Tracing

2N® Tracing & Wireshark

Quick guide

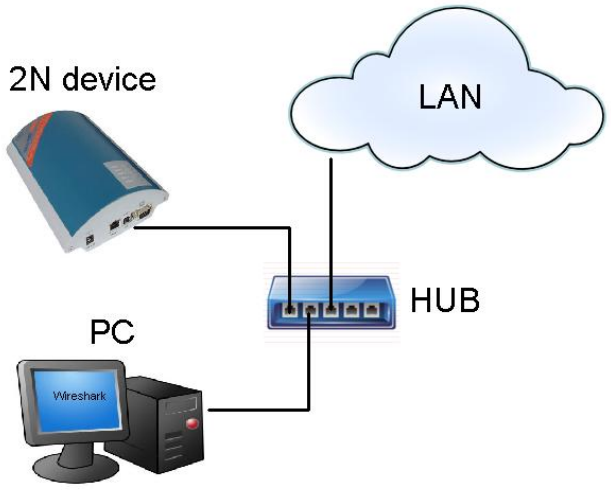
Version 1.00

www.2n.cz

Program Wireshark slouží na sledování komunikace mezi zařízeními propojenými pomocí LAN sítě. Komunikující zařízení (například PBX propojená s GSM bránou pomocí LAN) si mezi sebou vyměňují pakety, které tento program odchytává. Wireshark je distribuován pod Open source licencí (http://www.wireshark.org/download.html).

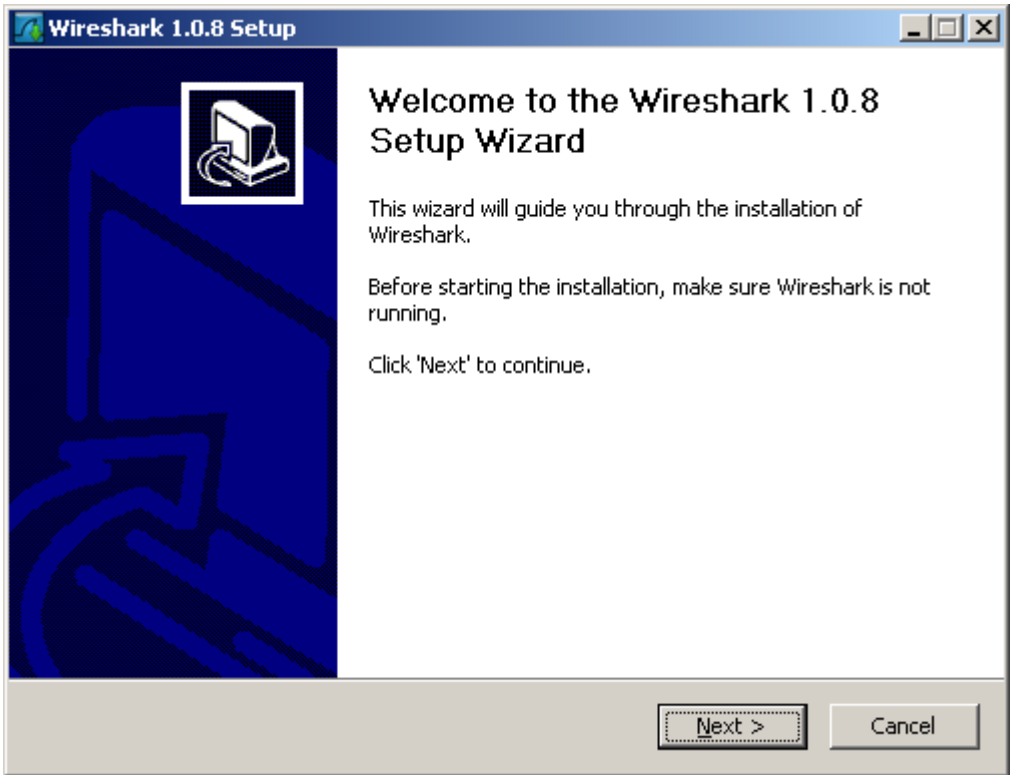
K tomu, abychom byli schopni komunikaci odchytávat musí všechny přístroje patřit do stejného segmentu sítě (**musí být vzájemně propojeny hubem** = rozbočovačem). Pokud nemáme hub, můžeme použít i switch jen v tom případě pokud podporuje port mirroring (http://en.wikipedia.org/wiki/Port_mirroring).

