TLS Visibility ***Inside*** the Data Center

Steve Fenter and Jason Witty

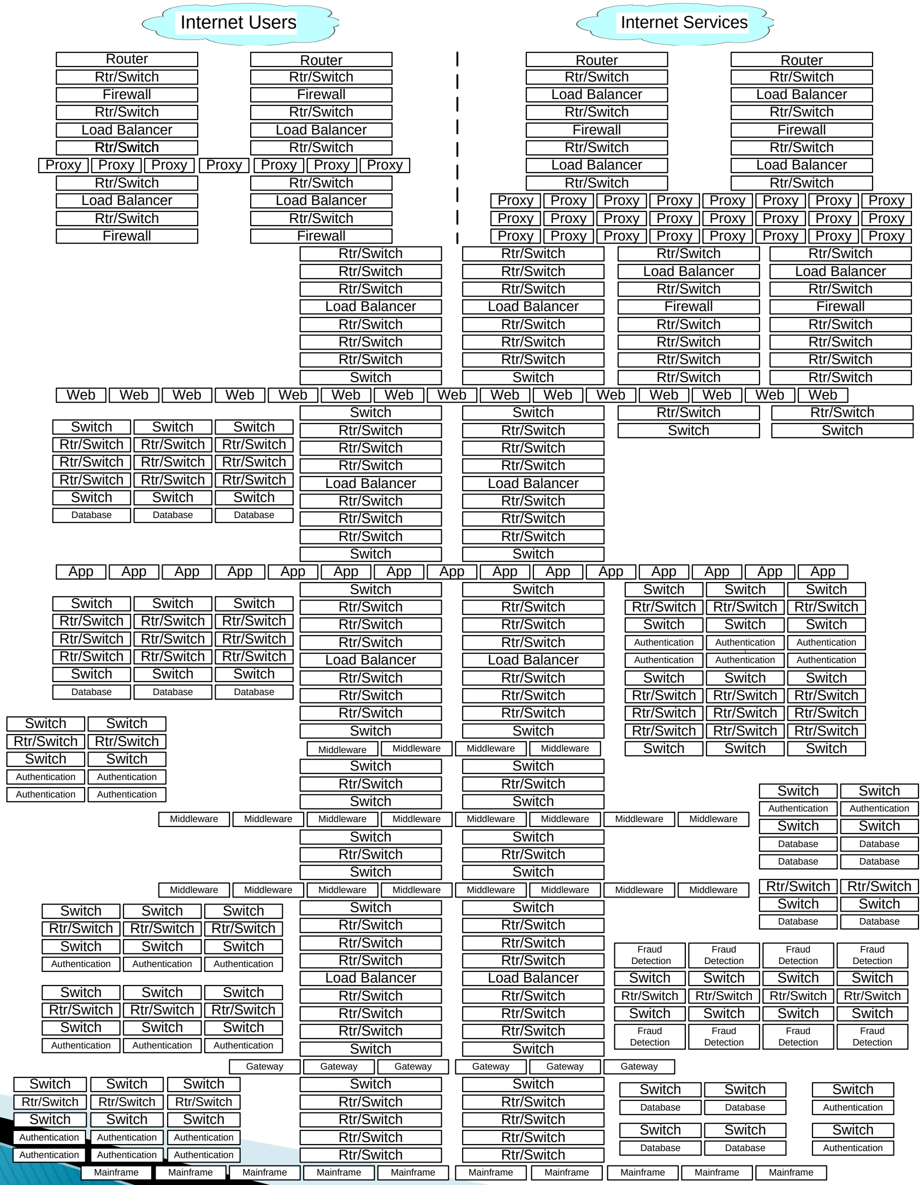
November 15, 2016

Introductions and Level-Set

- Who are we?
- Why are we here?
  - We want to collaborate with IETFers to standardize an enterprise visibility solution
- What are we trying to accomplish today?
  - Demonstrate the need for out-of-band visibility *inside* the data center and start to determine a way forward together.

The impact of encryption on enterprises is also laid out in Internet Draft "Effect of Ubiquitous Encryption", section 4

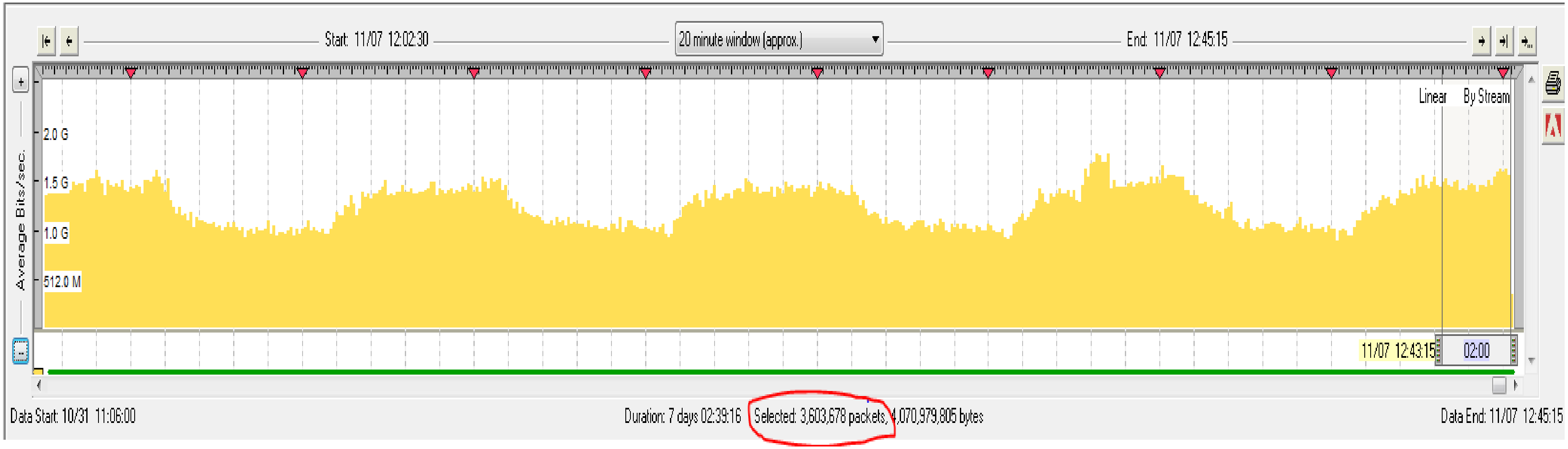
Enterprise Operational Support Environment


Internet Users
Internet Services
Router Router Router Router
Rtr/Switch Rtr/Switch Rtr/Switch Rtr/Switch
Firewall Firewall Load Balancer Load Balancer
Rtr/Switch Rtr/Switch Rtr/Switch Rtr/Switch
Load Balancer Load Balancer Firewall Firewall
Rtr/Switch Rtr/Switch Rtr/Switch Rtr/Switch
Proxy Proxy Proxy Proxy Proxy Proxy Proxy Load Balancer Load Balancer
Rtr/Switch Rtr/Switch Rtr/Switch Rtr/Switch
Load Balancer Load Balancer Proxy Proxy Proxy Proxy Proxy Proxy Proxy Proxy
Rtr/Switch Rtr/Switch Proxy Proxy Proxy Proxy Proxy Proxy Proxy Proxy
Firewall Firewall Proxy Proxy Proxy Proxy Proxy Proxy Proxy Proxy
Rtr/Switch Rtr/Switch Rtr/Switch Rtr/Switch
Rtr/Switch Rtr/Switch Load Balancer Load Balancer
Rtr/Switch Rtr/Switch Rtr/Switch Rtr/Switch
Load Balancer Load Balancer Firewall Firewall
Rtr/Switch Rtr/Switch Rtr/Switch Rtr/Switch
Rtr/Switch Rtr/Switch Rtr/Switch Rtr/Switch
Rtr/Switch Rtr/Switch Rtr/Switch Rtr/Switch
Switch Switch Rtr/Switch Rtr/Switch
Web Web Web Web Web Web Web Web Web Web Web Web Web Web Web
Switch Switch Rtr/Switch Rtr/Switch
Switch Switch Switch Rtr/Switch Rtr/Switch Switch Switch
Rtr/Switch Rtr/Switch Rtr/Switch Rtr/Switch Rtr/Switch
Rtr/Switch Rtr/Switch Rtr/Switch Rtr/Switch Rtr/Switch
Rtr/Switch Rtr/Switch Rtr/Switch Load Balancer Load Balancer
Switch Switch Switch Rtr/Switch Rtr/Switch
Database Database Database Rtr/Switch Rtr/Switch
Rtr/Switch Rtr/Switch
Switch Switch
App App App App App App App App App App App App App App App
Switch Switch Switch Switch Switch
Switch Switch Switch Rtr/Switch Rtr/Switch Rtr/Switch Rtr/Switch Rtr/Switch
Rtr/Switch Rtr/Switch Rtr/Switch Rtr/Switch Rtr/Switch Switch Switch Switch
Rtr/Switch Rtr/Switch Rtr/Switch Rtr/Switch Rtr/Switch Authentication Authentication Authentication
Rtr/Switch Rtr/Switch Rtr/Switch Load Balancer Load Balancer Authentication Authentication Authentication
Switch Switch Switch Rtr/Switch Rtr/Switch Switch Switch Switch
Database Database Database Rtr/Switch Rtr/Switch Rtr/Switch Rtr/Switch Rtr/Switch
Switch Switch Rtr/Switch Rtr/Switch Rtr/Switch Rtr/Switch Rtr/Switch
Rtr/Switch Rtr/Switch Switch Switch Rtr/Switch Rtr/Switch Rtr/Switch
Middleware Middleware Middleware Middleware Switch Switch Switch
Switch Switch Switch Switch
Authentication Authentication Rtr/Switch Rtr/Switch
Switch Switch
Authentication Authentication Switch Switch Authentication Authentication
Middleware Middleware Middleware Middleware Middleware Middleware Middleware Middleware
Switch Switch
Switch Switch Database Database
Rtr/Switch Rtr/Switch Database Database
Switch Switch
Rtr/Switch Rtr/Switch
Middleware Middleware Middleware Middleware Middleware Middleware Middleware Middleware
Switch Switch
Switch Switch Switch Switch Switch Database Database
Rtr/Switch Rtr/Switch Rtr/Switch Rtr/Switch Rtr/Switch
Switch Switch Switch Rtr/Switch Rtr/Switch Fraud Detection Fraud Detection Fraud Detection Fraud Detection
Authentication Authentication Authentication Rtr/Switch Rtr/Switch
Load Balancer Load Balancer Switch Switch Switch Switch
Switch Switch Switch Rtr/Switch Rtr/Switch Rtr/Switch Rtr/Switch Rtr/Switch Rtr/Switch
Rtr/Switch Rtr/Switch Rtr/Switch Rtr/Switch Rtr/Switch Switch Switch Switch Switch
Switch Switch Switch Rtr/Switch Rtr/Switch Fraud Detection Fraud Detection Fraud Detection Fraud Detection
Authentication Authentication Authentication Switch Switch
Gateway Gateway Gateway Gateway Gateway Gateway
Switch Switch Switch Switch Switch Switch Switch Switch
Rtr/Switch Rtr/Switch Rtr/Switch Rtr/Switch Rtr/Switch Database Database Authentication
Switch Switch Switch Rtr/Switch Rtr/Switch Switch Switch Switch
Authentication Authentication Authentication Rtr/Switch Rtr/Switch Database Database Authentication
Authentication Authentication Authentication Rtr/Switch Rtr/Switch
Mainframe Mainframe Mainframe Mainframe Mainframe Mainframe Mainframe Mainframe Mainframe Mainframe

