d0 3f c4  54 e9 13 d4 c0 bb 54 f1   ....d.?. T.....T.
00d0  43 b6 51 e8 0b 5d 6a 32  98 58 89 69 ba 6d da 46   C.Q..]j2 .X.i.m.F
00e0  83 a2 e8 9d 3d 2b 11 9d  8c cd 59 39 57 f4 f1 51   ....=+.. ..Y9W..Q
00f0  a6 a7 41 c5 2d 47 97 b6  f8 3c 4e 7f 09 c6 cd bf   ..A.-G.. .<N.....
0100  6c 5d 0b e0 6b 25 7d cd  15 e2 99 ca 70 a8 77 f8   l]..k%}. ....p.w.
0110  5e 11 da d3 a2 77 a0 01  8a 10 70 01 64 2d 0d b7   ^....w.. ..p.d-..
0120  39 54 6a 0f 47 d7 e7 e2  5c 4e 59 89 ef 72 c2 60   9Tj.G... \NY..r.`
0130  d4 8c e0 7a 51 69 c8 37  52 23 f2 06 82 70 0e 5e   ...zQi.7 R#...p.^
0140  48 f6 a9 ca a4 04 85 4b  e8 59 2e e4 00 c0 c7 b4   H......K .Y......
0150  c0 26 86 ef df 00 cb 93  47 38 b4 ec 44 69 96 a7   .&...... G8..Di..
0160  fa 7e 52 43 20 9d f3 db  5c 6f e2 ef 9b 96 f6 12   .~RC ... \o......
0170  be 34 a4 22 69 58 31 fa  46 4d f7 3a ff 7c 14 fd   .4."iX1. FM.:.|..
0180  c1 ef 5a 9b 48 11 ee df  27 a5 0a e4 50 30 44 e8   ..Z.H... '...P0D.
0190  6c db 86 4c 3e cc 19 f6  62 4a 54 a5 c2 30 c9 47   l..L>... bJT..0.G
01a0  c6 c8 96 fb 8f a0 f4 74  fa ba 37 a9 12 3e d5 9f   .......t ..7..>..
```

```
01c0  36 cb ae 07 51 fd c4 93  d1 c3 12 d4 ef 38 6c 71   6...Q... .....8lq
01d0  a6 87 f8 a7 4b 00 72 25  e1 76 50 e0 a5 45 29 9f   ....K.r% .vP..E).
01e0  69 69 34 0f 6a e2 7c 1d  3e 40 55 ea 5b e7 11 5b   ii4.j.|. >@U.[..[
01f0  0a 30 b0 46 e7 1e 41 4d  9b 7d 80 4e 02 42 f8 80   .0.F..AM .}.N.B..
0200  16 f5 72 8c 69 18 d5 e7  b7 ae 84 26 00 8b fc 48   ..r.i... ...&...H
0210  b0 53 fc 22 96 62 47 27  bc 02 55 89 5f 4b cd dd   .S.".bG' ..U._K..
0220  80 fd 6f f3 eb 2c 3a 70  c3 e6 33 bd 78 26 d1 53   ..o..,:p ..3.x&.S
0230  f6 af bc 96 1b 81 be 93  15 b2 c0 1e 80 99 85 fe   ........ ........
0240  eb 69 8a 17 59 3d c6 c2  a7 d7 db 61 e3 f7 b3 51   .i..Y=.. ...a...Q
0250  f8 07 64 38 93 86 a3 25  81 90 30 1e 1b 67 01 23   ..d8...% ..0..g.#
0260  16 17 a1 c6 64 d3 6f 6f  b2 85 e6 52 cf 80 11 80   ....d.oo ...R....
0270  28 26 b1 4e ee 47 4f fb  59 20 ce d3 91 28 d9 a9   (&.N.GO. Y ...(..
0280  30 a8 de c9 f1 81 4b 65  d9 e2 0a e5 50 20 54 bf   0.....Ke ....P T.
0290  08 f9 2d 70 dc 2a 82 38  c9 2d 29 fe a5 e4 55 1d   ..-p.*.8 .-)...U.
02a0  63 80 ab 54 ae 82 64 28  b4 68 20 95 e6 af 29 d8   c..T..d( .h ...).
02b0  d5 38 80 70 2f 88 02 9e  b0 fe 2d 5f 9c f2 70 6f   .8.p/... ..-_..po
02c0  a2 1a 46 37 24 65 75 61  65 b0 42 9f 62 ff 24 b9   ..F7$eua e.B.b.$.
02d0  88 74 bb db 32 3c 13 db  21 48 39 59 2f 6f 5b 2f   .t..2<.. !H9Y/o[/
02e0  48 35 0d e3 39 b9 c2 b2  39 db 73 70 d6 1c 5b 19   H5..9... 9.sp..[.
02f0  83 7f f2 a1 1a a7 76 e7  48 c2 4b 80 33 54 2f 8a   ......v. H.K.3T/.
