

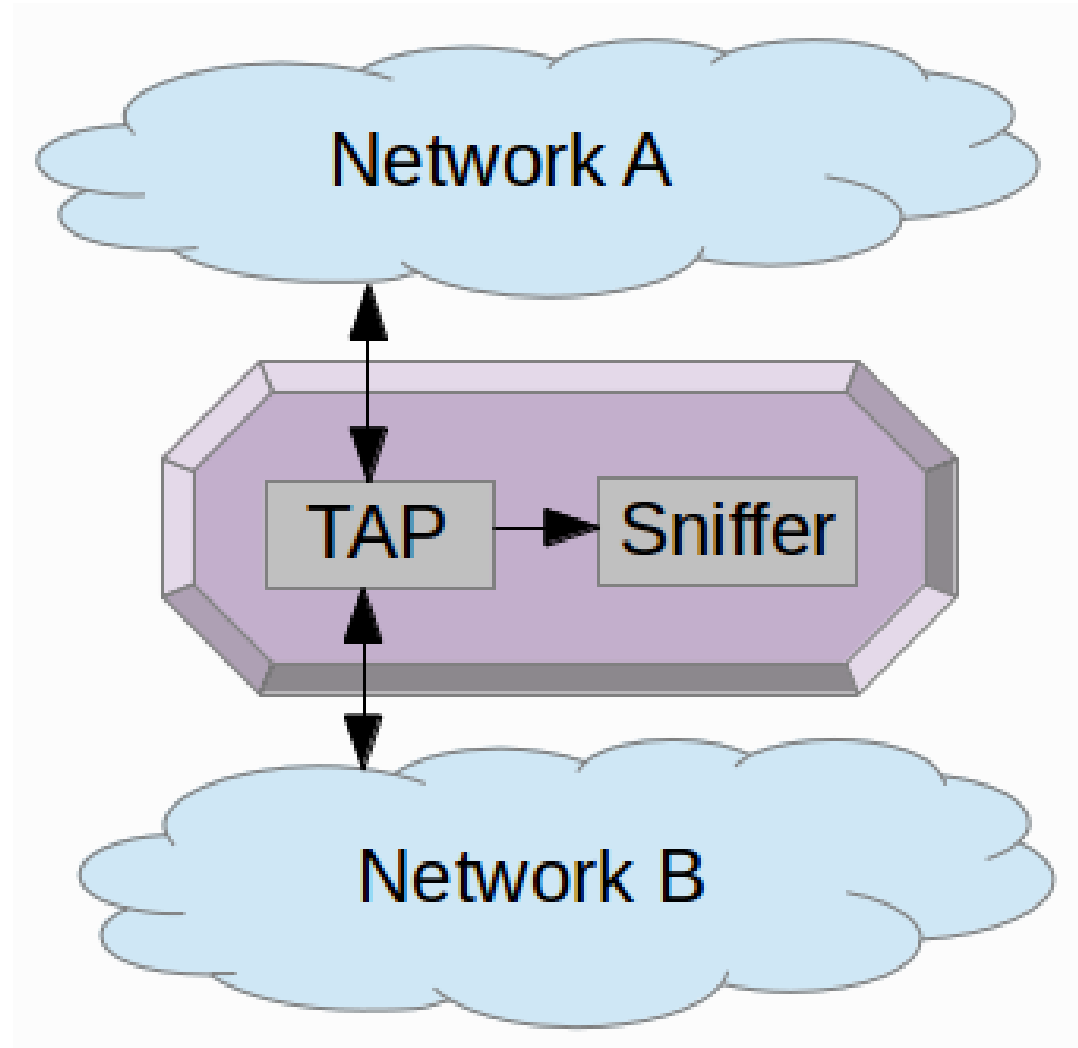
Wireshark

Um Analisador de Protocolos

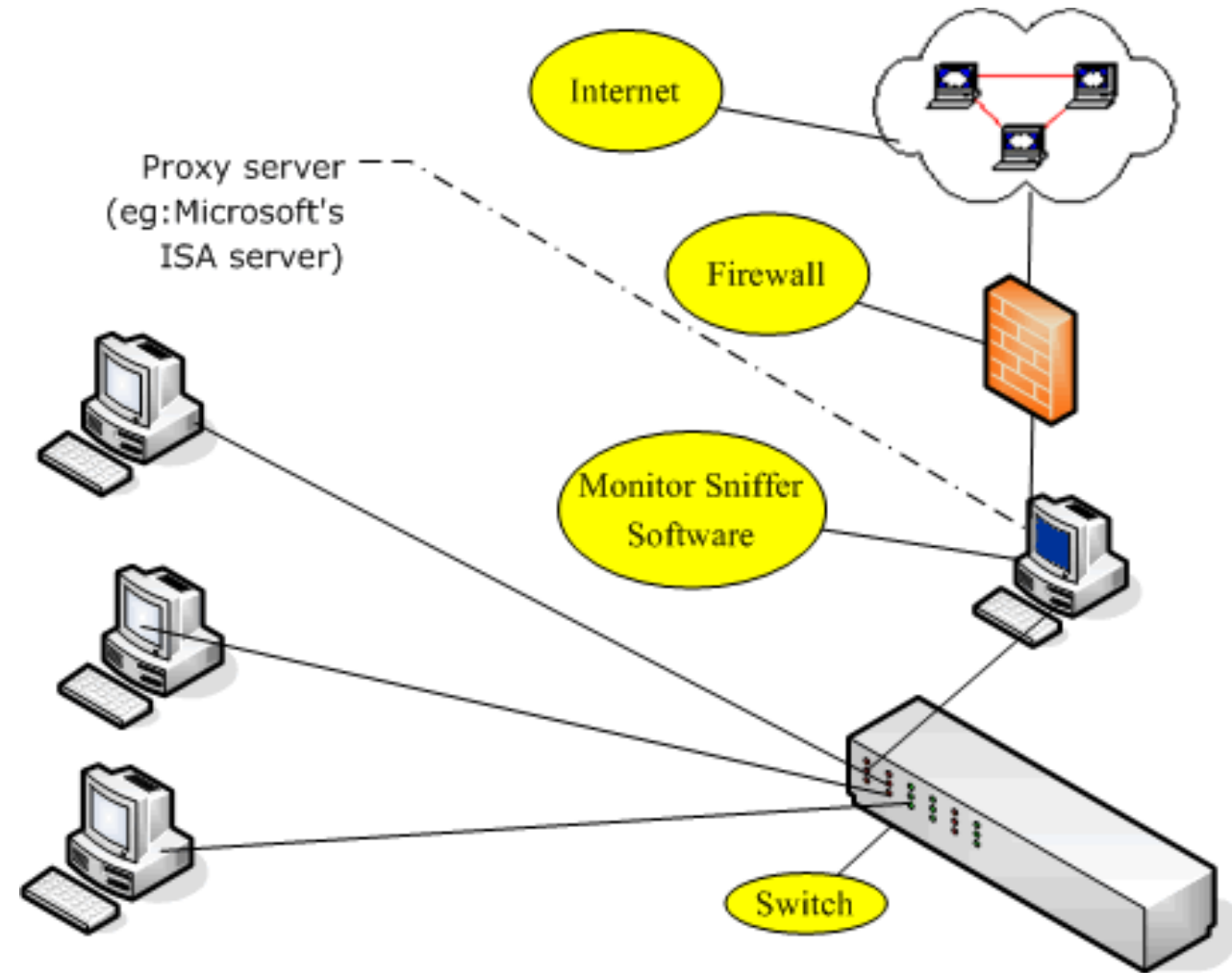
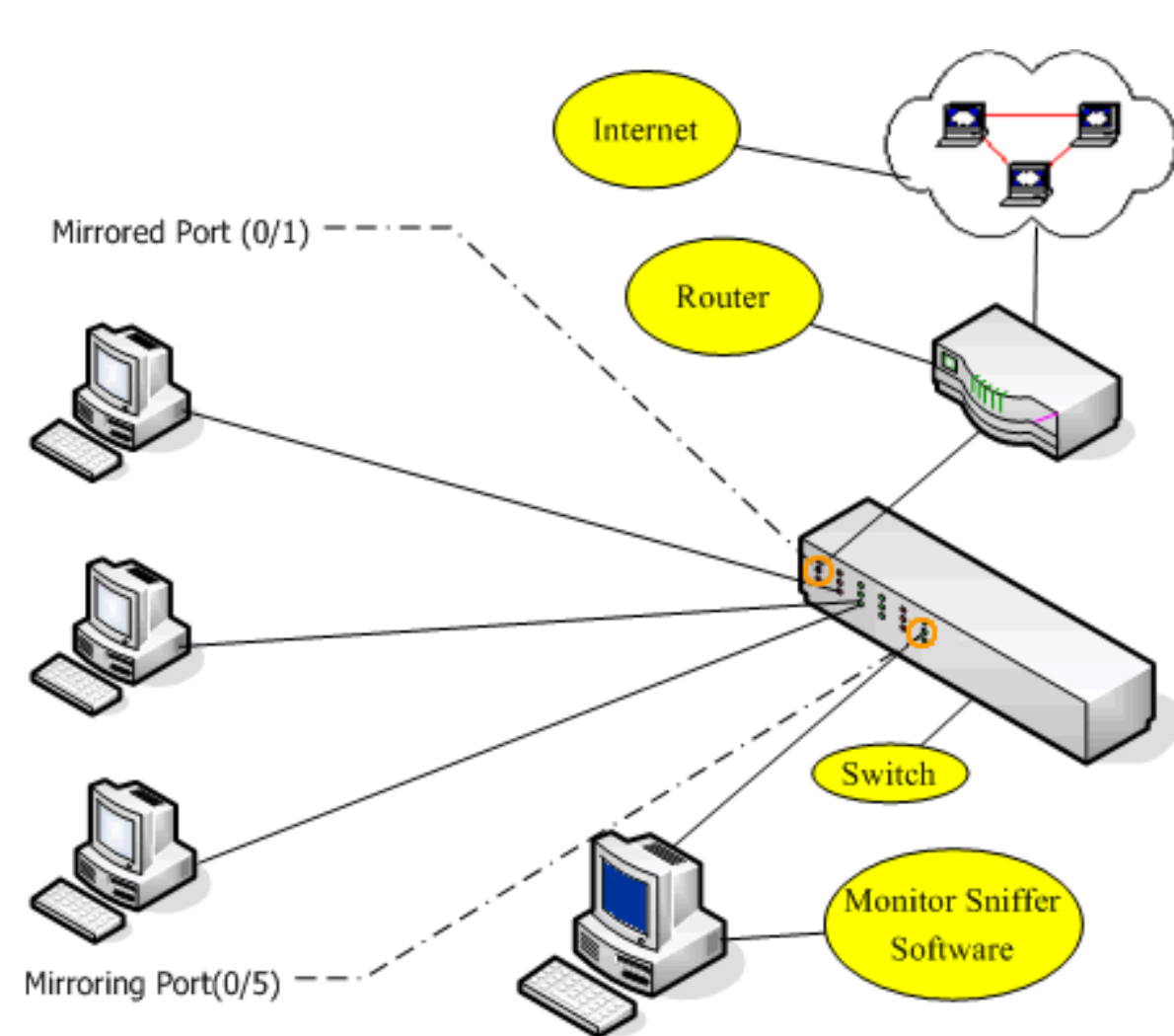
Prof. Dr. Eng. Fred Sauer
fsoliveira@unicarioca.edu.br

- ➡ Posicionamento adequado da estação
- ➡ Obtenção e Instalação do Wireshark
- ➡ Interface em modo promíscuo - Winpcap
- ➡ Escolha da(s) interface(s) a capturar
- ➡ Customização do aplicativo
- ➡ Uso dos filtros
 - ◆ Captura
 - ◆ Display
- ➡ Outras funcionalidades interessantes

