# Analyzing TCP protocol using Wireshark

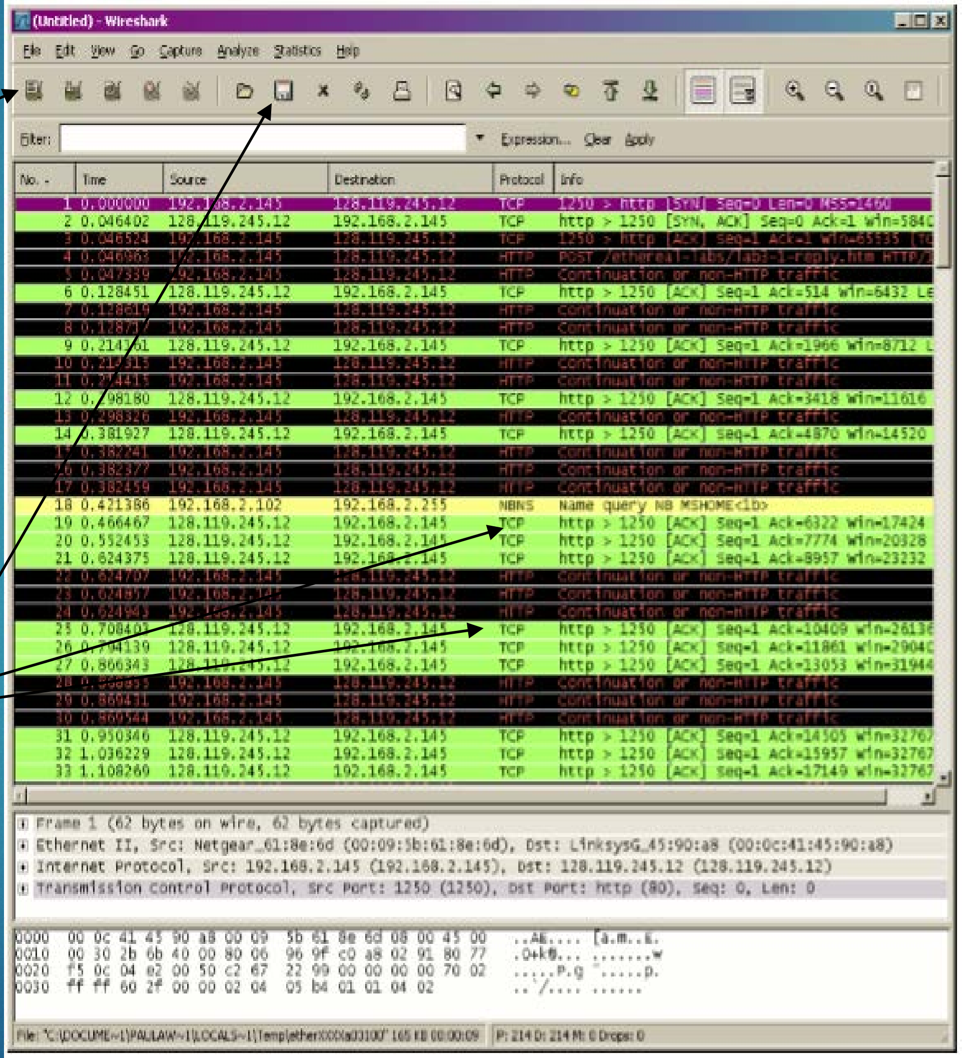
By – Naga Jayadeep Akula
Course – CPE/NIS 654

# TCP protocol

- TCP is a protocol which the network uses for a connection oriented service.
- TCP is chosen for applications like data transfer where we can’t afford data losses.
- For services which do not need a reliable connection,

# Running the TCP protocol

- To start collecting TCP packets, start wireshark and begin capture.
- Open the browser and go to a website. It is observed that we see collection of HTTP packets in wireshark.
- To start collecting TCP packets open a connection oriented service like a email, world wide web etc.
- Send a mail and observe the collection of TCP packets in wireshark.
- Now trop the tracing and save the packets for analysis.



