# Wireshark:
# Network Packet Analyzer

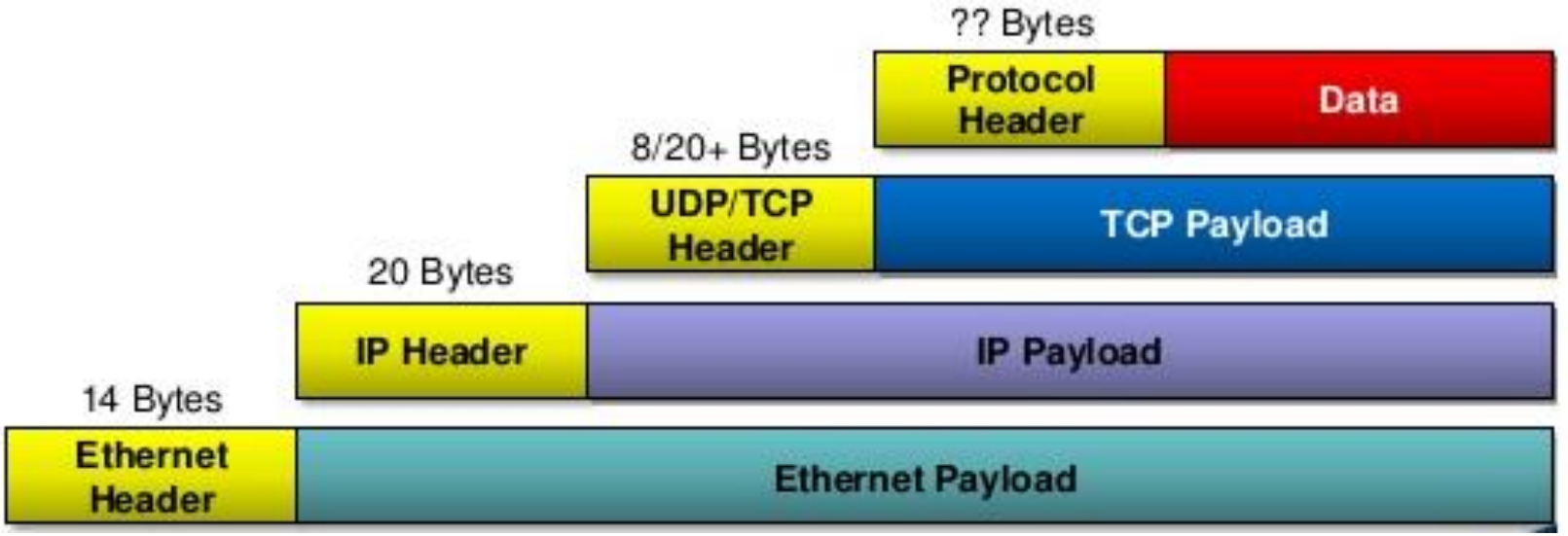
TA: Awad A Younis

Class: CS457

Fall 2014

# ❖Network Protocols (Packets) Have Headers

- Who sent the data
- Who Receives the data
- Information about the payload
- Other protocol specific information



## ❖What is Wireshark?

- Wireshark is a network packet analyzer.
- An open source
- Capture network packets and tries to display that packet data as detailed as possible.