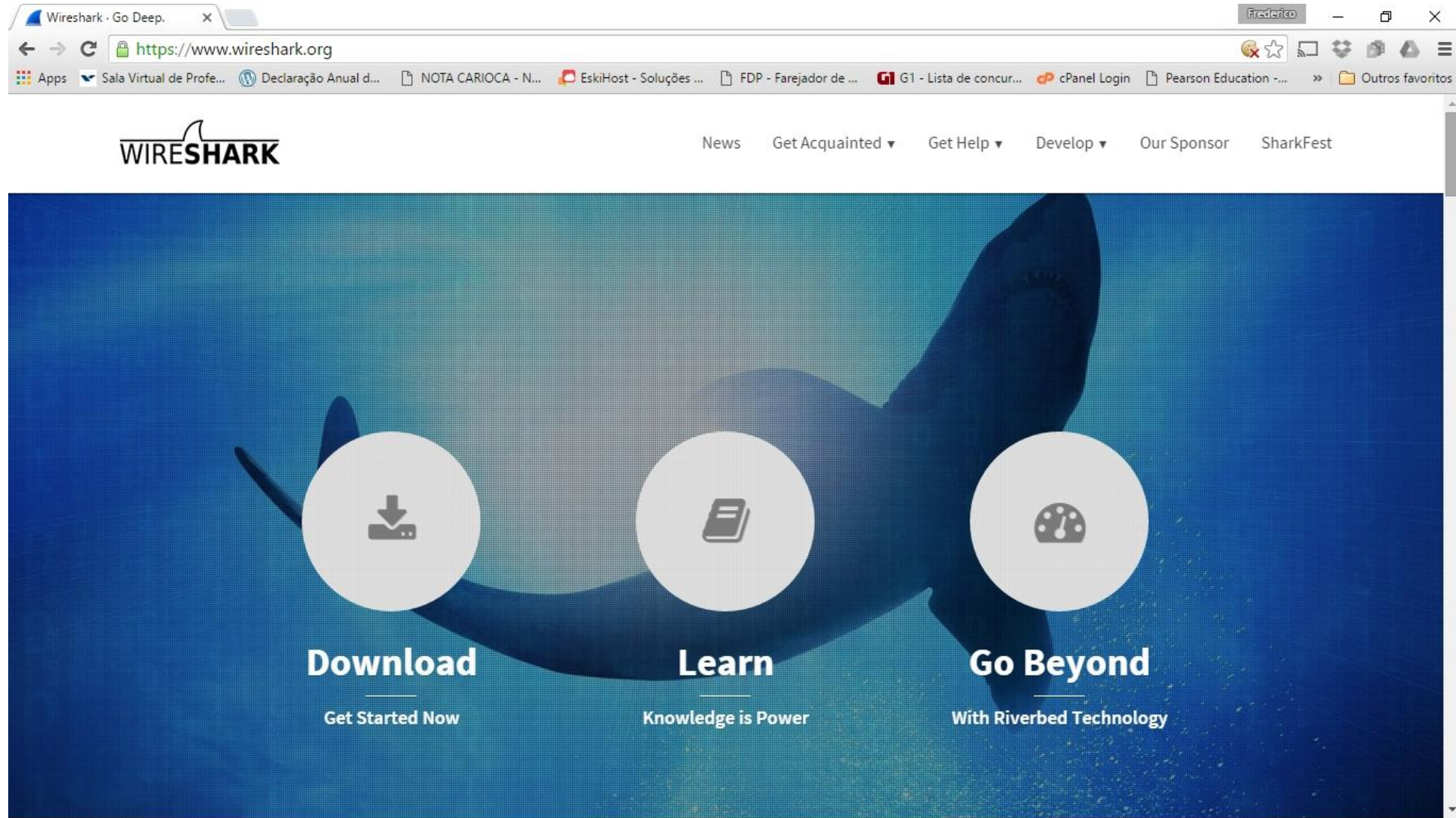
Posicionamento do Sniffer

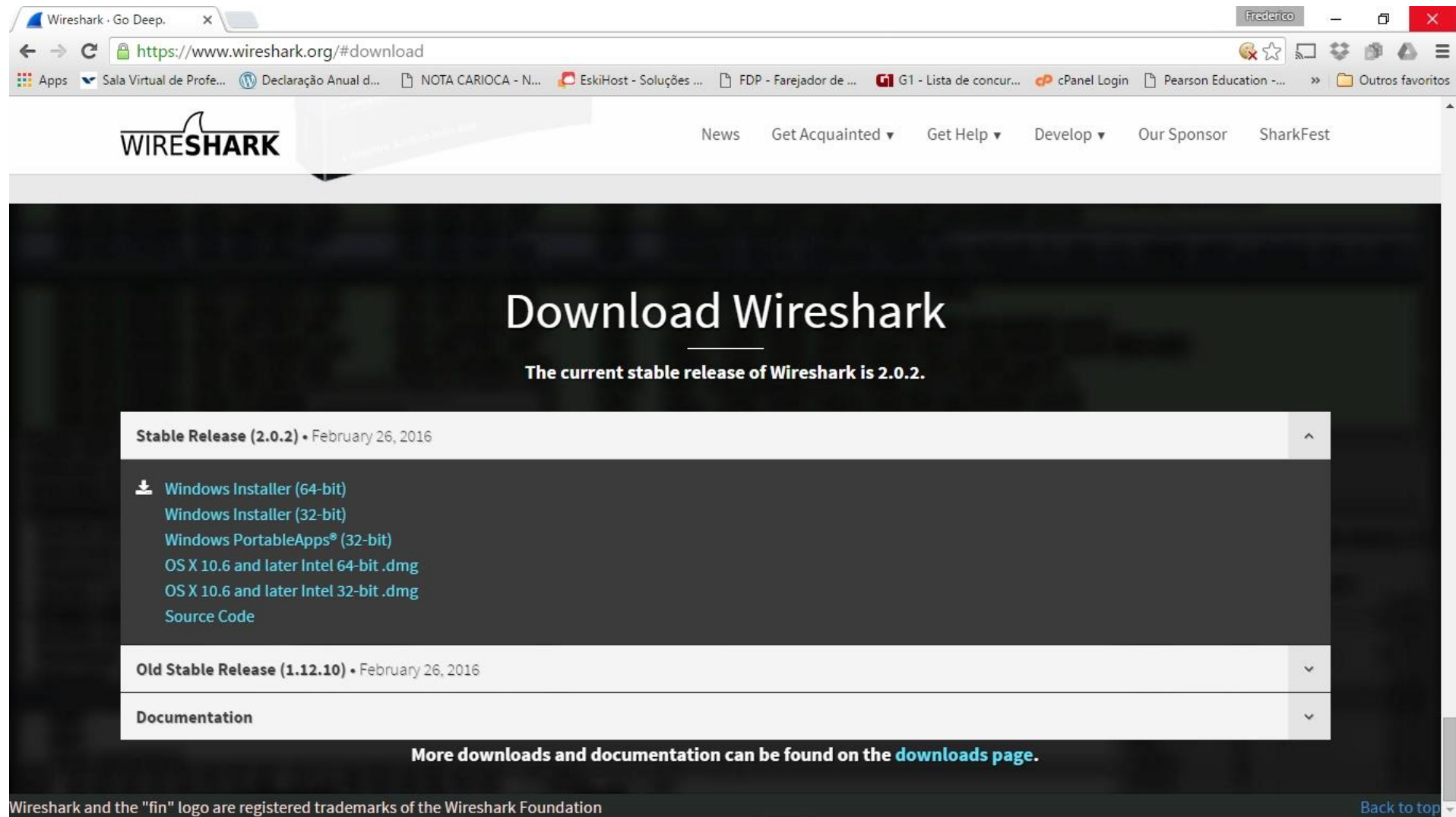


Posicionamento do Sniffer



Obtenção e Instalação





The screenshot shows a web browser window with the URL <https://www.wireshark.org/#download>. The page features the Wireshark logo and navigation links: News, Get Acquainted, Get Help, Develop, Our Sponsor, and SharkFest. The main heading is "Download Wireshark", followed by the text "The current stable release of Wireshark is 2.0.2." Below this, there are three expandable sections: "Stable Release (2.0.2) • February 26, 2016", "Old Stable Release (1.12.10) • February 26, 2016", and "Documentation". The "Stable Release" section is expanded, showing a list of download links: "Windows Installer (64-bit)", "Windows Installer (32-bit)", "Windows PortableApps® (32-bit)", "OS X 10.6 and later Intel 64-bit .dmg", "OS X 10.6 and later Intel 32-bit .dmg", and "Source Code". At the bottom, a footer states "Wireshark and the 'fin' logo are registered trademarks of the Wireshark Foundation" and a "Back to top" link is visible.

Wireshark · Go Deep.

<https://www.wireshark.org/#download>

Apps Sala Virtual de Profe... Declaração Anual d... NOTA CARIOCA - N... EskiHost - Soluções ... FDP - Farejador de ... G1 - Lista de concur... cPanel Login Pearson Education -... Outros favoritos

WIRESHARK

News Get Acquainted Get Help Develop Our Sponsor SharkFest

Download Wireshark

The current stable release of Wireshark is 2.0.2.

Stable Release (2.0.2) • February 26, 2016

- Windows Installer (64-bit)
- Windows Installer (32-bit)
- Windows PortableApps® (32-bit)
- OS X 10.6 and later Intel 64-bit .dmg
- OS X 10.6 and later Intel 32-bit .dmg
- Source Code

Old Stable Release (1.12.10) • February 26, 2016

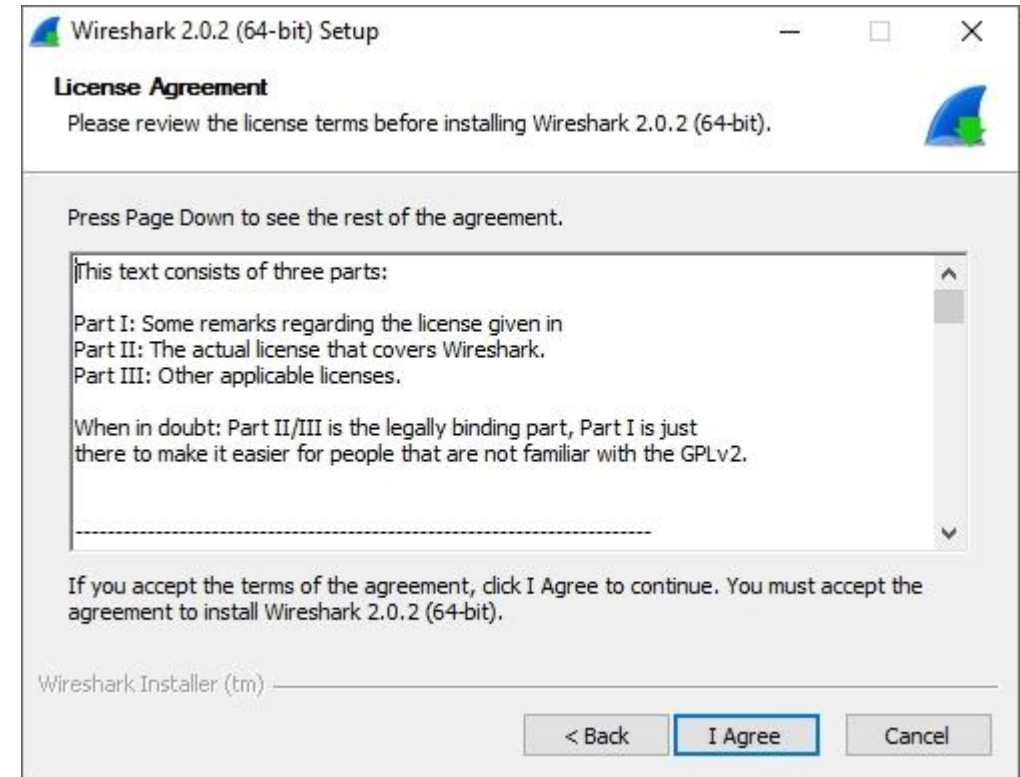
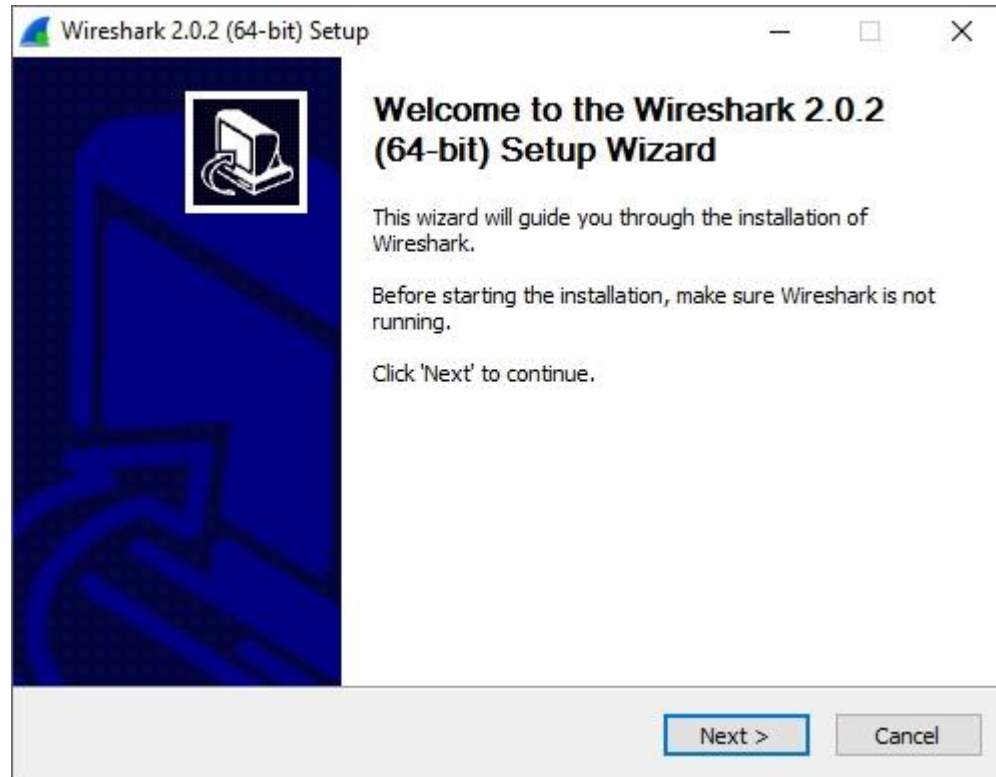
Documentation

More downloads and documentation can be found on the [downloads page](#).

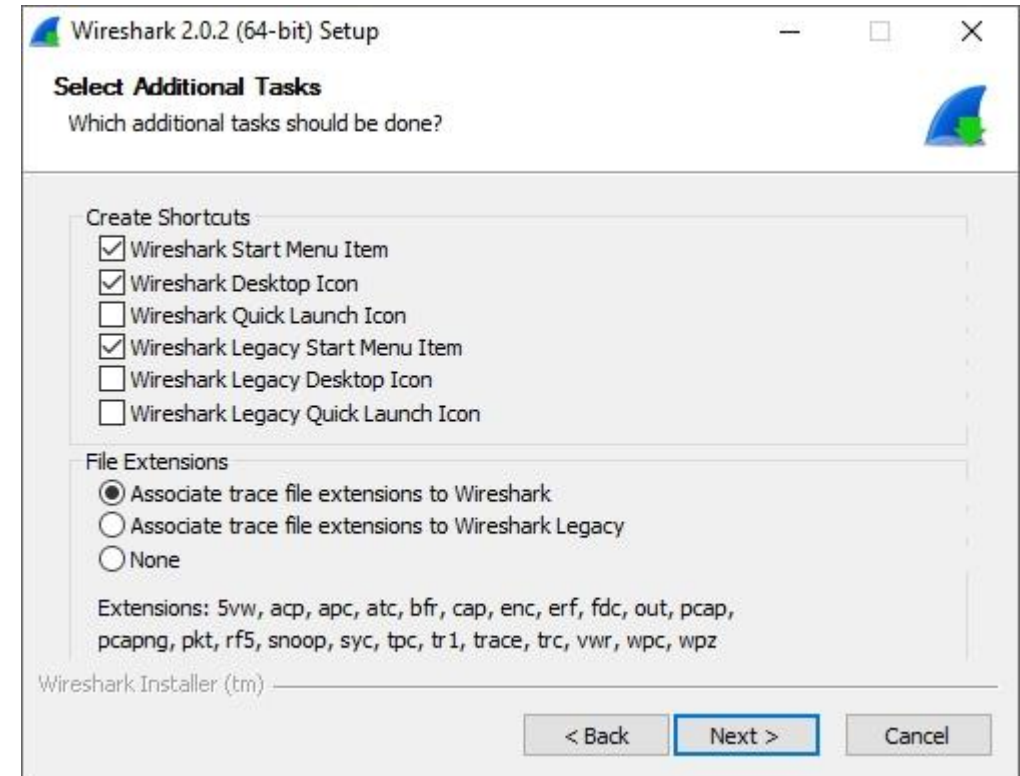
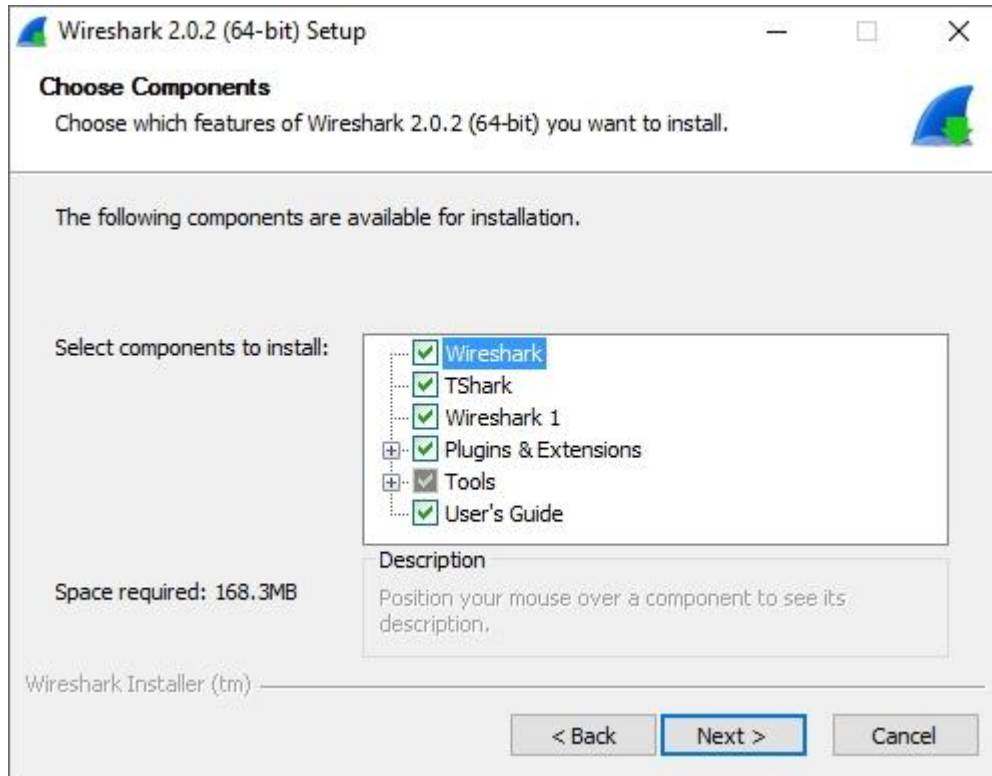
Wireshark and the "fin" logo are registered trademarks of the Wireshark Foundation

