UNICARIOCA 25 anos
Centro Universitário

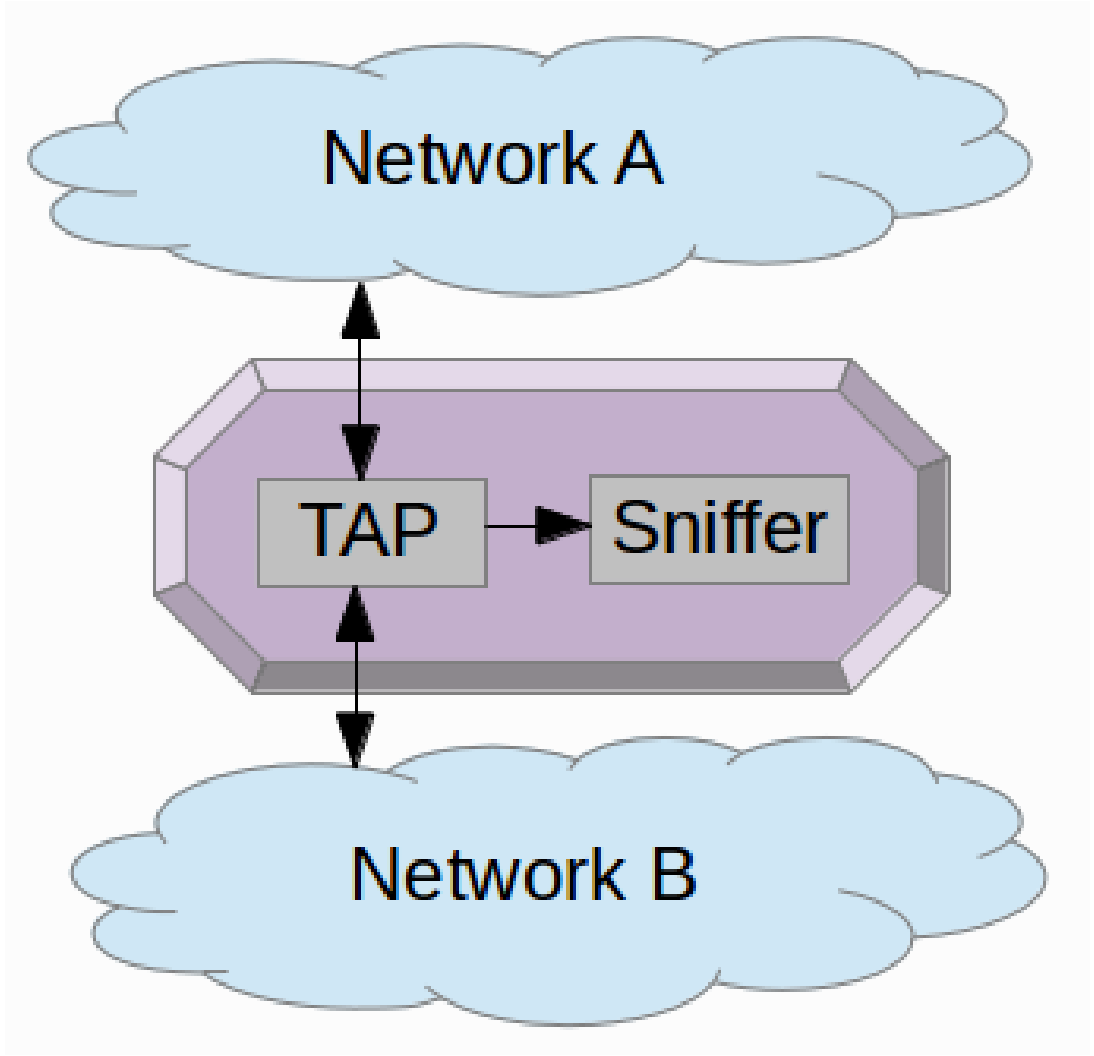
Wireshark
Um Analisador de Protocolos

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

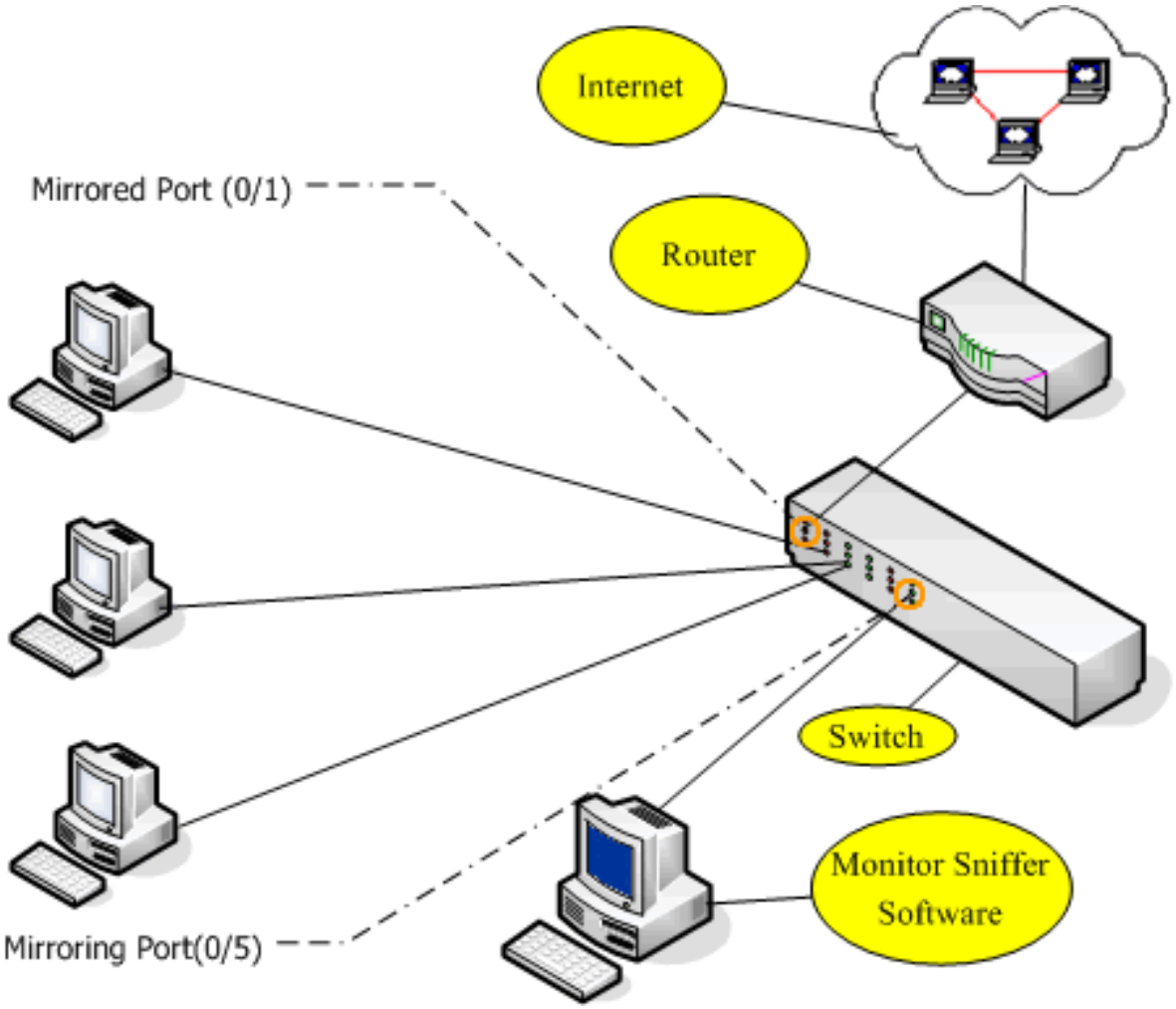
Fundamentos

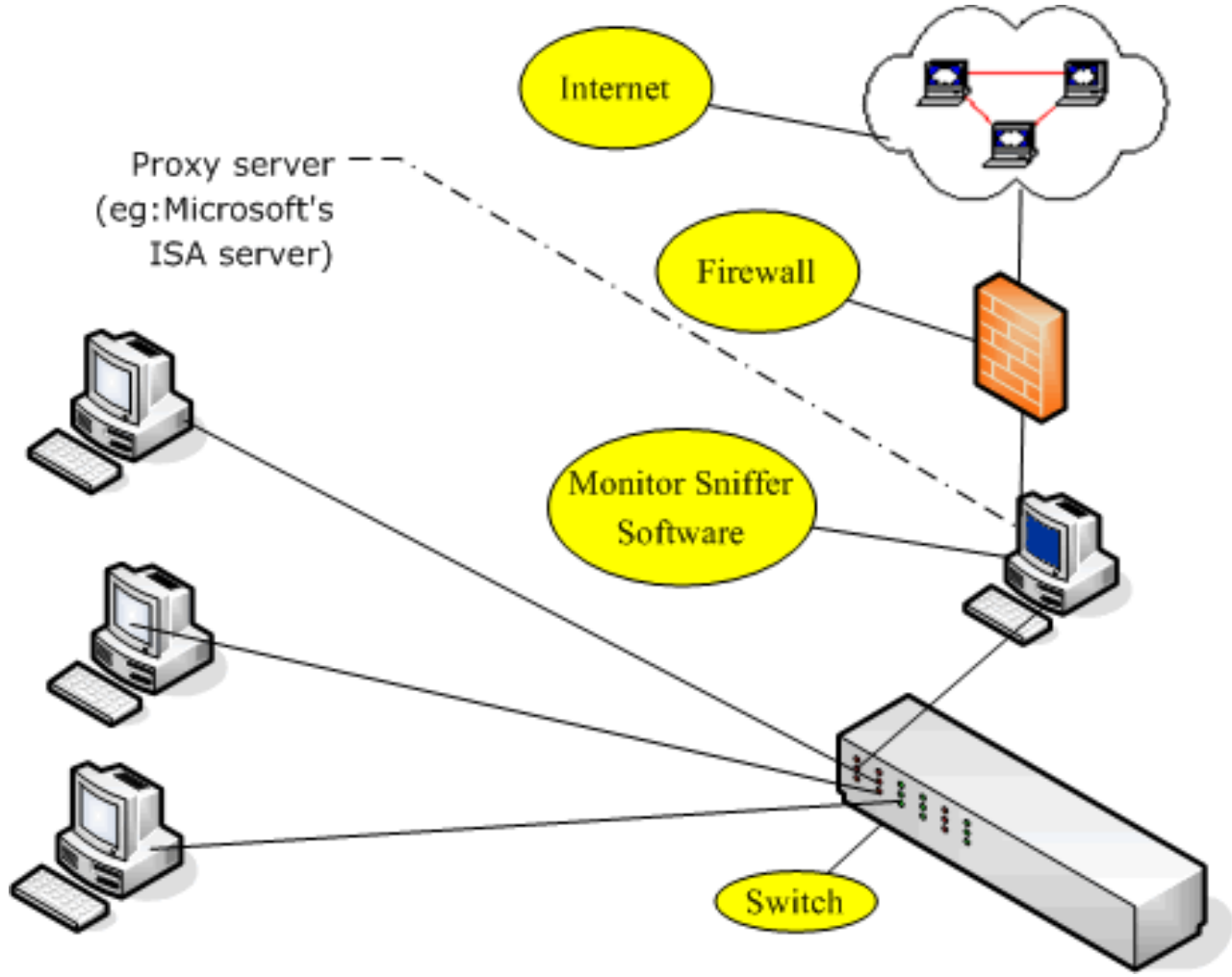
- Posicionamento adequado da estação
- Obtenção e Instalação do Wireshark
- Interface em modo promíscuo - Winpcap
- Escolha da(s) interface(s) a capturar
- Customização do aplicativo
- Uso dos filtros
  - Captura
  - Display
- Outras funcionalidades interessantes