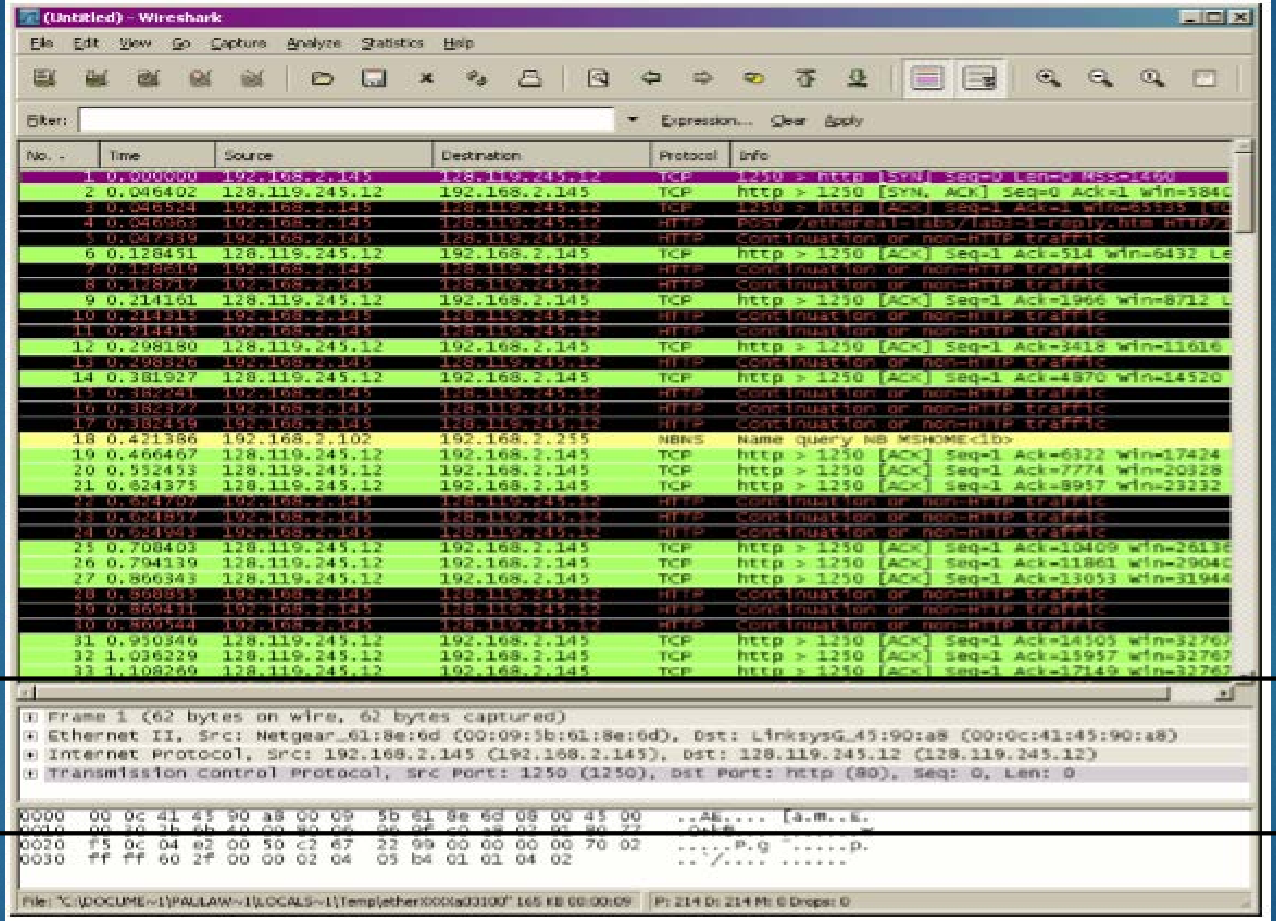
| No. | Time | Source | Destination | Protocol | Info |
|---|---|---|---|---|---|
| 1 | 0.000000 | 192.168.2.145 | 128.119.245.12 | TCP | 1250 > http [SYN] Seq=0 Len=0 MSS=1460 |
| 2 | 0.046402 | 128.119.245.12 | 192.168.2.145 | TCP | http > 1250 [SYN, ACK] Seq=0 Ack=1 Win=584C |
| 3 | 0.046524 | 192.168.2.145 | 128.119.245.12 | TCP | 1250 > http [ACK] Seq=1 Ack=1 Win=65535 [TC |
| 4 | 0.046963 | 192.168.2.145 | 128.119.245.12 | HTTP | POST /ethereal-labs/lab3-1-reply.htm HTTP/1 |
| 5 | 0.047339 | 192.168.2.145 | 128.119.245.12 | HTTP | Continuation or non-HTTP traffic |
| 6 | 0.128451 | 128.119.245.12 | 192.168.2.145 | TCP | http > 1250 [ACK] Seq=1 Ack=514 Win=6432 Le |
| 7 | 0.128619 | 192.168.2.145 | 128.119.245.12 | HTTP | Continuation or non-HTTP traffic |
| 8 | 0.128717 | 192.168.2.145 | 128.119.245.12 | HTTP | Continuation or non-HTTP traffic |
| 9 | 0.214161 | 128.119.245.12 | 192.168.2.145 | TCP | http > 1250 [ACK] Seq=1 Ack=1966 Win=8712 L |
| 10 | 0.214315 | 192.168.2.145 | 128.119.245.12 | HTTP | Continuation or non-HTTP traffic |
| 11 | 0.214415 | 192.168.2.145 | 128.119.245.12 | HTTP | Continuation or non-HTTP traffic |
| 12 | 0.298180 | 128.119.245.12 | 192.168.2.145 | TCP | http > 1250 [ACK] Seq=1 Ack=3418 Win=11616 |
| 13 | 0.298326 | 192.168.2.145 | 128.119.245.12 | HTTP | Continuation or non-HTTP traffic |
| 14 | 0.381927 | 128.119.245.12 | 192.168.2.145 | TCP | http > 1250 [ACK] Seq=1 Ack=4870 Win=14520 |
| 15 | 0.382241 | 192.168.2.145 | 128.119.245.12 | HTTP | Continuation or non-HTTP traffic |
| 16 | 0.382377 | 192.168.2.145 | 128.119.245.12 | HTTP | Continuation or non-HTTP traffic |
| 17 | 0.382459 | 192.168.2.145 | 128.119.245.12 | HTTP | Continuation or non-HTTP traffic |
| 18 | 0.421386 | 192.168.2.102 | 192.168.2.255 | NBNS | Name query NB MSHOME<1b> |
| 19 | 0.466467 | 128.119.245.12 | 192.168.2.145 | TCP | http > 1250 [ACK] Seq=1 Ack=6322 Win=17424 |
