

T2-10: Trace File Analysis - Case Studies: Samples of Wireshark in Action

Laura Chappell

Founder | Wireshark University

Betty DuBois

Principal Consultant | DuBois Training & Consulting, LLC

SHARKFEST '08

Foothill College

March 31 - April 2, 2008

Agenda – Network Troubleshooting

Whose fault is it? How do I prove it? What am I looking for?

Placement is critical – what if I have 2 Wiresharks and am looking at both places? Life is good.

The Network

- Packet Loss
- High Latency

The Server

- High TCP handshake times. What should it be?

The Application

- Slow response times
- Once is freaky – twice is a pattern
- Show statistics depending on which trace file I use

Best Practices for Protocol Analysis

Onsite v. offsite analysis

Create a baseline when performance is acceptable

Analyze application traffic before deployment (capacity planning)

Troubleshooting Tips:

- Who complained?
- Begin as close to the user as possible
- Name captures appropriately (sue1, sue2, sue3mac, etc.)
- Move analyzer as needed or use multiple analyzers and agents
- Time-sync if using multiple analyzers
- Have taps/hubs in place for when the need arises
- Focus on the time column (delta time setting)
- Consider command-line capture (nmcap/tshark)

Security Tips:

- Baseline protocols, applications, traffic patterns
- Examine summary and protocol information for anomalies
- Look for signatures in questionable traffic
- Snort website has many signatures in the rule sets

Configuration Problems

Network Loop

Is it a

- duplicate ACK
- or looped packet?

**Duplicate
ACK!**

```
Frame 392 (66 bytes on wire, 66 bytes captured)
Ethernet II, Src: Sony_f4:3a:09 (08:00:46:f4:3a:09), Dst: 3Com_c9:51:b6 (00:04:5b:c9:51:b6)
Internet Protocol, Src: 10.0.52.164 (10.0.52.164), Dst: [REDACTED]
  Version: 4
  Header length: 20 bytes
  Differentiated Services Field: 0x00 (DSCP 0x00: Default; ECN: 0x00)
  Total Length: 52
  Identification: 0x1aa9 (6825)
  Flags: 0x04 (Don't Fragment)
  Fragment offset: 0
  Time to live: 64
  Protocol: TCP (0x06)
  Header checksum: 0xa45e [correct]
  Source: 10.0.52.164 (10.0.52.164)
  Destination: [REDACTED]
Transmission Control Protocol, Src Port: ads (2550), Dst Port: http (80), Seq: [REDACTED]
```

```
Frame 394 (66 bytes on wire, 66 bytes captured)
Ethernet II, Src: Sony_f4:3a:09 (08:00:46:f4:3a:09), Dst: 3Com_c9:51:b6 (00:04:5b:c9:51:b6)
Internet Protocol, Src: 10.0.52.164 (10.0.52.164), Dst: [REDACTED]
  Version: 4
  Header length: 20 bytes
  Differentiated Services Field: 0x00 (DSCP 0x00: Default; ECN: 0x00)
  Total Length: 52
  Identification: 0x1aaa (6826)
  Flags: 0x04 (Don't Fragment)
  Fragment offset: 0
  Time to live: 64
  Protocol: TCP (0x06)
  Header checksum: 0xa45d [correct]
  Source: 10.0.52.164 (10.0.52.164)
  Destination: [REDACTED]
Transmission Control Protocol, Src Port: ads (2550), Dst Port: http (80), Seq: [REDACTED]
```

Configuration Problems

Network Loop

Is it a

- duplicate ACK
- or looped packet?

