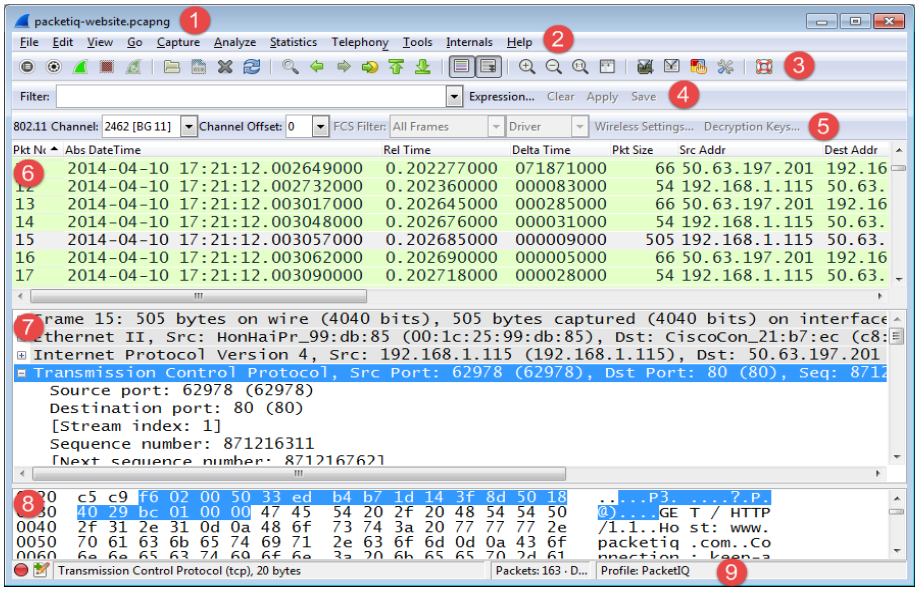
Wireshark Quick Reference

WS 101 - Features & Functions

PacketIQ®
Phone (321) 888-2288
Email: info@packetiq.com
www.packetiq.com

Wireshark User Interface Elements

Wireshark v1.10


packetiq-website.pcapng
1
File Edit View Go Capture Analyze Statistics Telephony Tools Internals Help
2
3
Filter:
Expression... Clear Apply Save
4
802.11 Channel: 2462 [BG 11]
Channel Offset: 0
FCS Filter: All Frames
Driver
Wireless Settings... Decryption Keys...
5
6
7
8
9

```
Pkt No  Abs DateTime                     Rel Time     Delta Time   Pkt Size  Src Addr        Dest Addr
        2014-04-10 17:21:12.002649000  0.202277000  071871000       66 50.63.197.201  192.16
12      2014-04-10 17:21:12.002732000  0.202360000  000083000       54 192.168.1.115  50.63.
13      2014-04-10 17:21:12.003017000  0.202645000  000285000       66 50.63.197.201  192.16
14      2014-04-10 17:21:12.003048000  0.202676000  000031000       54 192.168.1.115  50.63.
15      2014-04-10 17:21:12.003057000  0.202685000  000009000      505 192.168.1.115  50.63.
16      2014-04-10 17:21:12.003062000  0.202690000  000005000       66 50.63.197.201  192.16
17      2014-04-10 17:21:12.003090000  0.202718000  000028000       54 192.168.1.115  50.63.
```

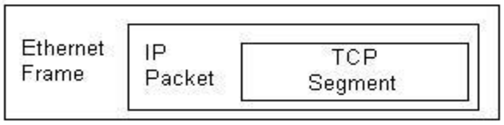
```
 Frame 15: 505 bytes on wire (4040 bits), 505 bytes captured (4040 bits) on interface
 Ethernet II, Src: HonHaiPr_99:db:85 (00:1c:25:99:db:85), Dst: CiscoCon_21:b7:ec (c8:
⊞ Internet Protocol Version 4, Src: 192.168.1.115 (192.168.1.115), Dst: 50.63.197.201
⊟ Transmission Control Protocol, Src Port: 62978 (62978), Dst Port: 80 (80), Seq: 8712
    Source port: 62978 (62978)
    Destination port: 80 (80)
    [Stream index: 1]
    Sequence number: 871216311
    [Next sequence number: 871216762]
```

```
0020  c5 c9 f6 02 00 50 33 ed  b4 b7 1d 14 3f 8d 50 18   .....P3. ....?.P.
0030  40 29 bc 01 00 00 47 45  54 20 2f 20 48 54 54 50   @)....GE T / HTTP
0040  2f 31 2e 31 0d 0a 48 6f  73 74 3a 20 77 77 77 2e   /1.1..Ho st: www.
0050  70 61 63 6b 65 74 69 71  2e 63 6f 6d 0d 0a 43 6f   packetiq .com..Co
0060  6e 6e 65 63 74 69 6f 6e  3a 20 6b 65 65 70 2d 61   nnection : keep-a
```

Transmission Control Protocol (tcp), 20 bytes | Packets: 163 · D... | Profile: PacketIQ

1. Title (trace file name)	**2. Menu**	**3. Main Toolbar**
4. Display Filter Toolbar	**5. Wireless Toolbar**	**6. Packet List Pane**
7. Packet Details Pane	**8. Packet Bytes Pane**	**9. Status Bar**

Frame vs Packet vs Segment



A **frame** is the entirety of the data package from the start of the Media Access Control (MAC) layer header (such as in an Ethernet header) to the end of the MAC trailer (Frame Check Sequence)(not always counted)

A **packet** is the payload of the frame minus the MAC header/trailer (Ethernet frame, for example)
To help remember the difference: a router strips off the previous Ethernet frame, internally routes the packet to the proper egress port, and wraps it in a new Ethernet Frame header/trailer (with different MAC layer addressing & FCS) for transmission

A **segment** is the payload contents following the TCP header - the application payload. The max size of this payload is the Maximum Segment Size (MSS)

IP and UDP packets carry *datagrams* vs *segments*

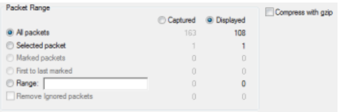
Features & Functions: File & Edit

File Menu > Open (Ctrl O) - browse for capture files

File > Open Recent - quick load of previous files
File > Merge - merge 2 or more capture files
File > Save As
File > File Set > List Files
Select from list of long-capture files
File > Export Specified Packets
Export filtered / displayed packets to a new file

Export Specified / Dissections Options:

Export Specified Packets



Packet Range

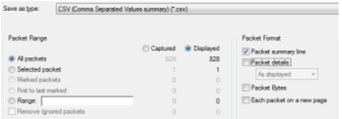
	○ Captured	● Displayed
● All packets	163	108
○ Selected packet	1	1
○ Marked packets	0	0
○ First to last marked	0	0
○ Range:	0	0
□ Remove Ignored packets	0	0

□ Compress with gzip

Captured or Displayed
.pcap or pcap.ng
Packet Range options
Range 4- or 4-63
Range 1,5,6-9

Export Packet Dissections

File >Export Packet Dissections
Export to .csv or other formats
File > Export Objects - save HTTP / DICOM / SMB/2 objects



Save as type: CSV (Comma Separated Values summary) (*.csv)

Packet Range

	○ Captured	● Displayed
● All packets	828	828
○ Selected packet	1	1
○ Marked packets	0	0
○ First to last marked	0	0
○ Range:	0	0
□ Remove Ignored packets	0	0

Packet Format
☑ Packet summary line
□ Packet details: As displayed
□ Packet Bytes
□ Each packet on a new page

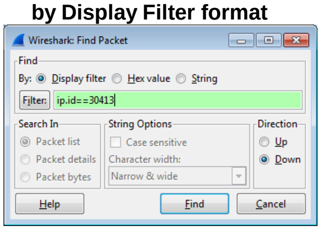
Marked / Ignored Pkts

Packet summary line: *all* columns exported

Enable 'Allow subdissector to reassemble TCP streams' in Preferences > Protocols > TCP

Edit Menu

Edit > Copy - copy contents from Packet Details fields (R-Click in Packet List or Details)
Edit > Find Packet (Ctrl-F)
by Display Filter format

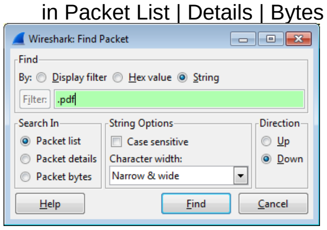


Find
By: ● Display filter ○ Hex value ○ String
Filter: ip.id==30413
Search In: ● Packet list ○ Packet details ○ Packet bytes
String Options: □ Case sensitive; Character width: Narrow & wide
Direction: ○ Up ● Down

by Hex value
(no '0x' needed) will find any occurrence of the value

Ctrl-N: Next
Ctrl-B: Prev

by String
in Packet List | Details | Bytes



Find
By: ○ Display filter ○ Hex value ● String
Filter: .pdf
Search In: ● Packet list ○ Packet details ○ Packet bytes
String Options: □ Case sensitive; Character width: Narrow & wide
Direction: ○ Up ● Down

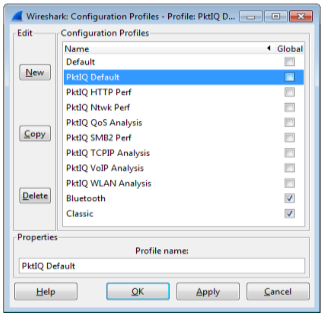
Edit > Mark | Unmark - highlights w/ Black background / White font - easier to find again
Edit > Ignore | Unignore - eliminate extraneous packets hard to eliminate w/ filters
Save trace w/o Ignored pkts - select 'Remove Ignored packets' in Export Specified Packets

Edit > Time Reference (Ctrl-T) - measure time from a specific packet to other pkts
Can be used multiple places - click Reload icon to reset - this is a temporary setting

Edit > Packet Comment (also **R-Click from Packet List**) - annotate packets with notes
Comments appear in Packet Details above the Frame meta data - highlighted in Green
Also listed in Analyze > Expert Info > Packet Comments tab. Must save trace as pcap-ng

Wireshark Configuration Profiles

Edit > Configuration Profiles…



Configuration Profiles

Name	Global
Default	□
PktIQ Default	□
PktIQ HTTP Perf	□
PktIQ Ntwk Perf	□
PktIQ QoS Analysis	□
PktIQ SMB2 Perf	□
PktIQ TCPIP Analysis	□
PktIQ VoIP Analysis	□
PktIQ WLAN Analysis	□
Bluetooth	☑
Classic	☑

Properties
Profile name: PktIQ Default

Create, copy, delete, or select custom configuration profiles

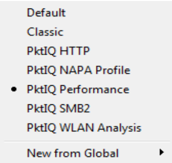
Wireshark settings are saved in profiles There are global and custom profiles, and you can create a set of custom profiles for multiple analysis environments

Custom profile files are found quickly by clicking:
Help > About Wireshark > Folders tab
Personal configuration > /profiles

Wireshark profile configuration files:

Capture Filters: *cfilters*	(these are all text-editable)
Coloring Rules: *colorfilters*	
Decode As settings: *decode_as_entries*	
Display Filters: *dfilters*	
Preferences: *preferences*	
GeoIP data files path: *geoip_db_paths*	(if configured)
Recent changes: *recent*	(do not modify)

preferences includes Filter Expression Button settings
You can ZIP a custom profile directory and share it
see also: **Global configuration** dir for default files



