

WIRESHARK

The image displays the Wireshark Network Analyzer interface. The top menu bar includes File, Edit, View, Go, Capture, Analyze, Statistics, Telephony, Wireless, Tools, and Help. Below the menu is a toolbar with various icons for file operations, capture, and analysis. A status bar at the top indicates "Apply a display filter ... <Ctrl-/>".

The main window is divided into three panes:

- Left Pane (Capture Filter):** Shows the "Welcome to Wireshark" message and a list of capture filters. The "Capture" section includes a text input field for "Enter a capture filter ..." and a dropdown menu for "All interfaces shown". Below this, a list of capture filters is displayed, including "vEthernet (WSL (Hyper-V firewall))", "Wi-Fi", "Local Area Connection* 2", "Adapter for loopback traffic capture", "Local Area Connection* 10", "Local Area Connection* 9", "Local Area Connection* 8", "Local Area Connection* 1", "Local Area Connection", and "Event Tracing for Windows (ETW) reader".
- Middle Pane (Packet List):** Displays a list of captured packets. The columns are No., Time, Source, Destination, Protocol, Length, and Info. The first packet is selected, showing details in the right pane.
- Right Pane (Packet Details):** Shows the details of the selected packet (Frame 1). It includes a tree view on the left with expandable sections: "Frame 1: 60 bytes on wire (480 bits), 60 bytes captured (480 bits) on interface \\Device\\NPF_{70238D93-1A...}", "Ethernet II, Src: CloudNetwork_F9:e6:bf (d8:80:83:f9:e6:bf), Dst: Broadcast (ff:ff:ff:ff:ff:ff)", and "Address Resolution Protocol (request)". The right side of the pane shows the raw packet data in hexadecimal and ASCII.

The status bar at the bottom indicates "Wi-Fi: <live capture in progress>" and "Packets: 422".

*Wi-Fi

File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help

http

No.	Time	Source	Destination	Protocol	Length	Info
18	0.717860	Sophos_fc:00:0f	Broadcast	ARP	60	Who has 10.1.2.217? Tell 10.1.0.1
19	0.717860	LiteonTechno_78:45:...	Broadcast	ARP	60	Who has 10.1.7.49? Tell 10.1.8.56
20	0.717860	32:2f:e7:3d:f2:2f	Broadcast	ARP	60	Gratuitous ARP for 10.1.0.179 (Reply)
21	0.819391	CloudNetwork_f9:e6:...	Broadcast	ARP	60	Who has 10.1.6.226? (ARP Probe)
22	0.819391	6a:f2:99:63:4b:b7	Broadcast	ARP	60	Who has 10.1.0.17? Tell 10.1.9.58
23	0.820364	fe80::c0e8:a7ff:fe0... ff02::1	ICMPv6	86	Neighbor Advertisement fe80::c0e8:a7ff:fe0... (ovr) is at d8:80:83:f9:e6:bf	
24	0.820364	fe80::c0e8:a7ff:fe0... ff02::2	ICMPv6	70	Router Solicitation from c2:e8:a7:03:52:d2	
25	0.921946	Sophos_fc:00:0f	Broadcast	ARP	60	Who has 10.1.1.110? Tell 10.1.0.1
26	0.921946	16:d1:a6:d8:4f:5a	Broadcast	ARP	60	Gratuitous ARP for 10.1.10.101 (Reply)
27	1.002454	10.1.5.119	104.208.16.92	TCP	55	58424 → 443 [ACK] Seq=1 Ack=1 Win=255 Len=1
28	1.024463	16:d1:a6:d8:4f:5a	Broadcast	ARP	60	Who has 10.1.0.17? Tell 10.1.10.101
29	1.034789	10.1.5.119	104.208.16.92	TCP	55	58423 → 443 [ACK] Seq=1 Ack=1 Win=254 Len=1
30	1.126587	de:47:55:a7:3f:e8	Broadcast	ARP	60	Who has 10.1.0.17? Tell 10.1.3.52
31	1.126587	1a:cd:bb:d6:0d:16	Broadcast	ARP	60	Who has 10.1.0.17? Tell 10.1.1.63
32	1.259841	104.208.16.92	10.1.5.119	TCP	66	443 → 58424 [ACK] Seq=1 Ack=2 Win=16382 Len=0 SLE=1 SRE=2
33	1.299486	104.208.16.92	10.1.5.119	TCP	66	443 → 58423 [ACK] Seq=1 Ack=2 Win=16381 Len=0 SLE=1 SRE=2
34	1.332665	Sophos_fc:00:0f	Broadcast	ARP	60	Who has 10.1.1.35? Tell 10.1.0.1
35	1.536701	Sophos_fc:00:0f	Broadcast	ARP	60	Who has 10.1.7.191? Tell 10.1.0.1

> Frame 16: 60 bytes on wire (480 bits), 60 bytes captured (480 bits) on interface \Device\NPF_{70238D93-...}

> Ethernet II, Src: Sophos_fc:00:0f (c8:4f:86:fc:00:0f), Dst: Broadcast (ff:ff:ff:ff:ff:ff)

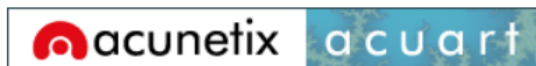
> Address Resolution Protocol (request)

ff ff ff ff ff ff ff ff e8 4f 86 fc 00 0f 00 00 00 010.....
0010 08 00 06 04 00 01 c8 4f 86 fc 00 0f 0a 01 00 010.....
0020 00 00 00 00 00 00 0a 01 00 4b 00 00 00 00 00K.....
0030 00 00 00 00 00 00 00 00 00 00 00 00 00 000.....