Looped
Packet!

```
⊞ Frame 17 (60 bytes on wire, 60 bytes captured)
⊞ Ethernet II, Src: Dell_11:a2:68 (00:1a:a0:11:a2:68), Dst: MS-NLB-VirtServer_aa:
⊞ Internet Protocol, Src: [REDACTED], Dst: [REDACTED]
  Version: 4
  Header length: 20 bytes
  ⊞ Differentiated Services Field: 0x00 (DSCP 0x00: Default; ECN: 0x00)
  Total Length: 40
  Identification: 0xb8c7 (47303)
⊞ Flags: 0x04 (Don't Fragment)
  Fragment offset: 0
  Time to live: 128
  Protocol: TCP (0x06)
⊞ Header checksum: 0x7d6e [correct]
  Source: [REDACTED]
  Destination: [REDACTED]
⊞ Transmission Control Protocol, Src Port: apri-lm (1447), Dst Port: http (80), S
```

```
⊞ Frame 18 (60 bytes on wire, 60 bytes captured)
⊞ Ethernet II, Src: Dell_11:a2:68 (00:1a:a0:11:a2:68), Dst: MS-NLB-VirtServer_aa:
⊞ Internet Protocol, Src: [REDACTED], Dst: [REDACTED]
  Version: 4
  Header length: 20 bytes
  ⊞ Differentiated Services Field: 0x00 (DSCP 0x00: Default; ECN: 0x00)
  Total Length: 40
  Identification: 0xb8c7 (47303)
⊞ Flags: 0x04 (Don't Fragment)
  Fragment offset: 0
  Time to live: 128
  Protocol: TCP (0x06)
⊞ Header checksum: 0x7d6e [correct]
  Source: [REDACTED]
  Destination: [REDACTED]
⊞ Transmission Control Protocol, Src Port: apri-lm (1447), Dst Port: http (80), S
```

Redirections and Interdependencies

Topic / Item	Count	Rate	Percent
HTTP Requests by HTTP Host	132	0.003711	
www.espn.com	1	0.000028	0.76%
espn.go.com	18	0.000506	13.64%
espn-ak.starwave.com	65	0.001827	49.24%
adsatt.espn.go.com	7	0.000197	5.30%
espn.starwave.com	2	0.000056	1.52%
sports.espn.go.com	6	0.000169	4.55%
espn-att.starwave.com	4	0.000112	3.03%
ad.doubleclick.net	1	0.000028	0.76%
m1.2mdn.net	1	0.000028	0.76%
js.adsonar.com	1	0.000028	0.76%
log.go.com	4	0.000112	3.03%
static.espn.go.com	10	0.000281	7.58%
adsatt.espn.starwave.com	2	0.000056	1.52%
ads.espn.adsonar.com	4	0.000112	3.03%
rsi.espn.go.com	2	0.000056	1.52%
3ps.go.com	1	0.000028	0.76%
simg.zedo.com	1	0.000028	0.76%
ehg-dig.hitbox.com	2	0.000056	1.52%

Topic / Item	Count	Rate	Percent
Total HTTP Packets	261	0.007337	
HTTP Request Packets	132	0.003711	50.57%
HTTP Response Packets	127	0.003570	48.66%
???: broken	0	0.000000	0.00%
1xx: Informational	0	0.000000	0.00%
2xx: Success	122	0.003429	96.06%
3xx: Redirection	4	0.000112	3.15%
301 Moved Permanently	1	0.000028	25.00%
302 Found	3	0.000084	75.00%
4xx: Client Error	1	0.000028	0.79%
404 Not Found	1	0.000028	100.00%
5xx: Server Error	0	0.000000	0.00%
Other HTTP Packets	2	0.000056	0.77%

