



# WONDER HOW TO

NULL BYTE

NEWS

## 8 Wireshark Filters Every Wiretapper

# Uses to Spy on Web Conversations and Surfing Habits

BY ALLEN FREEMAN

🕒 04/12/2012 7:52 PM

WIRESHARK

In my [Wireshark article](#), we talked a little bit about packet sniffing, but we focused more on the underlying protocols and models. Now, I'd like to dive right back into Wireshark and start stealing packets.

The filtering capabilities here are very comprehensive. You can filter on just about any field of any protocol,

🔥 HOT

🕒 LATEST

The image shows the Facebook logo, which consists of the word "facebook" in white lowercase letters on a blue rectangular background.

HOW TO

**4 Ways to Crack a Facebook Password & How to Protect Yourself from Them**



even down to the [hex values](#) in a data stream. Sometimes, the hardest part about setting a filter in Wireshark is remembering the syntax, so below are the top display filters that I use. All examples below are from a 10 minute period of packet capture on my lab network. I am simply using filters to manage the view.

## What Is a Filter?

When you first fire up Wireshark, it can be daunting. Servers are broadcasting, computers are asking for webpages, and on top of this, the colors are difficult to digest with confusing number sequences to boot. Working from this mess would be a headache!



HOW TO

**Get Unlimited Free Trials Using a "Real" Fake Credit Card Number**

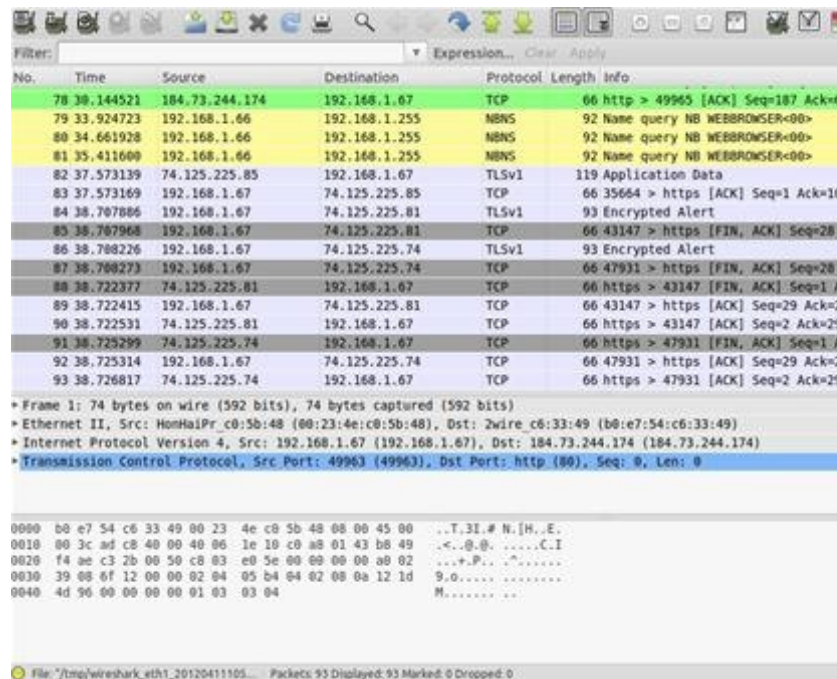


HOW TO

**Buy the Best Wireless Network Adapter for Wi-Fi Hacking in 2019**







No.	Time	Source	Destination	Protocol	Length	Info
78	30.144521	184.73.244.174	192.168.1.67	TCP	66	http > 49965 [ACK] Seq=187 Ack=62
79	33.924723	192.168.1.66	192.168.1.255	MBNS	92	Name query NB WEBBROWSER<00>
80	34.661928	192.168.1.66	192.168.1.255	MBNS	92	Name query NB WEBBROWSER<00>
81	35.411609	192.168.1.66	192.168.1.255	MBNS	92	Name query NB WEBBROWSER<00>
82	37.573139	74.125.225.85	192.168.1.67	TLSv1	119	Application Data
83	37.573169	192.168.1.67	74.125.225.85	TCP	66	35664 > https [ACK] Seq=1 Ack=107
84	38.707886	192.168.1.67	74.125.225.81	TLSv1	93	Encrypted Alert
85	38.787968	192.168.1.67	74.125.225.81	TCP	66	43147 > https [FIN, ACK] Seq=28 A
