FTP- authentification

📋 Énoncé du challenge

> 🎯 Un échange authentifié de fichier réalisé grâce au protocole FTP. Retrouvez le mot de passe utilisé par l'utilisateur.

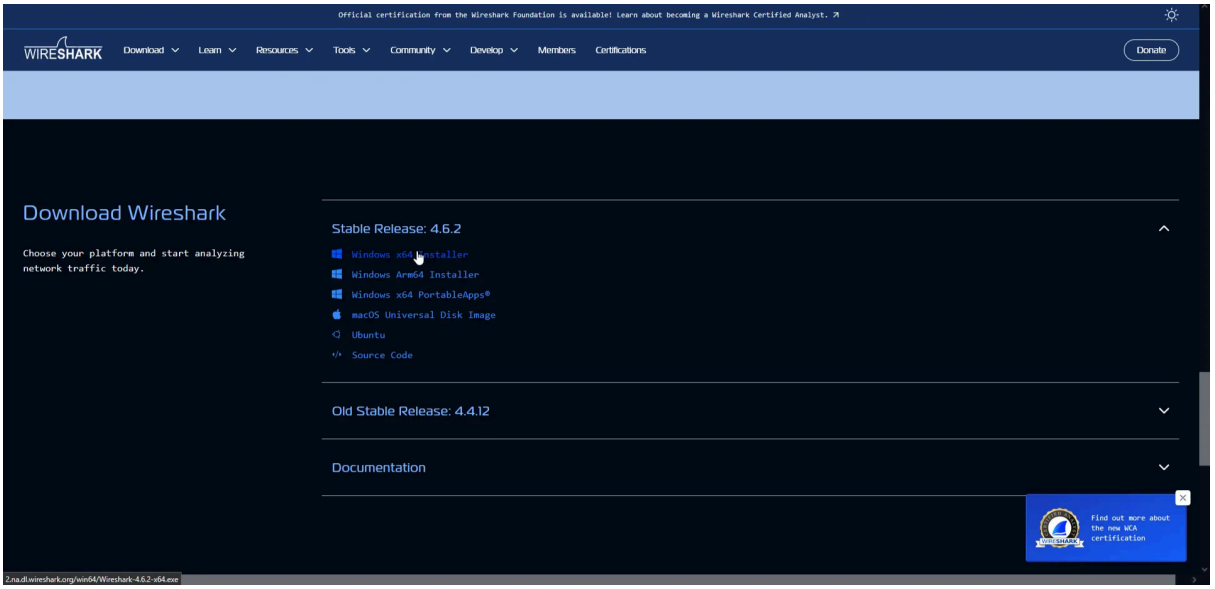
📦 Fichiers fournis

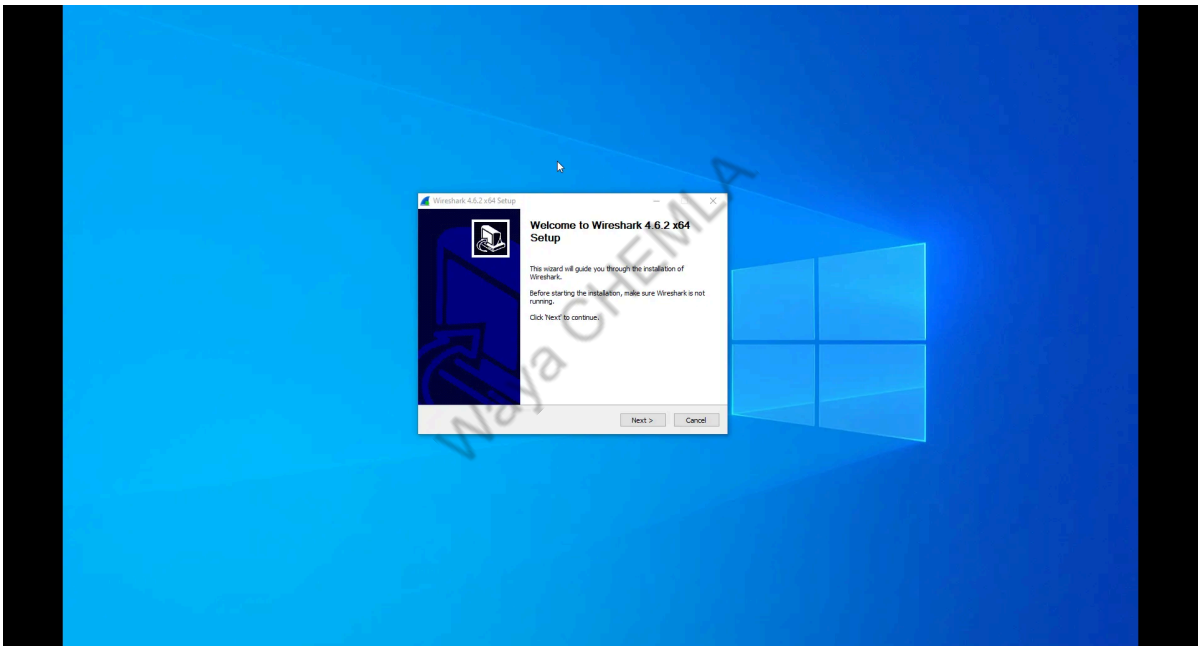
ch1.pcap

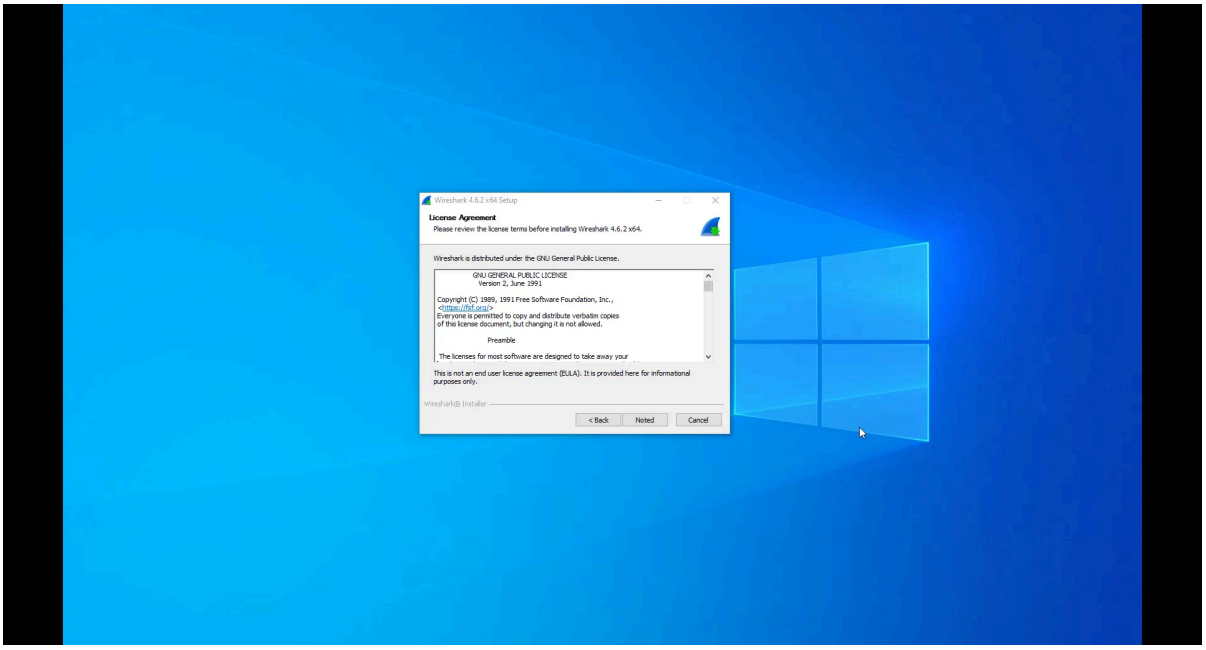
Ressource

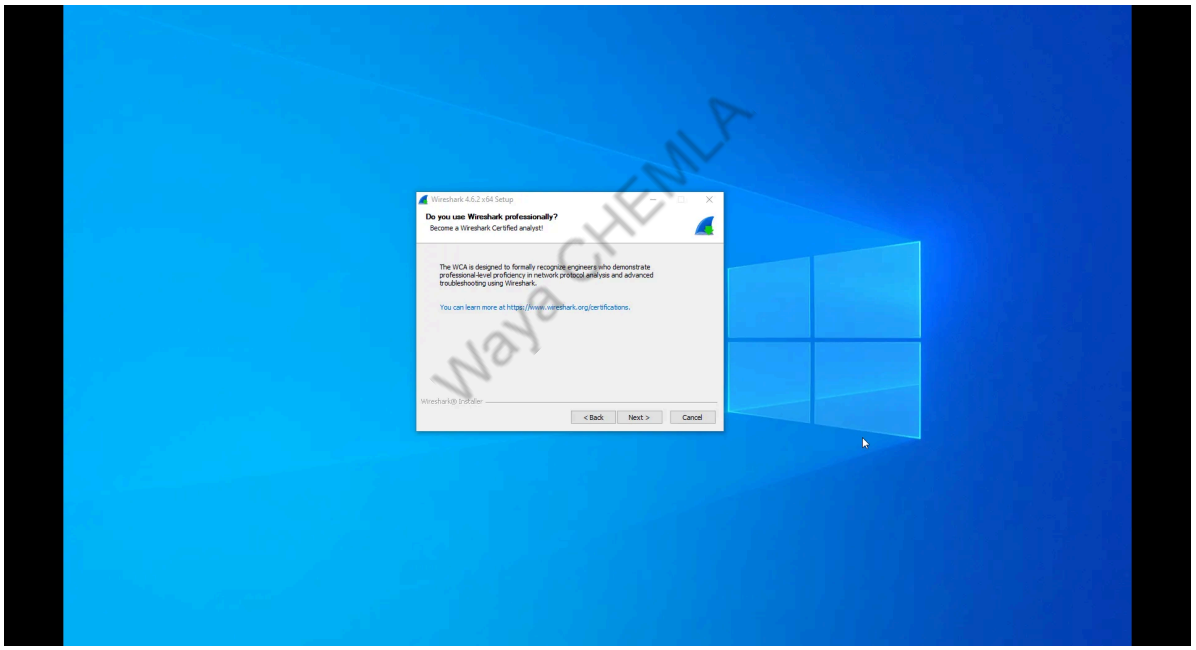
🔧 Étape 1 : Installation de Wireshark

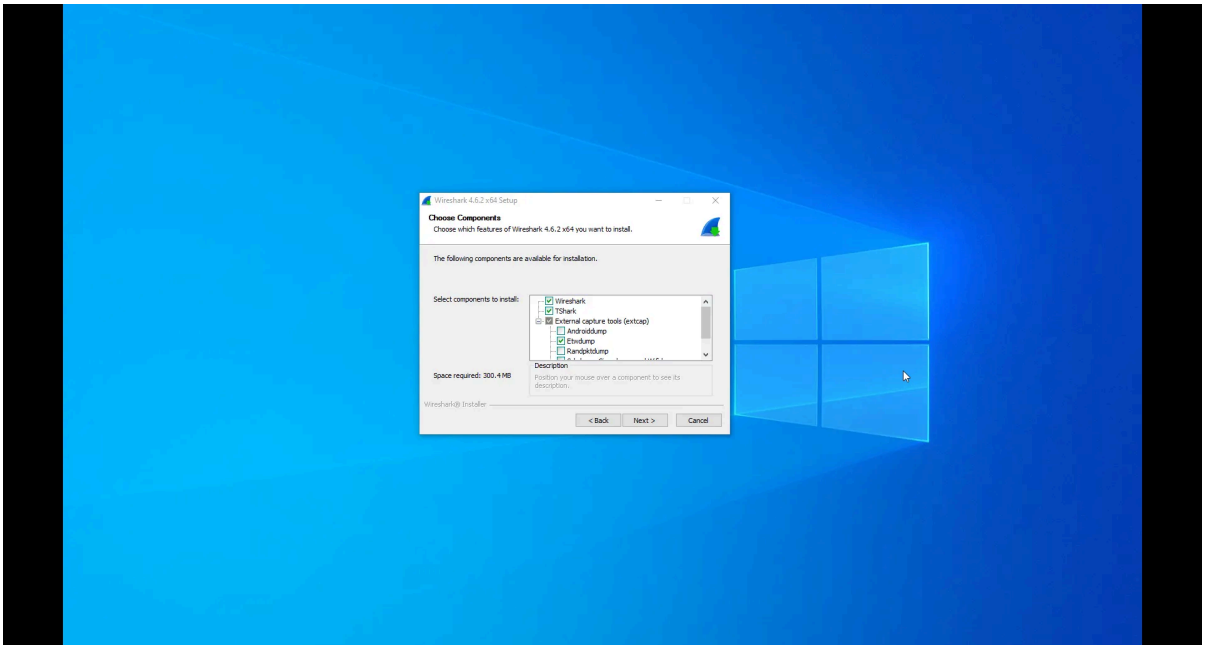
Pour analyser le fichier de capture réseau (.pcap), j'ai installé **Wireshark**, un outil d'analyse de protocoles réseau.

