# Labo http(s)

## HTTP(2)

**1. Welke versie van HTTP wordt door deze webserver gebruikt?**

*HTTP1.1*

**2. Is de connectie die je maakt met de webserver persistent ?**

*Persistent, 1.1 altijd + keep alive*

**3. Is er een beperking voor het starten van het programma met bepaalde poort, probeer en verklaar.**

*Ja, sommige poorten zijn voorzien van bepaalde services*

**4. Met welke client poort wordt hier verbonden?**

*53028, 53027*

**‐ Is dit eenmalig, of worden er nog verbindingen gemaakt?**

*Meerdere verbindingen*

**‐ Indien ja: welke verbindingen, met welke clientpoort?**

*53027*

**5. Welke HTTP method wordt gebruikt?**

*GET*

**6. Wat staat er in het cookie?**

*Cookie : Name=DSN\_PROG\_IOT Koekje van eigen deeg domain=home.lec* [*http://10.150.195.44:8080/*](http://10.150.195.44:8080/) *expires=20/10/2022 16:43:51 Language=dutch Content=Laurent Koen </p> </form>*

**7. Is dit een persistent cookie ?**

*Nee*

**‐ Vervalt dit cookie? Wanneer ?**

*20/10/2022 16:43:51*

## HTTP(3)

**1. Welke lagen van het TCP/IP model zijn vertegenwoordigd in het pakketje?**

5, fysieke laag, datalinklaag, netwerklaag, transportlaag, applicatielaag

**2. Uit hoeveel bytes bestaat het pakketje?**

659

**3. Wat is het IP adres van de server?**

193.191.180.79

**4. Wat is het MAC adres van de client?**

f4:b7:e2:77:25:5e

**5. Naar welke serverpoort wordt dit pakket verzonden?**

80

**6. Met welk protocol komt dit poortnummer overeen?**

HTTP

**7. Welke versie van het HTTP protocol werd gebruikt in deze communicatie?**

HTTP1.1

**8. Welke URL wordt er opgevraagd?**

www.bpost.be/nl/faqs

**9. Welke method wordt er gebruikt?**

GET

**10. Hoeveel headerlijnen bevat deze request?**

9

**11. Hoeveel data zit er in deze request?**

605 bytes

## HTTP(4)

**1. Stel bovenaan een display filter in zodat enkel de pakketjes van het HTTP protocol zichtbaar**

**blijven.**

**2. Welke website werd er bezocht?**

www.kowaja.be

**3. Geef een lijst van de embedded content die mee opgehaald wordt in deze HTTP stream**

Ruler.gif

Dtree.css

/gifs.folder.gif

/gifs/joinbottom.gif

**4. Welke opgevraagde file kon er door de server niet gevonden worden?**

Dtree.css

**5. Uit welke statuscode kan je dit afleiden?**404 not found

**Ga op een HTTP pakketje staan, rechts klik en kies voor “Follow” → "HTTP stream"**

**1. Wanneer is de homepage van de website voor de laatste keer aangepast?**

Woensdag 2 juni 2004 21:58:55 GMT

**2. Wanneer werd de website bezocht?**

Vrijdag 27 september 2019 09:29:38 GMT

**3. Welke font-family wordt er op de website gebruikt?**

Centaur

**4. Wat is het mailadres van de eigenaar / maker van deze website?**kowaja@pandora.be

## HTTP(5)

**Sluit de HTTP stream en kies bovenaan Wireshark voor “File” → “Export Objects” → "HTTP"**

**1. Hoeveel objecten zie je in de lijst?**

7

**2. Zijn deze allemaal succesvol via HTTP overgebracht?**

Nee

**3. Welke objecten uit deze lijst werden niet correct overgebracht van de server?**

dtree.css niet

**4. Wat is de reden dat het fout liep?**

Not found

**5. Wat is het grootste object?**

Ruler.gif

**6. Bewaar dit en open het door erop te dubbelklikken. In welk programma doet je computer dit**

**bestand open?**

Foto’s (images)

