Wireshark Oefeningen

Oefensessie 1 - Het IP-protocol

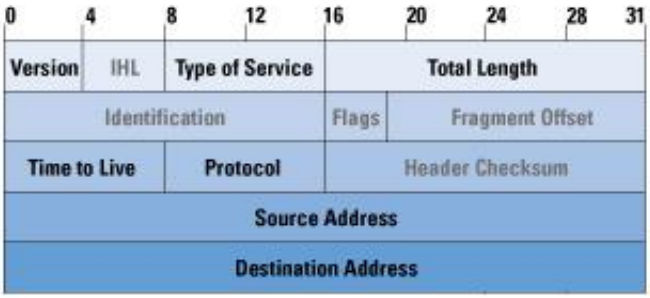
IP, Internet Protocol, wordt gebruikt in de Internetlaag van het TCP/IP-model. Het heeft als taak pakketten afkomstig van een zender via een packet-switched netwerk aan de bestemmeling af te leveren op basis van (IP-)adresinformatie.

Het is een connectieloos protocol, er wordt niet eerst via het netwerk een verbinding opgezet. de pakketten worden aan een node in het netwerk aangeboden en elk van deze nodes moet ze naar een volgende node versturen, zodat het pakket uiteindelijk ter bestemming zal geraken. Omdat er niet om een bevestiging van ontvangst gevraagd wordt, noemt men IP een send and pray protocol genoemd.

Momenteel zijn er 2 IP-versies gebruikt; IPv4 en IPv6. Die eerste gebruikt 32 bit IP-adressen en wordt het meest gebruikt. Maar omdat alle mogelijke adressen bijna in gebruik zijn, is men geleidelijk aan aan het overstappen naar IPv6 dat 128 bit adressen gebruikt. Zo zijn er veel meer mogelijke adressen.

Deze eerste oefening is om de samenstelling van een IP-pakket te bekijken. Er zijn twee grote onderdelen, de IP-header en de IP-payload. In deze laatste bevindt zich alle data die de gebruiker zelf opstuurde/ontving. De IP-header is samengesteld uit 20 bytes. Hierin staat onder andere het IP-adres van de zender en ontvanger, de versie van het IP-protocol die gebruikt wordt,...

IPv4 Header



IPv6 Header

Een IPv4-pakket kan 1500 bytes data bevatten, 20 voor de header, dus blijven er 1480 bytes over voor data. Aangezien 1480 bytes niet genoeg is voor een groot pakket in één keer door te sturen, wordt de data gefragmenteerd over verschillende pakketten.

Oefeningen

Start een Wireshark capturesessie.

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

Antwoord:

3. Welk IP-adres heeft je laptop en welk IP-adres heeft onze brustud server?
   Antwoord:

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

5. Werd er bij dit IP-pakket gefragmenteerd? Hoe weet je dat?
   Antwoord:

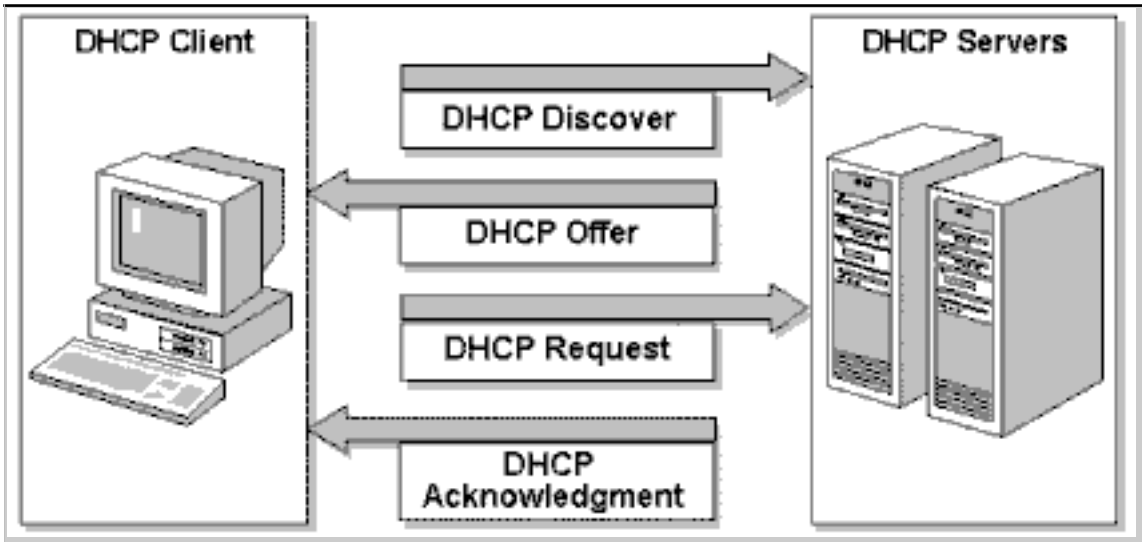
6. Geef de waarde van de IP-payload van het laatste echo request pakket. Antwoord:

Oefensessie 2 - Het DHCP-protocol

DHCP, Dynamic Host Configuration Protocol, is een protocol dat gebruikt wordt om automatisch tijdelijke IP-adressen aan hosts toe te kennen. Omdat private IP- adressen geen directe verbinding kunnen maken met een publiek adres, geeft de server één van zijn IP-adressen uit de pool aan de client. Deze IP-adressen zijn (meestal) slechts voor een bepaalde periode geldig, dit wordt de lease time genoemd. DHCP werkt volgens het Client/Server-principe, waarbij de server een pool IP-adressen bijhoudt. Elke Windows-computer heeft een ingebouwde

DHCP-client.

