Trace File Analysis

Packet Loss, Retransmissions, Fast Retransmissions, Duplicate ACKs, ACK Lost Segment and Out-of-Order Packets

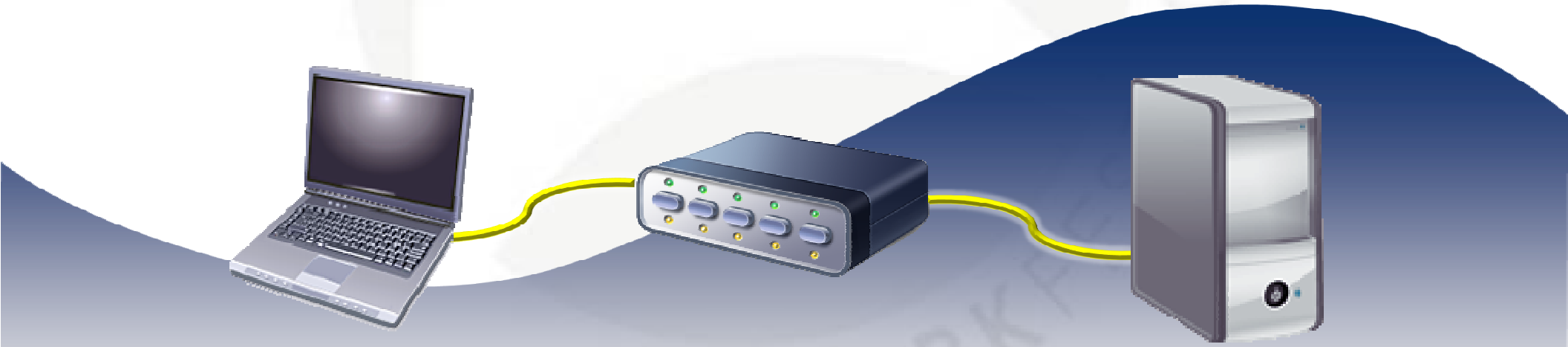
Laura Chappell
Founder | Wireshark University

SHARKFEST **'08**
Foothill College
March 31 - April 2, 2008

Tap-In Points

Tap-in points

- Hub networks: Easy
- Switch networks: Issues
- Routed networks: Issues
- Full-duplex: Issues



Packet Loss – TCP Recovery

SEQ 3000 – 1460 bytes of data; ACK 2000 →

SEQ 4460 – 1460 bytes of data; ACK 2000 →

← SEQ 2000 – 0 bytes of data; ACK 4460

← SEQ 2000 – 0 bytes of data; ACK 5920

SEQ 5920 – 1460 bytes of data; ACK 2000 →

SEQ 8840 – 1460 bytes of data; ACK 2000 →

← SEQ 2000 – 0 bytes of data; ACK 7380 First ACK

← SEQ 2000 – 0 bytes of data; ACK 10300

← SEQ 2000 – 0 bytes of data; ACK 7380 Dupe ACK #1

← SEQ 2000 – 0 bytes of data; ACK 7380 Dupe ACK #2

SEQ 7380– 1460 bytes of data; ACK 2000 →

CACE TECHNOLOGIES

www.wiresharkU.com WIRESHARK UNIVERSITY

IMPORTANT: Where is packet loss occurring?