Low Throughput

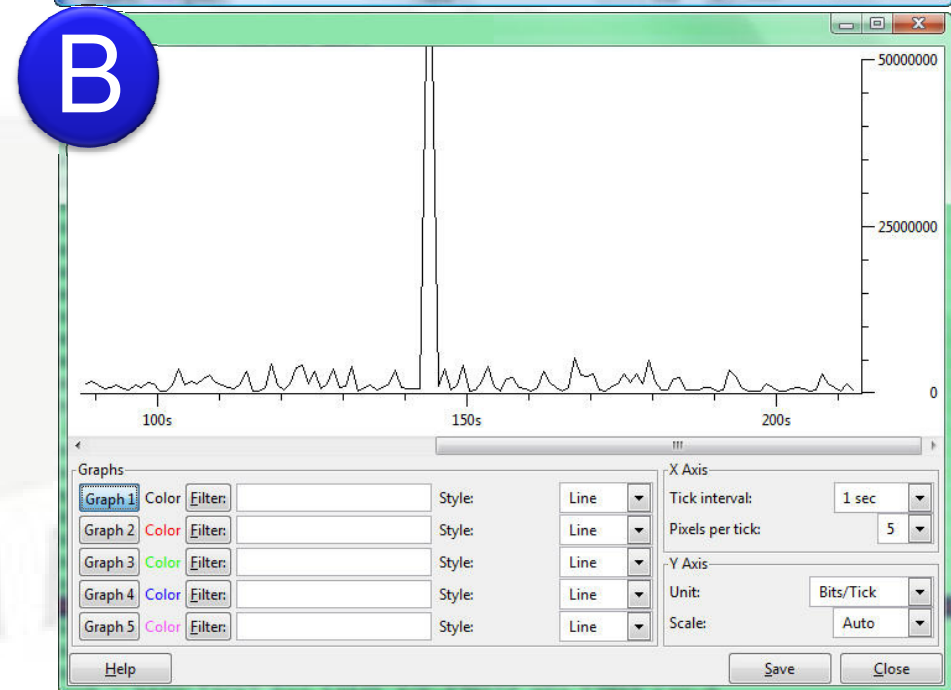
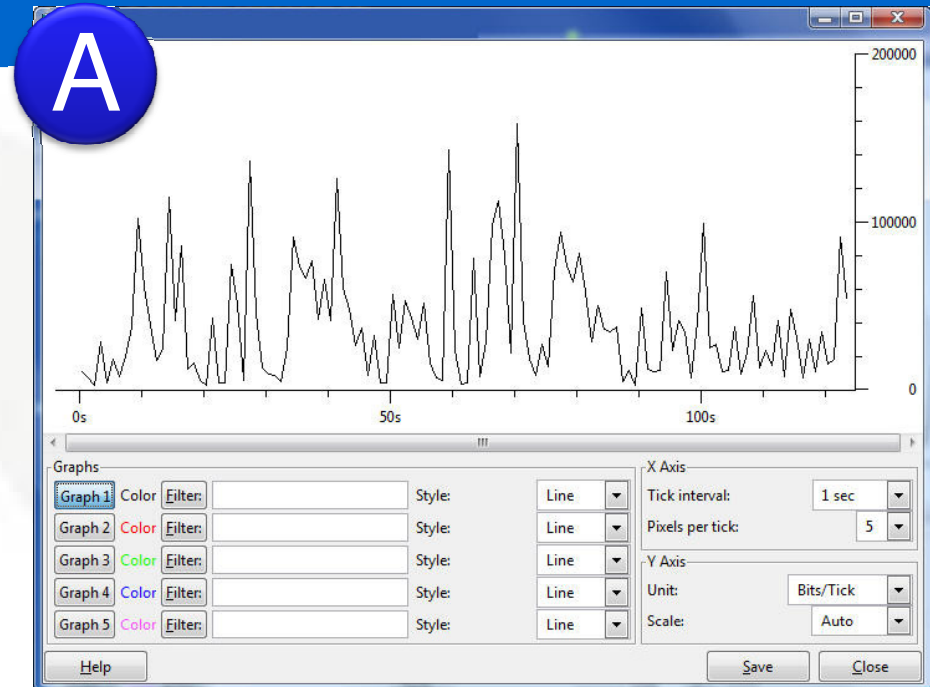
Determine maximum
mbits/sec

Application issue?

Network bottleneck?

Y axis in bits/second

- Y axis on A: 200,000
- Y axis on B: 50,000,000



Traces to Review

tcp-handshake-problem.pcap

ftp-pasv-fail.pcap

http-fault-post.pcap

http-espn.pcap

dns-ttl-issue.pcap

dhcp-server-slow.pcap

What's Next?

Laura's Lab Kit v9

In show bags as well as...

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

Wireshark University: www.wiresharkU.com

Laura's Blog: laurachappell.blogspot.com/