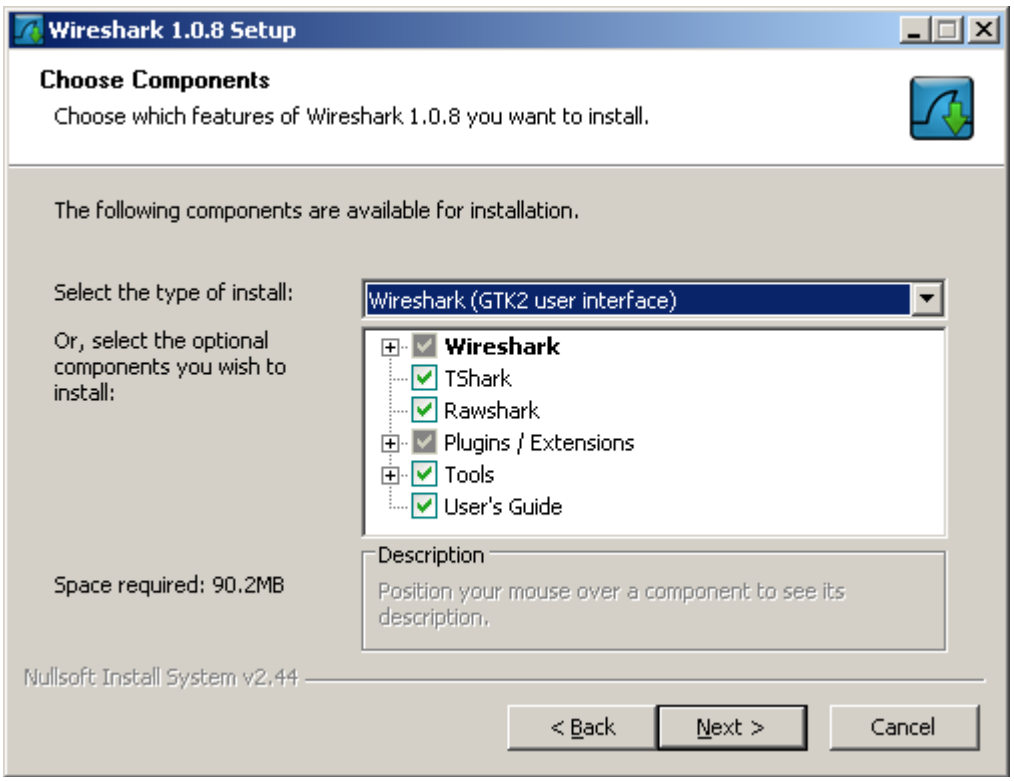
Takže odpovídající schéma je zde:

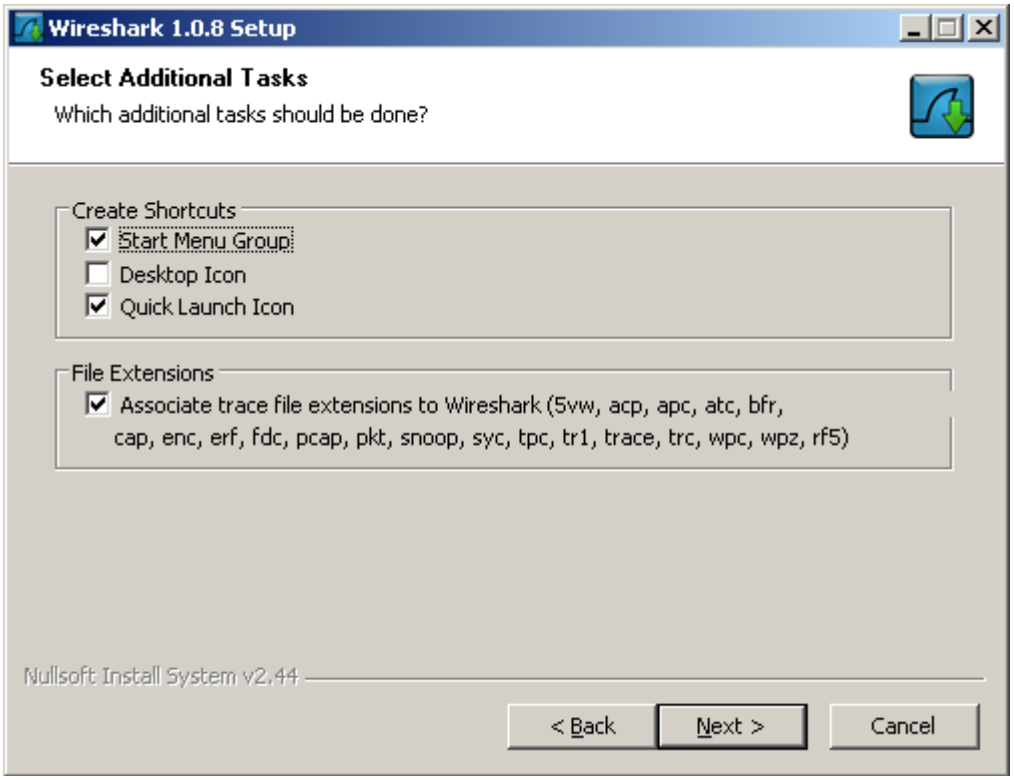


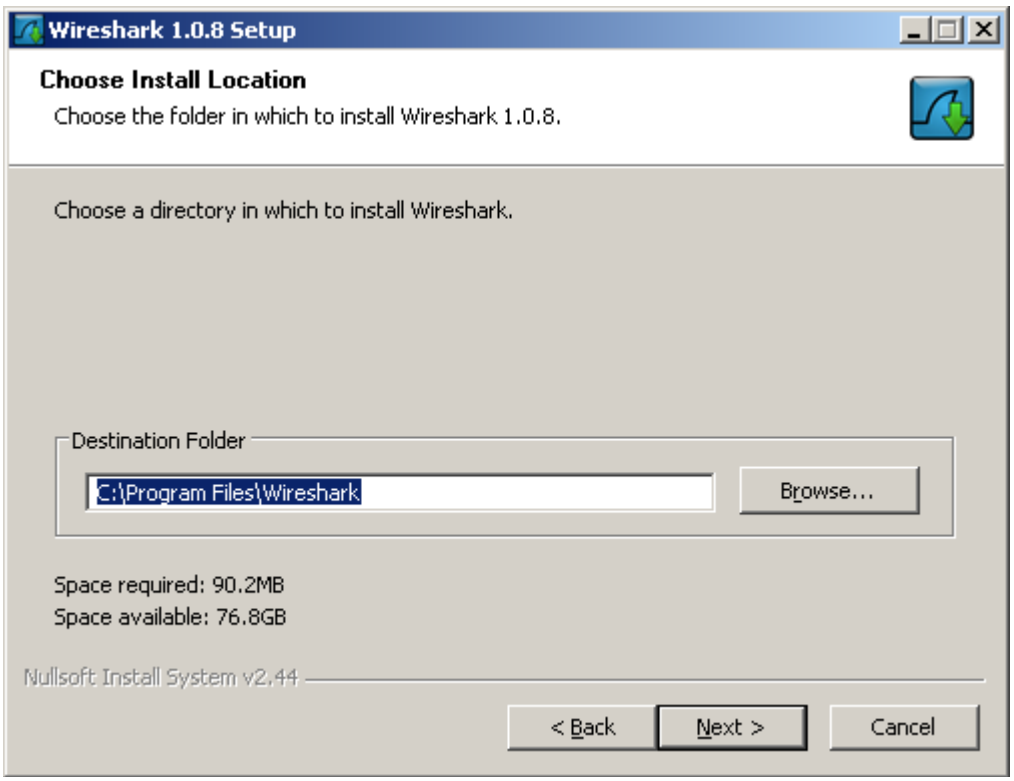
Instalace:

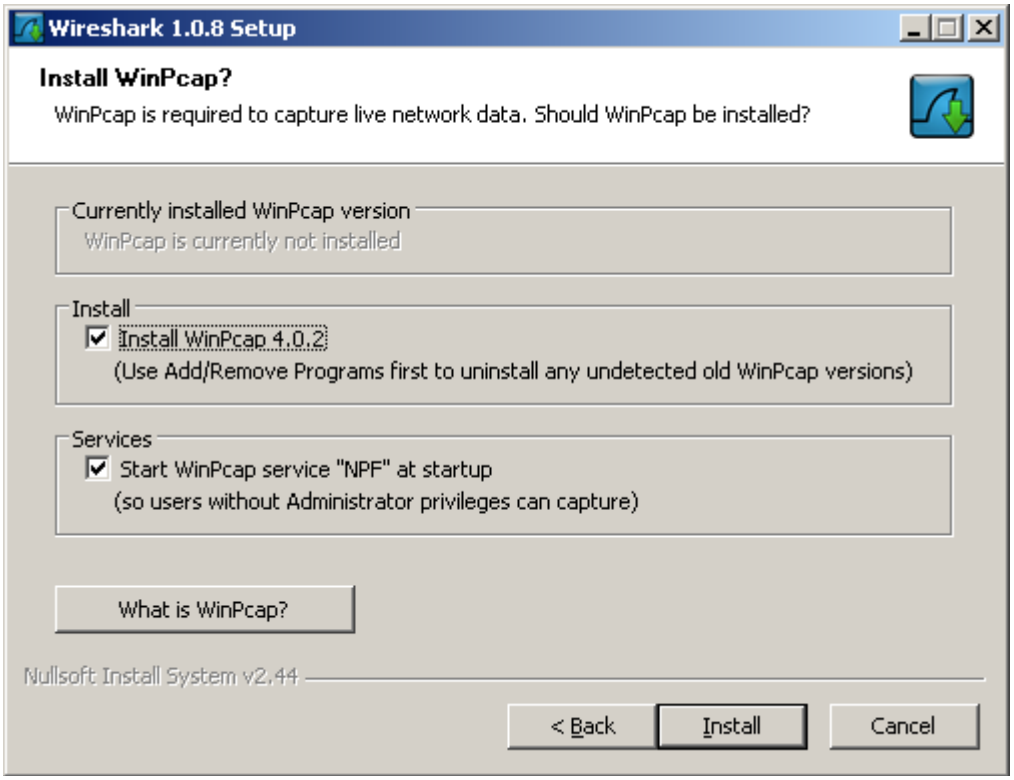
Stáhněte program a odpovídající instalátor (např. Windows installer).

