Playing with IP Capture Files

Who Am I?

- Jim O’Gorman
  - Jameso@elwood.net
  - Jogorman@gmail.com
  - http://www.elwood.net/

What are we going to cover?

- There are many interesting and informative things we can do with full pcap packet captures. We are going to explore some of the tasks one can do with these capture files.

What is a packet sniffer?

- A packet sniffer (also known as a network analyzer or protocol analyzer or, for particular types of networks, an Ethernet sniffer or wireless sniffer) is computer software or computer hardware that can intercept and log traffic passing over a digital network or part of a network. As data streams travel back and forth over the network, the sniffer captures each packet and eventually decodes and analyzes its content according to the appropriate RFC or other specifications. *(http://en.wikipedia.org/wiki/Packet_sniffer)*

What is a packet capture file?

- An “Image” of the data that has been transfered over a network that the packet sniffer was able to access.
- Not all traffic is accessible to a packet sniffer.
- Pcap utilities simply process the image, handling the sequence of the file as if it was sent over the network.

What use is this?

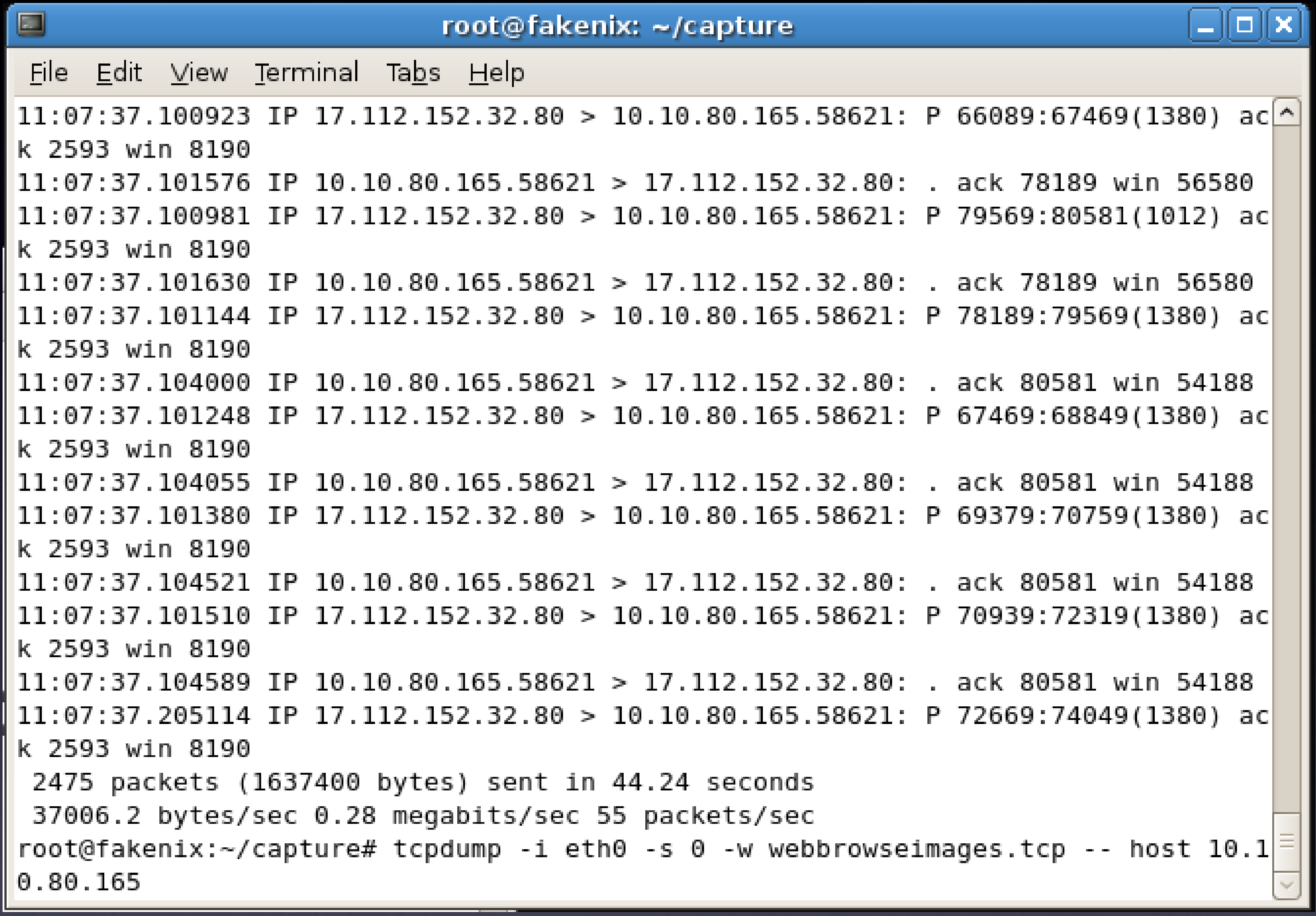
- With a full content network capture, you have a copy of everything that happened on the network.

So how do I get one of these capture files?

- tcpdump -i INTERFACE -s SNAPLEN -w OUTPUTFILE -- BPF Filter
- tcpdump -i fxp0 -s 0 -w outfile.tcp -- ‘ip and host 192.168.1.4’

What is a BPF Filter?