Default
Classic
PktIQ HTTP
PktIQ NAPA Profile
● PktIQ Performance
PktIQ SMB2
PktIQ WLAN Analysis
New from Global ▸

Click in the Profile section of the Status Bar to select/change profiles

R-Click in Profile section to select Manage Profiles

Features & Functions: Edit & View

Edit > Preferences (Ctrl-Shift-P) - Set/control all the settings for the current profile

View Menu

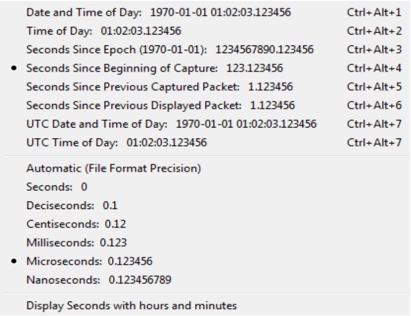
View > Time Display Format

These settings only affect / work with 'Time (format as specified)' field types

The two most useful time columns:

'Rel Time' column: progressive time
Seconds Since Beginning of Capture
Microseconds 0.123456

'Display Time' column: data flow times
Seconds Since Previous Displayed Packet
Microseconds 0.123456

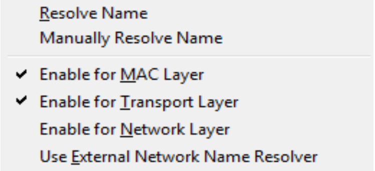

Date and Time of Day: 1970-01-01 01:02:03.123456 Ctrl+Alt+1
Time of Day: 01:02:03.123456 Ctrl+Alt+2
Seconds Since Epoch (1970-01-01): 1234567890.123456 Ctrl+Alt+3
• Seconds Since Beginning of Capture: 123.123456 Ctrl+Alt+4
Seconds Since Previous Captured Packet: 1.123456 Ctrl+Alt+5
Seconds Since Previous Displayed Packet: 1.123456 Ctrl+Alt+6
UTC Date and Time of Day: 1970-01-01 01:02:03.123456 Ctrl+Alt+7
UTC Time of Day: 01:02:03.123456 Ctrl+Alt+7
Automatic (File Format Precision)
Seconds: 0
Deciseconds: 0.1
Centiseconds: 0.12
Milliseconds: 0.123
• Microseconds: 0.123456
Nanoseconds: 0.123456789
Display Seconds with hours and minutes

View > Name Resolution

Resolve Name - one-time DNS lookup
Manually Resolve Name - enter hostname (temp)
MAC Layer - NIC manufacturers (enable)
Transport Layer - services by port #'s (enable)
Network Layer - IP addresses to host names
works with *Use External Network Name Resolver*, as follows:

Network Layer + External Resolver: does reverse PTR lookups - **creates DNS traffic**
Network Layer - External Resolver - use hosts file in Wireshark program or profile directory
Network Layer disabled +/- External Resolver - no IP to host name resolution

These are temp settings - use Preferences > Name Resolution to make permanent



View > Colorized Packet List - turn coloring rules / colorization on/off
View > Auto Scroll in Live Capture - On/Off (turn Off for busy captures)

Colors **Auto-Scroll**

View > Zoom In | Out | Normal (Ctrl + | Ctrl - | Ctrl =) - adjust font size

View > Resize All Columns (Ctrl-Shift-R) - auto-size Packet List columns **Resize**

View > Displayed Columns - lists all columns & allows turning the display of each On / Off

View > Expand Subtrees (Shift - Right)
View > Expand All (Ctrl - Right)
View > Collapse All (Ctrl - Left)

These controls affect the expansion / collapse of various levels of protocol headers to show / hide data fields in the Packet Details pane

View > Colorize Conversation (Ctrl - 1 thru 9 & 0) - *temporarily* make specific conversations more visible. Click on any packet in a conversation (in Packet List) & apply
View > Reset Coloring 1-10 (Ctrl Space) - removes conversation coloring

View > Coloring Rules - brings up Coloring Rules editor **Edit Coloring Rules**

View > Reload - reloads capture file / refreshes display **Reload**

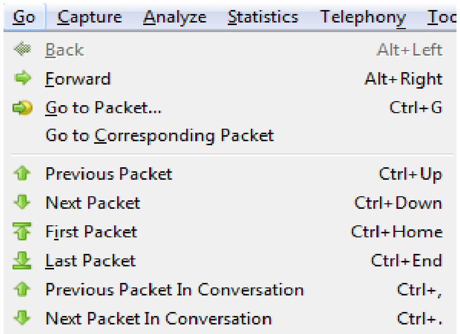
Go Menu

Back - Forward - move to / from packets in a reassembled PDU group

Go to Packet… - go to specific Pkt #

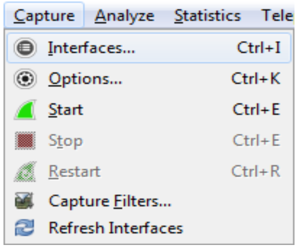
Go to Corresponding Packet - jump to a packet selected from a Reassembled PDU list in the Packet Details pane

Previous / Next Packet in Conversation move between packets in a conversation

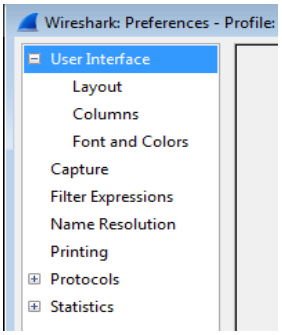

Go Capture Analyze Statistics Telephony Too
Back Alt+Left
Forward Alt+Right
Go to Packet... Ctrl+G
Go to Corresponding Packet
Previous Packet Ctrl+Up
Next Packet Ctrl+Down
First Packet Ctrl+Home
Last Packet Ctrl+End
Previous Packet In Conversation Ctrl+,
Next Packet In Conversation Ctrl+.

Capture Menu

Capture > Interfaces (Ctrl I) see next frame
Capture > Options (Ctrl K) - see next page for details
Capture > Start (Ctrl E)
Capture > Stop (Ctrl E)
Capture > Restart (Ctrl R) - new capture using the same interfaces and options - quick recover from a bad 1st capture
Capture > Filters… - see next page for details
Capture > Refresh Interfaces - refresh interfaces & counters



Wireshark Preferences



Edit > Preferences
Ctrl-Shift-P
Preferences Icon

You can set different preferences for each custom profile

Preferences settings are stored in the *preferences* file in each profile dir

Recommended Preference Settings:

User Interface - Maximum recent filters: 10 files: 10
Layout: Pane 1: Packet List Pane 2: Details 3: Bytes
Columns: Add | Remove | drag to move*
Font and Colors: Lucida Console Normal | 8

Capture - set Default interface & Capture as pcap-ng

Filter Expressions - Add | Remove | drag to move*

Name Resolution - disable Resolve network (IP) Addr
GeoIP database directories

Protocols - settings for every protocol
Type sequential letters to quickly select (Ex: 'T' 'C' 'P')

HTTP: Add TCP ports to recognize as HTTP traffic

IEEE 802.11: Add / edit Wireless Decription keys

IPv4: Validate IPv4 checksum if possible (disable)
Enable GoIP lookups (enable)(if used)

IPv6: Enable GeoIP lookups (enable)(if used)

RTP: Allow subdissector to reassemble RTP streams

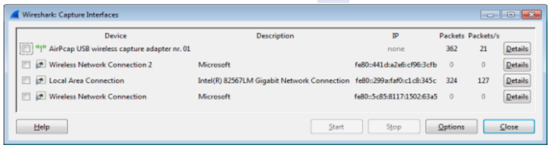
SMB: Reassemble SMB Transaction payload
Disable to measure First Byte response times
Enable to support exporting SMB objects

TCP: Validate TCP checksum if possible (disable)
Allow subdissector to reassemble TCP streams
Disable to measure First Byte response times
Enable to support exporting HTTP objects
Relative sequence numbers (enable)
Track number of bytes in flight (enable
Calculate conversation timestamps (enable)

UDP: Validate the UDP checksum if possible (disable)

* Easier to add / edit / move from the Packet List pane

Capture > Interfaces (Ctrl I) View / select intf(s)



	Device	Description	IP	Packets	Packets/s	
□	AirPcap USB wireless capture adapter nr. 01		none	362	21	Details
□	Wireless Network Connection 2	Microsoft	fe80::441d:a2e6:cf96:3cfb	0	0	Details
□	Local Area Connection	Intel(R) 82567LM Gigabit Network Connection	fe80::299a:faf0:c1c8:345c	324	127	Details
□	Wireless Network Connection	Microsoft	fe80::5c85:8117:1502:63a5	0	0	Details

Select interface(s) to capture from (can do multiple)
Click the **IP** header to toggle **IPv4 / IPv6 addresses**
(helpful for identifying a desired / configured interface)
Packets & Packets/s counters identify active intfs

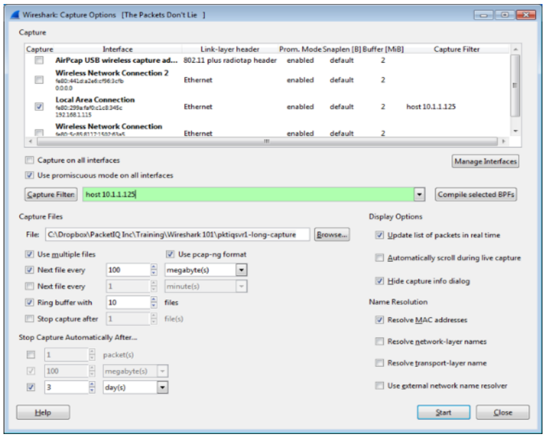
Interface **Details** offer a great deal of information
Options button opens the Capture > Options window

Capture Options

Capture > Options (Ctrl K) - select capture interfaces, filters, and options

Select interface(s) to capture from
IPv6 & IPv4 addresses are displayed

Select or enter/edit **Capture Filters** (sidebar)
This example captures pkts to/from 10.1.1.125
Specify **Capture Files** location (Browse)
Provide a file name and location; if saving multiple files, specify the leading file name - Wireshark will append a date-stamp to the end of each file. Be sure to add a file extension



Wireshark: Capture Options [The Packets Don't Lie]

Capture

Capture	Interface	Link-layer header	Prom. Mode	Snaplen [B]	Buffer [MiB]	Capture Filter
□	AirPcap USB wireless capture ad...	802.11 plus radiotap header	enabled	default	2	
□	Wireless Network Connection 2 fe80::441d:a2e6:cf96:3cfb 0.0.0.0	Ethernet	enabled	default	2	
☑	Local Area Connection fe80::299a:fa f0:c1c8:345c 192.168.1.115	Ethernet	enabled	default	2	host 10.1.1.125
□	Wireless Network Connection	Ethernet	enabled	default	2	

□ Capture on all interfaces
☑ Use promiscuous mode on all interfaces
Capture Filter: host 10.1.1.125

Capture Files
File: C:\Dropbox\PacketIQ Inc\Training\Wireshark 101\pktiqsvr1-long-capture
☑ Use multiple files ☑ Use pcap-ng format
☑ Next file every 100 megabyte(s)
□ Next file every 1 minute(s)
☑ Ring buffer with 10 files
□ Stop capture after 1 file(s)

Stop Capture Automatically After...
□ 1 packet(s)
☑ 100 megabyte(s)
☑ 3 day(s)

