Wireshark 101

Ravi Bhoraskar

(Slides borrowed/stolen generously from all over the internet)

Network Interfaces

- Linux box:
  - Show interfaces by “ifconfig”
  - Windows: “ipconfig /a” (I think)

- Look at routing table by running “netstat -r”
  - IP addresses are 32 bits
  - Network number, IP within the network
  - Next hop determined by longest prefix match on the IP address

Wireshark

- World's most popular and complete protocol analyzer
- Wireshark is free software, and is available for Linux, Mac and Windows.
- More than 10 million downloads at SourceForge so far.

What is wireshark?

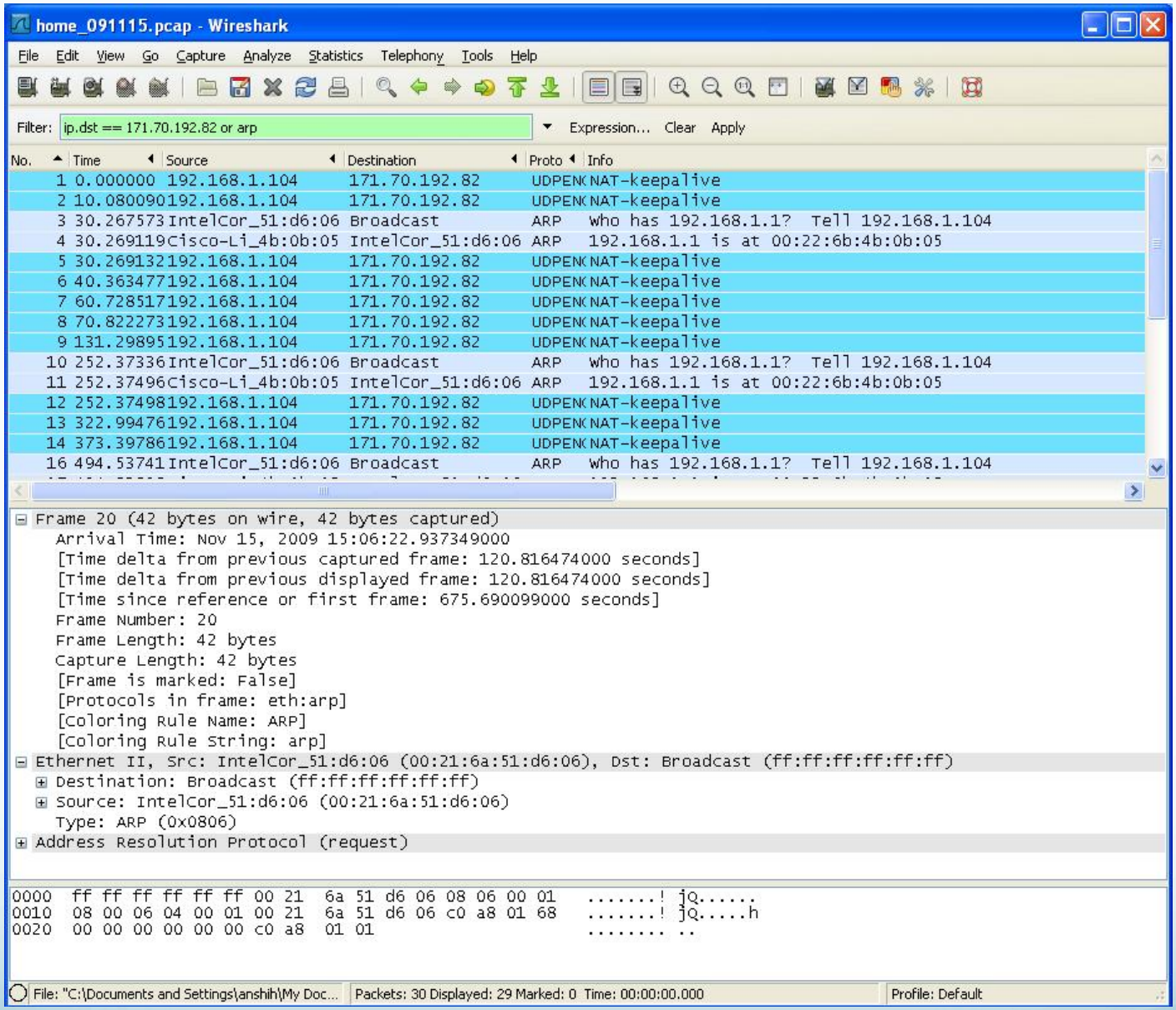
- Wireshark is a **protocol analyzer.**
- This means Wireshark is designed to decode not only packet bits and bytes but also the relations between packets and protocols.
- Wireshark understands protocol sequences.