86	38.788226	192.168.1.67	74.125.225.74	TLSv1	93	Encrypted Alert
87	38.788273	192.168.1.67	74.125.225.74	TCP	66	47931 > https [FIN, ACK] Seq=28 A
88	38.722377	74.125.225.81	192.168.1.67	TCP	66	https > 43147 [FIN, ACK] Seq=1 A
89	38.722415	192.168.1.67	74.125.225.81	TCP	66	43147 > https [ACK] Seq=29 Ack=2
90	38.722531	74.125.225.81	192.168.1.67	TCP	66	https > 43147 [ACK] Seq=2 Ack=29
91	38.725299	74.125.225.74	192.168.1.67	TCP	66	https > 47931 [FIN, ACK] Seq=1 A
92	38.725314	192.168.1.67	74.125.225.74	TCP	66	47931 > https [ACK] Seq=29 Ack=2
93	38.726817	74.125.225.74	192.168.1.67	TCP	66	https > 47931 [ACK] Seq=2 Ack=29

\*Frame 1: 74 bytes on wire (592 bits), 74 bytes captured (592 bits)  
 \* Ethernet II, Src: HonHaiPr\_c0:5b:48 (00:23:4e:c0:5b:48), Dst: Zwire\_c6:33:49 (b0:e7:54:c6:33:49)  
 \* Internet Protocol Version 4, Src: 192.168.1.67 (192.168.1.67), Dst: 184.73.244.174 (184.73.244.174)  
 \* Transmission Control Protocol, Src Port: 49963 (49963), Dst Port: http (80), Seq: 0, Len: 0

0000 b0 e7 54 c6 33 49 00 23 4e c0 5b 48 08 00 45 00 ..T.ZI.# N.[H..E.  
 0010 00 3c ad c8 40 00 40 06 1e 10 c0 a8 01 43 b8 49 ...@.@.....C.I  
 0020 f4 ae c3 2b 00 50 c8 03 e0 5e 00 00 00 a0 02 ...+.P.....  
 0030 39 08 6f 12 00 00 02 04 05 b4 04 02 08 0a 12 1d 9.o.....  
 0040 4d 90 00 00 00 00 01 03 03 04 M.....

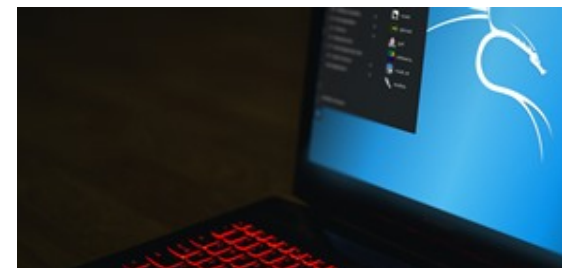
File: /tmp/wireshark\_eth1\_20120411105... Packets: 93 Displayed: 93 Marked: 0 Dropped: 0

Moving into larger wireless networks, the sheer amount of broadcast traffic alone will slow you down and get in your way. Thankfully, Wireshark includes a rich yet simple filter language that allows you to build quite complex expressions. You can compare values in packets, search for strings, hide protocols you don't need, and so much more.



## HOW TO HACK WI-FI

Get Anyone's Wi-Fi Password Without Cracking Using Wifiphisher



## HOW TO

Top 10 Things to Do After Installing Kali Linux

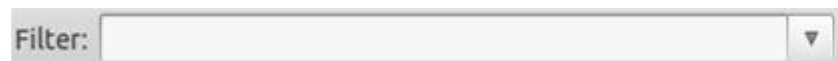


## HOW TO

Crack Any Master Combination Lock in 8 Tries or Less Using This Calculator

## Wait! Where Do I Find These Filters?!

The most visible and easy to use spot is right in front of you!