Display Options
☑ Update list of packets in real time
□ Automatically scroll during live capture
☑ Hide capture info dialog

Name Resolution
☑ Resolve MAC addresses
□ Resolve network-layer names
□ Resolve transport-layer name
□ Use external network name resolver

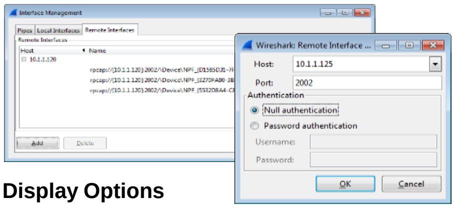
Use promiscuous mode on all intfs - enable
Use pcap-ng format - enable

Use multiple files - if you want to save a set of files, enable this then select the **Next File every** options by file size and/or time, optionally set a **Stop capture after** (x) files, and/or **Ring buffer with** (x) files. Ring Buffer use will save (x) number of on-going files, discarding the oldest file every time a new one is started

Stop Capture Automatically After… to stop after (x) packets or by file size and/or time

Manage Interfaces

Local Interfaces
Hide unuseable interfaces to avoid confusion
Remote Interfaces
List / Hide remote agent interfaces
Add - IP Addr & Port of remote rpcapd.exe agt



Interface Management — Pipes | Local Interfaces | Remote Interfaces

Remote Interfaces

Host	Name
⊟ 10.1.1.120	
	rpcap://[10.1.1.120]:2002/\Device\NPF_{D1585D31-7F
	rpcap://[10.1.1.120]:2002/\Device\NPF_{3270FAB0-3B
	rpcap://[10.1.1.120]:2002/\Device\NPF_{5532D8A4-CE

Wireshark: Remote Interface ...
Host: 10.1.1.125
Port: 2002
Authentication
● Null authentication
○ Password authentication
Username:
Password:

Display Options
Update list of packets in real time - enable
Automatically scroll during live capture - enable
Hide capture info dialog - enable

Name Resolution
Resolve MAC addresses - enable
Resolve network-layer names - disable
Resolve transport-layer name - enable
Use external network name resolver - disable

Features & Functions: Analyze

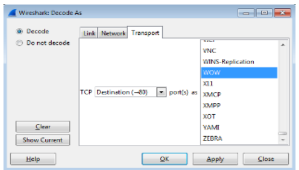
Analyze Menu

Analyze > Display Filters - **see side panel next page**
Analyze > Display Filter Macros - mechanism to create shortcuts for complex filters

These next three features act on a selected field in the Packet Details pane:
Analyze > Apply as Column - create a new column in the Packet List
Analyze > Apply as Filter - create a Display Filter
Analyze > Prepare a Filter - *prepare* (don't apply) a Display Filter

Selected
Not Selected
... and Selected
... or Selected
... and not Selected
... or not Selected

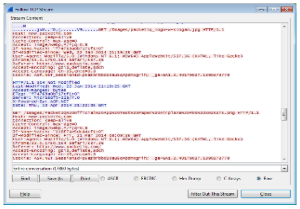
Analyze > Enable Protocols - enable/disable protocol dissectors
Analyze > Decode As… - decode a non-standard port as a specific protcol. Typically, choose the Transport port # to be decoded and the appropriate protocol to decode-as. You can use Edit > Preferences > Protocol | <protocol> to set this
Click 'Clear' to eliminate entries. These are temp settings - they are lost when closing Wireshark or changing profiles



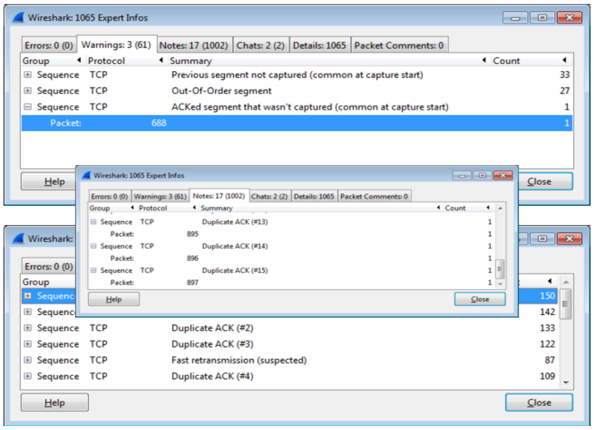
Wireshark: Decode As
● Decode
○ Do not decode
Link | Network | Transport
TCP Destination (→80) port(s) as
VNC
WINS-Replication
WOW
X11
XMCP
XMPP
XOT
YAMI
ZEBRA

Analyze > User Specified Decodes… - Clear or Save decode settings in current profile

Analyze > Follow TCP / UDP / SSL Stream
VERY useful for inspecting commands and data exchanged between clients and servers during a conversation w/o having to view data payloads across multiple pkts in a stream
Can print or save a conversation to a separate capture file



Analyze > Expert Info - one of the most useful features of Wireshark



Wireshark: 1065 Expert Infos

Errors: 0 (0) | Warnings: 3 (61) | Notes: 17 (1002) | Chats: 2 (2) | Details: 1065 | Packet Comments: 0

Group	Protocol	Summary	Count
⊞ Sequence	TCP	Previous segment not captured (common at capture start)	33
⊞ Sequence	TCP	Out-Of-Order segment	27
⊟ Sequence	TCP	ACKed segment that wasn't captured (common at capture start)	1
Packet:	688		1

Wireshark: 1065 Expert Infos (Notes: 17 (1002))

Group	Protocol	Summary	Count
⊟ Sequence	TCP	Duplicate ACK (#13)	1
Packet:	895		1
⊟ Sequence	TCP	Duplicate ACK (#14)	1
Packet:	896		1
⊟ Sequence	TCP	Duplicate ACK (#15)	1
Packet:	897		1

Group	Protocol	Summary	Count
⊞ Sequence			150
⊞ Sequence			142
⊞ Sequence	TCP	Duplicate ACK (#2)	133
⊞ Sequence	TCP	Duplicate ACK (#3)	122
⊞ Sequence	TCP	Fast retransmission (suspected)	87
⊞ Sequence	TCP	Duplicate ACK (#4)	109

Errors - packet / dissector errs

Warnings - unusual application and/or transport layer events - Out of Order packets, ACKed segment that wasn't captured (an indication of pkt loss), etc.

Notes - additional application / transport info, incl'd processes for events that were reported in a Warning - Duplicate ACKs, Fast Retransmissions, etc.

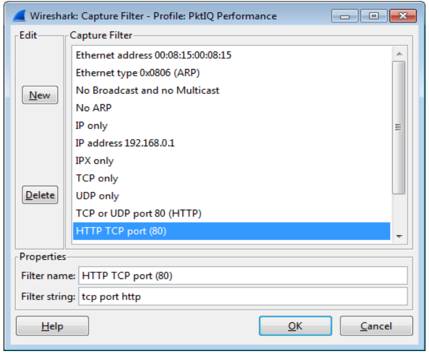
Chats - info about workflows, like TCP session setups / teardowns, GETs, etc.

Details - sequential list of Expert Info events
Packet Comments - listed by Packet #

A high count of Duplicate Acks (#xx) can indicate a high latency network path, but check to see how long the recovery period really was (delta time from 1st to last Dup ACK) - it may not be that long

Capture Filters

See wiki.wireshark.org/CaptureFilters for more examples



Wireshark: Capture Filter - Profile: PktIQ Performance

Edit — Capture Filter
Ethernet address 00:08:15:00:08:15
Ethernet type 0x0806 (ARP)
No Broadcast and no Multicast
No ARP
IP only
IP address 192.168.0.1
IPX only
TCP only
UDP only
TCP or UDP port 80 (HTTP)
HTTP TCP port (80)

Properties
Filter name: HTTP TCP port (80)
Filter string: tcp port http

Capture Filter Syntax & Examples

Hosts & Networks host *host* , src host, dst host
ether host, ether src, ether dst gateway host *host*
net *net/cidr* , net *net* mask *mask*

host 10.1.1.125 **ether host 00:1c:25:99:db:85**
wlan host ehost **wlan host 00:21:6a:86:0b:c2**
net 10.1.1.0/24 or **net 10.1.1.0 mask 255.255.255.0**
host <hostname> **host www.packetiq.com**
gateway host *host* (***host*** **name must be resolvable)**
captures pkts to/from the hardware address of a gw (typically a def router) but not the IP address of that gw

Ports & Protocols port, dst port, tcp port, tcp src, udp port, udp dst arp, icmp, ip, udp, tcp, http
port 80 (TCP or UDP port 80) DNS = port 53
not arp and port not 53 (no ARP & DNS)
DHCP = port 67 & 68

IPv6 ip6, icmp6 (replaces ARP & DNS)
DHCPv6 = port 546 & 547

Operators / Logic
= != > < >= <= ! not && and || or

Other Filters / Examples
len <= *length* , len >= *length* **len <= 128**
vlan [vlan_id] (IEEE 802.1Q VLAN pkts) **vlan 1**
not multicast and not broadcast

Offsets [# bytes from start of header, # bytes to match]
ip[2:2] > 576 (IP pkts > 576 bytes) **ip[1:1] > 0**
tcp[0:2] = 80 (TCP src port = 80) (DiffServ != 0)
Use capture filters sparingly so you don't miss anything!

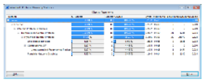
Features & Functions: Statistics

Statistics Menu

Statistics > Summary - capture summary & stats & Display Filter stats (if applicable)

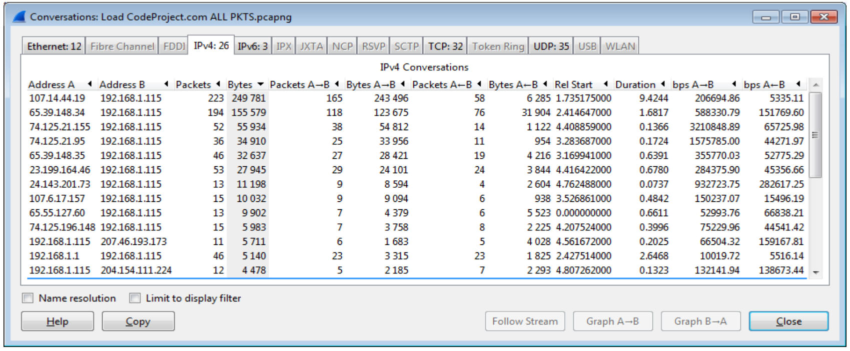
Statistics > Comments Summary - summary + Capture & Pkt Comments - can be copied

Statistics > Show Address Resolution - hosts data for current trace file (if Name Res on)



Statistics > Protocol Hierarchy - packet & byte counts & percentages by protocol. Useful for detecting anomalies / suspect traffic) - look for unusual protocols

Statistics > Conversations - conversation pairs + packets / bytes / time / rates by protocol



Conversations: Load CodeProject.com ALL PKTS.pcapng

Ethernet: 12 | Fibre Channel | FDDI | IPv4: 26 | IPv6: 3 | IPX | JXTA | NCP | RSVP | SCTP | TCP: 32 | Token Ring | UDP: 35 | USB | WLAN

