**LABO 5**

**KENNISMAKING WIRESHARK**

In dit labo leer je basishandelingen uitvoeren in Wireshark.

Gebruikershandleiding: https://www.wireshark.org/docs/wsug\_html\_chunked/

1. Mocht dit nog niet gebeurd zijn: Download de recentste en stabiele 64 bit versie (14 februari 2020: versie 3.2.1) van de netwerkprotocolanalyzer software **Wireshark** op <http://www.wireshark.org/>

Met deze open source software kan je netwerkpakketten die je netwerkkaart binnenkomen of verlaten, opvangen en de details ervan bekijken.

Installeer Wireshark **en zorg ervoor dat WinPcap mee geïnstalleerd wordt.** USBPcap mag, maar moet niet mee geïnstalleerd worden.

1. Download het bestand **Capture1.pcapng** (PCAPNG = Packet CAPture Next Generation) vanaf Leho (module Wireshark-files) en open dit bestand door erop te dubbelklikken.
2. Het geopende bestand bevat een aantal pakketten die tijdens een capteersessie van/naar een netwerkkaart van een computer verzonden werden.

Hoeveel pakketten werden er gecapteerd?

19.055

Het hoofdvenster van Wireshark bestaat van boven naar onder uit onderstaande onderdelen:

* Het menu
* De toolbar
* De filter toolbar
* Het packet list paneel
* Het packet list detail paneel
* Het packet list byte panel
* De statusbalk

1. De gecapteerde pakketten worden standaard volgens welbepaalde regels gekleurd.

Welk soort pakketten hebben een lichtgroene kleur? http-pakketten

Welk soort pakketten hebben een lichtblauwe kleur? TCP- en UDP-pakketten

Welke kleur hebben de ICMP-pakketten? Roze

Tip: gebruik het menu View > Coloring Rules om het antwoord te vinden.

1. Meestal ben je niet geïnteresseerd in alle pakketten, maar in een bepaald soort pakketten. Je kan het aantal pakketten beperken door gebruik te maken van een **display filter** die je moet intikken in de filter-toolbar (onder de gewone toolbar).

Zorg er mbv een display filter voor dat enkel de DNS-pakketten getoond worden in het packet list paneel.

dns intikken in filter toolbar + op Enter drukken

Hoeveel dergelijke pakketten zijn er? Je kan dit aantal terugvinden in één van de onderdelen van het Wireshark-venster…

182

1. Bewaar deze gefilterde pakketten in een apart bestand met als naam ***dns-packets.***

Menu File – Export specified packets – all packets – displayed

Open daarna dit nieuwe bestand om te controleren of het inderdaad enkel DNS-pakketten bevat.

1. Sluit daarna het DNS-packets bestand en keer terug naar het capture1 bestand.

Verwijder daarin de display filter zodat je weer alle pakketten te zien krijgt.

Op het kruisje klikken achteraan in de filter toolbar

1. In Wireshark kan je ook gebruikmaken van de zoekfunctie om naar welbepaalde pakketten te zoeken.

Welke toetsencombinatie kan je hiervoor gebruiken?

Ctrl-F

Maak hiervan gebruik om alle ICMP-pakketten op te sporen en noteer hieronder hun nummers.

**Pakketnummers =** 205 en 2352

1. Je kan ook binnen het dataveld van een pakket naar een welbepaalde **string** (woord, tekst, …) zoeken, op voorwaarde dat je dit expliciet aanduidt in het veldje vòòr het invulvak van de zoekfunctie (zie figuur hieronder).

Zoek op deze manier naar de string *user* in de packet bytes van het capture bestand.

Tip: maak hierbij gebruik van onderstaande selecties:



Wat is het nummer van het eerste pakket dat aan je zoekvoorwaarden voldoet?

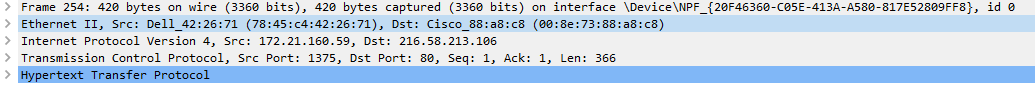
**Pakketnummer =** 206

1. Selecteer pakket **nr 254**. Doe dit door een toetsencombinatie in te drukken. Welke?

Tip: open het menu ***Go***.

**Toetsencombinatie =** Ctrl-G

1. Plak hieronder het detail pane van dit pakket.



Dit detail pane bestaat uit 5 regels die kunnen opengeklapt worden (door op het groter-dan-teken te klikken) om nog meer detailinfo te zien.

De eerste regel bevat algemene info over het pakket.

