# Het TCP/IP- en het OSI Model in actie

**Achtergrond**

Alvorens data door het netwerk reist, wordt het in stukjes opgesplitst. Algemeen noemen zo een stukje een PDU (Protocol Data Unit). Elke PDU krijgt een volgnummer, zodat de PDU’s weer aan elkaar kunnen worden geregen zodra ze op de bestemming aankomen. Afhankelijk van op welke laag de PDU zich bevindt, wordt dit met een andere naam aangeduid. Op laag 1 spreekt men van bits, op laag 2 van frames, op laag 3 van packets, op laag 4 van segmenten.

Wireschark is een netwerksniffer. Al de data die de sniffende netwerkkaart passeert, wordt getoond in deze applicatie. Ook de data die niet voor het ‘sniffende’ toestel bestemd is. Zo kun je de protocolinformatie en de data bekijken.

De volgende stappen leiden je door het proces van het opvragen van een webpagina van een webserver met behulp van de webbrowser-applicatie die beschikbaar is op een client-pc.

Hoewel veel van de weergegeven informatie later meer in detail zal worden besproken, is dit een gelegenheid om de functionaliteit van Wireshark te verkennen en de encapsulatie zichtbaar te maken.

## **1     Onderzoek van HTTP Web Traffic**

**Stap 1:**     **Genereer web (HTTP) traffic en ‘snif’ dit verkeer.**

1. Start Wireshark.
2. Onder *Capture,* kies je de Wifi interface.
3. Open de webstite <http://www.airindia.in/>

http is een applicatielaag-protocol dat data verstuurt in niet geëncrypte tekst. Vandaag zullen de meeste websites een ander protocol gebruiken zodat de verstuurde tekst wel geëncrypt wordt. Airindia zal een goede reden hebben om dit niet te doen (ondersteuning voor zeer oude browsers ???). Wij maken in deze opdracht dankbaar gebruik van deze website alhoewel vandaag http om bovenstaande reden steeds minder gebruik wordt!

1. Druk enkele keren op het *refresh*-symbooltje van je browser (wacht telkens tot de pagina opnieuw geladen is alvorens opnieuw te *refreshen*!).
2. Druk op het rode vierkantje in de knoppenbalk om het ‘sniffen’ te stoppen.

**Stap 2:**     **Onderzoek de inhoud van een HTTP packet.**

**De data**

1. Onder de knoppenbalk vind je een veld met daarin de tekst ‘Apply a display filter …’, typ hier **http** . Je zal nu enkel PDU’s zien die uitgewisseld zijn tussen de http-protocollen op de communicerende computers.
2. Speur naar een http-PDU met **line-based text data**. Je kan die herkennen door in de kolom **Info** te zoeken naar een vermelding **(tekst/html).**
3. Klik op een dergelijk pakketje en speur in het onderste veld voor **Line-based textdata : tekst html ( …. lines)** . Kies bij voorkeur een pakketje met minstens 100 lijnen.
4. Duid in het onderste veld met de muis het lijntje **Line-based textdata : tekst html ( …. lines)** aan en ga linksboven naar **File > Export Packet bytes …** . Een nieuw venster gaat open.
   1. Kies een bestandsnaam: **Data.htm,**
   2. bij **Opslaan als**: **All files (\*.\*)**
5. Open het bestand met een browser. Wat zie je? Accentueer je antwoord met fluo.

Html pagina met tekst

Je hebt zonet de ***data***in het pakketje bekeken. Al de overige informatie die je ziet in *Wireshark* is protocolinformatie. Die werd toegevoegd door de verschillende protocollen als de data werd voorbereid om verzonden te worden. Deze extra informatie is de ***overhead****. Overhead*  is informatie die mee verstuurd wordt over het netwerk maar niet wezenlijk tot de *data*  behoort.

Vergelijk het met een brief. De tekst in de brief is de *data*. De aanspreking in de brief ( Beste, Geachte, … ) de afsluiting in de brief ( Met vriendelijke groeten, hoogachtend, …), de informatie op de enveloppe (het adres van de bestemmeling, het adres van de ontvanger, de postzegel, de poststempel,…) is allemaal informatie die meegestuurd wordt maar niet wezenlijk hoort tot de *data* behoort: het is de ***overhead***. Deze ***overhead***wordt door de post om de brief te bezorgen.

Bij netwerkcommunicatie wordt de *overhead* gebruikt door de hardware en software van het netwerk om de data ter plaatse te krijgen. Het bevat adresinformatie, maar ook informatie die kan gebruikt worden door allerlei controlemechanismen.

Om datacommunicatie te beschrijven, maakt men gebruik van modellen. Twee veelgebruikte modellen zijn het **7-lagig OSI-model** en het **4-lagig TCP/IP** model. **Netwerktechnologie**, zowel de **hardware** als **de software** die in een netwerk gebruikt worden en hoe deze samenwerken, worden vaak uitgelegd a.d.h.v. deze modellen.