One Internet Facing Application

1500 Total Applications

Internet Logon



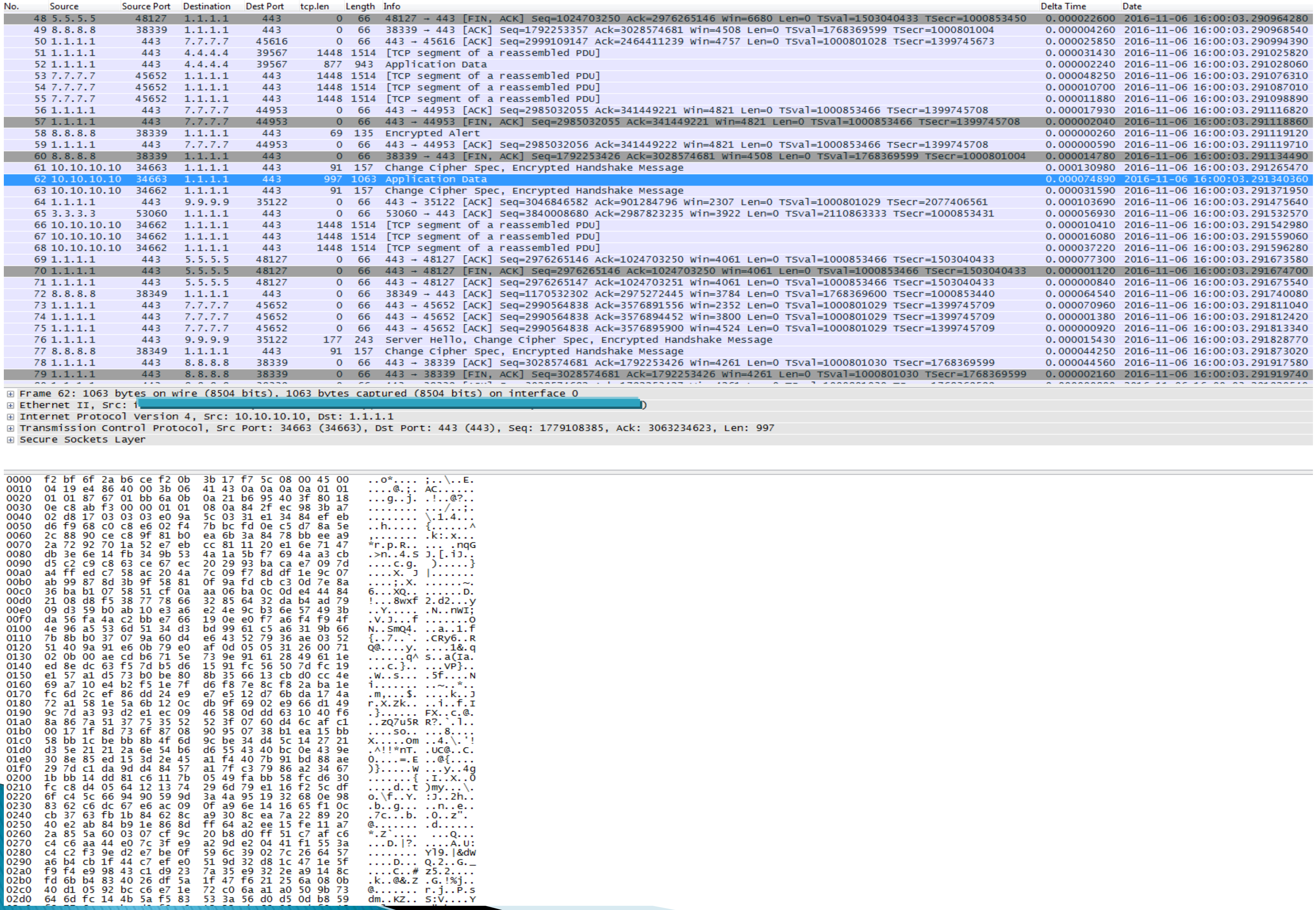
Start: 11/07 12:02:30

20 minute window (approx.)

End: 11/07 12:45:15

Data Start: 10/31 11:06:00 Duration: 7 days 02:39:16 Selected: 3,603,678 packets, 4,070,979,805 bytes Data End: 11/07 12:45:15