- Best documented in tcpdump(8)
- ex.
  - host 192.168.1.20 and dst port 80
  - net 10.10.20.0/24 and not port 80 and not port 25
  - etc.



```
11:07:37.100923 IP 17.112.152.32.80 > 10.10.80.165.58621: P 66089:67469(1380) ac
k 2593 win 8190
11:07:37.101576 IP 10.10.80.165.58621 > 17.112.152.32.80: . ack 78189 win 56580
11:07:37.100981 IP 17.112.152.32.80 > 10.10.80.165.58621: P 79569:80581(1012) ac
k 2593 win 8190
11:07:37.101630 IP 10.10.80.165.58621 > 17.112.152.32.80: . ack 78189 win 56580
11:07:37.101144 IP 17.112.152.32.80 > 10.10.80.165.58621: P 78189:79569(1380) ac
k 2593 win 8190
11:07:37.104000 IP 10.10.80.165.58621 > 17.112.152.32.80: . ack 80581 win 54188
11:07:37.101248 IP 17.112.152.32.80 > 10.10.80.165.58621: P 67469:68849(1380) ac
k 2593 win 8190
11:07:37.104055 IP 10.10.80.165.58621 > 17.112.152.32.80: . ack 80581 win 54188
11:07:37.101380 IP 17.112.152.32.80 > 10.10.80.165.58621: P 69379:70759(1380) ac
k 2593 win 8190
11:07:37.104521 IP 10.10.80.165.58621 > 17.112.152.32.80: . ack 80581 win 54188
11:07:37.101510 IP 17.112.152.32.80 > 10.10.80.165.58621: P 70939:72319(1380) ac
k 2593 win 8190
11:07:37.104589 IP 10.10.80.165.58621 > 17.112.152.32.80: . ack 80581 win 54188
11:07:37.205114 IP 17.112.152.32.80 > 10.10.80.165.58621: P 72669:74049(1380) ac
k 2593 win 8190
 2475 packets (1637400 bytes) sent in 44.24 seconds
 37006.2 bytes/sec 0.28 megabits/sec 55 packets/sec
root@fakenix:~/capture# tcpdump -i eth0 -s 0 -w webbrowseimages.tcp -- host 10.1
0.80.165
```

I Have My Capture File...

- Now what?

Capture File Overview(1)

- tcpdstat (http://staff.washington.edu/dittrich/talks/co)
    - Produces a per-protocol breakdown of traffic by bytes and packets, with average and maximum transfer rates, for a given libpcap file (e.g., from tcpdump, ethereal, snort, etc.) Useful for getting a high-level view of traffic patterns.

Capture File Overview(2)

- PADS (*http://passive.sourceforge.net/*)
  - PADS is a signature based detection engine used to passively detect network assets. It is designed to complement IDS technology by providing context to IDS alerts.

Make History Repeat

- tcpreplay *(http://tcpreplay.synfin.net/trac/wiki/tcpreplay)*
  - Replays pcap files at arbitrary speeds onto the network.

Session Information (1)

- Argus (http://qosient.com/argus/)
  - Argus is a fixed-model Real Time Flow Monitor designed to track and report on the status and performance of all network transactions seen in a data network traffic stream. Argus provides a common data format for reporting flow metrics such as connectivity, capacity, demand, loss, delay, and jitter on a per transaction basis. The record format that Argus uses is flexible and extensible, supporting generic flow identifiers and metrics, as well as application/protocol specific information.

Session Information (2)

- EtherApe (http://etherape.sourceforge.net/)
  - EtherApe is a graphical network monitor for Unix modeled after etherman. Featuring link layer, ip and TCP modes, it displays network activity graphically. Hosts and links change in size with traffic. Color coded protocols display. It supports Ethernet, FDDI, Token Ring, ISDN, PPP and SLIP devices. It can filter traffic to be shown, and can read traffic from a file as well as live from the network.

Content (1)

- dsniff suite *(http://monkey.org/~dugsong/dsniff/)*
  - dsniff - Decode passwords
  - mailsnarf - Decode SMTP/POP3
  - msgsnarf - Decode IMs
  - urlsnarf - Decode URLs
  - webspy - Watch web surfing

Content (2)

- tcpflow *(http://www.circlemud.org/~jelson/software/tcpflow/)*
  - tcpflow is a program that captures data transmitted as part of TCP connections (flows), and stores the data in a way that is convenient for protocol analysis or debugging. A program like 'tcpdump' shows a summary of packets seen on the wire, but usually doesn't store the data that's actually being transmitted. In contrast, tcpflow reconstructs the actual data streams and stores each flow in a separate file for later analysis.

Content (4)

- Wireshark *(http://www.wireshark.org/)*
  - Wireshark is the world's foremost network protocol analyzer, and is the standard in many industries. It is the continuation of a project that started in 1998. Hundreds of developers around the world have contributed to it, and it is still under active development.
- tshark - Command line.

Content (5)

- Driftnet (http://www.ex-parrot.com/~chris/driftne)
  - Driftnet is a program which listens to network traffic and picks out images from TCP streams it observes. Fun to run on a host which sees lots of web traffic.

SMB Transfers

- Possible to extract files.
  - Some times very difficult.
- Multiplexed transfers complicate it.

Build Your Own Sniffer

- Pcap libraries for various languages
  - http://en.wikipedia.org/wiki/Pcap
- Examples are using Ruby’s pcap library
  - http://www.goto.info.waseda.ac.jp/~fu

WARNING!

- I am brand new to Ruby - My code seems to work, but there are sure to be things done that are “Against the Ruby Way”.
  - I did this on purpose, to show how approachable these Pcap libraries can be.

Mail Sniffers

- POP3 - pop3dump.rb
- SMTP - smtpdump.rb

Questions?