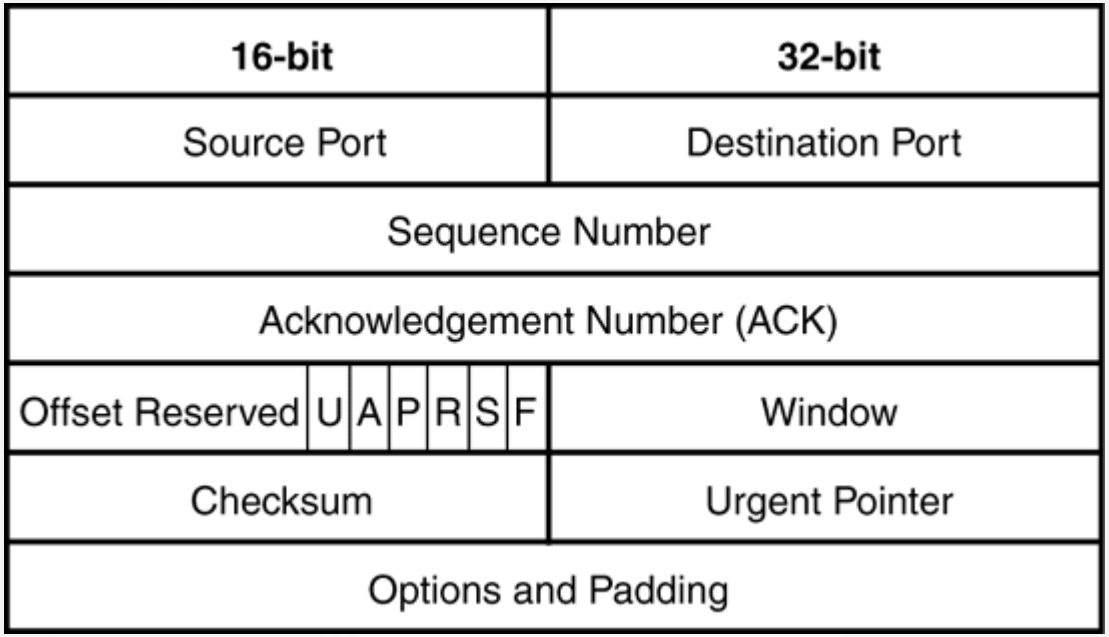
Advanced TCP Analysis

Advanced TCP Analysis

- Understanding and working with the TCP header
- What is the Transport Control Protocol (TCP)?
  - Layer 4
  - Connection establishment
  - Others
- Wireshark analysis
  - What can you find in the TCP header?

Advanced TCP Analysis



Advanced TCP Analysis

```
Transmission Control Protocol, Src Port: 53298 (53298), Dst Port: 2034 (2034), Seq: 1, Ack: 94, Len: 0
  Source Port: 53298 (53298)
  Destination Port: 2034 (2034)
  [Stream index: 0]
  [TCP Segment Len: 0]
  Sequence number: 1    (relative sequence number)
  Acknowledgment number: 94    (relative ack number)
  Header Length: 20 bytes
  .... 0000 0001 0000 = Flags: 0x010 (ACK)
    000. .... .... = Reserved: Not set
    ...0 .... .... = Nonce: Not set
    .... 0... .... = Congestion Window Reduced (CWR): Not set
    .... .0.. .... = ECN-Echo: Not set
    .... ..0. .... = Urgent: Not set
    .... ...1 .... = Acknowledgment: Set
    .... .... 0... = Push: Not set
    .... .... .0.. = Reset: Not set
    .... .... ..0. = Syn: Not set
    .... .... ...0 = Fin: Not set
  Window size value: 1351
  [Calculated window size: 1351]
  [Window size scaling factor: -1 (unknown)]
  Checksum: 0x19d7 [incorrect, should be 0x3f97 (maybe caused by "TCP checksum offload"?)]
  Urgent pointer: 0
  [SEQ/ACK analysis]
    [This is an ACK to the segment in frame: 13]
    [The RTT to ACK the segment was: 0.208766000 seconds]
```

Questions?