Internet Logon – Encrypted

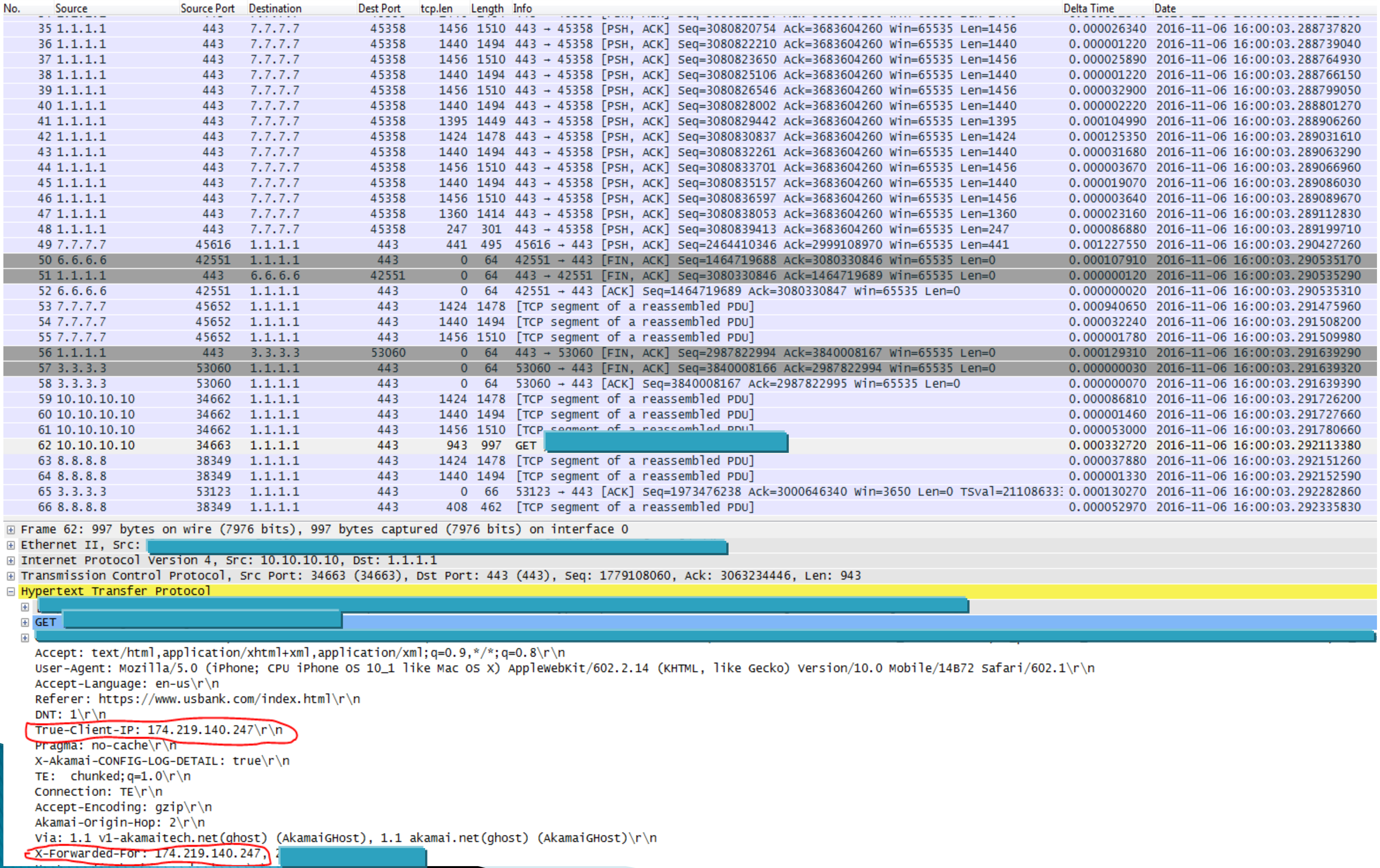


```
No.  Source       Source Port Destination Dest Port tcp.len Length Info                                                                                                      Delta Time   Date
  48 5.5.5.5        48127     1.1.1.1       443        0     66    48127 → 443 [FIN, ACK] Seq=1024703250 Ack=2976265146 Win=6680 Len=0 TSval=1503040433 TSecr=1000853450   0.000022600  2016-11-06 16:00:03.290964280
  49 8.8.8.8        38339     1.1.1.1       443        0     66    38339 → 443 [ACK] Seq=1792253357 Ack=3028574681 Win=4508 Len=0 TSval=1768369599 TSecr=1000801004        0.000004260  2016-11-06 16:00:03.290968540
  50 1.1.1.1          443     7.7.7.7     45616        0     66    443 → 45616 [ACK] Seq=2999109147 Ack=2464411239 Win=4757 Len=0 TSval=1000801028 TSecr=1399745673        0.000025850  2016-11-06 16:00:03.290994390
  51 1.1.1.1          443     4.4.4.4     39567     1448   1514    [TCP segment of a reassembled PDU]                                                                        0.000031430  2016-11-06 16:00:03.291025820
  52 1.1.1.1          443     4.4.4.4     39567      877    943    Application Data                                                                                          0.000002240  2016-11-06 16:00:03.291028060
  53 7.7.7.7        45652     1.1.1.1       443     1448   1514    [TCP segment of a reassembled PDU]                                                                        0.000048250  2016-11-06 16:00:03.291076310
  54 7.7.7.7        45652     1.1.1.1       443     1448   1514    [TCP segment of a reassembled PDU]                                                                        0.000010700  2016-11-06 16:00:03.291087010
  55 7.7.7.7        45652     1.1.1.1       443     1448   1514    [TCP segment of a reassembled PDU]                                                                        0.000011880  2016-11-06 16:00:03.291098890
  56 1.1.1.1          443     7.7.7.7     44953        0     66    443 → 44953 [ACK] Seq=2985032055 Ack=341449221 Win=4821 Len=0 TSval=1000853466 TSecr=1399745708         0.000017930  2016-11-06 16:00:03.291116820
  57 1.1.1.1          443     7.7.7.7     44953        0     66    443 → 44953 [FIN, ACK] Seq=2985032055 Ack=341449221 Win=4821 Len=0 TSval=1000853466 TSecr=1399745708    0.000002040  2016-11-06 16:00:03.291118860
  58 8.8.8.8        38339     1.1.1.1       443       69    135    Encrypted Alert                                                                                           0.000000260  2016-11-06 16:00:03.291119120
  59 1.1.1.1          443     7.7.7.7     44953        0     66    443 → 44953 [ACK] Seq=2985032056 Ack=341449222 Win=4821 Len=0 TSval=1000853466 TSecr=1399745708         0.000000590  2016-11-06 16:00:03.291119710
  60 8.8.8.8        38339     1.1.1.1       443        0     66    38339 → 443 [FIN, ACK] Seq=1792253426 Ack=3028574681 Win=4508 Len=0 TSval=1768369599 TSecr=1000801004   0.000014780  2016-11-06 16:00:03.291134490
  61 10.10.10.10    34663     1.1.1.1       443       91    157    Change Cipher Spec, Encrypted Handshake Message                                                           0.000130980  2016-11-06 16:00:03.291265470
  62 10.10.10.10    34663     1.1.1.1       443      997   1063    Application Data                                                                                          0.000074890  2016-11-06 16:00:03.291340360
  63 10.10.10.10    34662     1.1.1.1       443       91    157    Change Cipher Spec, Encrypted Handshake Message                                                           0.000031590  2016-11-06 16:00:03.291371950
  64 1.1.1.1          443     9.9.9.9     35122        0     66    443 → 35122 [ACK] Seq=3046846582 Ack=901284796 Win=2307 Len=0 TSval=1000801029 TSecr=2077406561         0.000103690  2016-11-06 16:00:03.291475640
  65 3.3.3.3        53060     1.1.1.1       443        0     66    53060 → 443 [ACK] Seq=3840008680 Ack=2987823235 Win=3922 Len=0 TSval=2110863333 TSecr=1000853431        0.000056930  2016-11-06 16:00:03.291532570
  66 10.10.10.10    34662     1.1.1.1       443     1448   1514    [TCP segment of a reassembled PDU]                                                                        0.000010410  2016-11-06 16:00:03.291542980
  67 10.10.10.10    34662     1.1.1.1       443     1448   1514    [TCP segment of a reassembled PDU]                                                                        0.000016080  2016-11-06 16:00:03.291559060
  68 10.10.10.10    34662     1.1.1.1       443     1448   1514    [TCP segment of a reassembled PDU]                                                                        0.000037220  2016-11-06 16:00:03.291596280
  69 1.1.1.1          443     5.5.5.5     48127        0     66    443 → 48127 [ACK] Seq=2976265146 Ack=1024703250 Win=4061 Len=0 TSval=1000853466 TSecr=1503040433        0.000077300  2016-11-06 16:00:03.291673580
  70 1.1.1.1          443     5.5.5.5     48127        0     66    443 → 48127 [FIN, ACK] Seq=2976265146 Ack=1024703250 Win=4061 Len=0 TSval=1000853466 TSecr=1503040433   0.000001120  2016-11-06 16:00:03.291674700
  71 1.1.1.1          443     5.5.5.5     48127        0     66    443 → 48127 [ACK] Seq=2976265147 Ack=1024703251 Win=4061 Len=0 TSval=1000853466 TSecr=1503040433        0.000000840  2016-11-06 16:00:03.291675540
  72 8.8.8.8        38349     1.1.1.1       443        0     66    38349 → 443 [ACK] Seq=1170532302 Ack=2975272445 Win=3784 Len=0 TSval=1768369600 TSecr=1000853440        0.000064540  2016-11-06 16:00:03.291740080
  73 1.1.1.1          443     7.7.7.7     45652        0     66    443 → 45652 [ACK] Seq=2990564838 Ack=3576891556 Win=2352 Len=0 TSval=1000801029 TSecr=1399745709        0.000070960  2016-11-06 16:00:03.291811040
  74 1.1.1.1          443     7.7.7.7     45652        0     66    443 → 45652 [ACK] Seq=2990564838 Ack=3576894452 Win=3800 Len=0 TSval=1000801029 TSecr=1399745709        0.000001380  2016-11-06 16:00:03.291812420
  75 1.1.1.1          443     7.7.7.7     45652        0     66    443 → 45652 [ACK] Seq=2990564838 Ack=3576895900 Win=4524 Len=0 TSval=1000801029 TSecr=1399745709        0.000000920  2016-11-06 16:00:03.291813340
  76 1.1.1.1          443     9.9.9.9     35122      177    243    Server Hello, Change Cipher Spec, Encrypted Handshake Message                                             0.000015430  2016-11-06 16:00:03.291828770
  77 8.8.8.8        38349     1.1.1.1       443       91    157    Change Cipher Spec, Encrypted Handshake Message                                                           0.000044250  2016-11-06 16:00:03.291873020
  78 1.1.1.1          443     8.8.8.8     38339        0     66    443 → 38339 [ACK] Seq=3028574681 Ack=1792253426 Win=4261 Len=0 TSval=1000801030 TSecr=1768369599        0.000044560  2016-11-06 16:00:03.291917580
  79 1.1.1.1          443     8.8.8.8     38339        0     66    443 → 38339 [FIN, ACK] Seq=3028574681 Ack=1792253426 Win=4261 Len=0 TSval=1000801030 TSecr=1768369599   0.000002160  2016-11-06 16:00:03.291919740
```

```
⊞ Frame 62: 1063 bytes on wire (8504 bits), 1063 bytes captured (8504 bits) on interface 0
⊞ Ethernet II, Src: [redacted])
⊞ Internet Protocol Version 4, Src: 10.10.10.10, Dst: 1.1.1.1
⊞ Transmission Control Protocol, Src Port: 34663 (34663), Dst Port: 443 (443), Seq: 1779108385, Ack: 3063234623, Len: 997
⊞ Secure Sockets Layer
```

```
0000  f2 bf 6f 2a b6 ce f2 0b  3b 17 f7 5c 08 00 45 00   ..o*.... ;..\..E.
0010  04 19 e4 86 40 00 3b 06  41 43 0a 0a 0a 0a 01 01   ....@.;. AC......
0020  01 01 87 67 01 bb 6a 0b  0a 21 b6 95 40 3f 80 18   ...g..j. .!..@?..
0030  0e c8 ab f3 00 00 01 01  08 0a 84 2f ec 98 3b a7   ........ .../..;.
0040  02 d8 17 03 03 03 e0 9a  5c 03 31 e1 34 84 ef eb   ........ \.1.4...
0050  d6 f9 68 c0 c8 e6 02 f4  7b bc fd 0e c5 d7 8a 5e   ..h..... {......^
0060  2c 88 90 ce c8 9f 81 b0  ea 6b 3a 84 78 bb ee a9   ,....... .k:.x...
0070  2a 72 92 70 1a 52 e7 eb  cc 81 11 20 e1 6e 71 47   *r.p.R.. ... .nqG
0080  db 3e 6e 14 fb 34 9b 53  4a 1a 5b f7 69 4a a3 cb   .>n..4.S J.[.iJ..
0090  d5 c2 c9 c8 63 ce 67 ec  20 29 93 ba ca e7 09 7d   ....c.g.  ).....}
00a0  a4 ff ed c7 58 ac 20 4a  7c 09 f7 8d df 1e 9c 07   ....X. J |.......
00b0  ab 99 87 8d 3b 9f 58 81  0f 9a fd cb c3 0d 7e 8a   ....;.X. ......~.
00c0  36 ba b1 07 58 51 cf 0a  aa 06 ba 0c 0d e4 44 84   6...XQ.. ......D.
00d0  21 08 d8 f5 38 77 78 66  32 85 64 32 da b4 ad 79   !...8wxf 2.d2...y
00e0  09 d3 59 b0 ab 10 e3 a6  e2 4e 9c b3 6e 57 49 3b   ..Y..... .N..nWI;
00f0  da 56 fa 4a c2 bb e7 66  19 0e e0 f7 a6 f4 f9 4f   .V.J...f .......O
0100  4e 96 a5 53 6d 51 34 d3  bd 99 61 c5 a6 31 9b 66   N..SmQ4. ..a..1.f
0110  7b 8b b0 37 07 9a 60 d4  e6 43 52 79 36 ae 03 52   {..7..`. .CRy6..R
0120  51 40 9a 91 e6 0b 79 e0  af 0d 05 05 31 26 00 71   Q@....y. ....1&.q
0130  02 0b 00 ae cd b6 71 5e  73 9e 91 61 28 49 61 1e   ......q^ s..a(Ia.
0140  ed 8e dc 63 f5 7d b5 d6  15 91 fc 56 50 7d fc 19   ...c.}.. ...VP}..
0150  e1 57 a1 d5 73 b0 be 80  8b 35 66 13 cb d0 cc 4e   .W..s... .5f....N
0160  69 a7 10 e4 b2 f5 1e 7f  d6 f8 7e 8c f8 2a ba 1e   i....... ..~..*..
0170  fc 6d 2c ef 86 dd 24 e9  e7 e5 12 d7 6b da 17 4a   .m,...$. ....k..J
0180  72 a1 58 1e 5a 6b 12 0c  db 9f 69 02 e9 66 d1 49   r.X.Zk.. ..i..f.I
0190  9c 7d a3 93 d2 e1 ec 09  46 58 0d dd 63 10 40 f6   .}...... FX..c.@.
01a0  8a 86 7a 51 37 75 35 52  52 3f 07 60 d4 6c af c1   ..zQ7u5R R?.`.l..
01b0  00 17 1f 8d 73 6f 87 08  90 95 07 38 b1 ea 15 bb   ....so.. ...8....
01c0  58 bb 1c be bb 8b 4f 6d  9c be 34 d4 5c 14 27 21   X.....Om ..4.\.'!
01d0  d3 5e 21 21 2a 6e 54 b6  d6 55 43 40 bc 0e 43 9e   .^!!*nT. .UC@..C.
01e0  30 8e 85 ed 15 3d 2e 45  a1 f4 40 7b 91 bd 88 ae   0....=.E ..@{....
01f0  29 7d c1 da 9d d4 84 57  a1 7f c3 79 86 a2 34 67   )}.....W ...y..4g
0200  1b bb 14 dd 81 c6 11 7b  05 49 fa bb 58 fc d6 30   .......{ .I..X..0
0210  fc c8 d4 05 64 12 13 74  29 6d 79 e1 16 f2 5c df   ....d..t )my...\.
0220  6f c4 5c 66 94 90 59 9d  3a 4a 95 19 32 68 0e 98   o.\f..Y. :J..2h..
0230  83 62 c6 dc 67 e6 ac 09  0f a9 6e 14 16 65 f1 0c   .b..g... ..n..e..
0240  cb 37 63 fb 1b 84 62 8c  a9 30 8c ea 7a 22 89 20   .7c...b. .0..z".
0250  40 e2 ab 84 b9 1e 86 8d  ff 64 a2 ee 15 fe 11 a7   @....... .d......
0260  2a 85 5a 60 03 07 cf 9c  20 b8 d0 ff 51 c7 af c6   *.Z`....  ...Q...
0270  c4 c6 aa 44 e0 7c 3f e9  a2 9d e2 04 41 f1 55 3a   ...D.|?. ....A.U:
0280  c4 c2 f3 9e d2 e7 be 0f  59 6c 39 02 7c 26 64 57   ........ Yl9.|&dW
0290  a6 b4 cb 1f 44 c7 ef e0  51 9d 32 d8 1c 47 1e 5f   ....D... Q.2..G._
02a0  f9 f4 e9 98 43 c1 d9 23  7a 35 e9 32 2e a9 14 8c   ....C..# z5.2....
02b0  fd 6b b4 83 40 26 df 5a  1f 47 f6 21 25 6a 08 0b   .k..@&.Z .G.!%j..
02c0  40 d1 05 92 bc c6 e7 1e  72 c0 6a a1 a0 50 9b 73   @....... r.j..P.s
02d0  64 6d fc 14 4b 5a f5 83  53 3a 56 d0 d5 0d b8 59   dm..KZ.. S:V....Y
```