IPv4 Conversations

Address A	Address B	Packets	Bytes	Packets A→B	Bytes A→B	Packets A←B	Bytes A←B	Rel Start	Duration	bps A→B	bps A←B
107.14.44.19	192.168.1.115	223	249 781	165	243 496	58	6 285	1.735175000	9.4244	206694.86	5335.11
65.39.148.34	192.168.1.115	194	155 579	118	123 675	76	31 904	2.414647000	1.6817	588330.79	151769.60
74.125.21.155	192.168.1.115	52	55 934	38	54 812	14	1 122	4.408859000	0.1366	3210848.89	65725.98
74.125.21.95	192.168.1.115	36	34 910	25	33 956	11	954	3.283687000	0.1724	1575785.00	44271.97
65.39.148.35	192.168.1.115	46	32 637	27	28 421	19	4 216	3.169941000	0.6391	355770.03	52775.29
23.199.164.46	192.168.1.115	53	27 945	29	24 101	24	3 844	4.416422000	0.6780	284375.90	45356.66
24.143.201.73	192.168.1.115	13	11 198	9	8 594	4	2 604	4.762488000	0.0737	932723.75	282617.25
107.6.17.157	192.168.1.115	15	10 032	9	9 094	6	938	3.526861000	0.4842	150237.07	15496.19
65.55.127.60	192.168.1.115	13	9 902	7	4 379	6	5 523	0.000000000	0.6611	52993.76	66838.21
74.125.196.148	192.168.1.115	15	5 983	7	3 758	8	2 225	4.207524000	0.3996	75229.96	44541.42
192.168.1.115	207.46.193.173	11	5 711	6	1 683	5	4 028	4.561672000	0.2025	66504.32	159167.81
192.168.1.1	192.168.1.115	46	5 140	23	3 315	23	1 825	2.427514000	2.6468	10019.72	5516.14
192.168.1.115	204.154.111.224	12	4 478	5	2 185	7	2 293	4.807262000	0.1323	132141.94	138673.44

☐ Name resolution ☐ Limit to display filter

Ethernet - station pairs by MAC Addr
IPv4 - host pairs by IP Addr or hostname
TCP - TCP stream conversations by port
UDP - UDP stream conversations by port
WLAN - WLAN conversations by STA Addr
Pay attention to: port #'s / services used, Pkts/Bytes A-B (relative traffic volumes), Rel Start - when did a thread start?, bps A->B, A<-B - impact on the network?

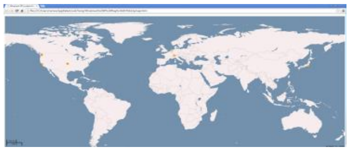
A VERY useful tool for identifying & filtering on conversations of interest from a capture:

1. Select IPv4 - Click the Bytes column twice - Top Talkers by IP Addr will top the list
2. ID the conversation of interest by name / IP
3. R-Click, select 'Apply as a Filter', 'Selected', 'A<->B' to apply a display filter for this conv
4. Inspect - if this is the desired conversation, save to a new file: **File > Export Specified Packets**

Name resolution - turn on/off to ID host pairs by IP or hostname (if resolution info available)

Limit to display filter - inspect TCP/UDP conversations related to a filtered IP host pair

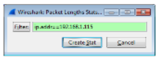
Statistics > Endpoints - displays stats like Conversations, but for single hosts
IPv4/v6 tabs support GeoIP mapping - Click 'Map' **->**
Country, City, & AS #'s for each host based on IP Addr

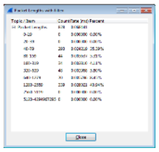


Setup GeoIP

1. Create a 'MaxMindGeoIP' directory on your hard drive
2. Open http://dev.maxmind.com/geoip/legacy/geolite/
3. Click / save the binary / gzip files for Country, City, & ASN (IPv4 & v6); unzip to .dat files
4. Edit > Preferences > Name Resolution | GeoIP database directories
5. Click New - navigate to MaxMind dir - choose 'Other…' - click 'Open'

(its easier to enter the path in the 'Location' field or edit geo_db_paths)





Statistics > Packet Lengths - useful for determining nominal pkt sizes
Can be used with a Display Filter setting. There shouldn't be any pkts < 40-79 bytes. 9000 byte Jumbo Packets may be enabled on 10GE intfs

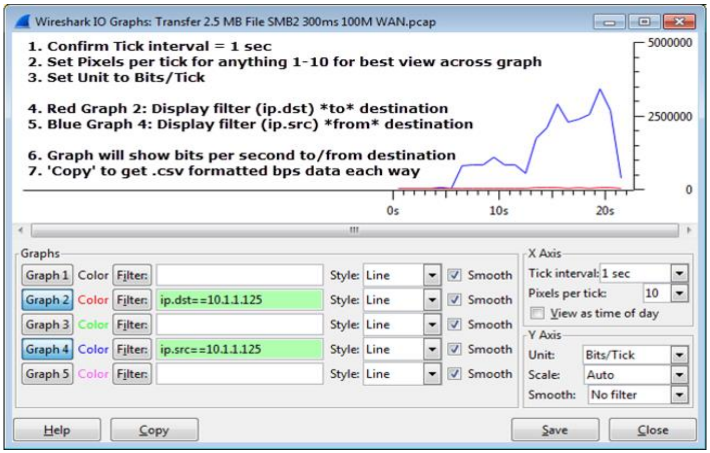
Statistics > IO Graph - this is another of the MOST useful Wireshark features
This Filter IO Graph example reveals bi-directional peak application demands in bits-per-sec

You can click on a point in the IO Graph to go to that packet in the Packet List

Set **Tick interval** to smaller units to provide increased per-pkt resolution

Set **Y Axis Unit** to **Advanced** for add'l functionality - see panel on right for more options

Copy the IO graph data points to save in .csv format or **Save** an image



Wireshark IO Graphs: Transfer 2.5 MB File SMB2 300ms 100M WAN.pcap

1. Confirm Tick interval = 1 sec
2. Set Pixels per tick for anything 1-10 for best view across graph
3. Set Unit to Bits/Tick

4. Red Graph 2: Display filter (ip.dst) *to* destination
5. Blue Graph 4: Display filter (ip.src) *from* destination

6. Graph will show bits per second to/from destination
7. 'Copy' to get .csv formatted bps data each way

Graphs

Graph 1	Color	Filter:		Style: Line	☑	Smooth
Graph 2	Color	Filter:	ip.dst==10.1.1.125	Style: Line	☑	Smooth
Graph 3	Color	Filter:		Style: Line	☑	Smooth
Graph 4	Color	Filter:	ip.src==10.1.1.125	Style: Line	☑	Smooth
Graph 5	Color	Filter:		Style: Line	☑	Smooth

X Axis
Tick interval: 1 sec
Pixels per tick: 10
☐ View as time of day

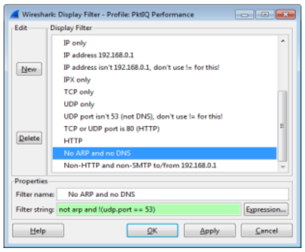
Y Axis
Unit: Bits/Tick
Scale: Auto
Smooth: No filter

Display Filters

Analyze > Display Filters - select, create, delete filters

To create a new filter enter the display filter name and filter string and then click 'New'

Display filters are saved in the *dfilters* profile file

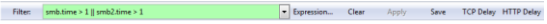


Wireshark: Display Filter - Profile: PktIQ Performance

Display Filter
IP only
IP address 192.168.0.1
IP address isn't 192.168.0.1, don't use != for this!
IPX only
TCP only
UDP only
UDP port isn't 53 (not DNS), don't use != for this!
TCP or UDP port is 80 (HTTP)
HTTP
No ARP and no DNS
Non-HTTP and non-SMTP to/from 192.168.0.1

Properties
Filter name: No ARP and no DNS
Filter string: not arp and !(udp.port == 53)

Display Filter Toolbar - enter/edit - Clear/Apply/Save



Filter: smb.time > 1 || smb2.time > 1

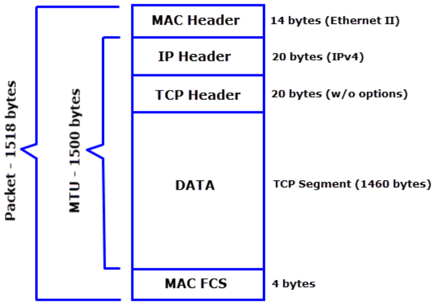
Filter opens the Display Filters window shown above
Expression... opens a window that walks you through creating a display filter - you can see all the possible filters and their extensions w/ descriptions
Save a display filter as a **Filter Expression Button** for quick and easy us of filters - very handy!! Configs for Filter Expression Buttons are saved in *preferences* files

Useful Display Filters			arp	bootp	dns
dhcp6	snmp	smb	smb2	icmp	rtp
ip	ipv6	udp	tcp	http	sip

ip.addr==10.1.1.125 && ip.addr==192.168.1.115
tcp.port==80 tcp.stream==1
Extended filter options are available for each protocol
Use Wireshark's auto-complete feature to list filters; type a protocol abbreviation and then a period to view and select a filter: Example: **tcp.analysis.xxxxxx**
There are **ip.geoip display filters** - for example:
ip and not ip.geoip.country == "United States"
Show nodes North of New York: ip.geoip.lat > 41
See http://www.wireshark.org/docs/dfref/ for more info

Packet Lengths

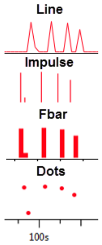
Most common data transfer methods use TCP/IP on Ethernet 802.3 networks supporting 1518-byte max frame sizes and a 1500-byte MTU (default in routers)



Ethernet (MAC) header + IP header + TCP header + Frame Check Sequence (FCS) = 58 bytes
1518 - 58 = 1460 byte Maximum Segment Size (MSS)

IO Graph Options

IO Graph Styles



X axis intervals:
.001, .01, .1, 1, 10 sec, 1 min, 10 min

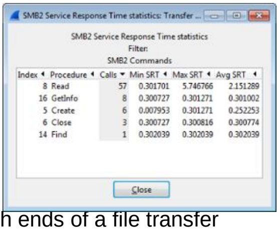
Y axis settings:
Packets - Bytes - Bits /Tick & Advanced
Scale - Auto, 10 to 2 Billion, logarithmic
Smoothing - plots a moving avg of data

Advanced Options:
SUM(*) Adds values of a field for a tick
MIN(*) Min value during a tick interval
AVG(*) Avg value during a tick interval
MAX(*) Max value during a tick interval
COUNT FRAMES(*) # of frames containing a field or characteristic seen during the tick interval
COUNT FIELDS(*) # of occurences of a field or characteristic seen during the tick interval
LOAD(*) Measures response time fields only

Features & Functions: Statistics & Telephony

Statistics Menu - Cont'd

Statistics > Conversation List - another way to open a Conversations window
Statistics > Endpoing List - another way to open an Endpoints window (w/ IPv4/v6 GeoIP)
Statistics > Service Response Time - tables of min, max, avg service response times for services such as SMB2. R-Click & build procedure filters **->**

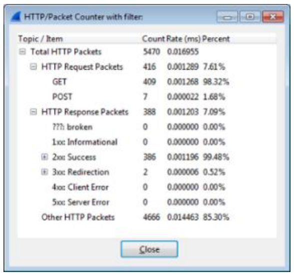

SMB2 Service Response Time statistics: Transfer ...