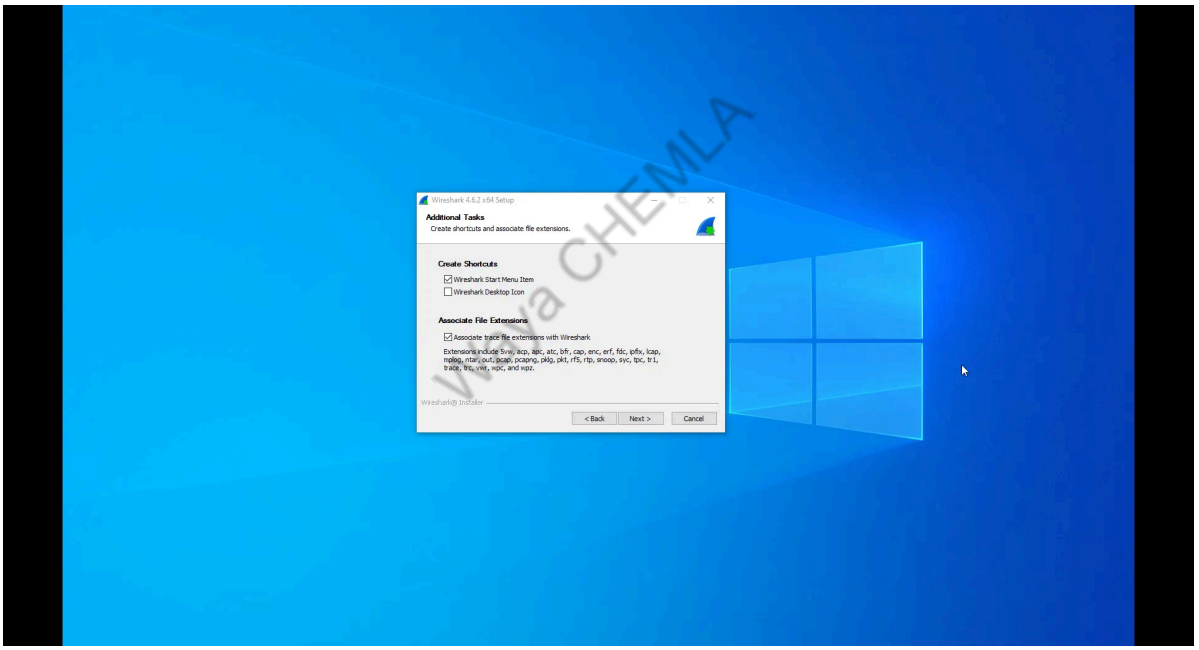

Official certification from the Wireshark Foundation is available! Learn about becoming a Wireshark Certified Analyst.
WIRESHARK
Download
Learn
Resources
Tools
Community
Develop
Members
Certifications
Donate
Download Wireshark
Choose your platform and start analyzing network traffic today.
Stable Release: 4.6.2
Windows x64 Installer
Windows Arm64 Installer
Windows x64 PortableApps®
macOS Universal Disk Image
Ubuntu
Source Code
Old Stable Release: 4.4.12
Documentation
Find out more about the new WCA certification
2.na.dl.wireshark.org/win64/Wireshark-4.6.2-x64.exe