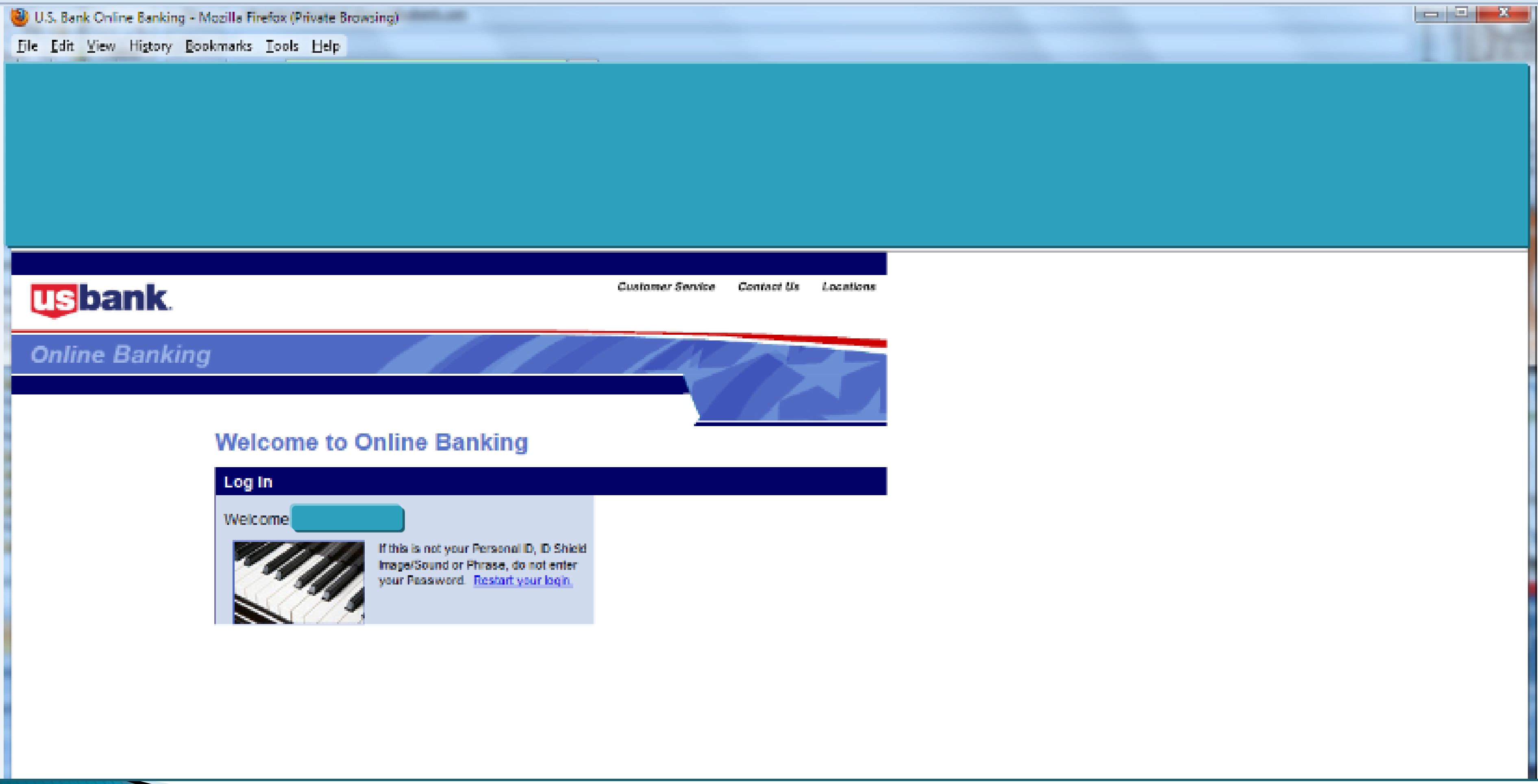
Internet Logon – Decrypted



```
No.  Source       Source Port  Destination  Dest Port  tcp.len  Length  Info                                                                                    Delta Time   Date
  35 1.1.1.1              443  7.7.7.7          45358     1456    1510  443 → 45358 [PSH, ACK] Seq=3080820754 Ack=3683604260 Win=65535 Len=1456                 0.000026340  2016-11-06 16:00:03.288737820
  36 1.1.1.1              443  7.7.7.7          45358     1440    1494  443 → 45358 [PSH, ACK] Seq=3080822210 Ack=3683604260 Win=65535 Len=1440                 0.000001220  2016-11-06 16:00:03.288739040
  37 1.1.1.1              443  7.7.7.7          45358     1456    1510  443 → 45358 [PSH, ACK] Seq=3080823650 Ack=3683604260 Win=65535 Len=1456                 0.000025890  2016-11-06 16:00:03.288764930
  38 1.1.1.1              443  7.7.7.7          45358     1440    1494  443 → 45358 [PSH, ACK] Seq=3080825106 Ack=3683604260 Win=65535 Len=1440                 0.000001220  2016-11-06 16:00:03.288766150
  39 1.1.1.1              443  7.7.7.7          45358     1456    1510  443 → 45358 [PSH, ACK] Seq=3080826546 Ack=3683604260 Win=65535 Len=1456                 0.000032900  2016-11-06 16:00:03.288799050
  40 1.1.1.1              443  7.7.7.7          45358     1440    1494  443 → 45358 [PSH, ACK] Seq=3080828002 Ack=3683604260 Win=65535 Len=1440                 0.000002220  2016-11-06 16:00:03.288801270
  41 1.1.1.1              443  7.7.7.7          45358     1395    1449  443 → 45358 [PSH, ACK] Seq=3080829442 Ack=3683604260 Win=65535 Len=1395                 0.000104990  2016-11-06 16:00:03.288906260
  42 1.1.1.1              443  7.7.7.7          45358     1424    1478  443 → 45358 [PSH, ACK] Seq=3080830837 Ack=3683604260 Win=65535 Len=1424                 0.000125350  2016-11-06 16:00:03.289031610
  43 1.1.1.1              443  7.7.7.7          45358     1440    1494  443 → 45358 [PSH, ACK] Seq=3080832261 Ack=3683604260 Win=65535 Len=1440                 0.000031680  2016-11-06 16:00:03.289063290
  44 1.1.1.1              443  7.7.7.7          45358     1456    1510  443 → 45358 [PSH, ACK] Seq=3080833701 Ack=3683604260 Win=65535 Len=1456                 0.000003670  2016-11-06 16:00:03.289066960
  45 1.1.1.1              443  7.7.7.7          45358     1440    1494  443 → 45358 [PSH, ACK] Seq=3080835157 Ack=3683604260 Win=65535 Len=1440                 0.000019070  2016-11-06 16:00:03.289086030
  46 1.1.1.1              443  7.7.7.7          45358     1456    1510  443 → 45358 [PSH, ACK] Seq=3080836597 Ack=3683604260 Win=65535 Len=1456                 0.000003640  2016-11-06 16:00:03.289089670
  47 1.1.1.1              443  7.7.7.7          45358     1360    1414  443 → 45358 [PSH, ACK] Seq=3080838053 Ack=3683604260 Win=65535 Len=1360                 0.000023160  2016-11-06 16:00:03.289112830
  48 1.1.1.1              443  7.7.7.7          45358      247     301  443 → 45358 [PSH, ACK] Seq=3080839413 Ack=3683604260 Win=65535 Len=247                  0.000086880  2016-11-06 16:00:03.289199710
  49 7.7.7.7            45616  1.1.1.1            443      441     495  45616 → 443 [PSH, ACK] Seq=2464410346 Ack=2999108970 Win=65535 Len=441                  0.001227550  2016-11-06 16:00:03.290427260
  50 6.6.6.6            42551  1.1.1.1            443        0      64  42551 → 443 [FIN, ACK] Seq=1464719688 Ack=3080330846 Win=65535 Len=0                    0.000107910  2016-11-06 16:00:03.290535170
  51 1.1.1.1              443  6.6.6.6          42551        0      64  443 → 42551 [FIN, ACK] Seq=3080330846 Ack=1464719689 Win=65535 Len=0                    0.000000120  2016-11-06 16:00:03.290535290
  52 6.6.6.6            42551  1.1.1.1            443        0      64  42551 → 443 [ACK] Seq=1464719689 Ack=3080330847 Win=65535 Len=0                         0.000000020  2016-11-06 16:00:03.290535310
  53 7.7.7.7            45652  1.1.1.1            443     1424    1478  [TCP segment of a reassembled PDU]                                                      0.000940650  2016-11-06 16:00:03.291475960
  54 7.7.7.7            45652  1.1.1.1            443     1440    1494  [TCP segment of a reassembled PDU]                                                      0.000032240  2016-11-06 16:00:03.291508200
  55 7.7.7.7            45652  1.1.1.1            443     1456    1510  [TCP segment of a reassembled PDU]                                                      0.000001780  2016-11-06 16:00:03.291509980
  56 1.1.1.1              443  3.3.3.3          53060        0      64  443 → 53060 [FIN, ACK] Seq=2987822994 Ack=3840008167 Win=65535 Len=0                    0.000129310  2016-11-06 16:00:03.291639290
  57 3.3.3.3            53060  1.1.1.1            443        0      64  53060 → 443 [FIN, ACK] Seq=3840008166 Ack=2987822994 Win=65535 Len=0                    0.000000030  2016-11-06 16:00:03.291639320
  58 3.3.3.3            53060  1.1.1.1            443        0      64  53060 → 443 [ACK] Seq=3840008167 Ack=2987822995 Win=65535 Len=0                         0.000000070  2016-11-06 16:00:03.291639390
  59 10.10.10.10        34662  1.1.1.1            443     1424    1478  [TCP segment of a reassembled PDU]                                                      0.000086810  2016-11-06 16:00:03.291726200
  60 10.10.10.10        34662  1.1.1.1            443     1440    1494  [TCP segment of a reassembled PDU]                                                      0.000001460  2016-11-06 16:00:03.291727660
  61 10.10.10.10        34662  1.1.1.1            443     1456    1510  [TCP                                                                                    0.000053000  2016-11-06 16:00:03.291780660
  62 10.10.10.10        34663  1.1.1.1            443      943     997  GET [redacted]                                                                          0.000332720  2016-11-06 16:00:03.292113380
  63 8.8.8.8            38349  1.1.1.1            443     1424    1478  [TCP segment of a reassembled PDU]                                                      0.000037880  2016-11-06 16:00:03.292151260
  64 8.8.8.8            38349  1.1.1.1            443     1440    1494  [TCP segment of a reassembled PDU]                                                      0.000001330  2016-11-06 16:00:03.292152590
  65 3.3.3.3            53123  1.1.1.1            443        0      66  53123 → 443 [ACK] Seq=1973476238 Ack=3000646340 Win=3650 Len=0 TSval=21108633          0.000130270  2016-11-06 16:00:03.292282860
  66 8.8.8.8            38349  1.1.1.1            443      408     462  [TCP segment of a reassembled PDU]                                                      0.000052970  2016-11-06 16:00:03.292335830

⊞ Frame 62: 997 bytes on wire (7976 bits), 997 bytes captured (7976 bits) on interface 0
⊞ Ethernet II, Src: [redacted]
⊞ Internet Protocol Version 4, Src: 10.10.10.10, Dst: 1.1.1.1
⊞ Transmission Control Protocol, Src Port: 34663 (34663), Dst Port: 443 (443), Seq: 1779108060, Ack: 3063234446, Len: 943
⊟ Hypertext Transfer Protocol
    ⊞ [redacted]
    ⊞ GET [redacted]
    ⊞ [redacted]
      Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8\r\n
      User-Agent: Mozilla/5.0 (iPhone; CPU iPhone OS 10_1 like Mac OS X) AppleWebKit/602.2.14 (KHTML, like Gecko) Version/10.0 Mobile/14B72 Safari/602.1\r\n
      Accept-Language: en-us\r\n
      Referer: https://www.usbank.com/index.html\r\n
      DNT: 1\r\n
      True-Client-IP: 174.219.140.247\r\n
      Pragma: no-cache\r\n
      X-Akamai-CONFIG-LOG-DETAIL: true\r\n
      TE:  chunked;q=1.0\r\n
      Connection: TE\r\n
      Accept-Encoding: gzip\r\n
      Akamai-Origin-Hop: 2\r\n
      Via: 1.1 v1-akamaitech.net(ghost) (AkamaiGHost), 1.1 akamai.net(ghost) (AkamaiGHost)\r\n
      X-Forwarded-For: 174.219.140.247, [redacted]
```