SMB2 Service Response Time statistics
Filter:
SMB2 Commands

Index	Procedure	Calls	Min SRT	Max SRT	Avg SRT
8	Read	57	0.301701	5.746766	2.151289
16	GetInfo	8	0.300727	0.301271	0.301002
5	Create	6	0.007953	0.301271	0.252253
6	Close	3	0.300727	0.300816	0.300774
14	Find	1	0.302039	0.302039	0.302039

Statistics > ANCP - Access Node Control Prot (DSL access)
Statistics > BACnet - Building Automation & Control Network
Statistics > BOOTP-DHCP - list of packets by type
Statistics > Collectd - info on Collectd daemon stats traffic (collector for an open source system performance project)
Statistics > Compare - supports comparing trace files from both ends of a file transfer based on IP IDs. Merge files w/ Mergecap then open & Compare (*not reliable this version*)
Statistics > Flow Graph - similar to a 'Bounce Diagram' - displays SMB2 or HTTP flows between nodes with elapsed time, Req/Resp and data flow info. Can be exported to txt file
Statistics > HART-IP - Highway Addressable Remote Transducer over IP stats

Statistics > HTTP - Packet Counter - packet distribution
Statistics > Requests - by HTTP host & list of requests
Statistics > Load Distribution - Reqs/Resps by Server


HTTP/Packet Counter with filter:

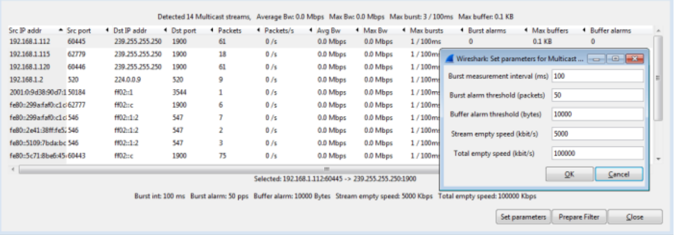
Topic / Item	Count	Rate (ms)	Percent
Total HTTP Packets	5470	0.016955	
HTTP Request Packets	416	0.001289	7.61%
GET	409	0.001268	98.32%
POST	7	0.000022	1.68%
HTTP Response Packets	388	0.001203	7.09%
???: broken	0	0.000000	0.00%
1xx: Informational	0	0.000000	0.00%
2xx: Success	386	0.001196	99.48%
3xx: Redirection	2	0.000006	0.52%
4xx: Client Error	0	0.000000	0.00%
5xx: Server Error	0	0.000000	0.00%
Other HTTP Packets	4666	0.014463	85.30%

Statistics > ONC-RPC - Min/Max/Avg service response times for the ONC variation of Remote Procedure Call
Statistics > Sametime - stats for Lotus Notes Sametime

Statistics > TCP StreamGraph - see panel on right

Statistics > UDP Multicast Streams - multicast source, destination, port, BW, & burst info

Stream analysis / burst parameters can be set. Multicast stream sources include OSPF, IGMP, & video streams


Detected 14 Multicast streams, Average Bw: 0.0 Mbps Max Bw: 0.0 Mbps Max burst: 3 / 100ms Max buffer: 0.1 KB

Src IP addr	Src port	Dst IP addr	Dst port	Packets	Packets/s	Avg Bw	Max Bw	Max bursts	Burst alarms	Max buffers	Buffer alarms
192.168.1.112	60445	239.255.255.250	1900	61	0 /s	0.0 Mbps	0.0 Mbps	1 / 100ms	0	0.1 KB	0
192.168.1.115	62779	239.255.255.250	1900	18	0 /s	0.0 Mbps	0.0 Mbps	1 / 100m			
192.168.1.120	60446	239.255.255.250	1900	61	0 /s	0.0 Mbps	0.0 Mbps	1 / 100m			
192.168.1.2	520	224.0.0.9	520	9	0 /s	0.0 Mbps	0.0 Mbps	1 / 100m			
2001:0:9d38:90d7:1	50184	ff02::1	3544	1	0 /s	0.0 Mbps	0.0 Mbps	1 / 100m			
fe80::299a:faf0:c1c	62777	ff02::c	1900	6	0 /s	0.0 Mbps	0.0 Mbps	1 / 100m			
fe80::299a:faf0:c1c	546	ff02::1:2	547	7	0 /s	0.0 Mbps	0.0 Mbps	1 / 100m			
fe80::2e41:38ff:fe5	546	ff02::1:2	547	2	0 /s	0.0 Mbps	0.0 Mbps	1 / 100m			
fe80::5109:7bda:bc	546	ff02::1:2	547	3	0 /s	0.0 Mbps	0.0 Mbps	1 / 100m			
fe80::5c71:8be6:45	60443	ff02::c	1900	75	0 /s	0.0 Mbps	0.0 Mbps	1 / 100m			

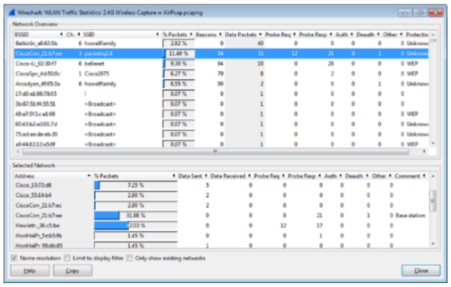
Wireshark: Set parameters for Multicast ...

Burst measurement interval (ms)	100
Burst alarm threshold (packets)	50
Buffer alarm threshold (bytes)	10000
Stream empty speed (kbit/s)	5000
Total empty speed (kbit/s)	100000

Selected: 192.168.1.112:60445 -> 239.255.255.250:1900

Burst int: 100 ms Burst alarm: 50 pps Buffer alarm: 10000 Bytes Stream empty speed: 5000 Kbps Total empty speed: 100000 Kbps

Statistics > WLAN Traffic
Provides WLAN traffic statistics incl'd BSSID, Channel, SSID, % Packets, and summary stats of frame types
Selecting a BSSID / Ch / SSID network provides statistics for that network: address, % Packets, data sent/rcvd, and management frame counts


Wireshark: WLAN Traffic Statistics: 2.4G Wireless Capture w AirPcap.pcapng

Network Overview

BSSID	Ch.	SSID	% Packets	Beacons	Data Packets	Probe Req	Probe Resp	Auth	Deauth	Other	Protectio
BelkinIn_e8:63:5b	6	howellfamily	2.82 %	0	40	0	0	0	0	0	Unknow
CiscoCon_21:b7:ee	3	packetiq2.4	11.49 %	94	35	12	21	0	1	0	Unknow
Cisco-Li_92:30:f7	6	bellanet	9.30 %	94	10	0	28	0	0	0	WEP
CiscoSpv_4d:50:9c	1	Cisco2675	6.27 %	79	8	0	2	0	0	0	WEP
Arcadyan_4f:05:3a	6	howellfamily	6.55 %	90	2	0	0	0	1	0	Unknow
17:d3:d1:98:78:05		!	0.07 %	0	1	0	0	0	0	0	
3b:87:51:f4:55:51		<Broadcast>	0.07 %	0	1	0	0	0	0	0	
48:a7:5f:1c:e1:08		<Broadcast>	0.07 %	0	1	0	0	0	0	0	WEP
60:43:b2:e3:01:7d		<Broadcast>	0.07 %	0	1	0	0	0	0	0	Unknow
75:ad:ee:de:eb:20		<Broadcast>	0.07 %	0	1	0	0	0	0	0	Unknow
a9:44:82:12:a5:8f		<Broadcast>	0.07 %	0	1	0	0	0	0	0	WEP

Selected Network

Address	% Packets	Data Sent	Data Received	Probe Req	Probe Resp	Auth	Deauth	Other	Comment
Cisco_13:72:d8	7.25 %	5	0	0	0	0	0	0	
Cisco_55:d4:b4	2.90 %	2	0	0	0	0	0	0	
CiscoCon_21:b7:ec	2.90 %	2	0	0	0	0	0	0	
CiscoCon_21:b7:ee	31.88 %	0	0	0	21	0	1	0	Base station
Hewlett-_36:c5:be	2.03 %	0	0	12	17	0	0	0	
HonHaiPr_5e:b5:fb	1.45 %	0	0	0	1	0	0	0	
HonHaiPr_99:db:85	1.45 %	1	0	0	0	0	0	0	

☑ Name resolution ☐ Limit to display filter ☐ Only show existing networks

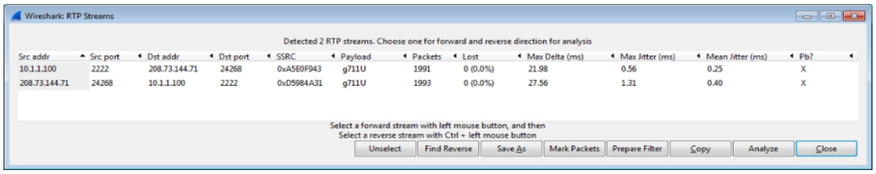
The 'rate' in stats below is packets / ms
Statistics > IP Destinations - IP **dest** addresses & pkt counts, rate, & % by protocol & port
Statistics > IP Addresses - IP addresses w/ total (src + dest) packets, rate, & % counts
Statistics > Protocol Types - total packet counts, rate (ms), & percents by protocol

Telephony Menu

Protocols for cellular radio & VoIP ntwks, SS7, etc.

Telephony > ANSI - BSMAP, DTAP, & MAP Operation A-Interface message stats
Telephony > GSM - Global System for Mobile Communications A-Interface msg stats
Telephony > H.225 - H.225 Message & Message Reason counters
Telephony > IAX2 - Inter-Asterisk stream analysis
Telephony > ISUP - ISDN User Part message Count Rate (ms) & percentages
Telephony > LTE - Long Term Evolution protocol MAC & Radio Link Control stats & graphs
Telephony > MTP3 - Message Transfer Part3 Message Signal Unit stats

Telephony > RTP > Show All Streams - lists & displays stats for RTP steams


Wireshark: RTP Streams

Detected 2 RTP streams. Choose one for forward and reverse direction for analysis

Src addr	Src port	Dst addr	Dst port	SSRC	Payload	Packets	Lost	Max Delta (ms)	Max Jitter (ms)	Mean Jitter (ms)	Pb?
10.1.1.100	2222	208.73.144.71	24268	0xA5E0F943	g711U	1991	0 (0.0%)	21.98	0.56	0.25	X
208.73.144.71	24268	10.1.1.100	2222	0xD5984A31	g711U	1993	0 (0.0%)	27.56	1.31	0.40	X

Select a forward stream with left mouse button, and then
Select a reverse stream with Ctrl + left mouse button

TCP Stream Graphs

Statistics > Stream Graphs - one of the more impressive but least understood / utilized features

For ALL of the TCP Stream Graphs:

1. Click a packet in the Packet List for the direction the data is flowing (a server pkt for a server->client transfer

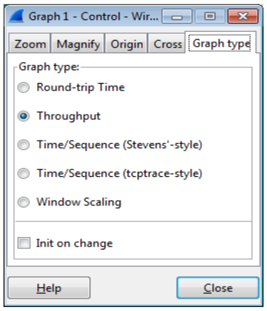
2. Statistics > TCP Stream Graph > <any graph>
If a graph is blank, select a packet in the other direction
!! Each graph is only for the selected packet's flow
Or open two graphs - one for each direction

3. Click on an area of interest and use keyboard '+' & '-' keys to zoom In/Out (Click/drag w/ mouse to zoom in)

4. Use keyboard arrow keys to go Left/Right / Up/Down

5. Clicking a point in the graph takes you to that pkt

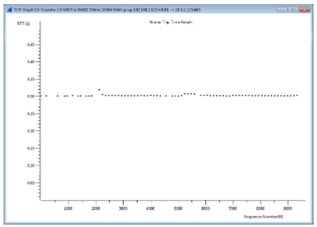
6. Along with any graph a Control window will appear - select a desired graph from the Graph Type tab


Graph 1 - Control - Wir...