Een DHCP-client krijgt een IP-adres in 4 fasen.
Eerst doet de client een DHCPDISCOVER via IP-broadcasting. Hij vraagt aan verschillende servers (vandaar broadcast) om een IP-adres.
Daarna stuurt één of meerdere servers een DHCPOFFER terug. Deze bevat een voorstel van een IP-adres, IP-adres van de server, lease duration en een hoop opties. Ook deze DHCPOFFER's gebeuren via broadcast
Vervolgens stuurt de client een DHCPREQUEST naar één server en maakt zijn keuze via een IP-broadcast bekend. Zo weten andere servers dat de client al gekozen heeft. De server wordt gekozen op basis van snelste reactie, de eerste die een DHCPOFFER stuurde.
Tenslotte stuurt de server een DHCPACK via broadcast naar de client. Dit is een bevestiging dat die client dat toegewezen IP-adres kan gebruiken van die server.



Als een DHCP-client heropstart, verstuurt deze automatisch via een unicast een DHCP-request naar de server waarvan hij een IP-adres gekregen heeft. Dit heet DHCP-renewal. Dit gebeurt ook automatisch wanneer de helft van de lease time verlopen is. De DHCP-server antwoordt met een DHCPACK als de client dat IP-adres kan blijven gebruiken, anders stuurt die een DHCPNACK.

Elke Windows-computer gebruikt standaard ook APIPA, Automatic Private IP Adressing. Dit houdt in dat als een client geen antwoord krijgt op de DHCPREQUEST kent deze automatisch aan zichzelf een IP-adres toe uit een speciale range toe (169.254.0.0-169.254.255.255). Dit gebeurt na met behulp van ARP gecontroleerd te hebben of niemand anders dit adres gebruikt. (Voor meer info over ARP, klik hier.)

De bedoeling van deze oefeningen is om aan te tonen dat de client een IP-adres aanvraagt bij de server, die dan een aanbod doet. Gaat de client hier op in dan stuurt de server een acknowledgement en dus ook de toestemming om een IP- adres uit de pool te gebruiken.

Oefeningen

Start een capturesessie in Wireshark.

1. Geef met behulp van een commando je IP-adres vrij.
   Antwoord:

2. Hernieuw met behulp van een commando je IP-adres.
   Antwoord:

   Stop de Wireshark capture.

3. Gebruik een gepaste filter in Wireshark om enkel de DHCP-gerelateerde pakketten te bekijken.
   Antwoord:

4. Welk van die pakketten zijn unicasts? Welke zijn broadcasts? Waarom is dat zo?
   Antwoord:

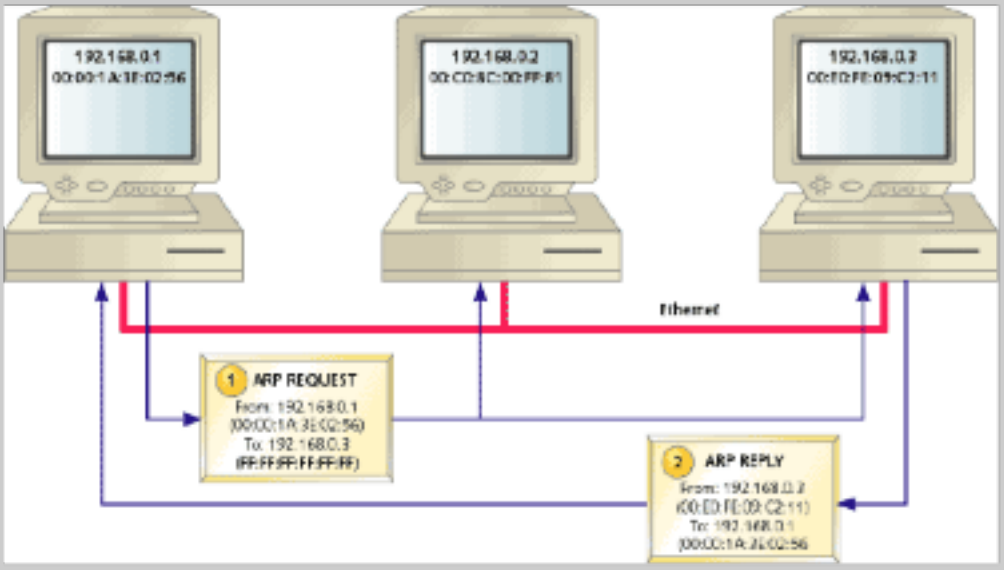
5. Ga na of je laptop inderdaad vraagt om terug zijn reeds eerder gebruikt IP-adres te mogen gebruiken.
   Antwoord:

6. Welke DHCP-opties worden er nog door de DHCP-server aan de DHCP- client meegegeven?
   Antw
7. Ga ook na van welk transportlaag-protocol DHCP gebruikmaakt: TCP of UDP. Welke poorten gebruikt DHCP hierbij?
   Antwoord:

Oefensessie 3 - Het ARP-protocol

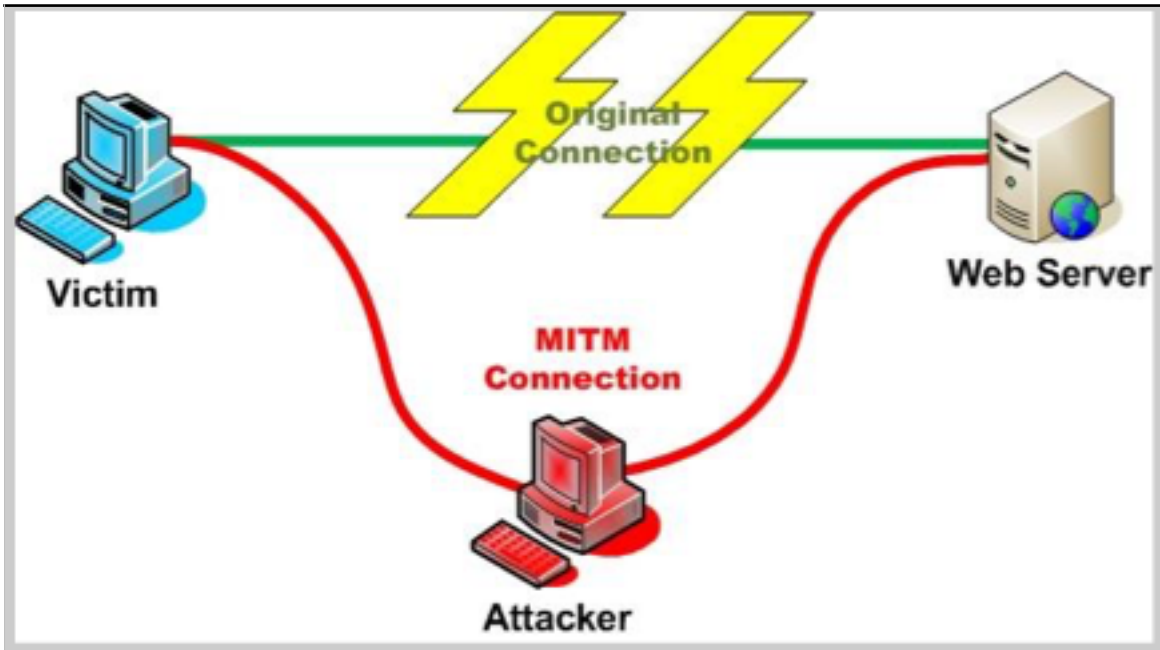
ARP, Address Resolution Protocol, komt voor in de netwerklaag in het OSI- model, of de internetlaag in het TCP/IP-model. De netwerkkaart van een computer kan namelijk enkel communiceren met andere computers via hun MAC-adres. Daarom zet het ARP-protocol de IP-adressen om in MAC-adressen.

De situatie is als volgt: Host A wil een pakket naar het IP-adres x.y.z.u sturen, maar kent het MAC-adres niet. Dus stuurt A via een broadcast een ART-request met de vraag "who has address x.y.z.u?". Enkel de betrokken host B met adres



x.y.z.u stuurt een ARP-reply terug. Deze reply bevat het MAC-adres van B, die host A samen met het IP-adres van B opslaat in zijn cachetabel.
Dit gebeurt om verder verkeer met B vlotter kan verlopen, in de meeste gevallen zal het verkeer niet bij één enkel pakket blijven. A moet nu niet steeds vragen wie het adres x.y.z.u heeft.

Met behulp van ARP is het ook mogelijk om data op te vangen tussen twee gebruikers, dit heet ARP-spoofing of ARP-cache poisoning. Hierbij gebruikt men een vals ARP-pakket waarin het MAC-adres van de aanvaller/ infiltrator geassocieerd wordt met het IP-adres van een andere (legitieme) host, meestal de router. Als gevolg komt alle data die naar X gestuurd wordt bij de aanvaller terecht.



De bedoeling van deze oefensessie is om aan te tonen hoe twee machines contact met elkaar maken door met ARP elkaars MAC-adres te verkrijgen.

Oefeningen

Start een Wireshark capturesessie en stop na enkele seconden.

