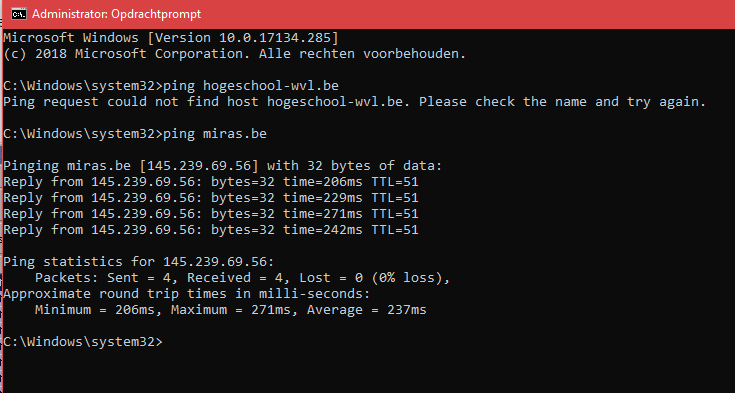
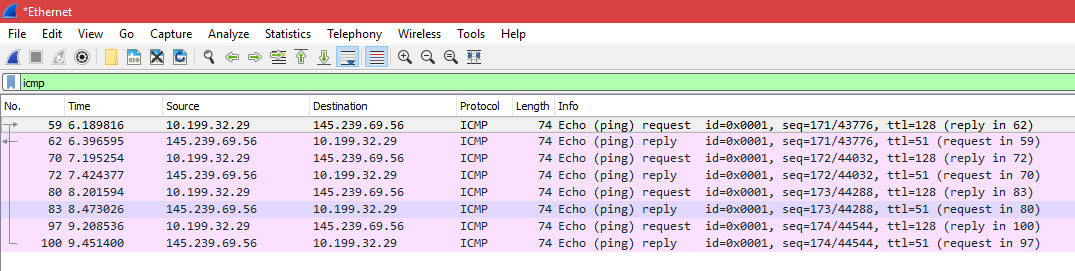
**Oefeningen Wireshark**

**Het IP-protocol**

1. Ping naar een website naar keuze ( miras.be )

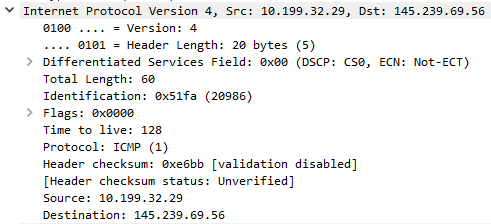


1. Gebruik een filter in Wireshark om enkel de 8 ping-pakketten te zien.

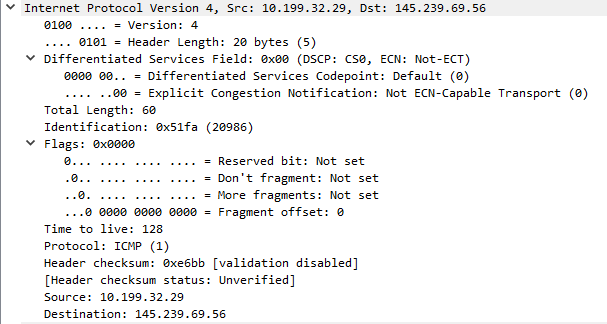


1. Welk IP-adres heeft je laptop en welk IP-adres heeft onze brustud server?

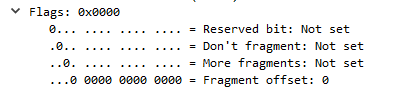
Source = mijn IP-adres en Destination = miras.be



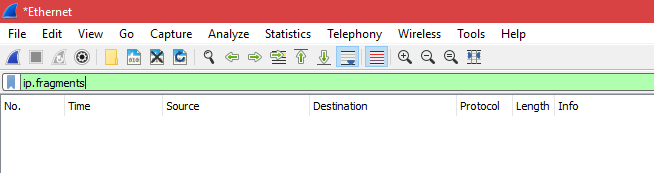
1. Geef de waarde van onderstaande velden uit de IP-header van het eerste echo request pakket.