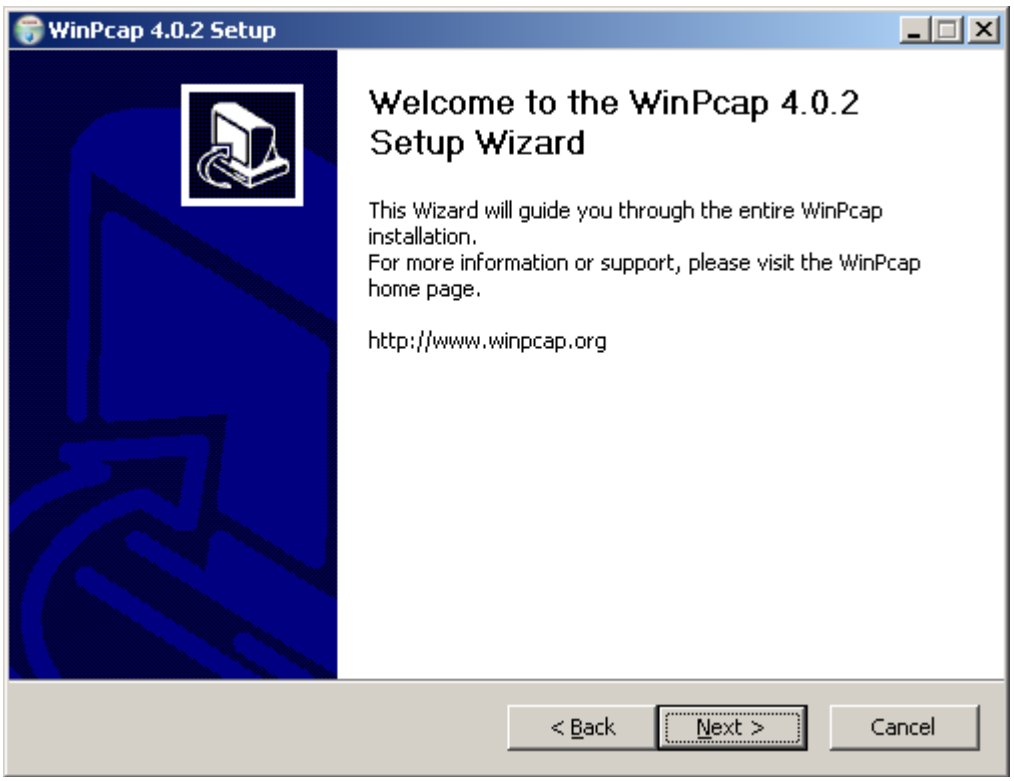


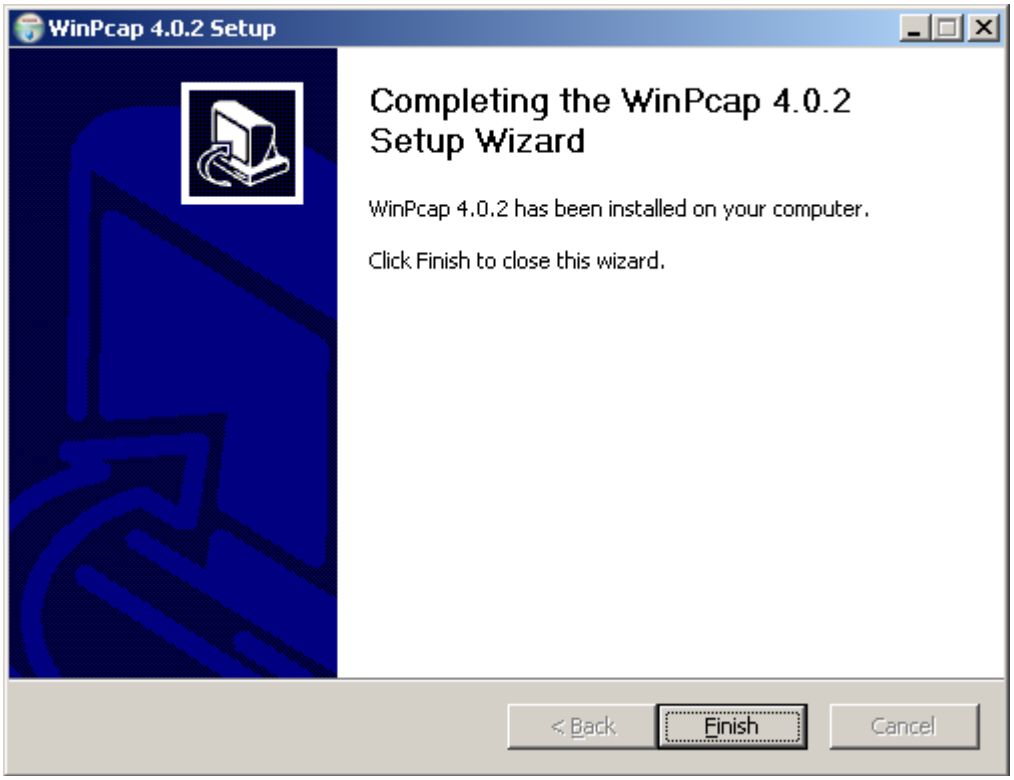

Wireshark 1.0.8 Setup
Choose Components
Choose which features of Wireshark 1.0.8 you want to install.
The following components are available for installation.
Select the type of install:
Wireshark (GTK2 user interface)
Or, select the optional components you wish to install:
Wireshark
TShark
Rawshark
Plugins / Extensions
Tools
User's Guide
Description
Position your mouse over a component to see its description.