Internet Banking Login Failure


U.S. Bank Online Banking - Mozilla Firefox (Private Browsing)
File Edit View History Bookmarks Tools Help
usbank
Customer Service
Contact Us
Locations
Online Banking

Welcome to Online Banking

Log In

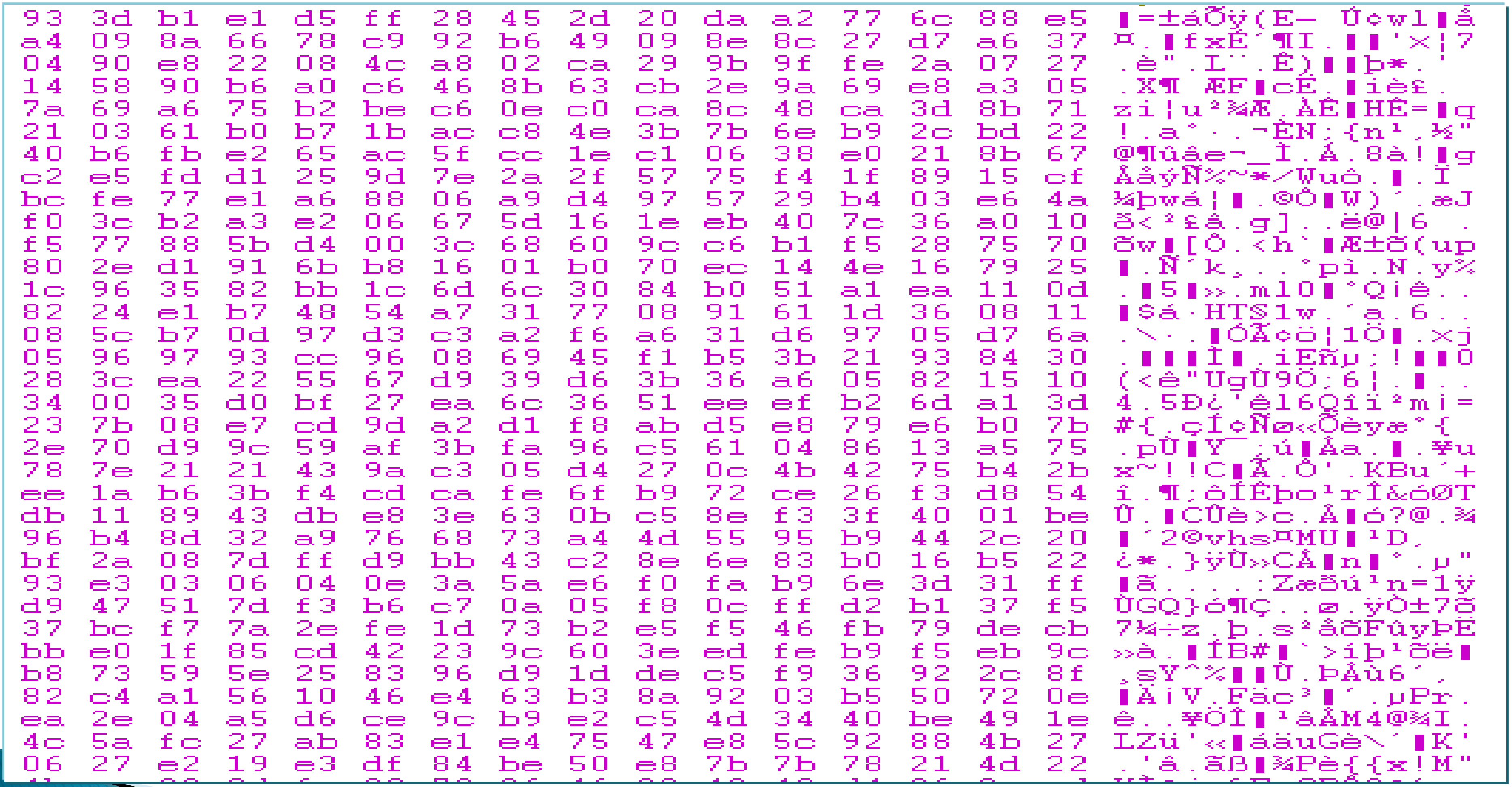
Welcome

If this is not your Personal ID, ID Shield Image/Sound or Phrase, do not enter your Password. Restart your login.