1. Werd er bij dit IP-pakket gefragmenteerd? Hoe weet je dat?

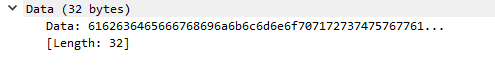


Als je volgende filter gebruikt krijg ik geen resultaat dus werden er geen pakketten gefragmenteerd



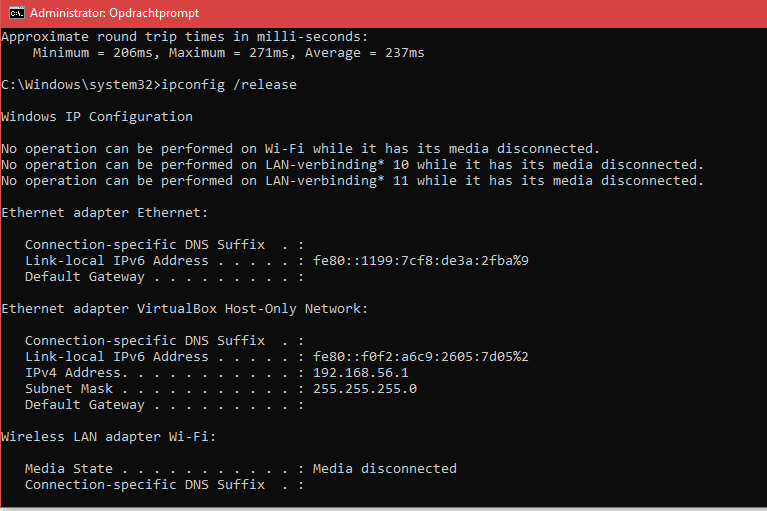
1. Geef de waarde van de IP-payload van het laatste echo request pakket.

Dit vind je onder Internet Control Message Protocol tab en dan bij Data.

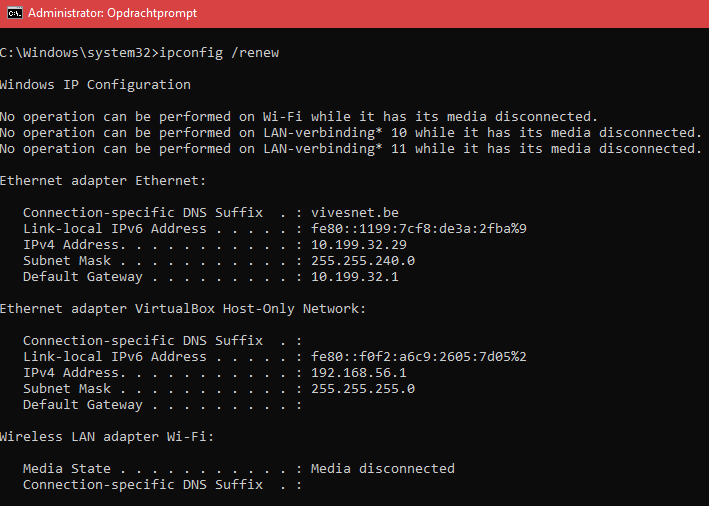


**Het DHCP-protocol**

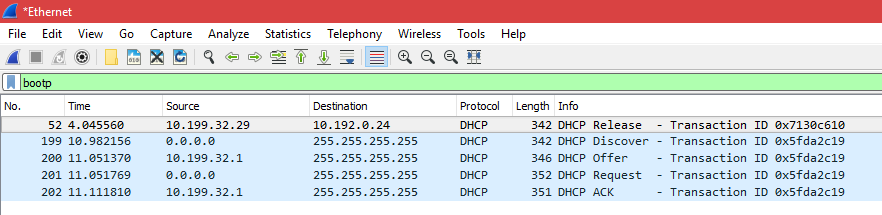
1. Geef met behulp van een commande je IP-adres vrij.



1. Hernieuw met behulp van een commando je IP-adres.



1. Gebruik een gepaste filter in Wireshark om enkel de DHCP gerelateerde pakketten te bekijken.



1. Welk van die pakketten zijn unicasts? Welke zijn broadcasts? Waarom is dat zo?

-Discover = Broadcast

-Offer = Unicast

-Request = Broadcast

-ACK = Unicast

Dit is volgens cisco handboek maar zoals je ziet is alles in broadcast gedaan.

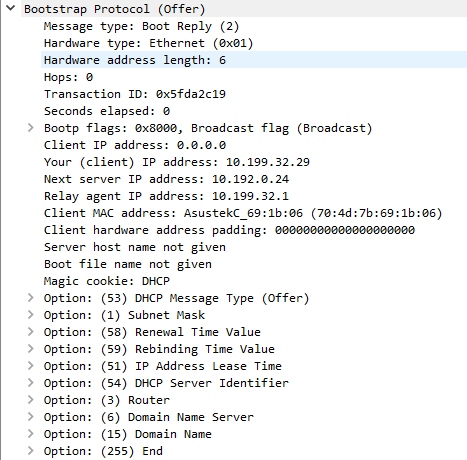
1. Ga na of je laptop inderdaad vraagt om terug zijn reeds eerder gebruikt IP-adres te mogen gebruiken.