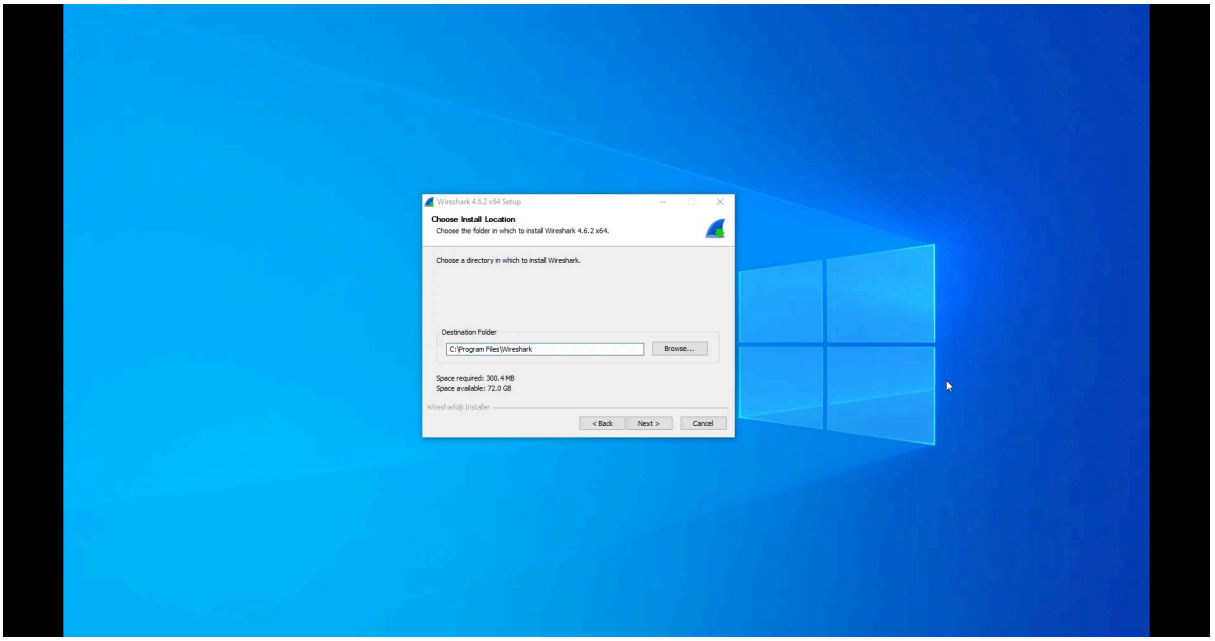

Wireshark 4.6.2 x64 Setup
Welcome to Wireshark 4.6.2 x64 Setup
This wizard will guide you through the installation of Wireshark.
Before starting the installation, make sure Wireshark is not running.
Click Next to continue.
Next >
Cancel

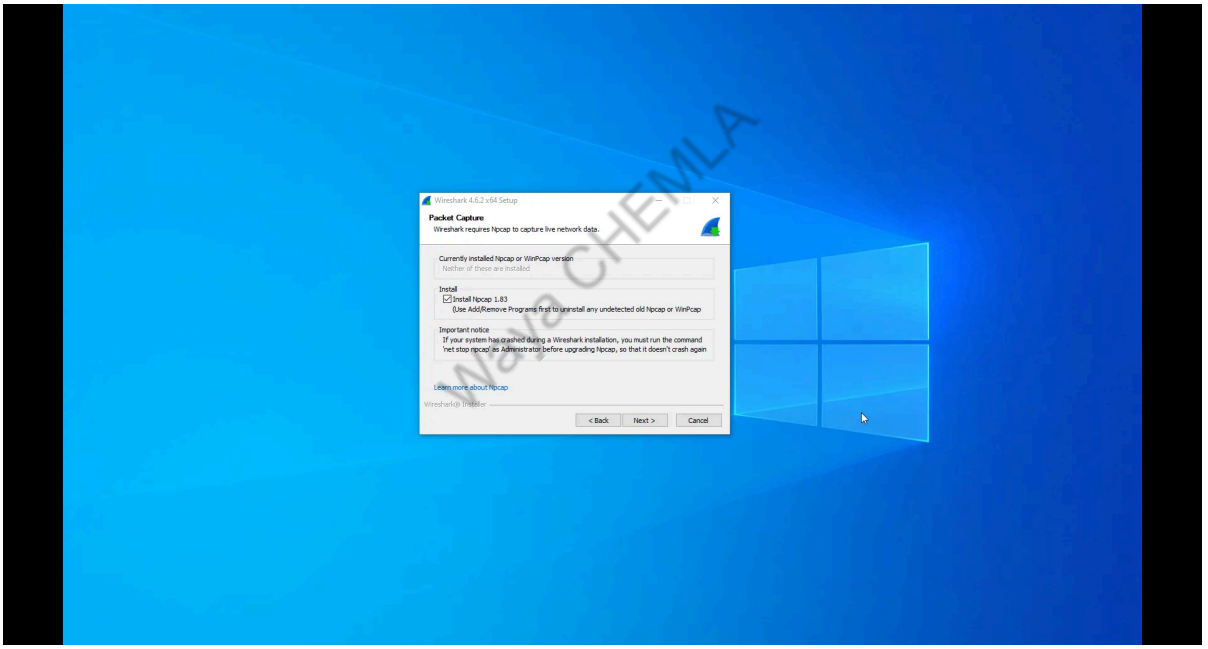

Wireshark 4.6.2 x64 Setup
License Agreement
Please review the license terms before installing Wireshark 4.6.2 x64.
Wireshark is distributed under the GNU General Public License.
GNU GENERAL PUBLIC LICENSE
Version 2, June 1991
Copyright (C) 1989, 1991 Free Software Foundation, Inc.,
<https://fsf.org/>
Everyone is permitted to copy and distribute verbatim copies
of this license document, but changing it is not allowed.
Preamble
The licenses for most software are designed to take away your
This is not an end user license agreement (EULA). It is provided here for informational purposes only.
Wireshark® Installer
< Back
Noted
Cancel