## ❖Why Wireshark?

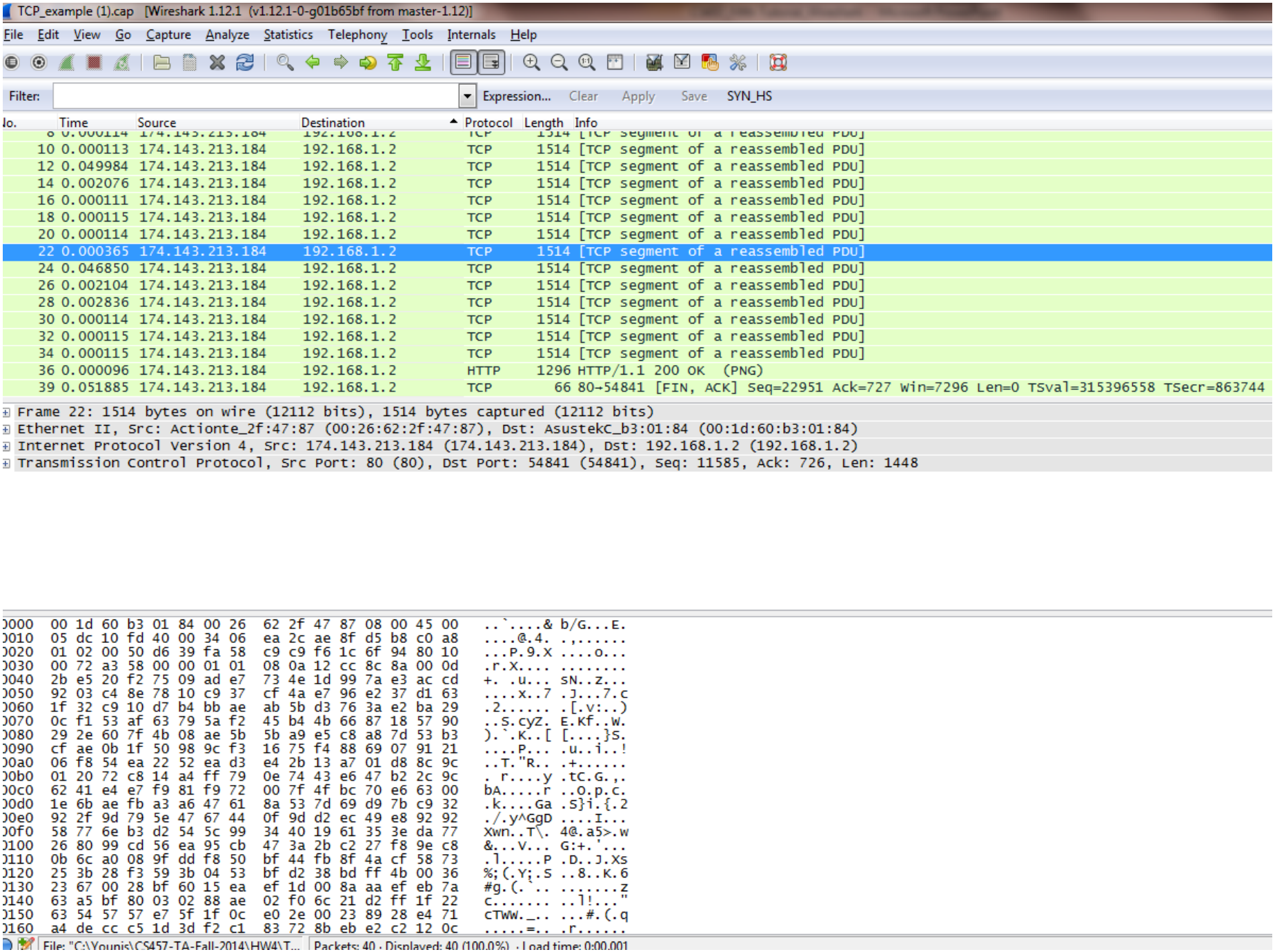
- Network administrators use it to **troubleshoot** network problems
- Network security engineers use it to **examine** security problems
- Developers use it to **debug** protocol implementations
- **People use it to learn network protocol internals**

