



Taming the (wire)Shark wireshark Hands on Lab



Matthias Burkhard mburkhar@de.ibm.com **IBM** Germany



August 8. 2012 4:30 PM – 5:30 PM **11342** Orange County Salon 2/3







Session Contents



Taming the (wire)Shark – Hands on Lab

Learn how to configure the wireshark trace tool to better suit your needs Change the Default Profile Create a profile for CICS Transaction Gateway Protocol problems



Download wireshark



http://www.wireshark.org/

Wireshark is constantly improved and updated so check out the website regularly As of August 2012, the latest stable release is 1.8.1 Help \rightarrow About Wireshark will tell you what's installed.



SHARE Technology - Canactilas - Results

2012



Default Configuration: Not to everyone's taste

🗹 d0731.client.pcap [Wireshark 1.8.1 (SVN Rev 43946 from /trunk-1.8)]							
File Edit View Go Capture Analyze Statistics Telephony Tools Internals Help							
I I I I I I I I I I I I I I I I I I I							
Filter: ip.checksum_bad==1							
ITime ISource Isrc_port IDestination Idst_port IProtocol Length lpid ITTL Info 766 0.484 192.168.90.43 64807 192.168.2.9 8497 TCP 447 0x1494 128 64807 > 8497 [PSH,							
79: Wireshark: 9337 Expert Infos							
799	[TCP Dup ACK 764#3]						
790 Errors: 1 (8630) Warnings: 3 (14) Notes: 18 (26) Chats: 5 (667) Details: 9337 Packet Comments: 0	[TCP Dup ACK 764#4]						
Group I Protocol I Summary I Count I	[TCP Dup ACK 764#5						
Type E Checksum IPv4 Bad checksum 8630							
800	[TCP Dup ACK 764#7						
801	[ТСР Dup ACK 764#9						
802 Depending on where the trace was taken, the JE	о Ск. 764#1 🗸						
Checksum might not be calculated yet	>						
Checksum might not be calculated yet.							
Flags: 0x02 (Don't Frage Need to disable IP checksum verification!							
Time to live: 128							
Protocol: TCP (6)							
Header checksum: 0x0000 [incorrect, should be 0x0720 (may be caused by "IP	checksum of						
0000 00 12 c1 f7 90 14 00 50 56 a6 40 3c 08 00 45 00P V.@ <e.< td=""><td></td></e.<>							
0010 01 bT 14 94 40 00 80 06 00 00 c0 a8 5a 2b c0 a8@							
0030 01 02 df 36 00 00 00 01 97 00 00 0e 47 00 0b6G							
0040 90 a0 27 05 02 ff 00 03 d1 00 40 04 c2 e2 d4 c9'							
🛑 💅 Header checksum (Packets: 26221 Displayed: 8630 Marked: 0 Load time: 0:01.312	Wrofile: Default .:						
	SHARE						
sessions evaluation online at SHARE.org/AnaheimEval	•••• in Anaheim						

2012



Default Configuration: Edit - Preferences

Change the configuration for IPV4 and TCP traffic

d 🗖	📶 d0731.client.pcap [Wireshark 1.8.1 (SVN Rev 43946 from /trunk-1.8)]										
Eile	Edit View Go Capture Analyze Statistics Telephony Tools Internals Help										
	_	Сору	🔼 Wireshark: Pi	Wireshark: Preferences - Profile: Default							
Filter	_	Find Packet Find Ne <u>x</u> t Find Pre <u>v</u> ious	ากากเหลกด Infiniband SD IPDC	P	Internet	Protocol Ver:	sion 4	Decode IPv	4 TOS field as [DiffServ field:	
75		<u>M</u> ark Packet (toggle) Mark All Displayed Pack	IPMI/ATCA IPv4	-1				Reassemble fi	agmented IPv	4 datagrams:	
7 9 7 9 7 9		Unmark All Displayed Pa Find Next Mark Find Previous Mark	IPv6 ISAKMP					Show IPv Validate th	4 summary in p e IPv4 checksu	protocol tree:	
7 : 7 : 7 : 7 : 7 :	· · · · · · · · · · · · · · · · · · ·	Ignore Packet (toggle) Ignore All Displayed Pa U <u>n</u> -Ignore All Packets	ISCSI ISDN ISMACRYP	Une Wh Off	check t ile you' oaded	he func re here to HW i	tions you don't , check out the in some TCP/II	need/like TCP check P stacks als	ksum!	hardware: IP lookups:	
70 70 70	0	Set Time Reference (to Un-Time Reference All I Find Next Time Referen	ISUP ITDM				Interp	Dret Rese	writy flag) (RFC 3514):	
70 70 70	0	Find Previous Time Refer	ence	Shift+Ctrl+T 4	8497 364807 355329	TCP TCP TCP	447 0x1494 40 0x6b50 40 0xdbb7	128 64807 > 59 8497 > 59 8497 >	8497 [PS 64807 55329	H,	
<	¥2	Edit or Add Packet Comm	ient							FFF	7
	*	<u>C</u> onfiguration Profiles Preferences		Shift+Ctrl+A Shift+Ctrl+P	00 45 () Load time:	0.01.140	@. <i><</i> ₽	Pro	file: Def		
Con	nple	te your sessions evalu	uation online at SH	ARE.org/Anah	eimEval					SHAI	RE Anaheim

2012



Default Configuration: Edit - Preferences

Add additional columns to the packet list window

🗖 d	d0731.client.pcap [Wireshark 1.8.1 (SVN Rev 43946 from /trunk-1.8)]									
<u>F</u> ile	<u>E</u> dit	t <u>V</u> iew <u>G</u> o <u>C</u> apture	Analyze Statistics Telephony	Tools Internals Help						
		Сору	Wireshark: Preferences	- Profile: Default						
Filter	_	Eind Packet Find Ne <u>x</u> t Find Pre <u>v</u> ious <u>Mark Packet (toggle)</u> Mark All Displayed Pack <u>Unmark All Displayed Pack</u> Find Next Mark Find Previous Mark	User Interface Layout Columns Font Colors Capture	Image: Constraint of the second consecond consecond constration of the second constration						
7 ! 7 ! 7 (7 (7 (7 (7 (7 (7 (7 (Ignore Packet (toggle) Ignore All Displayed Pac Un-Ignore All Packets Set Time Reference (to Un-Time Reference All F Find Next Time Reference Find Previous Time Reference	Printing Name Resolution Filter Expressions Statistics Protocols	sing a field type of Custom, you can select any ddressable field in a packet <pre> src_port Src port (unresolved) dst_port Dest port (unresolved) Info Information </pre>						
70	© 12	Time Shift Edit or Add Packet Comn	nent	4355329 TCP 40 0xdbb7 59 8497 > 55329						
0000	*	Configuration Profiles Preferences	Shift+Ctrl+A Shift+Ctrl+P	0.0 45 0.0 PV @< F 0 Load time: 0:01.140 Profile: Def						