8. Filter op ARP-pakketten. Antwoord:

9. Zijn de meeste ARP-pakketten ARP-requests of ARP-reply's? Waarom is dat zo?
   Antwoord:

10. Tussen de gecapturede pakketten zitten er enkele zogenaamde
    "gratuitous" ARP-reply pakketten. Waarvoor worden die pakketten gebruikt?

Antwoord:

Voor meer info klik hier voor de Wireshark wikipagina.

Start een nieuwe capturesessie en ping naar "bru-stud.hogeschool.wvl.be". Achterhaal nu het MAC-adres van de NIC van de server door de ARP-reply van die server te analyseren.
Antwoord: eerst ping je naar de site en filter je Wireshark op "arp". Kijk nu naar de replies, hier staat van waar ze komen. Hier is dat bijvoorbeeld van een DELL-server. zoek het ipadres waar je naar gepingd

hebt, dat is de reply van de server. Kijk nu bij de details van het pakket voor het

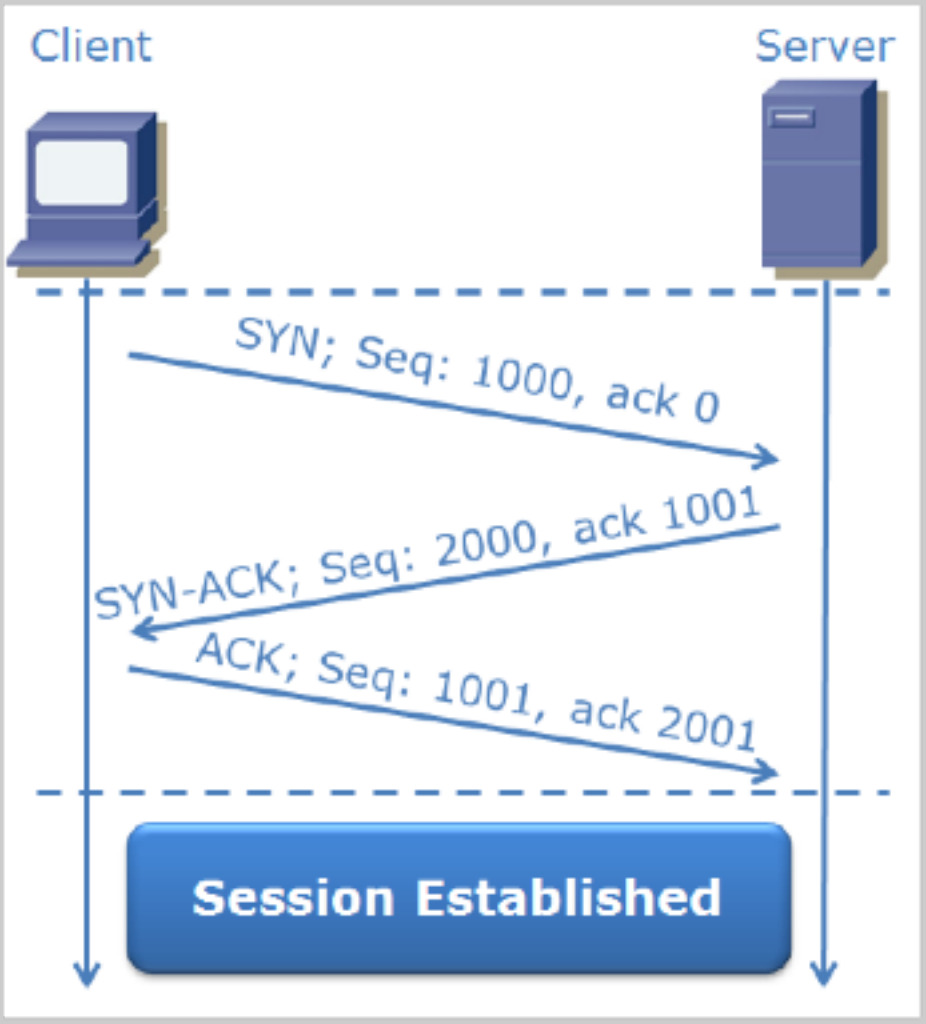
MAC-adres.

Oefensessie 4 - Het TCP-protocol

TCP, Transmission Control Protocol, is het meest gebruikte protocol in de transportlaag van het TCP/IP-model. Er zijn 3 fasen binnen een TCP-verbinding.

- Initialisatie
- Data-overdracht
- Finalisatie

De initialisatie, het opzetten van de verbinding gebeurt ook in 3 fasen, bekend als de 3-way handshaking-procedure. Hierbij wordt gebruik gemaakt van sequence- en acknowlegenummer om betrouwbare gegevensoverdracht te realiseren. Sequencenummer is het bytestroomnummer (de hoeveelste byte dit is van de volledige data) van de eerste byte in het segment/pakket.



Acknowledgementnr is het bytestroomnummer van de eerstvolgende byte die een ontvangende host van een zendende host verwacht.
ISN (Initial Sequence Number) is het volgnummer van het allereerste segment dat verstuurd wordt, en voorkomt duplicaten.