## ❖What Wireshark is not?

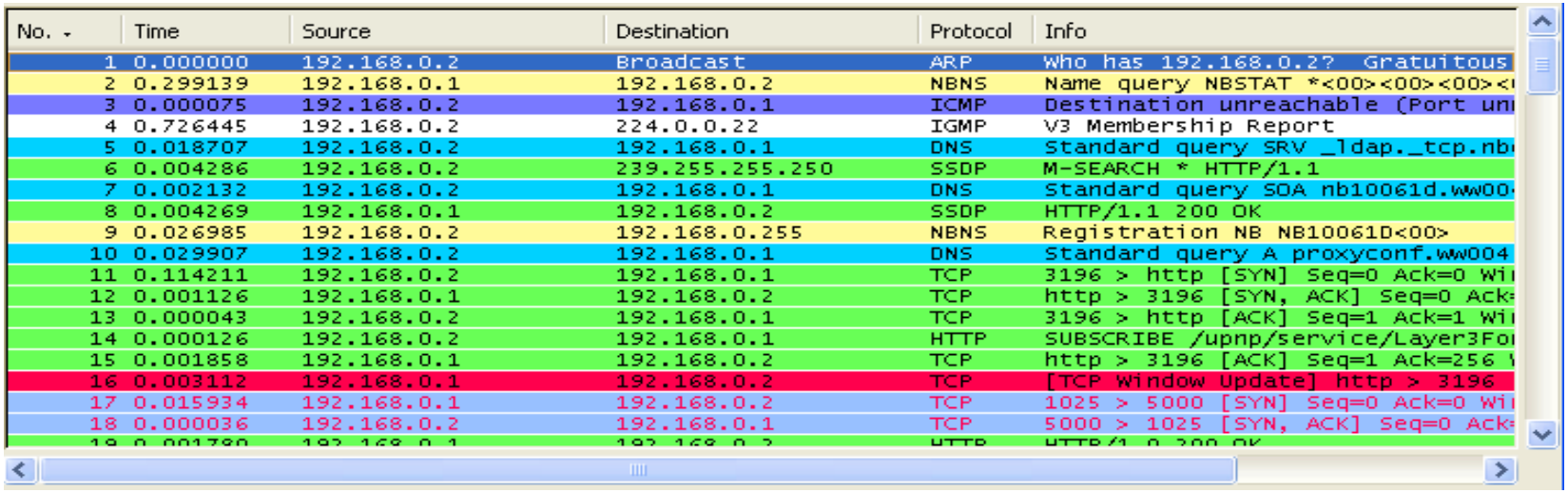
- Wireshark **isn't an intrusion detection** system
- However, if strange things happen, Wireshark might help you figure out what is really going on.
- Wireshark **will not manipulate things on the network**, it will only "**measure**" things from it.

## • Where to get Wireshark

- You can get the latest copy of the program from the Wireshark website at https://www.wireshark.org/download.html.
- The download page should **automatically** highlight the appropriate download for your **platform** and direct you to the nearest mirror.