**7. In welk frame van de HTTP stream zit dit grootste object**

23

**• Ga naar de Wireshark hoofdinterface en klik op dit frame. Hoe toont Wireshark dit object**

**daar?**

Data blocks

**• Rechts klik in dit frame op de HTTP payload en kies voor “show packet bytes” en speel eens**

**met de “show as” parameter.**

## HTTP(6)

**• Open het http3 Wireshark bestand dat op Digitap ter beschikking staat.**

**1. Welke status code zie je in deze stream die je in de vorige oefeningen nog niet bent**

**tegengekomen?**

304 (not modified)

**2. In welk frame zie je deze status code staan?**

2

**3. Waarom antwoord de server hiermee (als reactie op welke header line in de clien request)?**

‘If-modified-since: wed, 02 jun 2004 21:58:55’ enkel dan wordt het weergegeven. Dit is echter niet het geval

**4. Welke sitepagina wordt er in frame 5 opgevraagd?**

www.kowaja.be/contact.html

**(• Open een browser en surf naar de pagina waarvan sprake is in frame 5**

**‐ Vul het bovenste formulier in maar druk nog niet op "verstuur"**

**‐ Open Wireshark en start een capture**

**‐ Klik op "verstuur" in het bovenste formulier**

**‐ Stop de Wireshark capture**

**‐ Kan je de ingevulde gegevens ergens terugvinden?**

**• Welke method wordt er gebruikt)**

* Niet meer mogelijk, http wordt hoe langer hoe minder gebruikt.

## HTTPS(1)

**Open oefentrace\_https\_1 (download van digitap)**

**1. Welk protocol wordt hier gebruikt ?**

https

**2. Op welke laag van TCP/IP-model is dit actief?**

applicatielaag

**3. Op welk L5 protocol is dit gebaseerd?**

HTTP

**4. Welke versie TLS wordt hier gebruikt?**

1.2

**5. Identificeer client hello**

**1. Welke versie geeft client als ondersteunde versie door ?**

TLSv1.2

**2. Geef 3 mogelijke versleutel algoritmes die de client ondersteunt**

Cipher Suite: TLS\_ECDHE\_ECDSA\_WITH\_AES\_256\_CBC\_SHA384 (0xc024)

Cipher Suite: TLS\_ECDHE\_ECDSA\_WITH\_AES\_256\_GCM\_SHA384 (0xc02c)

Cipher Suite: TLS\_ECDHE\_ECDSA\_WITH\_AES\_128\_GCM\_SHA256 (0xc02b)

Afbeelding met tekst

Automatisch gegenereerde beschrijving

**6. Op welke lijn staat de bijbehorende server hello?**

6e lijn

1. **Welk versleutel algoritme zal gebruikt worden ?**

Cipher Suite: TLS\_ECDHE\_RSA\_WITH\_AES\_256\_GCM\_SHA384 (0xc030)

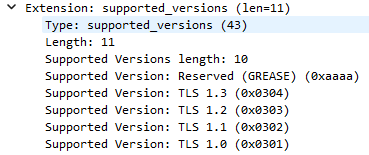
## HTTPS(2)

**1. Bekijk lijn 20 van de client hello, welke versie wordt hier gebruikt?**

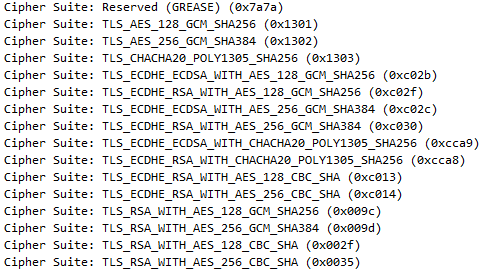
1.3

**1. Stelt de client nog andere versies voor ?**

1.3, 1.2, 1.1, 1.0



1. **Geef 3 mogelijke versleutel algoritmes die de client voorstelt**

****

1. **Zijn er andere versleutel algoritmes ten opzichte van onze eerste client hello?**