••••• in Anaheim 2012



Default Configuration: Coloring Rules

Assign different colors based on direction of traffic

d0731.client.pcap [Wireshark 1.8.1 (SVN Rev 43946 from /trunk-1.8)]										
Eile Edit View Go Capture Analyze Statistics Telephony Tools Internals Help										
	M 🔊 🕷) i i	🔼 Wiresha	rk: Coloring Rul	es - Pro	ofile: Default				
Filter:			Edit-	-Filter			Order			
		10			List is	processed in order until match is found				
No. 7	1 me	102 16		Name		String				
7	59 0.000	192.16	Edit	Bad TCP		tcp.analysis.flags && !tcp.analysis.windo	low_upda			
7	60 0.000	192.16		ICMP errors		icmp.type eq 3 icmp.type eq 4 icmp.	type eq .			
7	61 0.000	192.16	Enable	TCP RST		tcp.flags.reset eq 1				
7	62 0.000	192.16		TTL low or unexpe	ected	Initial TTL a care has used to	ide which the s			
7	63 0.003	192.16	Disable	TCD SVN/ETN		Initial TTLS can be used to	Identify the			
7	64 0.128	192.16				operating system of the set	ender			
7	65 0.000	192.16	Delete	Checksum Errors						
7	766 0.484 192.161 Windows TTL ip.ttl le 128 and ip.ttl ge 64 down									
7	67 0.001	192.16	-Manage	AIX		(ip.ttl le 60 and tcp) or (ip.ttl le 30 and u	udp)			
	68 0.110	192.16	Tennert	z/OS		ip.ttl le 64				
	70 0.000	102.16	[Tuborc]	IPX		ipx spx				
7	70 0.000	192.100	Export	DCERPC		deeroc				
- 7	72 0.000	192.16		Deutine		here II sizes II scaf II has II ado II yere				
773 0.000 192.168.										
774 0.000 192.168.2.8 59 0xdbbe 40 192.168.90.43TCP 8497 55329 8497 > 5532										
0000	00 50 5	6 56 40	26 00 12	c1 f7 00 14	08.00	45.00 DV @		\mathbf{x}		
	File: "C:\Dog	ument Par	kets: 26221 Disr	played: 26221 Marke	ox 00 d:01oa	d time: 0:00.828	Profile: Def	1/		
	Ther cripbe									

2012

aheim

Default Configuration: Display Filters



Change the pre-defined Display Filters

🗖 d0731.	.client.pca	p [Wireshark 1.8.1 (SVN Rev 43946 from /trun	run <mark>l</mark> 📶 Wireshark: Display Filter - Profile: Default	
<u>Eile E</u> dit	<u>V</u> iew <u>G</u> o	<u>Capture Analyze Statistics Telephony</u> <u>T</u> ools <u>I</u> nterna	erna Edit-Display Filter-	
	M 🕷 🕷	🖻 🐻 🗶 🤁 📇 🔍 🍬 🧼 🌍 👍 🛂	Ethernet address 00:08:15:00:08:15	
Titan (Ethernet type 0x0806 (ARP)	
Filter:	🔼 Wiresh	ark: Display Filter - Profile: Default 🛛 🗖 🔀	Ethernet broadcast	
No. 758	Edit-	Display Filter	No ARP	
759		3-way Handshake	IP only	
760		Delay greater 1 sec	IP address 192.168.0.1	
761	New	PING requests and replies	IP address isn't 192.168.0.1, don't use != for this!	
762		ICMP Errors	IPX only	
764		EEonly	TCP only	
765		EE Link up/down	reate your own Display Filters and koon	
760	Delete	HPR PATHSWITCH	Teale your own Display Fillers and keep	
768	Ecicic	HPR ARB_Slowdown	leffi for later use	
769		HPR GAP	Properties	
770	-Properties-			628
772	Filter name	HPR GAP		
773	Eilten atriaa		Filter string:	AND
774	Filter string	: sna.nip.trior.optional.0e.gap==1		151
	Help	OK Apply Cancel		
			B28 Profile: Def	
				ARE

in Anaheim



Default Configuration: Where is it kept?

Help \rightarrow About Wireshark \rightarrow Folders

🗖 About Wiresbark	
	🖙 Wireshark
Wireshark Authors Folders Plugins License	File Edit View Favorites Tools Help
Name IFolder	
"File" dialogs <u>C:\Documents and Settings\Administrator\Desktop\sha</u>	Back * 🖸 * 💋 Search
Temp <u>C:\DOCUME~1\ADMINI~1\LOCALS~1\Temp\</u>	Address 🗁 C: \Documents and Settings \Administrator \Application Data \Wireshark
Personal configuration <u>C:\Documents and Settings\Administrator\Application D</u>	Folders X Name
Global configuration <u>C:\Program Files\Wireshark</u>	
System <u>C:\Program Files\Wireshark</u>	
Program <u>C:\Program Files\Wireshark</u>	E V Computer
Personal Plugins <u>C:\Documents and Settings\Administrator\Application D</u>	
Global Plugins <u>C:\Program Files\Wireshark\plugins\1.8.1</u>	
	2 files form a wireshark (Drofile)
2 Wireshark	
File Edit View Favorites Tools Help	dfliters, colorfliters, preferences
	Copy those to the Global configuration
Back • 🕑 • 🥬 🔊 Search 🎼 Folders	
Address 🛅 C:\Program Files\Wireshark	
olders × Name	Size 🔺
🗀 PuTTY 💽 cfilters	1 KB
Colorfilters	2 KB
Compared Television Compared Television Compared Television	
🕀 🛅 Symantec 🛛 🔛 🖼 manuf	1. 146 KB
Complete your sessions evaluation online at SHARE.org/AnaheimEv	val •• in Anahei

New Profile: Create a Profile for ctg problems



Configuration for CICS Transaction Gateway problems Some Background on CICS Transaction Gateway flows

- CTG was using SNA LU6.2 (APPC) protocol originally
- Native TCP Socket support came later
- Inside the TCP segment there are still LU6.2 structures to be found
 - SNA Sequence Numbers
 - SNA RH (Request Response Headers
 - SNA FMH5 (0x0502FF) to start (ATTACH) a Transaction Program
 - SNA GDS Variables (0x12FF,0x12F2)
 - SNA FMH7 to report SNA Sense Codes