TCP_example (1).cap [Wireshark 1.12.1 (v1.12.1-0-g01b65bf from master-1.12)]
File Edit View Go Capture Analyze Statistics Telephony Tools Internals Help
Filter: Expression... Clear Apply Save SYN_HS
No. Time Source Destination Protocol Length Info
10 0.000113 174.143.213.184 192.168.1.2 TCP 1514 [TCP segment of a reassembled PDU]
12 0.049984 174.143.213.184 192.168.1.2 TCP 1514 [TCP segment of a reassembled PDU]
14 0.002076 174.143.213.184 192.168.1.2 TCP 1514 [TCP segment of a reassembled PDU]
16 0.000111 174.143.213.184 192.168.1.2 TCP 1514 [TCP segment of a reassembled PDU]
18 0.000115 174.143.213.184 192.168.1.2 TCP 1514 [TCP segment of a reassembled PDU]
20 0.000114 174.143.213.184 192.168.1.2 TCP 1514 [TCP segment of a reassembled PDU]
22 0.000365 174.143.213.184 192.168.1.2 TCP 1514 [TCP segment of a reassembled PDU]
24 0.046850 174.143.213.184 192.168.1.2 TCP 1514 [TCP segment of a reassembled PDU]
26 0.002104 174.143.213.184 192.168.1.2 TCP 1514 [TCP segment of a reassembled PDU]
28 0.002836 174.143.213.184 192.168.1.2 TCP 1514 [TCP segment of a reassembled PDU]
30 0.000114 174.143.213.184 192.168.1.2 TCP 1514 [TCP segment of a reassembled PDU]
32 0.000115 174.143.213.184 192.168.1.2 TCP 1514 [TCP segment of a reassembled PDU]
34 0.000115 174.143.213.184 192.168.1.2 TCP 1514 [TCP segment of a reassembled PDU]
36 0.000096 174.143.213.184 192.168.1.2 HTTP 1296 HTTP/1.1 200 OK (PNG)
39 0.051885 174.143.213.184 192.168.1.2 TCP 66 80→54841 [FIN, ACK] Seq=22951 Ack=727 Win=7296 Len=0 TSval=315396558 TSecr=863744
Frame 22: 1514 bytes on wire (12112 bits), 1514 bytes captured (12112 bits)
Ethernet II, Src: Actionte_2f:47:87 (00:26:62:2f:47:87), Dst: AsustekC_b3:01:84 (00:1d:60:b3:01:84)
Internet Protocol Version 4, Src: 174.143.213.184 (174.143.213.184), Dst: 192.168.1.2 (192.168.1.2)
Transmission Control Protocol, Src Port: 80 (80), Dst Port: 54841 (54841), Seq: 11585, Ack: 726, Len: 1448
0000 00 1d 60 b3 01 84 00 26 62 2f 47 87 08 00 45 00 ..`....& b/G...E.
0010 05 dc 10 fd 40 00 34 06 ea 2c ae 8f d5 b8 c0 a8 ....@.4. .,......
0020 01 02 00 50 d6 39 fa 58 c9 c9 f6 1c 6f 94 80 10 ...P.9.X ....o...
0030 00 72 a3 58 00 00 01 01 08 0a 12 cc 8c 8a 00 0d .r.X.... ........
0040 2b e5 20 f2 75 09 ad e7 73 4e 1d 99 7a e3 ac cd +. .u... sN..z...
0050 92 03 c4 8e 78 10 c9 37 cf 4a e7 96 e2 37 d1 63 ....x..7 .J...7.c
0060 1f 32 c9 10 d7 b4 bb ae ab 5b d3 76 3a e2 ba 29 .2...... .[.v:..)
0070 0c f1 53 af 63 79 5a f2 45 b4 4b 66 87 18 57 90 ..S.cyZ. E.Kf..W.
0080 29 2e 60 7f 4b 08 ae 5b 5b a9 e5 c8 a8 7d 53 b3 ).`.K..[ [....}S.
0090 cf ae 0b 1f 50 98 9c f3 16 75 f4 88 69 07 91 21 ....P... .u..i..!
00a0 06 f8 54 ea 22 52 ea d3 e4 2b 13 a7 01 d8 8c 9c ..T."R.. .+......
00b0 01 20 72 c8 14 a4 ff 79 0e 74 43 e6 47 b2 2c 9c . r....y .tC.G.,.
00c0 62 41 e4 e7 f9 81 f9 72 00 7f 4f bc 70 e6 63 00 bA.....r ..O.p.c.
00d0 1e 6b ae fb a3 a6 47 61 8a 53 7d 69 d9 7b c9 32 .k....Ga .S}i.{.2
00e0 92 2f 9d 79 5e 47 67 44 0f 9d d2 ec 49 e8 92 92 ./.y^GgD ....I...
00f0 58 77 6e b3 d2 54 5c 99 34 40 19 61 35 3e da 77 Xwn..T\. 4@.a5>.w
0100 26 80 99 cd 56 ea 95 cb 47 3a 2b c2 27 f8 9e c8 &...V... G:+.'...
0110 0b 6c a0 08 9f dd f8 50 bf 44 fb 8f 4a cf 58 73 .l.....P .D..J.Xs
0120 25 3b 28 f3 59 3b 04 53 bf d2 38 bd ff 4b 00 36 %;(.Y;.S ..8..K.6
0130 23 67 00 28 bf 60 15 ea ef 1d 00 8a aa ef eb 7a #g.(.`.. .......z
0140 63 a5 bf 80 03 02 88 ae 02 f0 6c 21 d2 ff 1f 22 c....... ..l!..."
0150 63 54 57 57 e7 5f 1f 0c e0 2e 00 23 89 28 e4 71 cTWW._.. ...#.(.q
0160 a4 de cc c5 1d 3d f2 c1 83 72 8b eb e2 c2 12 0c .....=.. .r......
File: "C:\Younis\CS457-TA-Fall-2014\HW4\T... Packets: 40 · Displayed: 40 (100.0%) · Load time: 0:00.001