What is Wireshark for YOU?

- Tool for examining packets on the ethernet/wireless mediums
- Need superuser access on machine
- Allows you to examine packets – all of them!
- Too much data, so you can employ filters
- Simplest case: just specify interface to snoop on

Demo 1 – Basic Run

- Run wireshark on en1



Wireshark Trace Example: What do these mean?

Filters

- We are often not interested in all packets flowing through the network
- Use filters to capture only packets of interest to us
- Two kind of filters
  - Capture Filter: Filtered while capturing. Like TCPDump
  - Display Filter: More detailed filtering. Allows to compare values in packets. Not real time

Demo 2

1. Capture only udp packets
   - Capture filter = “udp”
2. Capture only tcp packets
   - Capture filter = “tcp”

Demo 2 (contd.)

1. Capture only UDP packets with destination port 53 (DNS requests)
   - “udp dst port 53”
2. Capture only UDP packets with source port 53 (DNS replies)
   - “udp src port 53”
3. Capture only UDP packets with source or destination port 53 (DNS requests and replies)
   - “udp port 53”

Demo 2 (contd.)

1. Capture only packets destined to www.cs.washington.edu
   - "dst host www.cs.washington.edu"
2. Capture both DNS packets and TCP packets to/from www.cs.washington.edu
   - "(tcp and host www.cs.washington.edu) or udp port 53"

Display Filters

- Different Syntax
  - frame.len > 10
  - ip.addr == 129.111.0.0/16 [CIDR masking]
- More expressive
  - eth.src[1–2] == 00:83 [Check only bytes 1 and 2]
- Go crazy with logical expressions
  - tcp.dst[0:3] == 0.6.29 xor udp.src[1] == 42

How to write filters

- Refer cheat sheet slides at the end of this presentation
- Refer the tcpdump man page and wireshark documentation

Other tools

- TCPDump
  - Command line based [for the geeks in you!]
- IPsumdump
  - Summarize tcpdump output into human/machine readable form
  - http://www.cs.ucla.edu/~kohler/ipsumdump/
  - For instructions to use IPsumdump on EECS instructional accounts, see slide “Appendix: IPsumdump on EECS instructional accounts”
- Ethereal
  - ...is now wireshark
- Generally, wireshark is better!

Security/Privacy Issues

- Wireshark allows you to monitor other people's traffic
- WARNING: Do NOT use tcpdump to violate privacy or security
- Use filtering to restrict packet analysis to only the traffic associated with your program. The following is one way to ensure that you see only traffic associated with your client:
  - tcpdump –s 0 –r all_pkts.trace " –w my_pkts.trace "port 12345"
  - where 12345 is the ephemeral port which your echo_client uses to talk to the echo_server.

Cheat Sheet – Writing Filters (1)

- Specifying the hosts we are interested in
  - “dst host <name/IP>”
  - “src host <name/IP>”
  - “host <name/IP>” (either source or destination is name/IP)
- Specifying the ports we are interested in
  - “dst port <number>”
  - “src port <number>”
  - “port <number>”
  - Makes sense only for TCP and UDP packets

Cheat Sheet – Writing Filters (2)

- Specifying ICMP packets
  - “icmp”
- Specifying UDP packets
  - “udp”
- Specifying TCP packets
  - “tcp”

Cheat Sheet – Writing Filters (2)

- Combining filters
  - *and (&&)*
  - *or (||)*
  - *not (!)*
- Example:
  - All tcp packets which are not from or to host quasar.cs.berkeley.edu

    tcpdump "tcp and ! host quasar.cs.berkeley.edu"
  - Lots of examples in the EXAMPLES section of the man page