Whoop there it is. You can type filter syntax right into this field and watch in wonder as your once jumbled pile of messages transforms into a neat clean stack ordered how you tell it. This works on a live capture, as well as in files of dates you might be importing.

Also, as you type, notice the color of the text field changes from red to green, signaling when you have a

### HOW TO

**Crack Wi-Fi Passwords with Your Android Phone and Get Free Internet!**

### HOW TO

**Hack WPA & WPA2 Wi-Fi Passwords with a Pixie-Dust Attack Using Airedodn**

### ANDROID FOR HACKERS

**How to Turn an Android Phone into a Hacking Device Without Root**

valid filter. The auto complete guesses are also there to help you put together new combos of filtering.

## ip.addr ==x.x.x.x

Sets a filter for any packet with x.x.x.x, as either the source or destination IP address. This is useful if you want to look for specific machines or networks. A good example would be some odd happenings in your server logs, now you want to check outgoing traffic and see if it matches. This is a great filter for that.

Filter: ip.addr==192.168.1.67 Expression... Clear Apply					
No.	Time	Source	Destination	Protocol	Length Info
466	6.903752	58.18.261.178	192.168.1.67	TCP	66 http > 55532 [ACK] Seq=187 Ack=6
467	6.959820	69.63.190.72	192.168.1.67	TLSv1	1514 Server Hello
468	6.959856	192.168.1.67	69.63.190.72	TCP	66 58725 > https [ACK] Seq=172 Ack=
469	6.963882	69.63.190.72	192.168.1.67	TCP	1514 [TCP segment of a reassembled PD
470	6.963839	192.168.1.67	69.63.190.72	TCP	66 58725 > https [ACK] Seq=172 Ack=
471	6.966789	69.63.190.72	192.168.1.67	TCP	1266 [TCP segment of a reassembled PD
472	6.966822	192.168.1.67	69.63.190.72	TCP	66 58725 > https [ACK] Seq=172 Ack=
473	6.996956	69.63.190.72	192.168.1.67	TLSv1	191 Certificate, Server Hello Done
474	6.996990	192.168.1.67	69.63.190.72	TCP	66 58725 > https [ACK] Seq=172 Ack=
475	6.998647	192.168.1.67	69.63.190.72	TLSv1	252 Client Key Exchange, Change Ciph
476	7.036540	69.63.190.72	192.168.1.67	TCP	66 https > 58725 [ACK] Seq=4222 Ack
477	7.217735	69.63.190.72	192.168.1.67	TLSv1	320 Encrypted Handshake Message, Cha

### HOW TO

#### Brute-Force Nearly Any Website Login with Hatch

### HOW TO

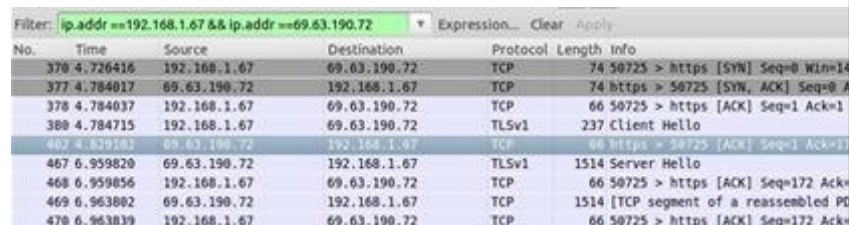
#### Check if Your Wireless Network Adapter Supports Monitor Mode & Packet Injection

### HOW TO

#### Hack Android Using Kali (Remotely)

`ip.addr ==x.x.x.x && ip.addr ==x.x.x.x`

Sets a conversation filter between the two IP addresses. This is useful to watch communication between two specific hosts or networks. Sometimes you only need specific data, so there is no need to bother sifting through the others.



