Created using Apache OpenOffice™ 4

#SHAREorg

SHARE
Technology · Connections · Results

Taming the Shark
Tips and Tricks on Using Wireshark
Hands On Labs

Matthias Burkhard
IBM Technical Support Services
IBM Germany

Thursday Aug. 15 2013 4:30-5:30 PM
Session 13282 Hynes Room 202

Twitter @mreede
Find us on Facebook at ip.wizards@groups.facebook.com
LinkedIn: de.linkedin.com/in/mreede/
IBM SmartCloud: Matthias Burkhard

SocialBusiness IBMSmartCloud

SHARE in Boston

Why use different profiles?
A trace is a trace is a trace – isn't it?

Filter: Expression... Clear Apply Save

No.	Time	Source	Destination	Protocol	Length	Info
1	0.000000000	10.9.1.17	170.225.15.117	TCP	74	13188 > ftp [SYN] Seq=0 Win=65535 Len=0 M
2	0.146856000	170.225.15.117	10.9.1.17	TCP	58	ftp > 13188 [SYN, ACK] Seq=0 Ack=1 Win=65
3	0.146869000	10.9.1.17	170.225.15.117	TCP	54	13188 > ftp [ACK] Seq=1 Ack=1 Win=65535 L
4	0.296484000	170.225.15.117	10.9.1.17	FTP	121	Response: 220-IBM's internal systems must
5	0.296501000	10.9.1.17	170.225.15.117	TCP	54	13188 > ftp [ACK] Seq=1 Ack=68 Win=65535
6	0.443922000	170.225.15.117	10.9.1.17	FTP	226	Response: 220-business or for purposes au
7	0.443936000	10.9.1.17	170.225.15.117	TCP	54	13188 > ftp [ACK] Seq=1 Ack=240 Win=65535
8	0.646292000	10.9.1.17	170.225.15.117	FTP	64	Request: AUTH TLS
9	0.792889000	170.225.15.117	10.9.1.17	FTP	72	Response: 234 SSLv23/TLSv1
10	0.792911000	10.9.1.17	170.225.15.117	TCP	54	13188 > ftp [PSH, ACK] Seq=11 Ack=258 Win
11	0.793030000	10.9.1.17	170.225.15.117	FTP	114	Request: \026\003\001\0007\001\000\0003\0
12	0.939289000	170.225.15.117	10.9.1.17	FTP	61	Response: \025\003\001\000\002\002(
13	0.939299000	10.9.1.17	170.225.15.117	TCP	54	13188 > ftp [PSH, ACK] Seq=71 Ack=265 Win
14	0.939634000	170.225.15.117	10.9.1.17	TCP	54	ftp > 13188 [FIN, ACK] Seq=265 Ack=71 Win
15	0.939637000	10.9.1.17	170.225.15.117	TCP	54	13188 > ftp [PSH, ACK] Seq=71 Ack=266 Win
16	0.939885000	10.9.1.17	170.225.15.117	TCP	54	13188 > ftp [FIN, PSH, ACK] Seq=71 Ack=26
17	1.088457000	170.225.15.117	10.9.1.17	TCP	54	ftp > 13188 [ACK] Seq=266 Ack=72 Win=6553

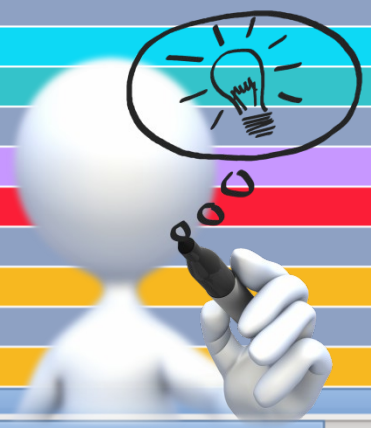
File: "/home/mburkhar/2013/PMRs/RIT/d0806/shop-z.systcpda.pcapng"... Packets: 17 Displayed: 17 Marked: 0 Load time:... Profile: _Default

Why use different profiles?
Coloring Rules! Show what's in there!