Men kan ook de hoeveelheid data die onbevestigd mag doorgestuurd worden controleren met behulp van het window-veld in de TCP-header. Zo zal er bij een

slechte verbinding een kleinere waarde zijn, dus moet er vaker bevestigd worden. In het algemeen noemt men dit flow control.

De betrouwbaarheid wordt ook verbeterd doordat de ontvanger na een (reeks) ontvangen segment(en) binnen een bepaalde afgesproken tijd een ontvangstbevestiging sturen naar de zender. Als na het verstrijken van die tijd nog geen bevestiging ontvangen werd, stuurt de zender die segmenten opnieuw door. Dit heet retransmission.

Oefeningen

1. Start een capture-sessie in Wireshark

2. Surf naar www.howest.be en klik op een link. Beëindig daarna de sessie.

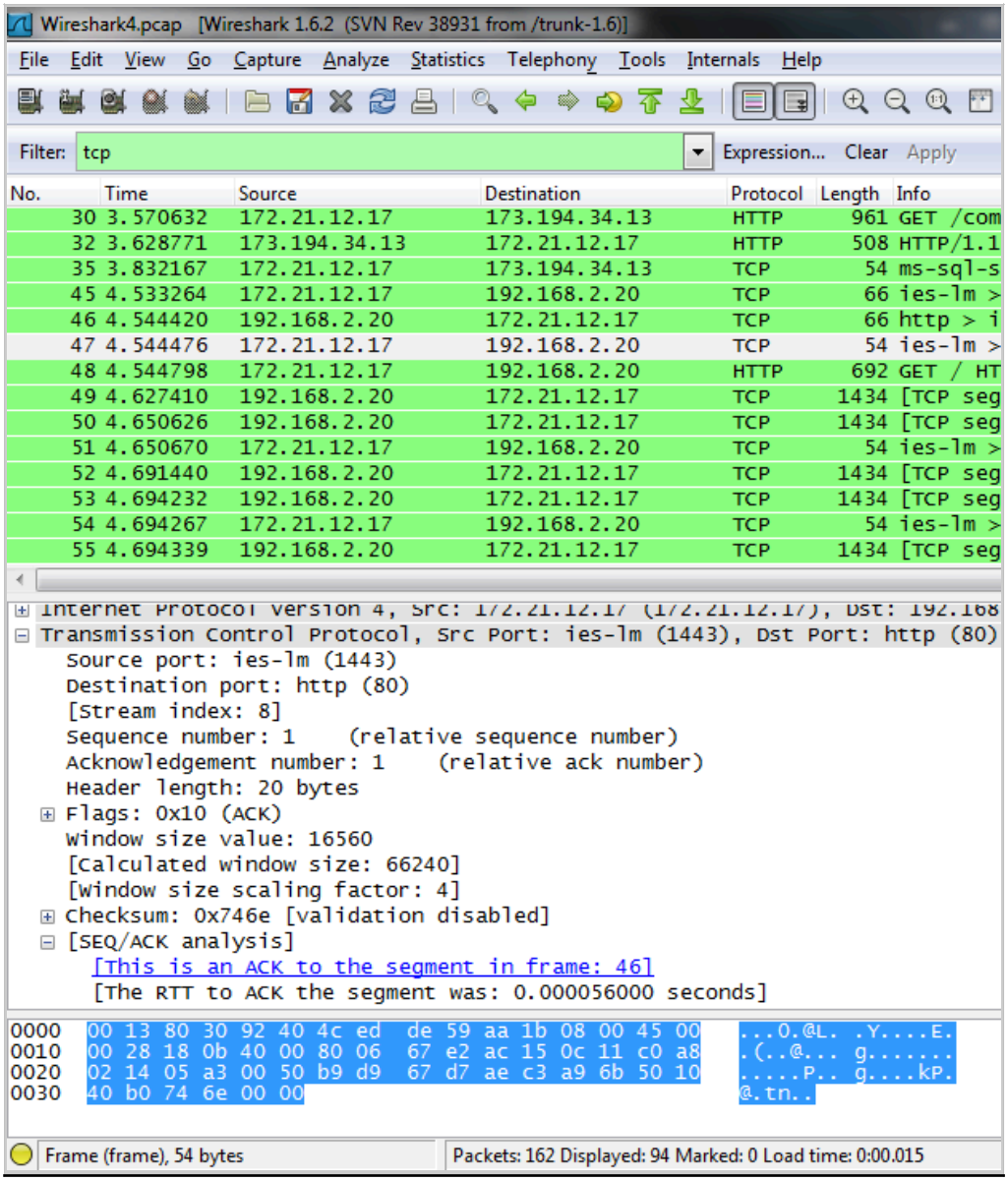
3. Filter in Wireshark op TCP-pakketten
   Antwoord:

4. 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.
   Antwoord:

Zoek nu naar het pakket met SYN, SYN+ACK en ACK. klik op Transmission Control Protocol en dan Flags.
Met de SYN vlag is de vlaggenbyte 02hex -> 00000010 (de 1 is de SYN vlag)
Met de SYN+ACK vlag is de vlaggenbyte 12hex -> 00010010 (de eerste 1 is de ACK vlag)
Met de ACK vlag is de vlaggenbyte 10hex -> 00010000

Klik nu op SEQ/ACK binnen Transmission Control Protocol van het ACK

pakket om te zien op welk pakket dit een antwoord is.