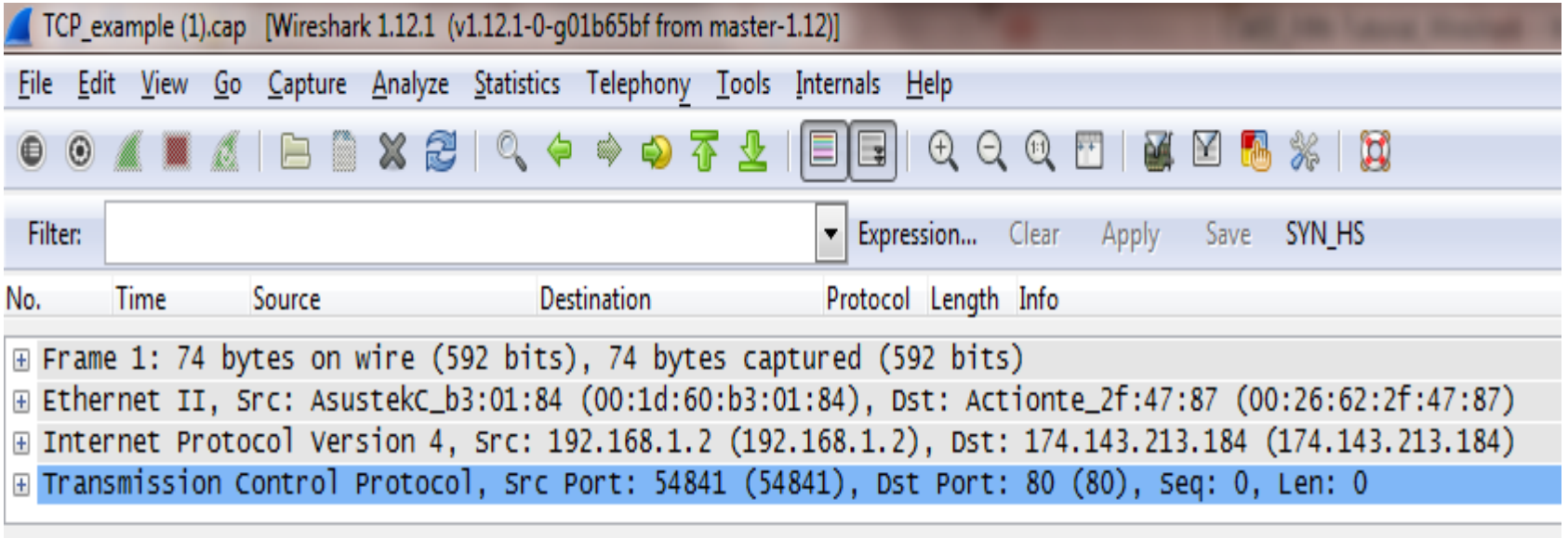
# ❖ Packet List



| No. | Time | Source | Destination | Protocol | Info |
|---|---|---|---|---|---|
| 1 | 0.000000 | 192.168.0.2 | Broadcast | ARP | Who has 192.168.0.2? Gratuitous |
| 2 | 0.299139 | 192.168.0.1 | 192.168.0.2 | NBNS | Name query NBSTAT *<00><00><00><( |
| 3 | 0.000075 | 192.168.0.2 | 192.168.0.1 | ICMP | Destination unreachable (Port un |
| 4 | 0.726445 | 192.168.0.2 | 224.0.0.22 | IGMP | V3 Membership Report |
| 5 | 0.018707 | 192.168.0.2 | 192.168.0.1 | DNS | Standard query SRV _ldap._tcp.nb |
| 6 | 0.004286 | 192.168.0.2 | 239.255.255.250 | SSDP | M-SEARCH * HTTP/1.1 |
| 7 | 0.002132 | 192.168.0.2 | 192.168.0.1 | DNS | Standard query SOA nb10061d.ww00 |
| 8 | 0.004269 | 192.168.0.1 | 192.168.0.2 | SSDP | HTTP/1.1 200 OK |
| 9 | 0.026985 | 192.168.0.2 | 192.168.0.255 | NBNS | Registration NB NB10061D<00> |
| 10 | 0.029907 | 192.168.0.2 | 192.168.0.1 | DNS | Standard query A proxyconf.ww004 |
| 11 | 0.114211 | 192.168.0.2 | 192.168.0.1 | TCP | 3196 > http [SYN] Seq=0 Ack=0 Wi |
| 12 | 0.001126 | 192.168.0.1 | 192.168.0.2 | TCP | http > 3196 [SYN, ACK] Seq=0 Ack |
| 13 | 0.000043 | 192.168.0.2 | 192.168.0.1 | TCP | 3196 > http [ACK] Seq=1 Ack=1 Wi |
| 14 | 0.000126 | 192.168.0.2 | 192.168.0.1 | HTTP | SUBSCRIBE /upnp/service/Layer3Fo |
| 15 | 0.001858 | 192.168.0.1 | 192.168.0.2 | TCP | http > 3196 [ACK] Seq=1 Ack=256 |
| 16 | 0.003112 | 192.168.0.1 | 192.168.0.2 | TCP | [TCP Window Update] http > 3196 |
| 17 | 0.015934 | 192.168.0.1 | 192.168.0.2 | TCP | 1025 > 5000 [SYN] Seq=0 Ack=0 Wi |
| 18 | 0.000036 | 192.168.0.2 | 192.168.0.1 | TCP | 5000 > 1025 [SYN, ACK] Seq=0 Ack |

