Wireshark Version 2 Setup and Usage For DeviceMaster Tracing

Install Wireshark using the defaults (include pcap when requested) and launch it. Wireshark may be downloaded using this link:

https://www.wireshark.org/download.html

he Wireshark Network Analyzer		- 🗆 ×		The Wireshark Network Analyzer				-	- 🗆	×
Edit View Go Capture Analyze Statistics Telephony	<u>W</u> ireless <u>T</u> ools <u>H</u> elp		Eil	Edit View Go Capture	<u>Analyze</u> <u>Statistics</u>	Telephony <u>W</u> ireless	<u>T</u> ools <u>H</u> elp			
I 🖉 💿 📙 🛱 🖉 🔍 🗢 🗢 🕾 T 🕹 🚍 🗐 (Ð, Q, Q, 🎹		<u> </u>	Сору	•	📃 📃 Q. Q.	₽, Ⅲ			
ply a display filter <ctrl-></ctrl->		Expression	+	Ar 🥱 Eind Packet	Ctrl+F				- Expressio	n
				Find Ne <u>x</u> t	Ctrl+N					
				Find Previous	Ctrl+B					
Welcome to Wireshark				Mark/Unmark Packet	Ctrl+M					
Capture				Mark All Displayed	Ctrl+Shift+M					
		•		Unmark All Displayed	Ctrl+Alt+M					-
				Next Mark	Ctrl+Shift+N					
Local Area Connection* 2	. No			Previous Mark	Ctrl+Shift+B					-
Wi-Fi				Ignore/Unignore Packet	Ctrl+D					_
				Ignore All Displayed	Ctrl+Shift+D					
				Unignore All Displayed	Ctrl+Alt+D					
				Set/Unset Time Reference	Ctrl+T					
				Unset All Time References	Ctrl+Alt+T					
				Next Time Reference	Ctrl+Alt+N					
				Previous Time Reference	Ctrl+Alt+B					
Learn				Time Shift	Ctrl+Shift+T					
User's Guide · Wiki · Questions and Answers · Mailing Lis	ts			Packet Comment		• Mailing Lists				
You are running Wireshark 2.0.2 (v2.0.2-0-ga 16e 22e from master - 2.0). Yo	u receive automatic updates.			Configuration Profiles	Ctrl+Shift+A	naster-2.0). You receive	e automatic updates			
				Preferences	Ctrl+Shift+P					
Ready to load or capture	No Packets	Profile: Default	. 2	Ready to load or capture			No Packets		Profile: D	efaul

Once installed click the "Edit" drop down menu. Select Preferences.



From the drop down list select your adapter. This may simply be 'Ethernet'





Wireshark · Preference	es	?	×
DVMRP EDONKEY ELF ENIP ENTTEC EPL ERF ERSPAN ESP ESS Etch Ethernet EVRC EVRC EVRC EVRC EVRC EVRC FC FC FC FC FC FC FC FC FDDI Fibre Channe File-PCAPNC FIX FMP	Ethernet Assume short frames which include a trailer contain padding Hixed ethernet trailer length Assume packets have FCS Assume packets have FCS Addate the Ethernet checksum if possible Interpret as FireWall-1 monitor file These are the conditions to match a payload against in order to determine if this is a CGSDS (Consultative Committee for Space Data Systems) packet within an 802.3 packet. A packet is considered as a possible CCSDS packet only if CCSDS Consultative Committee for Space Data Systems) packet only if CCSDS Consultative Committee for Space Data Systems) packet only if CCSDS System in header matches payload size CCSDS Version if is zero CCSDS Spare bit is deared	Held	

Select 'Ethernet'.

Clear the check mark on 'Validate the Ethernet checksum if possible'. Click OK.