Posicionamento do Sniffer

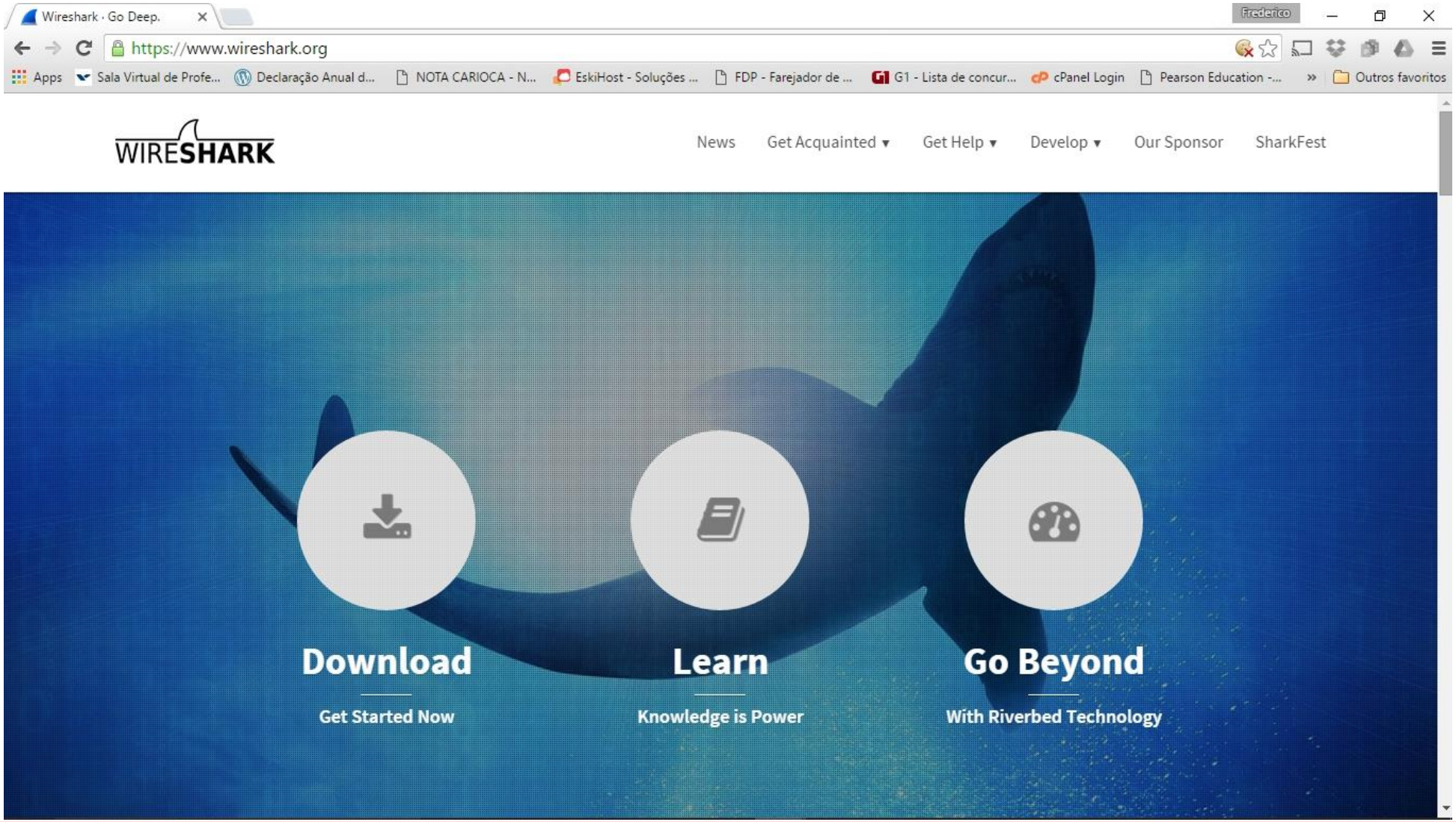


Posicionamento do Sniffer

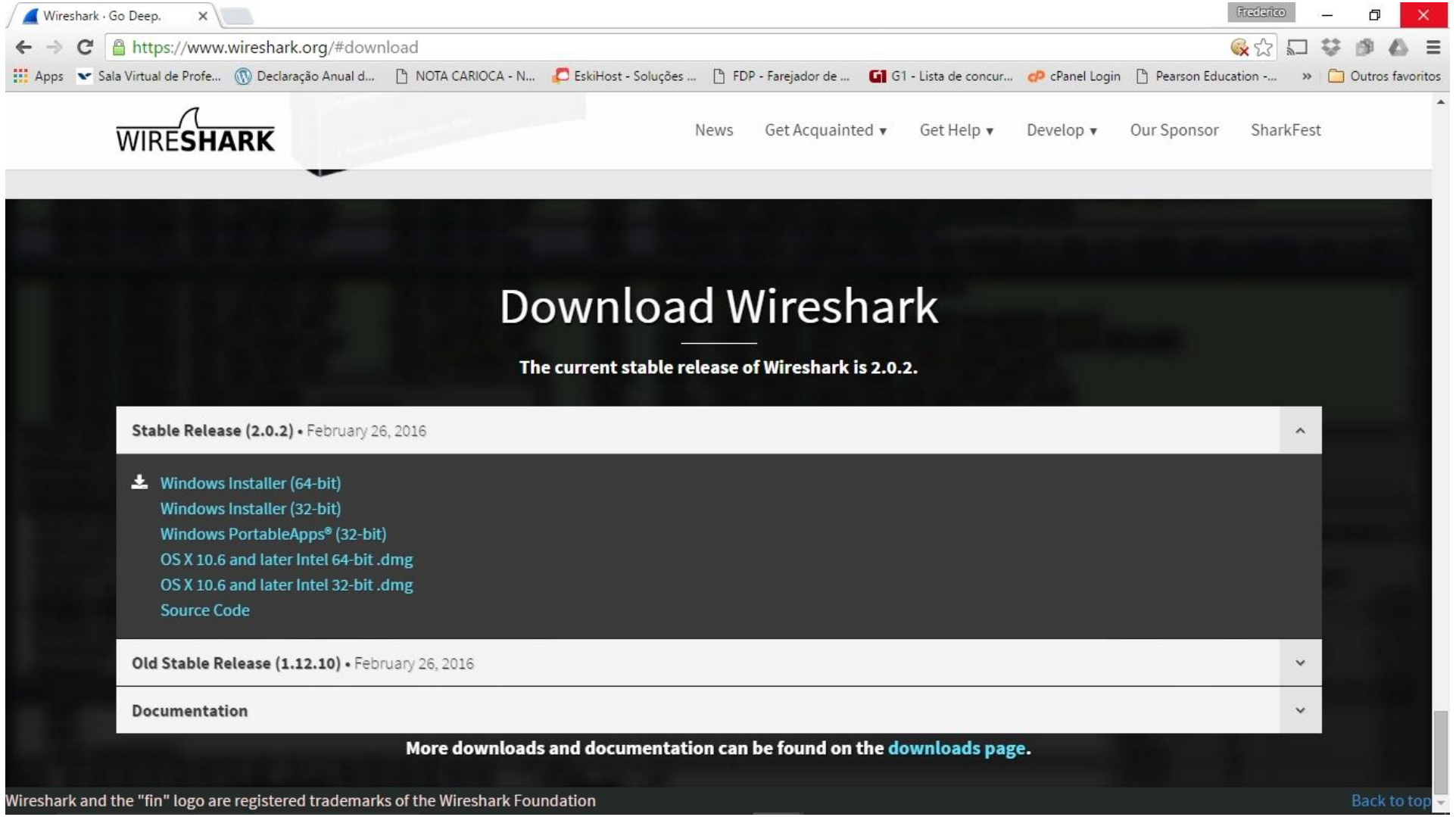




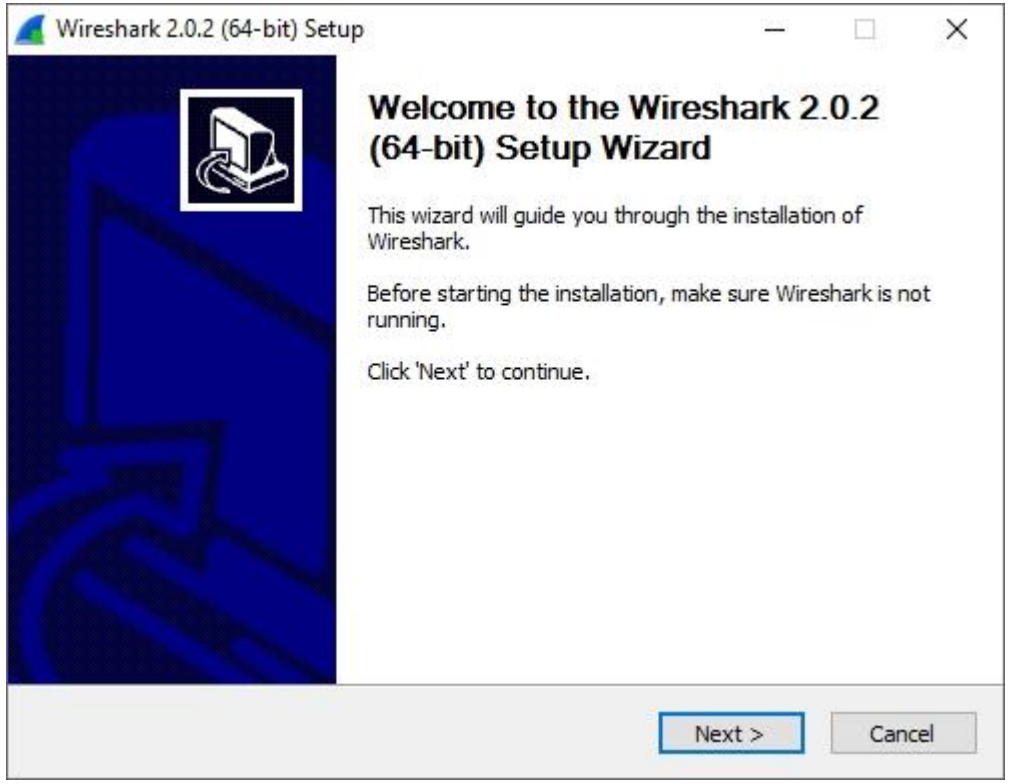
Obtenção e Instalação

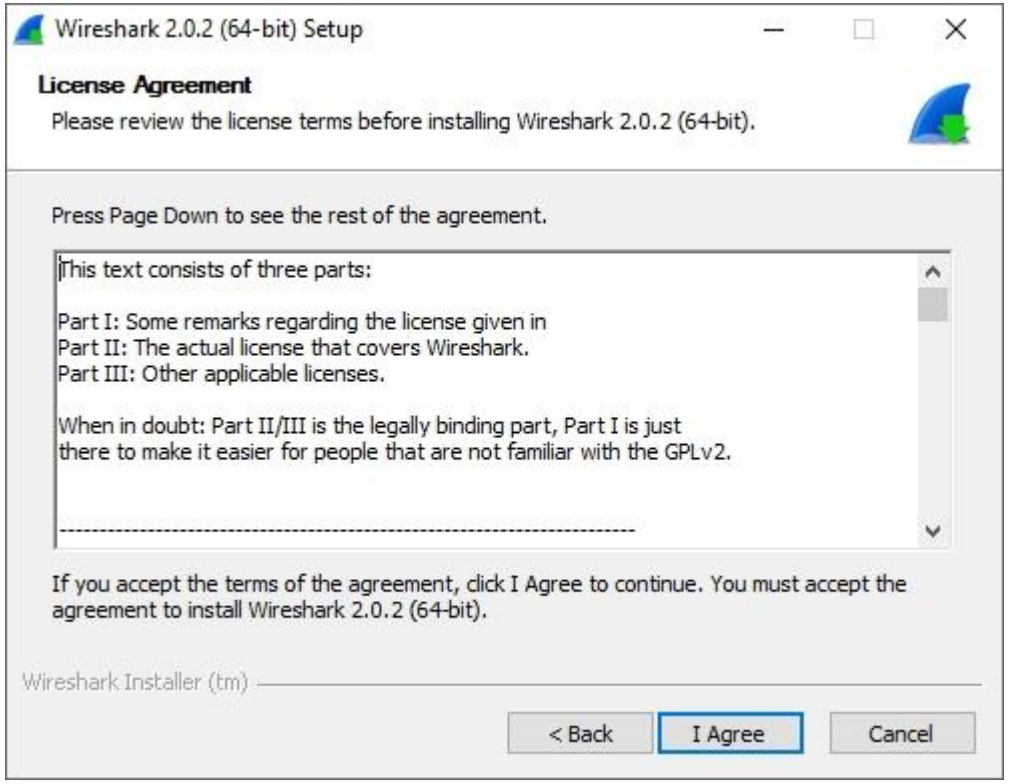


Obtenção e Instalação

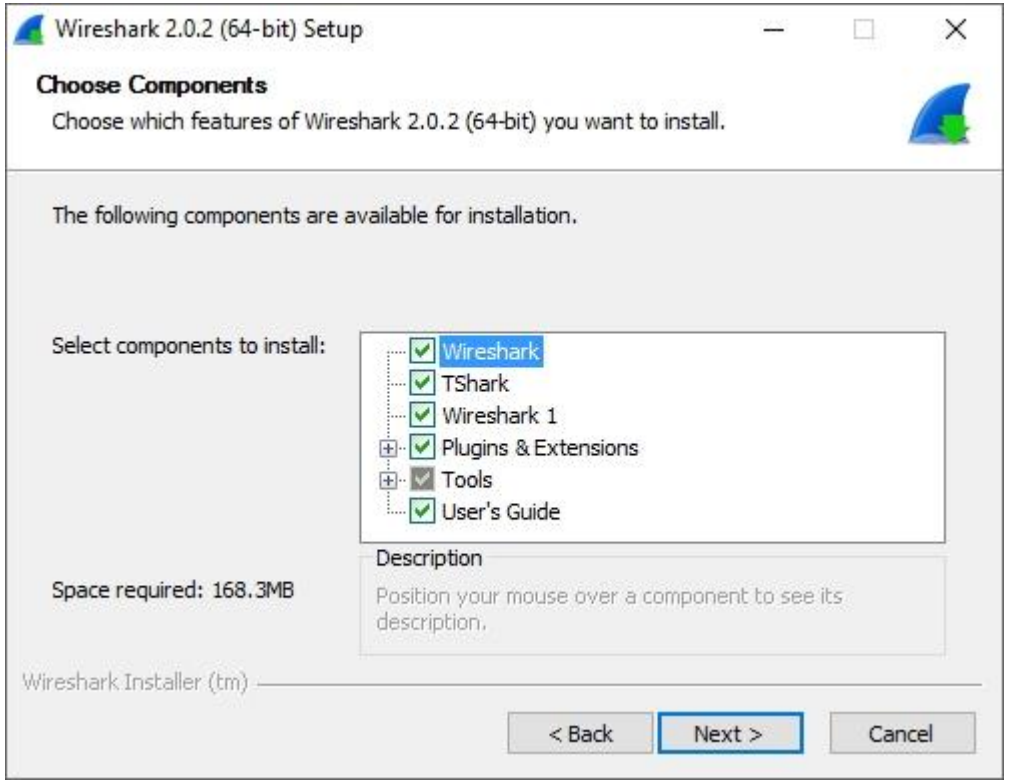


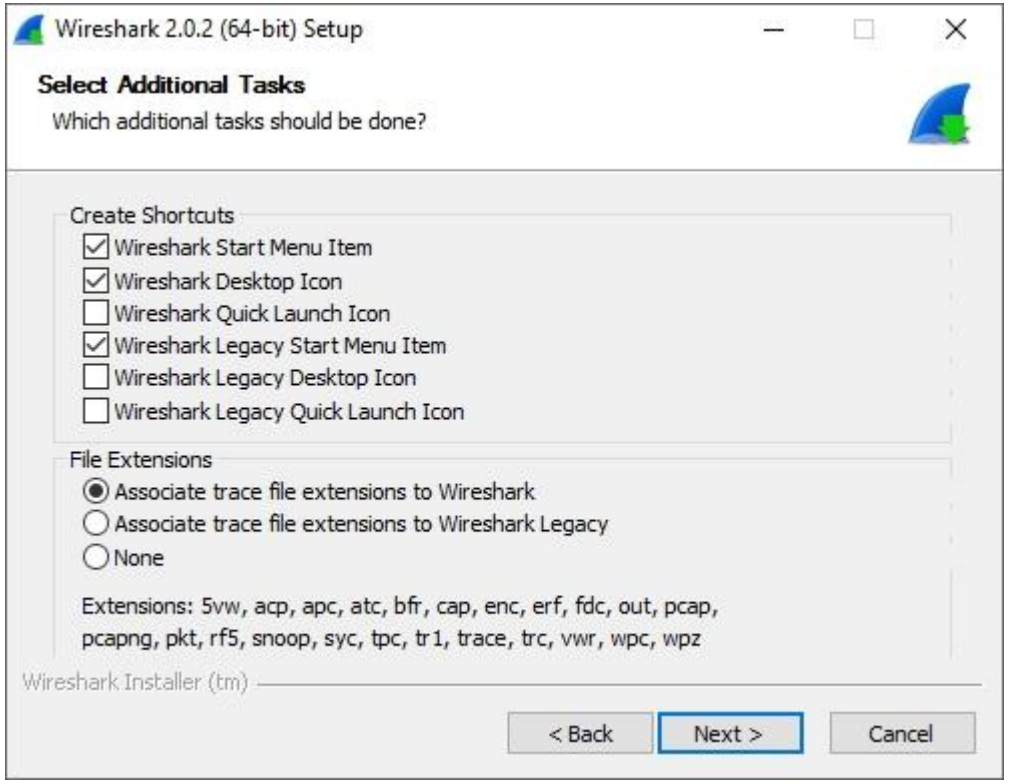
Instalação


Wireshark 2.0.2 (64-bit) Setup
Welcome to the Wireshark 2.0.2 (64-bit) Setup Wizard
This wizard will guide you through the installation of Wireshark.
Before starting the installation, make sure Wireshark is not running.
Click 'Next' to continue.
Next >
Cancel

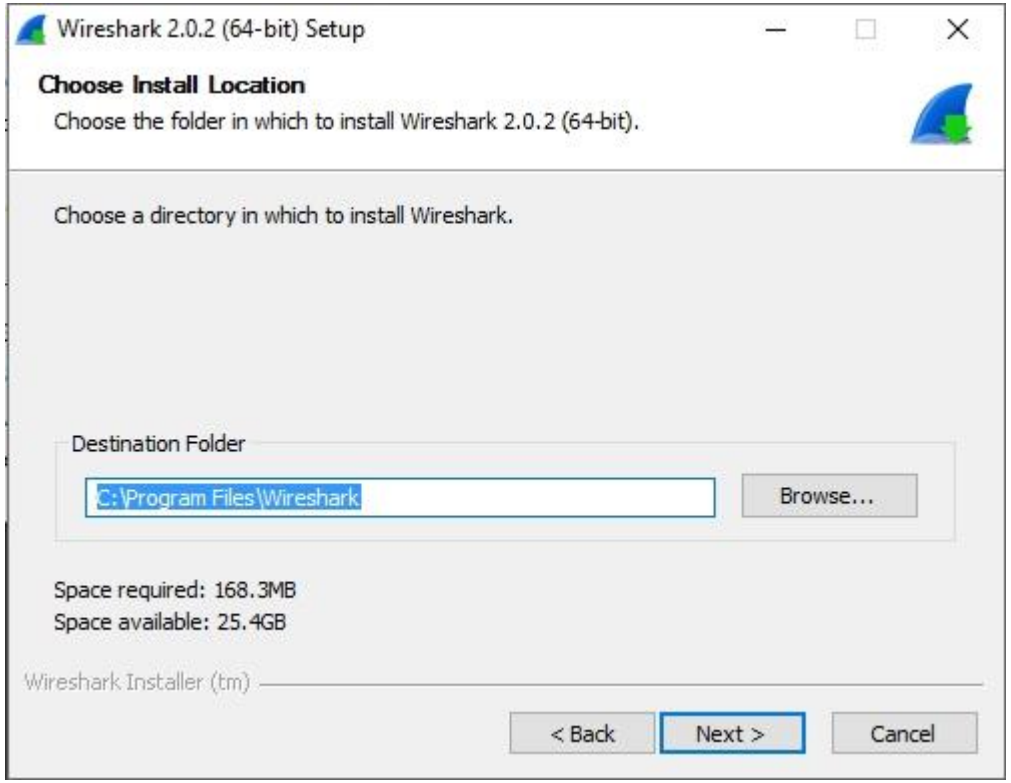

Wireshark 2.0.2 (64-bit) Setup
License Agreement
Please review the license terms before installing Wireshark 2.0.2 (64-bit).
Press Page Down to see the rest of the agreement.
This text consists of three parts:
Part I: Some remarks regarding the license given in
Part II: The actual license that covers Wireshark.
Part III: Other applicable licenses.
When in doubt: Part II/III is the legally binding part, Part I is just
there to make it easier for people that are not familiar with the GPLv2.
If you accept the terms of the agreement, click I Agree to continue. You must accept the agreement to install Wireshark 2.0.2 (64-bit).
Wireshark Installer (tm)
< Back
I Agree
Cancel

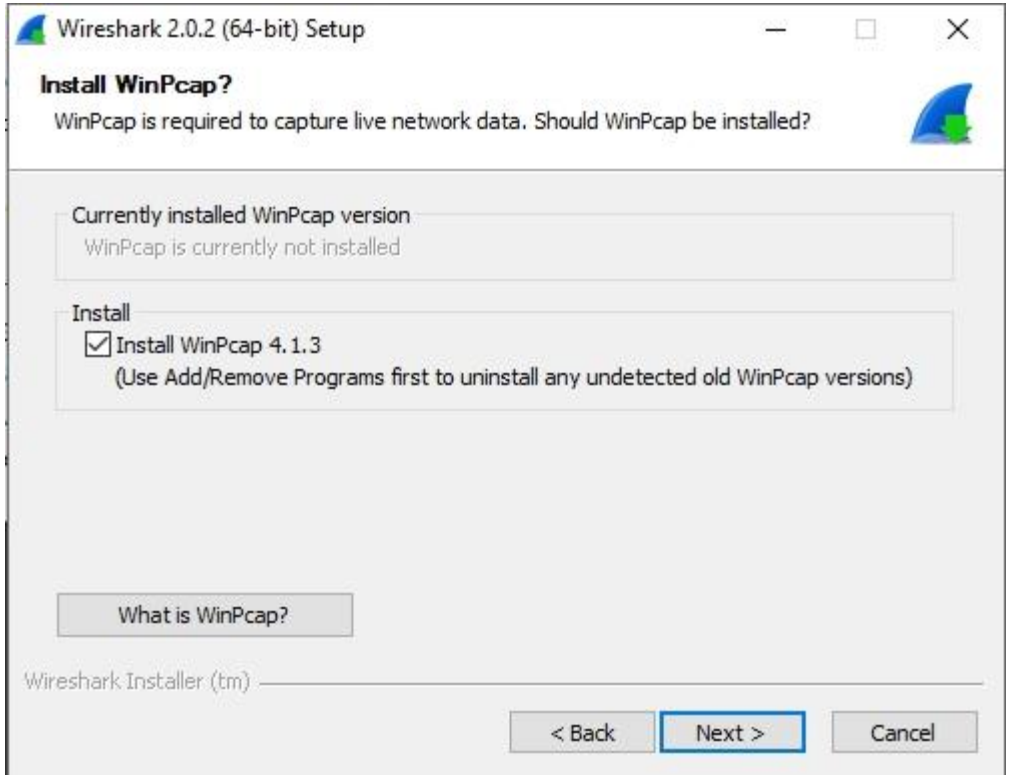
Instalação


Wireshark 2.0.2 (64-bit) Setup
Choose Components
Choose which features of Wireshark 2.0.2 (64-bit) you want to install.
The following components are available for installation.
Select components to install:
Wireshark
TShark
Wireshark 1
Plugins & Extensions
Tools
User's Guide
Description
Position your mouse over a component to see its description.
Space required: 168.3MB
Wireshark Installer (tm)
< Back
Next >
Cancel