Graph type:
○ Round-trip Time
● Throughput
○ Time/Sequence (Stevens'-style)
○ Time/Sequence (tcptrace-style)
○ Window Scaling
☐ Init on change

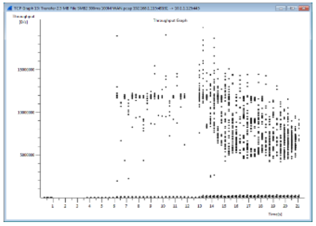
Round Trip Time

latency time between a TCP data packet and a related ACK packet. Investigate spikes or other anomalies



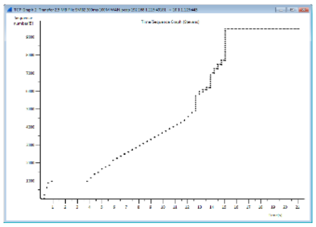
Throughput

Like an IO Graph but with dots (vs lines) and graphed in **Bytes** / sec
This graph reflects a high latency path w/ SMB2 transfer effects



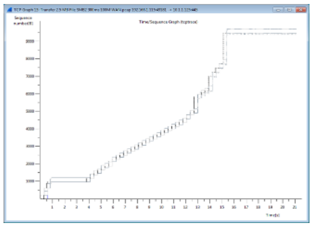
Time/Sequence (Steven's style)

Plots sequence #'s as they increase during a data transfer. Ideal plot is lower left to upper right in a smooth line.



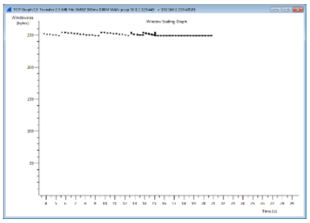
Time/Sequence (tcptrace style)

Also plots SEQ #'s but with more info. TCP segments are plotted in an I - bar format - taller bars contain more data. Horizontal is time, vertical is Byte-based Seq #s
Grey line is the window size - when I bars reach this line you have a Zero Window (no data flow) condition.



Window Scaling

Plots calculated window size in each pkt sent. To use select an ACK pkt from the host that is receiving data.



Features & Functions: Telephony & Tools & Internals

Telephony Menu - Cont'd

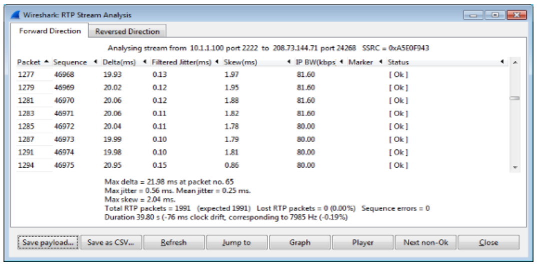
Telephony > RTP > Show All Streams - Cont'd RTP = Real-Time Transport Protocol

SSRC is the Synchronization Source Identifier that ID's a RTP stream timestamping source

Pb? indicates a problem in the RTP stream - pkt loss & errors, out of order seq #'s, etc.

Select Fwd & Revs streams, click Analyze to open Stream Analysis window for those streams

Telephony > RTP > Stream Analysis - displays per-pkt performance stats for RTP flows



Analysing stream from 10.1.1.100 port 2222 to 208.73.144.71 port 24268 SSRC = 0xA5E0F943

Packet	Sequence	Delta(ms)	Filtered Jitter(ms)	Skew(ms)	IP BW(kbps)	Marker	Status
1277	46968	19.93	0.13	1.97	81.60		[Ok]
1279	46969	20.02	0.12	1.95	81.60		[Ok]
1281	46970	20.06	0.12	1.88	81.60		[Ok]
1283	46971	20.06	0.11	1.82	81.60		[Ok]
1285	46972	20.04	0.11	1.78	80.00		[Ok]
1287	46973	19.99	0.10	1.79	80.00		[Ok]
1291	46974	19.98	0.10	1.81	80.00		[Ok]
1294	46975	20.95	0.15	0.86	80.00		[Ok]

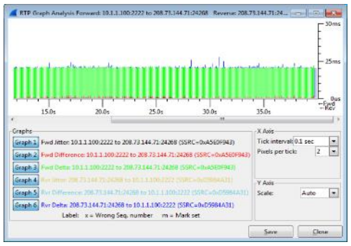
Max delta = 21.98 ms at packet no. 65
Max jitter = 0.56 ms. Mean jitter = 0.25 ms.
Max skew = 2.04 ms.
Total RTP packets = 1991 (expected 1991) Lost RTP packets = 0 (0.00%) Sequence errors = 0
Duration 39.80 s (-76 ms clock drift, corresponding to 7985 Hz (-0.19%)

Pkt #, Seq #, time delta, jitter, skew, IP bw (kbps), end of silence marker, status, & summary stats at bottom for Fwd & Reverse directions.

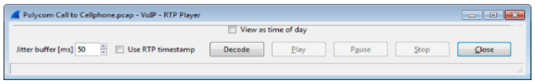
Click **Save payload** & save both channels in .au format for playback.

Click **Save as CSV** to save stats in csv format for analysis in Excel®.

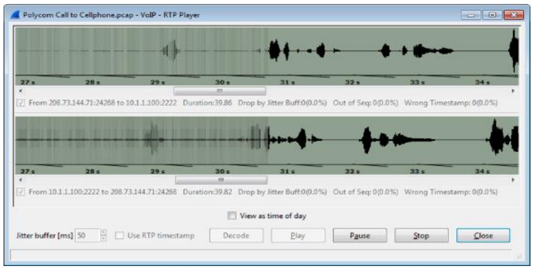
Click **Graph** to visualize per-packet jitter - adjust Tick interval & Pixels / tick for best display


RTP Graph Analysis Forward: 10.1.1.100:2222 to 208.73.144.71:24268 Reverse: 208.73.144.71:24...
30ms
25ms
0us
←Fwd
←Rev
15.0s
20.0s
25.0s
30.0s
35.0s
Graphs
Graph 1
Fwd Jitter: 10.1.1.100:2222 to 208.73.144.71:24268 (SSRC=0xA5E0F943)
Graph 2
Fwd Difference: 10.1.1.100:2222 to 208.73.144.71:24268 (SSRC=0xA5E0F943)
Graph 3
Fwd Delta: 10.1.1.100:2222 to 208.73.144.71:24268 (SSRC=0xA5E0F943)
Graph 4
Rvr Jitter: 208.73.144.71:24268 to 10.1.1.100:2222 (SSRC=0xD5984A31)
Graph 5
Rvr Difference: 208.73.144.71:24268 to 10.1.1.100:2222 (SSRC=0xD5984A31)
Graph 6
Rvr Delta: 208.73.144.71:24268 to 10.1.1.100:2222 (SSRC=0xD5984A31)
Label: x = Wrong Seq. number m = Mark set
X Axis
Tick interval: 0.1 sec
Pixels per tick: 2
Y Axis
Scale: Auto
Save
Close

Click **Player** then **Decode** to launch audio player



Click to **select Fwd & Rev streams** then **Play** to listen to call audio **->**

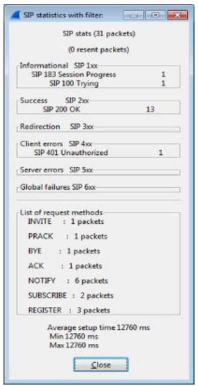

Polycom Call to Cellphone.pcap - VoIP - RTP Player
27 s
28 s
29 s
30 s
31 s
32 s
33 s
34 s
From 208.73.144.71:24268 to 10.1.1.100:2222 Duration:39.86 Drop by Jitter Buff:0(0.0%) Out of Seq: 0(0.0%) Wrong Timestamp: 0(0.0%)
From 10.1.1.100:2222 to 208.73.144.71:24268 Duration:39.82 Drop by Jitter Buff:0(0.0%) Out of Seq: 0(0.0%) Wrong Timestamp: 0(0.0%)
View as time of day
Jitter buffer [ms] 50
Use RTP timestamp
Decode
Play
Pause
Stop
Close

Telephony > RTSP > Packet Counter - displays Real Time Streaming Protocol request & response pkt Count Rate in pkts/ms & Percent. Resp pkts listed by resp code categories

SCTP = Stream Control Transport Protocol - transport layer protocol w/ elements of both UDP & TCP

Telephony > SCTP - Analyze & Show Associations (connections), (data) Chunk Counter

Telephony > SIP - Session Initiation Protocol stats & request methods



SIP stats (31 packets)
(0 resent packets)

Informational SIP 1xx
SIP 183 Session Progress 1
SIP 100 Trying 1

Success SIP 2xx
SIP 200 OK 13

Redirection SIP 3xx

Client errors SIP 4xx
SIP 401 Unauthorized 1

Server errors SIP 5xx

Global failures SIP 6xx

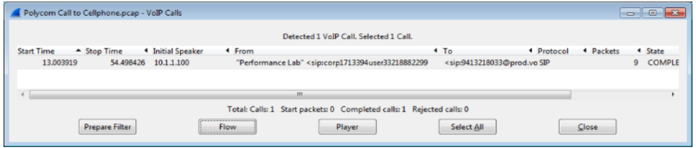
List of request methods
INVITE : 1 packets
PRACK : 1 packets
BYE : 1 packets
ACK : 1 packets
NOTIFY : 6 packets
SUBSCRIBE : 2 packets
REGISTER : 3 packets

Average setup time 12760 ms
Min 12760 ms
Max 12760 ms

Telephony > SMPPOperations - Short Message Peer Protocol stats

Telephony > UCP Messages - Universal Computer Protocol stats

Telephony > VoIP Calls - lists VoIP calls in a capture. Click Flow to open a Graph Analysis. Click Player to open the RTP player.



Detected 1 VoIP Call. Selected 1 Call.