Background: CICS Transaction Gateway

'SNA LU62' protocol within TCP

								2cIP	- TRACE	ΞĒ	ANALYS	IS PA	NEL -	+-		
Command ===>																
MAC_Eth_II IP	_V4_T0	CP CTG RH_	_REQ FM_FN	MH_05_LU6:	2 GD_12F2											
NA 192.168	.2.8()	8497) <- :	192.168.90	0.43(5532)	9) CTG <mark>AP</mark>	ReQ I	FMH-5	ATTAC	CH(BSMI) (JCD RU	()FMD				
RECORD 4(FI	LTERE	D) Len 498	8 Time 20:	12/07/31-:	15:22:57.	885933	Capt	SNIFF	FER							
MAC_Eth_II		MAC Ethe	ernet II													
	0000	0012C1F7	90140050	56A6403C	0800	EBC:<	A7	- & u	J	>	ASC:K		PV	eć		>
IP_V4		IP_V4 He	eader													
	0000	450001BC	14CD4000	80060000	C0A85A2B	EBC:<			{y!	>	ASC:K	E	0		Z+	>
	0010	C0A80208				EBC:<	{y			>	ASC:K					>
TCP		 TCP Head 	den													
	0000	D8212131	2F7527A5	6E7693C0	501800FD	EBC:<	Q	$\cdot \cdot \lor $	ι{&	>	ASC:K	!!1	/u' n	V P	1	>
	0010	DF320000				EBC:<	1.1			>	ASC:K	2				>
СТС		CTG CICS	S Transact	tion Gate	Jay											
	0000	00000194	00000E49	00		EBC:<	m			>	ASC:K		I			>
RH_REQ		Request	Header													
	0000	0B90A0				EBC:<				>	ASC:K					>
FM_FMH_05_LU	52	FM Heade	en 5: Ati	tach (LU I	5.2)			-								
	0000	270502FF	0003D100	4004C2E2	D4C9180B	EBC:<	·	J	BSMI	\geq	ASC: <	1.00	e			\geq
	0010	02030903	E2E4E2C5	D940400B	01860000	EBC:K	CIUS	SUSER		\geq	ASC:K			00		2
	0020	00000000	000000	(ULLA OF O		EBU:K				>	ASC:K					>
GD_12F2		User Cor	ntrol Data	B (X112F2)	r) GDS Vai	niable.		_				_				
	0000	016112F2	0850202	01020000	01040E43	EBU:K	1 2	e		2	HSC:K	а			U.	2
	0010	0E020000 E202E400	07610000	00000100	000H02E4	EBU:K	Veute	·	DOM T	2	HSU:K					2
	0020	E7U7E4U9	06202020	00020204	E2404E4E	EBU:K	XGOIC		5511	2	HSU:K		0000	eree	TON	2
	0030	01200126	000000000	30334333	- 33494F4E	EDU:K			1 *	1	HSU:K	11	0000	SESS	TON	ζ.
	0040	20202020	20202020	20202020 40454720	20202020	EBC:X				<	ASC 12		DI	NG		<
	0000	20202020	20202030	20202020	20202020	EBC: 4		· · · α		<			PI	na		<
	0000	20202020	20202020	56/1/055	45202020	EBC . Z			• • • • • • • •	<	ASC • Z		CETV			<
	0070	20202020	20474004	2021202020		EBC.			× •••	1	A80.7		GETV	HEOE		0

2cIP http://www.ansynova.com



AIX (CTG) closes the connection



Why? Who is at fault?