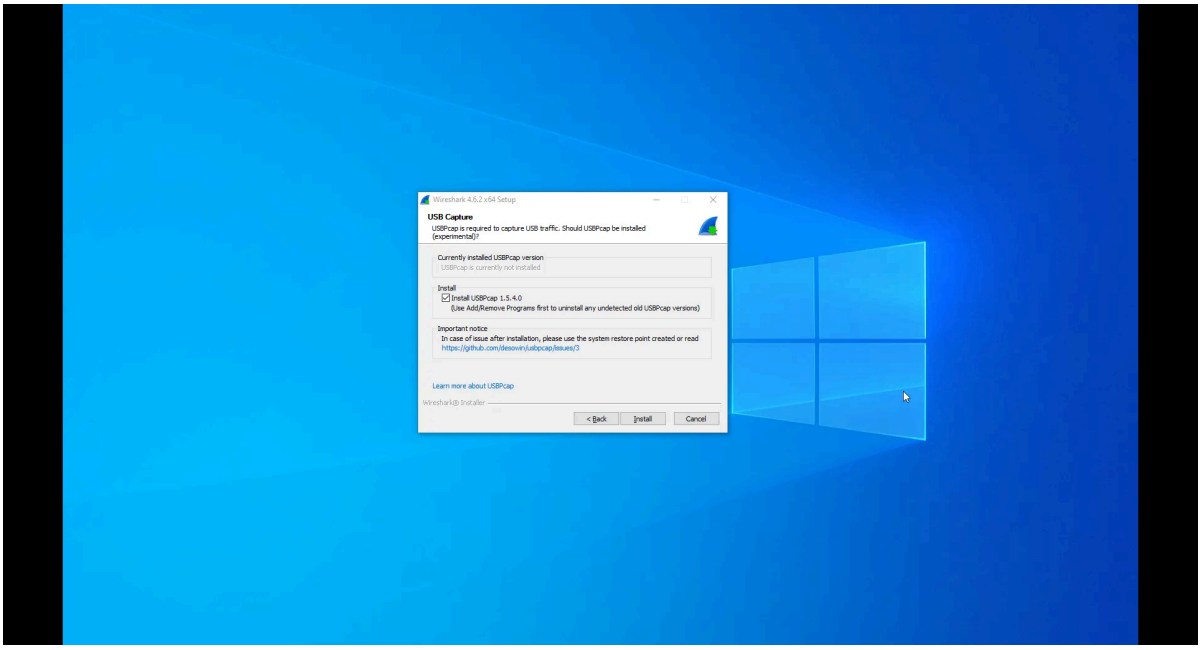

Wireshark 4.6.2 x64 Setup
Do you use Wireshark professionally?
Become a Wireshark Certified analyst!
The WCA is designed to formally recognize engineers who demonstrate professional-level proficiency in network protocol analysis and advanced troubleshooting using Wireshark.
You can learn more at https://www.wireshark.org/certifications.
Wireshark® Installer
< Back
Next >
Cancel
Waya CHEMLA

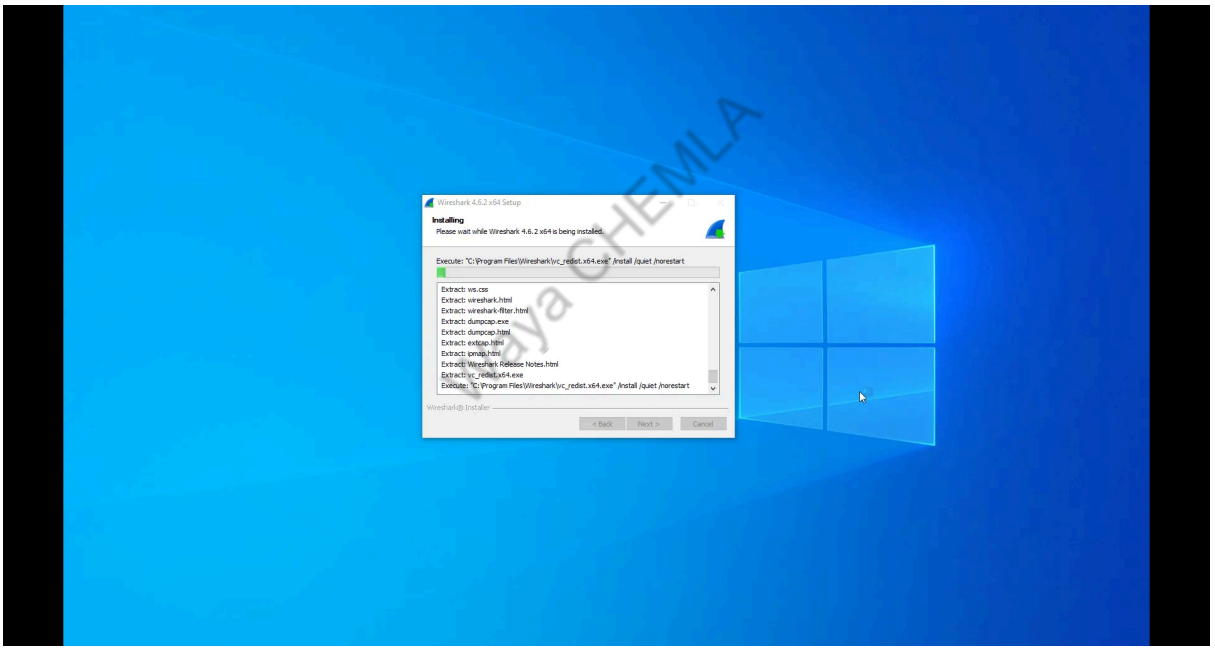

Wireshark 4.6.2 x64 Setup
Choose Components
Choose which features of Wireshark 4.6.2 x64 you want to install.
The following components are available for installation.
Select components to install:
Wireshark
TShark
External capture tools (extcap)
Androiddump
Etwdump
Randpktdump
Description
Space required: 300.4 MB
Position your mouse over a component to see its description.
Wireshark® Installer
< Back
Next >
Cancel

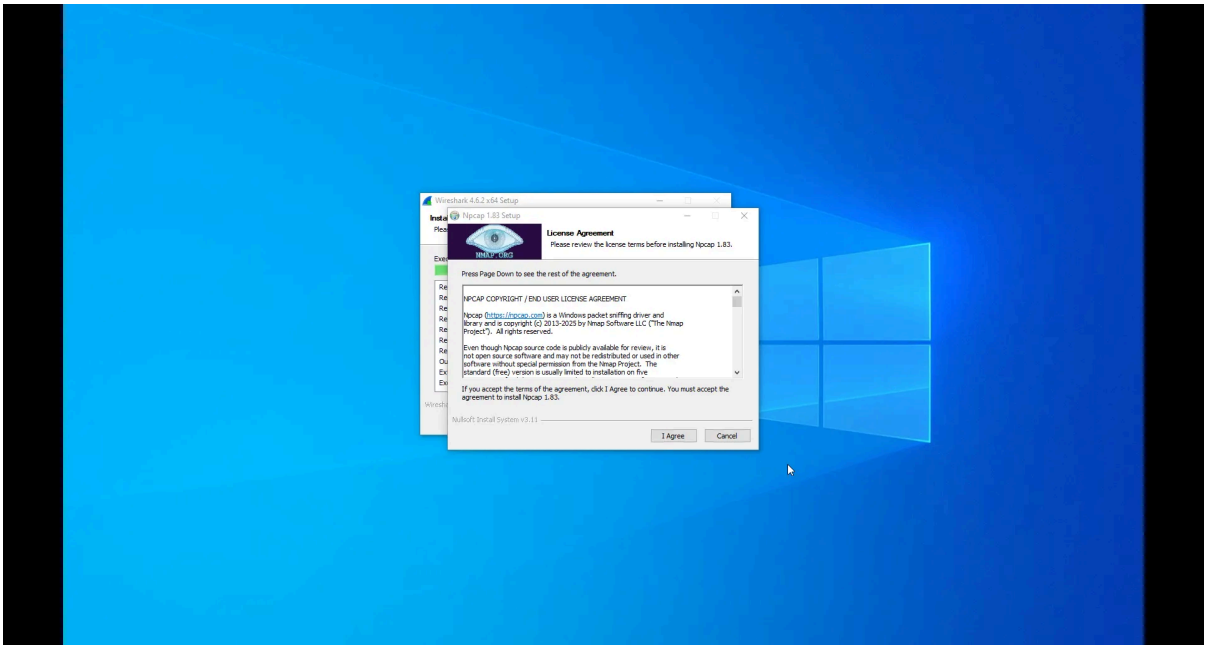

Wireshark 4.6.2 x64 Setup
Additional Tasks
Create shortcuts and associate file extensions.
Create Shortcuts
Wireshark Start Menu Item
Wireshark Desktop Icon
Associate File Extensions
Associate trace file extensions with Wireshark
Extensions include 5vw, acp, apc, atc, bfr, cap, enc, erf, fdc, ipfix, lcap, mpeg, ntar, out, pcap, pcapng, pkg, pkt, rf5, rtp, snoop, syc, tpc, tr1, trace, trc, vwr, wpc, and wpz.
Wireshark® Installer
< Back
Next >
Cancel