shop-z.systcpda.pcapng

File Edit View Go Capture Analyze Statistics Telephony Tools Internals Help

No.	Time	Source	d_port	whazzin	ACKed	RTT	Info
1	0.000	zOS-Client	21	p0f_zOS_Tstamp 65535:64:1:60:M*,N,W*,N,N,T			13188 > 21 [SYN] Seq=0 Win=65
2	0.146	shopz-FTP	13188	p0f_AIX 65535:60:1:44:M*	1	0.146	21 > 13188 [SYN, ACK] Seq=0 A
3	0.000	zOS-Client	21	zOS ACK	2	0.000	13188 > 21 [ACK] Seq=1 Ack=1
4	0.149	shopz-FTP	13188	FTP-220 Welcome			Response: 220-IBM's internal
5	0.000	zOS-Client	21	zOS ACK	4	0.000	13188 > 21 [ACK] Seq=1 Ack=68
6	0.147	shopz-FTP	13188	FTP-220 Welcome			Response: 220-business or for
7	0.000	zOS-Client	21	zOS ACK	6	0.000	13188 > 21 [ACK] Seq=1 Ack=24
8	0.202	zOS-Client	21	FTP-CMD: AUTH TLS			Request: AUTH TLS
9	0.146	shopz-FTP	13188	FTP-234 SSL OK	8	0.146	Response: 234 SSLv23/TLSv1
10	0.000	zOS-Client	21	zOS ACK	9	0.000	13188 > 21 [PSH, ACK] Seq=11
11	0.000	zOS-Client	21	Client Hello			Request: \026\003\001\0007\00
12	0.146	shopz-FTP	13188	TLS Alert	11	0.146	Response: \025\003\001\000\00
13	0.000	zOS-Client	21	zOS ACK	12	0.000	13188 > 21 [PSH, ACK] Seq=71
14	0.000	shopz-FTP	13188	tcp_down			21 > 13188 [FIN, ACK] Seq=265
15	0.000	zOS-Client	21	zOS ACK	14	0.000	13188 > 21 [PSH, ACK] Seq=71
16	0.000	zOS-Client	21	tcp_down			13188 > 21 [FIN, PSH, ACK] Se
17	0.148	shopz-FTP	13188		16	0.148	21 > 13188 [ACK] Seq=266 Ack=



File: "/home/mburkhar/2013/PMRs/RIT/d0806/shop-z.systcpda.pcapng"... Packets: 17 Displayed: 17 Marked: 0 Load time:... Profile: tcp

Wireshark Labs
3 Problems to chose from

- Problem 1: SMTP Performance Problem
  - TCP connections over WAN don't perform well
  - **http://www.cloudshark.org/captures/2021a63878f51**
- Problem 2: FTP TLS to ShopZ fails
  - FTP download from z/OS to ShopZ fails
  - **http://www.cloudshark.org/captures/0b9861a0cf43**
- Problem 3: iSCSI Performance Problem
  - SQL Server getting timeouts writing on storage array
  - **http://www.cloudshark.org/captures/a38f5226e356**

Lab1: SMTP Performance Problem
https://www.cloudshark.org/captures/2e96a1d22cdc

- Questions
  - Where was the trace taken, client or server?
  - How far away is the remote host?
  - What is the RTT on the connection
  - Wha is the largest windowsize offered?
    - By the client
    - By the server
  - Are there any retransmissions?
    - If so, why?
  - Who closes the connection?
  - How many bytes were sent/received?

Lab2: FTP TLS Problem
http://www.cloudshark.org/captures/0b9861a0cf43

- Questions
  - Where was the trace taken, client or server?
  - How far away is the remote host?
  - What is the RTT on the connection
  - What Ciphersuites does the client offer
    - By the client
    - By the server
  - How does the server react?
    - If so, why?
  - What can be done to fix this problem?

Lab3: SCSI Performance Problem
http://www.cloudshark.org/captures/a38f5226e356

- Questions
  - Where was the trace taken? Client or server
  - What is the operating system of the local host?
  - How far away is the remote host?
  - How many iSCSI requests are in the trace?
  - What are the iSCSI responsetimes?
  - How many retransmissions are in the trace?
  - How many delayed ACKs are in the trace?
  - What can be done to fix this problem?