Als je bij het request pakket kijkt en dan op bootstrap protocol > Option requested IP address klikt kan je zien dat hij zijn oude ip-adres terugvraagt.



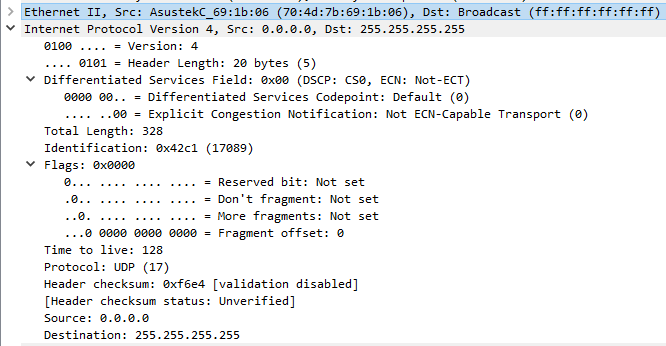
1. Welke DHCP opties worden er nog door de DHCP server aan de DHCP client meegegen?

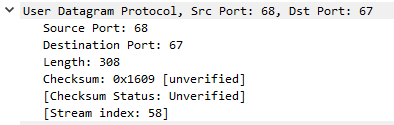
Bij het offer pakket kan je bij bootstrap protocol alle options openklikken en kijken welke informatie mee gegeven word.



1. Ga ook na van welk transportlaag protocol DHCP gebruikmaakt: TCP of UDP.

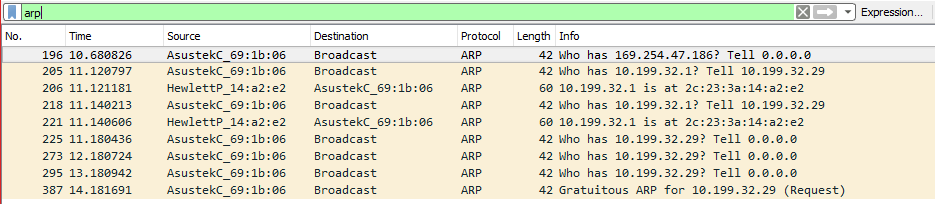
Welke poorten gebruikt DHCP hierbij?