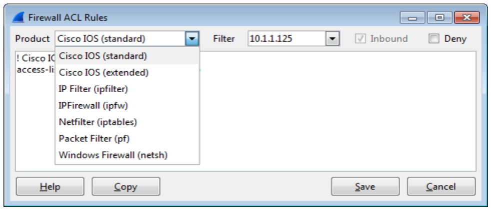
Start Time	Stop Time	Initial Speaker	From	To	Protocol	Packets	State
13.003919	54.498426	10.1.1.100	"Performance Lab" <sip:corp1713394user33218882299	<sip:9413218033@prod.vo	SIP	9	COMPLE

Total: Calls: 1 Start packets: 0 Completed calls: 1 Rejected calls: 0

Telephony > WAP-WSP… - Wireless Application Protocol-Wireless Session Protocol stats

Tools Menu

Tools > Firewall ACL Rules - creates ACL rules used by firewall products to block or allow traffic based on various characteristics found within packet traces. Click on a packet or field and launch, then Select **Product** and **Filter** options



Product Cisco IOS (standard) Filter 10.1.1.125 ☑ Inbound ☐ Deny

! Cisco IC
access-li

Cisco IOS (standard)
Cisco IOS (extended)
IP Filter (ipfilter)
IPFirewall (ipfw)
Netfilter (iptables)
Packet Filter (pf)
Windows Firewall (netsh)

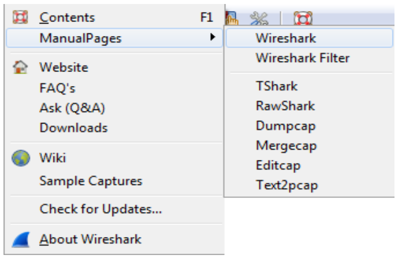
Tools > Lua - Lua is "a powerful, fast, lightweight, embeddable scripting language" added to Wireshark for prototyping and scripting, writing dissectors, post-dissectors, and 'taps'

Internals Menu

Internals > Dissector tables - variables/parameters that reflect defined standards for a protocol in each dissector. See TCP & UDP port integer tables, Heuristic svcs/abbreviations

Internals > Supported Protocols - exhaustive list of all protocols supported in Wireshark. **Display Filters Fields** tab lists ALL of >100,000 protocol and packet type fields recognized by Wireshark & can be used to create Display Filters - scroll right to see add'l type fields

Wireshark Help



Help > Contents (F1) - Wireshark User's Guide

Help > ManualPages - man-style html help pages

Help > Website http://www.wireshark.org

Help > FAQ's http://www.wireshark.org/faq.html

Help > Ask (Q&A) http://ask.wireshark.org

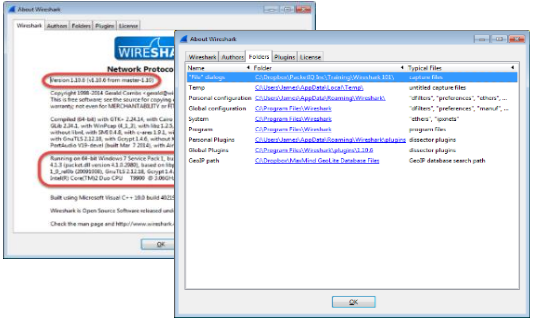
Help > Downloads http://www.wireshark.org/download.html

Help > Wiki http://wiki.wireshark.org

> Sample Captures http://wiki.wireshark.org/SampleCaptures

Help > Check for Updates… - online version check

Help > About Wireshark… > Wireshark - current version & info on your workstation! Even versions are stable releases, odd versions are development



Name	Folder	Typical Files
"File" dialogs	C:\Dropbox\PacketIQ Inc\Training\Wireshark 101\	capture files
Temp	C:\Users\James\AppData\Local\Temp\	untitled capture files
Personal configuration	C:\Users\James\AppData\Roaming\Wireshark\	"dfilters", "preferences", "ethers", ...
Global configuration	C:\Program Files\Wireshark	"dfilters", "preferences", "manuf", ...
System	C:\Program Files\Wireshark	"ethers", "ipxnets"
Program	C:\Program Files\Wireshark	program files
Personal Plugins	C:\Users\James\AppData\Roaming\Wireshark\plugins	dissector plugins
Global Plugins	C:\Program Files\Wireshark\plugins\1.10.6	dissector plugins
GeoIP path	C:\Dropbox\MaxMind GeoLite Database Files	GeoIP database search path

Help > About Wireshark… > Authors - all of the developers who have made this fine tool possible

Help > About Wireshark… > Folders - very handy! Personal profile files are in Personal configuration folder Command-line utilities in Program folder - GeoIP path Double-click a link to open that folder

Main Toolbar

GET IN THE HABIT OF USING THESE - Saves Time!

Capture Toolbar Icons

Restart Capture - quick recover from bad 1st capture

List Interfaces – Capture Options – Start – Stop – Restart Capture

Trace File Toolbar Icons

Many temp settings can be cleared by Reload File

Open File - Save File - Close File - Reload File

Navigation Toolbar Icons

Back returns to last pkt located

Find - Go Back - Fwd – Jump To – Go to First | Last Pkt

Color - Scroll - View Toolbar Icons

Pkt Coloring - Auto-Scroll **Zoom In | Out | 100% | Resize**

Filter Editors - Color Rules - Configuration - Help

View/edit filters & colors

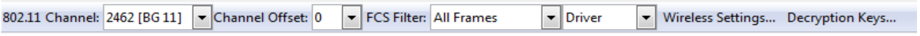
Set Preferences

Capture Filter Editor - Display Filter Editor

Coloring Rules Editor - Preferences - Help

Wireless Analysis

View > Wireless Toolbar to enable / view the toolbar

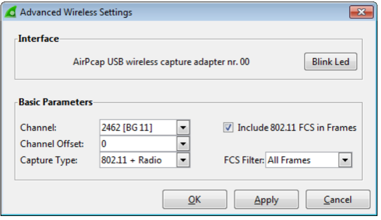

802.11 Channel: 2462 [BG 11] | Channel Offset: 0 | FCS Filter: All Frames | Driver | Wireless Settings... | Decryption Keys...

Controls: **Note**: 802.11 adapters must be set to *monitor mode* (*rfmon mode*) - not all can be

802.11 Channel to capture - **Channel Offset** w/AirPcap N/NX Adapters for a "wide channel"

FCS Filter: All Frames - Valid Frames - Invalid Frames only

Decryption Method - None, Wireshark, Driver (AirPcap driver)


Advanced Wireless Settings

Interface

AirPcap USB wireless capture adapter nr. 00 | Blink Led

Basic Parameters

Channel: 2462 [BG 11]
Channel Offset: 0
Capture Type: 802.11 + Radio
☑ Include 802.11 FCS in Frames
FCS Filter: All Frames

OK | Apply | Cancel

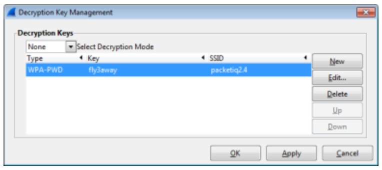
Advanced Wireless Settings - offers the same options you can set from the toolbar, plus:
A button to '**Blink LED**' on the AirPcap adapter
Set the **Capture Type** to:

802.11 Only

802.11 + Radio (default) - prepend a 'Radiotap' pseudoheader to each frame in Packet Details pane

802.11 + PPI = prepend Per-Packet Information pseudoheader in Packet Details Pane

Include 802.11 FCS in Frames (on by default)


Decryption Key Management

Decryption Keys

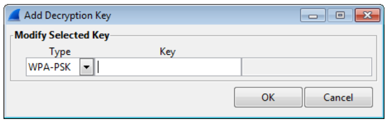
None — Select Decryption Mode

Type	Key	SSID
WPA-PWD	fly3away	packetiq2.4

New | Edit... | Delete | Up | Down

OK | Apply | Cancel

Decryption Keys… - Add / Edit / Delete keys
Decryption Mode - Driver, Wireshark, None
(select Wireshark to avoid saving keys in registry)


Add Decryption Key

Modify Selected Key

Type: WPA-PSK | Key:

OK | Cancel

Add Decryption Key - Type, Key, SSID (not labeled)

Type: WEP - parsed as WEP key
(wep:a1:b2:c3:d4:e5)
SPA-PWD - pswd + SSID
(wpa-pwd:MyPassword:MySSID)
WPA-PSK - raw pre-shared key (wpa-psk:01020304050607…5647392)

Right-Click Menus

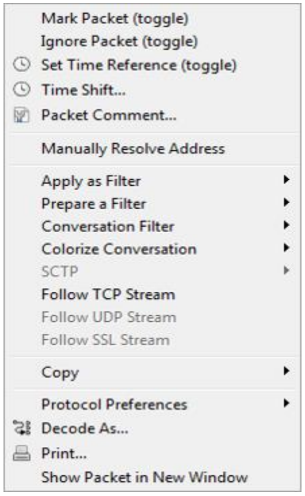
Many Wireshark tasks can be completed **much more** quickly using Right-Click menus

Different R-Clk options are available in Packet List, Packet Details, & Packet Bytes panes, depending on where (which field) you R-Click from. All of the options in R-Clk menus are covered in previous sections, but a few specifics apply:

The Display Filter string prepared when you Right-Click and select **Apply as Filter** or **Prepare a Filter** depends on the specific packet and field you clicked from

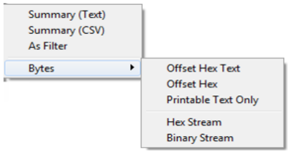
You can R-Clk > **Colorize Conversations** or create a **New Coloring Rule** - but you have to select View > Reset Coloring 1-10 (or Ctrl-Space) to remove the coloring

Packet List Right-Click Menu

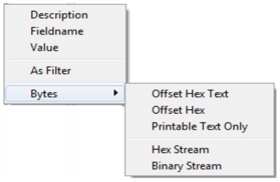


Right-Click > **Copy** options vary depending on the pane:

Packet List Pane

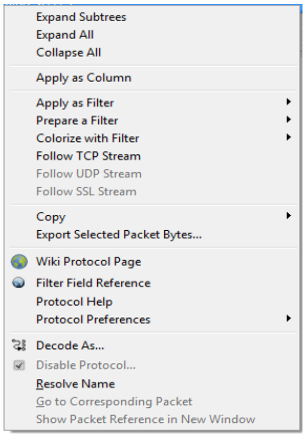


Packet Details Pane



R-Clk > **Protocol Preferences** offers a selection of the preferences options for the highest layer protocol in that pkt

Packet Details R-Click Menu

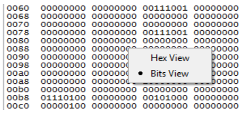


R-Clk on a protocol layer header & select **Expand Subtrees** to expand all of the headers UNDER that protocol layer, or **Expand All** / **Collapse All** to affect all the protocol layers

R-Clk > **Apply as Column** in Packet Details is a quick way to add a Pkt List pane column of the selected field values

R-Clk > **Wiki Protocol Page**, **Filter Field Reference**, & **Protocol Help** offers info based on the protocol/field selected

Packet Bytes R-Clk Menu


```
0060  00000000 00000000 00111001 00000000
0068  00000000 00000000 00000000 00000000
0070  00000000 00000000 00000000 00000000
0078  00000000 00000000 00111001 00000000
0080  00000000 00000000 00000000 00000000
0088  00000000 0000000
0090  00000000 0000000               00000
0098  00000000 0000000               00000
00a0  00000000 0000000               00000
00a8  00000000 0000000               00000
00b0  00000000 00000000 00000000 00000000
00b8  01110100 00000000 00101000 00000000
00c0  00000100 00000000 00000000 00000000
```

R-Clk > **Hex View** displays Packet Bytes contents as Hex octets & their ascii derivative (if possible)
R-Clk > **Bits View** displays each packet byte in 1's & 0's

Wireless Adapters

Wireless capture on on ANY channel w/o association requires AirPcap adapters like AirPCap NX USB 802.11a/b/g/n (capture + injection)

Catalog: http://www.cacetech.com/products/catalog/

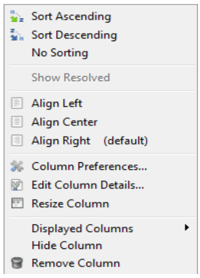
AirPcap Driver: *Can use up to 3 adapters for Ch 1+6+11*

https://support.riverbed.com/content/support/software/cascade/airpcap.html

Bug Fix: if the Wireless Toolbar stays greyed out with an AirPcap adapter installed - open Capture Options, Dbl-Click on the AirPcap entry, click OK, then Start