Session 13282 “Taming the Shark” SMTP Performance

boston2013_1.pcapng

File Edit View Go Capture Analyze Statistics Telephony Tools Internals Help

No.	Time	ACKed	ColoringRuleName	Source	TTL	s_port	d_port	Seq	tcp.len	NxtSeq	ACK	Info
1	0.000000		p0f_zOS_16k_Tstamp 32768:64:1:60:M*,N,W0,N,N	10.62.42.244	64	58839	25	0	0			58839 > 25 [SYN] Seq=
2	0.007702	1	p0f Linux 3S:64:1:*:M*,	10.64.4.19	61	25	58839	0	0		1	25 > 58839 [SYN, ACK]
3	0.000036	2	zOS outbound	10.62.42.244	64	58839	25	1	0		1	58839 > 25 [ACK] Seq=
4	0.019862		SMTP 220 Welcome	10.64.4.19	61	25	58839	1	32	33	1	S: 220 radiuslx.f
5	0.206128		Slow Retransmit	10.64.4.19	61	25	58839	1	32	33	1	[TCP Retransmission]
6	0.000022	4	DelayACK	10.62.42.244	64	58839	25	1	0		33	58839 > 25 [ACK] Seq=
7	18.89031		zOS outbound	10.62.42.244	64	58839	25	1	15	16	33	C [redacted] BT2
8	0.006324	7		10.64.4.19	61	25	58839	33	0		16	25 > 58839 [ACK] Seq=
9	0.000176			10.64.4.19	61	25	58839	33	87	120	16	S: 250-radiuslx.f
10	0.000090	9	zOS outbound	10.62.42.244	64	58839	25	16	28	44	120	C: MAIL FROM:<ver
11	0.013534	10		10.64.4.19	61	25	58839	120	8	128	44	S: 250 Ok
12	0.000038	11	zOS outbound	10.62.42.244	64	58839	25	44	28	72	128	C: RCPT TO:<pps@r
13	0.014050	12		10.64.4.19	61	25	58839	128	8	136	72	S: 250 Ok
14	0.000044	13	zOS outbound	10.62.42.244	64	58839	25	72	6	78	136	C: DATA
15	0.006148	14		10.64.4.19	61	25	58839	136	37	173	78	S: 354 End data w
16	0.000164	15	zOS outbound	10.62.42.244	64	58839	25	78	1169	1247	173	C: DATA fragment, 14
17	0.013106	16		10.64.4.19	61	25	58839	173	30	203	1247	S: 250 Ok: queued
18	0.000032	17	zOS outbound	10.62.42.244	64	58839	25	1247	6	1253	203	C: DATA fragment, 6 b
19	0.006204	18		10.64.4.19	61	25	58839	203	9	212	1253	S: 221 Bye
20	0.000000		tcp_down	10.64.4.19	61	25	58839	212	0		1253	25 > 58839 [FIN, ACK]
21	0.000024	20	zOS outbound	10.62.42.244	64	58839	25	1253	0		213	58839 > 25 [PSH, ACK]
22	0.000010		tcp_down	10.62.42.244	64	58839	25	1253	0		213	58839 > 25 [FIN, PSH,
23	0.006312	22		10.64.4.19	61	25	58839	213	0		1254	25 > 58839 [ACK] Seq=

Session 13282 “Taming the Shark”
http://tinyurl.com/TamingShark

SHARE_BOS2013.TamingShark1.pcapng

File Edit View Go Capture Analyze Statistics Telephony Tools Internals Help

Filter: smtp.req.parameter == "TO:<ip.wizards@facebook.com>" Expression... Clear Apply Save ip.wizards

No.	Time	ACKed	ColoringRuleName	Destination	Source	TTL
1	0.000			tinyurl.com/ipwizards	zOS.VTAM.TCPIP.expert	64
2	0.007	1		tinyurl.com/ipwizards	de.linkedin.com/in/mreede	61
3	0.000	2	zOS outbound	tinyurl.com/ipwizards	zOS.VTAM.TCPIP.expert	64
4	0.019		SMTP 220 Welcome	tinyurl.com/ipwizards	de.linkedin.com/in/mreede	61
5	0.206		Slow Retransmit	tinyurl.com/ipwizards	de.linkedin.com/in/mreede	61
6	0.000	4	DelayACK	tinyurl.com/ipwizards	zOS.VTAM.TCPIP.expert	64
7	1			wizards	zOS.VTAM.TCPIP.expert	64
8	0			wizards	de.linkedin.com/in/mreede	61
9	0			wizards	de.linkedin.com/in/mreede	61
10	0			wizards	zOS.VTAM.TCPIP.expert	64
11	0			wizards	de.linkedin.com/in/mreede	61

Frame
Coloring Rule Name (frame.coloring_rule.name)

capng" ... Packets: 23 Displayed... Profile: tcp

Edit or Add Capture Comments

Wireshark Hands-On Lab at SHARE in Boston Summer 2013
Want to give it a try?
Join the "ip.wizards" Community in IBM Greenhouse to get connected
http://tinyurl.com/ipwizards