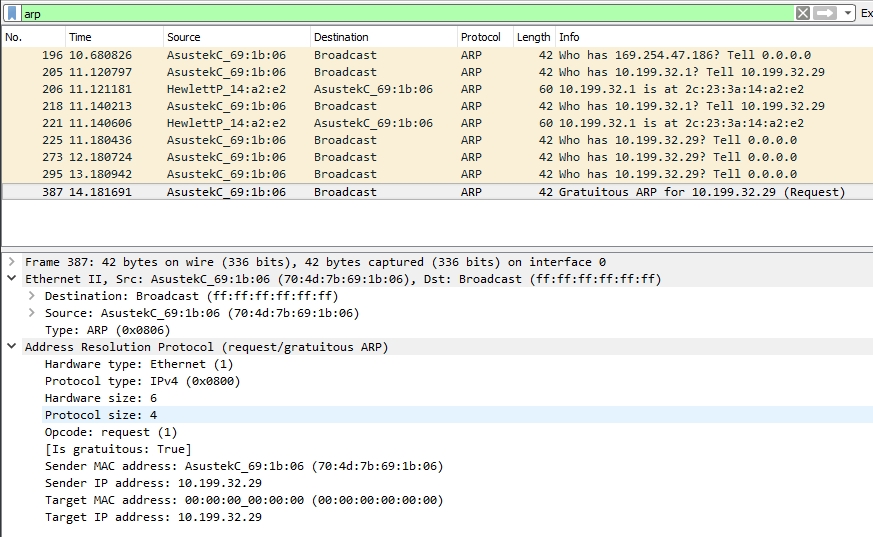


**Het ARP-Protocol**

1. Filter op ARP-pakketten

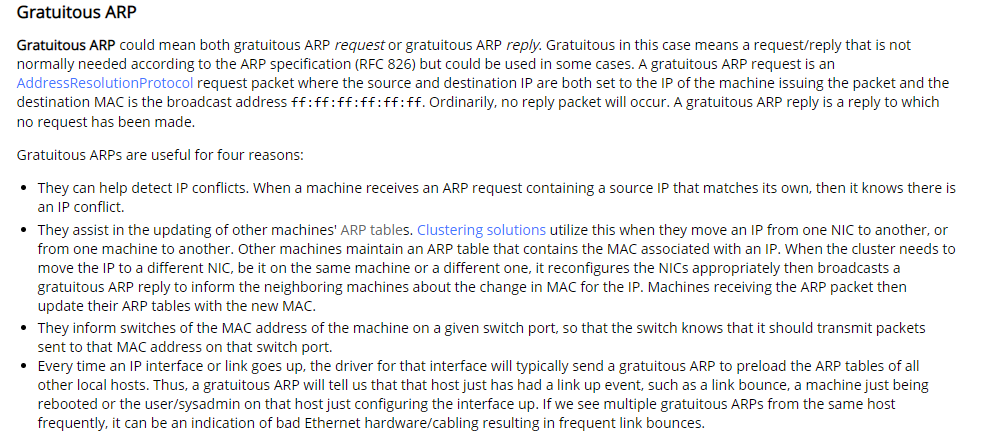


1. Zijn de meeste ARP-pakketten ARP-requests of ARP-reply’s? Waarom is dat zo?



Er zijn meer request dan reply’s (zie Opcode) omdat enkel de betrokkene antwoord heeft.

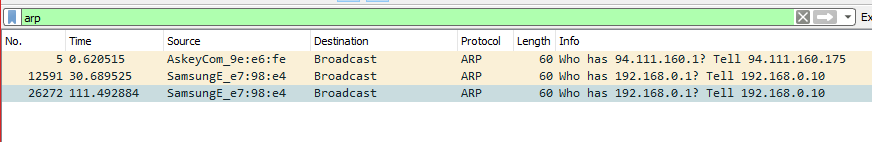
1. Tussen de gecapturede pakketten zitten er enkele zogenaamde “gratuitous” ARP-reply pakketten. Waarvoor worden die pakketten gebruikt?



Bron is van <https://wiki.wireshark.org/Gratuitous_ARP>

Voor de volgende oefening krijg ik geen reply ARP pakketten dus kan ik deze niet doen.

Ik heb ook op wiki wireshark proberen te zoeken waarom ik geen pakketten krijg maar vind er niets over. Deze 3 pakketten zijn de enige die ik kreeg na 10tallen websites te surfen