Application Log

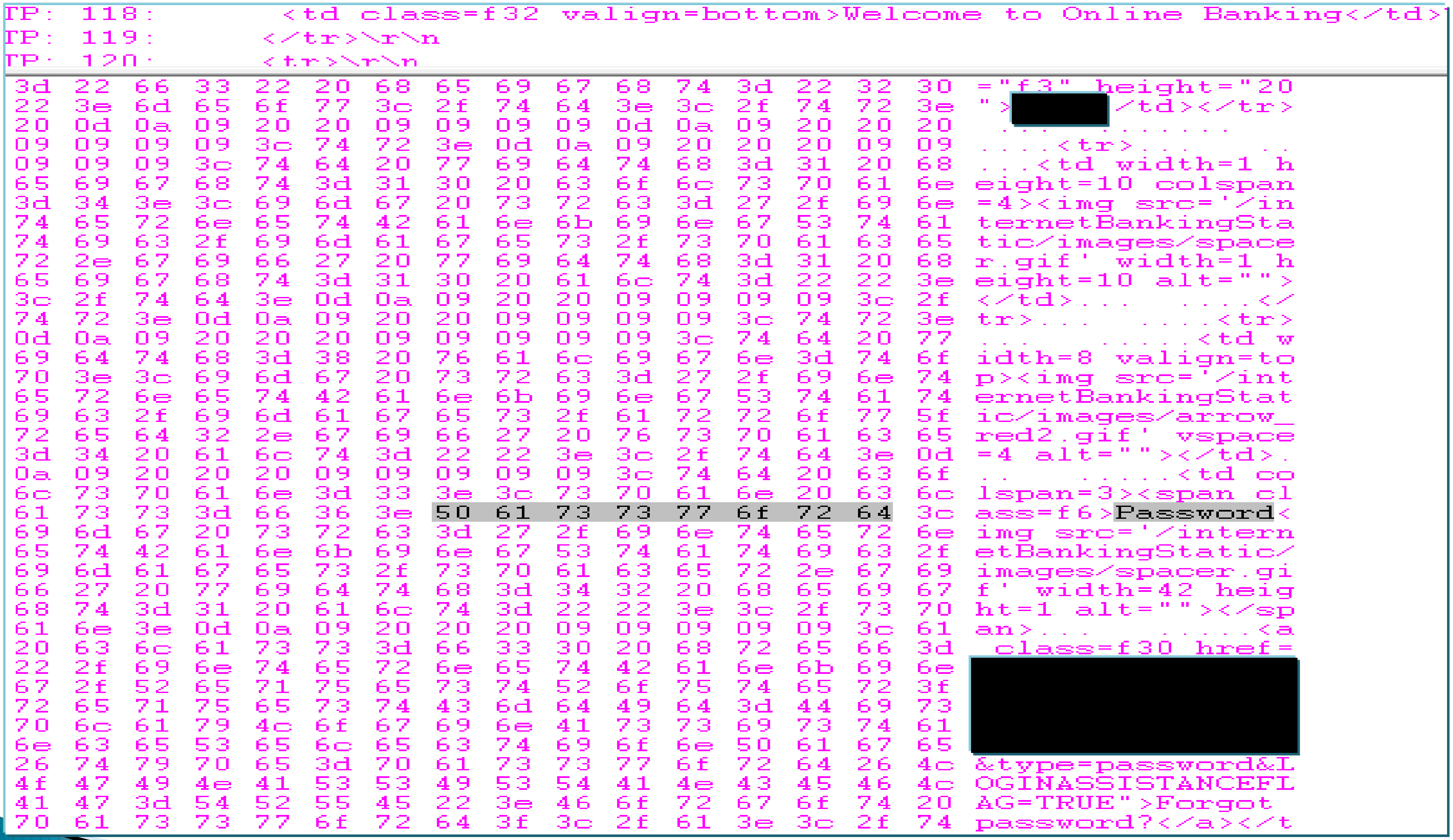
15:30:43	Column 12	10.10.10.10	Enter Userid	Challenge Question
15:30:59	Column 12	10.10.10.10	Challenge Answer	Answer OK
15:36:29	Column 12	10.10.10.10	Enter Userid	Challenge Question
15:36:34	Column 12	10.10.10.10	Challenge Answer	Answer OK
15:41:35	Column 11	10.10.10.10	Enter Userid	Challenge Question
15:41:44	Column 11	10.10.10.10	Challenge Answer	Answer OK
15:49:01	Column 6	10.10.10.10	Enter Userid	Challenge Question
15:49:06	Column 6	10.10.10.10	Challenge Answer	Answer OK
15:54:16	Column 9	10.10.10.10	Enter Userid	Challenge Question
15:54:22	Column 9	10.10.10.10	Challenge Answer	Answer OK

Internet Analysis – Encrypted Login Screen



```
93 3d b1 e1 d5 ff 28 45 2d 20 da a2 77 6c 88 e5  ▮=±áÕÿ(E– Ú¢wl▮å
a4 09 8a 66 78 c9 92 b6 49 09 8e 8c 27 d7 a6 37  ¤.▮fxÉ´¶I.▮▮'×¦7
04 90 e8 22 08 4c a8 02 ca 29 9b 9f fe 2a 07 27   .è".L¨.Ê)▮▮þ*.'
14 58 90 b6 a0 c6 46 8b 63 cb 2e 9a 69 e8 a3 05   .X¶ ÆF▮cË.▮iè£.
7a 69 a6 75 b2 be c6 0e c0 ca 8c 48 ca 3d 8b 71  zi¦u²¾Æ.ÀÊ▮HÊ=▮q
21 03 61 b0 b7 1b ac c8 4e 3b 7b 6e b9 2c bd 22  !.a°·.¬ÈN;{n¹,½"
40 b6 fb e2 65 ac 5f cc 1e c1 06 38 e0 21 8b 67  @¶ûâe¬_Ì.Á.8à!▮g
c2 e5 fd d1 25 9d 7e 2a 2f 57 75 f4 1f 89 15 cf  ÅåýÑ%~*/Wuô.▮.Ï
bc fe 77 e1 a6 88 06 a9 d4 97 57 29 b4 03 e6 4a  ¼þwá¦▮.©Ô▮W)´.æJ
f0 3c b2 a3 e2 06 67 5d 16 1e eb 40 7c 36 a0 10  ð<²£â.g]..ë@|6 .
f5 77 88 5b d4 00 3c 68 60 9c c6 b1 f5 28 75 70  õw▮[Ô.<h`▮Æ±õ(up
80 2e d1 91 6b b8 16 01 b0 70 ec 14 4e 16 79 25  ▮.Ñ´k¸..°pi.N.y%
1c 96 35 82 bb 1c 6d 6c 30 84 b0 51 a1 ea 11 0d  .▮5▮».ml0▮°Q¡ê..
82 24 e1 b7 48 54 a7 31 77 08 91 61 1d 36 08 11  ▮$á·HT§1w.´a.6..
08 5c b7 0d 97 d3 c3 a2 f6 a6 31 d6 97 05 d7 6a  .\·.▮ÓÃ¢ö¦1Ö▮.×j
05 96 97 93 cc 96 08 69 45 f1 b5 3b 21 93 84 30  .▮▮▮Ì▮.iEñµ;!▮▮0
28 3c ea 22 55 67 d9 39 d6 3b 36 a6 05 82 15 10  (<ê"UgÙ9Ö;6¦.▮..
34 00 35 d0 bf 27 ea 6c 36 51 ee ef b2 6d a1 3d  4.5Ð¿'êl6Qîï²m¡=
23 7b 08 e7 cd 9d a2 d1 f8 ab d5 e8 79 e6 b0 7b  #{.çÍ¢Ñø«Õèyæ°{
2e 70 d9 9c 59 af 3b fa 96 c5 61 04 86 13 a5 75  .pÙ▮Y¯;ú▮Åa.▮.¥u
78 7e 21 21 43 9a c3 05 d4 27 0c 4b 42 75 b4 2b  x~!!C▮Ã.Ô'.KBu´+
ee 1a b6 3b f4 cd ca fe 6f b9 72 ce 26 f3 d8 54  î.¶;ôÍÊþo¹rÎ&óØT
db 11 89 43 db e8 3e 63 0b c5 8e f3 3f 40 01 be  Û.▮CÛè>c.Å▮ó?@.¾
96 b4 8d 32 a9 76 68 73 a4 4d 55 95 b9 44 2c 20  ▮´2©vhs¤MU▮¹D,
bf 2a 08 7d ff d9 bb 43 c2 8e 6e 83 b0 16 b5 22  ¿*.}ÿÙ»CÅ▮n▮°.µ"
93 e3 03 06 04 0e 3a 5a e6 f0 fa b9 6e 3d 31 ff  ▮ã....:Zæðú¹n=1ÿ
d9 47 51 7d f3 b6 c7 0a 05 f8 0c ff d2 b1 37 f5  ÙGQ}ó¶Ç..ø.ÿÒ±7õ
37 bc f7 7a 2e fe 1d 73 b2 e5 f5 46 fb 79 de cb  7¼÷z.þ.s²åõFûyÞË
bb e0 1f 85 cd 42 23 9c 60 3e ed fe b9 f5 eb 9c  »à.▮ÍB#▮`>íþ¹õë▮
b8 73 59 5e 25 83 96 d9 1d de c5 f9 36 92 2c 8f  ¸sY^%▮▮Ù.ÞÅù6´,
82 c4 a1 56 10 46 e4 63 b3 8a 92 03 b5 50 72 0e  ▮Ä¡V.Fäc³▮´.µPr.
ea 2e 04 a5 d6 ce 9c b9 e2 c5 4d 34 40 be 49 1e  ê..¥ÖÎ▮¹âÅM4@¾I.
4c 5a fc 27 ab 83 e1 e4 75 47 e8 5c 92 88 4b 27  LZü'«▮áäuGè\´▮K'
06 27 e2 19 e3 df 84 be 50 e8 7b 7b 78 21 4d 22  .'â.ãß▮¾Pè{{x!M"
```