Help Cancel OK

Session 13282 “Taming the Shark”

http://www.cloudshark.org/captures/0b9861a0cf43

boston2013_2.pcapng

File Edit View Go Capture Analyze Statistics Telephony Tools Internals Help

Filter: smtp.req.parameter == "TO:<ip.wizards@facebook.com>" Expression... Clear Apply

No.	Time	ACKed	ColoringRuleName	Source	TTL	s_port	d_port
1	0.000000		p0f zOS_Tstamp 65535:64:1:60:M*,N,W*,N,N,T	zOS-Client	64	13188	21
2	0.146856	1	p0f_AIX 65535:60:1:44:M*	shopz-FTP	45	21	13188
3	0.000013	2	zOS ACK	zOS-Client	64	13188	21
4	0.149615		FTP-220 Welcome	shopz-FTP	45	21	13188
5	0.000017	4	zOS ACK	zOS-Client	64	13188	21
6	0.147421		FTP-220 Welcome	shopz-FTP	45	21	13188
7	0.000014	6	zOS ACK	zOS-Client	64	13188	21
8	0.202356		FTP-CMD: AUTH TLS	zOS-Client	64	13188	21
9	0.146597	8	FTP-234 SSL OK	shopz-FTP	45	21	13188
10	0.000022	9	zOS ACK	zOS-Client	64	13188	21
11	0.000119		TLS Client Hello	zOS-Client	64	13188	21
12	0.146259	11	TLS Alert	shopz-FTP	45	21	13188
13	0.000010	12	zOS ACK	zOS-Client	64	13188	21
14	0.000335		tcp_down	shopz-FTP	45	21	13188
15	0.000003	14	zOS ACK	zOS-Client	64	13188	21
16	0.000248		tcp_down	zOS-Client	64	13188	21
17	0.148572	16		shopz-FTP	45	21	13188

Session 13282 “Taming the Shark”

http://www.cloudshark.org/captures/a38f5226e356

SHARE_BOS2013.TamingShark.pcapng

File Edit View Go Capture Analyze Statistics Telephony Tools Internals Help

Filter: smtp.req.parameter == "TO:<ip.wizards@facebook.com>" Expression... Clear Apply Save

Frame
Coloring Rule Name (frame.coloring_rule.name)

No.	Time	ACKed	ColoringRuleName	Source	TTL	s_port	d_port	Seq	tcp
68	0.000			in.com/in/mreede	63	3260	63043	1509	1
69	0.000			m/ipwizards	128	63043	3260	67121	
70	0.000042		dup ack	tinyurl.com/ipwizards	128	63043	3260	67121	
71	0.060691	59	Slow Retransmit	de.linkedin.com/in/mreede	63	3260	63043	2969	1
72	0.000042		Slow Retransmit	de.linkedin.com/in/mreede	63	3260	63043	4429	1
73	0.000001		dup ack	tinyurl.com/ipwizards	128	63043	3260	67121	
74	0.000033		Slow Retransmit	de.linkedin.com/in/mreede	63	3260	63043	5889	1
75	0.000028		dup ack	tinyurl.com/ipwizards	128	63043	3260	67121	
76	0.000073		dup ack	tinyurl.com/ipwizards	128	63043	3260	67121	
77	0.001668	64		de.linkedin.com/in/mreede	63	3260	63043	8289	1
78	0.000049			de.linkedin.com/in/mreede	63	3260	63043	9749	1
79	0.000027			de.linkedin.com/in/mreede	63	3260	63043	11209	1
80	0.000033	78	Windows	tinyurl.com/ipwizards	128	63043	3260	67121	
81	0.202270	79	DelayACK	tinyurl.com/ipwizards	128	63043	3260	67121	
82	0.017877			de.linkedin.com/in/mreede	63	3260	63043	12669	1
83	0.000191			de.linkedin.com/in/mreede	63	3260	63043	14129	1
84	0.000008			de.linkedin.com/in/mreede	63	3260	63043	15589	1
85	0.000083	83	Windows	tinyurl.com/ipwizards	128	63043	3260	67121	
86	0.171382		Nagle	de.linkedin.com/in/mreede	63	3260	63043	17049	1

Coloring Rules!
Add some colors to your office ...

http://tinyurl.com/ipwizards

ip.wizards@groups.facebook.com

Your feedback is important:

This was session 13282 at SHARE in Boston 2013

Taming the Shark