The screenshot shows a Wireshark interface with a filter bar at the top containing the expression `ip.addr == 192.168.1.67 && ip.addr == 69.63.190.72`. Below the filter is a table of captured packets:

No.	Time	Source	Destination	Protocol	Length	Info
370	4.726416	192.168.1.67	69.63.190.72	TCP	74	50725 > https [SYN] Seq=0 Win=14
377	4.784017	69.63.190.72	192.168.1.67	TCP	74	https > 50725 [SYN, ACK] Seq=0 A
378	4.784037	192.168.1.67	69.63.190.72	TCP	66	50725 > https [ACK] Seq=1 Ack=1
380	4.784715	192.168.1.67	69.63.190.72	TLSv1	237	Client Hello
402	4.839102	69.63.190.72	192.168.1.67	TCP	66	https > 50725 [ACK] Seq=1 Ack=1
467	6.959820	69.63.190.72	192.168.1.67	TLSv1	1514	Server Hello
468	6.959856	192.168.1.67	69.63.190.72	TCP	66	50725 > https [ACK] Seq=172 Ack=
469	6.963802	69.63.190.72	192.168.1.67	TCP	1514	[TCP segment of a reassembled PD
470	6.963839	192.168.1.67	69.63.190.72	TCP	66	50725 > https [ACK] Seq=172 Ack=

Also of note with the '&&' operator—those of you who are familiar with programming will know this—but it

## HOW TO

### Find Vulnerable Webcams Across the Globe Using Shodan

## HACK LIKE A PRO

### How to Find Directories in Websites Using DirBuster

## HOW TO HACK BLUETOOTH, PART 1

### Terms, Technologies, & Security

could be repeated. The '&&' will return both conditions in the statement, and not one or the other as is sometimes thought. And yes, you need *both* of the ampersands.

## http or dns

Sets a filter based on protocol. You do not always need to know every single packet traveling across, so being able to narrow down to the exact protocol you need is helpful. Looking to track some odd FTP traffic? set it for 'ftp'. Looking to see why you can't find any websites? Try setting it to 'dns' and see what is going on.

HACK LIKE A PRO

**How to Hack Facebook (Facebook Password Extractor)**

HOW TO HACK WI-FI

**Stealing Wi-Fi Passwords with an Evil Twin Attack**

HOW TO

**Automate Wi-Fi Hacking with Wifite2**



No.	Time	Source	Destination	Protocol	Length	Info
459	5.901738	192.168.1.67	50.16.201.176	HTTP	688	GET /ping?hwonderhowto.com&p%2f
463	5.904590	50.16.201.176	192.168.1.67	HTTP	251	[TCP Out-of-Order] HTTP/1.1 200
1299	50.794862	192.168.1.67	50.16.201.176	HTTP	687	GET /ping?hwonderhowto.com&p%2f
1383	50.845030	50.16.201.176	192.168.1.67	HTTP	251	[TCP Out-of-Order] HTTP/1.1 200
1380	61.813243	192.168.1.67	239.255.255.250	SSDP	175	M-SEARCH * HTTP/1.1
1381	61.813275	192.168.1.67	239.255.255.250	SSDP	174	M-SEARCH * HTTP/1.1
1382	61.813364	192.168.1.67	239.255.255.250	SSDP	175	M-SEARCH * HTTP/1.1
1383	61.813378	192.168.1.67	239.255.255.250	SSDP	174	M-SEARCH * HTTP/1.1
1492	63.104549	192.168.1.67	204.9.163.247	HTTP	221	GET http://ui.skype.com/ui/2/2.2.
1494	63.139300	204.9.163.247	192.168.1.67	HTTP	455	HTTP/1.1 200 OK (text/html)
1656	78.812318	192.168.1.67	98.129.110.26	HTTP	1363	POST /ajax/KeepAlive.aspx?rt=jsor
1657	78.956981	98.129.110.26	192.168.1.67	HTTP	551	HTTP/1.1 200 OK (text/html)
1795	96.854909	192.168.1.67	239.255.255.250	SSDP	175	M-SEARCH * HTTP/1.1
1796	96.855057	192.168.1.67	239.255.255.250	SSDP	174	M-SEARCH * HTTP/1.1
1797	96.855112	192.168.1.67	239.255.255.250	SSDP	175	M-SEARCH * HTTP/1.1
1798	96.855216	192.168.1.67	239.255.255.250	SSDP	174	M-SEARCH * HTTP/1.1
2066	126.106126	192.168.1.67	50.16.209.140	HTTP	689	GET /ping?hwonderhowto.com&p%2f
2068	126.153107	50.16.209.140	192.168.1.67	HTTP	251	HTTP/1.1 200 OK (GIF89a)