131 ctg_big_data 0.00220 59 0xdc51 192.168.2.8 1300 1853275232 3830373830383520202030445242285347454C3030 132 ctp_delay ack 0.20219 128 0x151e 192.168.2.8 1300 1853276532 2030303130303330303630313530323130323230323 133 ctg_big_data 0.00071 59 0xdc72 192.168.2.8 1300 1853276532 2030303130303330303630313530323130323230323 135 ctg_big_data 0.00144 59 0xdc72 192.168.2.8 1300 1853277832 20A7393920A73633204444A73035534C53534C5353 136 ctg_big_data 0.00144 59 0xdc72 192.168.2.8 1300 1853277832 20A7393920A73633204444A73035534C53534C53534C53534 137 ctg_big_data 0.00079 59 0xdcc7 192.168.2.8 1300 185327132 30303434333343032384754C46454747454C30303 138 ctg_big_data 0.00076 59 0xdcc1 192.168.2.8 1300 1853281732 36303236303333303339303655A73237203044524 140 ctg_big_data 0.00076 59 0xdcd1 192.168.2.8 1300 1853281732 A7393920A73633204444A73035534C53534C53534 143 ctg_big_data 0.00001 128 0x152 192.168.2.8 1300 1853281732 A7393920A736332	No. 🗸	whazzin	Time	TTL	ip.id	Source	tcp_len	tcp.seq	data
132 tcp delay ack 0.20219 128 0x151e 192.168.90.4 0 796208225 133 tcp big data 0.00071 59 0xdc5e 192.168.2.8 1300 1833276532 20303313033330363031353032313032323033 134 tcp delay ack 0.20042 128 0x1523 192.168.2.8 1300 1853277832 20A7333920A73633204444A73035534C53534C53534C53534 136 ctn heartbeat 0.17204 128 0x1526 192.168.2.8 1300 1853277132 20A7333920A73633204444A73035534C53534C53534 136 ctn heartbeat 0.17204 128 0x1526 192.168.2.8 1300 1853279132 30303434333430323847454C46454747454C303033 138 tcp_ack 0.00002 128 0x1527 192.168.2.8 1300 1853284356 000014600006249000390010134125207436020 139 tcp_ack 0.00002 128 0x1527 192.168.2.8 1300 1853281732 A7393920A73633204444A73035534C53534C53534 140 ctg_big data 0.00007 59 0xdcd1 192.168.2.8 1300 1853281732 A7393920A73633204444A73035534C53534C53534 <	131	ctg_big_data	0.00220	59	0xdc51	192.168.2.8	1300	1853275232	38303738303835202020304452422B5347454C30303
133 ctg_big_data 0.00071 59 0xdc5e 192.168.2.8 1300 1853276532 20303031303033330303630313530323130323230333 134 tcp_delay ack 0.20042 128 0x1523 192.168.90.4 0 796208225 135 ctg_big_data 0.00144 59 0xdc72 192.168.90.4 100 1853277832 2047393920473633204444A73035534C53533333333	132	<pre>tcp_delay_ack</pre>	0.20219	128	0x151e	192.168.90.4	Θ	796208225	
134 tcp delay ack 0.20042 128 0x1523 192.168.90.* 0 796208225 135 ctg big data 0.00144 59 0xdc72 192.168.2.8 1300 1853277832 20A7393920A73633204444A73035534C53534265324545454545454545454545454545454545454	133	ctg_big_data	0.00071	59	0xdc5e	192.168.2.8	1300	1853276532	2030303130303330303630313530323130323230323
135 ctg_big_data 0.00144 59 0xdc72 192.168.2.8 1300 1853277832 20A7393920A73633204444A73035534C53534C	134	<pre>tcp_delay_ack</pre>	0.20042	128	0x1523	192.168.90.4	Θ	796208225	
136 ctg heartbeat 0.17204 128 0x1526 192.168.90.4 404 796208225 0000019400000E50000B90A0270502FF0003D10044 137 ctg big data 0.00098 59 0xdcc2 192.168.2.8 1300 1853279132 30303434333430323847454C46454747454C303034 138 ctg heartbeat 0.000779 59 0xdcc2 192.168.2.8 1300 1853279132 30303434333430323847454C46454747454C303034 139 tcp_ack 0.00002 128 0x1527 192.168.2.8 1300 1853280432 36303236303333303339303635A732372030445243 141 tcp_ack 0.00003 128 0x1528 192.168.90.4 0 796208629 142 ctg big data 0.00076 59 0xdcd1 192.168.90.4 0 796208629 143 tcp_ack 0.00001 128 0x1529 192.168.90.4 0 796208629 144 ctg big data 0.0001 128 0x152a 192.168.90.4 0 796208629 144 ctg big data 0.00001 128 0x152a 192.168.90.4 0 796208629 144 ctg big data 0.00001 128 0x152a 192.168.90.4 0 796208629 144 ctg big data 0.00001 128 0x152a 192.168	135	ctg_big_data	0.00144	59	0xdc72	192.168.2.8	1300	1853277832	20A7393920A73633204444A73035534C53534C53534
137 ctg big data 0.00098 59 0xdcc2 192.168.2.8 130 1853279132 30303434333430323847454C46454747454C303034 138 ctg heartbeat 0.00779 59 0xdccc 192.168.2.8 1300 1853284363 00001450000054900039001015A12F2074305020 139 tcp_ack 0.00002 128 0x1527 192.168.90.4 0 796208629 140 ctg big data 0.00076 59 0xdcd 192.168.90.4 0 796208629 142 ctg big data 0.00076 59 0xdcd1 192.168.2.8 1300 1853281732 A7393920A73633204444A73035534C53534C53534C535344 143 tcp_ack 0.00001 128 0x1529 192.168.90.4 0 796208629 144 ctg big data 0.00076 59 0xdcd1 192.168.2.8 1300 1853281732 A7393920A73633204444A73035534C53534533333333	136	ctg_heartbeat	0.17204	128	0x1526	192.168.90.4	404	796208225	0000019400000E50000B90A0270502FF0003D100400
138 ctg heartbeat 0.00779 59 0xdccc 192.168.2.8 1300 1853284368 0000014600000E4900039001013A12F207430E0201 139 tcp_ack 0.00002 128 0x1527 192.168.90.4 0 796208629 140 ctg_big_data 0.00076 59 0xdcd0 192.168.2.8 1300 1853280432 36303236303333303339303635A732372030445243 141 tcp_ack 0.000076 59 0xdcd1 192.168.2.8 1300 1853280432 3630323630333303339303635A732372030445243 143 tcp_ack 0.00007 59 0xdcd1 192.168.2.8 1300 1853281732 A7393920A73633204444A73035534C53534C53534C53534C53534C53534C53534C53534C53534C53534C53534C545354C5453544 143 tcp_ack 0.00001 128 0x1529 192.168.2.8 1300 1853283032 383037383	137	ctg_big_data	0.00098	59	0xdcc2	192.168.2.8	1300	1853279132	30303434333430323847454C46454747454C3030383
139 tcp_ack 0.00002 128 0x1527 192.168.90.4 0 796208629 140 ctg_big_data 0.00076 59 0xdcd0 192.168.2.8 1300 1853280432 3630323630333303339303635A732372030445242 141 tcp_ack 0.00003 128 0x1528 192.168.90.4 0 796208629 142 ctg_big_data 0.00001 128 0x1529 192.168.90.4 0 796208629 144 tcg_big_data 0.00001 128 0x1529 192.168.90.4 0 796208629 144 tcg_big_data 0.00001 128 0x152a 192.168.2.8 1300 1853281732 A7393920A73633204444A73035534C53534C52 144 tcg_big_data 0.00001 128 0x152a 192.168.2.8 1300 1853281568 20202023 147 tcp_ack 0.00004 128 0x152b 192.168.2.8 4 1853285672 1304 1853285672 148 ctg_big_data 0.000051 59 0xdcd5 192.168.2.8 19 1853285672 155328642 0000001	138	ctg_heartbeat	0.00779	59	0xdccc	192.168.2.8	1300	1853284368	0000014600000E4900039001013A12F207430E02000
140 ctg_big_data 0.00076 59 0xdcd0 192.168.2.8 1300 1853280432 36303236303333303339303635A732372030445242 141 tcp_ack 0.00003 128 0x1528 192.168.90.4 0 796208629 142 ctg_big_data 0.00076 59 0xdcd1 192.168.2.8 1300 1853281732 A7393920A73633204444A73035534C5353423323636333333333333333333333333333	139	tcp_ack	0.00002	128	0x1527	192.168.90.4	Θ	796208629	
141 tcp_ack 0.00003 128 0x1528 192.168.90.4 0 796208629 142 ctg_big_data 0.00076 59 0xdcd1 192.168.2.8 1300 1853281732 A7393920A73633204444A73035534C535340 1853285672	140	ctg_big_data	0.00076	59	0xdcd0	192.168.2.8	1300	1853280432	36303236303333303339303635A7323720304452422