	Wiresha	rk										-		×
<u>F</u> ile	Edit	<u>V</u> iev	v <u>G</u> o <u>M</u> ain To	<u>C</u> apture olbar	<u>A</u> nalyze	<u>S</u> tatistics	Telep	hony	<u>W</u> ireless ⊕	<u>T</u> ools ©, Ⅲ	<u>H</u> elp			
	Apply a d	~ ~	<u>F</u> ilter Too Wire <u>l</u> ess <u>S</u> tatus Ba	olbar Toolbar ar								 	Expression	n +
	We Caj	× × ×	Packet <u>L</u> Packet <u>D</u> Packet <u>B</u>	ist Jetails Lytes									•]
	Loca Ethe		<u>T</u> ime Dis Name R	play Form	nat		۰ ۲		m		m	 	M	
	WI-F		<u>Z</u> oom				•							
			Expand S	Subtrees		Shift+Ri	ght	L						
			Expand /			Ctrl+Rig	ht +	L						
			Colorize	Packet Lis	÷									
		_	Coloring	Rules				1						
	Lor		Colorize	Conversa	tion		•							
	Usei	<u>**</u>	Resize C	olumns		Ctrl+Shi	ft+R	iilina Li	sts					
			Internals				•							
			Show Pa	cket in Ne	w <u>W</u> indow	(L						
Z	Ready	G	<u>R</u> eload			Ctrl+R				No Pac	kets		Profile: De	alt

From the 'View' drop down menu select 'Coloring Rules'

🧲 Wireshark · Coloring Rules · Defau	lt ?	×	Wireshark · Coloring Rules · Default	?
Name	Filter	^	Name F	ilter
✓ Bad TCP	tcp.analysis.flags && !tcp.analysis.window_u	ipc	🗹 Bad TCP to	cp.analysis.flags && !tcp.analysis.window_u
HSRP State Change	hsrp.state != 8 && hsrp.state != 16		✓ HSRP State Change h	srp.state != 8 && hsrp.state != 16
🗹 Spanning Tree Topology Change	e stp.type == 0x80		🗹 Spanning Tree Topology Change s	tp.type == 0x80
OSPF State Change	ospf.msg != 1		OSPF State Change o	spf.msg != 1
ICMP errors	icmp.type eq 3 icmp.type eq 4 icmp.type	eq	✓ ICMP errors id	:mp.type eq 3 icmp.type eq 4 icmp.type
ARP ARP	arp		ARP a	rp
ICMP	icmp icmpv6		ICMP id	:mp icmpvб
TCP RST	tcp.flags.reset eq 1		🗹 TCP RST 👘 te	cp.flags.reset eq 1
SCTP ABORT	sctp.chunk_type eq ABORT		SCTP ABORT si	ctp.chunk_type eq ABORT
TTL low or unexpected	(! ip.dst == 224.0.0.0/4 && ip.ttl < 5 && !pin	n 8	✓ TTL low or unexpected (! ip.dst == 224.0.0.0/4 && ip.ttl < 5 && !pir
Checksum Errors	eth.fcs_bad==1 ip.checksum_bad==1 tcp	o.cl	Checksum Errors e	th.fcs_bad==1 ip.checksum_bad==1 tcj
SMB	smb nbss nbns nbipx ipxsap netbios		SMB si	mb nbss nbns nbipx ipxsap netbios
HTTP HTTP	http tcp.port == 80 http2		HTTP h	ttp tcp.port == 80 http2
IPX IPX	ipx spx		IPX ip	ox spx
DCERPC	dcerpc		DCERPC d	cerpc
🗹 Routing	hsrp eigrp ospf bgp cdp vrrp carp	ll g	Routing h	srp eigrp ospf bgp cdp vrrp carp
TCP SYN/FIN	tcp.flags & 0x02 tcp.flags.fin == 1	~	TCP SYN/FIN to	cp.flags & 0x02 tcp.flags.fin == 1
	±	>		
Double click to edit, Drag to move, Rules are p	rocessed in order until a match is found,		Double click to edit, Drag to move, Rules are proce	essed in order until a match is found.
+ - 12			+ - Po Foreground	Background
OK Cano	el Import Export Help	Þ	OK Cancel	Import Export Hel