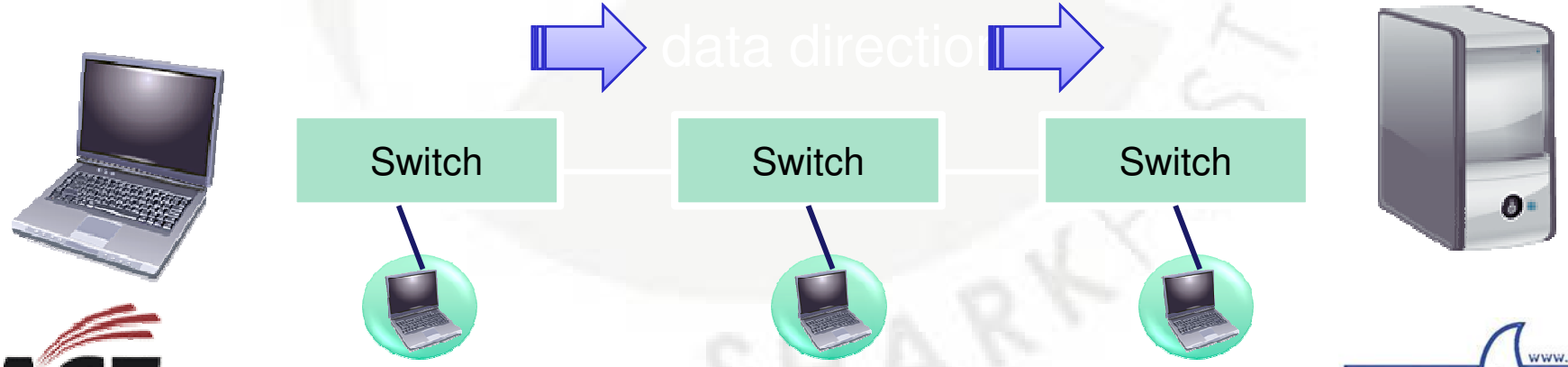
Did you see the original packet as well as the retransmission?

No

Packet loss is occurring upstream from you. Move toward the **source** host.

Yes

Packet loss is occurring downstream from you. Move toward the **destination** host.



CACE TECHNOLOGIES

www.wiresharkU.com
WIRESHARK UNIVERSITY

Packet Loss – Selective ACKs

SEQ 7380 – 1460 bytes of data; ACK 2000

SEQ 10300 – 1460 bytes of data; ACK 2000

SEQ 2000 – ACK 8840; ; SACK LE10300/RE11760 — First SACK

SEQ 2000 – ACK 8840; SACK LE10300/RE11760 — Dupe SACK #1

SEQ 11760 – 1460 bytes of data; ACK 2000

SEQ 2000 – ACK 8840; SACK LE10300/RE13220 — Dupe SACK #2

SEQ 8840 – 1460 bytes of data; ACK 2000

SEQ 2000 – ACK 13220

See download-bad
[pkt 4222]

CACE TECHNOLOGIES

www.wiresharkU.com
WIRESHARK UNIVERSITY

Retransmissions

Expert Note in TCP Dissector

anonsvn.wireshark.org/wireshark/trunk/epan/dissectors/packet-tcp.c

RETRANSMISSION/FAST RETRANSMISSION/OUT-OF-ORDER

> "If the segments contain data and if it does not advance sequence number it must be either of these three. Only test for this if we know what the seq number should be"
>
> (tcpd->fwd->nextseq)