Space required: 90.2MB
Nullsoft Install System v2.44
< Back
Next >
Cancel

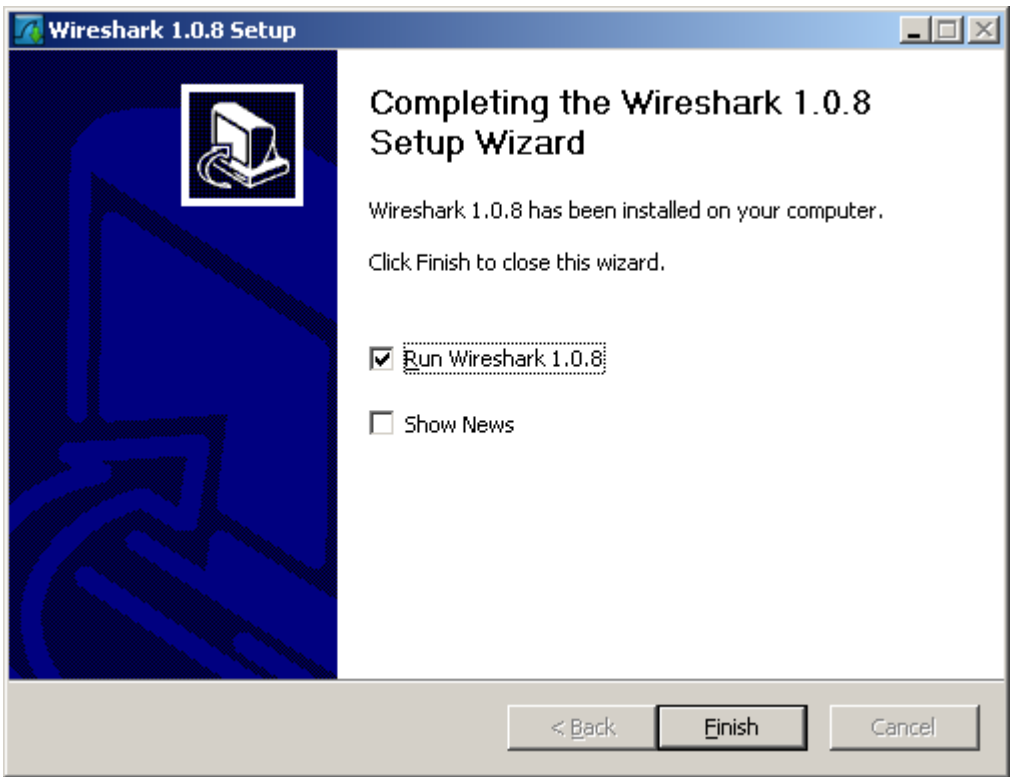

Wireshark 1.0.8 Setup
Select Additional Tasks
Which additional tasks should be done?
Create Shortcuts
Start Menu Group
Desktop Icon
Quick Launch Icon
File Extensions
Associate trace file extensions to Wireshark (5vw, acp, apc, atc, bfr, cap, enc, erf, fdc, pcap, pkt, snoop, syc, tpc, tr1, trace, trc, wpc, wpz, rf5)
Nullsoft Install System v2.44
< Back
Next >
Cancel