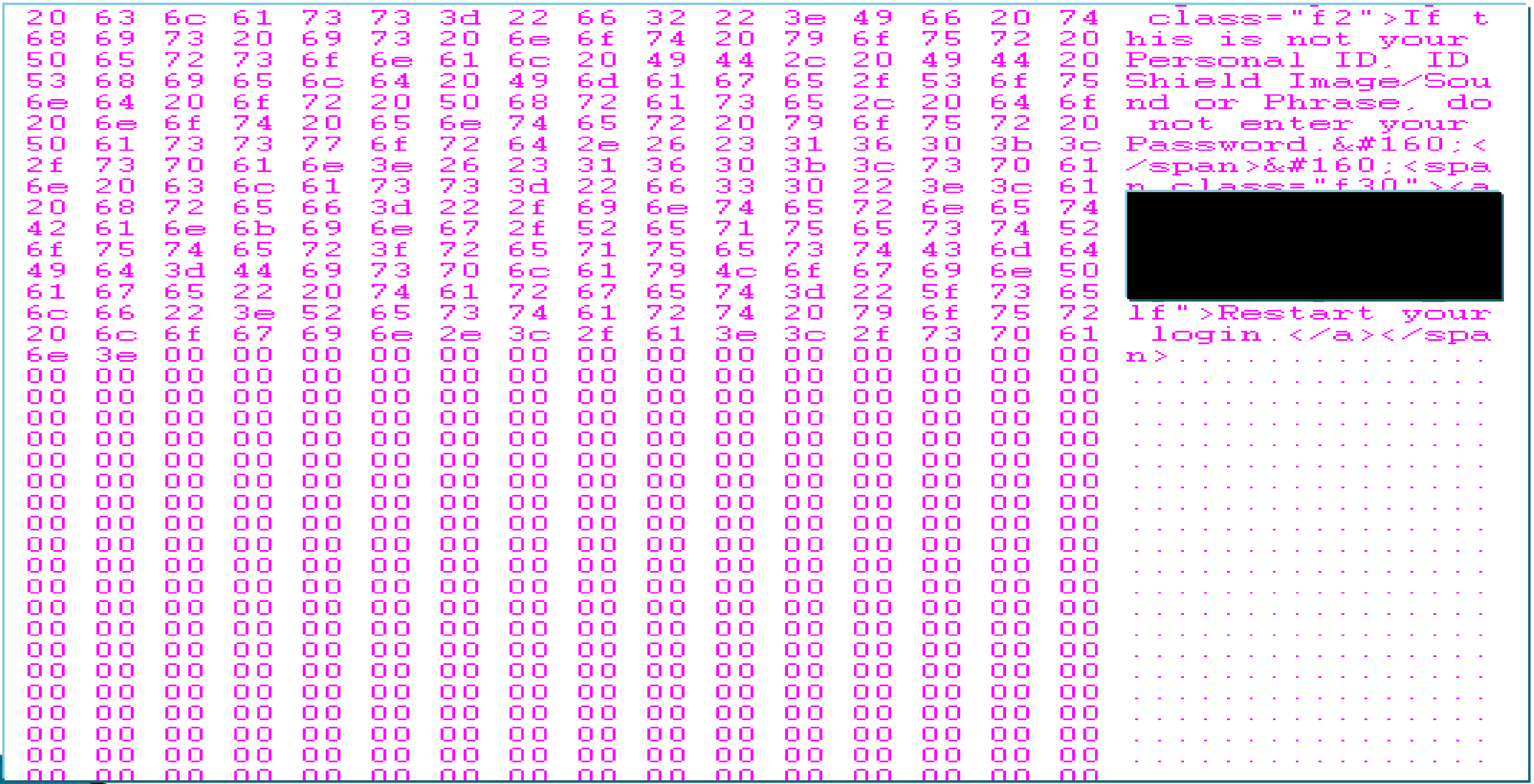
Internet Analysis – Decrypted Login Screen



```
TP:  118:        <td class=f32 valign=bottom>Welcome to Online Banking</td>
TP:  119:       </tr>\r\n
TP:  120:       <tr>\r\n
```

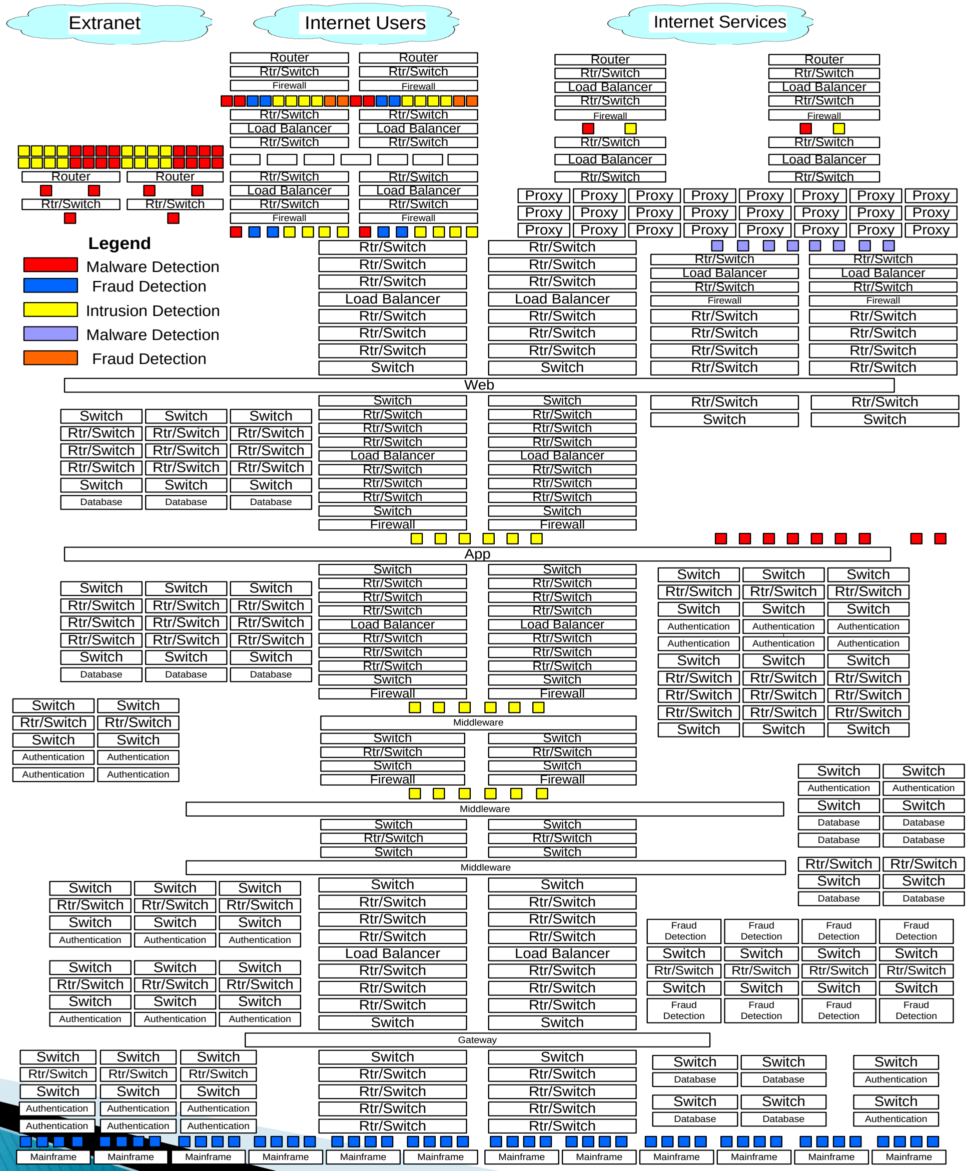
```
3d 22 66 33 22 20 68 65 69 67 68 74 3d 22 32 30  ="f3" height="20
22 3e 6d 65 6f 77 3c 2f 74 64 3e 3c 2f 74 72 3e  ">[redacted]</td></tr>
20 0d 0a 09 20 20 09 09 09 09 0d 0a 09 20 20 20   ...  .......   
09 09 09 09 3c 74 72 3e 0d 0a 09 20 20 20 09 09  ....<tr>...   ..
09 09 09 3c 74 64 20 77 69 64 74 68 3d 31 20 68  ...<td width=1 h
65 69 67 68 74 3d 31 30 20 63 6f 6c 73 70 61 6e  eight=10 colspan
3d 34 3e 3c 69 6d 67 20 73 72 63 3d 27 2f 69 6e  =4><img src='/in
74 65 72 6e 65 74 42 61 6e 6b 69 6e 67 53 74 61  ternetBankingSta
74 69 63 2f 69 6d 61 67 65 73 2f 73 70 61 63 65  tic/images/space
72 2e 67 69 66 27 20 77 69 64 74 68 3d 31 20 68  r.gif' width=1 h
65 69 67 68 74 3d 31 30 20 61 6c 74 3d 22 22 3e  eight=10 alt="">
3c 2f 74 64 3e 0d 0a 09 20 20 09 09 09 09 3c 2f  </td>...  ....</
74 72 3e 0d 0a 09 20 20 09 09 09 09 3c 74 72 3e  tr>...  ....<tr>
0d 0a 09 20 20 20 09 09 09 09 09 3c 74 64 20 77  ...   .....<td w
69 64 74 68 3d 38 20 76 61 6c 69 67 6e 3d 74 6f  idth=8 valign=to
70 3e 3c 69 6d 67 20 73 72 63 3d 27 2f 69 6e 74  p><img src='/int
65 72 6e 65 74 42 61 6e 6b 69 6e 67 53 74 61 74  ernetBankingStat
69 63 2f 69 6d 61 67 65 73 2f 61 72 72 6f 77 5f  ic/images/arrow_
72 65 64 32 2e 67 69 66 27 20 76 73 70 61 63 65  red2.gif' vspace
3d 34 20 61 6c 74 3d 22 22 3e 3c 2f 74 64 3e 0d  =4 alt=""></td>.
0a 09 20 20 20 09 09 09 09 09 3c 74 64 20 63 6f  ..   .....<td co
6c 73 70 61 6e 3d 33 3e 3c 73 70 61 6e 20 63 6c  lspan=3><span cl
61 73 73 3d 66 36 3e 50 61 73 73 77 6f 72 64 3c  ass=f6>Password<
69 6d 67 20 73 72 63 3d 27 2f 69 6e 74 65 72 6e  img src='/intern
65 74 42 61 6e 6b 69 6e 67 53 74 61 74 69 63 2f  etBankingStatic/
69 6d 61 67 65 73 2f 73 70 61 63 65 72 2e 67 69  images/spacer.gi
66 27 20 77 69 64 74 68 3d 34 32 20 68 65 69 67  f' width=42 heig
68 74 3d 31 20 61 6c 74 3d 22 22 3e 3c 2f 73 70  ht=1 alt=""></sp
61 6e 3e 0d 0a 09 20 20 20 09 09 09 09 09 3c 61  an>...   .....<a
20 63 6c 61 73 73 3d 66 33 30 20 68 72 65 66 3d   class=f30 href=
22 2f 69 6e 74 65 72 6e 65 74 42 61 6e 6b 69 6e  [redacted]
67 2f 52 65 71 75 65 73 74 52 6f 75 74 65 72 3f
72 65 71 75 65 73 74 43 6d 64 49 64 3d 44 69 73
70 6c 61 79 4c 6f 67 69 6e 41 73 73 69 73 74 61
6e 63 65 53 65 6c 65 63 74 69 6f 6e 50 61 67 65
26 74 79 70 65 3d 70 61 73 73 77 6f 72 64 26 4c  &type=password&L
4f 47 49 4e 41 53 53 49 53 54 41 4e 43 45 46 4c  OGINASSISTANCEFL
41 47 3d 54 52 55 45 22 3e 46 6f 72 67 6f 74 20  AG=TRUE">Forgot 
70 61 73 73 77 6f 72 64 3f 3c 2f 61 3e 3c 2f 74  password?</a></t
```