- **No**: The number of the packet in the capture file. This number won't change, even if a display filter is used.
- **Time:** The timestamp of the packet. The presentation format of this timestamp can be changed, see Section 6.12, "Time display formats and time references".
- **Source:** The address where this packet is coming from.
- **Destination:** The address where this packet is going to.
- **Protocol:** The protocol name in a short (perhaps abbreviated) version.
- **Info:** Additional information about the packet content.

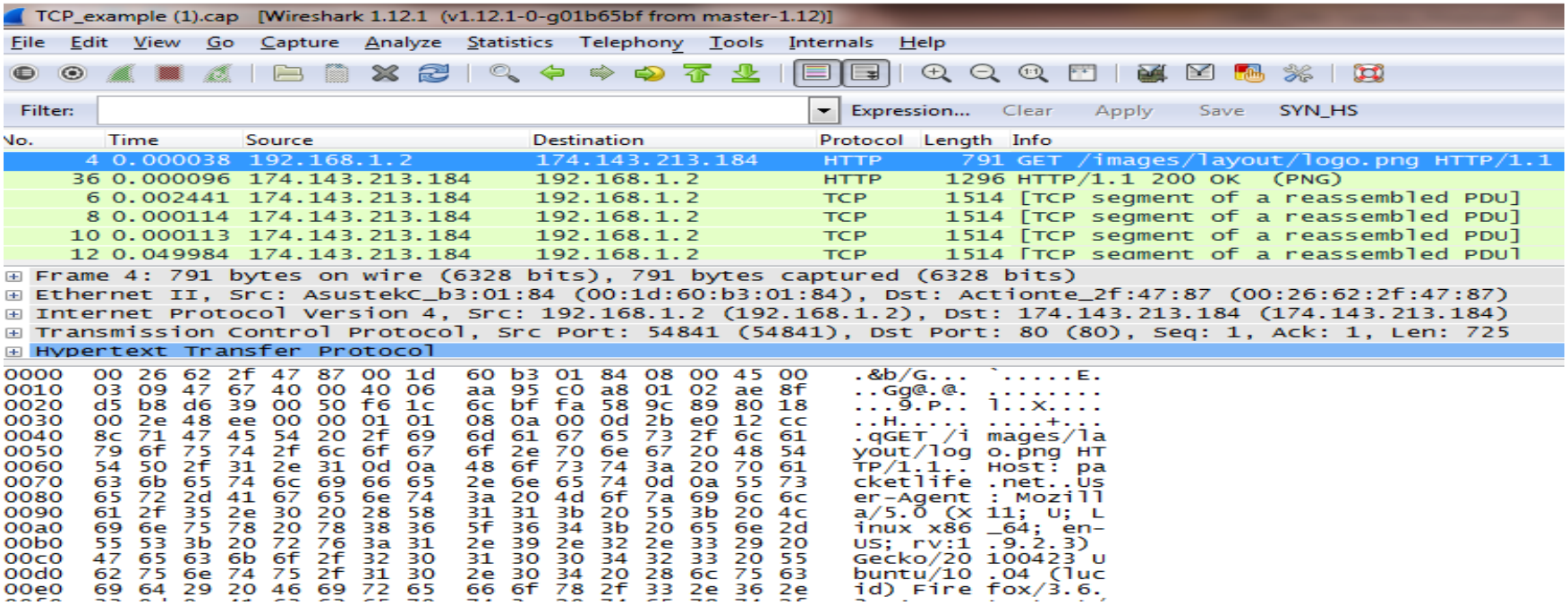
# ❖ Packet Details




- This shows the protocols and protocol fields of the packet selected in the “Packet List” pane.