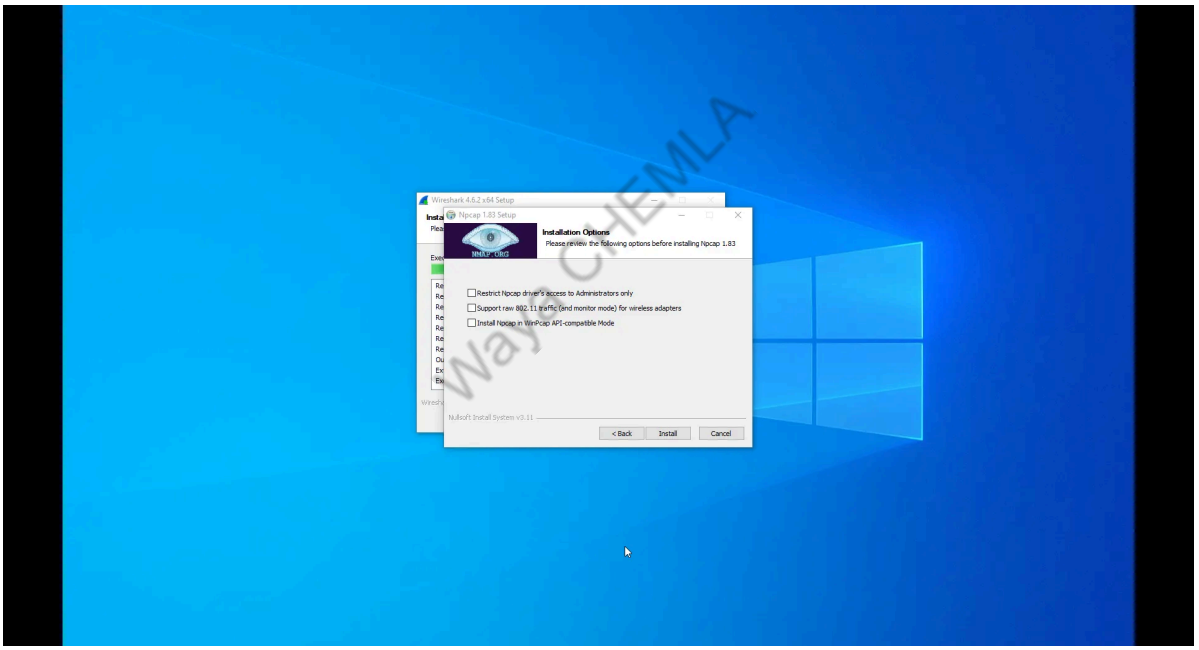

Wireshark 4.6.2 x64 Setup
Choose Install Location
Choose the folder in which to install Wireshark 4.6.2 x64.
Choose a directory in which to install Wireshark.
Destination Folder
C:\Program Files\Wireshark
Browse...
Space required: 300.4 MB
Space available: 72.0 GB
Wireshark® Installer
< Back
Next >
Cancel

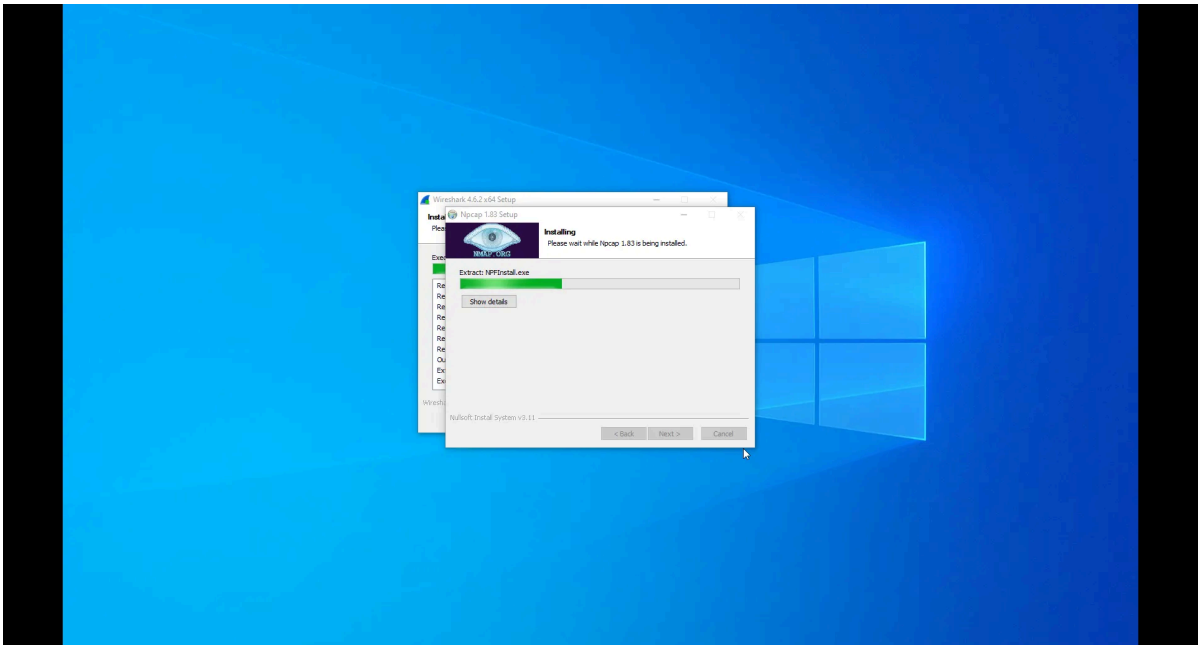

Wireshark 4.6.2 x64 Setup
Packet Capture
Wireshark requires Npcap to capture live network data.
Currently installed Npcap or WinPcap version
Neither of these are installed
Install
Install Npcap 1.83
(Use Add/Remove Programs first to uninstall any undetected old Npcap or WinPcap
Important notice
If your system has crashed during a Wireshark installation, you must run the command
'net stop npcap' as Administrator before upgrading Npcap, so that it doesn't crash again
Learn more about Npcap
Wireshark® Installer
< Back
Next >
Cancel


Wireshark 4.6.2 x64 Setup
USB Capture
USBPcap is required to capture USB traffic. Should USBPcap be installed (experimental)?
Currently installed USBPcap version
USBPcap is currently not installed
Install
Install USBPcap 1.5.4.0
(Use Add/Remove Programs first to uninstall any undetected old USBPcap versions)
Important notice
In case of issue after installation, please use the system restore point created or read
https://github.com/desowin/usbpcap/issues/3
Learn more about USBPcap
Wireshark® Installer
< Back
Install
Cancel


Wireshark 4.6.2 x64 Setup
Installing
Please wait while Wireshark 4.6.2 x64 is being installed.
Execute: "C:\Program Files\Wireshark\vc_redist.x64.exe" /install /quiet /norestart
Extract: ws.css
Extract: wireshark.html
Extract: wireshark-filter.html
Extract: dumpcap.exe
Extract: dumpcap.html
Extract: extcap.html
Extract: pmap.html
Extract: Wireshark Release Notes.html
Extract: vc_redist.x64.exe
Execute: "C:\Program Files\Wireshark\vc_redist.x64.exe" /install /quiet /norestart
Wireshark® Installer
< Back
Next >
Cancel