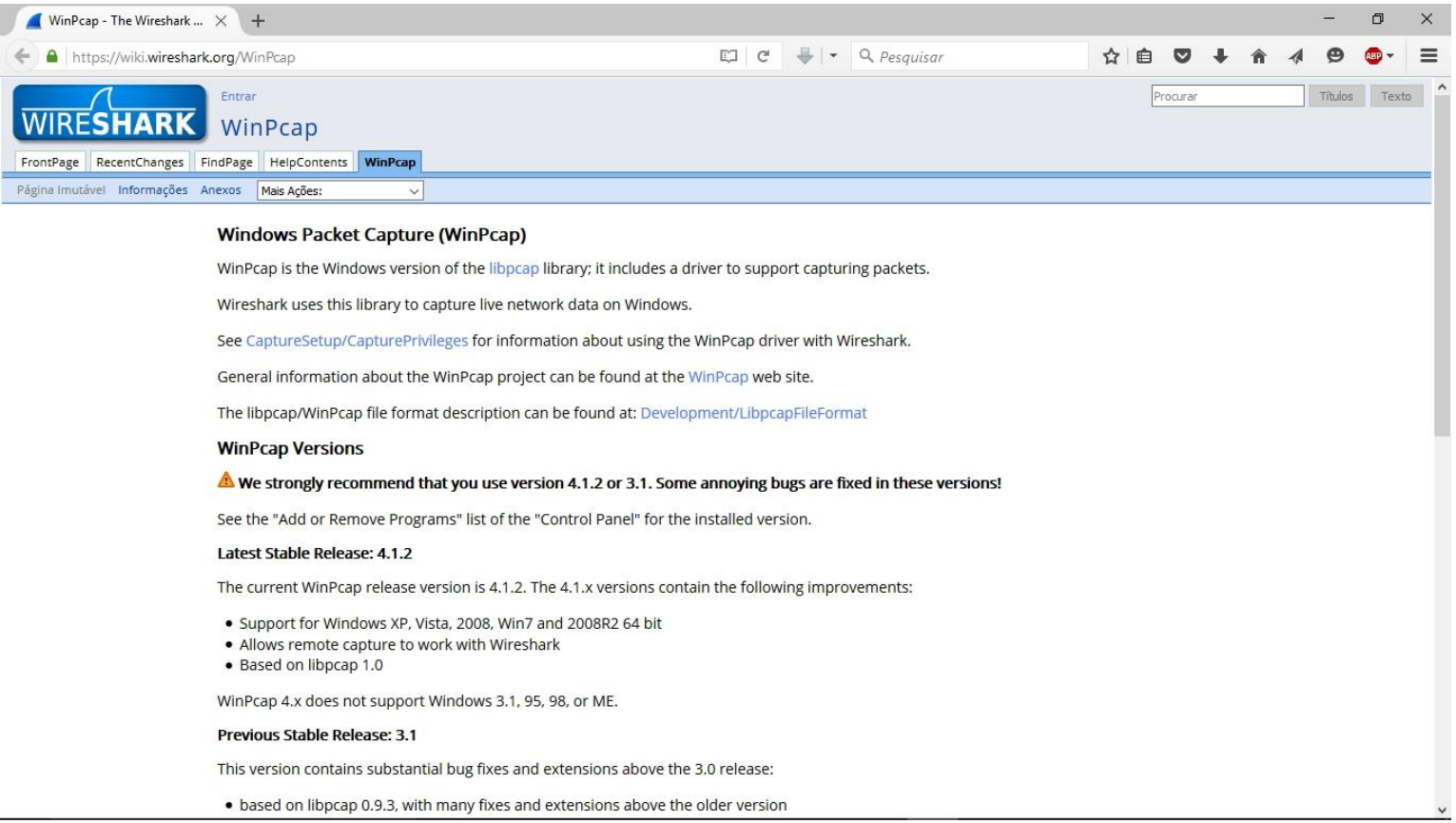

Wireshark 2.0.2 (64-bit) Setup
Select Additional Tasks
Which additional tasks should be done?
Create Shortcuts
Wireshark Start Menu Item
Wireshark Desktop Icon
Wireshark Quick Launch Icon
Wireshark Legacy Start Menu Item
Wireshark Legacy Desktop Icon
Wireshark Legacy Quick Launch Icon
File Extensions
Associate trace file extensions to Wireshark
Associate trace file extensions to Wireshark Legacy
None
Extensions: 5vw, acp, apc, atc, bfr, cap, enc, erf, fdc, out, pcap, pcapng, pkt, rf5, snoop, syc, tpc, tr1, trace, trc, vwr, wpc, wpz
Wireshark Installer (tm)
< Back
Next >
Cancel

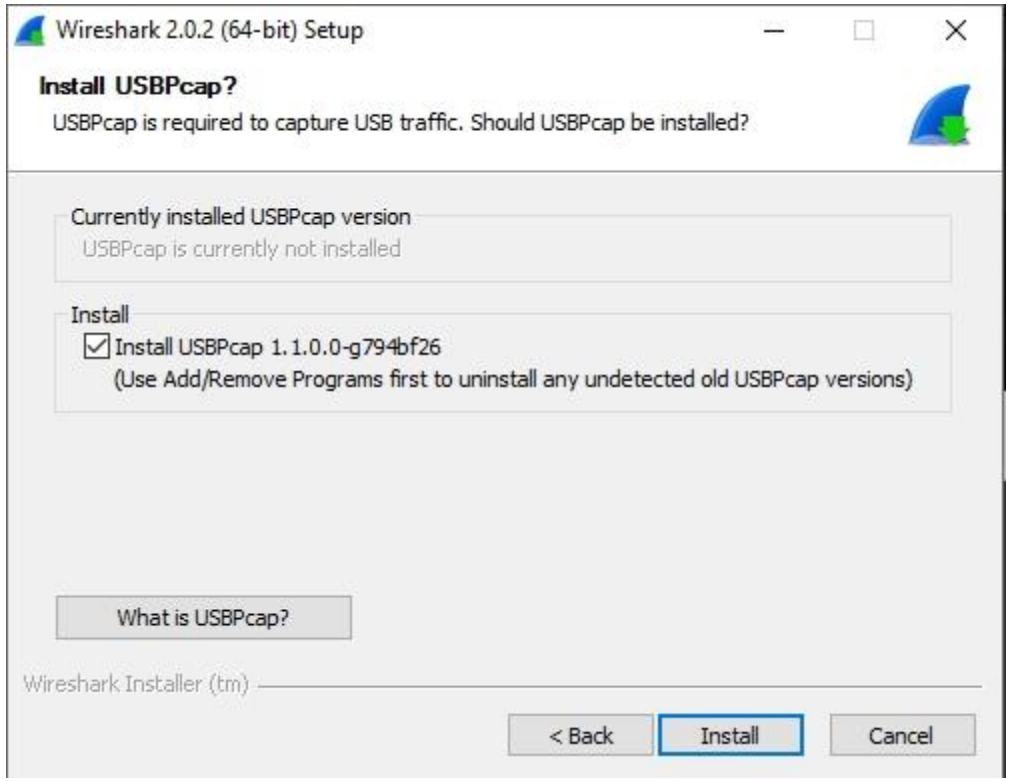
Instalação


Wireshark 2.0.2 (64-bit) Setup
Choose Install Location
Choose the folder in which to install Wireshark 2.0.2 (64-bit).
Choose a directory in which to install Wireshark.
Destination Folder
C:\Program Files\Wireshark
Browse...
Space required: 168.3MB
Space available: 25.4GB
Wireshark Installer (tm)
< Back
Next >
Cancel


Wireshark 2.0.2 (64-bit) Setup
Install WinPcap?
WinPcap is required to capture live network data. Should WinPcap be installed?
Currently installed WinPcap version
WinPcap is currently not installed
Install
Install WinPcap 4.1.3
(Use Add/Remove Programs first to uninstall any undetected old WinPcap versions)
What is WinPcap?
Wireshark Installer (tm)
< Back
Next >
Cancel

Instalação


WinPcap - The Wireshark ...
https://wiki.wireshark.org/WinPcap
Pesquisar
Entrar
WIRESHARK
WinPcap
Procurar
Títulos
Texto
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

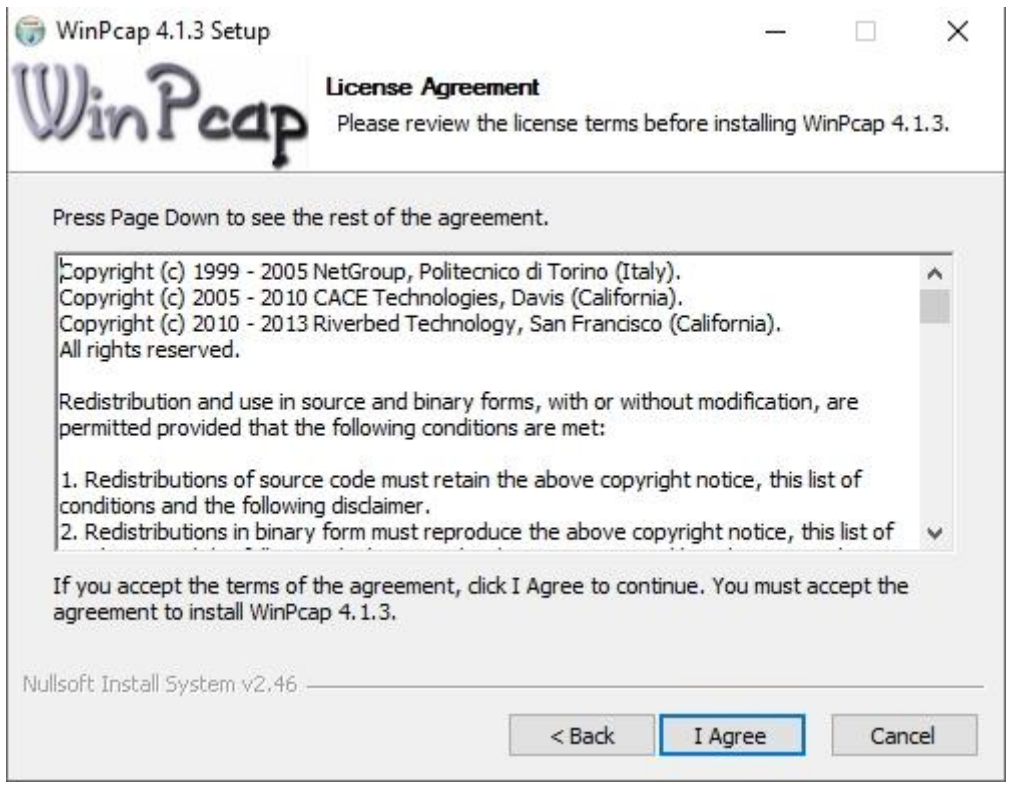

Wireshark 2.0.2 (64-bit) Setup
Install USBPcap?
USBPcap is required to capture USB traffic. Should USBPcap be installed?
Currently installed USBPcap version
USBPcap is currently not installed
Install
Install USBPcap 1.1.0.0-g794bf26
(Use Add/Remove Programs first to uninstall any undetected old USBPcap versions)
What is USBPcap?
Wireshark Installer (tm)
< Back
Install
Cancel

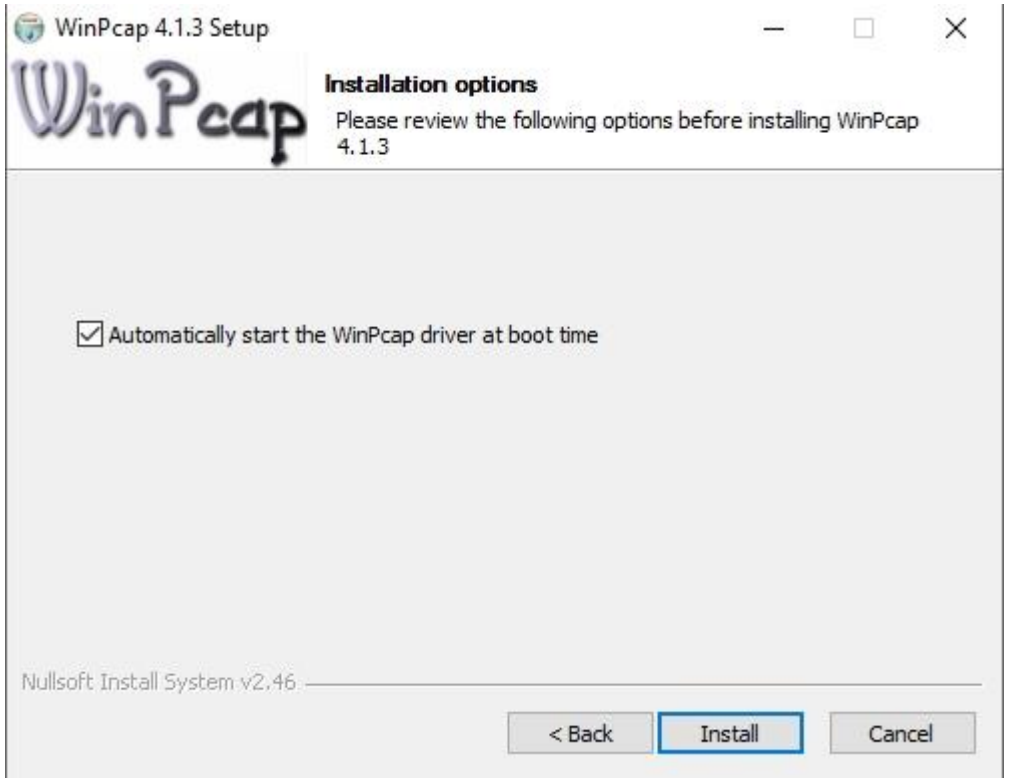
Instalação


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 commited 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
Google Groups
Subscribe to USBPcap
Email:
Subscribe
Visit this group

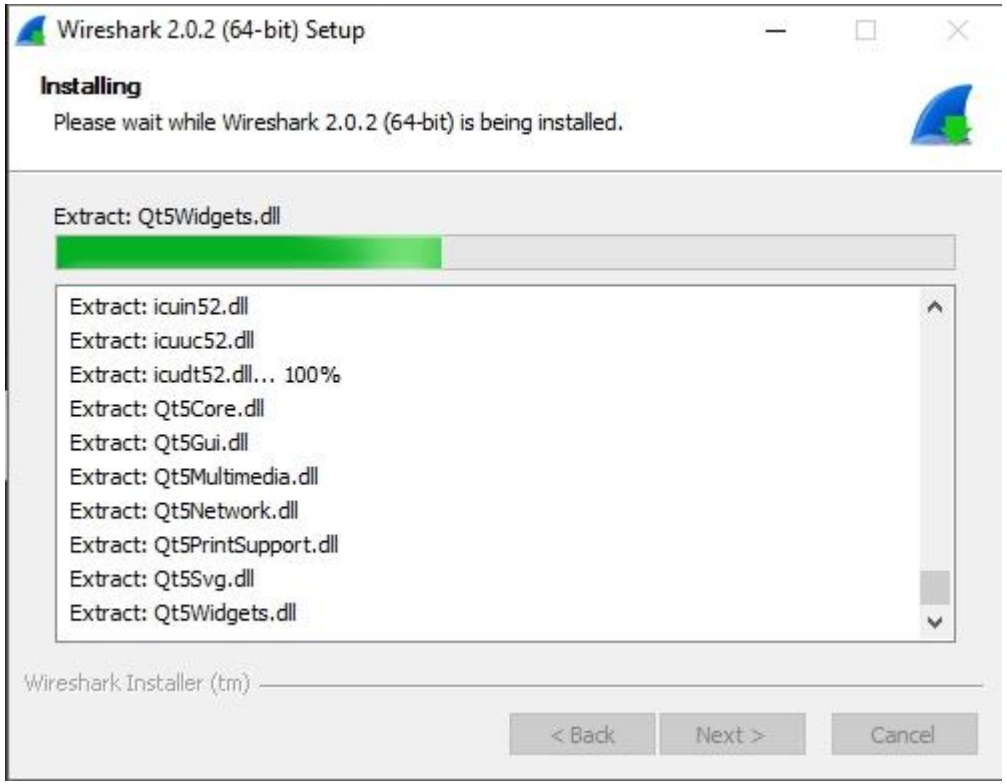

WinPcap 4.1.3 Setup
Welcome to the WinPcap 4.1.3 Setup Wizard
This Wizard will guide you through the entire WinPcap installation.
For more information or support, please visit the WinPcap home page.
http://www.winpcap.org
Next >
Cancel

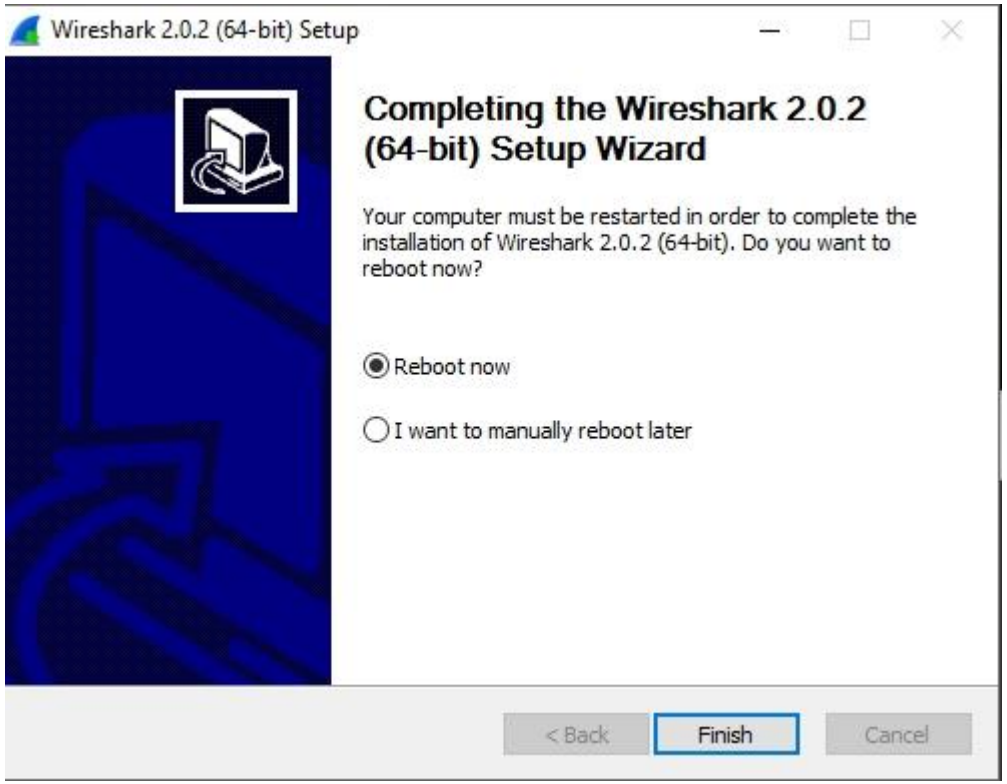
Instalação


WinPcap 4.1.3 Setup
License Agreement
Please review the license terms before installing WinPcap 4.1.3.
Press Page Down to see the rest of the agreement.
Copyright (c) 1999 - 2005 NetGroup, Politecnico di Torino (Italy).
Copyright (c) 2005 - 2010 CACE Technologies, Davis (California).
Copyright (c) 2010 - 2013 Riverbed Technology, San Francisco (California).
All rights reserved.
Redistribution and use in source and binary forms, with or without modification, are permitted provided that the following conditions are met:
1. Redistributions of source code must retain the above copyright notice, this list of conditions and the following disclaimer.
2. Redistributions in binary form must reproduce the above copyright notice, this list of
If you accept the terms of the agreement, click I Agree to continue. You must accept the agreement to install WinPcap 4.1.3.
Nullsoft Install System v2.46
< Back
I Agree
Cancel