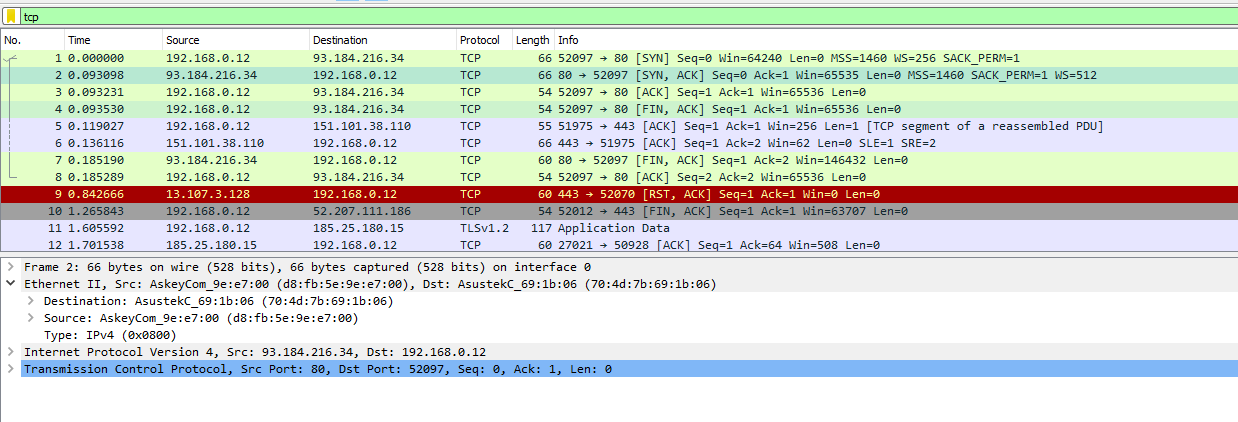


**Het ARP-Protocol**

1.Capture sessie

2. Surf naar [www.howest.be](http://www.howest.be) en klik op een link. Stop sessie.

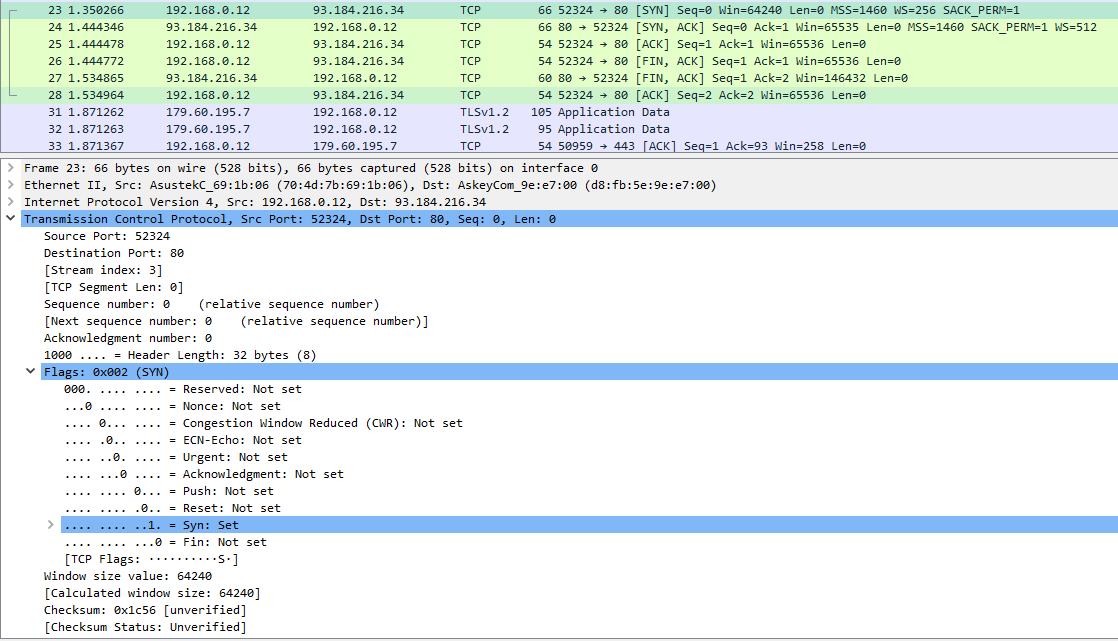
3. Filter op TCP-pakketten



1. Ga na of je de 3-way handshake procedure van de initialisatie van de TCP-sessie kunt terugvinden. Besteed hierbij de nodige aandacht aan het gebruik van de TCP-flags.



Zoek nu naar het pakket met SYN,SYN+ACK en ACK. Klik op Transmission Control Protocol en dan flags.



Ik zie die 02hex -> 00000010 nergens staan.

1. Welke poort gebruikt je laptop bij die TCP-sessie?



1. Ga na hoe de wisselwerking tussen sequence-en acknowledgementnummer gebeurt bij z’n surfsessie.

Bij pakket 1 staan het op 0



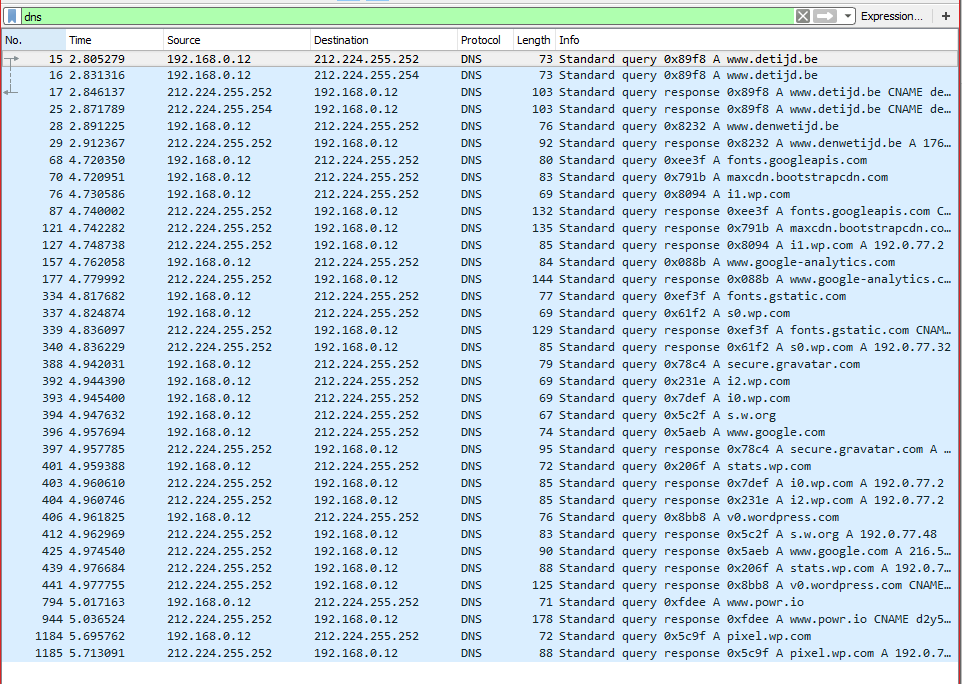
Als 0 bevestigd word dan staat het nummer op 1