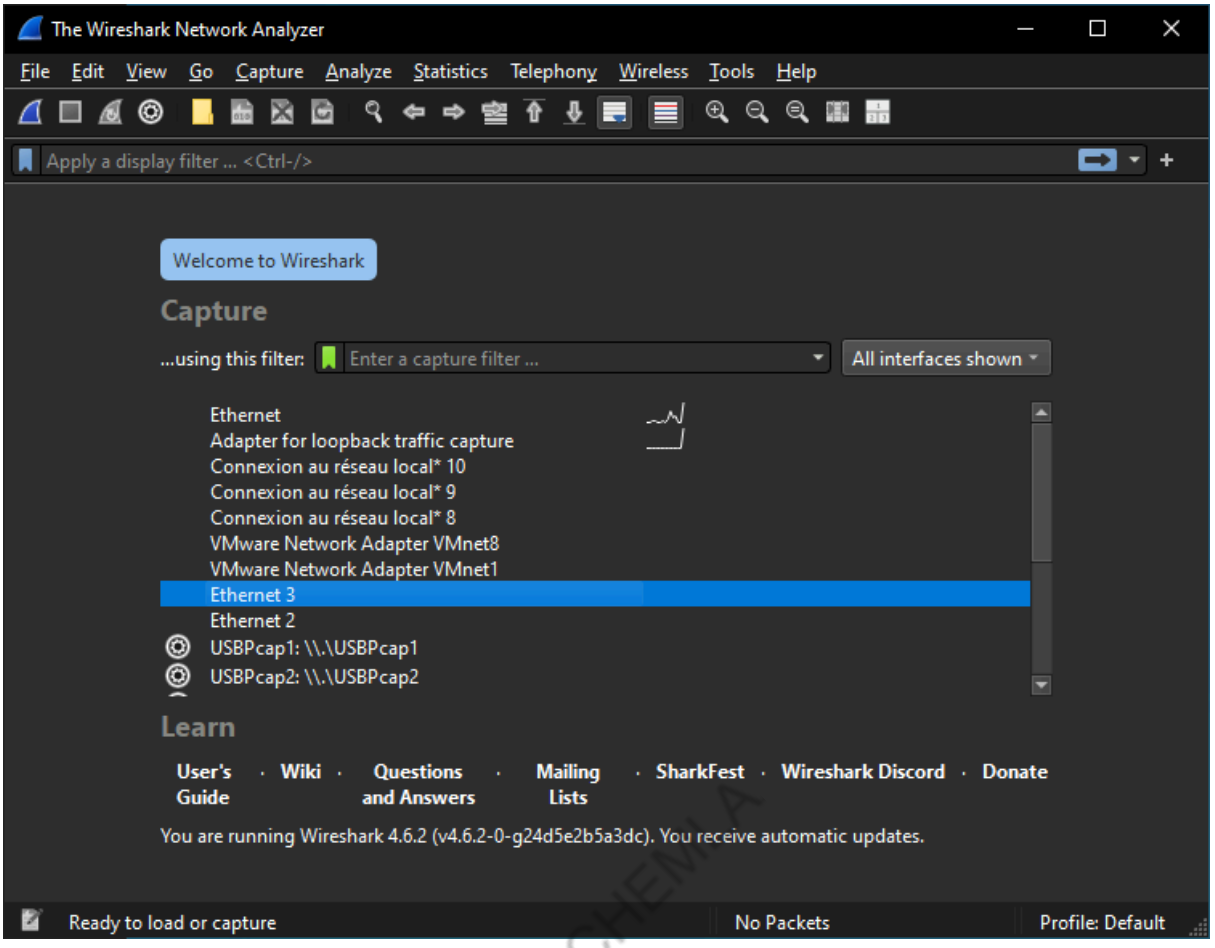

Wireshark 4.6.2 x64 Setup
Npcap 1.83 Setup
License Agreement
Please review the license terms before installing Npcap 1.83.
Press Page Down to see the rest of the agreement.
NPCAP COPYRIGHT / END USER LICENSE AGREEMENT
Npcap (https://npcap.com) is a Windows packet sniffing driver and
library and is copyright (c) 2013-2025 by Nmap Software LLC ("The Nmap
Project"). All rights reserved.
Even though Npcap source code is publicly available for review, it is
not open source software and may not be redistributed or used in other
software without special permission from the Nmap Project. The
standard (free) version is usually limited to installation on five
If you accept the terms of the agreement, click I Agree to continue. You must accept the
agreement to install Npcap 1.83.
Nullsoft Install System v3.11
I Agree
Cancel

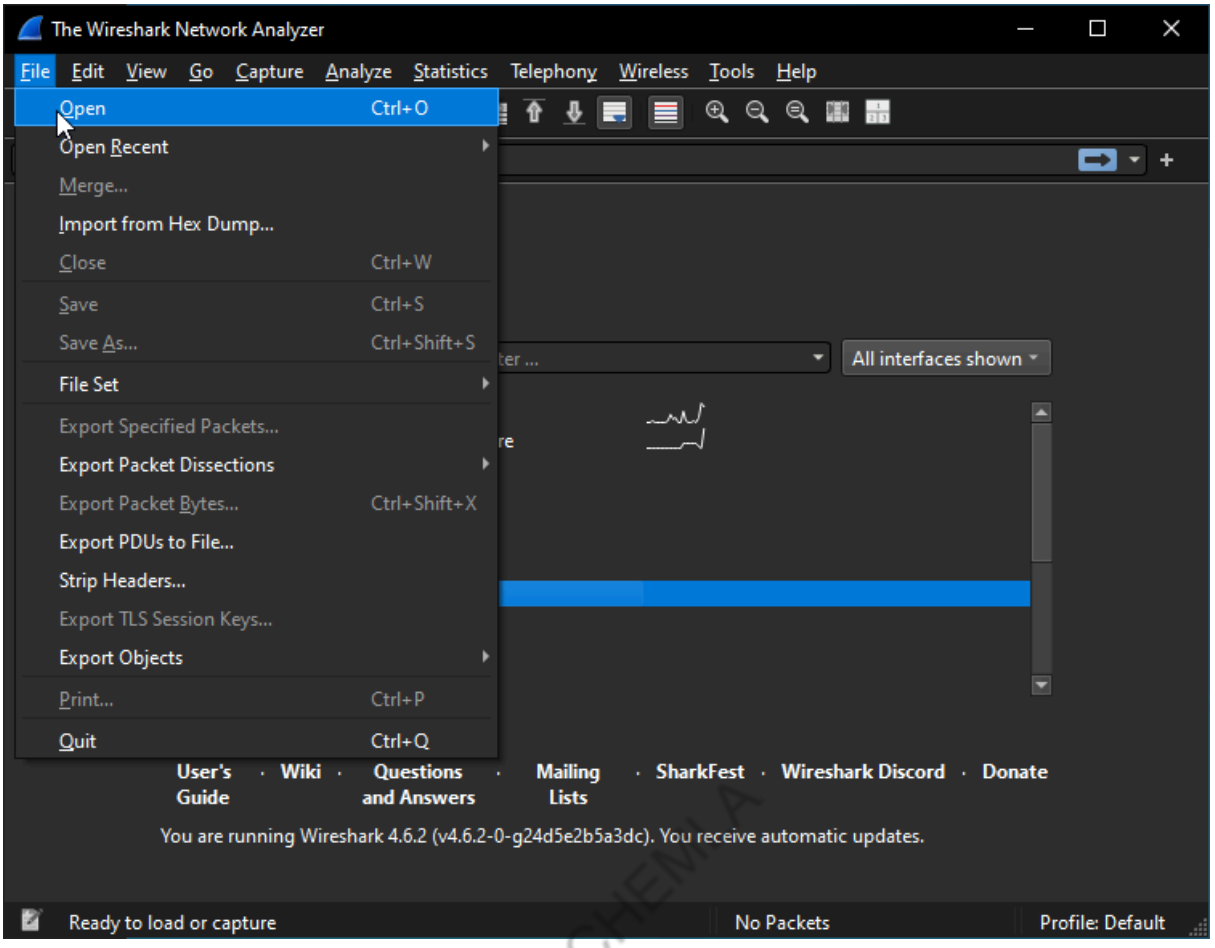

Wireshark 4.6.2 x64 Setup
Npcap 1.83 Setup
Installation Options
Please review the following options before installing Npcap 1.83
Restrict Npcap driver's access to Administrators only
Support raw 802.11 traffic (and monitor mode) for wireless adapters
Install Npcap in WinPcap API-compatible Mode
Nullsoft Install System v3.11
< Back
Install
Cancel

