

Wireshark

Netwerkpakketjes bekijken en opzoeken met Wireshark

1. Installatie Wireshark (of al gedaan?)
<https://www.wireshark.org/download.html>
Onder Windows ook pcap installeren (default optie)
2. Start Wireshark en kies Wifi in het start-up scherm.
Kijk wat er binnenkomt, herken je wat?
3. Start en stop capturing met het 'blauwe vinnetje' (start) en het 'rode vierkantje' (stop) links boven in het scherm.
[Start-stop-wireshark.jpg](#)

4. Sluit zoveel mogelijk internetverkeer af, browsers, Spotify etc.
Dit doe je om het netwerkverkeer zoveel mogelijk te beperken, zodat je straks eenvoudiger en sneller kan zoeken.
5. Start één browser (bij voorkeur Chrome) en open [pagina met geheime boodschappen](#)
Alle boodschappen/linkjes zijn gelijk maar gebruik elke keer een nieuwe boodschap zodat je zeker weet dat de pagina wordt geladen en niet uit de browser cache komt.
6. Ga naar Wireshark en druk op stop capture (rood vierkantje)
7. Start capture (blauwe vinnetje)
8. Laadt een boodschap (webpagina) door op een van de linkjes te klikken op e pagina die je net hebt geopend.
9. Stop de capture in wireshark (rode knopje links bovenaan)

10. Ga nu naar Wireshark en zoek naar het pakketje met het woord 'appelboom'.

[Wireshark find.jpg](#) unknown

- Edit – Find packet
- Display filter -> string
- Packet Details
- Zoek naar 'appel'

11. Gevonden? Als het goed is zie je nu dat je het pakketje (vrachtwagenlading) gewoon kunt lezen.

Stel voor dat je een wachtwoord op een website had ingevuld dan had elke router die je onderweg was tegengekomen dit kunnen lezen!

We kunnen dit voorkomen door in de browser het slotje te gebruiken. Dit doe je door in de URL (web address) HTTPS te gebruiken in plaats van HTTP.

Zoek op internet waar HTTP en HTTPS voor staan.

12. We openen nu opnieuw de [pagina met geheime boodschappen](#)

Maar zie je dat er nu HTTPS wordt gebruikt (en er een slotje voor het internet address staat)

Wat denk je? Kun je nu de 'geheime boodschap weer 'afluisteren?

13. Voer stap 6 tot en met 10 opnieuw uit maar nu met de boodschappen via een beveiligde verbinding.

Kun je de boodschap (appleboom) nu weer vinden?

-
1. Indien klaar:

lees theorie <https://773084957.netacad.com/>

en kies 18/19 Pilot serie, module 1.5

Vergeet de quiz aan het eind niet!

[boodschap01](#) [boodschap02](#) [boodschap03](#) [boodschap04](#) [boodschap05](#)
[boodschap06](#) [boodschap07](#) [boodschap08](#) [boodschap09](#) [boodschap10](#)

[boodschap11](#) [boodschap12](#) [boodschap13](#) [boodschap14](#) [boodschap15](#)
[boodschap16](#) [boodschap17](#) [boodschap18](#) [boodschap19](#) [boodschap20](#)

Revision #3

Created 17 August 2019 20:46:13 by Admin

Updated 17 August 2019 21:09:02 by Admin