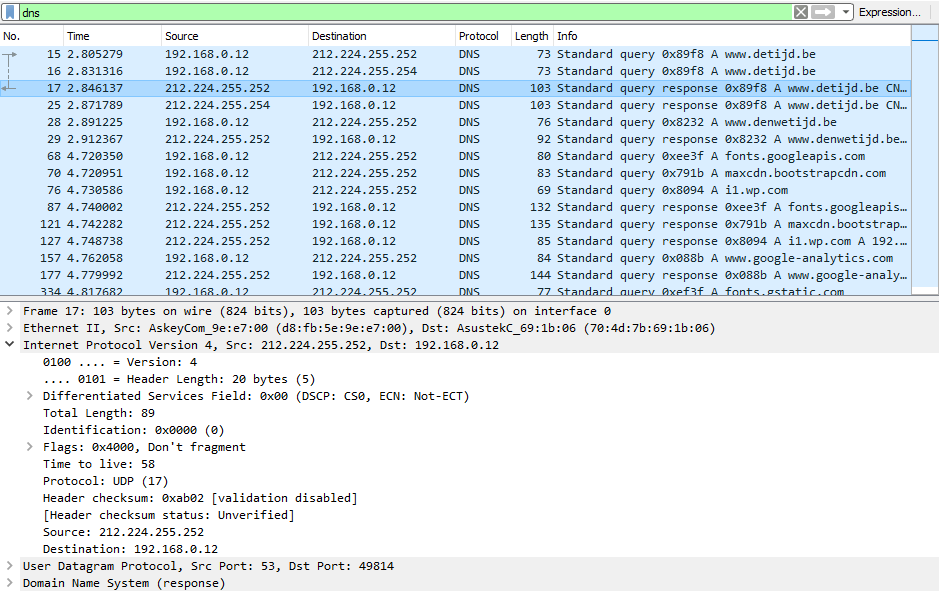
Dit is omdat hij een bevestiging van 1 verwacht.

**Het DNS-protocol**

1. Start sessie, surf naar [www.detijd.be](http://www.detijd.be) en stop sessie
2. Ga na dat je laptop een DNS-query gestuurd heeft naar een DNS-server met de vraag om de ingetikte DNS-naam naar een IP-adres te vertalen.



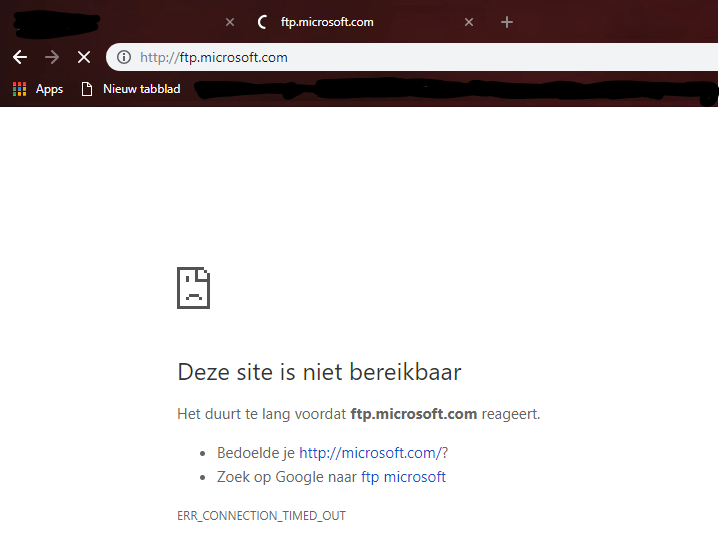
1. Zoek ook het antwoord op die DNS-query op om het IP-adres van die website te vinden.