\* Frame 459: 688 bytes on wire (5504 bits), 688 bytes captured (5504 bits)

\* Ethernet II, Src: HonMaiPr\_c0:5b:48 (08:23:4e:c0:5b:48), Dst: 2wire\_c6:33:49 (b0:e7:54:c6:33:49)

\* Internet Protocol Version 4, Src: 192.168.1.67 (192.168.1.67), Dst: 50.16.201.176 (50.16.201.176)

\* Transmission Control Protocol, Src Port: 55532 (55532), Dst Port: http (80), Seq: 1, Ack: 1, Len: 622

\* Hypertext Transfer Protocol, Request

```

0000  b0 e7 54 c6 33 49 00 23 4e c0 5b 48 00 00 45 00  ..T.II.# N.[H..E.
0010  82 a2 4b 3f 40 80 40 06 2f 6b c0 a0 01 43 32 10  ..K70.0. /k...C2.
0020  c9 b9 d8 ec 00 50 82 a0 c8 ef 20 d6 f8 96 80 18  ....P.....
0030  03 91 ae df 00 00 01 01 00 0a 00 0a 83 dc 3e ae  ....>.....
0040  c3 64 47 45 54 20 2f 70 69 6e 67 3f 68 3d 77 6f  .dGET /p ing?hw
0050  8e 64 65 72 68 6f 77 74 6f 2e 63 6f 6d 26 70 3d  nderhowt o.com&p
0060  25 32 46 62 6c 6f 67 25 32 46 74 65 6e 2d 67 72  %2Fblog% 2Ften-gr
0070  65 61 74 2d 77 69 72 65 73 68 61 72 6b 2d 66 69  eat-wire shark-fi
0080  74 68 73 75 7d 47 68 74 7d 70 6f 78 7d 67 69  746873757d4768747d706f787d6769

```

File: /tmp/wireshark\_eth1\_20120411121... Packets: 3975 Displayed: 32 Marked: 0 Dropped: 0

## HOW TO HACK WI-FI

## Cracking WPA2 Passwords Using the New PMKID Hashcat Attack

## HACK LIKE A PRO

## How to Secretly Hack Into, Switch On, & Watch Anyone's Webcam Remotely

ALL FEATURES



© 2019 WonderHowTo, Inc.

tcp.port==xxx

Sets filters based on TCP port numbers. Because port numbers can be reassigned and used in various places (within obvious limitations), it is useful to be able to just look at traffic going into and out of a specific port. Here we will look for all traffic using port 80 (HTTP).



No.	Time	Source	Destination	Protocol	Length	Info
436	5.903293	192.168.1.67	50.16.201.176	TCP	74	55532 > http [STN] Seq=1 Win=1460
457	5.901521	50.16.201.176	192.168.1.67	TCP	74	http > 55532 [SYN, ACK] Seq=0 Ack=1
458	5.901558	192.168.1.67	50.16.201.176	TCP	66	55532 > http [ACK] Seq=1 Ack=1
459	5.901738	192.168.1.67	50.16.201.176	HTTP	688	GET /ping?h=wonderhowto.com&p=42
460	5.948656	50.16.201.176	192.168.1.67	TCP	66	http > 55532 [ACK] Seq=1 Ack=623
461	5.964353	50.16.201.176	192.168.1.67	TCP	66	[TCP Previous segment lost] http
462	5.964382	192.168.1.67	50.16.201.176	TCP	78	[TCP Dup ACK 459#1] 55532 > http
463	5.964598	50.16.201.176	192.168.1.67	HTTP	251	[TCP Out-Of-Order] HTTP/1.1 200
464	5.964613	192.168.1.67	50.16.201.176	TCP	66	55532 > http [ACK] Seq=623 Ack=1
465	5.965217	192.168.1.67	50.16.201.176	TCP	66	55532 > http [FIN, ACK] Seq=623