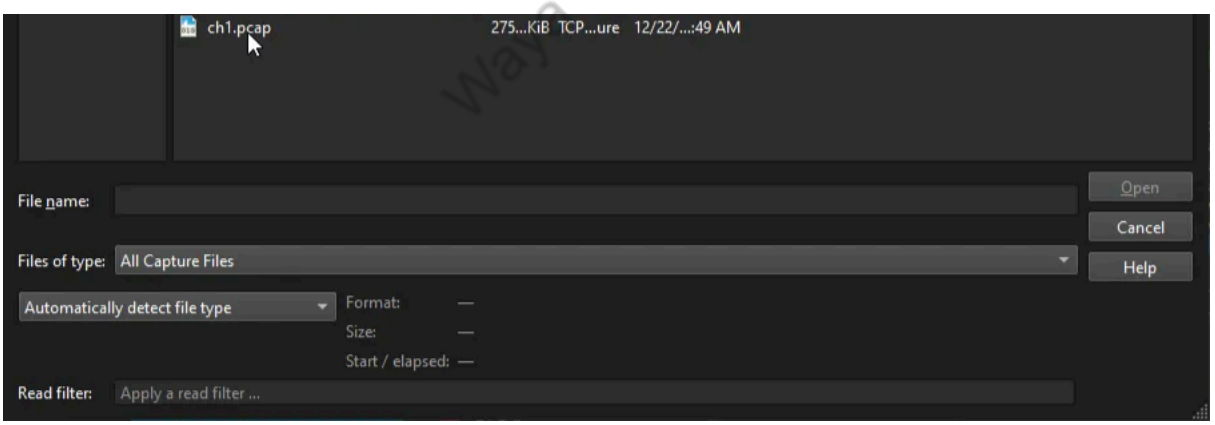


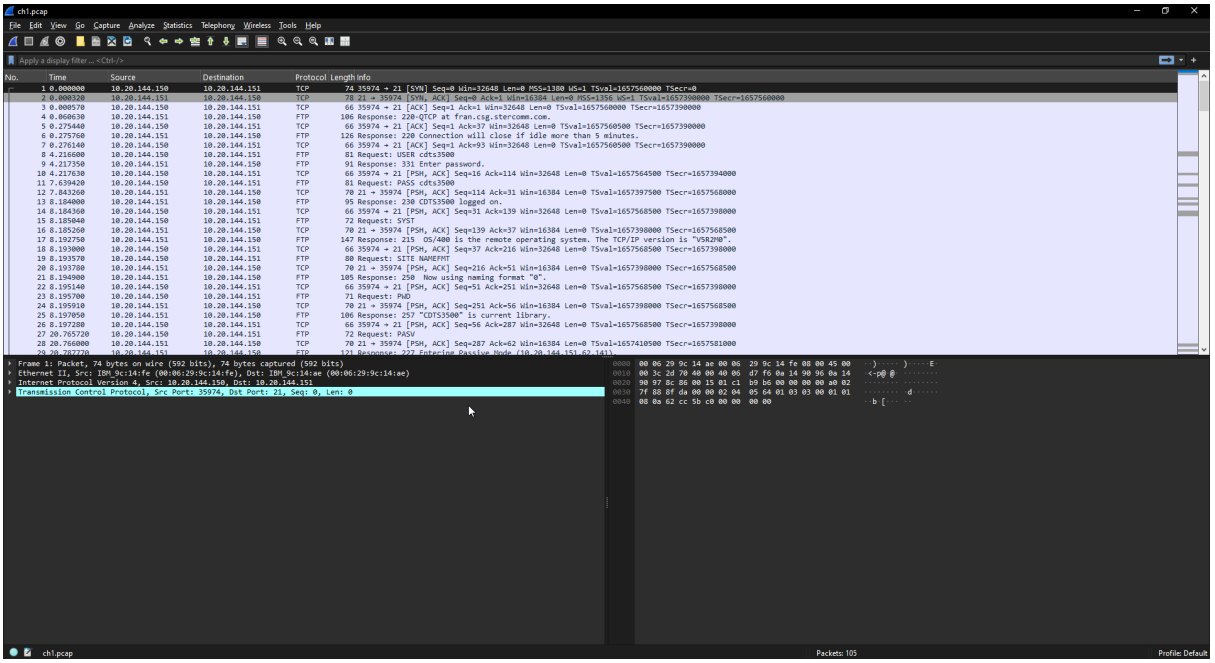
🔍 Étape 2 : Ouverture du fichier de capture

Une fois Wireshark installé, j'ai lancé le programme et ouvert le fichier .pcap téléchargé depuis Root-me.


The Wireshark Network Analyzer
File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help
Apply a display filter ... <Ctrl-/>
Welcome to Wireshark
Capture
...using this filter: Enter a capture filter ...
All interfaces shown
Ethernet
Adapter for loopback traffic capture
Connexion au réseau local* 10
Connexion au réseau local* 9
Connexion au réseau local* 8
VMware Network Adapter VMnet8
VMware Network Adapter VMnet1
Ethernet 3
Ethernet 2
USBPcap1: \\.\USBPcap1
USBPcap2: \\.\USBPcap2
Learn
User's Guide · Wiki · Questions and Answers · Mailing Lists · SharkFest · Wireshark Discord · Donate
You are running Wireshark 4.6.2 (v4.6.2-0-g24d5e2b5a3dc). You receive automatic updates.
Ready to load or capture
No Packets
Profile: Default

