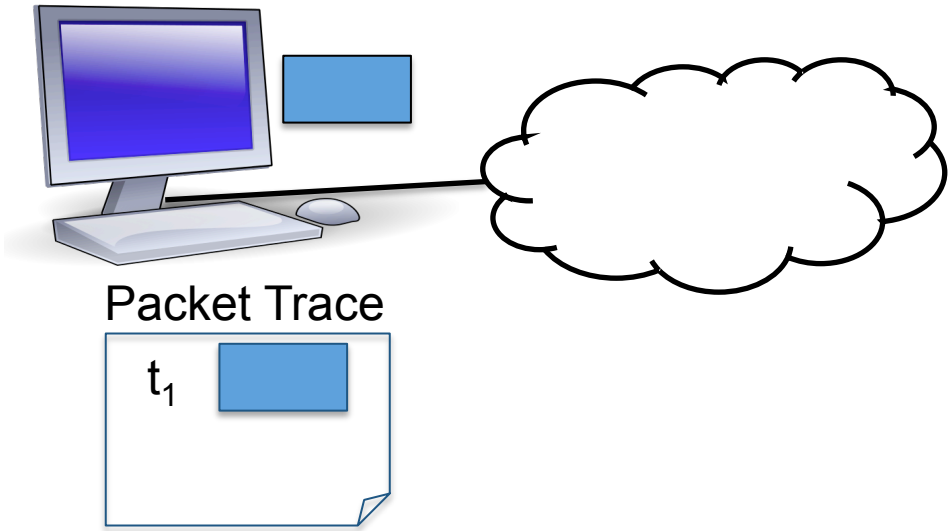
Week 5: Traffic measurements

1. Introduction
2. **Packet capture**
   A. **End systems**
   B. Network
3. Interface counts
4. Flow capture
5. Traffic matrix
6. Anonymization of packet traces
7. Conclusion

Packet capture on end systems

- Basic method
  - Capture and record packets passing through an interface



Tools

- tcpdump
  - Command-line packet capture
- libpcap
  - C/C++ library for packet capture
- Wireshark
  - Packet capture and analysis

Parameters: monitored interfaces

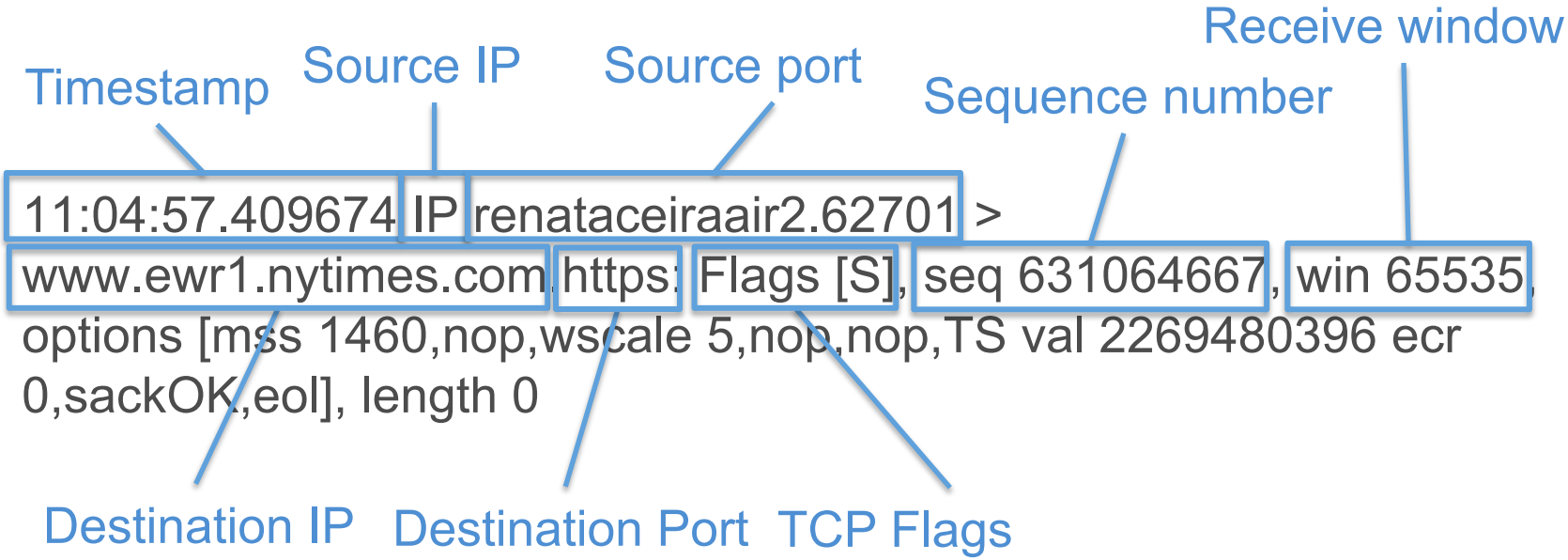
- Example
  - `tcpdump -i eth0`



Parameters: packet filters

- Packets to collect
  - E.g., TCP port 80 packets or packets to a given IP address
- Part of packets
  - E.g., IP/TCP headers

Example output: tcpdump



Possible measurement artifacts

- Dropped packets are common under high utilization
  - Inspect report of dropped packets
- Other less frequent artifacts
  - Fail to report drops
  - Falsely report drops
  - Duplicate packets
  - Re-ordered packets
  - Misfilter

Picture credits

- Slides 2 & 4: **Desktop computer clip art** by OpenClipArt.org (public domain)
- Slide 4: **WIFI icon** by Canopus49, https://commons.wikimedia.org/wiki/File:WIFI_icon.svg (CC BY-SA 3.0)