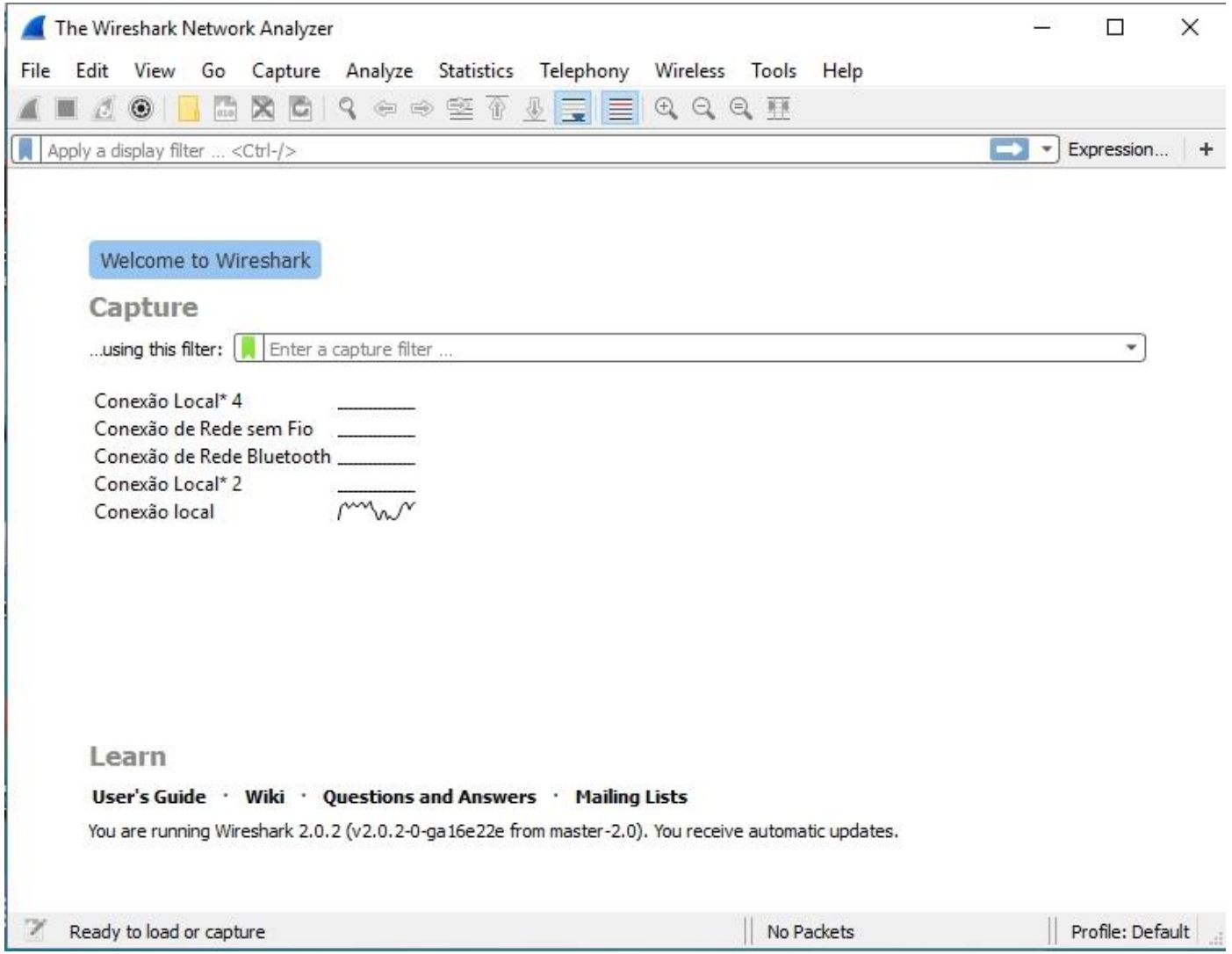

WinPcap 4.1.3 Setup
Installation options
Please review the following options before installing WinPcap 4.1.3
Automatically start the WinPcap driver at boot time
Nullsoft Install System v2.46
< Back
Install
Cancel

Instalação

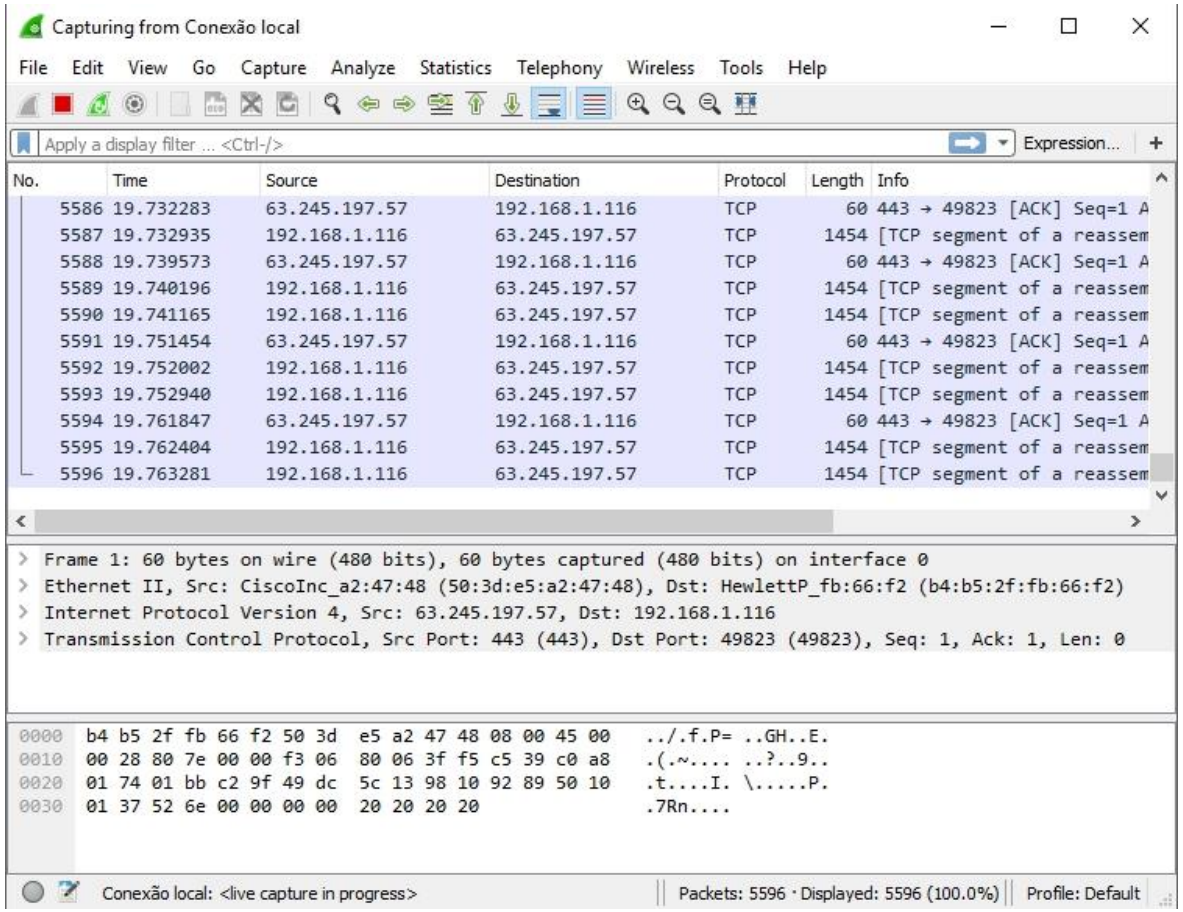

Wireshark 2.0.2 (64-bit) Setup
Installing
Please wait while Wireshark 2.0.2 (64-bit) is being installed.
Extract: Qt5Widgets.dll
Extract: icuin52.dll
Extract: icuuc52.dll
Extract: icudt52.dll... 100%
Extract: Qt5Core.dll
Extract: Qt5Gui.dll
Extract: Qt5Multimedia.dll
Extract: Qt5Network.dll
Extract: Qt5PrintSupport.dll
Extract: Qt5Svg.dll
Extract: Qt5Widgets.dll
Wireshark Installer (tm)
< Back
Next >
Cancel

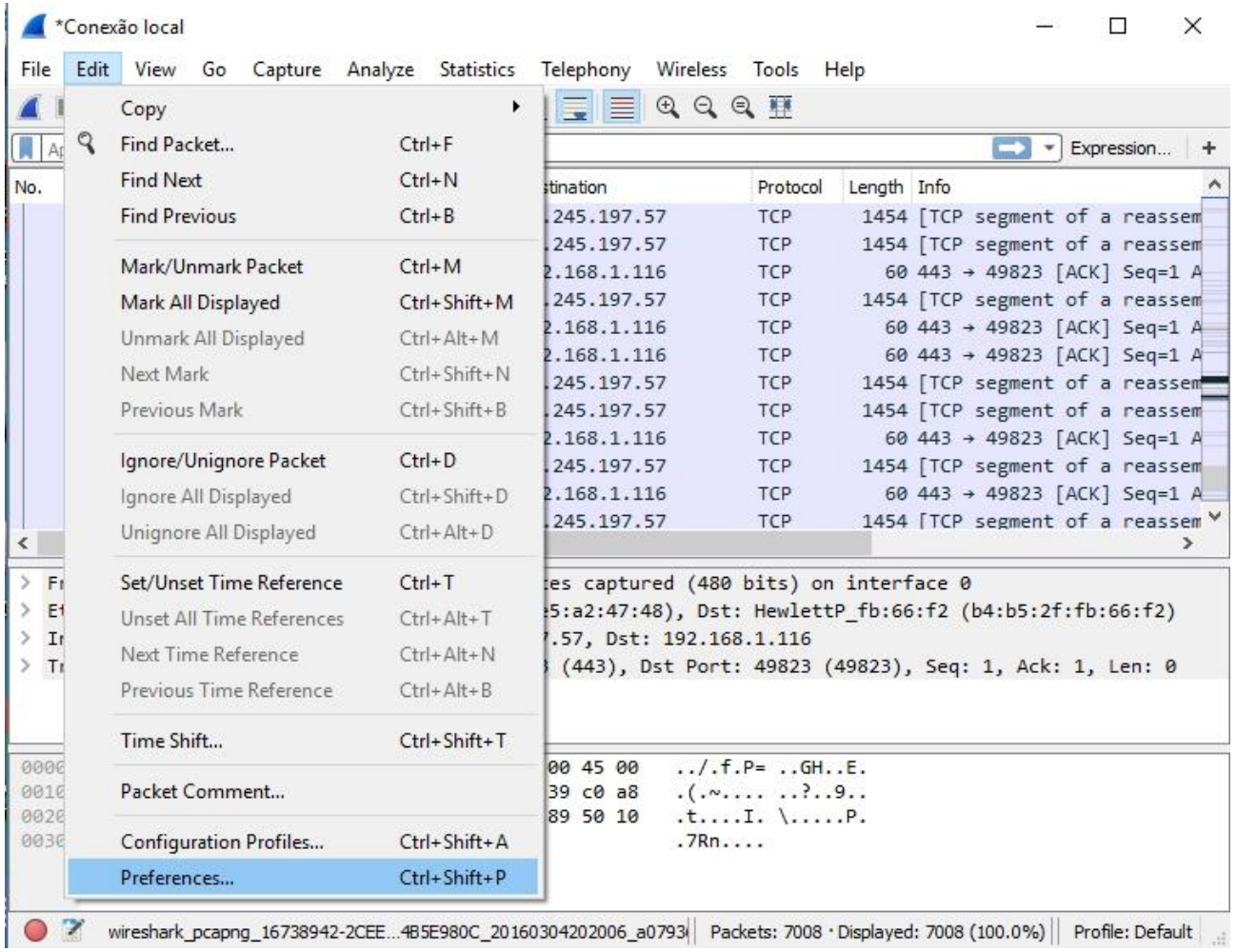

Wireshark 2.0.2 (64-bit) Setup
Completing the Wireshark 2.0.2 (64-bit) Setup Wizard
Your computer must be restarted in order to complete the installation of Wireshark 2.0.2 (64-bit). Do you want to reboot now?
Reboot now
I want to manually reboot later
< Back
Finish
Cancel

Instalação


The Wireshark Network Analyzer
File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help
Apply a display filter ... <Ctrl-/>
Expression...
Welcome to Wireshark
Capture
...using this filter:
Enter a capture filter ...
Conexão Local* 4
Conexão de Rede sem Fio
Conexão de Rede Bluetooth
Conexão Local* 2
Conexão local
Learn
User's Guide · Wiki · Questions and Answers · Mailing Lists
You are running Wireshark 2.0.2 (v2.0.2-0-ga16e22e from master-2.0). You receive automatic updates.
Ready to load or capture
No Packets
Profile: Default