Packet List Columns

Column Header R-Click Menu



R-Clk > **Sort** options are quicker to do by just clicking a column header multiple times

R-Clk a column header and select **Align Left** - **Center** - **Right** or **Resize Column**

You can **click & drag** a column to another location in the Packet List

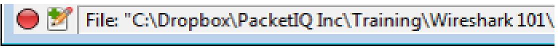
R-Clk > **Column Preferences** brings up Preferences window for selecting / customizing columns

R-Clk > **Edit Column Details** allows modification of the Title, Field type, Field name, and occurrence (for filters that match more than one field in a packet)

R-Clk > **Displayed Columns** list all available columns, which are currently displayed, and the ability to select

R-Clk > **Hide Column** hides (but does not delete) the selected column from being displayed in Packet List
RC > **Remove Column** deletes a column permanently

Status Bar

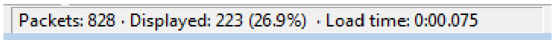

File: "C:\Dropbox\PacketIQ Inc\Training\Wireshark 101\

Expert Info Button - click to bring up Expert Infos
Button color indicates highest analysis level:

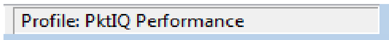
Red	Errors	Yellow	Warnings
Cyan	Notes	Blue	Chats
Green	Packet comments, but no Errors / Warnings / Notes		
Grey	No Expert Info items		

Trace File Annotation Button - Add / Edit / Cancel comments about the entire trace file

File Information Column - path/directory & file name, file size, & packet capture duration

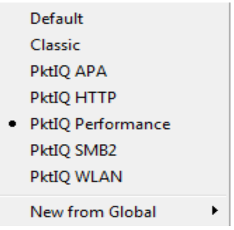

Packets: 828 · Displayed: 223 (26.9%) · Load time: 0:00.075

Packet Information Column - displays Packet counts: Total - Displayed - Marked - Dropped (during capture)

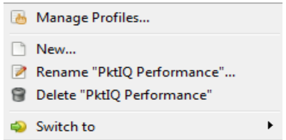

Profile: PktIQ Performance

Profile Column - Click to select profiles / Right-Click to select Manage Profile options

Profile Selection Menu



Profile Management Menu



Working with Time

There are several Wireshark time fields available

Absolute (actual capture date/times)

Absolute date & time - actual capture date and time based on the time zone of analysis host
Absolute time - actual capture time (no date) based on time zone of analysis host

Relative (to start of capture)

Relative time - time from the first packet in a trace file
Relative time (conversation) - time from the first packet in the trace file for the conversation
Time (format as specified) - this setting displays a value set using View > Time Display Format

Delta (from previous frames)

Delta time (frame.time_delta) - end of the current frame from the end of the prevoius frame
Delta time (conversation) - end of one packet to the end of the next packet *in a conversation*
Delta time displayed - end of one packet to the end of next packet *of displayed packets only*

Wireshark saves a GMT/UTC offset value of the capture machine in the packet trace file, and converts the timestamps to the number of seconds since the UNIX 'epoch' - # of seconds since Jan 1, 1970 @ 00:00:00 GMT. When the trace file is opened the GMT/UTC offset is again applied to display the timestamps. **If a capture from one time zone is viewed in another time zone, the absolute date/time stamps will be off by the difference in the time zones.**

Selecting Wireshark Time Displays

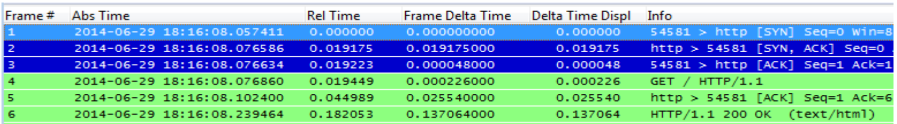
You need to know when an event occurred in a capture

Absolute Time: locating events related to user reports / logs
Relative Time: how far into a capture an event occurred

You need the delay between pkts in a conversation, especially responses to requests

Delta time: time between packets *in a conversation*

This example shows the differences between Abs, Rel, Frame Delta, and Displayed Delta times:



Frame #	Abs Time	Rel Time	Frame Delta Time	Delta Time Displ	Info
1	2014-06-29 18:16:08.057411	0.000000	0.000000000	0.000000	54581 > http [SYN] Seq=0 Win=8
2	2014-06-29 18:16:08.076586	0.019175	0.019175000	0.019175	http > 54581 [SYN, ACK] Seq=0
3	2014-06-29 18:16:08.076634	0.019223	0.000048000	0.000048	54581 > http [ACK] Seq=1 Ack=1
4	2014-06-29 18:16:08.076860	0.019449	0.000226000	0.000226	GET / HTTP/1.1
5	2014-06-29 18:16:08.102400	0.044989	0.025540000	0.025540	http > 54581 [ACK] Seq=1 Ack=6
6	2014-06-29 18:16:08.239464	0.182053	0.137064000	0.137064	HTTP/1.1 200 OK (text/html)

Abs Time steadily increases… as does **Relative time**
Frame Delta Time varies - is the difference between frames
Delta Time Displayed is diff between displayed frames
Also see: tcp.time_relative & tcp.time_delta times for TCP
Create multiple time columns and Show / Hide as needed

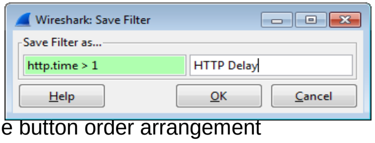
GET / is request for a homepage
ACK comes 25.5 ms later
First Byte resp 137 ms after that
Total First Byte RT is 163 ms
(with a network RTT of 19 ms)

Enable 'calculate conversation timestamps' in TCP Preferences to support delta times

Filter Expression Buttons

One of the best new features in Wireshark - quickly apply & clear useful analysis filters

1. Prepare & test a Display Filter
2. Click 'Save' on Display Filter Toolbar
3. Enter a button name - OK



http.time > 1
HTTP Delay

These are saved in your Personal Configuration *preferences* file. Edit this file manually to change the button order arrangement

Command Line Utilities

Tshark or **Dumpcap** for packet captures
tshark -h or dumpcap -h for options
-D to get list of interfaces - use intf # in cmd
-f <capture filter> in BPF format
-i <interface name or #>
-w <outfile> (pcap format)
Ex: tshark -i 2 -w tcapture.pcap
dumpcap -i 2 -f "host 192.168.1.116"
-b filesize:100000 -b files:3 -w capture.pcap
Ctrl-C to stop capture

Mergecap to merge packet trace files
mergecap -h for options

mergecap -w <outfile> <infile> <infile> [<inf…
-s <snaplen> - truncate to <snaplen> bytes
Ex: mergecap -w outfile.pcap infile1.pcap infile2.pcap infile3.pcap -s 128

Editcap to edit trace files -h for options
editcap [options] <infile> <outfile>
[<pkt #> [-<pkt #>] … (start @ Pkt # or range)
-A <start time> -B <stop> (YYYY-MM-DD hh:mm:ss)
-d remove duplicate packets (def window = 5)
-D <dup window> (0 to 1000000 pkts)
-w <dup time window> (rel sec e.g. 0.000001)
-t <time adjustment> - in rel sec e.g. -0.5 | 60
-c <pkts per file> -i <sec per file>
Ex: split a large trace file into multiple smaller files of 600 seconds: (outfiles will be #'d)
editcap -i 600 infile.pcap outfile_.pcap

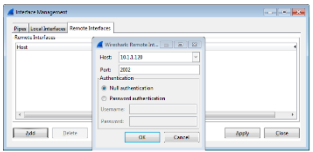
Capinfos to get trace info -h for options
capinfos [options] <infile>
-c # of pkts -d data size -u capture dur (s)
Ex: capinfos -cdu MyCapture.pcap

Remote Captures (Windows only)

Install WinPcap & start rpcapd.exe on remote machine

CMD window - navigate to WinPcap install directory
rpcapd -n (C:\Program Files (x86)\WinPcap\ )
You can use a -l (lower case 'L') with rpcapd to specify which hosts can connect. **rpcapd -h** for help

Wireshark:
Capture Options >
Manage Interfaces >
Remote Interfaces >
Add - enter remote machine's IP address & Port 2002 (default) - Ok - Close



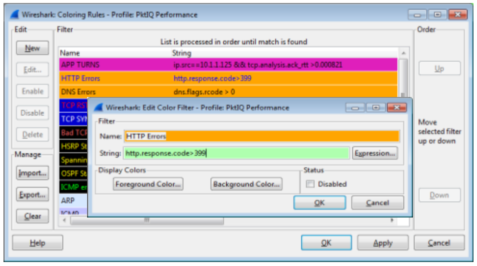
Host: 10.1.1.120
Port: 2002
● Null authentication
○ Password authentication
Username:
Password:

Capture Options:
Un-select unwanted interfaces - the desired intf will have the correct IP address listed under the Interface ID
Click **Start** - Click OK and ignore the capture buffer msg

Be aware that captured packets are sent from the remote machine to the controlling Wireshark machine

Coloring Rules

Colorization can be an effective tool for identifying and highlighting packets of interest. Wireshark has predefined coloring rules in a default file (colorfilters). But… sometimes too many colors can be distracting. Turn off most default rules, leave useful ones on or add your own based on Display Filter syntax and your colors


Wireshark: Coloring Rules - Profile: PktIQ Performance
Edit
New
Edit...
Enable
Disable
Delete
Manage
Import...
Export...
Clear
Filter
List is processed in order until match is found
Order
Up
Move selected filter up or down
Down
Help
OK
Apply
Cancel
Wireshark: Edit Color Filter - Profile: PktIQ Performance
Filter
Expression...
Display Colors
Foreground Color...
Background Color...
Status
OK
Cancel

Name	String
APP TURNS	ip.src==10.1.1.125 && tcp.analysis.ack_rtt >0.000821
HTTP Errors	http.response.code>399
DNS Errors	dns.flags.rcode > 0
TCP RST	
TCP SYN	
Bad TCP	
HSRP St	
Spannin	
OSPF St	
ICMP er	
ARP	
ICMP	

Name: HTTP Errors
String: http.response.code>399
□ Disabled

New / **Edit** / **Delete** - create, edit, or delete a rule
New/Edit: name, display filter string, fg and bg color
Enable / **Disable** - turn a rule on/off w/o deleting it

Up / **Down** - change the rule order. Wireshark evalutes coloring rules from top to bottom - first match is used, so you should **put more specific rules near the top**

Import / **Export** - import or share coloring rule files
Clear - remove all personal rules & revert to default rules

Analysis Tips

1. Turn off TCP releative sequence numbers to match captures from 2 or more locations by SEQ/ACK #'s
2. Turn off 'Allow subdissector to reassemble TCP streams' with HTTP to get 1st Byte response times
3. http.response.code > 399 to see HTTP err msgs
4. Disable Checksum Validations to eliminate false errs
5. Clear Win DNS cache: ipconfig / flushdns
   Linux: restart nscd (name service cache daemon)
6. Clear Win arp cache (elevated CMD): arp -d -a
7. WS frame dissector calcs / adds frame meta-data:
   frame # & timestamp - frame length & captured len
   coloring rules applied & coloring rule string

This guide is provided with PacketIQ Wireshark 101: Features & Functions training. WS 201: Performance Analysis and WS 301: Packets & Protocols training is also available. Contact **info@packetiq.com** or call us at **+1 321-888-2288** www.packetiq.com | Training