HyperText Transfer Protocol: Protocol

Packets: 2833 - Dropped: 0 (0.0%)

Profile: Default



TEST and Demonstration site for **Acunetix Web Vulnerability Scanner**

[home](#) | [categories](#) | [artists](#) | [disclaimer](#) | [your cart](#) | [guestbook](#) | [AJAX Demo](#)

search art

[Browse categories](#)

[Browse artists](#)

[Your cart](#)

[Signup](#)

[Your profile](#)

[Our guestbook](#)

[AJAX Demo](#)

Links

[Security art](#)

[PHP scanner](#)

[PHP vuln help](#)

[Fractal Explorer](#)



If you are already registered please enter your login information below:

Username :

Password :

You can also [signup here](#).

Signup disabled. Please use the username **test** and the password **test**.

[About Us](#) | [Privacy Policy](#) | [Contact Us](#) | ©2019 Acunetix Ltd

Warning: This is not a real shop. This is an example PHP application, which is intentionally vulnerable to web attacks. It is intended to help you test Acunetix. It also helps you understand how developer errors and bad configuration may let someone break into your website. You can use it to test other tools and your manual hacking skills as well. Tip: Look for potential SQL Injections, Cross-site Scripting (XSS), and Cross-site Request Forgery (CSRF), and more.

Wi-Fi

File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help

http

No.	Time	Source	Destination	Protocol	Length	Info
755	29.145102	10.1.5.119	23.44.5.227	HTTP	165	GET /connecttest.txt HTTP/1.1
761	29.217065	23.44.5.227	10.1.5.119	HTTP	241	HTTP/1.1 200 OK (text/plain)
1357	55.390462	10.1.5.119	23.44.5.227	HTTP	178	GET /ncsi.txt HTTP/1.1
1360	55.449431	23.44.5.227	10.1.5.119	HTTP	233	HTTP/1.1 200 OK (text/plain)
1454	59.426071	10.1.5.119	23.200.218.161	HTTP	165	GET /connecttest.txt HTTP/1.1
1457	59.486979	23.200.218.161	10.1.5.119	HTTP	241	HTTP/1.1 200 OK (text/plain)
2479	89.577953	10.1.5.119	23.211.60.150	HTTP	165	GET /connecttest.txt HTTP/1.1
2484	89.620369	23.211.60.150	10.1.5.119	HTTP	241	HTTP/1.1 200 OK (text/plain)

> Frame 755: 165 bytes on wire (1320 bits), 165 bytes captured (1320 bits) on interface \Device\NPF_{70236...}

> Ethernet II, Src: AzureWaveTec_50:6a:f1 (f8:54:f6:50:6a:f1), Dst: Sophos_fc:00:0f (c8:4f:86:fc:00:0f)

> Internet Protocol Version 4, Src: 10.1.5.119, Dst: 23.44.5.227

> Transmission Control Protocol, Src Port: 58429, Dst Port: 80, Seq: 1, Ack: 1, Len: 111

> Hypertext Transfer Protocol

0000 c8 4f 86 fc 00 0f f8 54 f6 50 6a f1 08 00 45 00 -O....T.Pj...E-

0010 00 97 1d 80 40 00 00 06 b0 5a 0a 01 05 77 17 2c ...@...Z...w,

0020 05 e3 e4 1d 00 50 cc da 3b b0 a4 7d b2 87 50 18 ...aP...8...P

0030 00 ff 81 7f 00 00 47 45 54 20 2f 63 6f 6e 6e 65GET /conne

0040 63 74 74 65 73 74 2e 74 78 74 20 48 54 54 50 2f cttest.txt HTTP/

0050 31 2e 31 0d 0a 43 6f 6e 6e 65 63 74 69 6f 6e 3a 1.1 -Con nection:

0060 20 43 6c 6f 73 65 0d 0a 55 73 65 72 2d 41 67 65 Close - User-Age

0070 6e 74 3a 20 4d 69 63 72 6f 73 6f 66 74 20 4e 43 nt: Micr osoft NC

0080 53 49 0d 0a 48 6f 73 74 3a 20 77 77 77 2e 6d 73 SI -Host : www.ms

0090 66 74 63 6f 6e 6e 65 63 74 74 65 73 74 2e 63 6f ftconnec ttest.co

00a0 6d 0d 0a 0d 0a m....

wireshark_Wi-Fi2DBIC3.pcapng

Packets: 2833 - Displayed: 8 (0.3%) - Dropped: 0 (0.0%)

Profile: Default