| 20 | 0.552453 | 128.119.245.12 | 192.168.2.145 | TCP | http > 1250 [ACK] Seq=1 Ack=7774 Win=20328 |
| 21 | 0.624375 | 128.119.245.12 | 192.168.2.145 | TCP | http > 1250 [ACK] Seq=1 Ack=8957 Win=23232 |
| 22 | 0.624707 | 192.168.2.145 | 128.119.245.12 | HTTP | Continuation or non-HTTP traffic |
| 23 | 0.624857 | 192.168.2.145 | 128.119.245.12 | HTTP | Continuation or non-HTTP traffic |
| 24 | 0.624943 | 192.168.2.145 | 128.119.245.12 | HTTP | Continuation or non-HTTP traffic |
| 25 | 0.708403 | 128.119.245.12 | 192.168.2.145 | TCP | http > 1250 [ACK] Seq=1 Ack=10409 Win=2613 |
| 26 | 0.794139 | 128.119.245.12 | 192.168.2.145 | TCP | http > 1250 [ACK] Seq=1 Ack=11861 Win=2904 |
| 27 | 0.866343 | 128.119.245.12 | 192.168.2.145 | TCP | http > 1250 [ACK] Seq=1 Ack=13053 Win=3194 |
| 28 | 0.868855 | 192.168.2.145 | 128.119.245.12 | HTTP | Continuation or non-HTTP traffic |
| 29 | 0.869431 | 192.168.2.145 | 128.119.245.12 | HTTP | Continuation or non-HTTP traffic |
| 30 | 0.869544 | 192.168.2.145 | 128.119.245.12 | HTTP | Continuation or non-HTTP traffic |
| 31 | 0.950346 | 128.119.245.12 | 192.168.2.145 | TCP | http > 1250 [ACK] Seq=1 Ack=14505 Win=3276 |
| 32 | 1.036229 | 128.119.245.12 | 192.168.2.145 | TCP | http > 1250 [ACK] Seq=1 Ack=15957 Win=3276 |
| 33 | 1.108269 | 128.119.245.12 | 192.168.2.145 | TCP | http > 1250 [ACK] Seq=1 Ack=17149 Win=3276 |

```
⊞ Frame 1 (62 bytes on wire, 62 bytes captured)
⊞ Ethernet II, Src: Netgear_61:8e:6d (00:09:5b:61:8e:6d), Dst: LinksysG_45:90:a8 (00:0c:41:45:90:a8)
⊞ Internet Protocol, Src: 192.168.2.145 (192.168.2.145), Dst: 128.119.245.12 (128.119.245.12)
⊞ Transmission Control Protocol, Src Port: 1250 (1250), Dst Port: http (80), Seq: 0, Len: 0
```

```
0000  00 0c 41 45 90 a8 00 09  5b 61 8e 6d 08 00 45 00   ..AE.... [a.m..E.
0010  00 30 2b 6b 40 00 80 06  96 9f c0 a8 02 91 80 77   .0+k@... .......w
0020  f5 0c 04 e2 00 50 c2 67  22 99 00 00 00 00 70 02   .....P.g ".....p.
0030  ff ff 60 2f 00 00 02 04  05 b4 01 01 04 02         ..`/.... ......
```