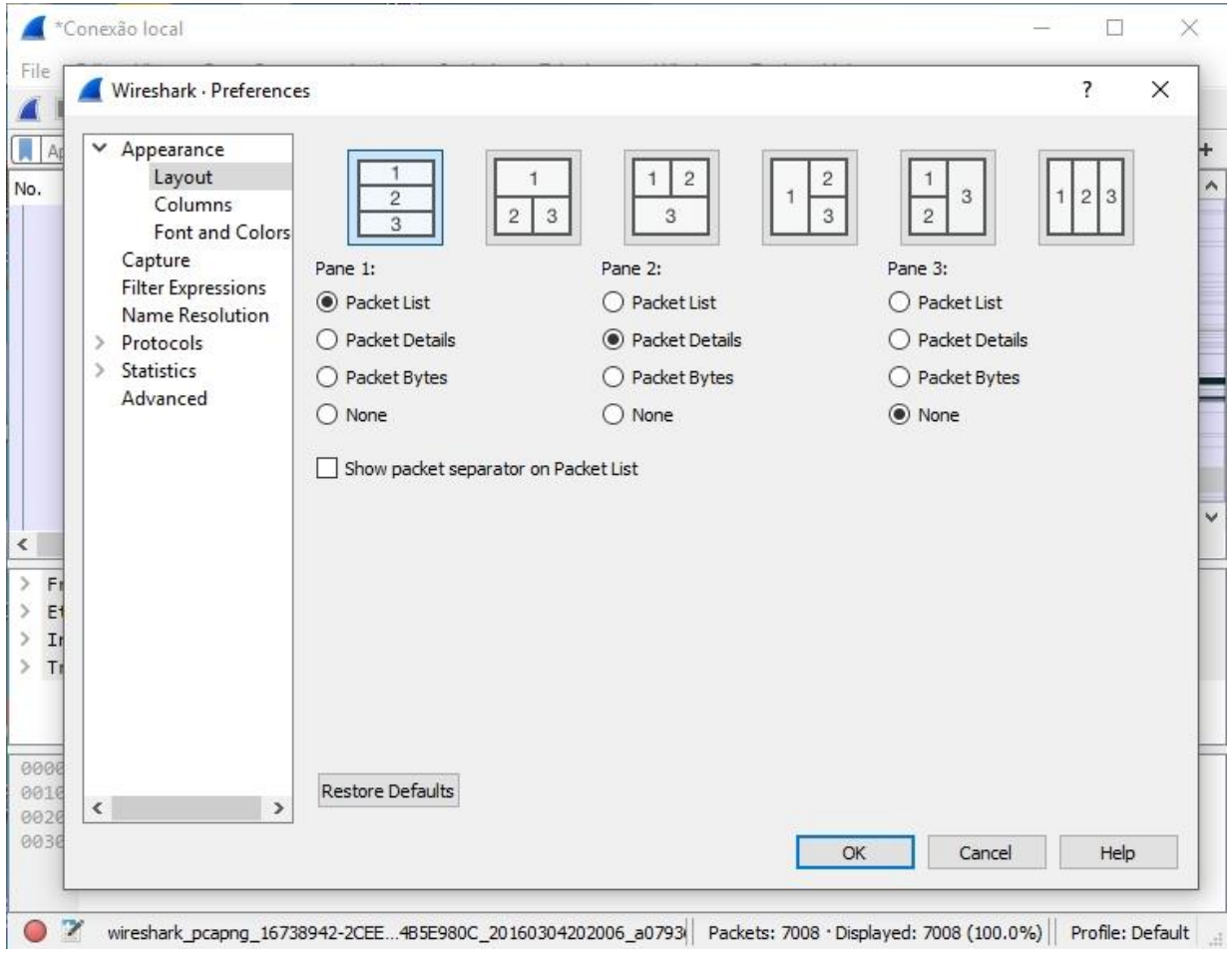
Customização

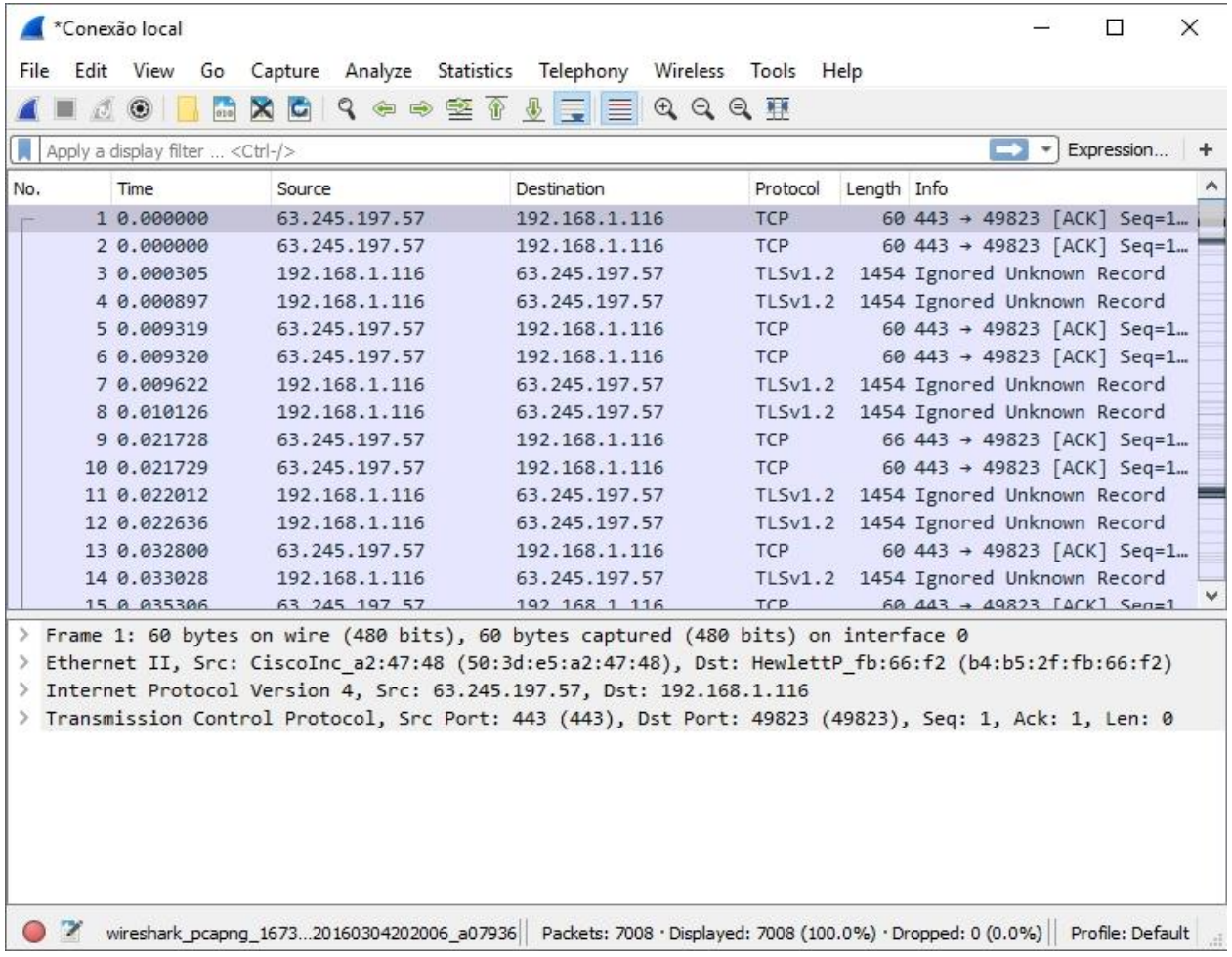




UNICARIOCA 25 anos
Centro Universitário

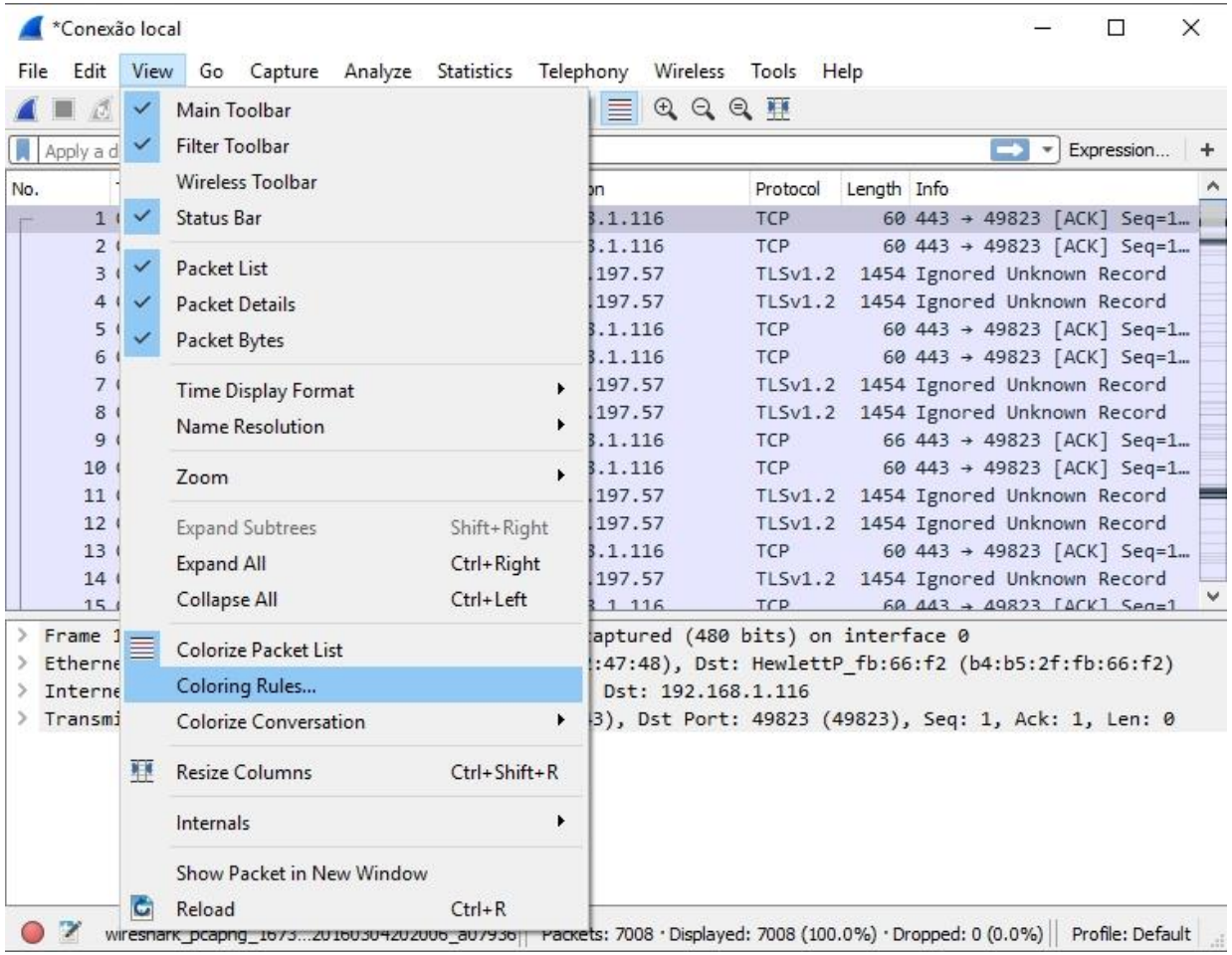
Customização

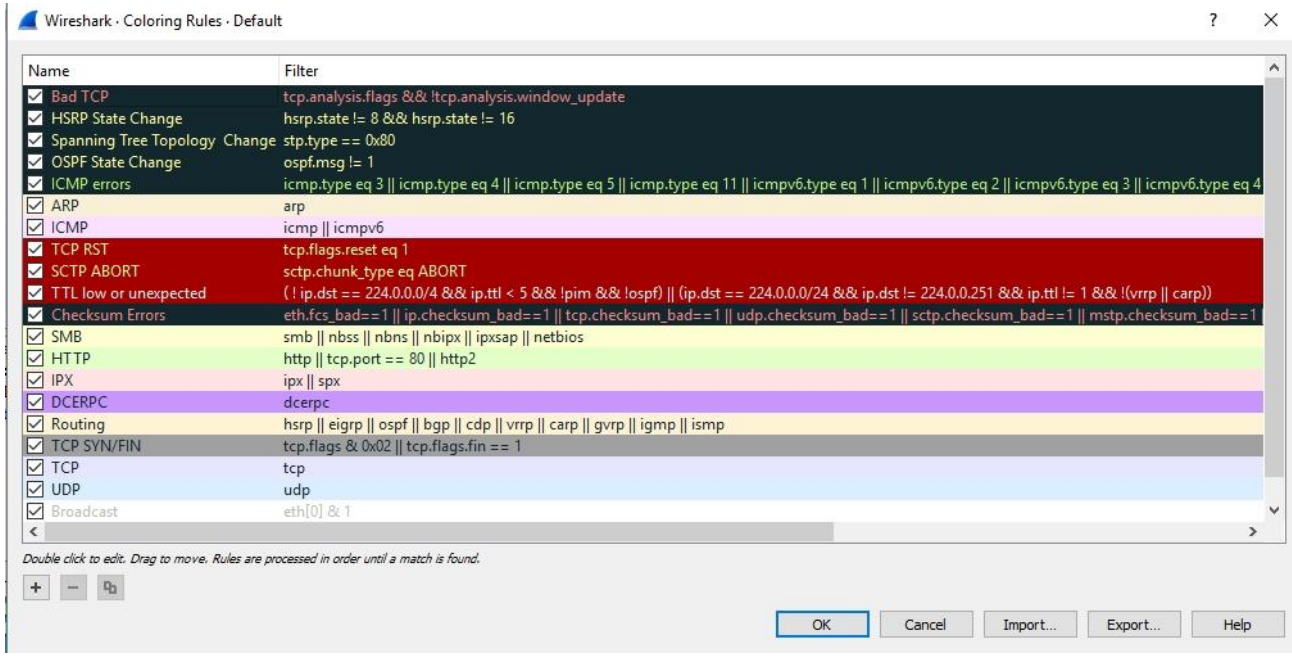




UNICARIOCA 25 anos
Centro Universitário

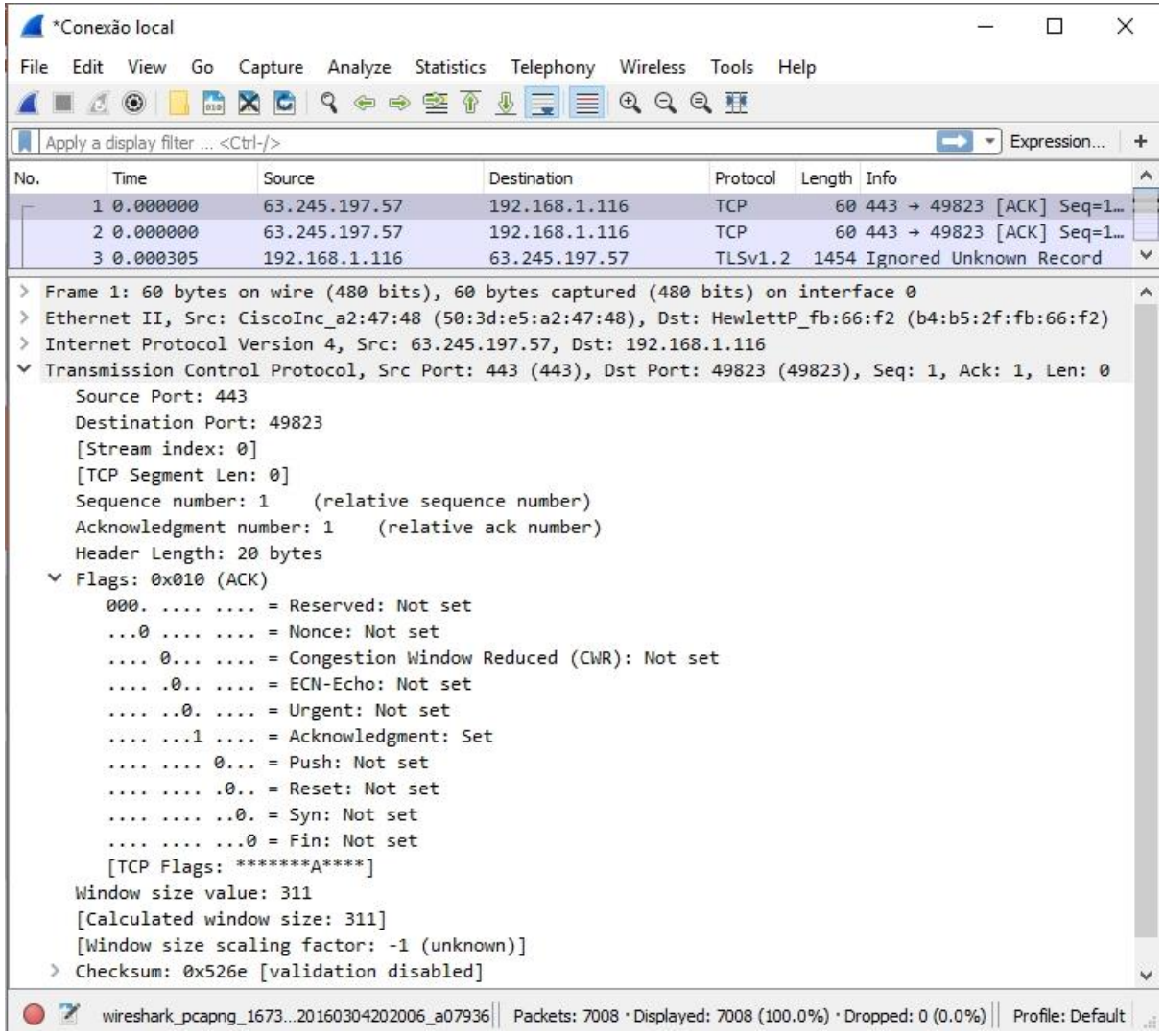
Customização



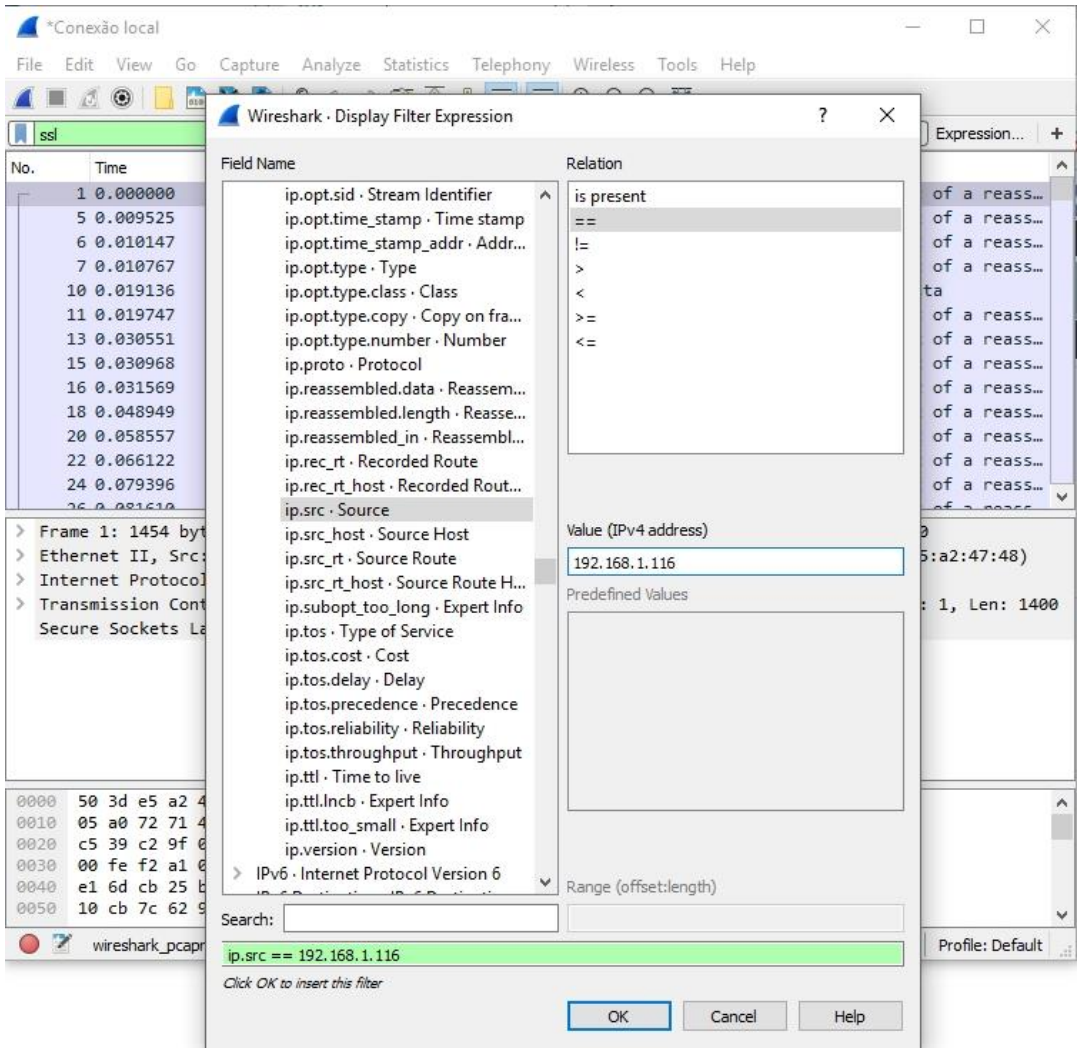