## `tcp.flags.reset==1`

Sets filters to show all TCP resets. Each packet contains a TCP header. Each of these headers contains a bit known as the "reset" flag. In most packets, this bit is set to 0 and has no effect, however if this bit is set to 1, it indicates to the receiving computer that it should immediately stop using the connection —A TCP reset basically kills a TCP connection instantly.

Filter: tcp.flags.reset==1		Expression... Clear Apply			
No.	Time	Source	Destination	Protocol	Length Info
561	8.704360	192.168.1.67	8.18.42.210	TCP	54 53908
563	8.704565	192.168.1.67	8.18.42.210	TCP	54 53908
565	8.706573	192.168.1.67	8.18.42.210	TCP	54 53908
568	8.709705	192.168.1.67	96.16.123.206	TCP	54 52348
570	8.709888	192.168.1.67	96.16.123.206	TCP	54 52348
572	8.710712	192.168.1.67	96.16.123.206	TCP	54 52348

## http.request

Sets a filter for all [HTTP](#) GET and POST requests. This will show webpages being accessed for the most part here.

Filter: http.request		Expression... Clear Apply			
No.	Time	Source	Destination	Protocol	Length Info
438	5.901738	192.168.1.67	50.16.201.176	HTTP	688 GET /ping?h=wonderhowto.com&p=42
1299	50.794862	192.168.1.67	50.16.201.176	HTTP	687 GET /ping?h=wonderhowto.com&p=42
1380	61.013243	192.168.1.67	239.255.255.250	SSDP	175 M-SEARCH * HTTP/1.1
1381	61.013275	192.168.1.67	239.255.255.250	SSDP	174 M-SEARCH * HTTP/1.1
1382	61.013364	192.168.1.67	239.255.255.250	SSDP	175 M-SEARCH * HTTP/1.1
1383	61.013378	192.168.1.67	239.255.255.250	SSDP	174 M-SEARCH * HTTP/1.1
1492	63.104549	192.168.1.67	204.9.163.247	HTTP	221 GET http://ui.skype.com/ui/2/2.2
1656	78.012318	192.168.1.67	98.129.110.26	HTTP	1363 POST /ajax/KeepAlive.aspx?rt=json
1795	96.054909	192.168.1.67	239.255.255.250	SSDP	175 M-SEARCH * HTTP/1.1

## tcp contains xxx

Set a filter based on a string you provide and searches TCP packets for that string. If you were looking for a specific item or user name you knew was appearing in the packet, this is a filter you could use. Here we type 'wonder' as I am writing this article and we see:

Filter: tcp contains wonder					
No.	Time	Source	Destination	Protocol	Length Info
459	5.901738	192.168.1.67	50.16.201.176	HTTP	688 GET /ping?h=wonderhowto.com&p=529
1299	56.794862	192.168.1.67	50.16.201.176	HTTP	687 GET /ping?h=wonderhowto.com&p=529
1656	78.812318	192.168.1.67	98.129.110.26	HTTP	1363 POST /ajax/KeepAlive.aspx?rt=json
2066	126.196126	192.168.1.67	50.16.209.140	HTTP	689 GET /ping?h=wonderhowto.com&p=529

\* Frame 459: 688 bytes on wire (5504 bits), 688 bytes captured (5504 bits)  
 \* Ethernet II, Src: HonMaiPr c8:5b:48 (08:23:4e:c8:5b:48), Dst: Zwire c6:33:49 (b8:e7:54:c6:33:49)  
 \* Internet Protocol Version 4, Src: 192.168.1.67 (192.168.1.67), Dst: 50.16.201.176 (50.16.201.176)  
 \* Transmission Control Protocol, Src Port: 55532 (55532), Dst Port: http (80), Seq: 1, Ack: 1, Len: 622

## !(arp or icmp or dns)

This filter format is designed to filter out certain types of protocols you might not want. In my example, we have ARP, ICMP, and DNS—all of which are broadcasts—to hide. This lets our eyes work on other things.