File: "C:\DOCUME~1\PAULAW~1\LOCALS~1\Temp\etherXXXXa03100" 165 KB 00:00:09 | P: 214 D: 214 M: 0 Drops: 0

# Sample workspace



```
(Untitled) - Wireshark
File  Edit  View  Go  Capture  Analyze  Statistics  Help

Filter:                                   Expression...  Clear  Apply

No. -  Time       Source           Destination      Protocol  Info
    1  0.000000   192.168.2.145    128.119.245.12   TCP       1250 > http [SYN] Seq=0 Len=0 MSS=1460
    2  0.046402   128.119.245.12   192.168.2.145    TCP       http > 1250 [SYN, ACK] Seq=0 Ack=1 Win=5840
    3  0.046524   192.168.2.145    128.119.245.12   TCP       1250 > http [ACK] Seq=1 Ack=1 Win=65535 [TC
    4  0.046963   192.168.2.145    128.119.245.12   HTTP      POST /ethereal-labs/lab3-1-reply.htm HTTP/1
    5  0.047339   192.168.2.145    128.119.245.12   HTTP      Continuation or non-HTTP traffic
    6  0.128451   128.119.245.12   192.168.2.145    TCP       http > 1250 [ACK] Seq=1 Ack=514 Win=6432 Le
    7  0.128619   192.168.2.145    128.119.245.12   HTTP      Continuation or non-HTTP traffic
    8  0.128717   192.168.2.145    128.119.245.12   HTTP      Continuation or non-HTTP traffic
    9  0.214161   128.119.245.12   192.168.2.145    TCP       http > 1250 [ACK] Seq=1 Ack=1966 Win=8712 L
   10  0.214313   192.168.2.145    128.119.245.12   HTTP      Continuation or non-HTTP traffic
   11  0.214415   192.168.2.145    128.119.245.12   HTTP      Continuation or non-HTTP traffic
   12  0.298180   128.119.245.12   192.168.2.145    TCP       http > 1250 [ACK] Seq=1 Ack=3418 Win=11616
   13  0.298326   192.168.2.145    128.119.245.12   HTTP      Continuation or non-HTTP traffic
   14  0.381927   128.119.245.12   192.168.2.145    TCP       http > 1250 [ACK] Seq=1 Ack=4870 Win=14520
   15  0.382241   192.168.2.145    128.119.245.12   HTTP      Continuation or non-HTTP traffic
   16  0.382377   192.168.2.145    128.119.245.12   HTTP      Continuation or non-HTTP traffic
   17  0.382459   192.168.2.145    128.119.245.12   HTTP      Continuation or non-HTTP traffic
   18  0.421386   192.168.2.102    192.168.2.255    NBNS      Name query NB MSHOME<1b>
   19  0.466467   128.119.245.12   192.168.2.145    TCP       http > 1250 [ACK] Seq=1 Ack=6322 Win=17424
   20  0.552453   128.119.245.12   192.168.2.145    TCP       http > 1250 [ACK] Seq=1 Ack=7774 Win=20328
   21  0.624375   128.119.245.12   192.168.2.145    TCP       http > 1250 [ACK] Seq=1 Ack=8957 Win=23232
   22  0.624707   192.168.2.145    128.119.245.12   HTTP      Continuation or non-HTTP traffic
   23  0.624857   192.168.2.145    128.119.245.12   HTTP      Continuation or non-HTTP traffic
   24  0.624943   192.168.2.145    128.119.245.12   HTTP      Continuation or non-HTTP traffic
   25  0.708403   128.119.245.12   192.168.2.145    TCP       http > 1250 [ACK] Seq=1 Ack=10409 Win=26136
   26  0.794139   128.119.245.12   192.168.2.145    TCP       http > 1250 [ACK] Seq=1 Ack=11861 Win=29040
   27  0.866343   128.119.245.12   192.168.2.145    TCP       http > 1250 [ACK] Seq=1 Ack=13053 Win=31944
   28  0.868855   192.168.2.145    128.119.245.12   HTTP      Continuation or non-HTTP traffic
   29  0.869431   192.168.2.145    128.119.245.12   HTTP      Continuation or non-HTTP traffic
   30  0.869544   192.168.2.145    128.119.245.12   HTTP      Continuation or non-HTTP traffic
   31  0.950346   128.119.245.12   192.168.2.145    TCP       http > 1250 [ACK] Seq=1 Ack=14505 Win=32767
   32  1.036229   128.119.245.12   192.168.2.145    TCP       http > 1250 [ACK] Seq=1 Ack=15957 Win=32767
   33  1.108269   128.119.245.12   192.168.2.145    TCP       http > 1250 [ACK] Seq=1 Ack=17149 Win=32767

⊞ Frame 1 (62 bytes on wire, 62 bytes captured)
⊞ Ethernet II, Src: Netgear_61:8e:6d (00:09:5b:61:8e:6d), Dst: LinksysG_45:90:a8 (00:0c:41:45:90:a8)
⊞ Internet Protocol, Src: 192.168.2.145 (192.168.2.145), Dst: 128.119.245.12 (128.119.245.12)
⊞ Transmission Control Protocol, Src Port: 1250 (1250), Dst Port: http (80), Seq: 0, Len: 0

0000  00 0c 41 45 90 a8 00 09  5b 61 8e 6d 08 00 45 00   ..AE.... [a.m..E.
0010  00 30 7b 6b 40 00 80 06  06 0f c0 a8 02 91 80 77   .0{k@... .......w
0020  f5 0c 04 e2 00 50 c2 67  22 99 00 00 00 00 70 02   .....P.g "......p.
0030  ff ff 60 2f 00 00 02 04  05 b4 01 01 04 02         ..`/.... ......

File: "C:\DOCUME~1\PAULAW~1\LOCALS~1\Temp\etherXXXXa03100" 165 KB 00:00:09   P: 214 D: 214 M: 0 Drops: 0
```