Wireshark 1.0.8 Setup
Choose Install Location
Choose the folder in which to install Wireshark 1.0.8.
Choose a directory in which to install Wireshark.
Destination Folder
C:\Program Files\Wireshark
Browse...
Space required: 90.2MB
Space available: 76.8GB
Nullsoft Install System v2.44
< Back
Next >
Cancel

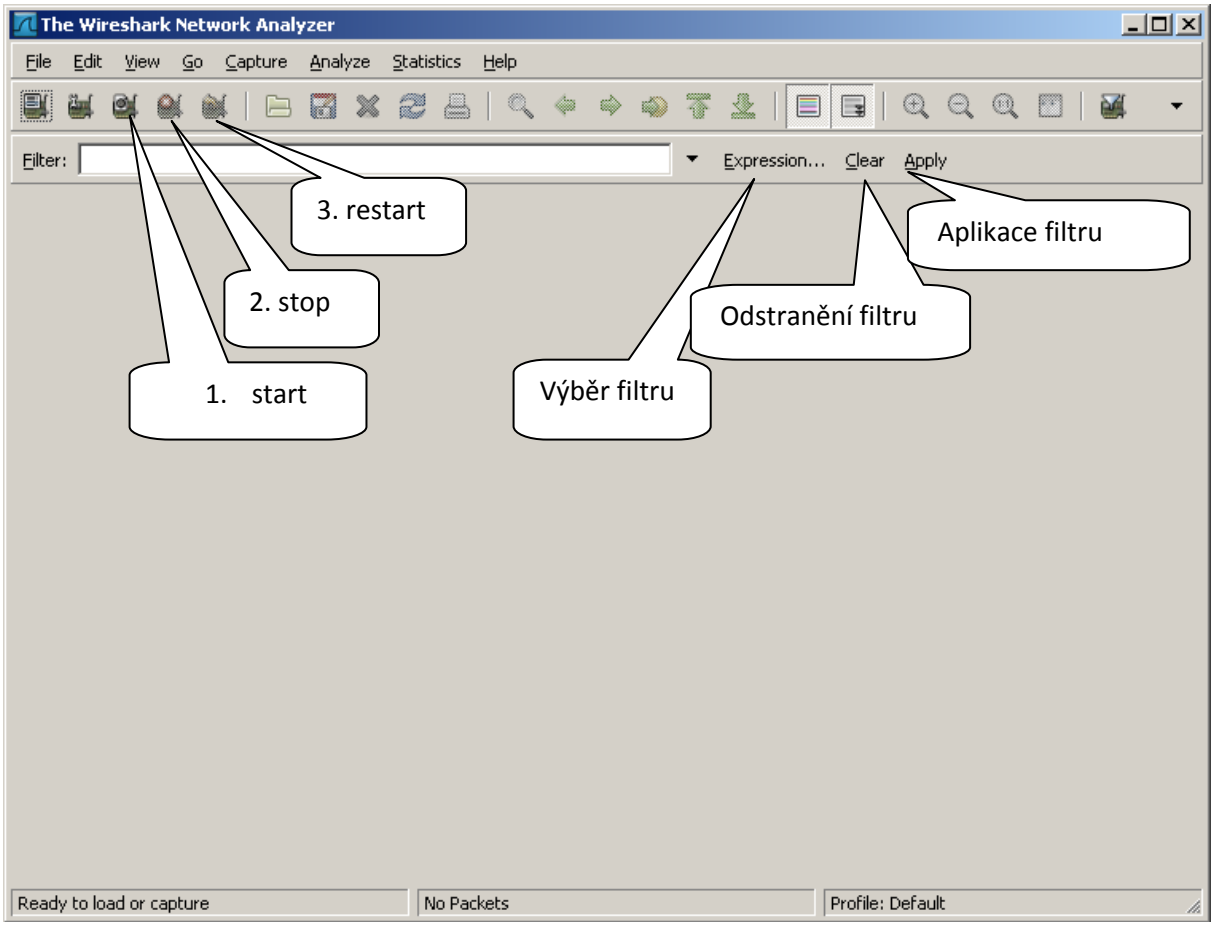

Wireshark 1.0.8 Setup
Install WinPcap?
WinPcap is required to capture live network data. Should WinPcap be installed?
Currently installed WinPcap version
WinPcap is currently not installed
Install
Install WinPcap 4.0.2
(Use Add/Remove Programs first to uninstall any undetected old WinPcap versions)
Services
Start WinPcap service "NPF" at startup
(so users without Administrator privileges can capture)
What is WinPcap?
Nullsoft Install System v2.44
< Back
Install
Cancel