Ja, daarnet 19, nu 16

**2. Welke lijn staat bijbehorende server hello**

21e

1. **Welk versleutel algoritme wordt gebruikt?**

Cipher Suite: TLS\_AES\_128\_GCM\_SHA256 (0x1301)

## HTTPS(3)

**• De firma Nednoobs doet nog eens beroep op jullie expertise**

‐ **Ze hebben een paar websites www.netnoobs.be en bestelling.netnoobs.be, deze werken met een IIS webserver**

‐ **Deze zouden ze graag van een certificaat voorzien om bezoekers veilig te stellen.**

**• Welk type certificaat zou je hun aanraden?**

Multiple

**‐ Waarom?**

Verschillende namen met een ééndezelfde eindigende suffix

**• Formuleer ook een voorstel dat hen naar de toekomst meer uitbreidingsmodelijkheden voorziet**

**• Geef hiervoor een indicatie wat dit hen zou kunnen kosten**

• **Genereer een CSR bestand om dit certificaat te kunnen aanmaken**

## COOKIES(1)

**• Doe online research en beschrijf in je eigen woorden wat men wil zeggen met onderstaande termen:**

**‐ Session cookies**

Cookies die bijgehouden worden zolang de sessie (uw browser) aanstaat

**‐ Persistent cookies**

Cookies die blijven zelf nadat je sessie is afgesloten

**‐ First-party cookies**

Cookies die bijgehouden worden door de website die gebruikt kunnen worden voor data analyse

**‐ Third-party cookies**

Cookies die gebruikt kunnen worden door sites waar je momenteel niet op zit

**‐ Zombie cookies**

Cookies die nooit weggaan zelf als ze verwijderd zijn door de gebruiker, deze dienen als automatisch informatie verzamelen

**• In private of incognito browsing modus zal je browser geen aanwezige persistente cookies op je systeem gebruiken. Er kunnen wel cookies aangemaakt worden in deze browsing modus, maar bij het afsluiten van de browser, worden deze automatisch gewist (ook de nieuw aangemaakte persistente cookies). Er worden ook geen wachtwoorden of formulierdata opgeslagen in deze modus.0**

**‐ Zoek van jouw browser op hoe je een private of incognito sessie kan starten**

**‐ Zoek van jouw browser op hoe je deze automatisch in incognito of private modus laat starten.**

## COOKIES(2)

## COOKIES(3)

## COOKIES(4)

## BROWSER FINGERPRINTING

**• Zelfs als je alle cookies blokkeert, kunnen websites je identificeren als unieke gebruiker aan de hand van een techniek die fingerprinting heet.**

**• Lees dit artikel** [**https://www.consumentenbond.nl/internet-privacy/browser-fingerprinting**](https://www.consumentenbond.nl/internet-privacy/browser-fingerprinting) **en zorg dat je weet wat browser fingerprinting is**

**•Zoek zelf uit hoe uniek jouw browser fingerprint is op** [**https://amiunique.org/fp**](https://amiunique.org/fp)

**‐ Hoe lager bepaalde percentages, hoe unieker je bent**

**‐ Hoe unieker je bent, des te beter kunnen sites je traceren zonder cookies**

## CONTENT CACHING

**• Zoek online op hoe je voor jouw browser de lokale cache kan wissen.**

**• Surf naar https://refreshyourcache.com/en/cache-test/ en maak gebruik van de "reset the image" link die je daar ziet. Je moet "the red image" zien.**

**‐ Refresh je pagina (herladen)**

**‐ Wis je browser cache**

**‐ Refresh de pagina opnieuw (herladen)**

**‐ Welk gedrag neem je waar?**

## PROXY

**• Zoek op waar in jouw browser je de proxy-instellingen kan terugvinden**

**• Zoek een lijst van proxy servers die je zou kunnen instellen in je browser**

**• Zoek op of er ook online proxy servers bestaan die jouw surf requests kunnen afhandelen**

**• Welke redenen kan je bedenken waarom je wel of niet zou werken met een web proxy?**