Internet Analysis – Hex Data



```
20 63 6c 61 73 73 3d 22 66 32 22 3e 49 66 20 74   class="f2">If t
68 69 73 20 69 73 20 6e 6f 74 20 79 6f 75 72 20  his is not your
50 65 72 73 6f 6e 61 6c 20 49 44 2c 20 49 44 20  Personal ID, ID
53 68 69 65 6c 64 20 49 6d 61 67 65 2f 53 6f 75  Shield Image/Sou
6e 64 20 6f 72 20 50 68 72 61 73 65 2c 20 64 6f  nd or Phrase, do
20 6e 6f 74 20 65 6e 74 65 72 20 79 6f 75 72 20   not enter your
50 61 73 73 77 6f 72 64 2e 26 23 31 36 30 3b 3c  Password.&#160;<
2f 73 70 61 6e 3e 26 23 31 36 30 3b 3c 73 70 61  /span>&#160;<spa
6e 20 63 6c 61 73 73 3d 22 66 33 30 22 3e 3c 61  n class="f30"><a
20 68 72 65 66 3d 22 2f 69 6e 74 65 72 6e 65 74  [redacted]
42 61 6e 6b 69 6e 67 2f 52 65 71 75 65 73 74 52
6f 75 74 65 72 3f 72 65 71 75 65 73 74 43 6d 64
49 64 3d 44 69 73 70 6c 61 79 4c 6f 67 69 6e 50
61 67 65 22 20 74 61 72 67 65 74 3d 22 5f 73 65
6c 66 22 3e 52 65 73 74 61 72 74 20 79 6f 75 72  lf">Restart your
20 6c 6f 67 69 6e 2e 3c 2f 61 3e 3c 2f 73 70 61   login.</a></spa
6e 3e 00 00 00 00 00 00 00 00 00 00 00 00 00 00  n>..............
00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00  ................
00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00  ................
00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00  ................
00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00  ................
00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00  ................
00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00  ................
00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00  ................
00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00  ................
00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00  ................
00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00  ................
00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00  ................
00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00  ................
00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00  ................
00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00  ................
00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00  ................
00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00  ................
00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00  ................
00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00  ................
00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00  ................
00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
```

Enterprise Security Challenges



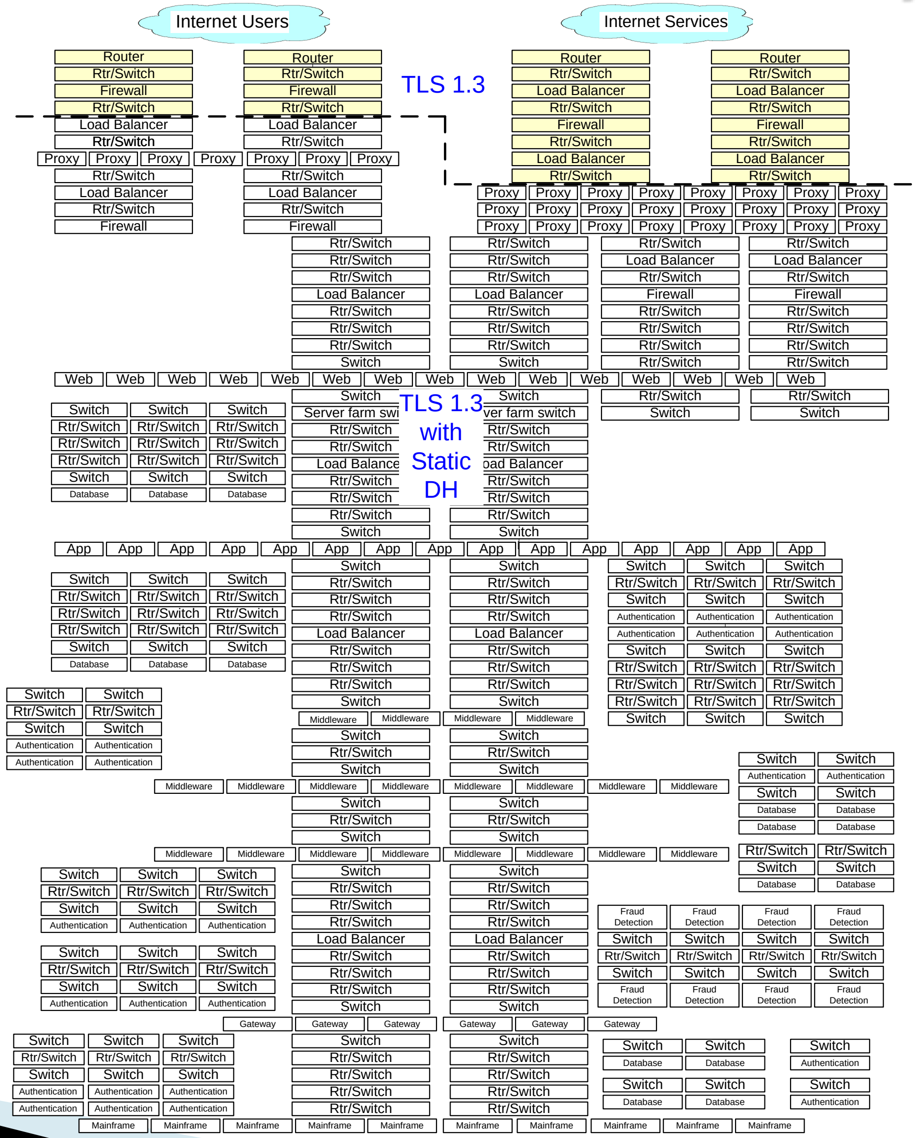
Legend

- 🟥 Malware Detection
- 🟦 Fraud Detection
- 🟨 Intrusion Detection
- 🟪 Malware Detection
- 🟧 Fraud Detection

Summary

- This is an industry-wide concern
  - Financial, Health Care, Retail, Government and others are affected
- We’re not asking for the return of RSA Key Establishment
- Regulators look to Internet standards and apply them inside the enterprise
  - TLS 1.2 is not a long term solution

Proposed Data Center Visibility Solution



Internet Users

Internet Services

TLS 1.3

TLS 1.3 with Static DH

Router | Rtr/Switch | Firewall | Rtr/Switch | Load Balancer | Rtr/Switch | Proxy Proxy Proxy | Rtr/Switch | Load Balancer | Rtr/Switch | Firewall

Router | Rtr/Switch | Firewall | Rtr/Switch | Load Balancer | Rtr/Switch | Proxy Proxy Proxy Proxy | Rtr/Switch | Load Balancer | Rtr/Switch | Firewall

Router | Rtr/Switch | Load Balancer | Rtr/Switch | Firewall | Rtr/Switch | Load Balancer | Rtr/Switch

Router | Rtr/Switch | Load Balancer | Rtr/Switch | Firewall | Rtr/Switch | Load Balancer | Rtr/Switch

Proxy Proxy Proxy Proxy Proxy Proxy Proxy Proxy

Proxy Proxy Proxy Proxy Proxy Proxy Proxy Proxy

Proxy Proxy Proxy Proxy Proxy Proxy Proxy Proxy

Rtr/Switch | Rtr/Switch | Rtr/Switch | Load Balancer | Rtr/Switch | Rtr/Switch | Rtr/Switch | Switch

Rtr/Switch | Rtr/Switch | Rtr/Switch | Load Balancer | Rtr/Switch | Rtr/Switch | Rtr/Switch | Switch

Rtr/Switch | Load Balancer | Rtr/Switch | Firewall | Rtr/Switch | Rtr/Switch | Rtr/Switch | Rtr/Switch

Rtr/Switch | Load Balancer | Rtr/Switch | Firewall | Rtr/Switch | Rtr/Switch | Rtr/Switch | Rtr/Switch

Web Web Web Web Web Web Web Web Web Web Web Web Web Web Web

Switch | Rtr/Switch | Rtr/Switch | Rtr/Switch | Switch | Database (×3)

Switch | Server farm swi | Rtr/Switch | Rtr/Switch | Load Balance | Rtr/Switch | Rtr/Switch | Rtr/Switch | Switch

Switch | ver farm switch | Rtr/Switch | Rtr/Switch | oad Balancer | Rtr/Switch | Rtr/Switch | Rtr/Switch | Switch

Rtr/Switch | Switch (×2)

App App App App App App App App App App App App App App App

Switch | Rtr/Switch | Rtr/Switch | Rtr/Switch | Switch | Database (×3)

Switch | Rtr/Switch | Rtr/Switch | Rtr/Switch | Load Balancer | Rtr/Switch | Rtr/Switch | Rtr/Switch | Switch (×2)

Switch | Rtr/Switch | Switch | Authentication | Authentication | Switch | Rtr/Switch | Rtr/Switch | Rtr/Switch | Switch (×3)

Switch | Rtr/Switch | Switch | Authentication | Authentication (×2)

Middleware Middleware Middleware Middleware

Switch | Rtr/Switch | Switch (×2)

Middleware Middleware Middleware Middleware Middleware Middleware Middleware Middleware

Switch | Rtr/Switch | Switch (×2)

Middleware Middleware Middleware Middleware Middleware Middleware Middleware Middleware

Switch | Authentication | Switch | Database | Database | Rtr/Switch | Switch | Database (×2)

Switch | Rtr/Switch | Switch | Authentication | Switch | Rtr/Switch | Switch | Authentication (×3)

Switch | Rtr/Switch | Rtr/Switch | Rtr/Switch | Load Balancer | Rtr/Switch | Rtr/Switch | Rtr/Switch | Switch (×2)

Fraud Detection | Switch | Rtr/Switch | Switch | Fraud Detection (×4)

Gateway Gateway Gateway Gateway Gateway Gateway

Switch | Rtr/Switch | Switch | Authentication | Authentication (×3)

Switch | Rtr/Switch | Rtr/Switch | Rtr/Switch | Rtr/Switch (×2)

Switch | Database | Switch | Database (×2)

Switch | Authentication | Switch | Authentication

Mainframe Mainframe Mainframe Mainframe Mainframe Mainframe Mainframe Mainframe Mainframe Mainframe

How do we meet the need for internal visibility?

- #1 We would like to collaborate with the TLS WG to incorporate an enterprise-centric solution in your base specification.
  - This would ensure the same well-studied and interoperable solution that works throughout the world.
    - draft-green-tls-static-dh-in-tls13-00.txt
    - Using Static Diffie Hellman In TLS 1.3 (Working Draft) http://bit.ly/2fhYtVo

- #2 Being part of an IETF standard is needed for vendor adoption of a data center visibility solution.