142 ctg_big_data 0.00076 59 0xdcd1 192.168.2.8 1300 1853281732 A7393920A73633204444A73035534C53534C53534C53534C 143 tcp_ack 0.00001 128 0x1529 192.168.90.4 0 796208629 144 ctg_big_data 0.00108 59 0xdcd2 192.168.2.8 1300 1853283032 383037383	141	tcp_ack	0.00003	128	0x1528	192.168.90.4	Θ	796208629	
143 tcp_ack 0.00001 128 0x1529 192.168.90.4 0 796208629 144 ctg_big_data 0.00108 59 0xdcd2 192.168.2.8 1300 1853283032 38303738307 145 tcs	142	ctg_big_data	0.00076	59	0xdcd1	192.168.2.8	1300	1853281732	A7393920A73633204444A73035534C53534C53534B5
144 ctg big data 0.00108 59 0xdcd2 192.168.2.8 1300 1853283032 38303738307	143	tcp_ack	0.00001	128	0x1529	192.168.90.4	Θ	796208629	
145 tcp_ack 0.00001 128 0x152a 192.168.90.4 0 796208629 146 ctg_heartbeat 0.00097 59 0xdcd3 192.168.2.8 1300 1853284332 A73036304E312C3232373635A73035303631322C3 147 tcp_ack 0.00004 128 0x152b 192.168.90.4 0 796208629 148 ctg_big_data 0.00080 59 0xdcd4 192.168.2.8 4 1853285668 2D2D2D23 149 FMH7 0.12260 128 0x1548 192.168.90.4 19 796208629 0000001300000E46000B900107070864000000 150 tcp_ack 0.00051 59 0xdcd5 192.168.2.8 0 1853285672 151 FMH7 0.01838 128 0x154d 192.168.90.4 19 796208648 0000001300000E49000B900107070864000000 152 tcp_ack 0.00112 59 0xdcd5 192.168.2.8 0 1853285672 153 FMH7 0.00005 59 0xdcd6 192.168.2.8 19 1853285672 0000001300000E46000B900107071008600B00 154 FIN 0.000001 59 0xdcd8 192.168.2.8 0 1853285691 155 tcp_ack 0.00001 128 0x154e 192.168.2.8 0 1853285691 </td <td>144</td> <td>ctg_big_data</td> <td>0.00108</td> <td>59</td> <td>0xdcd2</td> <td>192.168.2.8</td> <td>1300</td> <td>1853283032</td> <td>3830373830373830373830373830373830373830373830383</td>	144	ctg_big_data	0.00108	59	0xdcd2	192.168.2.8	1300	1853283032	3830373830373830373830373830373830373830373830383
146 ctg heartbeat 0.00097 59 0xdcd3 192.168.2.8 1300 1853284332 A73036304E312C3232373635A73035303631322C30 147 tcp_ack 0.00004 128 0x152b 192.168.90.4 0 796208629 148 ctg_big_data 0.00080 59 0xdcd4 192.168.2.8 4 1853285668 2D2D2D23 149 FMH7 0.12260 128 0x1548 192.168.2.8 0 1853285672 150 tcp_ack 0.00051 59 0xdcd5 192.168.2.8 0 1853285672 151 FMH7 0.01838 128 0x154d 192.168.2.8 0 1853285672 152 tcp_ack 0.00112 59 0xdcd5 192.168.2.8 0 1853285672 153 FMH7 0.00005 59 0xdcd7 192.168.2.8 0 1853285672 153 FMH7 0.00005 59 0xdcd7 192.168.2.8 0 1853285672 153 FMH7 0.00005 59 0xdcd7 192.168.2.8 0 1853285672	145	tcp_ack	0.00001	128	0x152a	192.168.90.4	Θ	796208629	
147 tcp_ack 0.00004 128 0x152b 192.168.90.4 0 796208629 148 ctg_big_data 0.00080 59 0xdcd4 192.168.2.8 4 1853285668 2D2D2D23 149 FMH7 0.12260 128 0x1548 192.168.90.4 19 796208629 0000001300000E46000B900107070864000000 150 tcp_ack 0.00051 59 0xdcd5 192.168.2.8 0 1853285672 151 FMH7 0.01838 128 0x154d 192.168.90.4 19 796208648 0000001300000E46000B900107070864000000 152 tcp_ack 0.00112 59 0xdcd6 192.168.2.8 0 1853285672 153 FMH7 0.00005 59 0xdcd6 192.168.2.8 0 1853285672 153 FMH7 0.00005 59 0xdcd7 192.168.2.8 19 1853285672 0000001300000E46000B900107071008600B00 154 FIN 0.00000 59 0xdcd8 192.168.2.8 0 1853285691 1853285691 155 tcp_ack 0.00001 128 0x154e 192.168.90.4 0 796208667 0 796208667	146	ctg_heartbeat	0.00097	59	0xdcd3	192.168.2.8	1300	1853284332	A73036304E312C3232373635A73035303631322C303
148 ctg_big_data 0.00080 59 0xdcd4 192.168.2.8 4 1853285668 2D2D2D23 149 FMH7 0.12260 128 0x1548 192.168.90.4 19 796208629 0000001300000E46000B900107070864000000 150 tcp_ack 0.00051 59 0xdcd5 192.168.2.8 0 1853285672 151 FMH7 0.01838 128 0x154d 192.168.90.4 19 796208648 0000001300000E49000B900107070864000000 152 tcp_ack 0.00112 59 0xdcd6 192.168.2.8 0 1853285672 153 FMH7 0.00005 59 0xdcd7 192.168.2.8 0 1853285672 154 FIN 0.00000 59 0xdcd8 192.168.2.8 19 1853285672 0000001300000E46000B900107071008600B00 154 FIN 0.00000 59 0xdcd8 192.168.2.8 0 1853285691 155 tcp_ack 0.00001 128 0x154e 192.168.90.4 0 796208667	147	tcp_ack	0.00004	128	0x152b	192.168.90.4	Θ	796208629	
149 FMH7 0.12260 128 0x1548 192.168.90.4 19 796208629 0000001300000E46000B900107070864000000 150 tcp_ack 0.00051 59 0xdcd5 192.168.2.8 0 1853285672 151 FMH7 0.01838 128 0x154d 192.168.90.4 19 796208648 0000001300000E49000B900107070864000000 152 tcp_ack 0.00112 59 0xdcd6 192.168.2.8 0 1853285672 153 FMH7 0.00005 59 0xdcd7 192.168.2.8 0 1853285672 0000001300000E46000B900107071008600B00 154 FIN 0.00000 59 0xdcd8 192.168.2.8 0 1853285691 155 tcp_ack 0.00001 128 0x154e 192.168.90.4 0 796208667	148	ctg_big_data	0.00080	59	0xdcd4	192.168.2.8	4	1853285668	2D2D2D23
150 tcp_ack 0.00051 59 0xdcd5 192.168.2.8 0 1853285672 151 FMH7 0.01838 128 0x154d 192.168.90.4 19 796208648 0000001300000E49000B900107070864000000 152 tcp_ack 0.00112 59 0xdcd6 192.168.2.8 0 1853285672 153 FMH7 0.00005 59 0xdcd7 192.168.2.8 19 1853285672 0000001300000E46000B900107071008600B00 154 FIN 0.00000 59 0xdcd8 192.168.2.8 0 1853285691 155 tcp_ack 0.00001 128 0x154e 192.168.90.4 0 796208667	149	FMH7	0.12260	128	0x1548	192.168.90.4	19	796208629	0000001300000E46000B900107070864000000
151 FMH7 0.01838 128 0x154d 192.168.90.4 19 796208648 0000001300000E49000B900107070864000000 152 tcp_ack 0.00112 59 0xdcd6 192.168.2.8 0 1853285672 153 FMH7 0.00005 59 0xdcd7 192.168.2.8 19 1853285672 0000001300000E46000B900107071008600B00 154 FIN 0.00000 59 0xdcd8 192.168.2.8 0 1853285691 155 tcp_ack 0.00001 128 0x154e 192.168.90.4 0 796208667	150	tcp_ack	0.00051	59	0xdcd5	192.168.2.8	Θ	1853285672	
152 tcp_ack 0.00112 59 0xdcd6 192.168.2.8 0 1853285672 153 FMH7 0.00005 59 0xdcd7 192.168.2.8 19 1853285672 0000001300000E46000B900107071008600B00 154 FIN 0.00000 59 0xdcd8 192.168.2.8 0 1853285691 155 tcp_ack 0.00001 128 0x154e 192.168.90.4 0 796208667	151	FMH7	0.01838	128	0x154d	192.168.90.4	19	796208648	0000001300000E49000B900107070864000000
153 FMH7 0.00005 59 0xdcd7 192.168.2.8 19 1853285672 0000001300000E46000B900107071008600B00 154 FIN 0.00000 59 0xdcd8 192.168.2.8 0 1853285691 155 tcp_ack 0.00001 128 0x154e 192.168.90.4 0 796208667	152	tcp_ack	0.00112	59	0xdcd6	192.168.2.8	Θ	1853285672	
154 FIN 0.00000 59 0xdcd8 192.168.2.8 0 1853285691 155 tcp_ack 0.00001 128 0x154e 192.168.90.4 0 796208667	153	FMH7	0.00005	59	0xdcd7	192.168.2.8	19	1853285672	0000001300000E46000B900107071008600B00
155 tcp_ack 0.00001 128 0x154e 192.168.90.4 0 796208667	154	FIN	0.00000	59	0xdcd8	192.168.2.8	Θ	1853285691	
	155	tcp_ack	0.00001	128	0x154e	192.168.90.4	Θ	796208667	
156 FMH7 0.01749 128 0x1556 192.168.90.4 19 796208667 0000001300000E4A000B900107070864000000	156	FMH7	0.01749	128	0x1556	192.168.90.4	19	796208667	0000001300000E4A000B900107070864000000
157 RST AIX 0.00104 59 0xdcdf 192.168.2.8 0 1853285692	157	RST AIX	0.00104	59	0xdcdf	192.168.2.8	Θ	1853285692	