Select Checksum Errors and clear the check mark and then click OK

4 v	Viresha	ark													-		×
Eile	Edit	View	Go	Cap	ture	Analyze	Statistic	cs Te	elephony	Wireles	s <u>T</u> o	ols H	elp				
()		۲	010	۲	<u>O</u> pti	ons	-	Ctrl+K		0,0	0, 3	E					
Ap	ply a d	isplay f	ilter <	Â.	Start			Ctrl+E						-	T E	xpression	+
					Stop			Ctrl+E							_		
				đ	<u>R</u> est	art		Ctrl+R	t I								
	We	lcome	to Wir		Capt	ture <u>F</u> ilters											
	Car	otur	e		Refr	esh Interfa	ces	F5									
	uein	on this f	 Alter: []	Ent	ter a c	anture filter								 		•	l
			<u> </u>														-
	Wi-F	7												 			
	Lea	arin r's Guir	de · ·	Wiki	· Qu	estions a	nd Answ	ers '	Mailing	Lists							

Select the "Capture drop down menu and select 'Options'

This opens the optional file save rules.

Click the 'Output tab. You may enter a permanent file save name for a single file with no limit to the file size.

You may elect to save to multiple files based on either time or size. A new file will be created as the time period is reached or the file size limit has been reached. If the trace will run for prolonged periods, this option should be selected. A 1000 kilobyte file is recommended. Only the file showing the error would then need be provided to Comtrol.

A ring buffer may also be selected which limits the number of partial files created. When the ring number has been reached, it will automatically begin over writing in the first file.

In normal circumstances Comtrol will request a Wireshark trace with no filtering taking place. In this case leave the 'using this filter' blank as it will not be used.

Should Comtrol ask for a filtered trace the type of filter will depend on the way the Comtrol DeviceMaster driver is configured and how many DeviceMaster units are to be traced.

📕 TH	ne Wiresh	ark N	etwor	k Analyz	er												-		\times
ile	<u>E</u> dit <u>V</u> i	ew	<u>G</u> o	<u>C</u> apture	e <u>A</u> r	nalyze	<u>S</u> tatisti	ics	Telep	hony	W	ireless	Ī	ols	<u>H</u> elp				
[1 🖉 🖸		010	XC	9		> \$ T	î.	₽.		Ð	Q	Ξ,	E.					
App	ply a displa	ay filte	r <	Ctrl-/>														Expression.	. •
	Welco	me to	Wire	eshark															
	Cant	ire																	
	capu															 			
	using th	ns filte	er: 🚺	ether p	roto U	x11fe a	nd ether	host	t 00:c0	:4e:08:	:00:2	a						× •	
	Local A	rea Co	onnec	tion* 2 _												 			
	Etherne	t		-					······			h				 -Mr-		~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~	
	Wi-Fi																		
	Learr	1																	
	User's (Guide	÷ v	Viki ·	Quest	tions a	nd Answ	ers	÷ M	ailing	List	5							
	You are n	unning) Wire:	shark 2.0	.2 (v2	.0.2-0-g	a16e22e	fron	m masti	er-2.0)	. You	receiv	e auto	omati	: updates				
19	Read	v to lo	ad or i	ranture									II No	Pad	rets		11	Profile: Def	ault

To trace a single DeviceMaster operated in MAC Mode enter: ether proto 0x11fe and ether host 00:c0:4e:xx:yy:zz Replacing xx:yy:zz with the actual MAC address of the DeviceMaster.

To trace all DeviceMaster units operating in MAC Mode enter: ether proto 0x11fe

To trace a single DeviceMaster operating in IP Mode enter: host 192.168.250.250 Replace the sample IP address with the IP address of the DeviceMaster.