Voorbeelden van **hardware zijn de toestellen( je netwerkkaart, routers, switchen, accesspoints, kabels, …),** voorbeelden van software zijn **browsers, outlook, maar ook software op de routers, bvb. routing protocollen, … of op switchen, bvb. STP,… ).**

|  |  |
| --- | --- |
|  |  |

|  |  |
| --- | --- |
|  | Wanneer data v**erzonden** wordt stroomt het door het model van **boven naar beneden door het model.** Op elke laag waar de data passeert, zal een protocol de data niet wijzigen maar extra informatie aan deze ontvangen data toevoegen. Dit proces noem we de **encapsulatie/*encapsulation.***  De hoeveelheid data die een protocol van bovenuit ontvangt, is de ***payload*.** De informatie die het protocol voor de data plaatst, noemen we de (protocol)**header.** Hoeveel informatie het protocol toevoegt, wordt gegeven door de **header length.** |

**De *protocoloverhead***

In wat nu volgt, onderzoeken we enkele velden met protocolinformatie. We gebruiken hierbij het TCP/IP-model.

1. Klik in *Wireshark* terug op het http-pakketje met de tekst.
2. In het onderste veld naast het pijltje (>) verschijnen de namen van de protocollen die gebruikt zijn bij het verzenden van de data. Welke protocollen werden er gebruikt? Accentueer je antwoord in fluo.

Hypertext Transfer Protocol, Transmission control protocol, internet protocol version 4

1. Schrijf a.d.h.v. de figuur van het TCP/IP-model naast elk protocol op welke laag of lagen van het TCP/IP-model dit protocol actief is. Gebruik de figuur van het TCP/IP-model. Accentueer je antwoord in fluo.

HTTP : applicatie laag

TCP : transport laag (header)

IPV4 : Netwerk laag

**TCP**

1. Klik het pijltje (>) naast Transmission Control Protocol (beter bekend als TCP). De protocolinformatie toegevoegd door TCP wordt zichtbaar.

Op je computer of op een server zijn meerdere netwerkapplicaties actief. Om de netwerkapplicaties op één enkele computer te onderscheiden, hebben die allemaal een eigen ‘adres’ op deze computers. We noemen deze adressen ‘poorten’.

Beantwoord de volgende vragen. Accentueer je antwoorden in fluo.

* 1. Wat is de source port?

80

* 1. De source port is dat de poort van de zendende of de ontvangende applicatie?

Zendende

* 1. Wat is de destination port?

51984

* 1. De destination port is dat de poort van de zendende of de ontvangende applicatie?

ontvangende

1. Onderzoek de poorten die in gebruik zijn op je computer (enkel voor Windows OS).
   1. Open een opdrachtregel*/ command line* op je pc.
   2. Typ het commando **netstat -a -n**  gevolgd door enter.

Scroll door de output van dit commando.

Elk rijtje dat je ziet in de output, is een sessie tussen 2 netwerkapplicaties. De rijtjes die beginnen met TCP zijn applicaties die gebruik maken van TCP. De rijtjes die gevolgd worden door LISTENING zijn niet actief en wachten op een inkomende sessie. De lijntjes gevolgd door ESTABLISHED zijn actieve sessies tussen applicaties op jouw computer en een andere computer.

1. Zoek in de TCP-protocolinformatie naar *Sequence number .* Wat zou de betekenis van deze informatie zijn? Accentueer je antwoord in fluo.

Het is een willekeurig gekozen volgnummer. (24949)

1. Hoeveel bytes aan data ontvangt TCP van het protocol *Hypertext Transfer Protocol* (beter bekend als http)? In welk veld staat deze informatie? Accentueer je antwoord in fluo.

663 bytes. Dit vind je in dit geval onder het TCP payload veld

1. Hoeveel bytes aan data voegt TCP toe aan de informatie ontvangen van *Hypertext Transfer Protocol?* In welk veld staat deze informatie? Accentueer je antwoord in fluo.

20 bytes. Dit vind je in het Header Length veld van TCP

1. Hoeveel is de payload in TCP? Accentueer je antwoord in fluo.

663 bytes

**IP**

1. Klik het pijltje (>) naast Internet Protocol Version 4 (beter bekend als IP). De protocolinformatie toegevoegd door IP wordt zichtbaar.

Op een IP-netwerk als het internet moet elke computer een uniek adres hebben. Dit is het ip-adres.

1. Zoek in de IP-protocolinformatie naar source. Dit is het ip-adres van de de computer die de data zendt. Wat is de waarde? Is dit het adres van de webserver of het adres van jouw computer. Accentueer je antwoord in fluo.

92.122.122.137, adres webserver

1. Zoek in de IP-protocolinformatie naar Destination. Dit is het ip-adres van de de computer die de data ontvangt. Is dit het adres van de webserver of het adres van jouw computer. Wat is de waarde? Accentueer je antwoord in fluo.

172.16.197.219, adres van mijn computer

1. Hoeveel bytes aan data ontvangt IP van het protocol TCP? Hoe heb je deze informatie gevonden? Accentueer je antwoord in fluo.

663 bytes. Dit bereken je door de TCP payload en de Header Lenght van de TCP op te tellen. Je kan dit verifiëren door onder te tab IP naar “Total Lenght” te gaan kijken en daarvan de Header Length van het IP af te trekken.

1. Hoeveel bytes aan data voegt IP toe aan de informatie ontvangen van TCP*?* In welk veld staat deze informatie? Accentueer je antwoord in fluo.
2. Onder het tab IPv4 vind u een veld genaamd “Header Length”. Dit bedraagt 20 bytes.

**Ethernet**

Klik het pijltje (>) naast Ethernet II.

1. Welk is het adres van je computer? Het *source* of het *destination* adres?

Het destination adres

1. Zijn dit laag 2-adressen of laag 3-adressen? Verklaar je antwoord.

Dit zijn laag 2-adressen omdat het MAC-adressen zijn die in de datalink laag vallen.