Complete your sessions evaluation online at SHARE.org/AnaheimEval





Windows CICS Client ABENDs the transaction SHAR

... sends FMH7 with SNA sense 08640000

No whazzin Time TTL ip.id Source tcp_len tcp_seq data 50 ctg_start_tx 0.55268 128 0x1490 192.168.90.4 821 796206192 0000033500000E46000B90A0270502FF0003D11 95 ctg_reply 0.59758 59 0xdbd3 192.168.2.8 1300 1853253132 00007A0400000E460003900179F812F207430E0 149 FMH7 3.86227 128 0x1548 192.168.2.8 19 796208629 0000001300000E460003900179F812F207430E0 153 FMH7 0.02007 59 0xdcd7 192.168.2.8 19 796208629 0000001300000E460003900170F812F207430E0 (III III Src CheckPoi_f7:90:14 (00:12:c1:f7:90:14), Dst: Vmware_a6:40:3c (00:50:56:a6:40:3c)) b Ethernet II, Src: CheckPoi_f7:90:14 (00:12:c1:f7:90:14), Dst: Vmware_a6:40:3c (00:50:56:a6:40:3c)) b Transmission Control Protocol, Src: Port: 8497 (8497), Dst Port: 55329 (55329), Seq: 1853253132, Ack: 79620701:) Data (1300 bytes) ILength: 1300] .9 .9 .9 .9 0003		data.data[6:2] eq 0	e46	✓ Exp	ression Clear Apply			
50 ctg_start_tx 0.55268 128 0x1490 192.168.90. 821 796206192 0000033500000E46000B90A0270502FF0003D1 95 ctg_reply 0.59758 59 0xdbd3 192.168.2.8 1300 1853253132 00007A0400000E46000B90A0270502FF0003D1 149 FMH7 3.86227 128 0x1548 192.168.90. 19 796208629 000001300000E46000B90017070864000000 153 FMH7 0.02007 59 0xdcd7 192.168.2.8 19 1853285672 0000001300000E46000B9001707100864000000 153 FMH7 0.02007 59 0xdcd7 192.168.2.8 19 1853285672 0000001300000E46000B9001707100864000000 153 FMH7 0.02007 59 0xdcd7 192.168.2.8 19 1853285672 0000001300000E46000B9001707100864000000 153 FMH7 0.02007 59 0xdcd7 192.168.2.8 19 1853285672 0000001300000E46000B90017071008600B00 153 FMH7 0.02007 59 0xdcd7 192.168.2.8 192.168.90.43 (192.168.90.43) 122.168.20.130 192.168.90.43 192.168.90.43 192.168.90.43 192.168.90.43 192.168.90.43 192.168.90.43 192.168.90.43 192.168.90.43 192.168.90.43 192.168.90.43 192.168.9	No	whazzin	Time TTL ip.id	Source tcp_len	tcp.seq data			
95 ctg reply 0.59758 59 0xdbd3 192.168.2.8 1300 1853253132 00007A0400000E460003900179F812F207430E 149 FMH7 3.86227 128 0x1548 192.168.90.4 19 796208629 00000130000E46000890010707864000000 153 FMH7 0.02007 59 0xdcd7 192.168.2.8 19 185325572 00000130000E46000890010707864000000 153 FMH7 0.02007 59 0xdcd7 192.168.2.8 19 1853285672 00000130000E46008900107071086600800 (50) ctg_start_tx	0.55268 128 0x14	490 192.168.90.4 8	21 796206192 00000335000	000E46000B90A0270502FF0003D10		
149 FMH7 3.86227 128 0x1548 192.168.90.4 19 796208629 0000001300000E46000B900107070864000000 153 FMH7 0.02007 59 0xdcd7 192.168.2.8 19 1853285672 000000130000E46000B900107071086600B000 Image: Constraint of the state of the s	95	5 ctg_reply	0.59758 59 0xdb	od3 192.168.2.8 13	00 1853253132 00007A04000	000E460003900179F812F207430E0		
153 FMH7 0.02007 59 0xdcd7 192.168.2.8 19 1853285672 0000001300000E46000B90017071008660B00	149	FMH7	3.86227 128 0x15	548 192.168.90.4	19 796208629 00000013000	000E46000B900107070864000000		
✓ III > ▷ Frame 95 (1354 bytes on wire, 1354 bytes captured) > ▷ Ethernet II, Src: CheckPoi_f7:90:14 (00:12:c1:f7:90:14), Dst: Vmware_a6:40:3c (00:50:56:a6:40:3c) ▷ Internet Protocol, Src: 192.168.2.8 (192.168.2.8), Dst: 192.168.90.43 (192.168.90.43) ▷ Transmission Control Protocol, Src Port: 8497 (8497), Dst Port: 55329 (55329), Seq: 1853253132, Ack: 79620701: ▽ Data: 00007A0400000E460003900179F812F207430E0200000079 [Length: 1300] ✓ III Ø030 80 39 7f 05 00 00 00 00 7a 04 00 00 e46 00 03 .9 Ø040 90 01 79 f8 12 f2 07 43 0e 02 00 00 00 79 ed 06 .yCy. Ø050 30 30 31 50 4f 53 20 02 02 02 02 02 02 02 02 02 02 02 02 0001P0S Ø060 20 20 4c 45 53 45 4e 20 20 20 20 20 20 20 20 20 20 20 LESEN Ø070 20 20 47 45 54 2d 44 45 41 4c 44 41 54 41 20 20 GET-DE ALDATA	153	B FMH7	0.02007 59 0xdo	d7 192.168.2.8	19 1853285672 00000013000	000E46000B900107071008600B00		
▷ Frame 95 (1354 bytes on wire, 1354 bytes captured) ▷ Ethernet II, Src: CheckPoi_f7:90:14 (00:12:c1:f7:90:14), Dst: Vmware_a6:40:3c (00:50:56:a6:40:3c) ▷ Internet Protocol, Src: 192.168.2.8 (192.168.2.8), Dst: 192.168.90.43 (192.168.90.43) ▷ Transmission Control Protocol, Src Port: 8497 (8497), Dst Port: 55329 (55329), Seq: 1853253132, Ack: 79620701: ▽ Data (1300 bytes) □ Data: 00007A0400000E460003900179F812F207430E0200000079 [Length: 1300] ✓	<	Ш				>		
▷ Ethernet II, Src: CheckPoi_f7:90:14 (00:12:c1:f7:90:14), Dst: Vmware_a6:40:3c (00:50:56:a6:40:3c) ▷ Internet Protocol, Src: 192.168.2.8 (192.168.2.8), Dst: 192.168.90.43 (192.168.90.43) ▷ Transmission Control Protocol, Src Port: 8497 (8497), Dst Port: 55329 (55329), Seq: 1853253132, Ack: 79620701: ♡ Data (1300 bytes) □ Data: 00007A0400000E460003900179F812F207430E0200000079 [Length: 1300] ○ 179 f8 12 f2 07 43 0e 02 00 00 00 79 ed 06 ○ 000 179 f8 12 f2 07 43 0e 02 00 00 00 79 ed 06 ○ 000 179 f8 12 f2 07 43 0e 02 00 00 079 ed 06 ○ 0001POS 0050 30 30 31 50 4f 53 20 20 20 20 20 20 20 20 20 20 ○ 0001POS 0060 20 20 20 4c 45 53 45 4e 20 20 20 20 20 20 20 20 20 20 20 20 20 ○ Data ESEN 0070 20 20 47 45 54 2d 44 45 41 4c 44 41 54 41 20 20	▶ Fra	ame 95 (1354 byt	tes on wire, 1354	bytes captured)				
▷ Internet Protocol, Src: 192.168.2.8 (192.168.2.8), Dst: 192.168.90.43 (192.168.90.43) ▷ Transmission Control Protocol, Src Port: 8497 (8497), Dst Port: 55329 (55329), Seq: 1853253132, Ack: 79620701; ♡ Data (1300 bytes) □ Data: 00007A0400000E460003900179F812F207430E0200000079 [Length: 1300] ○ 0179 f8 12 f2 07 43 0e 02 00 00 00 79 ed 06 ○ 000 79 ed 06 ○ 01 79 f8 12 f2 07 43 0e 02 00 00 00 79 ed 06 ○ 000 30 30 31 50 4f 53 20 20 20 20 20 20 20 20 20 20 20 20 20	▷ Eth	hernet II, Src:	CheckPoi f7:90:14	(00:12:c1:f7:90:14),	Dst: Vmware a6:40:3c (00)	50:56:a6:40:3c)		