Packet details box

When we select a packet in the capture window, we can see the packet details in the packet details box. When we press on the protocol, it will create a tree which has all the information about The packet

# Exercise

1. What is the IP address and TCP port number used by the client computer (source) that is transferring the file to gaia.cs.umass.edu? To answer this question, it's probably easiest to select an HTTP message and explore the details of the TCP packet used to carry this HTTP message, using the "details of the selected packet header window" (refer to Figure 2 in the "Getting Started with Wireshark" Lab if you're uncertain about the Wireshark windows.

2. What is the IP address of gaia.cs.umass.edu? On what port number is it sending and receiving TCP segments for this connection?

3. What is the IP address and TCP port number used by your client computer (source) to transfer the file to gaia.cs.umass.edu?

# Exercise

- 4. What is the sequence number of the TCP SYN segment that is used to initiate the TCP connection between the client computer and gaia.cs.umass.edu? What is it in the segment that identifies the segment as a SYN segment?
- 5. What is the sequence number of the SYNACK segment sent by gaia.cs.umass.edu to the client computer in reply to the SYN? What is the value of the ACKnowledgement field in the SYNACK segment? How did gaia.cs.umass.edu determine that value? What is it in the segment that identifies the segment as a SYNACK segment?
- 6. What is the sequence number of the TCP segment containing the HTTP POST command? Note that in order to find the POST command, you'll need to dig into the packet content field at the bottom of the Wireshark window, looking for a segment with a "POST" within its DATA field.

# Exercise

7. Consider the TCP segment containing the HTTP POST as the first segment in the TCP connection. What are the sequence numbers of the first six segments in the TCP connection (including the segment containing the HTTP POST)? At what time was each segment sent? When was the ACK for each segment received?

8. What is the length of each of the first six TCP segments?

9. What is the minimum amount of available buffer space advertised at the received for the entire trace? Does the lack of receiver buffer space ever throttle the sender?

10. Are there any retransmitted segments in the trace file? What did you check for (in the trace) in order to answer this question?

# Exercise

11. How much data does the receiver typically acknowledge in an ACK? Can you identify cases where the receiver is ACKing every other received segment.

12. What is the throughput (bytes transferred per unit time) for the TCP connection? Explain how you calculated this value.