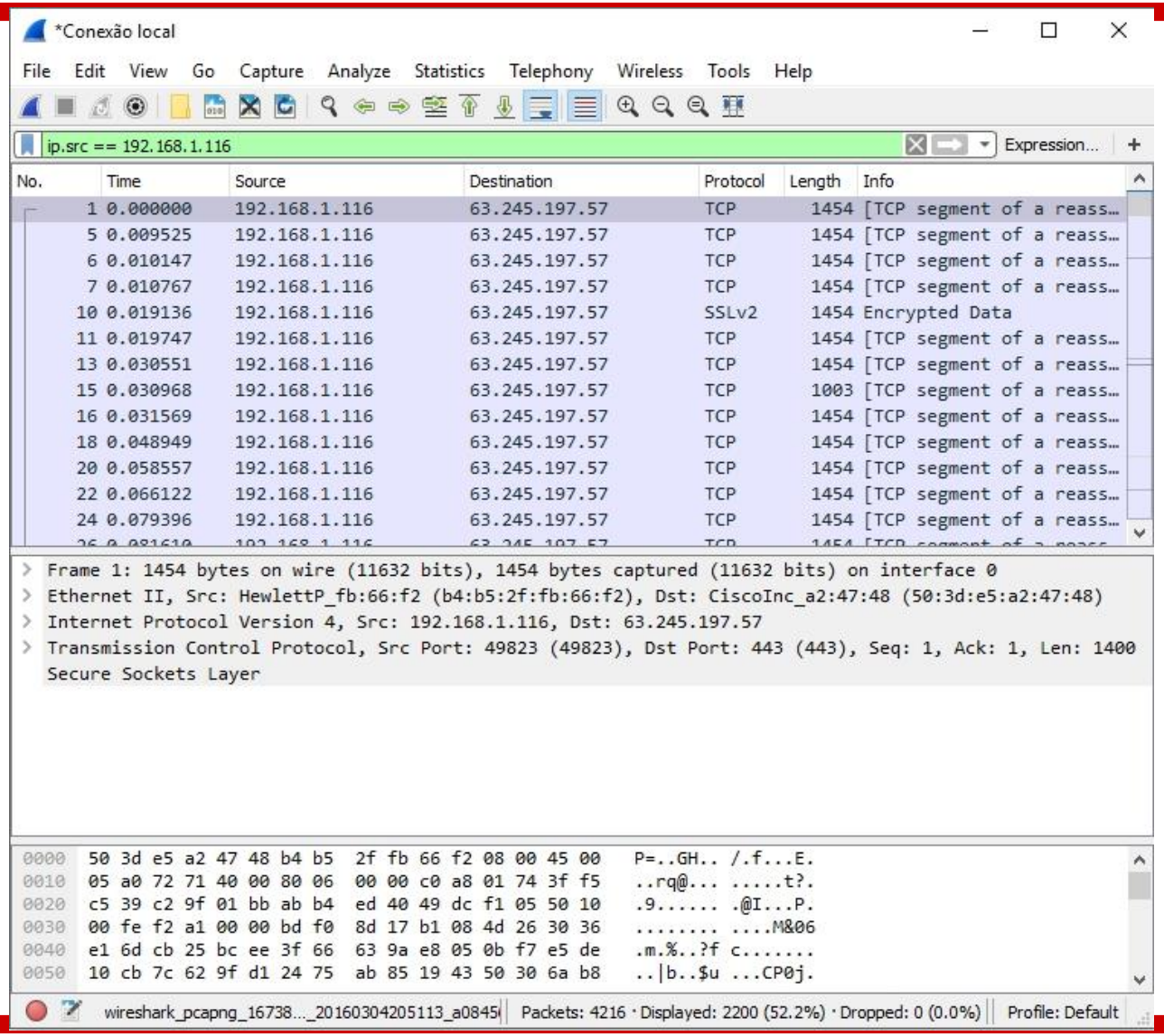
UNICARIOCA 25 anos
Centro Universitário

Uso do Wireshark

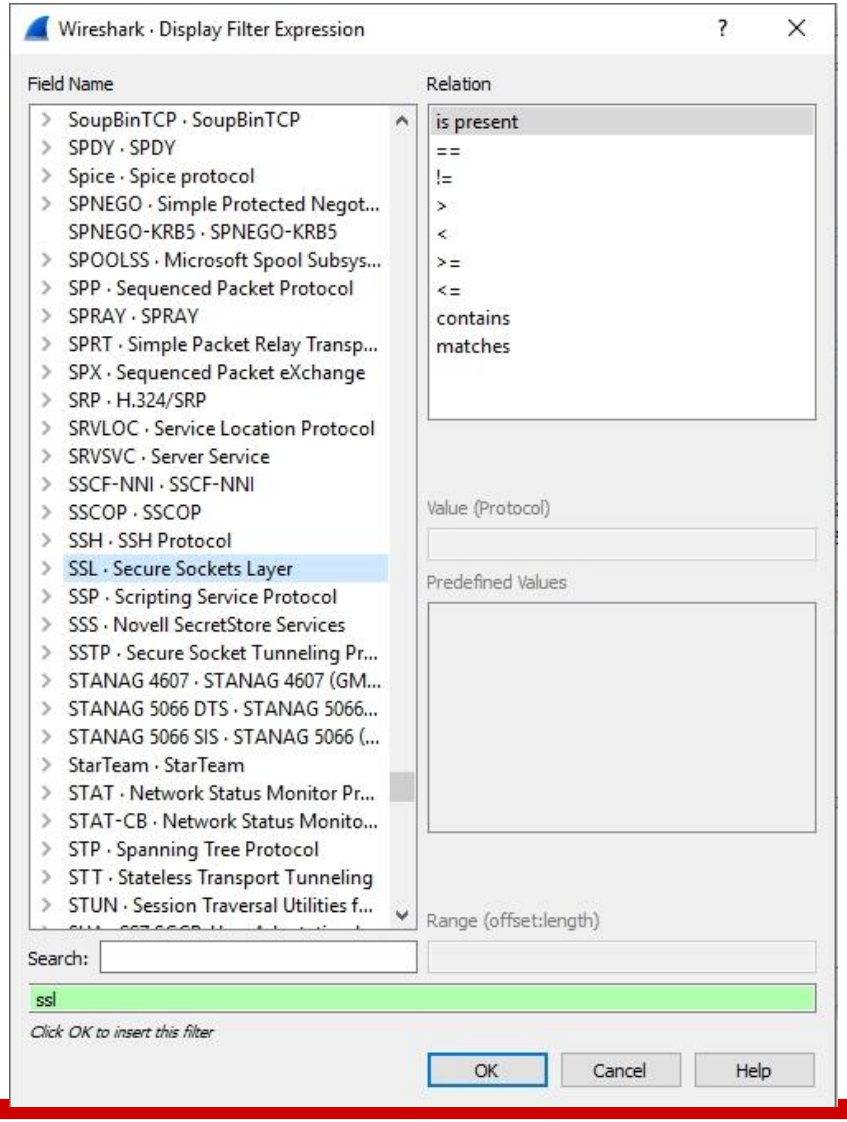


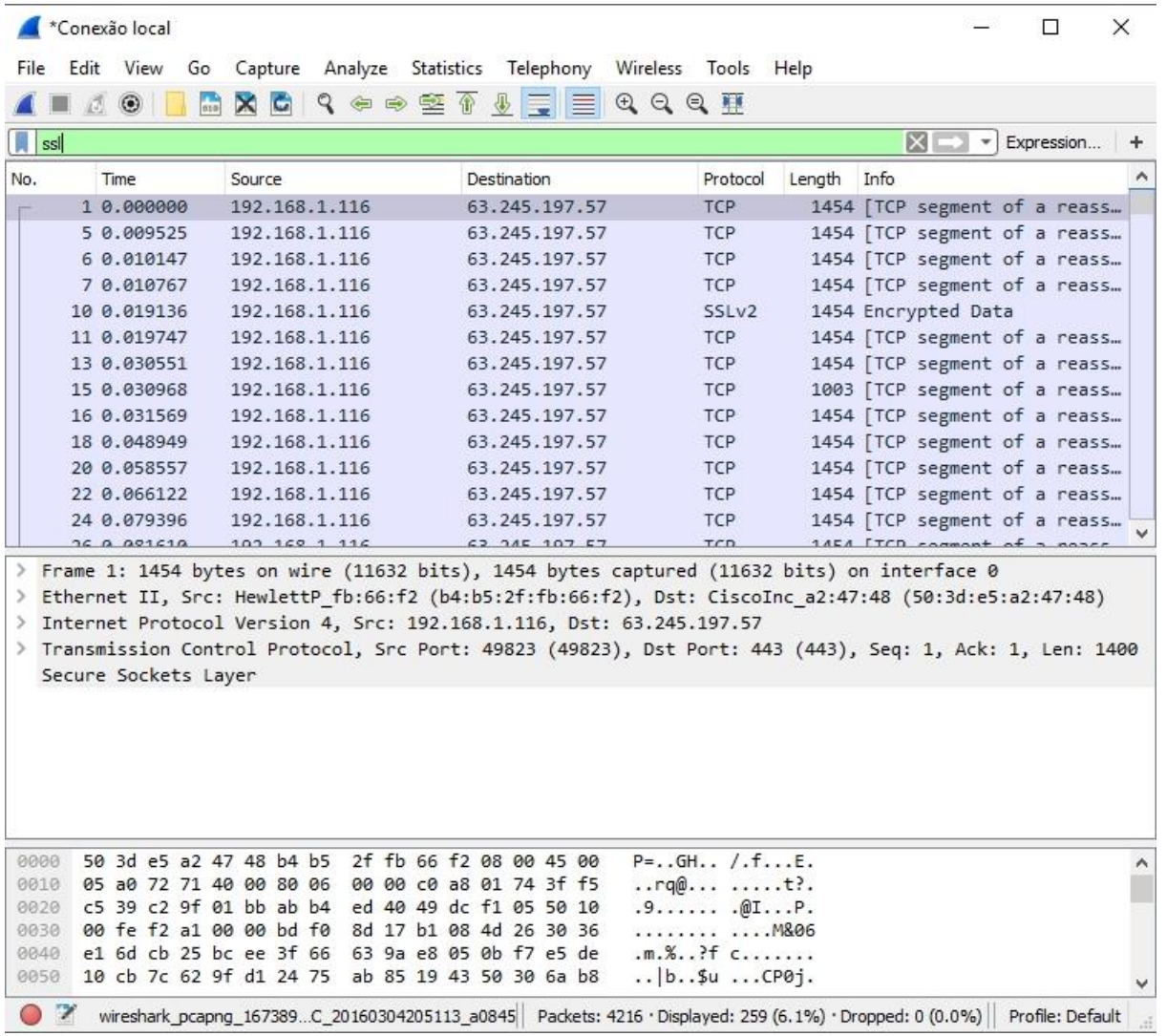
Filtros: Display



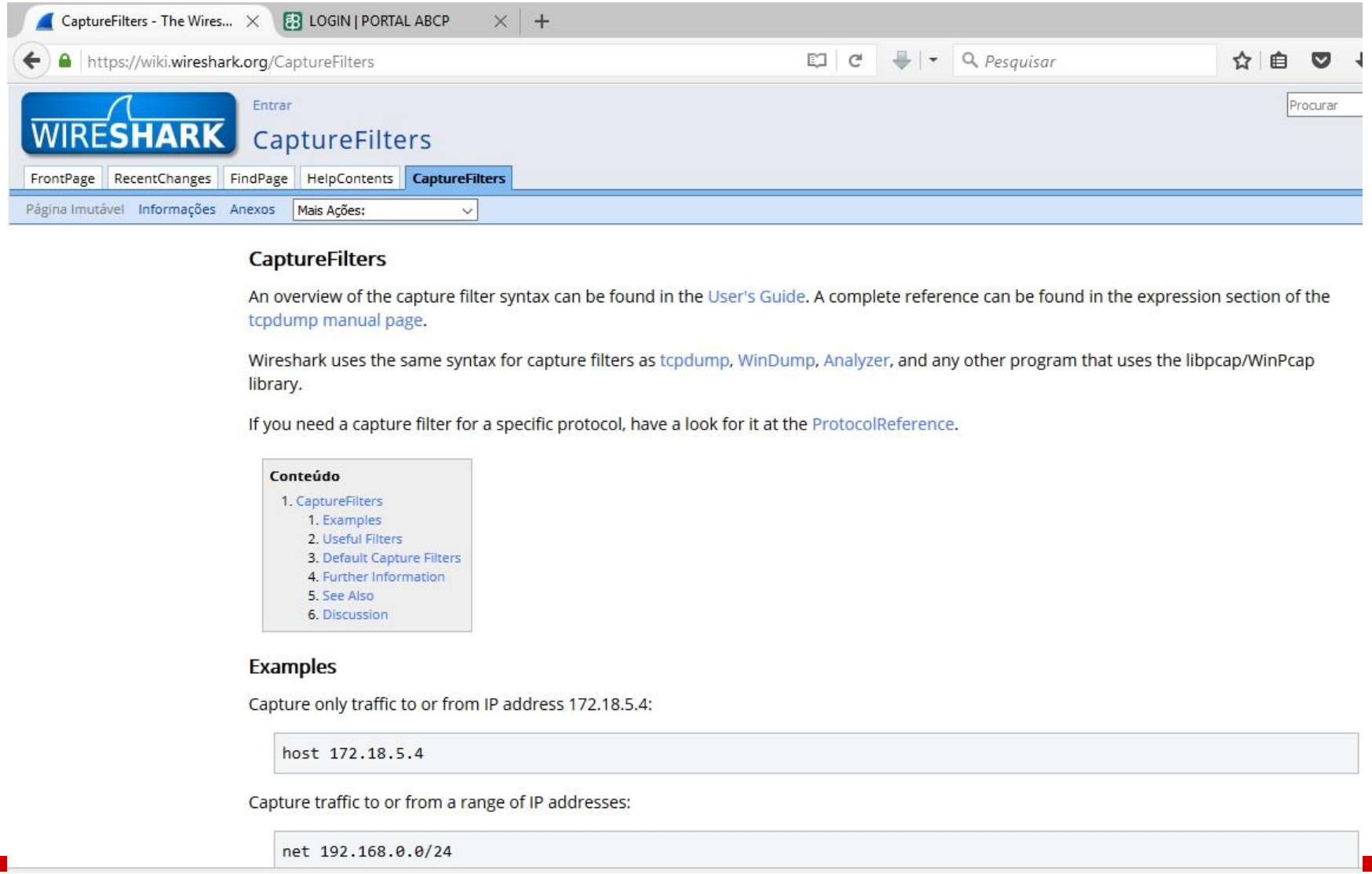


Filtros: Display

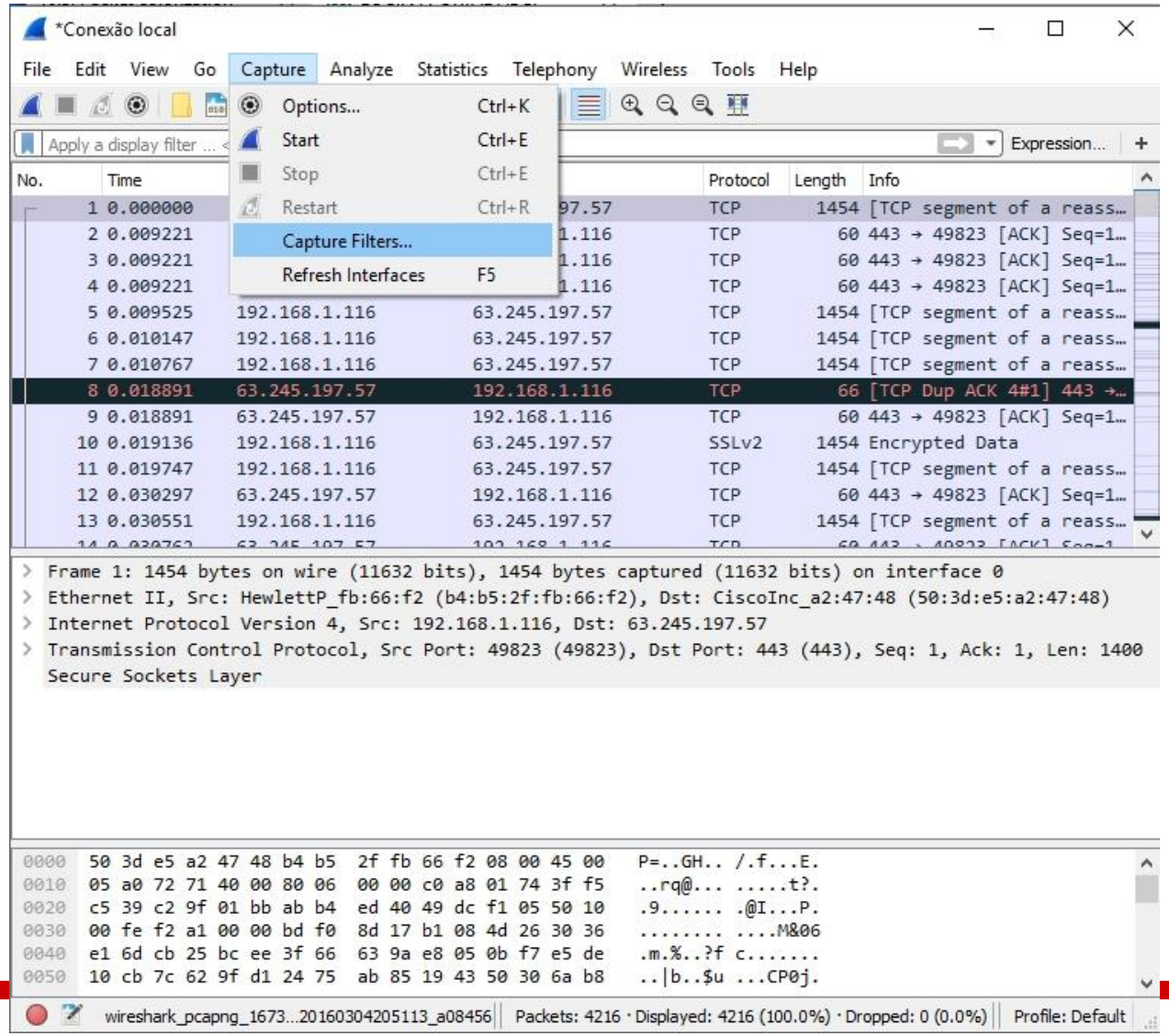


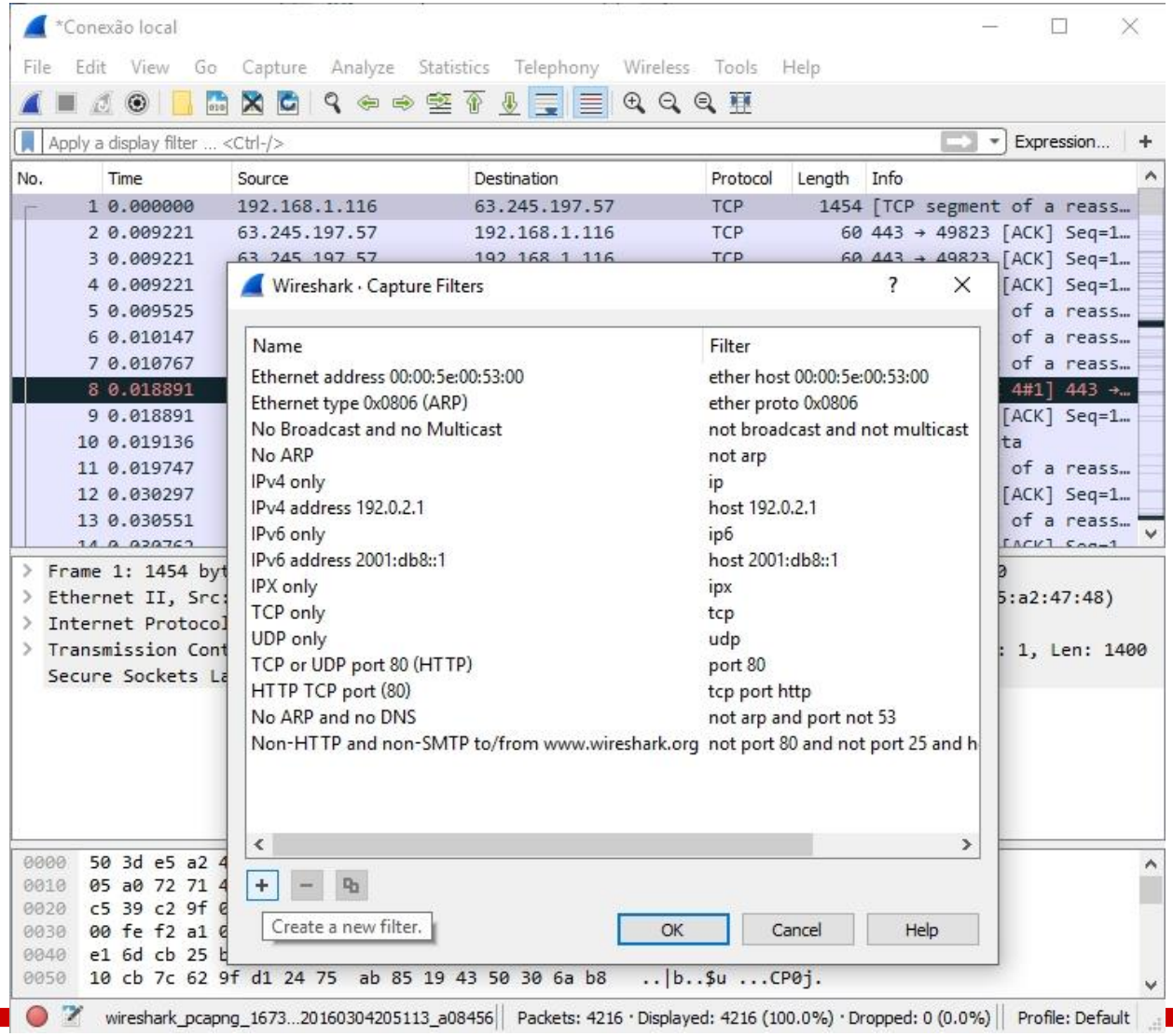