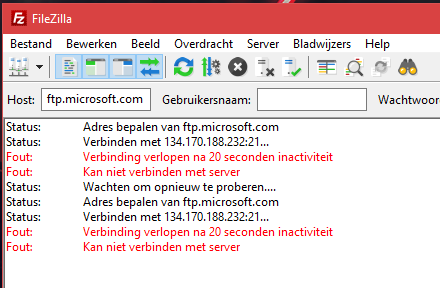


1. Van welk protocol maakt DNS gebruik: TCP of UDP? UDP
2. Welk wellknown port number wordt hierbij gebruikt? 53

**Het FTP-protocol**

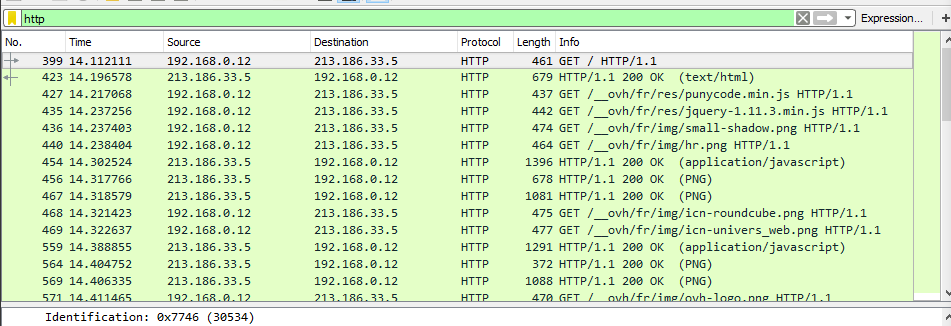
De link werkt niet meer voor deze oefeningen.



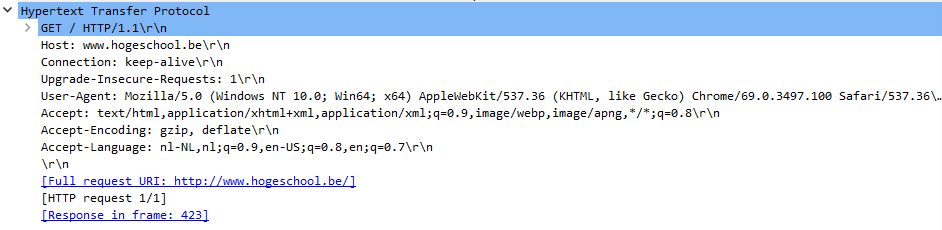


**Het HTTP-protocol**

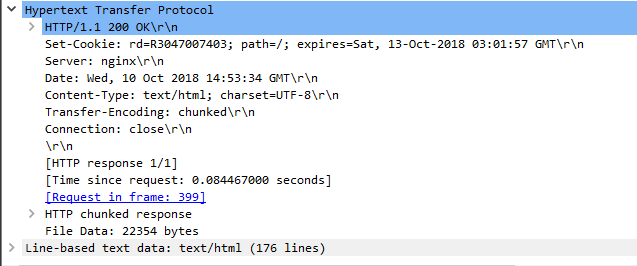
1. Start nieuwe sessie, surf naar [www.hogeschool.be](http://www.hogeschool.be) en stop dan je sessie
2. Filter op het HTTP-protocol



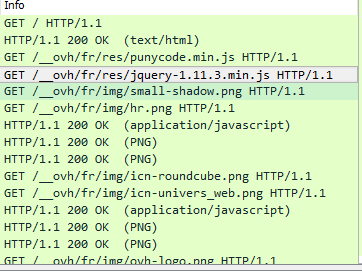
1. Open de eerste HTTP-request en led er onderstaande zaken uit af:



1. Open de HTTP-responce op deze request en leid er onderstaande zaken uit.



1. Ga na welke soort files er met behulp van de volgende HTTP-requests opgevraagd worden. Ga ook na of de webserver de gevraagde files ook effectief naar je browser doorstuurt. Indien niet : waarom niet?