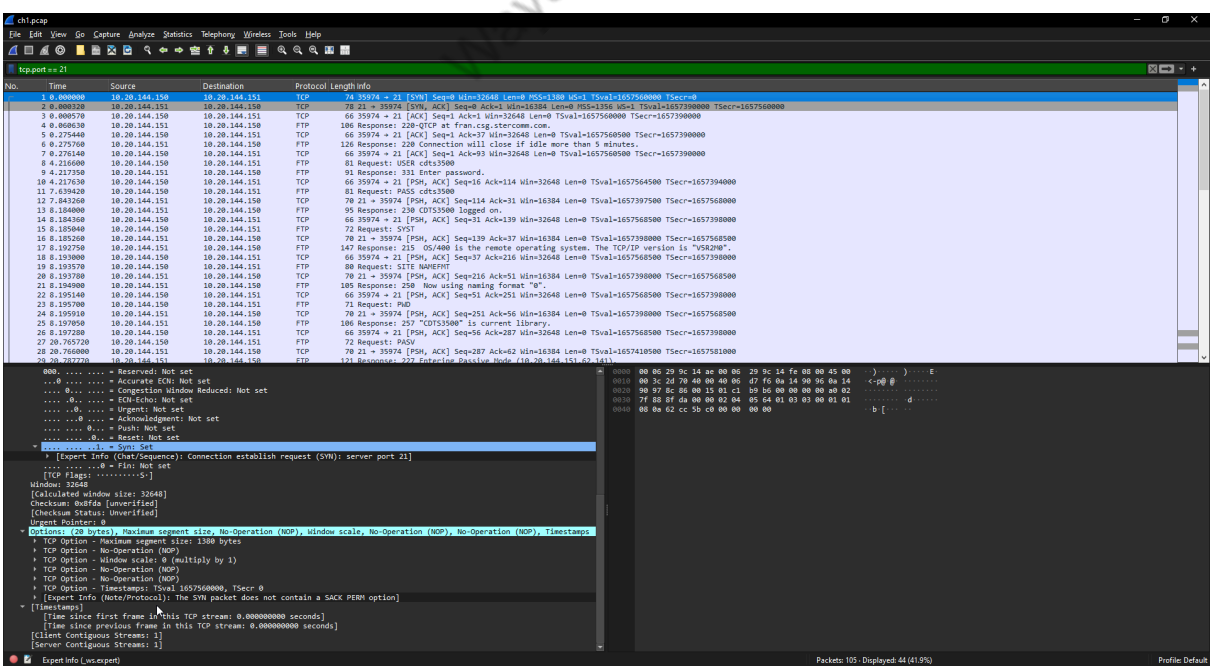

The Wireshark Network Analyzer
File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help
Open Ctrl+O
Open Recent
Merge...
Import from Hex Dump...
Close Ctrl+W
Save Ctrl+S
Save As... Ctrl+Shift+S
File Set
Export Specified Packets...
Export Packet Dissections
Export Packet Bytes... Ctrl+Shift+X
Export PDUs to File...
Strip Headers...
Export TLS Session Keys...
Export Objects
Print... Ctrl+P
Quit Ctrl+Q
All interfaces shown
User's Guide · Wiki · Questions and Answers · Mailing Lists · SharkFest · Wireshark Discord · Donate
You are running Wireshark 4.6.2 (v4.6.2-0-g24d5e2b5a3dc). You receive automatic updates.
Ready to load or capture
No Packets
Profile: Default


ch1.pcap 275...KiB TCP...ure 12/22/...:49 AM
File name:
Open
Cancel
Help
Files of type: All Capture Files
Automatically detect file type
Format:
Size:
Start / elapsed:
Read filter: Apply a read filter ...

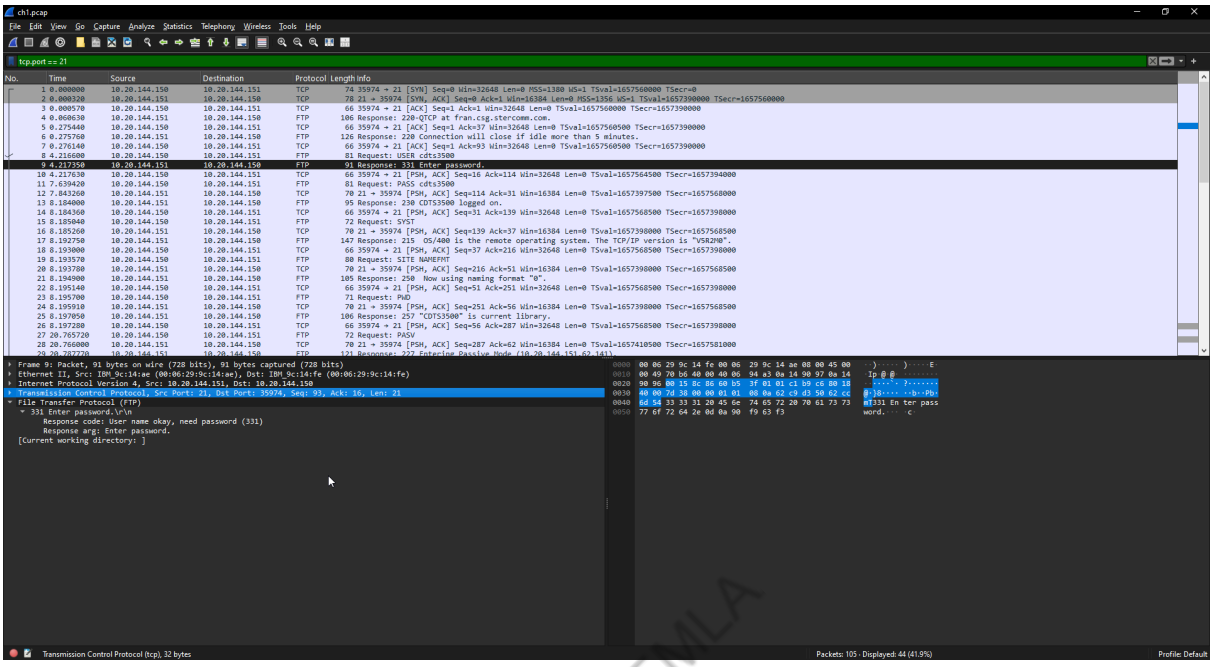


🕵️ Étape 3 : Analyse du protocole FTP

Puisque l'énoncé mentionne un échange authentifié via le protocole FTP, j'ai appliqué un filtre sur le protocole **FTP** pour isoler les paquets pertinents.



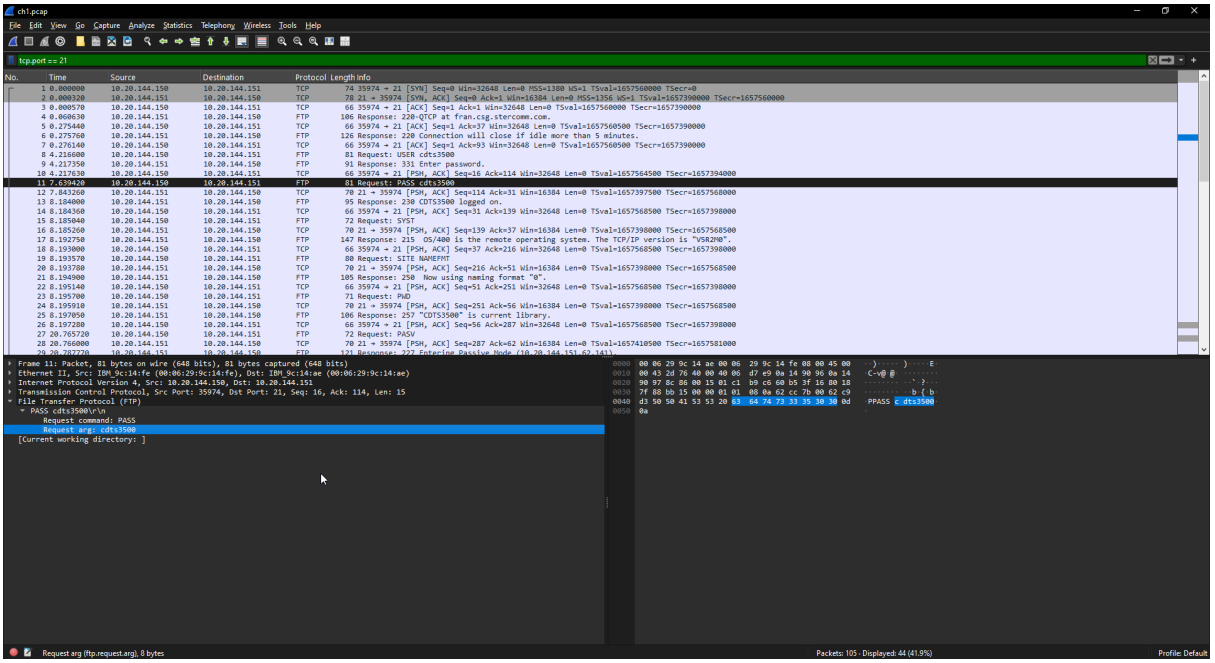
💡 **Objectif** : Comprendre où l'authentification a lieu et identifier les commandes FTP utilisées.



✅ Solution

En analysant les paquets FTP, j'ai identifié la commande **PASS** qui contient le mot de passe en clair.

🔑 **Mot de passe trouvé** : `cdts3500`



📝 Conclusion

Ce challenge démontre que le protocole FTP transmet les identifiants en clair, ce qui le rend vulnérable aux attaques de type "sniffing". Il est préférable d'utiliser des protocoles sécurisés comme SFTP ou FTPS pour les échanges de fichiers authentifiés.

Challenge réalisé sur la plateforme Root-me