Normal v. Fast Retransmissions

Fast Retransmission

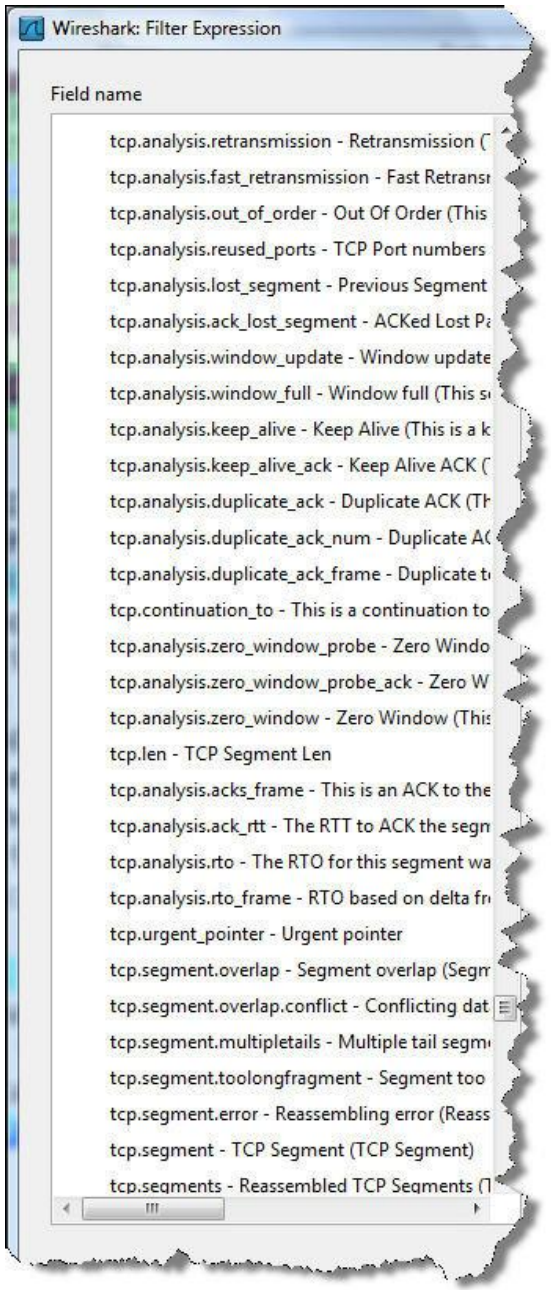
If there were >=2 duplicate ACKs in the reverse direction (there might be duplicate acks missing from the trace) and if this sequence number matches those ACKs and if the packet occurs **within 20ms of the last duplicate ack** then this is a fast retransmission

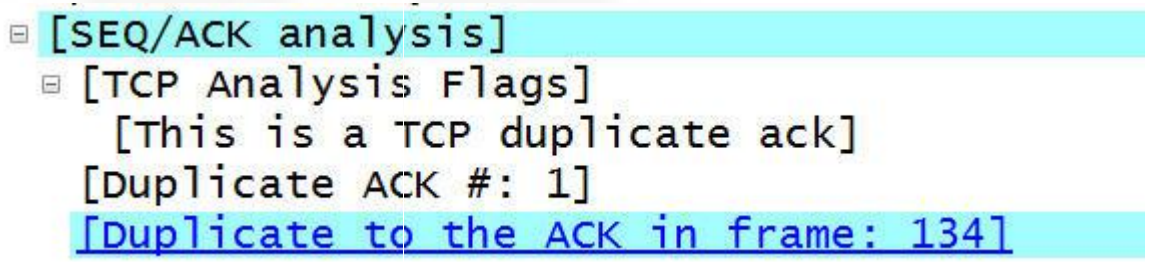
Out-of-Order Segments

"If the segments contain data and if it ***does not advance sequence number*** it must be either of these three"

If the segment came <3ms since the segment with the highest seen sequence number, then it is an OUT-OF-ORDER segment. (3ms is an arbitrary number)

Filter Expressions and IO Graphing





Demo - Graphing:

ftp-faileduplоad.pcap

tcp.analysis.retransmission

tcp.analysis.fast_retransmission

tcp.analysis.duplicate_ack

www.wiresharkU.com
WIRESHARK UNIVERSITY

Lab: Charting

Issue: downloads take too long

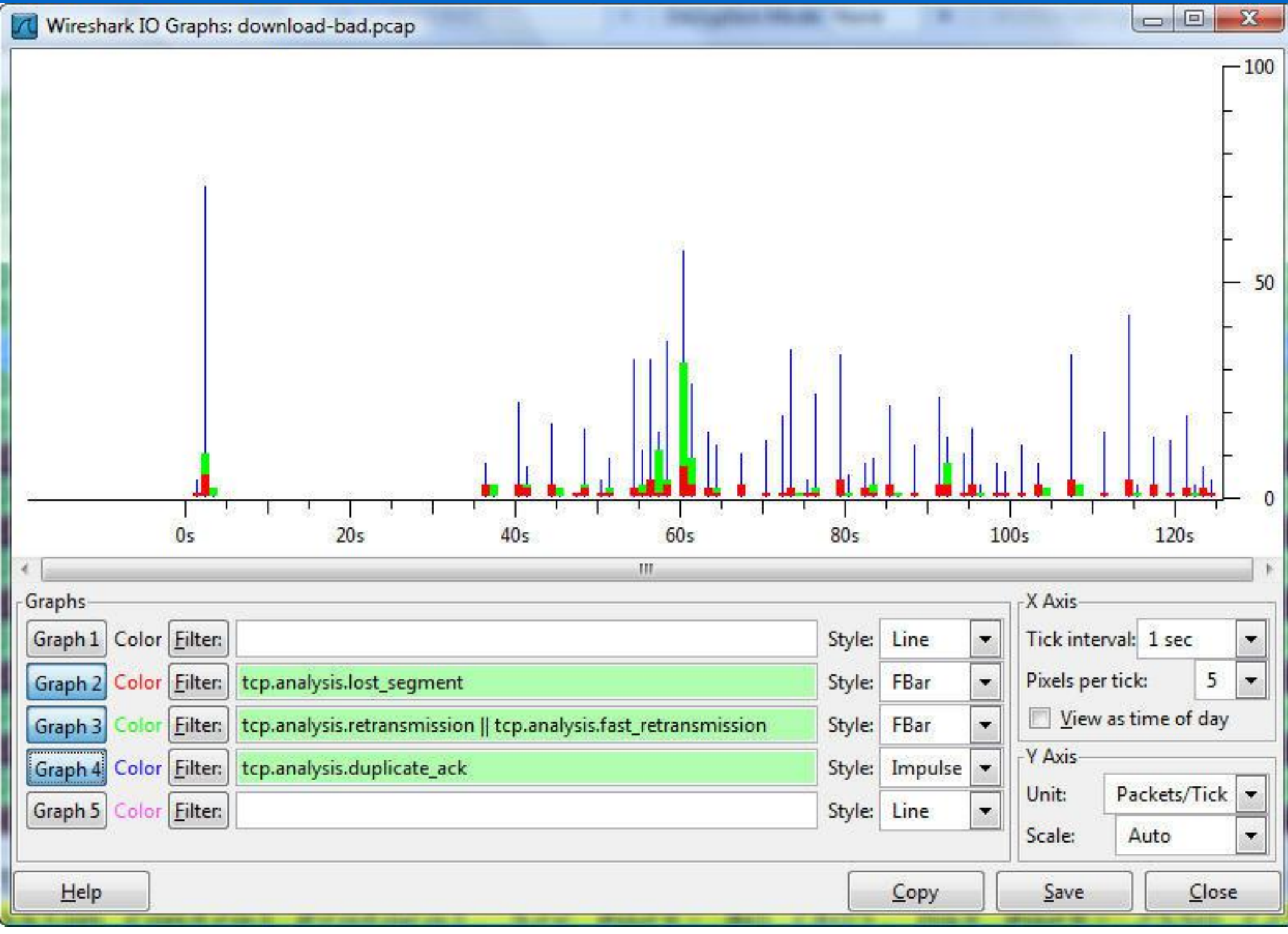
File: download-bad.pcap

Open the trace file and graph the following:

-Red Lost segments (Fbar)

-Green Retransmissions or fast retransmissions (Fbar)

-Blue Duplicate ACKs (Impulse)