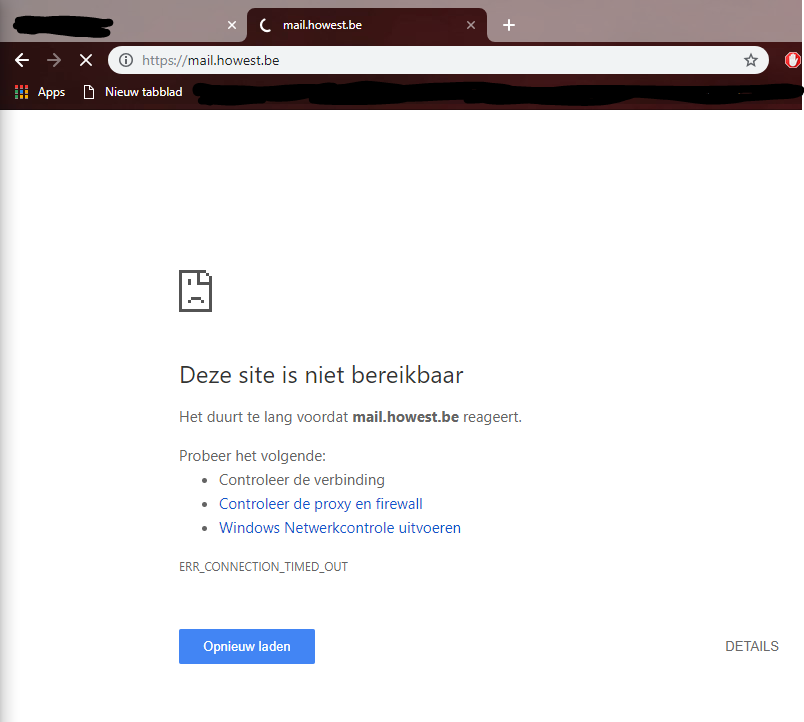


Met code 200 word bevestigd dat de files doorgestuurd zijn naar je browser. Zoniet zitten die bestand in je cache en zijn ze ongewijzigt.

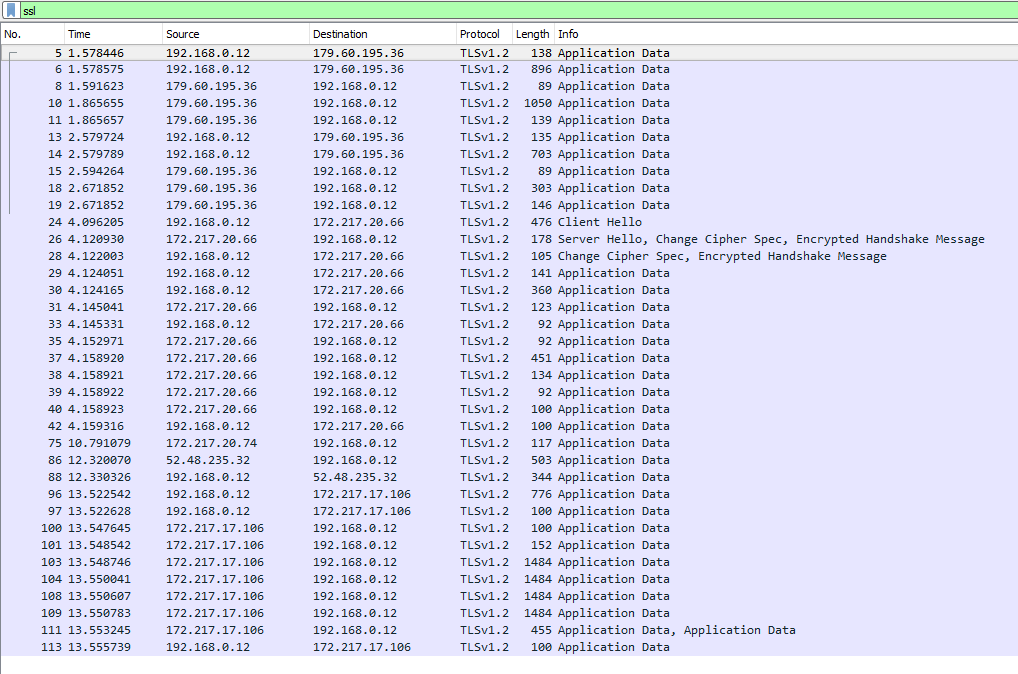


1. Start een nieuwe sessie en surft naar <https://mail.howest.be> en meld je aan. Stop de sessie

Deze link werkt niet.



1. Met behulp van welke expression kan je HTTPS verkeer(die gebruik maakt van TLSV1) filteren. Met SSL filter



Welke informatie over het certificaat dat door de webmailserver met je browser uitgewisseld word, kun je terugvinden? Normaliteit moet je die info ook via je browser kunnen opvragen..

Server Hello, Certificate, Certificate Status, Server Hello Done". Daar klik je dan bij details Secure Sockets Layer -> Handshake Protocol: Certificate -> Certificates