📕 The Wireshark Network Analyzer	:	Capturing from Ethernet (net 192.168.2.82)	- 🗆 X
<u>File Edit View Go</u> <u>Capture Analyze Statistics Telephony Wireless</u>	<u>T</u> ools <u>H</u> elp	File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help	
📶 🔳 🖉 💿 📴 💿 Options Ctrl+K	3. 理	🖉 📕 🧔 🛞 🛛 🔚 🛞 Options Ctrl+K 🛛 🗮 🔍 🔍 🔍 🐺	
Apply a display filter < A Start Ctrl+E	Expression	+ Apoly a disolar filter A Start Ctrl+E	Expression +
Stop Ctrl+E		No, Time Stop Ctrl+E on Protocol Leng	ith Info
Restart Ctri+R		2 8.661910 🥖 Restart Ctrl+R 5.255.255 UDP 1	72 4606 → 50091 Len=130
Welcome to Wir Capture Filters		3 10.237414 Capture <u>Filters</u> 5.255.255 UDP 1	72 4606 → 50092 Len=130
Capture		< Refresh Interfaces F5	>
Local Area Connection* 2 Ethernet Wi-Fi User's Guide · Wiki · Questions and Answers · Mailing Lists You are running Wireshark 2.0.2 (v2.0.2-0-ga 16e22e from master-2.0). You receive	automatic updates.	<pre>> Frame 1: 172 bytes on wire (1376 bits), 172 bytes captured (1376 bits) on > Ethernet II, Src: ComtrolC_08:00:2a (00:c0:4e:08:00:2a), Dst: Broadcast (f > Internet Protocol Version 4, Src: 192.168.282, Dst: 255.255.255 > User Datagram Protocol, Src Port: 4606 (4606), Dst Port: 50090 (50090) > Data (130 bytes) 0000 ff ff ff ff ff ff ff ff 00 c0 4e 08 00 2a 08 00 45 00 N*E. 0010 ff 11 fc 3a a0 08 a 13 dr a9 8d fd 53 fa 32 0030 78 08 00 ed 08 00 20 16 66 00 c2 4e 08 00 2a x N* 0040 100 2b 01 03 2c 04 00 4c 53 7c 2f 01 08 30 01N.* 0050 00 32 01 03 2d 01 01 2e 01 01 12 07 43 6f 6d 74cm. N* 0050 7 72 14 0d 4c 53 2d 4c 66 5c 66 06 33 03 2c 30 37 rNS-Link 10.07 0050 20 al a01 00 1b 01 00 12 70 4c 0a 80 25 18 04 #Cont 0050 ff ff 00 00 19 04 c0 a8 00 6f dic 04 c0 a8 02 52R. 0030 1d 04 ff ff 00 00 1e 04 c0 a8 00 fd 1c 04 c0 a8 02 52R.</pre>	interface 0 ^
Ready to load or capture	No Packets Profile: Defaul	t 🔐 Ethernet: Ethernet: ecapture in progress> Packets: 3 · Displa	ayed: 3 (100.0%) Profile: Default

Once the filters are set, Click the "Options" drop down menu and select 'Start'. When the trace is complete, Click the "Options" drop down menu and select 'Stop'

<u>Edit View Go</u> Capture	<u>Analyze</u>	tatistics Telephony <u>W</u> irele	is <u>T</u> ools <u>H</u>	elp			Save in:	E Desktop	~	🌀 🏂 📂 🛄	-
Open Copen Recent Merge Import from Hex Dump Close Save Sa File Set Export Specified Packets Export Packet Bytes Export Packet Bytes Export Packet Bytes	Ctrl+O Ctrl+W Ctrl+S Ctrl+Shift+S Ctrl+H	Image: Constraint of the state of	Protocol UDP UDP (1376 bits) :s: Broadcas :s: 255.255 :090 (50090)	Length Info 172 4606 ÷ 172 4606 ÷ 172 4606 ÷	<pre>Expressio 50091 Len=: 50092 Len=: e 0 ff:ff:ff)</pre>	h + ^ 30 30 × × × × ×	Quick access Desktop Libraries	Name	^ No items match your :	Date modified search.	
Export SsL Session Keys Export Objects Print Quit	> Ctrl+P Ctrl+Q	27 43 6f 6d 74 .2. 3 4d 61 73 74 65 rol 31 30 2e 30 37 r.1 a8 02 52 18 04 # 04 c0 a6 02 52 1 fd	Co .Dev iceMas IS-Li nk 10.	or mt te 07 R R			This PC	< File <u>n</u> ame: Save as <u>type</u> :	Casenumber12345 Wireshark/ pcapng (*,pcapng,*,	∽ pcapng.gz;* ∽	(

From the "File' drop down menu select 'Save As' Proved a file name such as your case number or your name Send the resultant file to your Comtrol Technical Support Representative

If the file is over 10Mb, contact your Technical Support Representative to find how to send the file to Comtrol using a password protected FTP upload site.