De tweede regel bevat TCP/IP Layer 1 (OSI layer 1 en 2) headerinformatie.

De derde regel bevat TCP/IP Layer 2 (OSI layer 3) headerinformatie.

De vierde regel bevat TCP/IP Layer 3 (OSI layer 4) headerinformatie.

De vijfde regel bevat de TCP/IP Layer 4 (OSI layer 5 tem 7) headerinformatie en de data van het pakket.

1. Van welke 4 protocollen wordt er in die frame (nr 254) gebruikgemaakt? Situeer deze protocollen **in het TCP/IP-model** door de namen ervan in de 2de kolom van onderstaande tabel in te vullen.

|  |  |
| --- | --- |
| **TCP/IP layer number and name** | **Protocol name** |
| L4: Application Layer | HTTP |
| L3: Transport Layer | TCP |
| L2: Internet Layer | IP |
| L1: Network Access Layer | Ethernet |

1. Vul in de eerste tabel hieronder de namen van de protocolheaders die vòòr het HTTP-dataveld van deze frame (nr 254) staan. Noteer onder elke veld ook hoeveel bytes groot dat veld is.

Vul in de tweede tabel hieronder de aangeduide (sub)velden van deze headers in. In die tabel staan enkel de belangrijkste (sub)velden (er zijn dus nog andere velden die niet in deze tabel opgenomen werden).

Gebruikte afkortingen:

* SA = Source Address
* DA = Destination Address
* SP = Source Port
* DP = Destination Port

|  |  |  |  |
| --- | --- | --- | --- |
| Ethernet HEADER | IP HEADER | TCP HEADER | HTTP DATA |

14 B 20 B 20 B 366 B

DA SA SA DA SP DP

|  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- |
| 00:8E:73:88:A8:C8 | 78:45:C4:42:26:71 | 172.21.160.59 | 216.58.213.106 | 1375 | 80 | HTTP DATA |

1. Wie heeft de netwerkkaarten van de zender en de ontvanger van frame nr 206 gefabriceerd?

Tip: dit is Layer 1 info.

**Fabrikant NIC v/d zender =** Dell

**Fabrikant NIC v/d ontvanger =** Cisco

1. Wireshark kan ook gebruikt worden om live te capteren.

Ga hiervoor als volgt te werk om de pakketten te capturen die door een PING-commando uitgestuurd en ontvangen worden.

* Sluit in Wireshark de geopende file (zonder Wireshark af te sluiten).
* Dubbelklik in het welkomstscherm van Wireshark onder rubriek “Capture” op je draadloze NIC om het capteren te starten.
* Ga naar de command-prompt van je host en ping er naar de computer met IP-adres 172.21.1.111. Wacht tot je alle reply’s gekregen hebt.
* Ga terug naar Wireshark en stop het capteren. Dit kan heel snel met de rode knop in de werkbalk.

1. Het zou best kunnen dat niet alle gecapteerde pakketten een gevolg zijn van je PING-commando.

Het PING-commando steunt op het gebruik van het ICMP-protocol. Toon daarom enkel de ICMP-pakketten **die het gevolg zijn van je PING-commando**.

Onderstaande filter toepassen:

icmp and ip.addr eq 172.21.1.111

Hoeveel ICMP-pakketten werden er gecapteerd?

8

Leg uit waarom juist dit aantal ICMP-pakketten gecapteerd werd.

Het Windows PING-commando stuurt 4 testpakketten (echo requests) naar de computer met het aangeduide IP-adres en op elk van deze 4 testpakketten zal die computer een antwoord (echo reply’s) terugsturen. Dus in totaal 4 + 4 = 8 pakketten.

Is het MAC-adres van de bestemming in de gecapteerde echo request pakketten, het MAC-adres van de gepingde computer (dus deze met IP-adres 172.21.1.111), of is dat het MAC-adres van de default gateway?

Default gateway

Verklaar je antwoord. Geef voldoende uitleg!

De computer met adres 172.21.1.111 behoort niet tot hetzelfde netwerk als je laptop, dus zal je laptop de ICMP-pakketten naar de default gateway sturen.

Reden waarom de computer niet tot hetzelfde netwerk als je laptop behoort: je laptop heeft een IP-adres dat begint met 172.31 en vermits het bijhorend subnetmasker 255.255.255.0 is (cfr output van het ipconfig-commando), betekent dit dat een computer tot je eigen netwerk behoort als de eerste 3 getallen van een IP-adres dezelfde zijn van je eigen IP-adres (en dit is hier dus duidelijk niet het geval).

1. Bekijk ook eens het data-gedeelte van zo’n ICMP-pakket in het packet list byte panel. Welk soort tekens zitten daarin?

(Kleine) letters van het alfabet.