[Back to top](#)

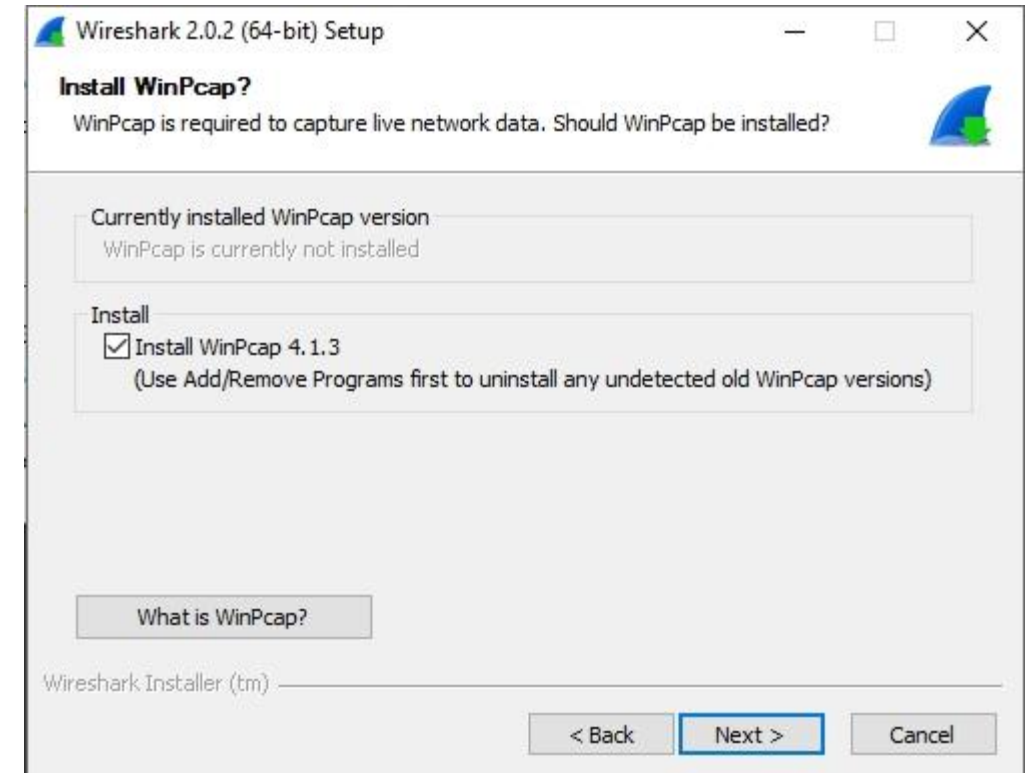
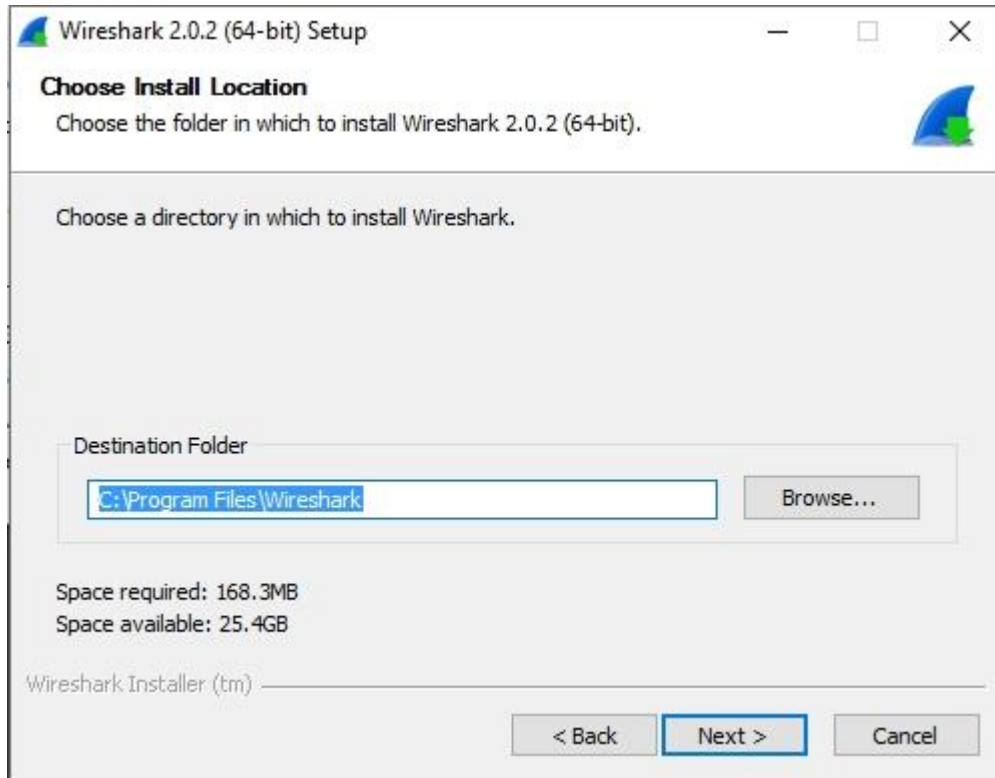
Instalação



Instalação



Instalação



Instalação

WinPcap - The Wireshark ...

https://wiki.wireshark.org/WinPcap

WIRESHARK WinPcap

FrontPage RecentChanges FindPage HelpContents WinPcap

Página Imutável Informações Anexos Mais Ações:

Windows Packet Capture (WinPcap)

WinPcap is the Windows version of the [libpcap](#) library; it includes a driver to support capturing packets. Wireshark uses this library to capture live network data on Windows.

See [CaptureSetup/CapturePrivileges](#) for information about using the WinPcap driver with Wireshark.

General information about the WinPcap project can be found at the [WinPcap](#) web site.

The libpcap/WinPcap file format description can be found at: [Development/LibpcapFileFormat](#)

WinPcap Versions

⚠ We strongly recommend that you use version 4.1.2 or 3.1. Some annoying bugs are fixed in these versions!

See the "Add or Remove Programs" list of the "Control Panel" for the installed version.

Latest Stable Release: 4.1.2

The current WinPcap release version is 4.1.2. The 4.1.x versions contain the following improvements:

- Support for Windows XP, Vista, 2008, Win7 and 2008R2 64 bit
- Allows remote capture to work with Wireshark
- Based on libpcap 1.0

WinPcap 4.x does not support Windows 3.1, 95, 98, or ME.

Previous Stable Release: 3.1

This version contains substantial bug fixes and extensions above the 3.0 release:

- based on libpcap 0.9.3, with many fixes and extensions above the older version

Wireshark 2.0.2 (64-bit) Setup

Install USBPcap?

USBPcap is required to capture USB traffic. Should USBPcap be installed?

Currently installed USBPcap version
USBPcap is currently not installed

Install

☒ Install USBPcap 1.1.0.0-g794bf26
(Use Add/Remove Programs first to uninstall any undetected old USBPcap versions)

What is USBPcap?

Wireshark Installer (tm)

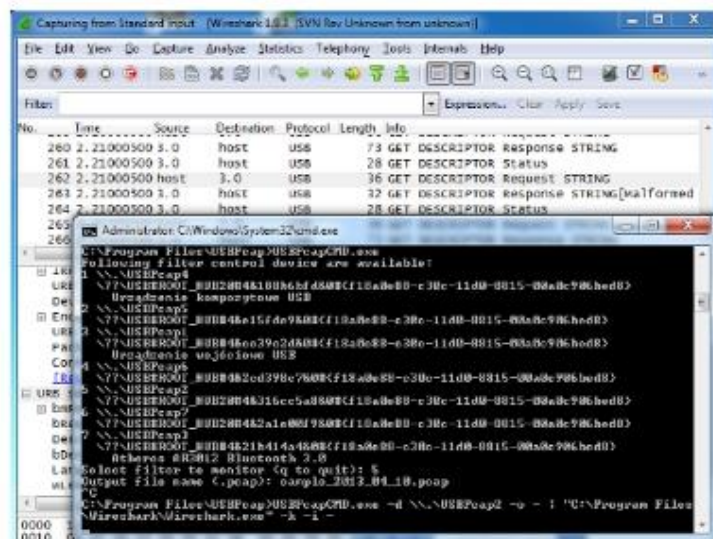
< Back Install Cancel

Open Source USB Packet capture for Windows

... works on XP, Vista, 7 and 8

USBPCap - USB Packet capture for Windows

USBPCap is an open-source USB sniffer for Windows.



Download

Digitally signed installer for Windows XP, Vista, 7 and 8, both x86 and x64 is available at Bintray. After installation you must restart your computer.

USBPCapSetup-1.0.0.7.exe

Wireshark

USBPCap support was committed in revision 48847 (**Wireshark #8503**). The first official Wireshark version that supports USBPCap is **1.10.0rc1**.

USBPCap

- Main page
- Illustrated Tour
- Capture format
- Capture limitations
- Donors

Develop

- Develop
- Block diagram
- Capture buffer
- Wireshark dissectors
- USBPCap TODO

Links

- GitHub project page
- Report issue
- Changelog
- Wiki

Follow @USBPCap
Open Hub usbpcap

Google Groups

Subscribe to USBPCap

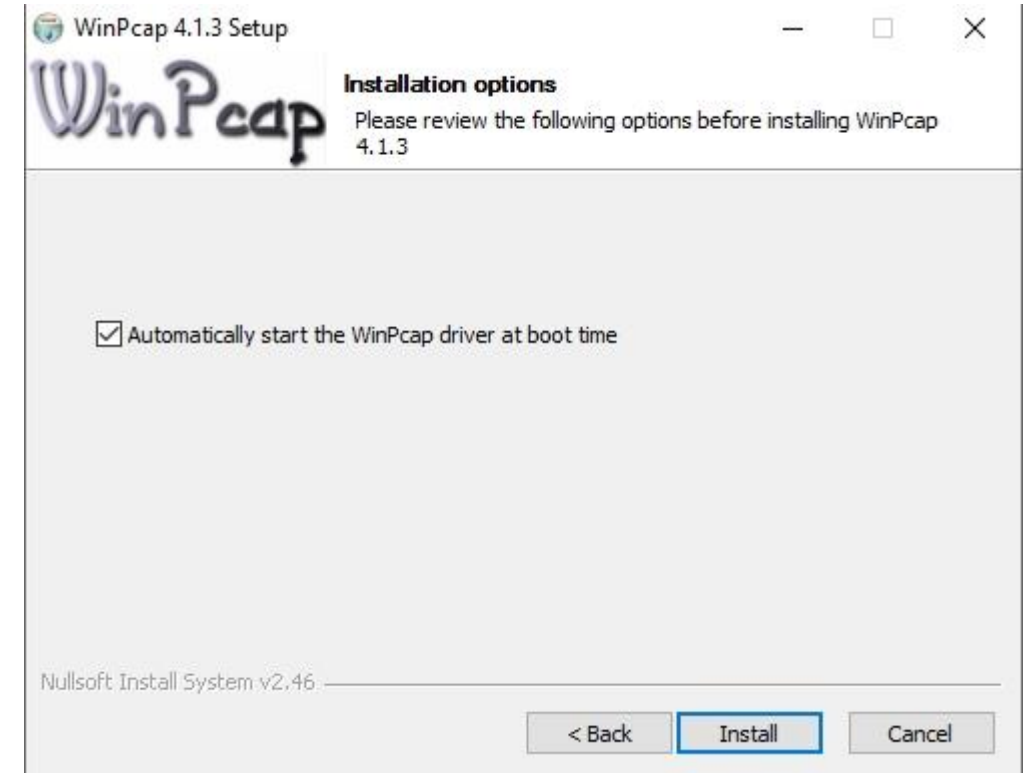
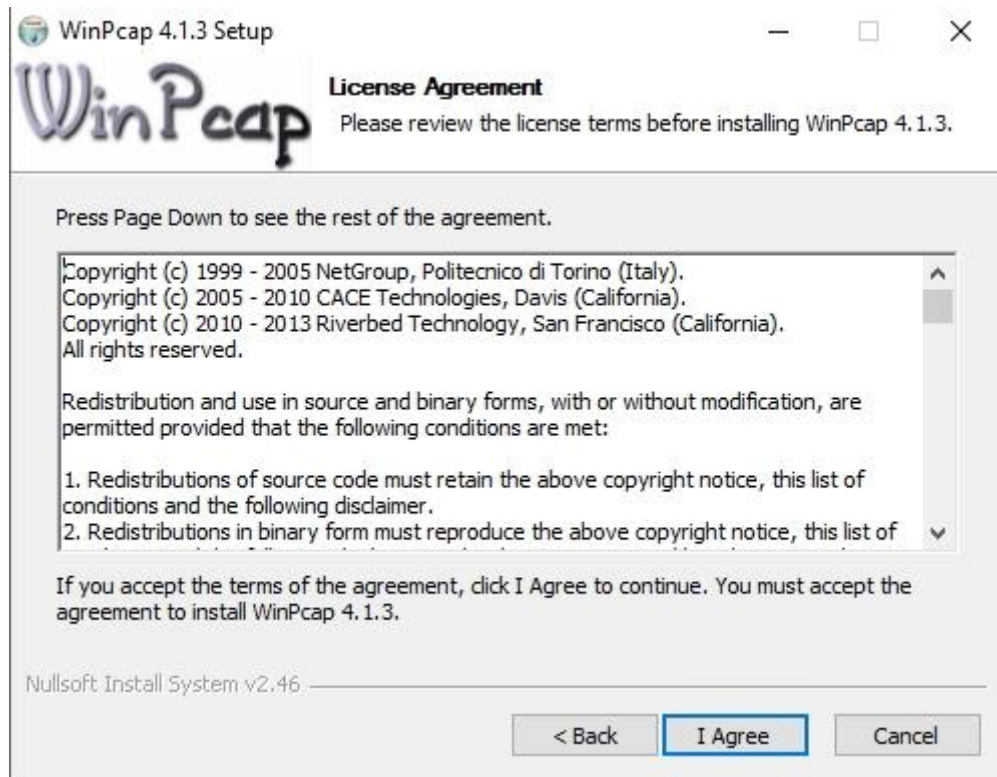
Email:

Subscribe

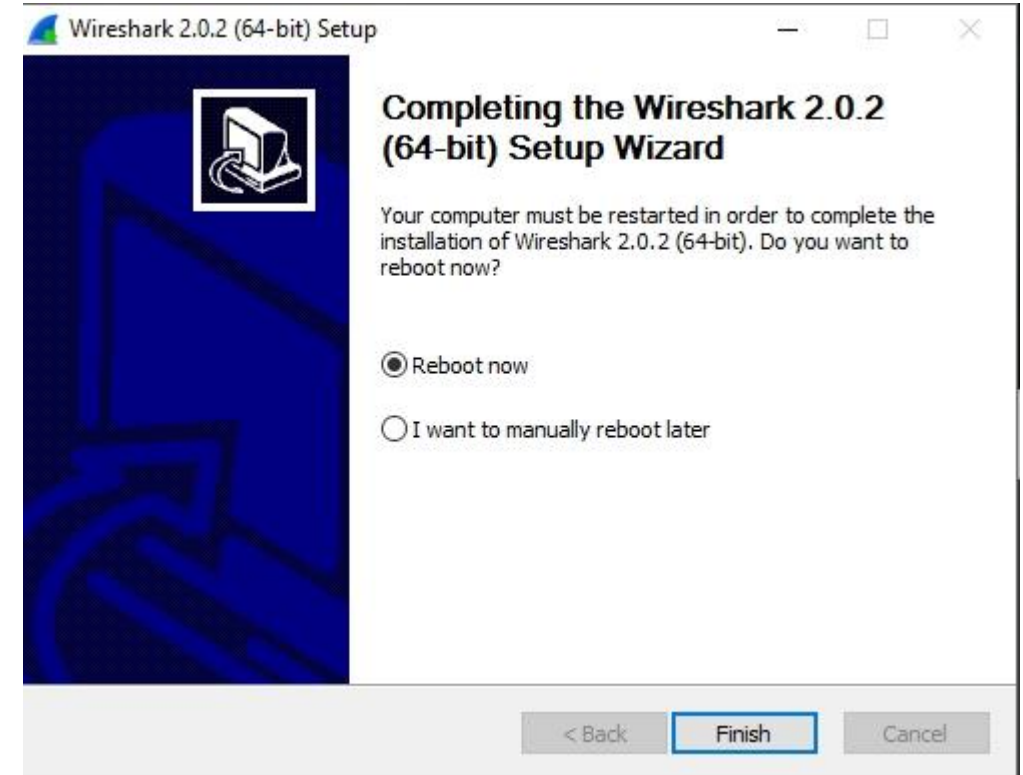
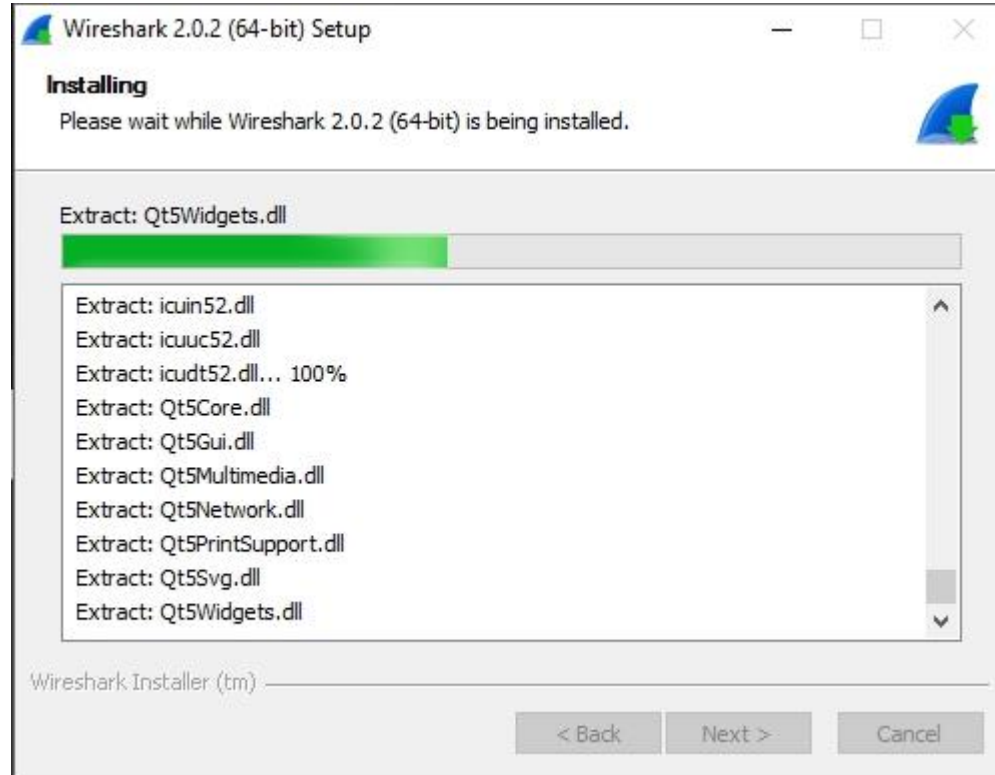
Visit this group

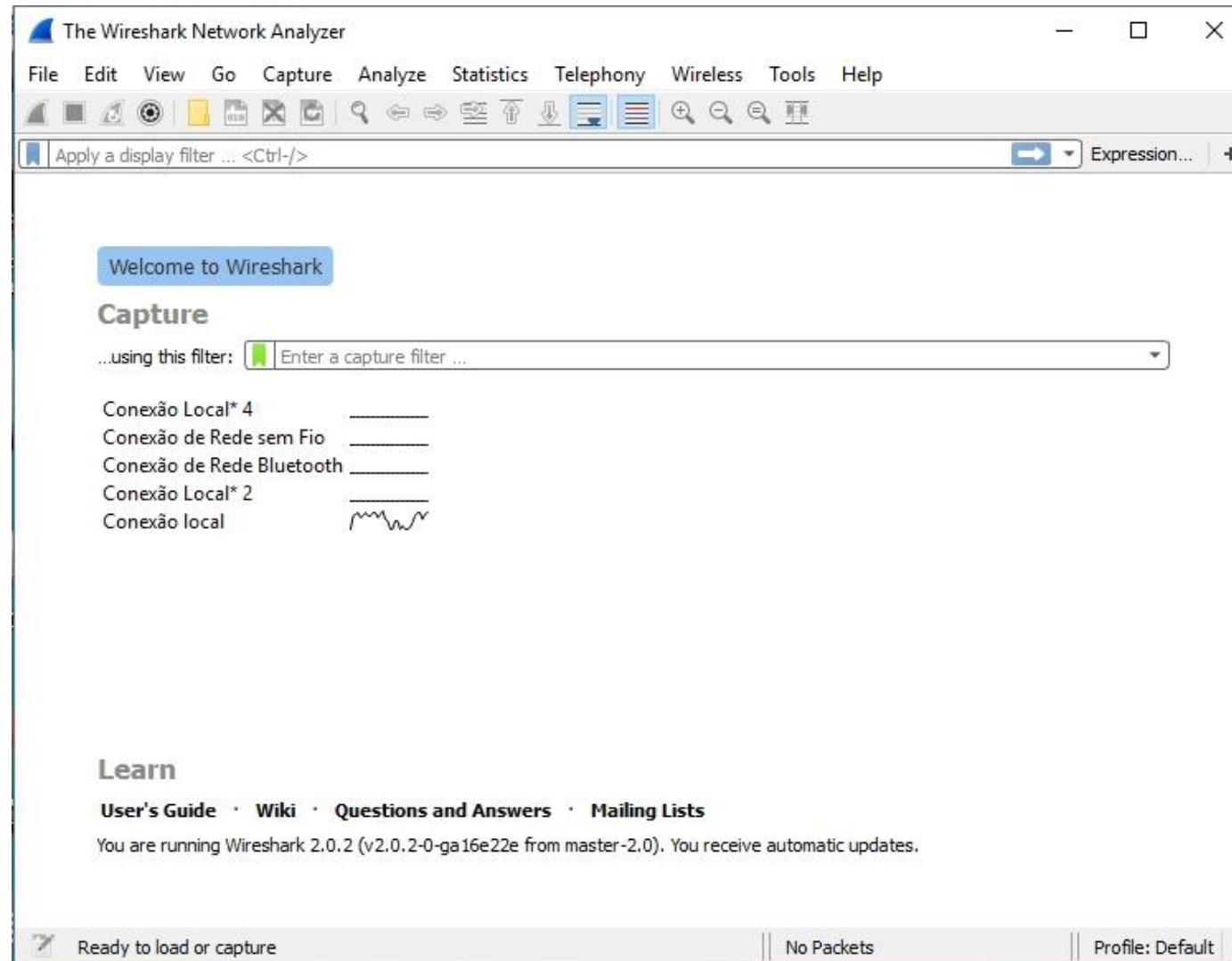


Instalação



Instalação





Customização

Capturing from Conexão local

File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help

Apply a display filter ... <Ctrl-/> Expression...

No.	Time	Source	Destination	Protocol	Length	Info
5586	19.732283	63.245.197.57	192.168.1.116	TCP	60	443 → 49823 [ACK] Seq=1 A
5587	19.732935	192.168.1.116	63.245.197.57	TCP	1454	[TCP segment of a reassem
5588	19.739573	63.245.197.57	192.168.1.116	TCP	60	443 → 49823 [ACK] Seq=1 A
5589	19.740196	192.168.1.116	63.245.197.57	TCP	1454	[TCP segment of a reassem
5590	19.741165	192.168.1.116	63.245.197.57	TCP	1454	[TCP segment of a reassem
5591	19.751454	63.245.197.57	192.168.1.116	TCP	60	443 → 49823 [ACK] Seq=1 A
5592	19.752002	192.168.1.116	63.245.197.57	TCP	1454	[TCP segment of a reassem
5593	19.752940	192.168.1.116	63.245.197.57	TCP	1454	[TCP segment of a reassem
5594	19.761847	63.245.197.57	192.168.1.116	TCP	60	443 → 49823 [ACK] Seq=1 A
5595	19.762404	192.168.1.116	63.245.197.57	TCP	1454	[TCP segment of a reassem
5596	19.763281	192.168.1.116	63.245.197.57	TCP	1454	[TCP segment of a reassem

> Frame 1: 60 bytes on wire (480 bits), 60 bytes captured (480 bits) on interface 0
 > Ethernet II, Src: CiscoInc_a2:47:48 (50:3d:e5:a2:47:48), Dst: HewlettP_fb:66:f2 (b4:b5:2f:fb:66:f2)
 > Internet Protocol Version 4, Src: 63.245.197.57, Dst: 192.168.1.116
 > Transmission Control Protocol, Src Port: 443 (443), Dst Port: 49823 (49823), Seq: 1, Ack: 1, Len: 0

0000 b4 b5 2f fb 66 f2 50 3d e5 a2 47 48 08 00 45 00 ../.f.P= ..GH..E.
 0010 00 28 80 7e 00 00 f3 06 80 06 3f f5 c5 39 c0 a8 ..(~.... ..?...9..
 0020 01 74 01 bb c2 9f 49 dc 5c 13 98 10 92 89 50 10 .t....I. \.....P.
 0030 01 37 52 6e 00 00 00 00 20 20 20 20 .7Rn....

Conexão local: <live capture in progress> | Packets: 5596 · Displayed: 5596 (100.0%) | Profile: Default

*Conexão local

File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help

Copy
 Find Packet... Ctrl+F
 Find Next Ctrl+N
 Find Previous Ctrl+B
 Mark/Unmark Packet Ctrl+M
 Mark All Displayed Ctrl+Shift+M
 Unmark All Displayed Ctrl+Alt+M
 Next Mark Ctrl+Shift+N
 Previous Mark Ctrl+Shift+B
 Ignore/Unignore Packet Ctrl+D
 Ignore All Displayed Ctrl+Shift+D
 Unignore All Displayed Ctrl+Alt+D
 Set/Unset Time Reference Ctrl+T
 Unset All Time References Ctrl+Alt+T
 Next Time Reference Ctrl+Alt+N
 Previous Time Reference Ctrl+Alt+B
 Time Shift... Ctrl+Shift+T
 Packet Comment...
 Configuration Profiles... Ctrl+Shift+A
 Preferences... Ctrl+Shift+P