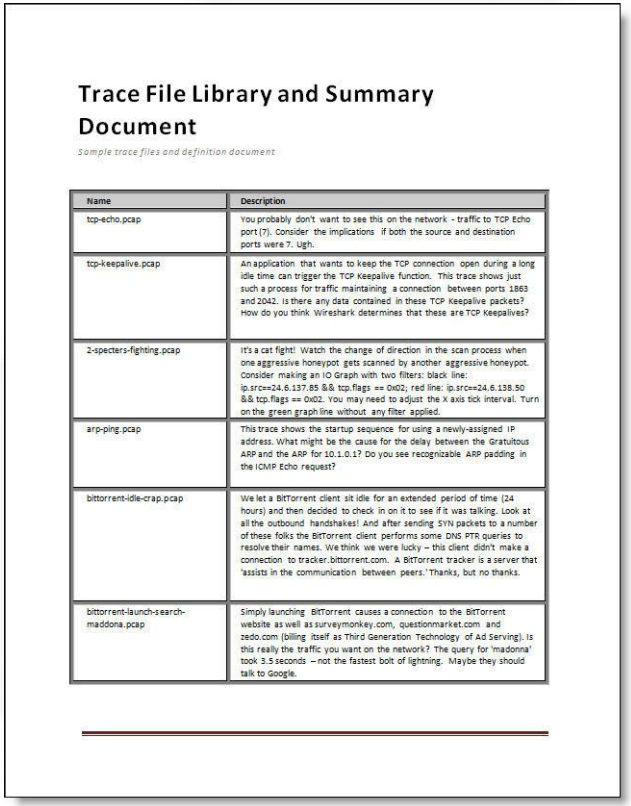

Wireshark IO Graphs: download-bad.pcap
100
50
0
0s
20s
40s
60s
80s
100s
120s
Graphs
Graph 1
Color
Filter:
Style:
Line
Graph 2
Color
Filter:
tcp.analysis.lost_segment
Style:
FBar
Graph 3
Color
Filter:
tcp.analysis.retransmission || tcp.analysis.fast_retransmission
Style:
FBar
Graph 4
Color
Filter:
tcp.analysis.duplicate_ack
Style:
Impulse
Graph 5
Color
Filter:
Style:
Line
X Axis
Tick interval:
1 sec
Pixels per tick:
5
View as time of day
Y Axis
Unit:
Packets/Tick
Scale:
Auto
Help
Copy
Save
Close

What's Next?

Laura's Lab Kit v9

In show bags as well as…

ISO image: www.novell.com/connectionmagazine/laurachappell.html



Trace File Library and Summary Document

Sample trace files and definition document

Name	Description
tcp-echo.pcap	You probably don't want to see this on the network - traffic to TCP Echo port (7). Consider the implications if both the source and destination ports were 7. Ugh.
tcp-keepalive.pcap	An application that wants to keep the TCP connection open during a long idle time can trigger the TCP Keepalive function. This trace shows just such a process for traffic maintaining a connection between ports 1863 and 2042. Is there any data contained in these TCP Keepalive packets? How do you think Wireshark determines that these are TCP Keepalives?
2-specters-fighting.pcap	It's a cat fight! Watch the change of direction in the scan process when one aggressive honeypot gets scanned by another aggressive honeypot. Consider making an IO Graph with two filters: black line: ip.src==24.6.137.85 && tcp.flags == 0x02; red line: ip.src==24.6.138.50 && tcp.flags == 0x02. You may need to adjust the X axis tick interval. Turn on the green graph line without any filter applied.
arp-ping.pcap	This trace shows the startup sequence for using a newly-assigned IP address. What might be the cause for the delay between the Gratuitous ARP and the ARP for 10.1.0.1? Do you see recognizable ARP padding in the ICMP Echo request?
bittorrent-idle-crap.pcap	We let a BitTorrent client sit idle for an extended period of time (24 hours) and then decided to check in on it to see if it was talking. Look at all the outbound handshakes! And after sending SYN packets to a number of these folks the BitTorrent client performs some DNS PTR queries to resolve their names. We think we were lucky – this client didn't make a connection to tracker.bittorrent.com. A BitTorrent tracker is a server that 'assists in the communication between peers.' Thanks, but no thanks.
bittorrent-launch-search-maddona.pcap	Simply launching BitTorrent causes a connection to the BitTorrent website as well as surveymonkey.com, questionmarket.com and zedo.com (billing itself as Third Generation Technology of Ad Serving!). Is this really the traffic you want on the network? The query for 'madonna' took 3.5 seconds – not the fastest bolt of lightning. Maybe they should talk to Google.

CACE TECHNOLOGIES

www.wiresharkU.com WIRESHARK UNIVERSITY