▶ Transmission Control Protocol, Src Port: 8497 (8497), Dst Port: 55329 (55329), Seq: 1853253132, Ack: 79620701. ▼ Data (1300 bytes) □ Data: 00007A0400000E460003900179F812F207430E020000079 [Length: 1300] (0030 80 39 7f 05 00 00 01 79 78 12 12 0050 30 </td <td>▷ Int</td> <td>ternet Protocol,</td> <td>, Src: 192.168.2.8</td> <td>(192.168.2.8), Dst: 1</td> <td>92.168.90.43 (192.168.90</td> <td>43)</td>	▷ Int	ternet Protocol,	, Src: 192.168.2.8	(192.168.2.8), Dst: 1	92.168.90.43 (192.168.90	43)		
✓ Data (1300 bytes) Data: 00007A0400000E460003900179F812F207430E020000079 [Length: 1300] ✓ III 0030 80 39 7f 05 00 00 00 00 7a 04 00 00 0e 46 00 03 0040 90 01 79 f8 12 f2 07 43 0e 02 00 00 00 79 ed 06 0050 30 30 31 50 4f 53 20 20 20 20 20 20 20 20 20 20 20 20 20 0060 20 20 20 4c 45 53 45 4e 20 20 20 20 20 20 20 20 20 20 20 20 0070 20 20 47 45 54 2d 44 45 41 4c 44 41 54 41 20 20	D Tra	ansmission Cont	rol Protocol, Src (Port: 8497 (8497), Dst	Port: 55329 (55329), See	<mark>: 1853253132, Ack: 796207013</mark>		
Data: 00007A0400000E460003900179F812F207430E020000079 [Length: 1300] Image: Colspan="2">Image: Colspan="2" (Colspan="2") (Colspan="2") Image: Colspan="2">Image: Colspan="2" (Colspan="2") (Colspan="2") Image: Colspan="2">Image: Colspan="2" (Colspan="2") Image: Colspan="2">Image: Colspan="2">Image: Colspan="2" (Colspan="2") Image: Colspan="2" (Colspan="2") Image: Colspan="2") Image: Colspan="2">Image: Colspan="2" (Colspan="2") Image: Colspan="2") Image: Colspan="2" (Colspan="2") <th (colspan="2")="" <="" colspan="2" td=""><td>⊽ Dat</td><td>ta (1300 bytes)</td><td></td><td></td><td></td><td></td></th>	<td>⊽ Dat</td> <td>ta (1300 bytes)</td> <td></td> <td></td> <td></td> <td></td>		⊽ Dat	ta (1300 bytes)				
[Length: 1300] Image: Colspan="5">Image: Colspan="5" Image: Colspan="	[Data: 00007A040	0000E460003900179F	812F207430E0200000079				
Image: Non-Sector Non-Se		[Length: 1300]						
0030 80 39 7f 05 00 <	<			III		>		
0040 90 01 79 f8 12 f2 07 43 0e 02 00 00 79 ed 06 y C y 0050 30 30 31 50 4f 53 20 20 20 20 20 0001P0S 0060 20 20 20 20 20 20 20 LESEN 0070 20 20 47 45 54 41 44 41 20 20 GET-DE ALDATA								
0050 30 30 31 50 4f 53 20 20 20 20 20 20 20 20 20 0001P0S 0060 20 20 20 4c 45 53 45 4e 20 20 20 20 20 20 20 20 LESEN 0070 20 20 47 45 54 2d 44 45 41 4c 44 41 54 41 20 20 GET-DE ALDATA	0030	80 39 7f 05 00	00 00 00 7a 04 0	0 00 0e 46 00 03 .9.				
0060 20 20 20 4c 45 53 45 4e 20 20 20 20 20 20 20 20 LESEN 0070 20 20 47 45 54 2d 44 45 41 4c 44 41 54 41 20 20 GET-DE ALDATA	0030 0040	80 39 7f 05 00 90 01 79 f8 12	<mark>00</mark> 000007a040 f207430e020	0 00 0e 46 00 03 .9 0 00 00 79 ed 06 . .y	F /Cy			
0070 20 20 47 45 54 2d 44 45 41 4c 44 41 54 41 20 20 GET-DE ALDATA	0030 0040 0050	80 39 7f 05 00 90 01 79 f8 12 30 30 30 31 50	00 00 00 7a 04 0 f2 07 43 0e 02 0 4f 53 20 20 20 2	0 00 0e 46 00 03 .9 0 00 00 79 ed 06 0 20 20 20 20 20 20 000	cy 01POS			
	0030 0040 0050 0060	80 39 7f 05 00 90 01 79 f8 12 30 30 30 31 50 20 20 20 4c 45	00 00 00 7a 04 0 f2 07 43 0e 02 0 4f 53 20 20 20 2 53 45 4e 20 20 2	0 00 0e 46 00 03 .9 0 00 00 79 ed 06 0 20 20 20 20 20 000 0 20 20 20 20 20 20	F yCy p1POS LESEN			
0080 20 20 20 20 20 20 20 20 20 20 20 20 20	0030 0040 0050 0060 0070	80 39 7f 05 00 90 01 79 f8 12 30 30 30 31 50 20 20 20 4c 45 20 20 47 45 54	00 00 00 7a 04 0 f2 07 43 0e 02 0 4f 53 20 20 20 2 53 45 4e 20 20 2 2d 44 45 41 4c 4	0 00 0e 46 00 03 .9 0 00 00 79 ed 06 0 20 20 20 20 20 00 0 20 20 20 20 20 20 4 41 54 41 20 20				
0090 47 45 54 48 45 58 54 20 20 20 20 20 20 20 20 20 0 GEINEXT	0030 0040 0050 0060 0070 0080	80 39 7f 05 00 90 01 79 f8 12 30 30 30 31 50 20 20 20 4c 45 20 20 47 45 54 20 20 20 20 20	00 00 00 7a 04 0 f2 07 43 0e 02 0 4f 53 20 20 20 2 53 45 4e 20 20 2 2d 44 45 41 4c 4 20 20 20 20 2 2	0 00 0e 46 00 03 .9 0 00 00 79 ed 06 0 20 20 20 20 20 20 0 20 20 20 20 20 20 4 41 54 41 20 20 0 20 20 20 20 20 20 0 20 20 20 20 20 20				
O Data (data data) 1300 by Backets: 157 Displayed: 4 Marked: 0	0030 0040 0050 0060 0070 0080 0090	80 39 7f 05 00 90 01 79 f8 12 30 30 30 31 50 20 20 20 4c 45 20 20 47 45 54 20 20 20 20 20 20 47 45 54 4e 45 20 20 20 20 20 20	00 00 00 7a 04 0 f2 07 43 0e 02 0 4f 53 20 20 20 2 53 45 4e 20 20 2 2d 44 45 41 4c 4 20 20 20 20 2 2 58 54 20 20 2 2 20 20 2 2 2 2	0 00 0e 46 00 03 .9 0 00 00 79 ed 06 0 20 20 20 20 20 00 0 20 20 20 20 20 00 0 20 20 20 20 20 00 0 20 20 20 20 20 20 4 41 54 41 20 20 0 0 20 20 20 20 20 0 0 20 20 20 20 20 0 0 20 20 20 20 20 0 0 20 20 20 20 20 GET 0 20 20 20 31 30				
	0030 0040 0050 0060 0070 0080 0090 00a0	80 39 7f 05 00 90 01 79 f8 12 30 30 30 31 50 20 20 20 4c 45 20 20 20 47 45 54 20 20 20 20 20 20 47 45 54 4e 45 20 20 20 20 20 47 45 54 4e 45 20 20 20 20 20	00 00 00 7a 04 0 f2 07 43 0e 02 0 4f 53 20 20 20 2 53 45 4e 20 20 2 2d 44 45 41 4c 4 20 20 20 20 20 2 58 54 20 20 2 2 20 20 20 2 2 2 20 20 2 2 2 2 58 54 20 2 2 2 20 20 2 2 2 2 2	0 00 0e 46 00 03 .9 0 00 00 79 ed 06 0 20 20 20 20 00 0 20 20 20 20 00 0 20 20 20 20 00 0 20 20 20 20 20 4 41 54 41 20 20 0 0 20 20 20 20 20 0 0 20 20 20 20 20 0 0 20 20 20 20 20 GET 0 20 20 20 20 31 30		Drofile: cta		
CUADE	0030 0040 0050 0060 0070 0080 0090 0090 00a0	80 39 7f 05 00 90 01 79 f8 12 30 30 30 31 50 20 20 20 4c 45 20 20 20 4c 45 20 20 20 20 20 47 45 54 4e 45 20 20 20 20 20 20 47 45 54 4e 45 20 20 20 20 20 20 4 45 54 4e 45 20 20 20 20 20 20 a (data.data), 1300 b 54 54 54	00 00 00 7a 04 0 f2 07 43 0e 02 0 4f 53 20 20 20 2 53 45 4e 20 20 2 2d 44 45 41 4c 4 20 20 20 20 20 2 58 54 20 20 2 2 20 20 20 2 2 2 20 20 2 2 2 2 20 20 2 2 2 2 20 2 2 2 2 2 2 20 2 2 2 2 2 2 2 20 2 2 2 2 2 2 2 20 2 2 2 2 2 2 2 2 20 2 2 2 2 2 2 2 2 </td <td>0 00 0e 46 00 03 .9 0 00 00 79 ed 06 0 20 20 20 20 20 00 0 20 20 20 20 20 00 0 20 20 20 20 20 00 0 20 20 20 20 20 00 4 41 54 41 20 20 0 0 0 20 20 20 20 20 20 0 0 0 20 20 20 20 20 GET 0 0 20 20 20 31 30 0 0 Iayed: 4 Marked: 0</td> <td></td> <td>Profile: ctg</td>	0 00 0e 46 00 03 .9 0 00 00 79 ed 06 0 20 20 20 20 20 00 0 20 20 20 20 20 00 0 20 20 20 20 20 00 0 20 20 20 20 20 00 4 41 54 41 20 20 0 0 0 20 20 20 20 20 20 0 0 0 20 20 20 20 20 GET 0 0 20 20 20 31 30 0 0 Iayed: 4 Marked: 0		Profile: ctg		