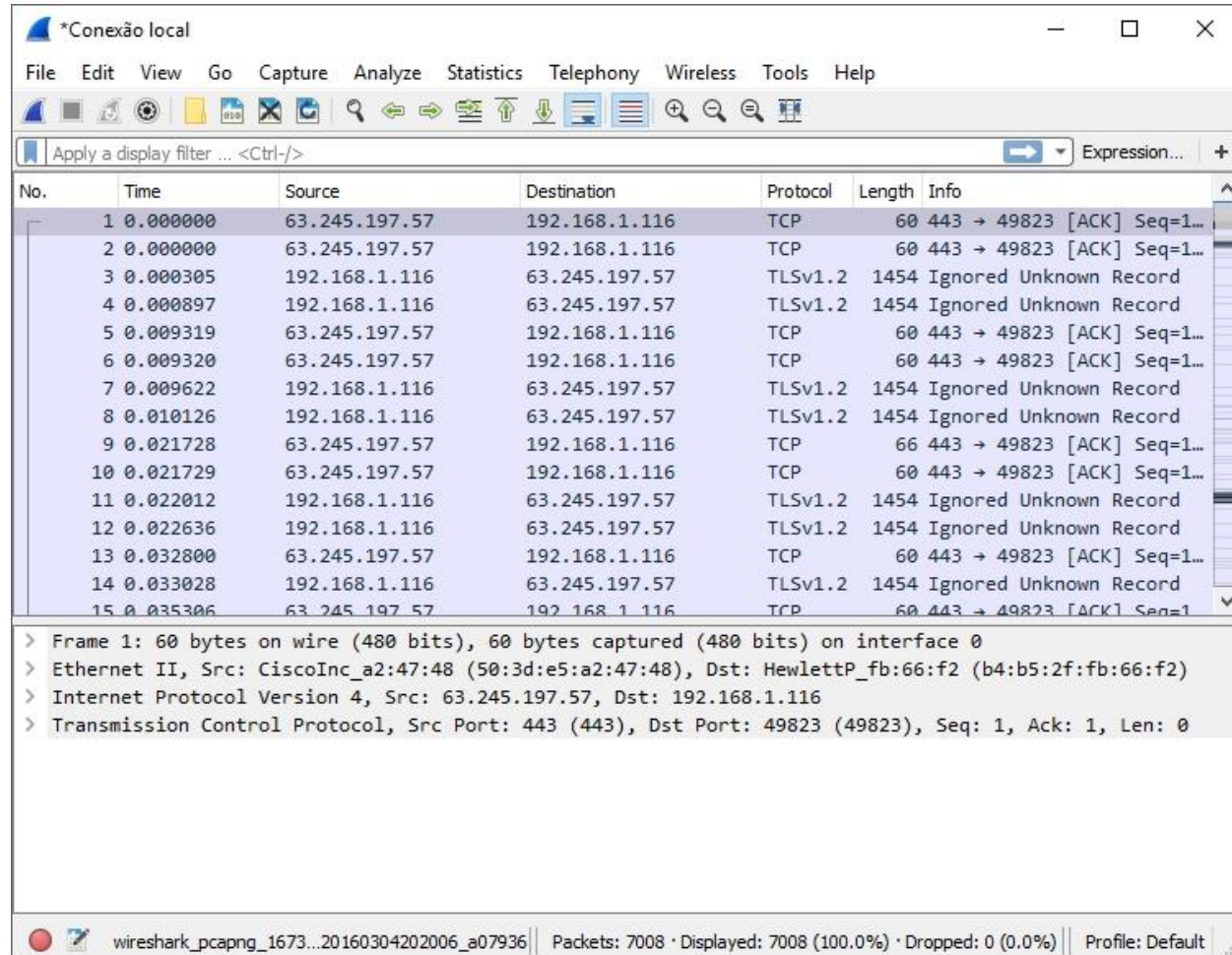
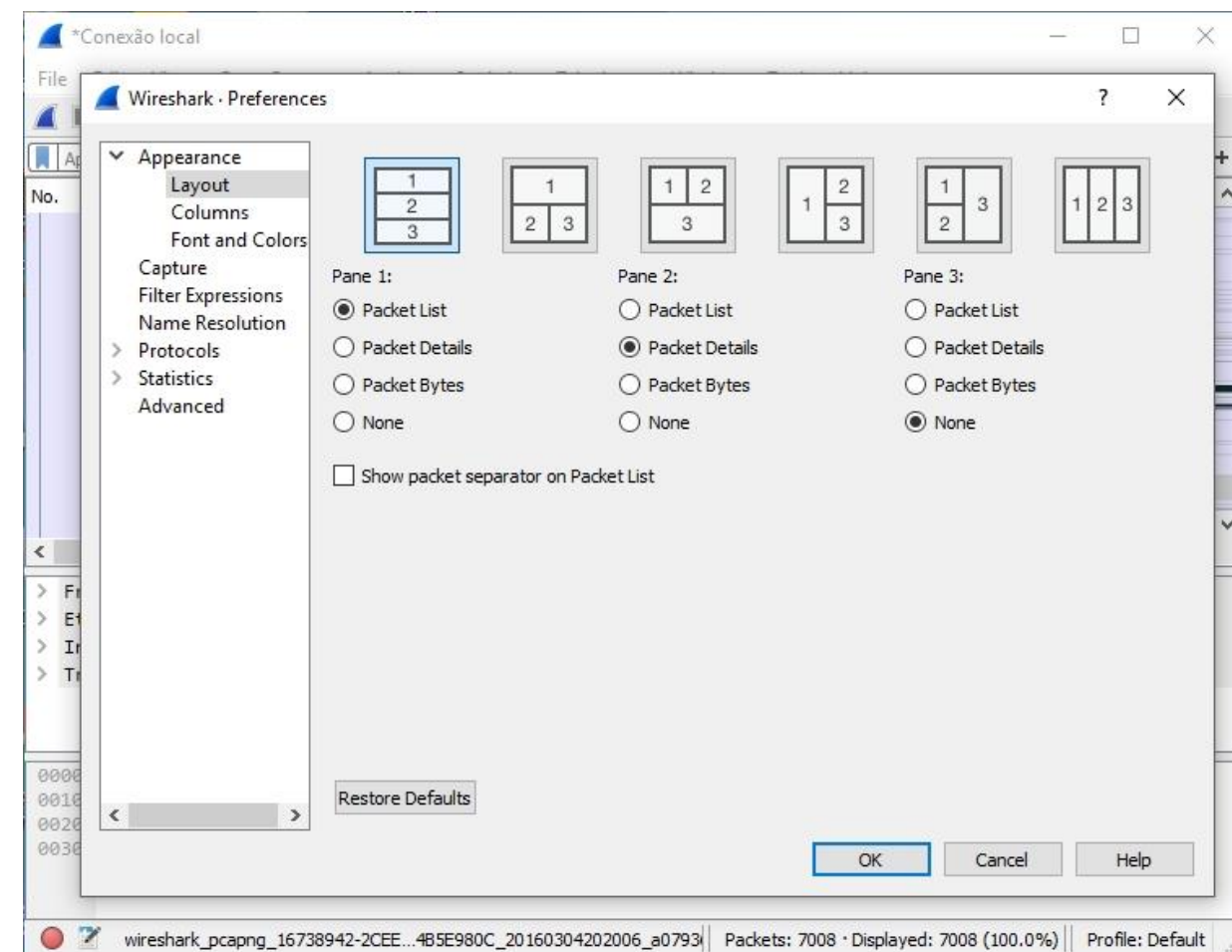
No.	Time	Source	Destination	Protocol	Length	Info
5586	19.732283	63.245.197.57	192.168.1.116	TCP	60	443 → 49823 [ACK] Seq=1 A
5587	19.732935	192.168.1.116	63.245.197.57	TCP	1454	[TCP segment of a reassem
5588	19.739573	63.245.197.57	192.168.1.116	TCP	60	443 → 49823 [ACK] Seq=1 A
5589	19.740196	192.168.1.116	63.245.197.57	TCP	1454	[TCP segment of a reassem
5590	19.741165	192.168.1.116	63.245.197.57	TCP	1454	[TCP segment of a reassem
5591	19.751454	63.245.197.57	192.168.1.116	TCP	60	443 → 49823 [ACK] Seq=1 A
5592	19.752002	192.168.1.116	63.245.197.57	TCP	1454	[TCP segment of a reassem
5593	19.752940	192.168.1.116	63.245.197.57	TCP	1454	[TCP segment of a reassem
5594	19.761847	63.245.197.57	192.168.1.116	TCP	60	443 → 49823 [ACK] Seq=1 A
5595	19.762404	192.168.1.116	63.245.197.57	TCP	1454	[TCP segment of a reassem
5596	19.763281	192.168.1.116	63.245.197.57	TCP	1454	[TCP segment of a reassem

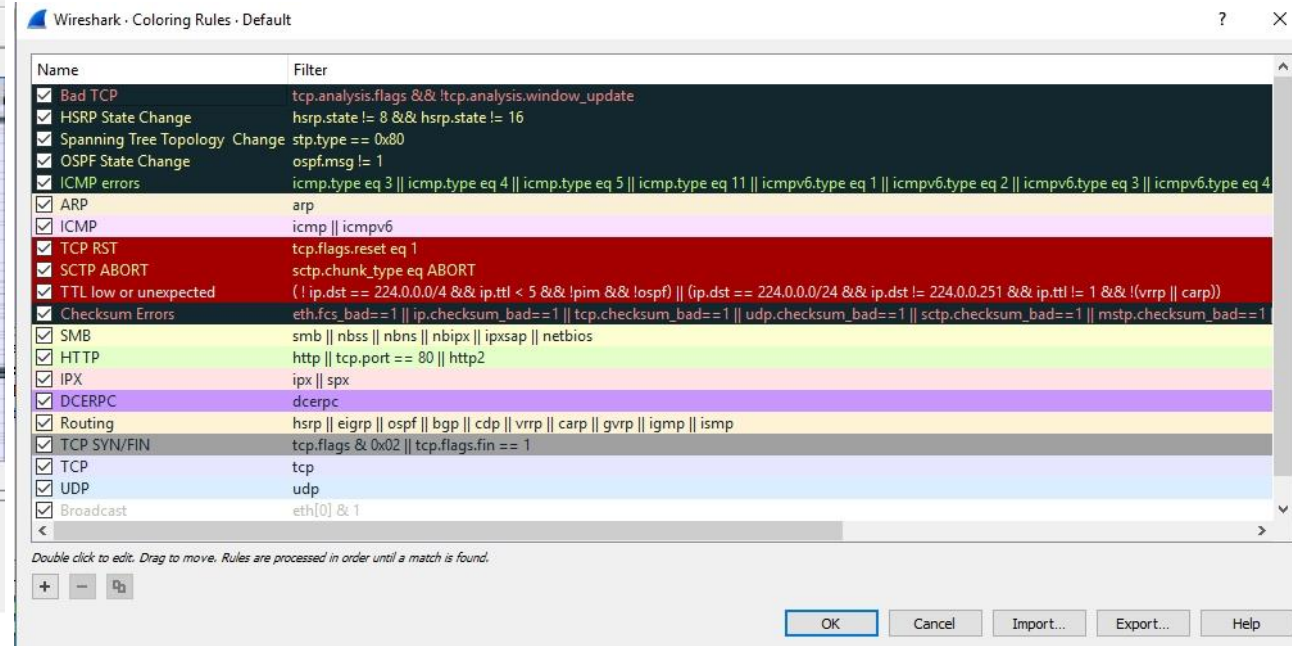
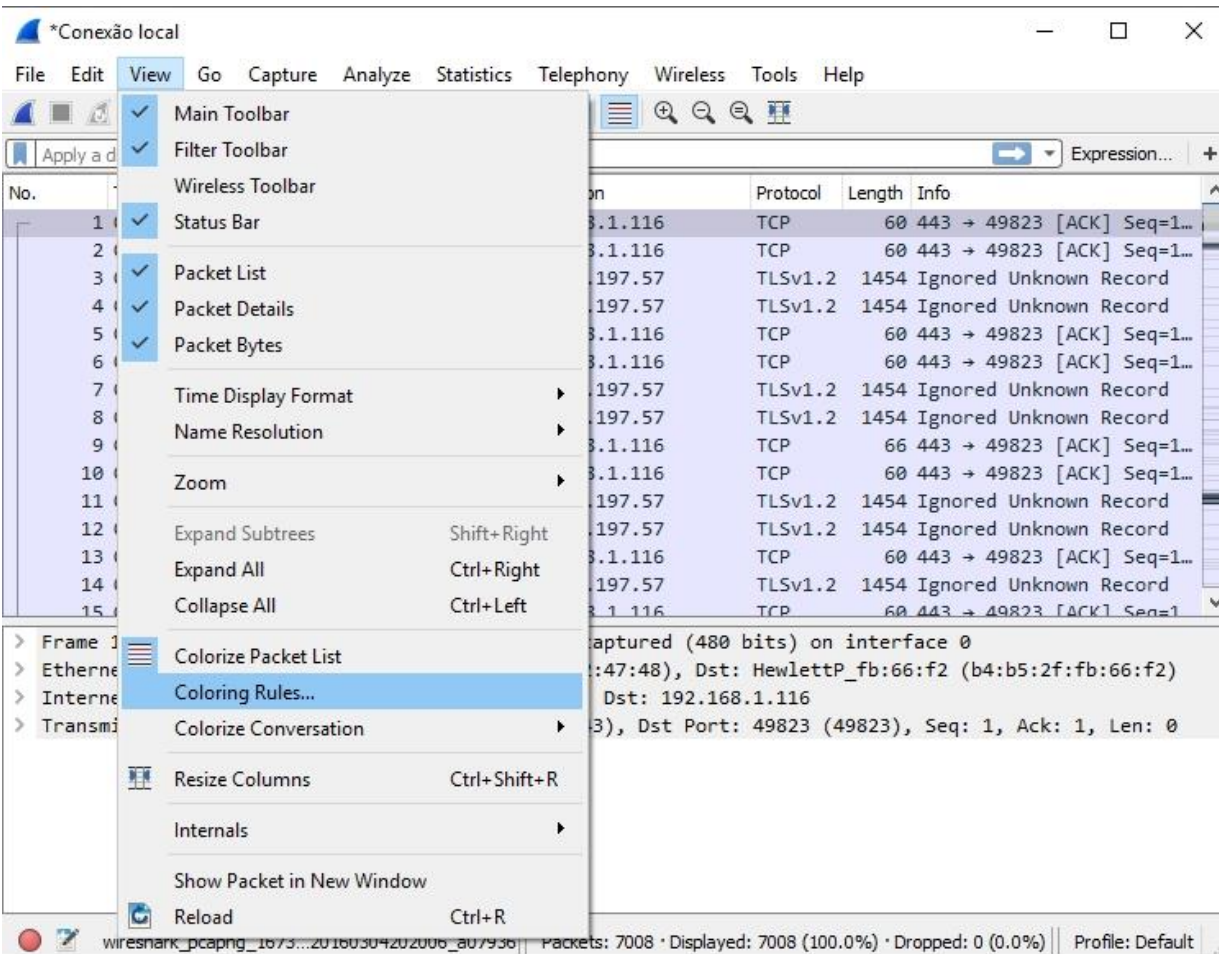
> Frame 1: 60 bytes on wire (480 bits), 60 bytes captured (480 bits) on interface 0
 > Ethernet II, Src: CiscoInc_a2:47:48 (50:3d:e5:a2:47:48), Dst: HewlettP_fb:66:f2 (b4:b5:2f:fb:66:f2)
 > Internet Protocol Version 4, Src: 63.245.197.57, Dst: 192.168.1.116
 > Transmission Control Protocol, Src Port: 443 (443), Dst Port: 49823 (49823), Seq: 1, Ack: 1, Len: 0

0000 b4 b5 2f fb 66 f2 50 3d e5 a2 47 48 08 00 45 00 ../.f.P= ..GH..E.
 0010 00 28 80 7e 00 00 f3 06 80 06 3f f5 c5 39 c0 a8 ..(~.... ..?...9..
 0020 01 74 01 bb c2 9f 49 dc 5c 13 98 10 92 89 50 10 .t....I. \.....P.
 0030 01 37 52 6e 00 00 00 00 20 20 20 20 .7Rn....

wireshark_pcapng_16738942-2CEE...4B5E980C_20160304202006_a0793 | Packets: 7008 · Displayed: 7008 (100.0%) | Profile: Default

Customização





*Conexão local

File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help

Apply a display filter ... <Ctrl-/> Expression...