Filtros: Captura

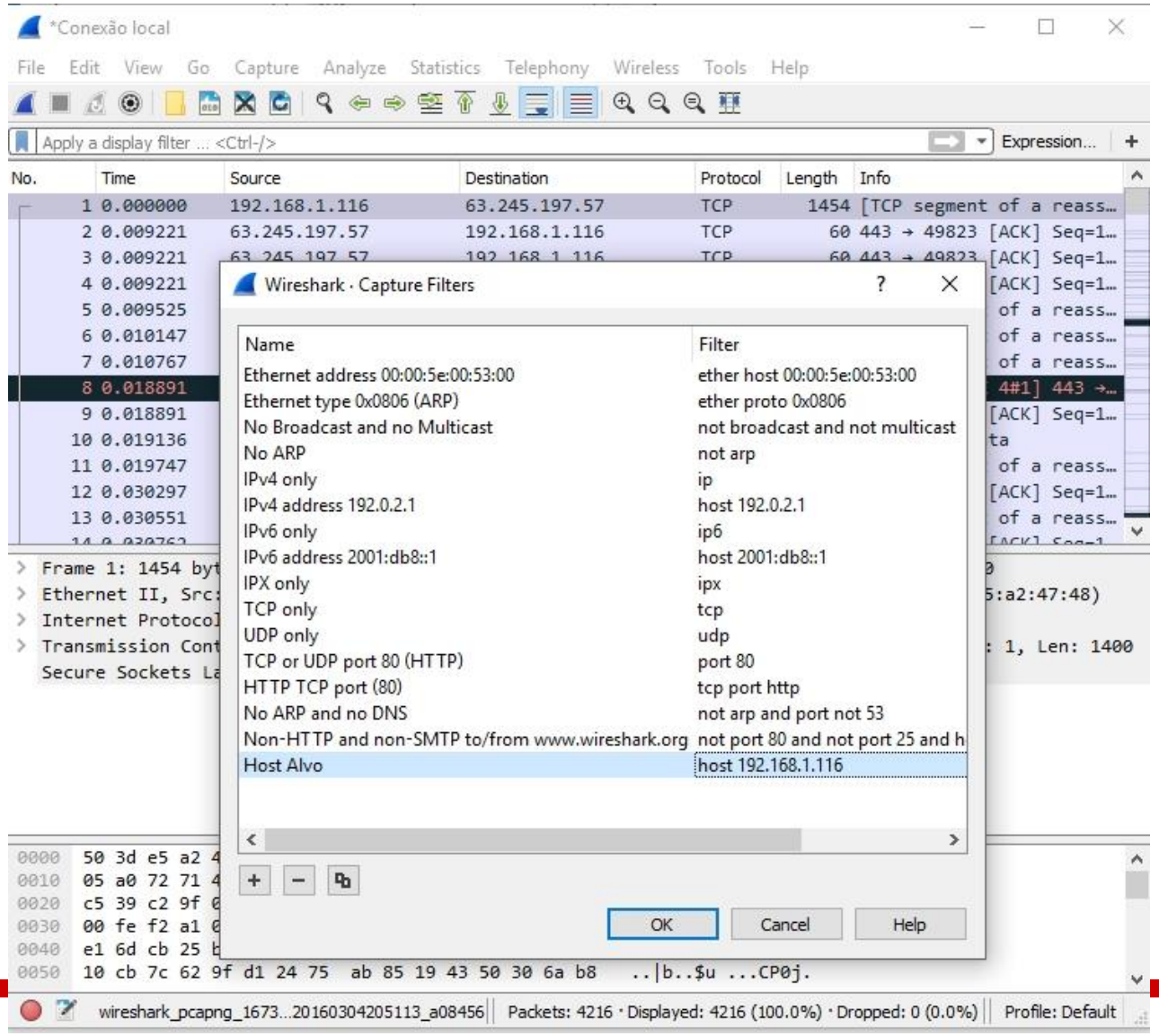


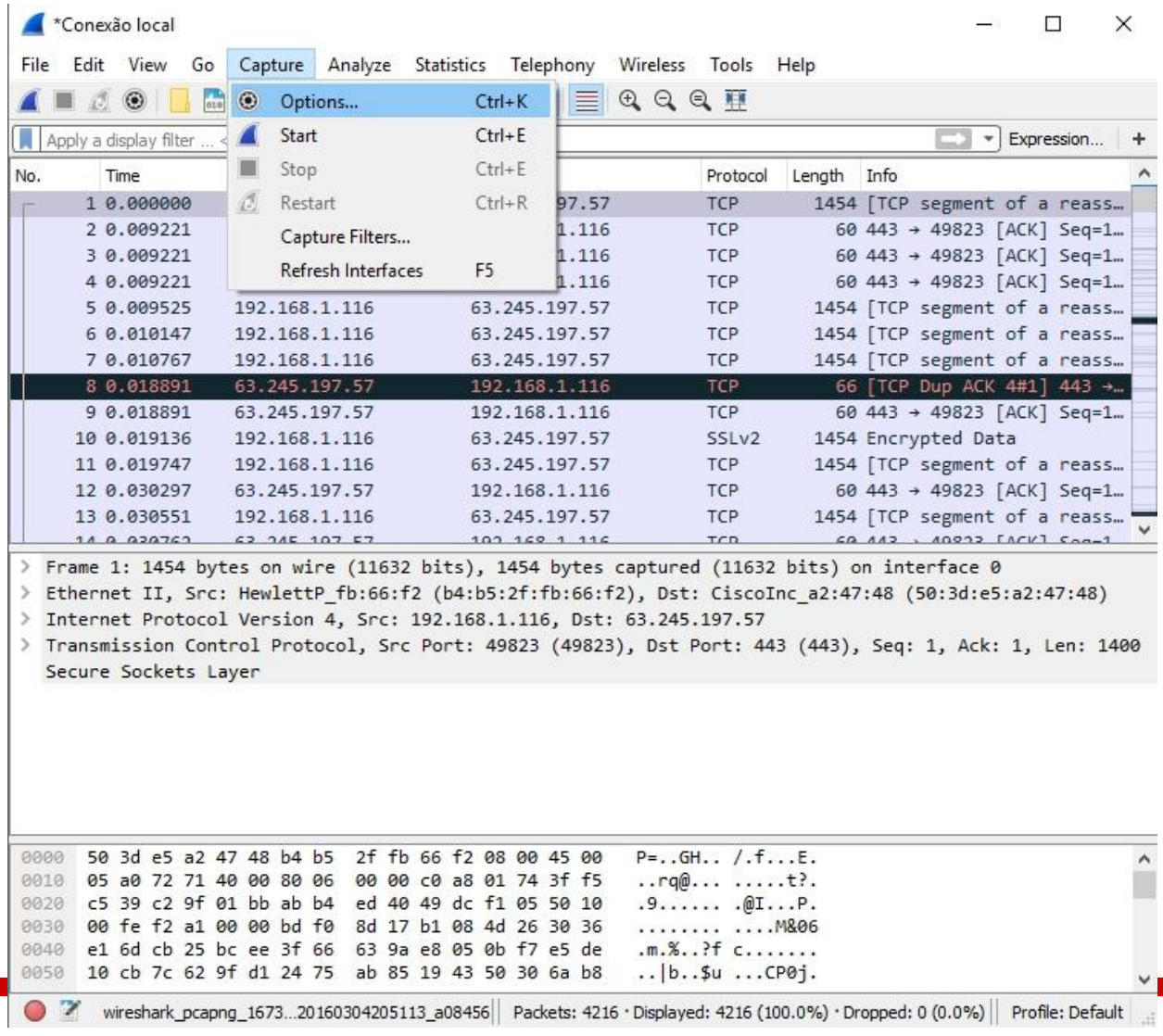
Filtros: Captura



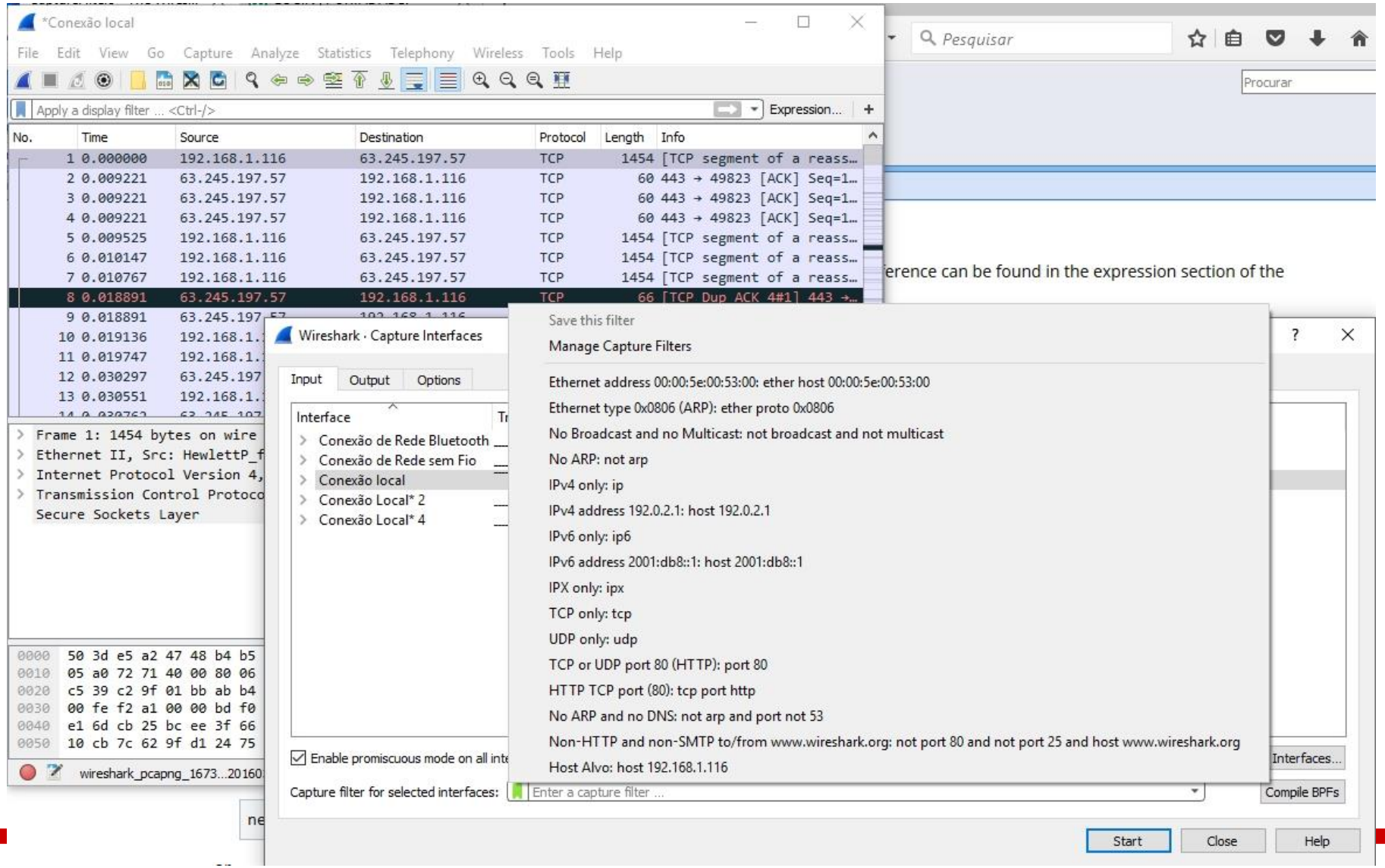


Filtros: Captura

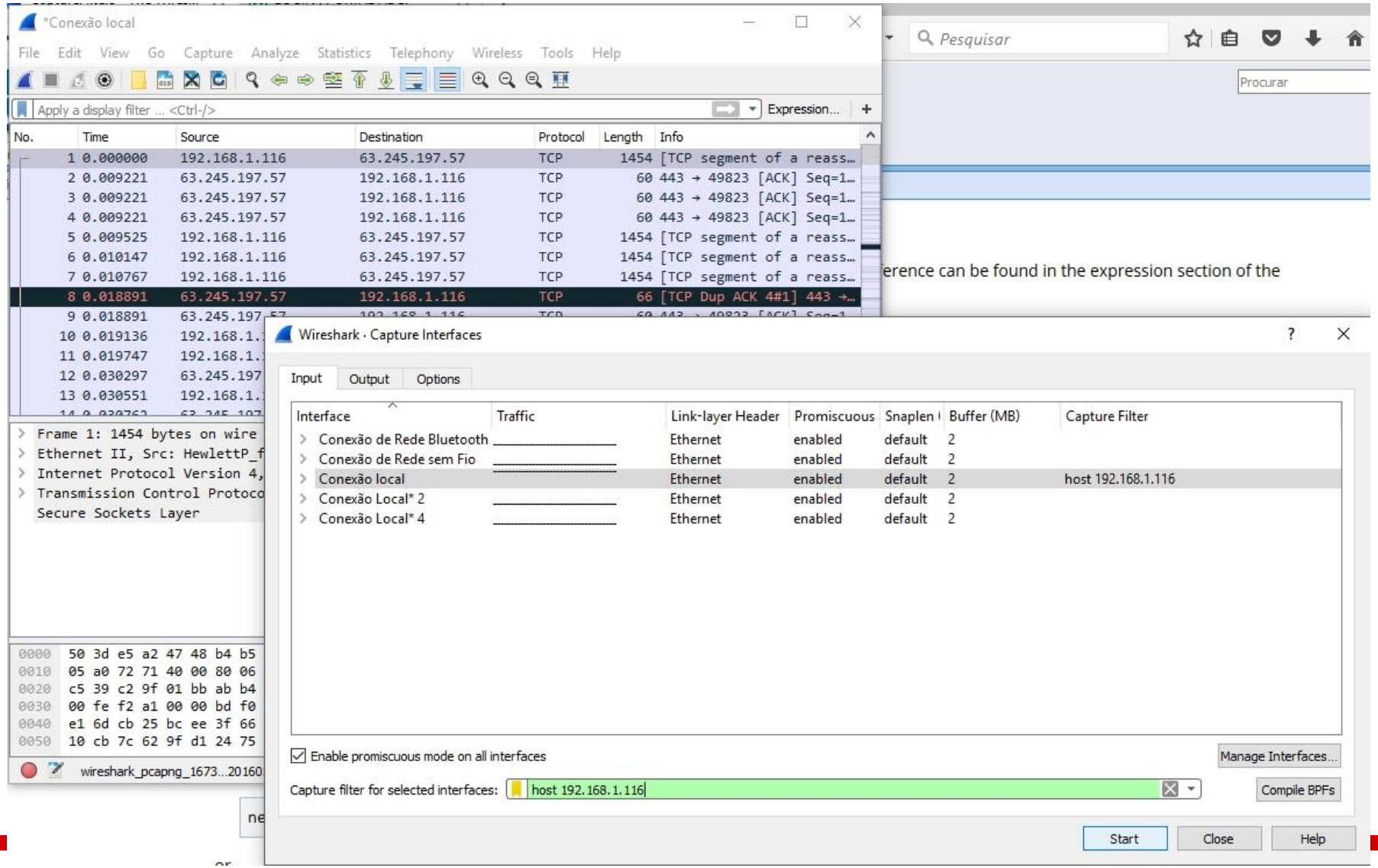




Filtros: Captura

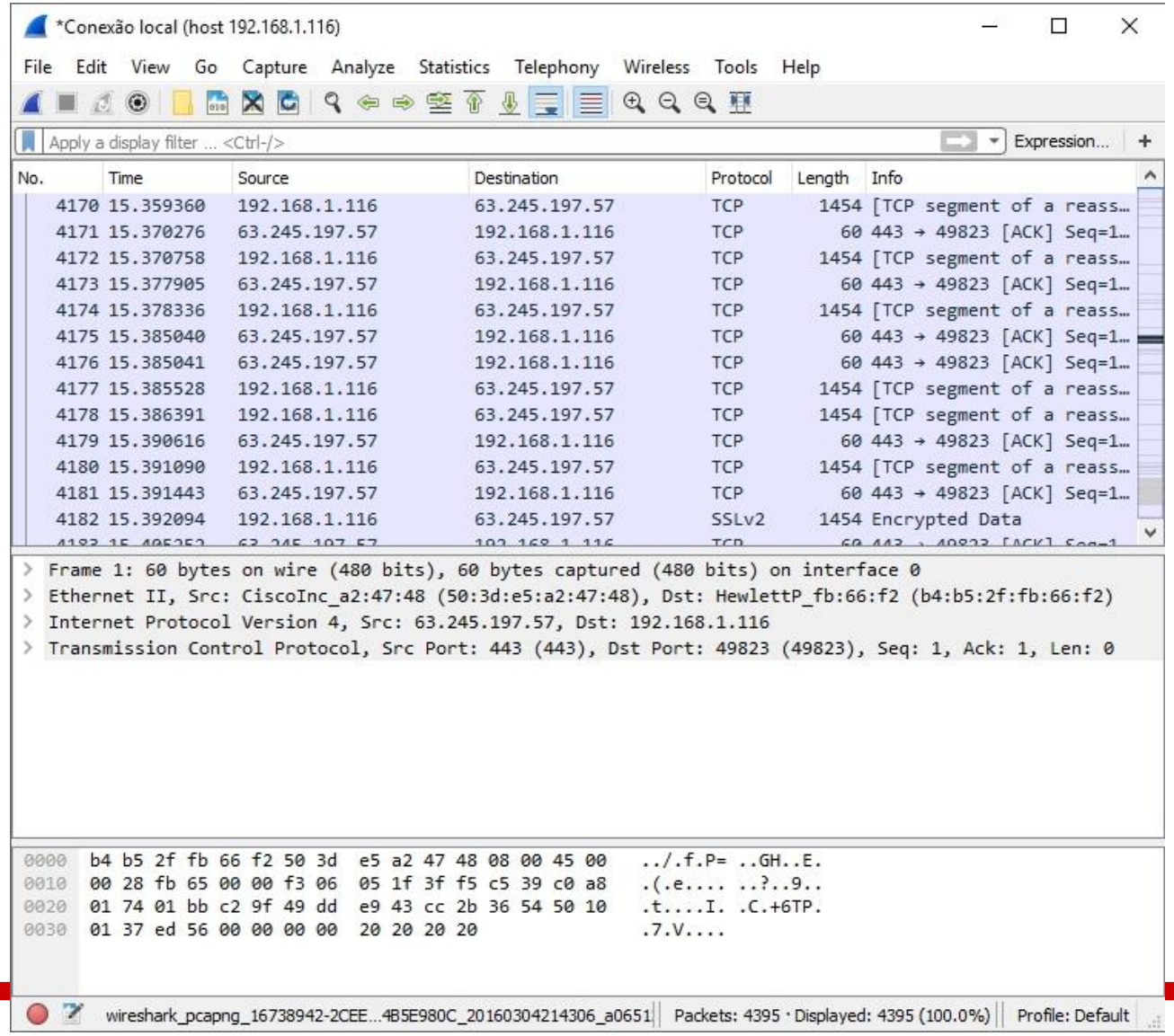


Filtros: Captura

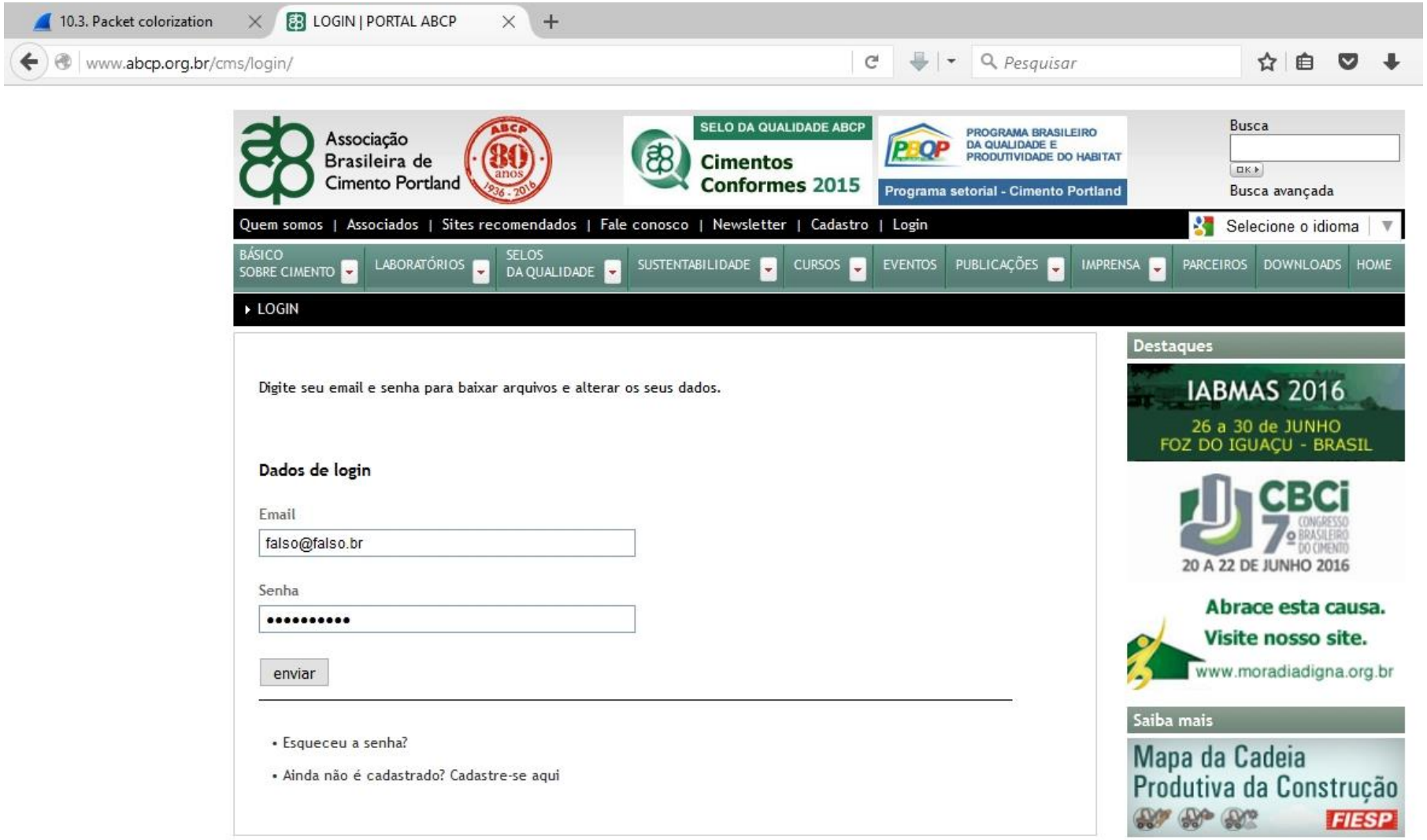


UNICARIOCA 25 anos
