

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: | Image: Wireshark Image: The Shark Image: Wireshark Image: Wireshark | | | |
| Space required: 90.2MB | Position your mouse over a component to see its description. | | | |
| Nullsoft Install System v2.44 | | | | |
| | < <u>B</u> ack <u>N</u> ext > | Cancel | | |
| - | | | | |
| Wireshark 1.0.8 Setup | | | | |
| Select Additional Tasks Which additional tasks should b | e done? | 1 | | |
| Create Shortcuts Start Menu Group Desktop Icon Quick Launch Icon | | | | |
| File Extensions 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 | < <u>B</u> ack <u>N</u> ext > | 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 | ς, | | |
| | | | |
| Destination Folder | | | |
| C:\Program Files\Wireshark | | Brow | Nse |
| Space required: 90.2MB | | | |
| Space available: 76.8GB | | | |
| Nullsoft Install System v2.44 | | | |
| | < <u>B</u> ack | <u>N</u> ext > | Cancel |
| Wireshark 1.0.8 Setup | | | |
| Install WinPcap? WinPcap is required to capture live network da | ta. Should WinPo | cap be installed? | |
| Currently installed WinPcap version WinPcap is currently not installed | | | |
| Install Install WinPcap 4.0.2 (Use Add/Remove Programs first to unin | stall any undete | cted old WinPcap | versions) |
| Services Service "NPF" at startup | | | |
| (so users without Administrator privilege | s can capture) | | |
| | | | |
| What is WinPcap? | | | |
| Nullsoft Install System v2.44 | | | |
| | < <u>B</u> ack | Install | 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:

| 📶 pokus_wireshark.pcap - Wireshark | | | | |
|--|--|--------------------------|------------------------|--|
| <u> Eile Edit View Go Capture Analyze S</u> | tatistics <u>H</u> elp | | | |
| | 2 占 🔍 🗢 🔹 🞝 7 | । 🔁 🛛 🔁 🖓 | Q 🔍 🖭 🌌 🛛 | |
| Eilter: Expression Clear Apply | | | | |
| No Time Source | Destination | Protocol | Info | |
| 57 5-773219 192-168-2- | . op Spanning-tre | e-tron-priste 255 UDP | RST. RUUL = 327087 | |
| 58 6.055340 192.168.2.1 | 239.255.255. | 250 SSDP | M-SEARCH * HTTP/1. | |
| 59 6.056268 192.168.2.1 | L28 239.255.255. | 250 SSDP | M-SEARCH * HTTP/1. | |
| 60 6.079625 HewlettP_4 | 2:82:26 Broadcast | ARP | Who has 192.168.1. | |
| 1 = 0.098099 = 192.168.2.1 | 139 192.108.3.20 1:29:50 Broadcast | | who has 192 168 2 | |
| 6,279981 192,168,1.2 | 22 192.168.3.25 | 5 NBNS | Name query NB DC2N | |
| | | 1 | | |
| | | | | |
| ■ Frame (956 bytes on wire, | 956 bytes captured) | | | |
| Ether ↓ I, Src: HwServer_0 | 0:bb:97 (00:0a:59:00:bb: | :97), Dst: Broadcas | st (##:##:##:##:##:##) | |
| Intern rotocol, Src: 192. | 168.2.56 (192.168.2.56), | Dst: 255.255.255. | 255 (255.255.255.255) | |
| User D m Protocol, Src | Port: distinct (9999), D |)st Port: distinct | (9999) | |
| ⊞ Data (¶ tes) | | | | |
| | | | ו | |
| | | апепо ракети | | |
| | | _ | J | |
| | | | | |
| | | Llovadacim | | |
| T. | | пехацести | | |
| | | | | |
| 0000 TT TT TT TT TT TT 00 0a 0010 03 aa df a8 00 00 40 11 | 59 00 66 97 08 00 45 00 d4 76 c0 38 07 38 ff ff | ····· Y | E. 🔺 | |
| 0020 ff ff 27 0f 27 0f <u>03 9a</u> | 22 fe 3c 3f 78 6d <u>6c 20</u> | '.'."" | i — | |
| 0030 76 65 72 73 69 6f 6e 3d | 22 31 2e 30 22 20 65 6e | version= "1.0" | en | |
| 0040 63 67 64 69 6e 67 3d 22 | 55 54 46 2d 38 22 3f 3e | coding="UTF-8" | | |
| Frame (frame), 956 bytes | Packets: 63 Displayed: 63 Marked: 0 | Profile: Defau | ult // | |

Příklad odchycené síťové komunikace po aplikování filtru:

| 🗖 pokus_wireshark.pcap - Wireshark | |
|--|--|
| Eile Edit View Go Capture Analyze Statistics Help | |
| | . ⇔ ⇔ ⊋ 7 ⊻ 🗏 🗏 Q Q Q 🗹 🕷 🔸 |
| Eilter: jp.src_host=="192.168.2.56" and udp | ▼ Expression ⊆lear Apply |
| No Time Source | Destination Protocol Info |
| 27 2.634493 192.168.2.56 36 3.703857 192.168.2.56 | 255.255.255.255 UDP Source port: disti 255.255.255.255 UDP Source port: disti |
| 57 5.773219 192.168.2.56 | 255.255.255.255 UDP Source port: disti |
| | |
| | |
| 4 | |
| € Frame 57 (956 bytes on wire, 956 bytes | |
| Ethernet II, Src: HwServer_00:bb:97 (00 | 0:0a:59:00:bb:97), Dst: Broadcast (ff:ff:ff:ff:ff:ff:ff) |
| User Datagram Protocol, Src: 192.108.2.56 (1 User Datagram Protocol, Src Port: disti | inct (9999), Dst Port: distinct (9999) |
| 🗄 Data (914 bytes) | |
| | |
| | |
| | |
| | |
| | |
| 0000 TT TT TT TT TT TT 00 0a 59 00 bb 9 0010 03 ae df e8 00 00 40 11 d4 76 c0 at | 07 08 00 45 00 YE. |
| 0020 ff ff 27 0f 27 0f 03 9a 22 fe 3c 31 0030 76 65 72 73 69 6f 6e 3d 22 31 2e 30 | 77 78 6d 6c 20 |
| 0040 63 6f 64 69 6e 67 3d 22 55 54 46 20 | d 38 22 3f 3e coding="UTF-8"?> |
| File: "C:\Users\krcmarik\Desktop\pokus_wireshar Packets: 63 Dis | splayed: 3 Marked: 0 Profile: Default // |

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