0300  87 39 4d 89 38 06 43 93  06 04 fd d3 da da c7 30   .9M.8.C. .......0
0310  aa 98 d9 ef 16 0a 29 d2  40 e3 17 24 9e 43 42 7a   ......). @..$.CBz
0320  d4 45 06 c0 43 5a 01 c6  c0 da a2 04 53 eb 52 0c   .E..CZ.. ....S.R.
0330  05 44 25 57 43 da a9 ee  d6 f5 29 eb 18 09 33 b3   .D%WC... ..)...3.
0340  b5 45 8c 0c 24 0b c1 e8  e2 ef c4 15 c4 c5 e4 37   .E..$... .......7
0350  89 b5 dc 4d be bb b9 52  3b 73 99 5c 20 4e ec 94   ...M...R ;s.\ N..
0360  29 47 7b 38 e1 f7 e6 73  bb 9e 95 f4 05 eb ea 39   )G{8...s .......9
```

(3) decrypted packet content.

```
0000  50 4f 53 54 20 2f 61 63  63 6f 75 6e 74 5f 76 61   POST /ac count_va
0010  6c 69 64 61 74 69 6f 6e  2e 70 68 70 20 48 54 54   lidation .php HTT
0020  50 2f 31 2e 31 0d 0a 48  6f 73 74 3a 20 61 63 63   P/1.1..H ost: acc
0030  65 73 73 75 68 2e 75 68  2e 65 64 75 0d 0a 43 6f   essuh.uh .edu..Co
0040  6e 6e 65 63 74 69 6f 6e  3a 20 6b 65 65 70 2d 61   nnection : keep-a
0050  6c 69 76 65 0d 0a 43 6f  6e 74 65 6e 74 2d 4c 65   live..Co ntent-Le
0060  6e 67 74 68 3a 20 31 32  37 0d 0a 41 63 63 65 70   ngth: 12 7..Accep
0070  74 3a 20 61 70 70 6c 69  63 61 74 69 6f 6e 2f 6a   t: appli cation/j
0080  73 6f 6e 2c 20 74 65 78  74 2f 6a 61 76 61 73 63   son, tex t/javasc
0090  72 69 70 74 2c 20 2a 2f  2a 3b 20 71 3d 30 2e 30   ript, */ *; q=0.0
00a0  31 0d 0a 4f 72 69 67 69  6e 3a 20 68 74 74 70 73   1..Origi n: https
00b0  3a 2f 2f 61 63 63 65 73  73 75 68 2e 75 68 2e 65   ://acces suh.uh.e
00c0  64 75 0d 0a 58 2d 52 65  71 75 65 73 74 65 64 2d   du..X-Re quested-
00d0  57 69 74 68 3a 20 58 4d  4c 48 74 74 70 52 65 71   With: XM LHttpReq
00e0  75 65 73 74 0d 0a 55 73  65 72 2d 41 67 65 6e 74   uest..Us er-Agent
00f0  3a 20 4d 6f 7a 69 6c 6c  61 2f 35 2e 30 20 28 57   : Mozill a/5.0 (W
0100  69 6e 64 6f 77 73 20 4e  54 20 31 30 2e 30 3b 20   indows N T 10.0;
0110  57 69 6e 36 34 3b 20 78  36 34 29 20 41 70 70 6c   Win64; x 64) Appl
0120  65 57 65 62 4b 69 74 2f  35 33 37 2e 33 36 20 28   eWebKit/ 537.36 (
0130  4b 48 54 4d 4c 2c 20 6c  69 6b 65 20 47 65 63 6b   KHTML, l ike Geck
0140  6f 29 20 43 68 72 6f 6d  65 2f 36 31 2e 30 2e 33   o) Chrom e/61.0.3
0150  31 36 33 2e 31 30 30 20  53 61 66 61 72 69 2f 35   163.100  Safari/5
0160  33 37 2e 33 36 0d 0a 43  6f 6e 74 65 6e 74 2d 54   37.36..C ontent-T
0170  79 70 65 3a 20 61 70 70  6c 69 63 61 74 69 6f 6e   ype: app lication
0180  2f 78 2d 77 77 77 2d 66  6f 72 6d 2d 75 72 6c 65   /x-www-f orm-urle
0190  6e 63 6f 64 65 64 3b 20  63 68 61 72 73 65 74 3d   ncoded;  charset=
01a0  55 54 46 2d 38 0d 0a 52  65 66 65 72 65 72 3a 20   UTF-8..R eferer:
```

4. Implication of what you learned in this assignment.

Wireshark is a powerful tool to capture network traffic and helps us to analyze the reassembled packets, error packets, duplicate packets and several other statistics. It provides a big picture of the types of packets like http,tcp,dns,ARP in our network. Using the coloring rules, packets can be classified and identified easily. One of the most powerful implications that I have observed is the communication between server and client can be sniffed which results in compromising of the security and privacy of both sender and receiver. Though a secure communication is established between server and client using SSL/TLS but beyond that using decryption in wireshark we can actually see and read the data that is being circulated between them.