No.	Time	Source	Destination	Protocol	Length	Info
1	0.000000	63.245.197.57	192.168.1.116	TCP	60	443 → 49823 [ACK] Seq=1...
2	0.000000	63.245.197.57	192.168.1.116	TCP	60	443 → 49823 [ACK] Seq=1...
3	0.000305	192.168.1.116	63.245.197.57	TLSv1.2	1454	Ignored Unknown Record

> Frame 1: 60 bytes on wire (480 bits), 60 bytes captured (480 bits) on interface 0
 > Ethernet II, Src: CiscoInc_a2:47:48 (50:3d:e5:a2:47:48), Dst: HewlettP_fb:66:f2 (b4:b5:2f:fb:66:f2)
 > Internet Protocol Version 4, Src: 63.245.197.57, Dst: 192.168.1.116
 ✓ Transmission Control Protocol, Src Port: 443 (443), Dst Port: 49823 (49823), Seq: 1, Ack: 1, Len: 0
 Source Port: 443
 Destination Port: 49823
 [Stream index: 0]
 [TCP Segment Len: 0]
 Sequence number: 1 (relative sequence number)
 Acknowledgment number: 1 (relative ack number)
 Header Length: 20 bytes
 Flags: 0x010 (ACK)
 000. = Reserved: Not set
 ...0 = Nonce: Not set
 ...0... = Congestion Window Reduced (CWR): Not set
 ...0.. = ECN-Echo: Not set
 0. = Urgent: Not set
 1. = Acknowledgment: Set
 0... = Push: Not set
 0.. = Reset: Not set
 0. = Syn: Not set
 0 = Fin: Not set
 [TCP Flags: *****A****]
 Window size value: 311
 [Calculated window size: 311]
 [Window size scaling factor: -1 (unknown)]
 Checksum: 0x526e [validation disabled]

wireshark_pcapng_1673...20160304202006_a07936 | Packets: 7008 · Displayed: 7008 (100.0%) · Dropped: 0 (0.0%) | Profile: Default

Filtros: Display

*Conexão local

File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help

Wireshark · Display Filter Expression

Field Name Relation Value (IPv4 address)

ip.opt.sid · Stream Identifier is present

ip.opt.time_stamp · Time stamp ==

ip.opt.time_stamp_addr · Addr... !=

ip.opt.type · Type >

ip.opt.type.class · Class <

ip.opt.type.copy · Copy on fra... >=

ip.opt.type.number · Number <=

ip.proto · Protocol

ip.reassembled.data · Reassem...

ip.reassembled.length · Reasse...

ip.reassembled.in · Reassembl...

ip.rec_rt · Recorded Route

ip.rec_rt_host · Recorded Rout...

ip.src · Source

ip.src_host · Source Host

ip.src_rt · Source Route

ip.src_rt_host · Source Route H...

ip.subopt_too_long · Expert Info

ip.tos · Type of Service

ip.tos.cost · Cost

ip.tos.delay · Delay

ip.tos.precedence · Precedence

ip.tos.reliability · Reliability

ip.tos.throughput · Throughput

ip.ttl · Time to live

ip.ttl.incb · Expert Info

ip.ttl.too_small · Expert Info

ip.version · Version

IPv6 · Internet Protocol Version 6

Search:

ip.src == 192.168.1.116

Click OK to insert this filter

OK Cancel Help

*Conexão local

File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help

ip.src == 192.168.1.116

No.	Time	Source	Destination	Protocol	Length	Info
1	0.000000	192.168.1.116	63.245.197.57	TCP	1454	[TCP segment of a reass...
5	0.009525	192.168.1.116	63.245.197.57	TCP	1454	[TCP segment of a reass...
6	0.010147	192.168.1.116	63.245.197.57	TCP	1454	[TCP segment of a reass...
7	0.010767	192.168.1.116	63.245.197.57	TCP	1454	[TCP segment of a reass...
10	0.019136	192.168.1.116	63.245.197.57	SSLv2	1454	Encrypted Data
11	0.019747	192.168.1.116	63.245.197.57	TCP	1454	[TCP segment of a reass...
13	0.030551	192.168.1.116	63.245.197.57	TCP	1454	[TCP segment of a reass...
15	0.030968	192.168.1.116	63.245.197.57	TCP	1003	[TCP segment of a reass...
16	0.031569	192.168.1.116	63.245.197.57	TCP	1454	[TCP segment of a reass...
18	0.048949	192.168.1.116	63.245.197.57	TCP	1454	[TCP segment of a reass...
20	0.058557	192.168.1.116	63.245.197.57	TCP	1454	[TCP segment of a reass...
22	0.066122	192.168.1.116	63.245.197.57	TCP	1454	[TCP segment of a reass...
24	0.079396	192.168.1.116	63.245.197.57	TCP	1454	[TCP segment of a reass...

> Frame 1: 1454 bytes on wire (11632 bits), 1454 bytes captured (11632 bits) on interface 0

> Ethernet II, Src: HewlettP_fb:66:f2 (b4:b5:2f:fb:66:f2), Dst: CiscoInc_a2:47:48 (50:3d:e5:a2:47:48)

> Internet Protocol Version 4, Src: 192.168.1.116, Dst: 63.245.197.57

> Transmission Control Protocol, Src Port: 49823 (49823), Dst Port: 443 (443), Seq: 1, Ack: 1, Len: 1400

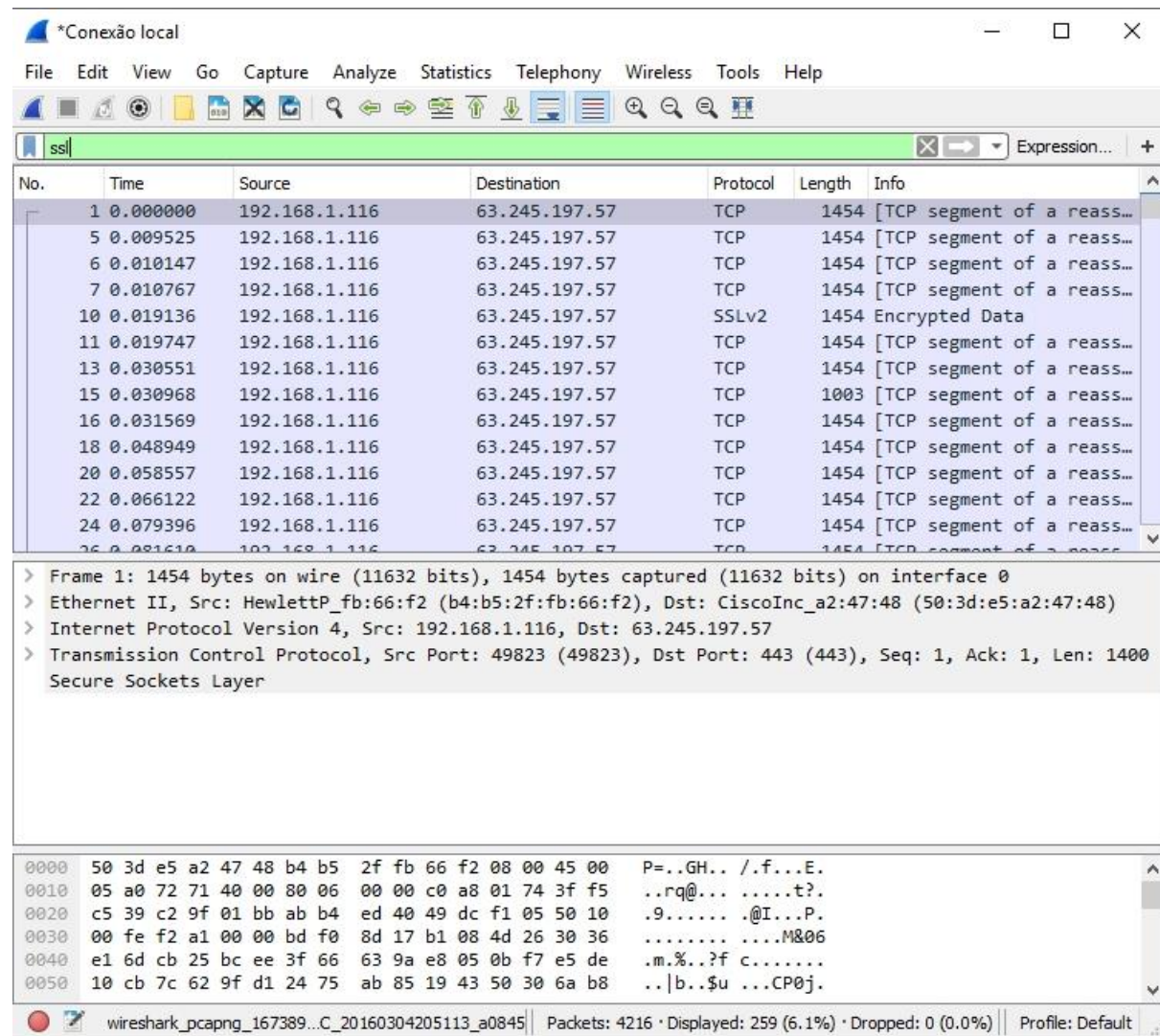
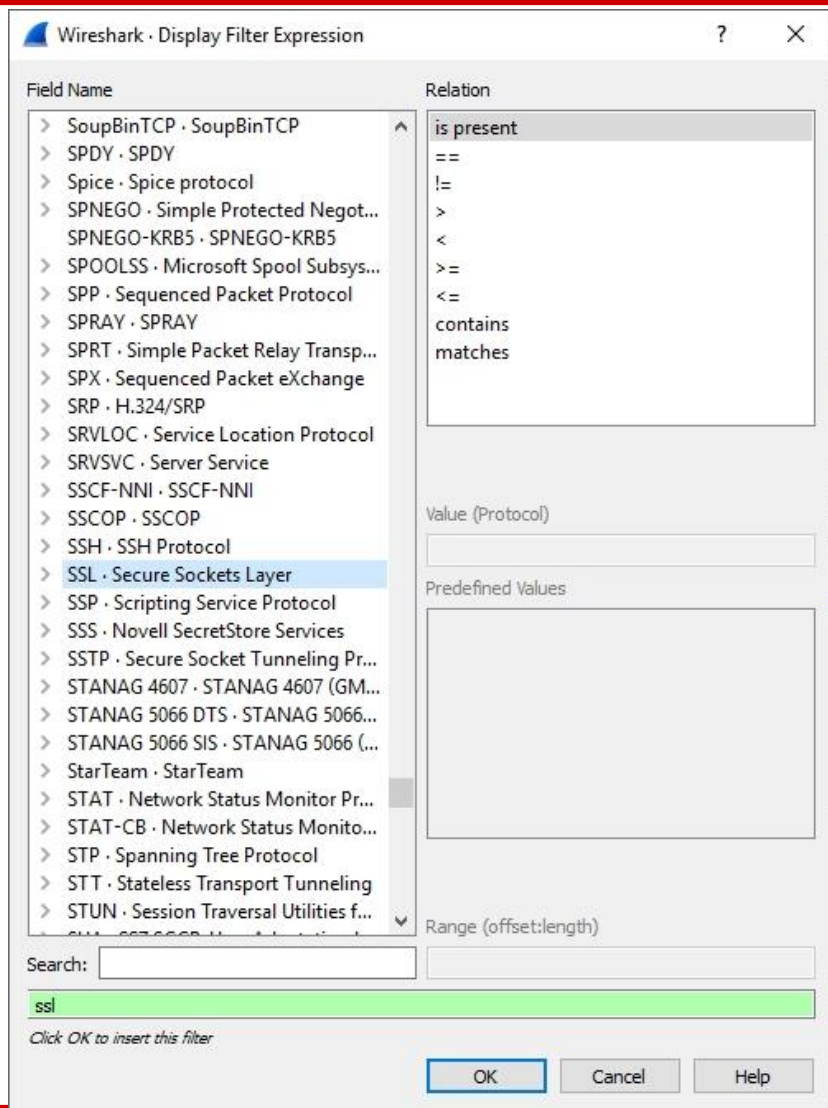
Secure Sockets Layer

```

0000  50 3d e5 a2 47 48 b4 b5 2f fb 66 f2 08 00 45 00  P=..GH.. /.f...E.
0010  05 a0 72 71 40 00 80 06 00 00 c0 a8 01 74 3f f5  ..rq@... ..t?.
0020  c5 39 c2 9f 01 bb ab b4 ed 40 49 dc f1 05 50 10  .9..... .@I...P.
0030  00 fe f2 a1 00 00 bd f0 8d 17 b1 08 4d 26 30 36  ....M&06
0040  e1 6d cb 25 bc ee 3f 66 63 9a e8 05 0b f7 e5 de  .m.%..?f c.....
0050  10 cb 7c 62 9f d1 24 75 ab 85 19 43 50 30 6a b8  ..|b..$u ...CP0j.
    
```

wireshark_pcapng_16738..._20160304205113_a0845 | Packets: 4216 · Displayed: 2200 (52.2%) · Dropped: 0 (0.0%) | Profile: Default

Filtros: Display





CaptureFilters

An overview of the capture filter syntax can be found in the [User's Guide](#). A complete reference can be found in the expression section of the [tcpdump manual page](#).

Wireshark uses the same syntax for capture filters as [tcpdump](#), [WinDump](#), [Analyzer](#), and any other program that uses the libpcap/WinPcap library.

If you need a capture filter for a specific protocol, have a look for it at the [ProtocolReference](#).

Conteúdo

1. [CaptureFilters](#)
1. [Examples](#)
2. [Useful Filters](#)
3. [Default Capture Filters](#)
4. [Further Information](#)
5. [See Also](#)
6. [Discussion](#)

Examples

Capture only traffic to or from IP address 172.18.5.4:

```
host 172.18.5.4
```

Capture traffic to or from a range of IP addresses:

```
net 192.168.0.0/24
```

Filtros: Captura

The screenshot shows the Wireshark interface with the 'Capture Filters...' option highlighted in the 'Capture' menu. The packet list shows several TCP segments, with packet 8 selected. The packet details pane shows the structure of the selected packet: Ethernet II, Internet Protocol Version 4, and Transmission Control Protocol.

No.	Time	Source	Destination	Protocol	Length	Info
1	0.000000	192.168.1.116	63.245.197.57	TCP	1454	[TCP segment of a reass...
2	0.009221	192.168.1.116	63.245.197.57	TCP	60	443 → 49823 [ACK] Seq=1...
3	0.009221	192.168.1.116	63.245.197.57	TCP	60	443 → 49823 [ACK] Seq=1...
4	0.009221	192.168.1.116	63.245.197.57	TCP	60	443 → 49823 [ACK] Seq=1...
5	0.009525	192.168.1.116	63.245.197.57	TCP	1454	[TCP segment of a reass...
6	0.010147	192.168.1.116	63.245.197.57	TCP	1454	[TCP segment of a reass...
7	0.010767	192.168.1.116	63.245.197.57	TCP	1454	[TCP segment of a reass...
8	0.018891	63.245.197.57	192.168.1.116	TCP	66	[TCP Dup ACK 4#1] 443 →...
9	0.018891	63.245.197.57	192.168.1.116	TCP	60	443 → 49823 [ACK] Seq=1...
10	0.019136	192.168.1.116	63.245.197.57	SSLv2	1454	Encrypted Data
11	0.019747	192.168.1.116	63.245.197.57	TCP	1454	[TCP segment of a reass...
12	0.030297	63.245.197.57	192.168.1.116	TCP	60	443 → 49823 [ACK] Seq=1...
13	0.030551	192.168.1.116	63.245.197.57	TCP	1454	[TCP segment of a reass...