Centro Universitário

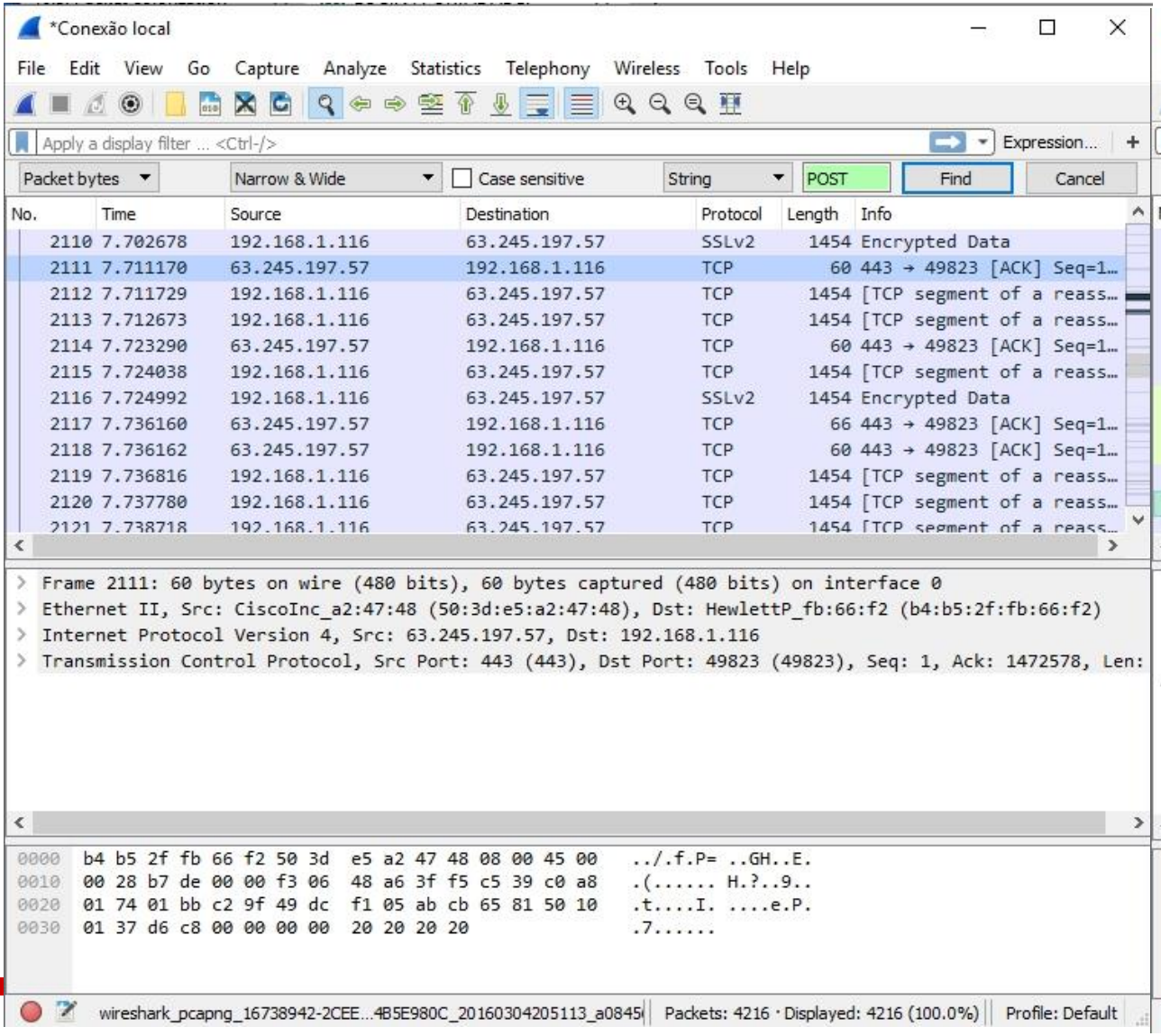
Filtros: Captura

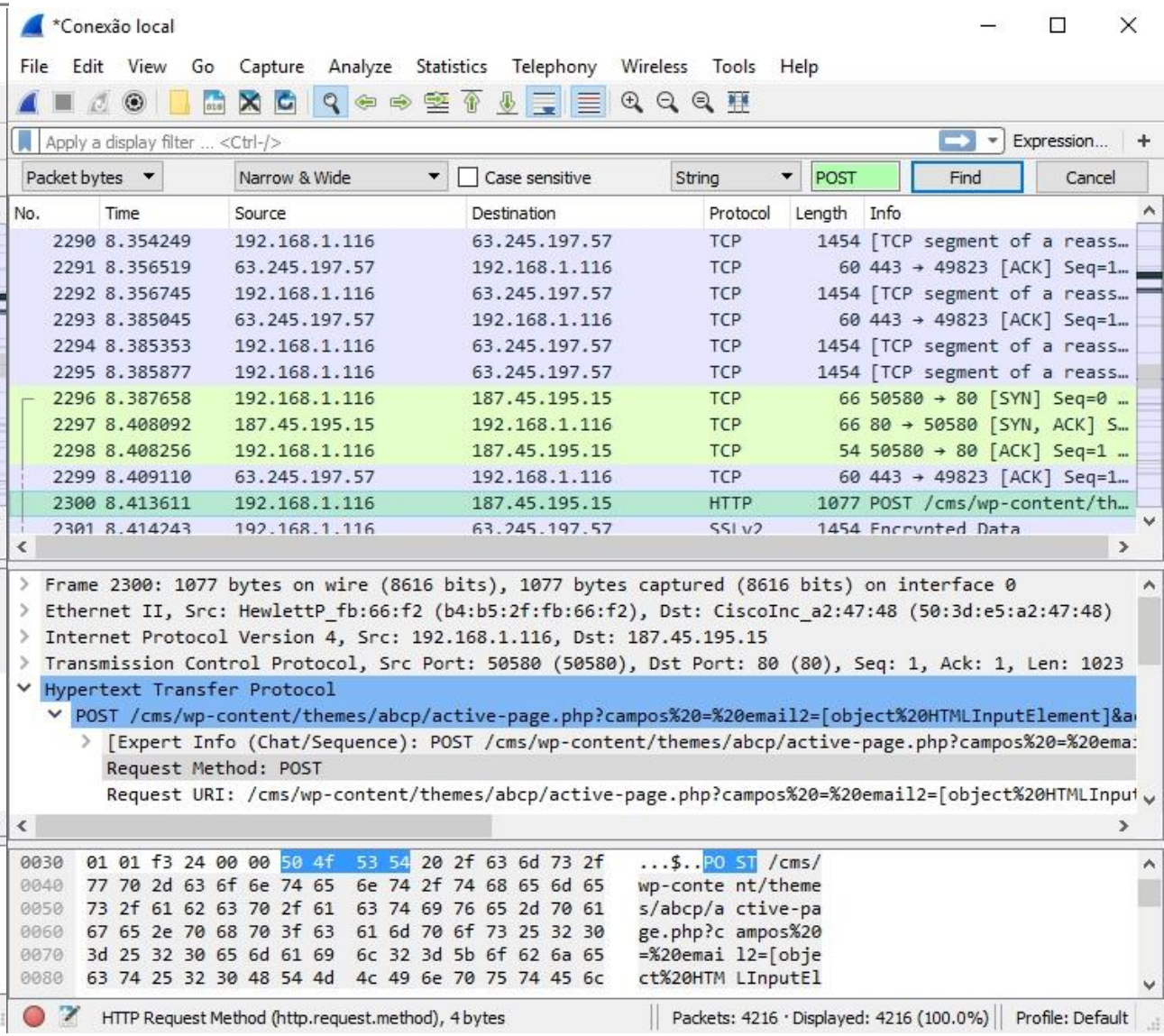


Outras Funcionalidades Interessantes

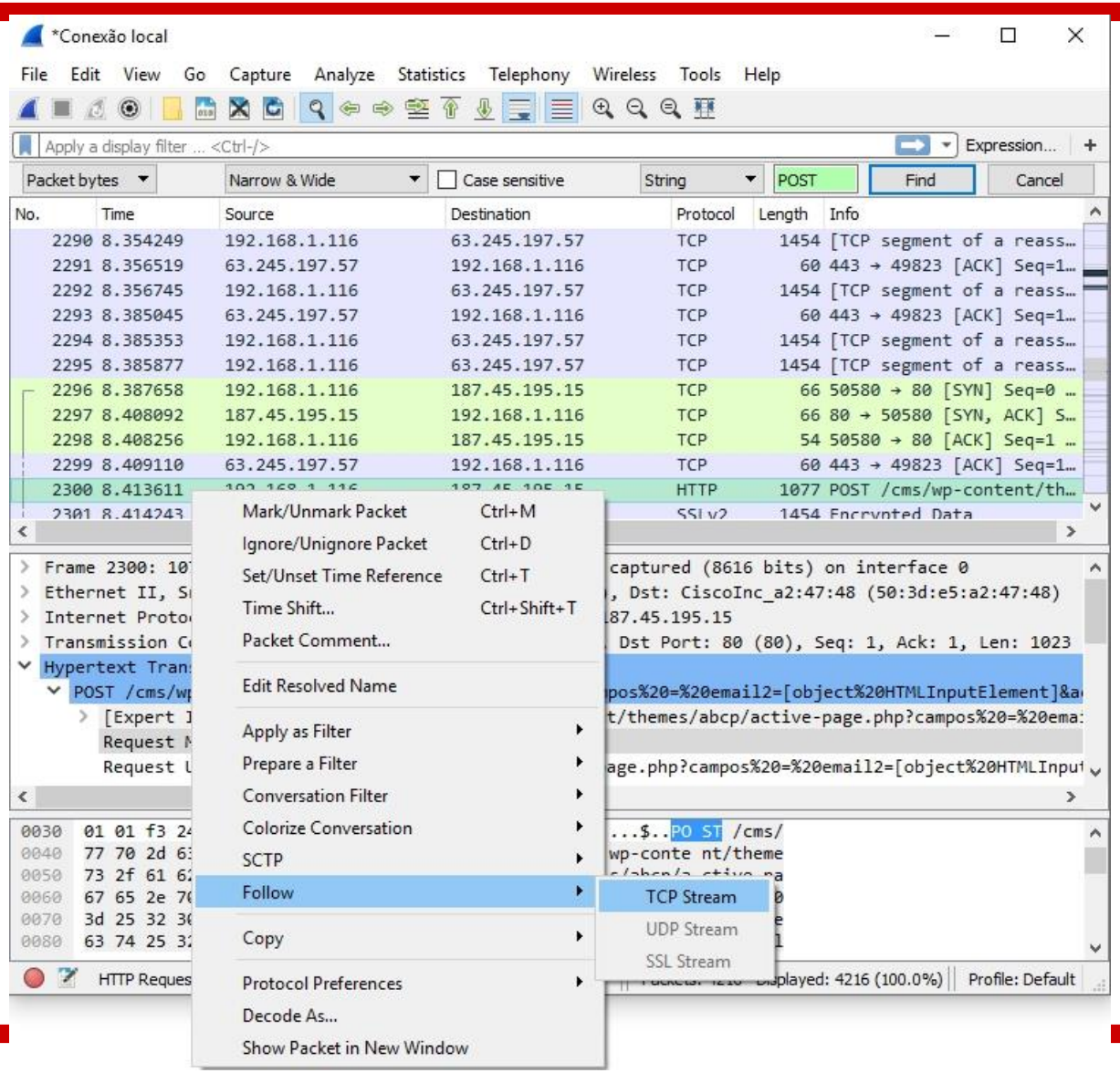


Outras Funcionalidades Interessantes





Outras Funcionalidades Interessantes



Outras funções importantes

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