WinPcap 4.0.2 Setup
Welcome to the WinPcap 4.0.2 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
< Back
Next >
Cancel


WinPcap 4.0.2 Setup
Completing the WinPcap 4.0.2 Setup Wizard
WinPcap 4.0.2 has been installed on your computer.
Click Finish to close this wizard.
< Back
Finish
Cancel



Spustí se aplikace Wireshark:



Start odchytávání: „Capture->Start" nebo přes ikonku 1
Konec odchytávání: „Capture->Stop" nebo přes ikonku 2

Restart odchytávání s vymazáním předešlých paketů: „Capture->Restart“ nebo přes ikonku 3
Uložení výsledku: „File->Save As->Wireshark/tcpdump/… -libpcap(*.pcap;*.cap)
Načtení uloženého tracu: „File->Open”
Aplikování filtru:
1) Chci filtrovat podle zdrojové IP adresy – např: ip.src_host==“192.168.5.7“

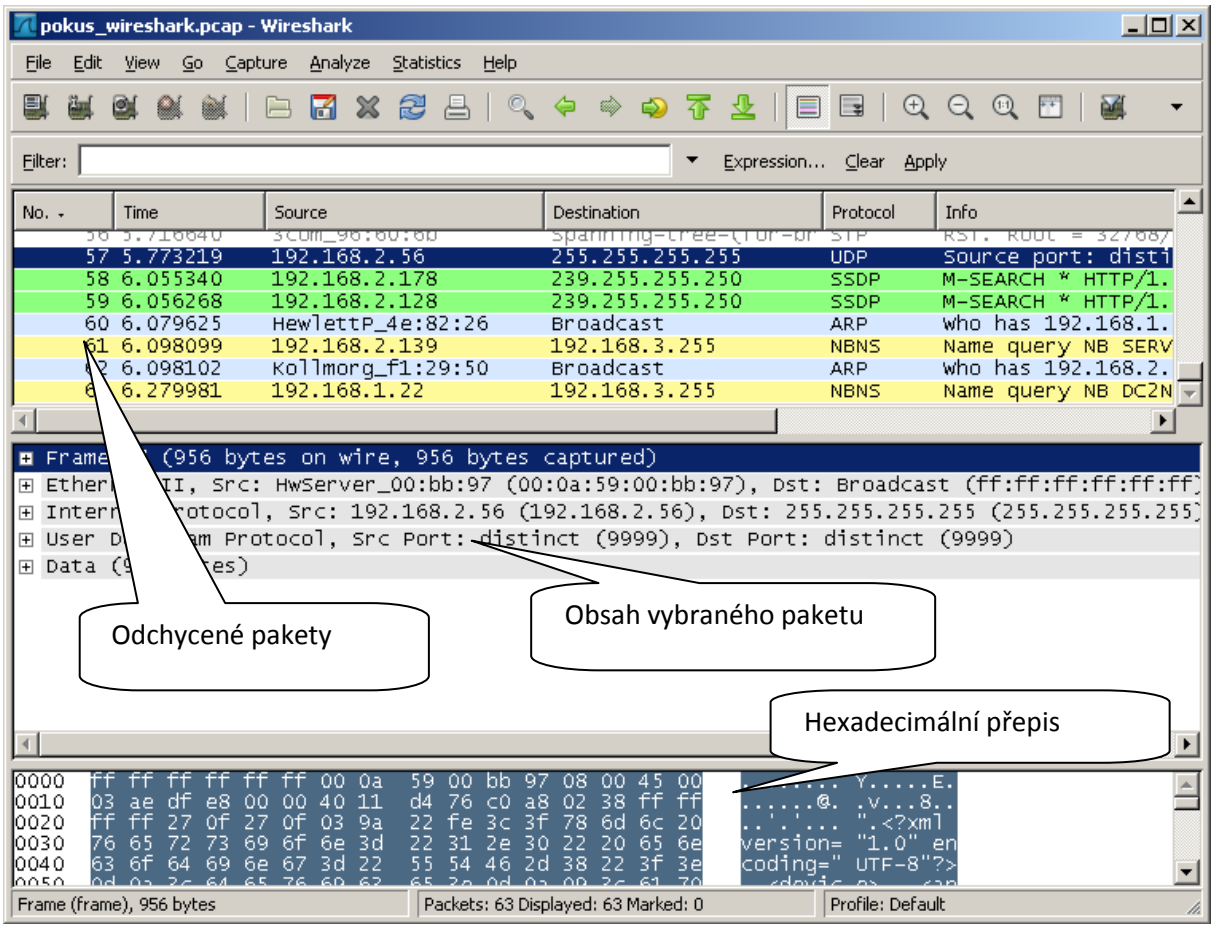
2) Chci filtrovat podle cílové IP adresy – např: ip.dst_host==“192.168.5.7“