- The protocols and fields of the packet are displayed using a tree, which can be expanded and collapsed.

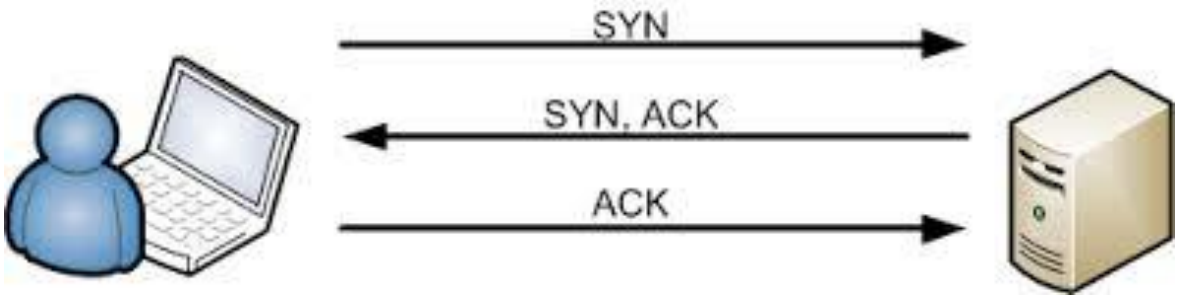
1. **Frame**
2. **Data Link:** EN
3. **Network:** IP
4. **Transport:** TCP
5. **Data:** Payload

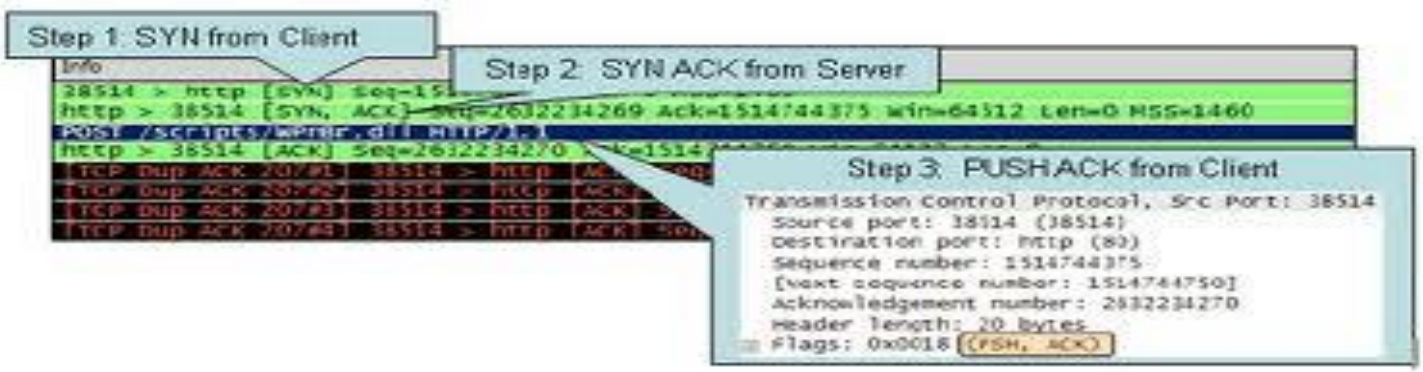
# ❖ Packet Bytes




- The packet bytes pane shows the data of the current packet (selected in the “Packet List” pane) in a hexdump style
- As usual for a hexdump,
  - the **left** side shows the **offset** in the packet data,
  - in the **middle** the packet data is shown in a **hexadecimal** representation
  - and on the **right** the corresponding **ASCII** characters

# ❖Three way TCP Handshake



# Thank You