Frame 1: 1454 bytes on wire (11632 bits), 1454 bytes captured (11632 bits) on interface 0
 Ethernet II, Src: HewlettP_fb:66:f2 (b4:b5:2f:fb:66:f2), Dst: CiscoInc_a2:47:48 (50:3d:e5:a2:47:48)
 Internet Protocol Version 4, Src: 192.168.1.116, Dst: 63.245.197.57
 Transmission Control Protocol, Src Port: 49823 (49823), Dst Port: 443 (443), Seq: 1, Ack: 1, Len: 1400
 Secure Sockets Layer

0000 50 3d e5 a2 47 48 b4 b5 2f fb 66 f2 08 00 45 00 P=..GH.. /.f...E.
 0010 05 a0 72 71 40 00 80 06 00 00 c0 a8 01 74 3f f5 ..rq@... ..t?..
 0020 c5 39 c2 9f 01 bb ab b4 ed 40 49 dc f1 05 50 10 .9..... .@I...P.
 0030 00 fe f2 a1 00 00 bd f0 8d 17 b1 08 4d 26 30 36M&06
 0040 e1 6d cb 25 bc ee 3f 66 63 9a e8 05 0b f7 e5 de .m.%...?f c.....
 0050 10 cb 7c 62 9f d1 24 75 ab 85 19 43 50 30 6a b8 ..|b..\$u ...CP0j.

wireshark_pcapng_1673...20160304205113_a08456 | Packets: 4216 · Displayed: 4216 (100.0%) · Dropped: 0 (0.0%) | Profile: Default

The screenshot shows the 'Capture Filters' dialog box in Wireshark. The dialog lists various filters that can be applied to the capture. The 'Name' column lists the filter names, and the 'Filter' column shows the corresponding filter expressions.

Name	Filter
Ethernet address 00:00:5e:00:53:00	ether host 00:00:5e:00:53:00
Ethernet type 0x0806 (ARP)	ether proto 0x0806
No Broadcast and no Multicast	not broadcast and not multicast
No ARP	not arp
IPv4 only	ip
IPv4 address 192.0.2.1	host 192.0.2.1
IPv6 only	ip6
IPv6 address 2001:db8::1	host 2001:db8::1
IPX only	ipx
TCP only	tcp
UDP only	udp
TCP or UDP port 80 (HTTP)	port 80
HTTP TCP port (80)	tcp port http
No ARP and no DNS	not arp and port not 53
Non-HTTP and non-SMTP to/from www.wireshark.org	not port 80 and not port 25 and h

Buttons: Create a new filter., OK, Cancel, Help

wireshark_pcapng_1673...20160304205113_a08456 | Packets: 4216 · Displayed: 4216 (100.0%) · Dropped: 0 (0.0%) | Profile: Default

Filtros: Captura

*Conexão local

File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help

Apply a display filter ... <Ctrl-/> Expression...

No.	Time	Source	Destination	Protocol	Length	Info
1	0.000000	192.168.1.116	63.245.197.57	TCP	1454	[TCP segment of a reass...
2	0.009221	63.245.197.57	192.168.1.116	TCP	60	443 → 49823 [ACK] Seq=1...
3	0.009221	63.245.197.57	192.168.1.116	TCP	60	443 → 49823 [ACK] Seq=1...
4	0.009221					[ACK] Seq=1...
5	0.009525					of a reass...
6	0.010147					of a reass...
7	0.010767					of a reass...
8	0.018891					4#1] 443 →...
9	0.018891					[ACK] Seq=1...
10	0.019136					ta
11	0.019747					of a reass...
12	0.030297					[ACK] Seq=1...
13	0.030551					of a reass...
14	0.030762					[ACK] Seq=1...

Wireshark · Capture Filters

Name	Filter
Ethernet address 00:00:5e:00:53:00	ether host 00:00:5e:00:53:00
Ethernet type 0x0806 (ARP)	ether proto 0x0806
No Broadcast and no Multicast	not broadcast and not multicast
No ARP	not arp
IPv4 only	ip
IPv4 address 192.0.2.1	host 192.0.2.1
IPv6 only	ip6
IPv6 address 2001:db8::1	host 2001:db8::1
IPX only	ipx
TCP only	tcp
UDP only	udp
TCP or UDP port 80 (HTTP)	port 80
HTTP TCP port (80)	tcp port http
No ARP and no DNS	not arp and port not 53
Non-HTTP and non-SMTP to/from www.wireshark.org	not port 80 and not port 25 and h
Host Alvo	host 192.168.1.116

OK Cancel Help

0000 50 3d e5 a2 47 48 b4 b5 2f fb 66 f2 08 00 45 00 P=..GH.. /.f...E.
 0010 05 a0 72 71 40 00 80 06 00 00 c0 a8 01 74 3f f5 ..rq@... ..t?..
 0020 c5 39 c2 9f 01 bb ab b4 ed 40 49 dc f1 05 50 10 .9..... @I...P..
 0030 00 fe f2 a1 00 00 bd f0 8d 17 b1 08 4d 26 30 36 M&06..
 0040 e1 6d cb 25 bc ee 3f 66 63 9a e8 05 0b f7 e5 de ..m.%?f c.....
 0050 10 cb 7c 62 9f d1 24 75 ab 85 19 43 50 30 6a b8 ..|b..\$u ...CP0j.

wireshark_pcapng_1673...20160304205113_a08456 Packets: 4216 · Displayed: 4216 (100.0%) · Dropped: 0 (0.0%) · Profile: Default

*Conexão local

File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help

Options... Ctrl+K
 Start Ctrl+E
 Stop Ctrl+E
 Restart Ctrl+R
 Capture Filters...
 Refresh Interfaces F5

Apply a display filter ... <Ctrl-/> Expression...

No.	Time	Source	Destination	Protocol	Length	Info
1	0.000000					
2	0.009221					
3	0.009221					
4	0.009221					
5	0.009525	192.168.1.116	63.245.197.57	TCP	1454	[TCP segment of a reass...
6	0.010147	192.168.1.116	63.245.197.57	TCP	1454	[TCP segment of a reass...
7	0.010767	192.168.1.116	63.245.197.57	TCP	1454	[TCP segment of a reass...
8	0.018891	63.245.197.57	192.168.1.116	TCP	66	[TCP Dup ACK 4#1] 443 →...
9	0.018891	63.245.197.57	192.168.1.116	TCP	60	443 → 49823 [ACK] Seq=1...
10	0.019136	192.168.1.116	63.245.197.57	SSLv2	1454	Encrypted Data
11	0.019747	192.168.1.116	63.245.197.57	TCP	1454	[TCP segment of a reass...
12	0.030297	63.245.197.57	192.168.1.116	TCP	60	443 → 49823 [ACK] Seq=1...
13	0.030551	192.168.1.116	63.245.197.57	TCP	1454	[TCP segment of a reass...
14	0.030762	63.245.197.57	192.168.1.116	TCP	60	443 → 49823 [ACK] Seq=1...

Frame 1: 1454 bytes on wire (11632 bits), 1454 bytes captured (11632 bits) on interface 0
 Ethernet II, Src: HewlettP_fb:66:f2 (b4:b5:2f:fb:66:f2), Dst: CiscoInc_a2:47:48 (50:3d:e5:a2:47:48)
 Internet Protocol Version 4, Src: 192.168.1.116, Dst: 63.245.197.57
 Transmission Control Protocol, Src Port: 49823 (49823), Dst Port: 443 (443), Seq: 1, Ack: 1, Len: 1400
 Secure Sockets Layer

0000 50 3d e5 a2 47 48 b4 b5 2f fb 66 f2 08 00 45 00 P=..GH.. /.f...E.
 0010 05 a0 72 71 40 00 80 06 00 00 c0 a8 01 74 3f f5 ..rq@... ..t?..
 0020 c5 39 c2 9f 01 bb ab b4 ed 40 49 dc f1 05 50 10 .9..... @I...P..
 0030 00 fe f2 a1 00 00 bd f0 8d 17 b1 08 4d 26 30 36 M&06..
 0040 e1 6d cb 25 bc ee 3f 66 63 9a e8 05 0b f7 e5 de ..m.%?f c.....
 0050 10 cb 7c 62 9f d1 24 75 ab 85 19 43 50 30 6a b8 ..|b..\$u ...CP0j.

wireshark_pcapng_1673...20160304205113_a08456 Packets: 4216 · Displayed: 4216 (100.0%) · Dropped: 0 (0.0%) · Profile: Default

The screenshot displays the Wireshark network protocol analyzer interface. The main window shows a list of captured packets. The selected packet (No. 8) is a TCP segment from 192.168.1.116 to 63.245.197.57. The packet details pane on the left shows the structure of the selected packet: Ethernet II, Internet Protocol Version 4, and Transmission Control Protocol.

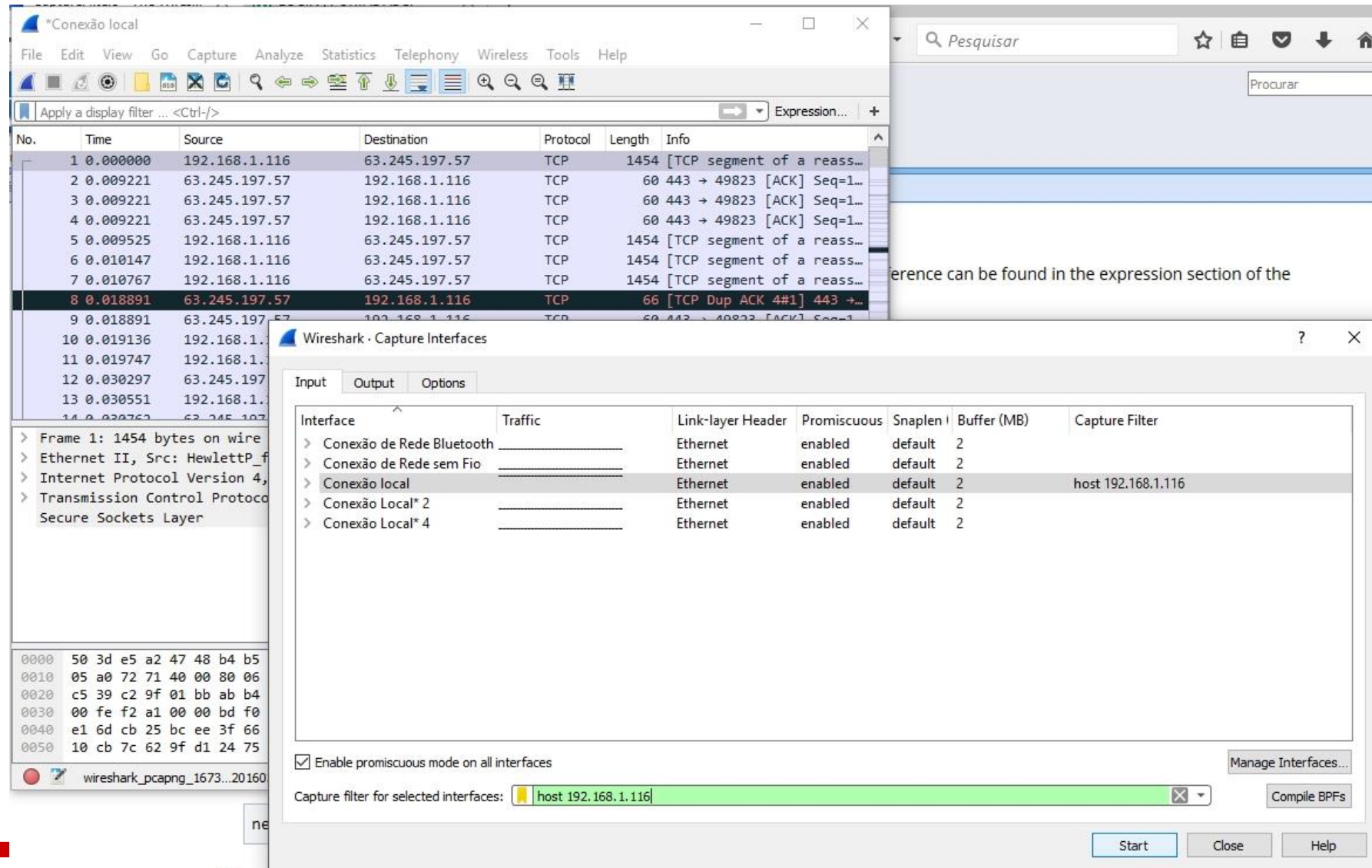
Overlaid on the main window is the 'Wireshark - Capture Interfaces' dialog box. This dialog allows users to select the network interface for capturing traffic. The 'Input' tab is active, showing a list of available interfaces. The 'Conexão local' interface is selected.

Below the interface list, there are checkboxes for 'Enable promiscuous mode on all interfaces' and 'Capture filter for selected interfaces'. The 'Capture filter for selected interfaces' field is currently empty, with a placeholder text 'Enter a capture filter ...'.

On the right side of the dialog, there is a 'Manage Capture Filters' section. This section lists various predefined filters that can be applied to the capture. The filters listed include:

- Ethernet address 00:00:5e:00:53:00: ether host 00:00:5e:00:53:00
- Ethernet type 0x0806 (ARP): ether proto 0x0806
- No Broadcast and no Multicast: not broadcast and not multicast
- No ARP: not arp
- IPv4 only: ip
- IPv4 address 192.0.2.1: host 192.0.2.1
- IPv6 only: ip6
- IPv6 address 2001:db8::1: host 2001:db8::1
- IPX only: ipx
- TCP only: tcp
- UDP only: udp
- TCP or UDP port 80 (HTTP): port 80
- HTTP TCP port (80): tcp port http
- No ARP and no DNS: not arp and port not 53
- Non-HTTP and non-SMTP to/from www.wireshark.org: not port 80 and not port 25 and host www.wireshark.org
- Host Alvo: host 192.168.1.116

At the bottom of the dialog, there are buttons for 'Start', 'Close', and 'Help'.



Filtros: Captura

*Conexão local (host 192.168.1.116)

File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help

Apply a display filter ... <Ctrl-/> Expression...