Complete your sessions evaluation online at SHARE.org/AnaheimEval

•...• in Anaheim 2012

ctg profile

dfilters



Expression...



"ctg_up_down" tcp.flags.syn==1 or tcp.flags.fin==1 or tcp.flags.reset==1 or data.data contains 0b:9001:0707 or (data.data[13:3] eq 05:02:ff and data.data[22:4] eq c3c3:c9d5) or data.data[12:4] eq 0034:12ff "3-way_handshake" tcp.flags.syn==1 or (tcp.ack==1 and tcp.seq==1 and tcp.len==0 and !tcp.analysis.window_update) "delay" frame.time_delta gt 0.02 "p0f fingerprints" tcp.flags.syn==1 or tcp.flags.reset==1 "ctg_response GDS12F2" data.data contains 12f2 and !data.data contains 0502:ff "ctg_request FMH5 ALLOCATE" data.data contains 0b:90:a0 and data.data contains 0502:ff "ctg_req_resp filter on SNA SNF " data.data[6:2] eq 0e46 "ctg_init FMH5 TP:CCIN" (data.data[13:3] eq 05:02:ff and data.data[22:4] eq c3c3:c9d5) or data.data[12:4] eq 0034:12ff "ctg_heartbeat 'PING'" (data.data contains 013a:12f2 or data.data contains 0502:ff) && data.data contains 2020:5049:4e47 "ctg_large_data : No TG at offs 0 in segment" tcp.len gt 0 and !data.data[0:2] eq 0000 and !data.data[4:2] eq 0000 "ctg_req_rsp" data.data contains 0b:9000 or data.data contains 03:9001 or data.data contains 0b:9001

Filter string: data.data[6:2] eq 0e46

•...• in Anaheim

ctg profile

colorfilters

λ Wireshark: Coloring Rules - Profile: ctg _ 🗆 🗙 Edit Filter Order List is processed in order until match is found New ~ Name String SYN ZOS tcp.flags.syn == 1 and ip.ttl le 64 and tcp.window_size eq 65535 Edit... Up SYN WinXp tcp.flags.syn == 1 and ip.ttl gt 64 and ip.ttl le 128 and tcp.window size eg 65535 tcp.flags.syn == 1 and ip.ttl gt 64 and ip.ttl le 128 and tcp.window size eg 8192 and tcp.options contains (SYN Win7+ Enable tcp.flags.syn == 1 and ip.ttl le 64 and tcp.window_size eq 49232 SYN Solaris TCP RST tcp.flags.reset eq 1 Disable ctg CCIN (data.data[13:3] eq 05:02:ff and data.data[22:4] eq c3c3:c9d5) or data.data[12:4] eq 0034:12ff FMH7 data.data contains 000b:9001:0707 Move selected filter Delete ctg heartbeat (data.data contains 013a:12f2 or data.data contains 0502:ff) and data.data contains 2020:5049:4e47 up or down data.data[8:4] eq 0003:9001 ctg_reply Manage ctg_start_tx data.data contains 0b:90:a0 and data.data contains 0502:ff SSL Handshake data.data[0:3] eq 16:03:01 or ssl.handshake or data.data[0:3] eq 14:03:01 or data.data[0:3] eq 80:1f:01 Import... tcp.len gt 0 and !data.data[0:2] eg 0000 and !data.data[4:2] eg 0000 ctg big data delay 20 ms frame.time_delta_gt 0.02 Export... tcp.flags.syn==1 or (tcp.seq==1 and tcp.ack==1 and tcp.len==0) Down 3-way-HS tcp.flags.fin==1 and ip.ttl <= 60 FIN ¥ Clear **FIN Win** ten flags fin==1 and in ttl > 100 and in ttl<=128 111 > Apply OK Help Cancel SHARE in Anaheim

15 Complete your sessions evaluation online at SHARE.org/AnaheimEval



ctg profile

preferences

Λ				Wireshark: Preferences - Profile: ctg
V	User Interface	ſ	Columns	
	Layout		[1	The first list entry will be displayed as the leftmost column - Dr
	Columns		Title	Field type
	Font		No.	Number
	Colors		whazzin	Custom (frame.coloring_rule.name)
	Capture		Time	Time (format as specified)
	Printing		TTL	Custom (ip.ttl)
	Name Resolution		ip.id	Custom (ip.id)
	Statistics		Source	Net src addr (resolved)
⊳	Protocols		tcp_len	Custom (tcp.len)
			tcp.seq	Custom (tcp.seq)
			data	Custom (data.data)
			Info	Information
			tcp_ack	Custom (tcp.ack)
			nxt.seq	Custom (tcp.nxtseq)
			delta_time	Custom (frame.time_delta)
			tcp_ws	Custom (tcp.window_size)







Thank You for your time!