5. Welke poort gebruikt je laptop bij die TCP-sessie?
   Antwoord:

6. Ga na hoe de wisselwerking tussen sequence-en acknowledgementnummer gebeurt bij zo'n surfsessie.

Antwoord:

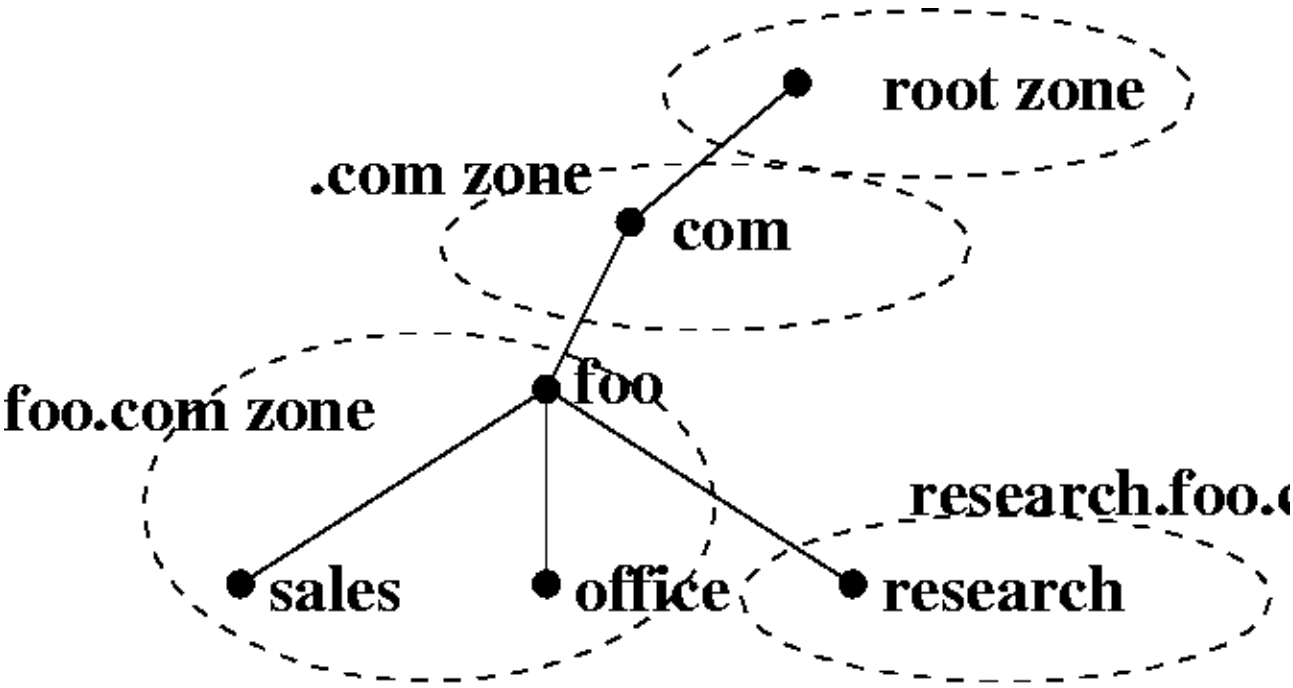
Oefensessie 5 - Het DNS-protocol

DNS, Domain Name System, zorgt voor de vertaling van een hostnaam naar een IP-adres, en omgekeerd. Deze worden bijgehouden in databases van DNS- servers die hiërarchisch georganiseerd zijn. Elke laag in die hiërarchie wordt een domein genoemd. Het hoogste domein, het zogenaamde root domein, is

naamloos en wordt voorgesteld als een punt. het laagste domein zijn de hosts van de site zelf. Een voorbeeld van domeinhiërarchie; www.sitenaam.be bestaat uit volgende domeinen:

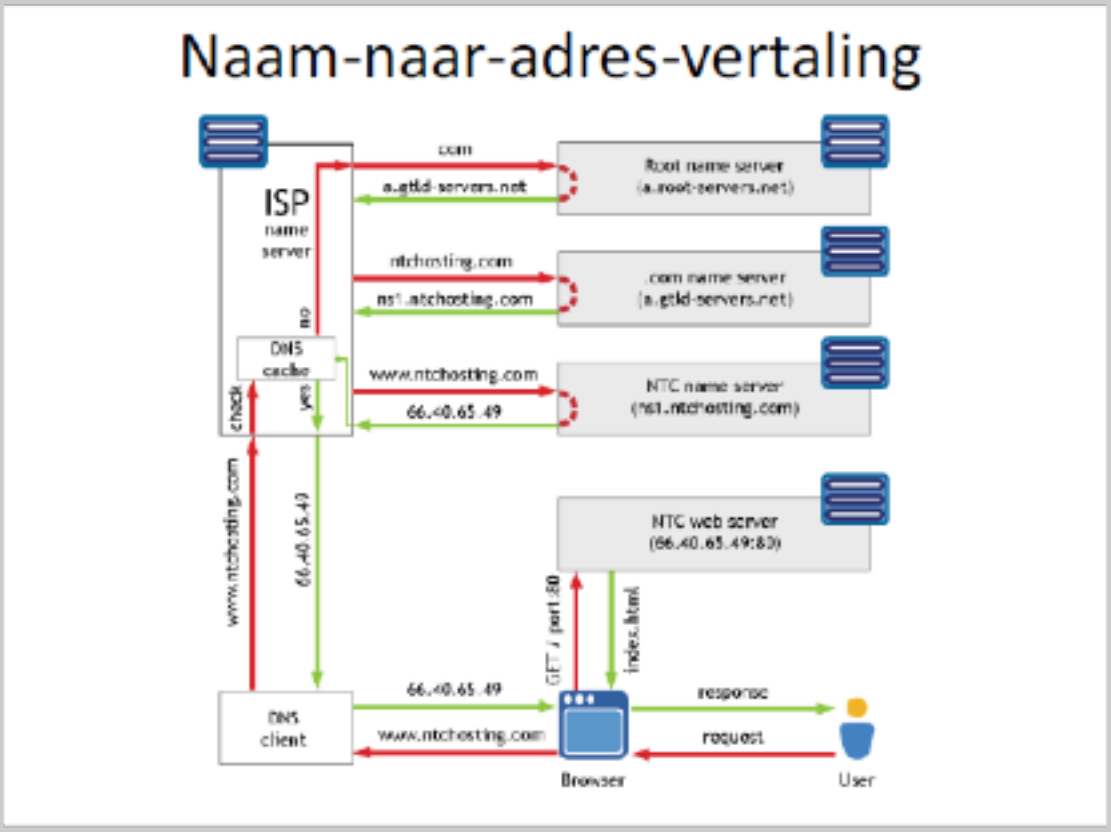
1. Het sitenaam-domein
2. Het be-domein
3. Het root-domein

Een namespace is ook opgesplitst in verschillende aaneengesloten porties, DNS-zones. Elk van die zones heeft minstens één DNS-server die verantwoordelijk is voor de naam-naar-adresvertaling binnen die zone. Zo'n zone kan bestaan uit een enkel DNS-domein, of een DNS-domein en een aantal van zijn subdomeinen waarvoor het verantwoordelijk is.



Aangezien een server normaliter geen vast IP-adres heeft, zitten we met een probleem. Wanneer het IP-adres door ISP gewijzigd wordt, wordt de naam van de server aan een verkeerd IP-adres gekoppeld. De oplossing hiervoor is werken met dynamic DNS (DDNS).
Als een dynamisch IP-adres verandert updatet het Firewall/NAT toestel zijn interface zodat die IP verandering overgenomen wordt. Als de Dynamische DNS client dan een pollt naar het toestel om veranderingen te controleren, en er wordt effectief een gevonden, stuurt de DDNS client een update naar de externe DNS server, die dan zijn data updatet.

Hoe werkt DNS nu wanneer een client naar een site surft? De gebruiker zal meestal een www-adres gebruiken, dus de browser stuurt die door naar de DNS



client. Deze vraagt dan aan de ISP op wat het IP-adres is van die site. De ISP zelf vraagt dan, beginnende bij de root name server, aan telkens de onderliggende name server de doorgegeven site op. Totdat die een effectief IP- adres krijgt. Deze wordt dan teruggestuurd naar de DNS client, die het doorstuurt naar de browser. De browser kan dan verbinding maken en de pagina opvragen aan de server waarop deze zich bevindt. Daarna krijgt de user eindelijk zijn site te zien.

Zowel DNS-client als server houden een DNS-cache bij met recent opgevraagde naam-naar-adresvertalingen. Hierdoor kunnen veel DNS-query's sneller beantwoord worden. Deze cache groeit niet oneindig aan, na verloop van tijd wordt data uit de cache verwijderd. Het enige wat steeds in de DNS-cache van

de client aanwezig is, is de inhoud van de HOSTS-file. Deze bevat naam-naar- adresvertalingen die manueel ingevoerd werden.

Oefeningen

1.Start een Wireshark capture-sessie.

2.Surf naar www.tijd.be en beëindig de sessie.

3.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. Antwoord: Dit zijn de eerste pakketten die je ziet als je op "dns" filtert. Deze zijn allemaal DNS-pakketten die het adres vertalen.