Filter: !(arp or icmp or dns)					
No.	Time	Source	Destination	Protocol	Length Info
459	5.901738	192.168.1.67	50.16.201.176	HTTP	688 GET /ping?h=wonderhowto.com&p=529
460	5.948656	50.16.201.176	192.168.1.67	TCP	66 http > 55532 [ACK] Seq=1 Ack=623
461	5.964353	50.16.201.176	192.168.1.67	TCP	66 [TCP Previous segment lost] http
462	5.964383	192.168.1.67	50.16.201.176	TCP	78 [TCP Dup ACK 459#1] 55532 > http
463	5.964598	50.16.201.176	192.168.1.67	HTTP	251 [TCP Out-Of-Order] HTTP/1.1 200
464	5.964613	192.168.1.67	50.16.201.176	TCP	66 55532 > http [ACK] Seq=623 Ack=1
465	5.965217	192.168.1.67	50.16.201.176	TCP	66 55532 > http [FIN, ACK] Seq=623
466	6.003752	50.16.201.176	192.168.1.67	TCP	66 http > 55532 [ACK] Seq=187 Ack=6
467	6.959820	69.63.190.72	192.168.1.67	TLSv1	1514 Server Hello
468	6.959856	192.168.1.67	69.63.190.72	TCP	66 50725 > https [ACK] Seq=172 Ack=
469	6.963892	69.63.190.72	192.168.1.67	TCP	1514 [TCP segment of a reassembled PD
470	6.963839	192.168.1.67	69.63.190.72	TCP	66 50725 > https [ACK] Seq=172 Ack=

## In Closing



Do you have other filters you use? Share them with us! There are a lot of useful combos and I know I did not list all of them here.

Leave us a comment below, shoot [me a message](#) or start a thread in [our forum](#).

- Follow Null Byte on [Twitter](#), [Flipboard](#), and [YouTube](#)
- Sign up for [Null Byte's weekly newsletter](#)
- Follow WonderHowTo on [Facebook](#), [Twitter](#), [Pinterest](#), and [Flipboard](#)

Image by HSC

## Never Miss a Hacking or Security Guide

New Null Byte in your inbox, every week.

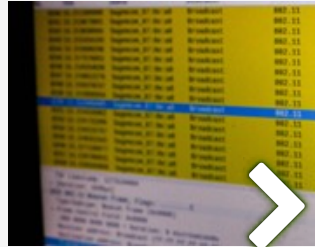
 GET THE NEWSLETTER

## Related



HOW TO

**Stealthfully Sniff Wi-Fi Activity Without Connecting to a Target Router**



HOW TO

**Detect Script-Kiddie Wi-Fi Wireshark**

## 2 Comments



**OSKAR VANHOVE**  
2 YEARS AGO

2



nice and juicy

↩ REPLY



**GAIRALA VAU**  
2 YEARS AGO

1



cool

↩ REPLY

## Share Your Thoughts



YOU

LOGIN TO COMMENT

Click to share your thoughts

[WonderHowTo.com](#) [About Us](#) [Privacy Policy](#) [Terms of Use](#)

Don't Miss:

[New iOS 13 Features — The 200+ Best, Hidden & Most Exciting New Changes for iPhone](#)

[13 Apple Maps Features & Changes in iOS 13 You Need to Know About](#)

[15 Awesome 'Reminders' Features in iOS 13 That'll Make You Actually Want to Use the App](#)

[The Best New Siri Features & Commands in iOS 13 for iPhone](#)

[Memoji Stickers, Improved Search & More New Apple Messages Features in iOS 13 for iPhone](#)

[20+ Features in iOS 13's Safari You Don't Want to Miss](#)

[iOS 13's Notes App Is Packing 15 Cool New Features & Changes](#)

[31 New Features for Camera & Photos in iOS 13](#)