3) Typ protokolu: tcp, udp, sip, …

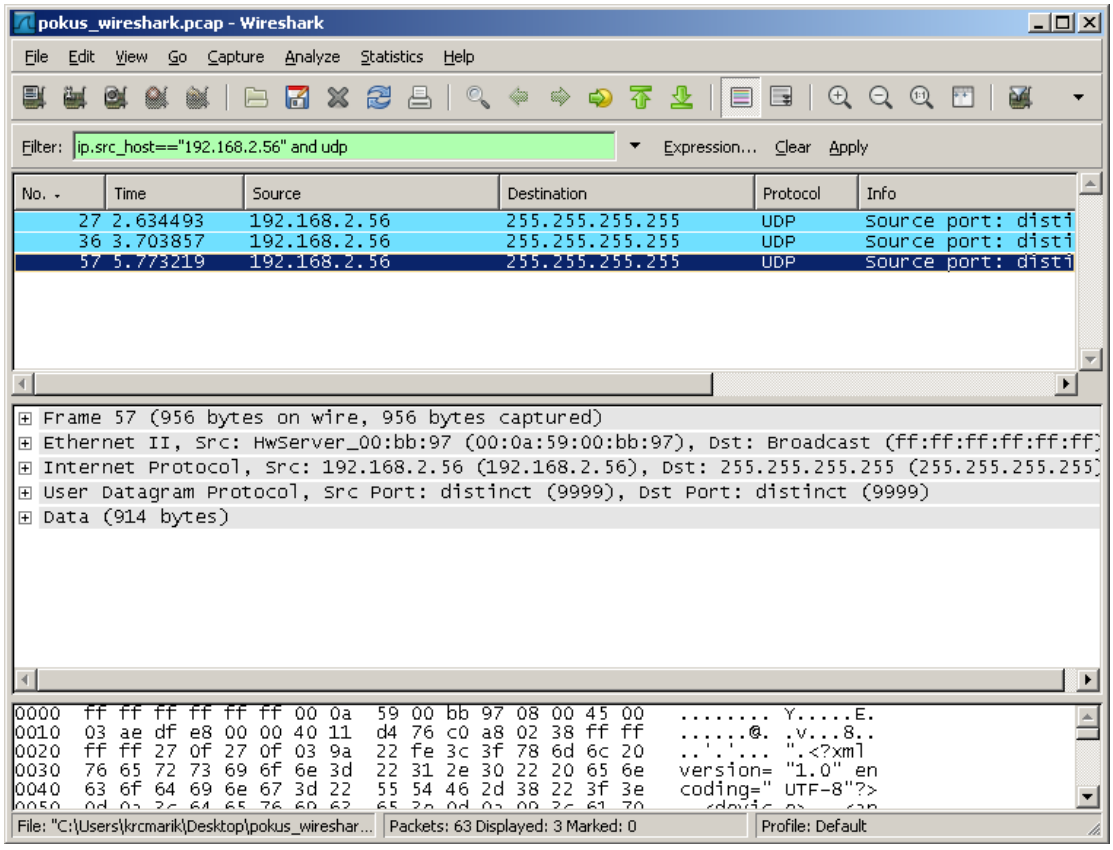
4) Jednotlivé podmínky se dají logicky spojovat: and, or, not, …

5) Pro potvrzení filtru – Apply, pro vymazání filtru – Clear

Příklad odchycené síťové komunikace:



Příklad odchycené síťové komunikace po aplikování filtru:



Důležité: Při ukládání tracu kvůli identifikaci problému u nesprávně fungujícího produktu, prosím nepoužívejte žádný filtr (jednoduše odchytávejte celou komunikaci na LAN). Po testovacím hovoru uložte výsledek přes **Save as>Wireshark/tcpdump/… - libpcap(*.pcap;*.cap)** a pošlete nám ho.

2N TELEKOMUNIKACE a.s.

Modřanská 621, 143 01 Praha 4
tel.: 261 301 111, fax: 261 301 999,
e-mail: sales@2n.cz
www.2n.cz