No.	Time	Source	Destination	Protocol	Length	Info
4170	15.359360	192.168.1.116	63.245.197.57	TCP	1454	[TCP segment of a reass...
4171	15.370276	63.245.197.57	192.168.1.116	TCP	60	443 → 49823 [ACK] Seq=1...
4172	15.370758	192.168.1.116	63.245.197.57	TCP	1454	[TCP segment of a reass...
4173	15.377905	63.245.197.57	192.168.1.116	TCP	60	443 → 49823 [ACK] Seq=1...
4174	15.378336	192.168.1.116	63.245.197.57	TCP	1454	[TCP segment of a reass...
4175	15.385040	63.245.197.57	192.168.1.116	TCP	60	443 → 49823 [ACK] Seq=1...
4176	15.385041	63.245.197.57	192.168.1.116	TCP	60	443 → 49823 [ACK] Seq=1...
4177	15.385528	192.168.1.116	63.245.197.57	TCP	1454	[TCP segment of a reass...
4178	15.386391	192.168.1.116	63.245.197.57	TCP	1454	[TCP segment of a reass...
4179	15.390616	63.245.197.57	192.168.1.116	TCP	60	443 → 49823 [ACK] Seq=1...
4180	15.391090	192.168.1.116	63.245.197.57	TCP	1454	[TCP segment of a reass...
4181	15.391443	63.245.197.57	192.168.1.116	TCP	60	443 → 49823 [ACK] Seq=1...
4182	15.392094	192.168.1.116	63.245.197.57	SSLv2	1454	Encrypted Data
4183	15.405353	63.245.197.57	192.168.1.116	TCP	60	443 → 49823 [ACK] Seq=1...

> Frame 1: 60 bytes on wire (480 bits), 60 bytes captured (480 bits) on interface 0

> Ethernet II, Src: CiscoInc_a2:47:48 (50:3d:e5:a2:47:48), Dst: HewlettP_fb:66:f2 (b4:b5:2f:fb:66:f2)

> Internet Protocol Version 4, Src: 63.245.197.57, Dst: 192.168.1.116

> Transmission Control Protocol, Src Port: 443 (443), Dst Port: 49823 (49823), Seq: 1, Ack: 1, Len: 0

```

0000  b4 b5 2f fb 66 f2 50 3d  e5 a2 47 48 08 00 45 00  ../.f.P= ..GH..E.
0010  00 28 fb 65 00 00 f3 06  05 1f 3f f5 c5 39 c0 a8  .(.e.... ..?...9..
0020  01 74 01 bb c2 9f 49 dd  e9 43 cc 2b 36 54 50 10  .t....I. .C.+6TP.
0030  01 37 ed 56 00 00 00 00  20 20 20 20                .7.V....
  
```

wireshark_pcapng_16738942-2CEE...4B5E980C_20160304214306_a0651 | Packets: 4395 · Displayed: 4395 (100.0%) | Profile: Default

10.3. Packet colorization X LOGIN | PORTAL ABCP X +

www.abcp.org.br/cms/login/ Pesquisar

Associação Brasileira de Cimento Portland 80 anos 1936 - 2016

SELO DA QUALIDADE ABCP Cimentos Conformes 2015

PROGRAMA BRASILEIRO DA QUALIDADE E PRODUTIVIDADE DO HABITAT

Programa setorial - Cimento Portland

Busca

Busca avançada

Quem somos | Associados | Sites recomendados | Fale conosco | Newsletter | Cadastro | Login

Selecione o idioma

BÁSICO SOBRE CIMENTO LABORATÓRIOS SELOS DA QUALIDADE SUSTENTABILIDADE CURSOS EVENTOS PUBLICAÇÕES IMPRENSA PARCEIROS DOWNLOADS HOME

LOGIN

Digite seu email e senha para baixar arquivos e alterar os seus dados.

Dados de login

Email

falso@falso.br

Senha

.....

enviar

• Esqueceu a senha?

• Ainda não é cadastrado? Cadastre-se aqui

Destaques

IABMAS 2016

26 a 30 de JUNHO

FOZ DO IGUAÇU - BRASIL

CBCi

7º CONGRESSO BRASILEIRO DO CIMENTO

20 A 22 DE JUNHO 2016

Abrace esta causa.

Visite nosso site.

www.moradiadigna.org.br

Saiba mais

Mapa da Cadeia Produtiva da Construção

FIESP

Outras Funcionalidades Interessantes

*Conexão local

File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help

Apply a display filter ... <Ctrl-/> Expression...

Packet bytes Narrow & Wide Case sensitive String POST Find Cancel

No.	Time	Source	Destination	Protocol	Length	Info
2110	7.702678	192.168.1.116	63.245.197.57	SSLv2	1454	Encrypted Data
2111	7.711170	63.245.197.57	192.168.1.116	TCP	60	443 → 49823 [ACK] Seq=1...
2112	7.711729	192.168.1.116	63.245.197.57	TCP	1454	[TCP segment of a reass...
2113	7.712673	192.168.1.116	63.245.197.57	TCP	1454	[TCP segment of a reass...
2114	7.723290	63.245.197.57	192.168.1.116	TCP	60	443 → 49823 [ACK] Seq=1...
2115	7.724038	192.168.1.116	63.245.197.57	TCP	1454	[TCP segment of a reass...
2116	7.724992	192.168.1.116	63.245.197.57	SSLv2	1454	Encrypted Data
2117	7.736160	63.245.197.57	192.168.1.116	TCP	66	443 → 49823 [ACK] Seq=1...
2118	7.736162	63.245.197.57	192.168.1.116	TCP	60	443 → 49823 [ACK] Seq=1...
2119	7.736816	192.168.1.116	63.245.197.57	TCP	1454	[TCP segment of a reass...
2120	7.737780	192.168.1.116	63.245.197.57	TCP	1454	[TCP segment of a reass...
2121	7.738718	192.168.1.116	63.245.197.57	TCP	1454	[TCP segment of a reass...

> Frame 2111: 60 bytes on wire (480 bits), 60 bytes captured (480 bits) on interface 0
 > Ethernet II, Src: CiscoInc_a2:47:48 (50:3d:e5:a2:47:48), Dst: HewlettP_fb:66:f2 (b4:b5:2f:fb:66:f2)
 > Internet Protocol Version 4, Src: 63.245.197.57, Dst: 192.168.1.116
 > Transmission Control Protocol, Src Port: 443 (443), Dst Port: 49823 (49823), Seq: 1, Ack: 1472578, Len:

b4 b5 2f fb 66 f2 50 3d e5 a2 47 48 00 00 45 00 .../.f.P= ..GH..E.
 0010 00 28 b7 de 00 00 f3 06 48 a6 3f f5 c5 39 c0 a8 ..(..... H.?.9..
 0020 01 74 01 bb c2 9f 49 dc f1 05 ab cb 65 81 50 10 .t....I.e.P.
 0030 01 37 d6 c8 00 00 00 00 20 20 20 20 .7.....

wireshark_pcapng_16738942-2CEE...4B5E980C_20160304205113_a0845 | Packets: 4216 · Displayed: 4216 (100.0%) | Profile: Default

*Conexão local

File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help

Apply a display filter ... <Ctrl-/> Expression...

Packet bytes Narrow & Wide Case sensitive String POST Find Cancel

No.	Time	Source	Destination	Protocol	Length	Info
2290	8.354249	192.168.1.116	63.245.197.57	TCP	1454	[TCP segment of a reass...
2291	8.356519	63.245.197.57	192.168.1.116	TCP	60	443 → 49823 [ACK] Seq=1...
2292	8.356745	192.168.1.116	63.245.197.57	TCP	1454	[TCP segment of a reass...
2293	8.385045	63.245.197.57	192.168.1.116	TCP	60	443 → 49823 [ACK] Seq=1...
2294	8.385353	192.168.1.116	63.245.197.57	TCP	1454	[TCP segment of a reass...
2295	8.385877	192.168.1.116	63.245.197.57	TCP	1454	[TCP segment of a reass...
2296	8.387658	192.168.1.116	187.45.195.15	TCP	66	50580 → 80 [SYN] Seq=0 ...
2297	8.408092	187.45.195.15	192.168.1.116	TCP	66	80 → 50580 [SYN, ACK] S...
2298	8.408256	192.168.1.116	187.45.195.15	TCP	54	50580 → 80 [ACK] Seq=1 ...
2299	8.409110	63.245.197.57	192.168.1.116	TCP	60	443 → 49823 [ACK] Seq=1...
2300	8.413611	192.168.1.116	187.45.195.15	HTTP	1077	POST /cms/wp-content/th...
2301	8.414243	192.168.1.116	63.245.197.57	SSLv2	1454	Encrypted Data

> Frame 2300: 1077 bytes on wire (8616 bits), 1077 bytes captured (8616 bits) on interface 0
 > Ethernet II, Src: HewlettP_fb:66:f2 (b4:b5:2f:fb:66:f2), Dst: CiscoInc_a2:47:48 (50:3d:e5:a2:47:48)
 > Internet Protocol Version 4, Src: 192.168.1.116, Dst: 187.45.195.15
 > Transmission Control Protocol, Src Port: 50580 (50580), Dst Port: 80 (80), Seq: 1, Ack: 1, Len: 1023

Hypertext Transfer Protocol
 POST /cms/wp-content/themes/abcp/active-page.php?campos%20=%20email2=[object%20HTMLInputElement]&a
 [Expert Info (Chat/Sequence): POST /cms/wp-content/themes/abcp/active-page.php?campos%20=%20ema:
 Request Method: POST
 Request URI: /cms/wp-content/themes/abcp/active-page.php?campos%20=%20email2=[object%20HTMLInput

0030 01 01 f3 24 00 00 50 4f 53 54 20 2f 63 6d 73 2f ...\$...PO ST /cms/
 0040 77 70 2d 63 6f 6e 74 65 6e 74 2f 74 68 65 6d 65 wp-conte nt/theme
 0050 73 2f 61 62 63 70 2f 61 63 74 69 76 65 2d 70 61 s/abcp/a ctive-pa
 0060 67 65 2e 70 68 70 3f 63 61 6d 70 6f 73 25 32 30 ge.php?c ampos%20
 0070 3d 25 32 30 65 6d 61 69 6c 32 3d 5b 6f 62 6a 65 =%20emai l2=[obje
 0080 63 74 25 32 30 48 54 4d 4c 49 6e 70 75 74 45 6c ct%20HTM LInputEl

HTTP Request Method (http.request.method), 4 bytes | Packets: 4216 · Displayed: 4216 (100.0%) | Profile: Default

Outras Funcionalidades Interessantes

*Conexão local

File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help

Apply a display filter ... <Ctrl-/> Expression...

Packet bytes Narrow & Wide Case sensitive String POST Find Cancel

No.	Time	Source	Destination	Protocol	Length	Info
2290	8.354249	192.168.1.116	63.245.197.57	TCP	1454	[TCP segment of a reass...
2291	8.356519	63.245.197.57	192.168.1.116	TCP	60	443 → 49823 [ACK] Seq=1...
2292	8.356745	192.168.1.116	63.245.197.57	TCP	1454	[TCP segment of a reass...
2293	8.385045	63.245.197.57	192.168.1.116	TCP	60	443 → 49823 [ACK] Seq=1...
2294	8.385353	192.168.1.116	63.245.197.57	TCP	1454	[TCP segment of a reass...
2295	8.385877	192.168.1.116	63.245.197.57	TCP	1454	[TCP segment of a reass...
2296	8.387658	192.168.1.116	187.45.195.15	TCP	66	50580 → 80 [SYN] Seq=0 ...
2297	8.408092	187.45.195.15	192.168.1.116	TCP	66	80 → 50580 [SYN, ACK] S...
2298	8.408256	192.168.1.116	187.45.195.15	TCP	54	50580 → 80 [ACK] Seq=1 ...
2299	8.409110	63.245.197.57	192.168.1.116	TCP	60	443 → 49823 [ACK] Seq=1...
2300	8.413611	192.168.1.116	187.45.195.15	HTTP	1077	POST /cms/wp-content/th...
2301	8.414243	192.168.1.116	187.45.195.15	SSLv2	1454	Encrypted Data

Frame 2300: 1077 bytes captured (8616 bits) on interface 0
Ethernet II, Src: CiscoInc_a2:47:48 (50:3d:e5:a2:47:48), Dst: 187.45.195.15
Internet Protocol Version 4, Src: 192.168.1.116, Dst: 187.45.195.15
Transmission Control Protocol, Src Port: 49823, Dst Port: 80 (80), Seq: 1, Ack: 1, Len: 1023
Hypertext Transfer Protocol
POST /cms/wp-content/themes/abcp/active-page.php?campos%20=%20email2=[object%20HTMLInputElement]&act=login&email=falso@falso.br&senha=falsofalso HTTP/1.1 200 OK

Mark/Unmark Packet Ctrl+M
Ignore/Unignore Packet Ctrl+D
Set/Unset Time Reference Ctrl+T
Time Shift... Ctrl+Shift+T
Packet Comment...
Edit Resolved Name
Apply as Filter
Prepare a Filter
Conversation Filter
Colorize Conversation
SCTP
Follow
Copy
Protocol Preferences
Decode As...
Show Packet in New Window

TCP Stream
UDP Stream
SSL Stream

1 client pkt(s), 1 server pkt(s), 1 turn(s).

Entire conversation (1346 bytes) Show data as ASCII Stream 7

Find: Find Next

Hide this stream Print Save as... Close Help

Wireshark · Follow TCP Stream (tcp.stream eq 7) · wireshark_p...

```
POST /cms/wp-content/themes/abcp/active-page.php?campos%20=
%20email2=[object
%20HTMLInputElement]&act=login&email=falso@falso.br&senha=falsofalso HTTP/1.1
Host: www.abcp.org.br
User-Agent: Mozilla/5.0 (Windows NT 10.0; WOW64; rv:43.0) Gecko/
20100101 Firefox/43.0
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8
Accept-Language: pt-BR,pt;q=0.8,en-US;q=0.5,en;q=0.3
Accept-Encoding: gzip, deflate
Referer: http://www.abcp.org.br/cms/login/
Content-Length: 89
Content-Type: text/plain; charset=UTF-8
Cookie:
wpesc_customer_cookie_114f3da04c4fca0074727984ae650c43=9126%7C145
7308165%7Cee2b6f79503d4b6ec34a323f2da82fcc;
PHPSESSID=2i8h43l7ub4fi69imhftc560f1;
__utma=37579504.2045452273.1457135346.1457135346.1457135346.1;
__utmb=37579504.2.10.1457135346; __utmc=37579504;
__utmz=37579504.1457135346.1.1.utmcsr=google|utmccn=(organic)|
utmcmd=organic|utmctr=(not%20provided); __utmt=1
Connection: keep-alive

campos = email2=[object
HTMLInputElement]&act=login&email=falso@falso.br&senha=falsofalso HTTP/1.1 200 OK
Date: Fri, 04 Mar 2016 23:51:19 GMT
Server: Apache
Expires: Thu, 19 Nov 1981 08:52:00 GMT
Cache-Control: no-store, no-cache, must-revalidate, post-check=0, pre-check=0
Pragma: no-cache
Content-Length: 35
```

1 client pkt(s), 1 server pkt(s), 1 turn(s).

Entire conversation (1346 bytes) Show data as ASCII Stream 7

Find: Find Next

Hide this stream Print Save as... Close Help

- ▶ Abrir arquivos de capturas
- ▶ Armazenar capturas
 - ◆ Inteiras
 - ◆ Filtradas
- ▶ Verificar estatísticas, características do tráfego, etc.