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

_____

Antwoord:

_____

5. Van welk protocol maakt DNS gebruik: TCP of UDP? Welk well-known port number wordt hierbij gebruikt?
Antwoord:

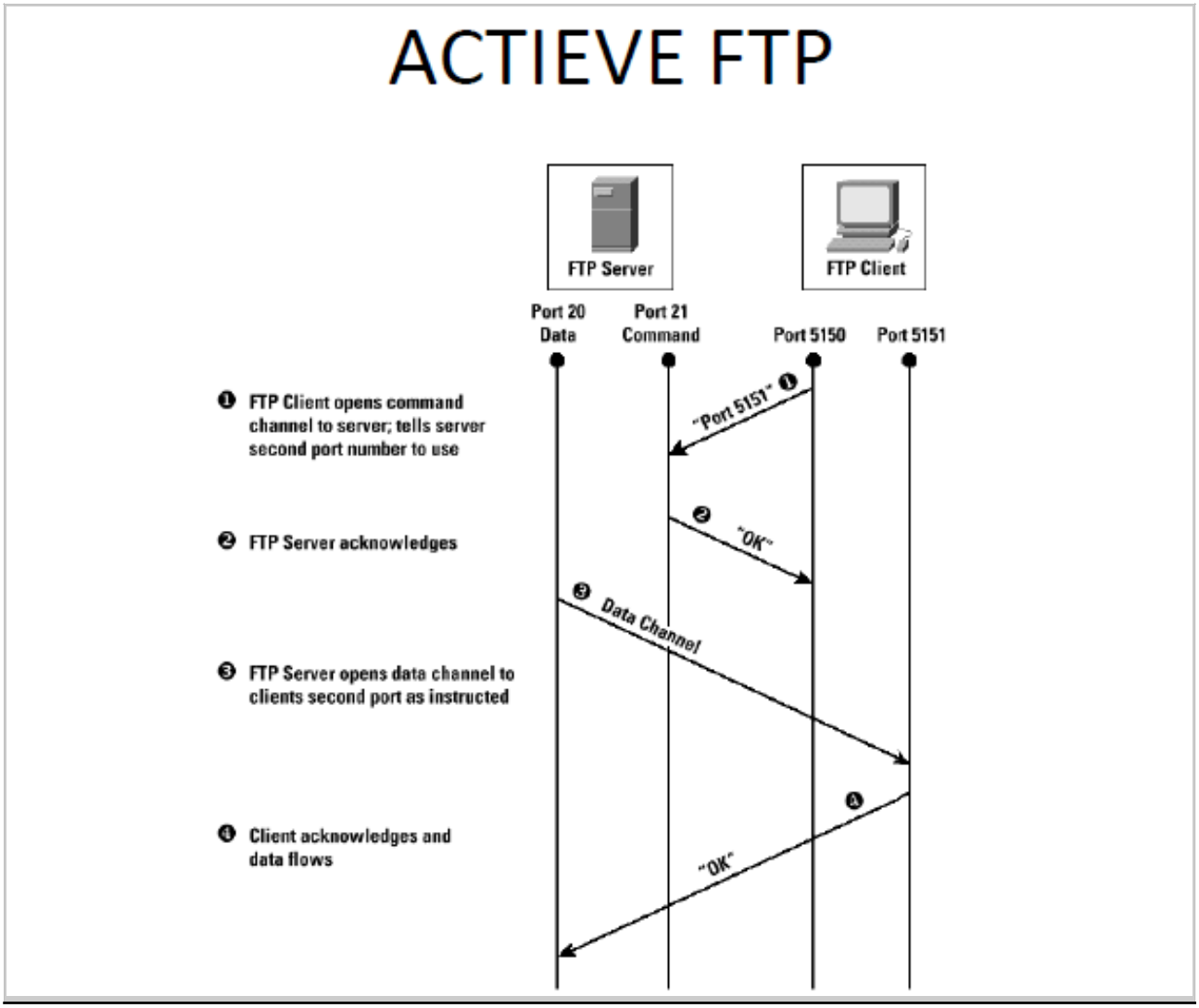
_____

Oefensessie 6 - Het FTP-Protocol

FTP, File Transfer Protocol, wordt gebruikt om bestanden tussen twee machines uit te wisselen. Dit kan gebruikt worden om een site van een client naar een server te sturen, die de site dan online zet. Er wordt een onderscheid gemaakt tussen actieve en passieve FTP.

Bij actieve FTP opent de client een kanaal naar de server en zegt welke poort deze moet gebruiken. Nadat de server een bevestiging gestuurd heeft, opent die een datakanaal naar de gekozen poort van de client. Als de client dat bevestigt begint de dataflow.

Passieve FTP draait de rollen op sommige punten om. Weer begint de FTP- client met een kanaal naar de server te openen, maar deze keer vraagt de client "passive mode" te gebruiken. De server wijst een poort toe voor het datakanaal, en stuurt het poortnummer op naar de client. Deze opent dan het datakanaal op

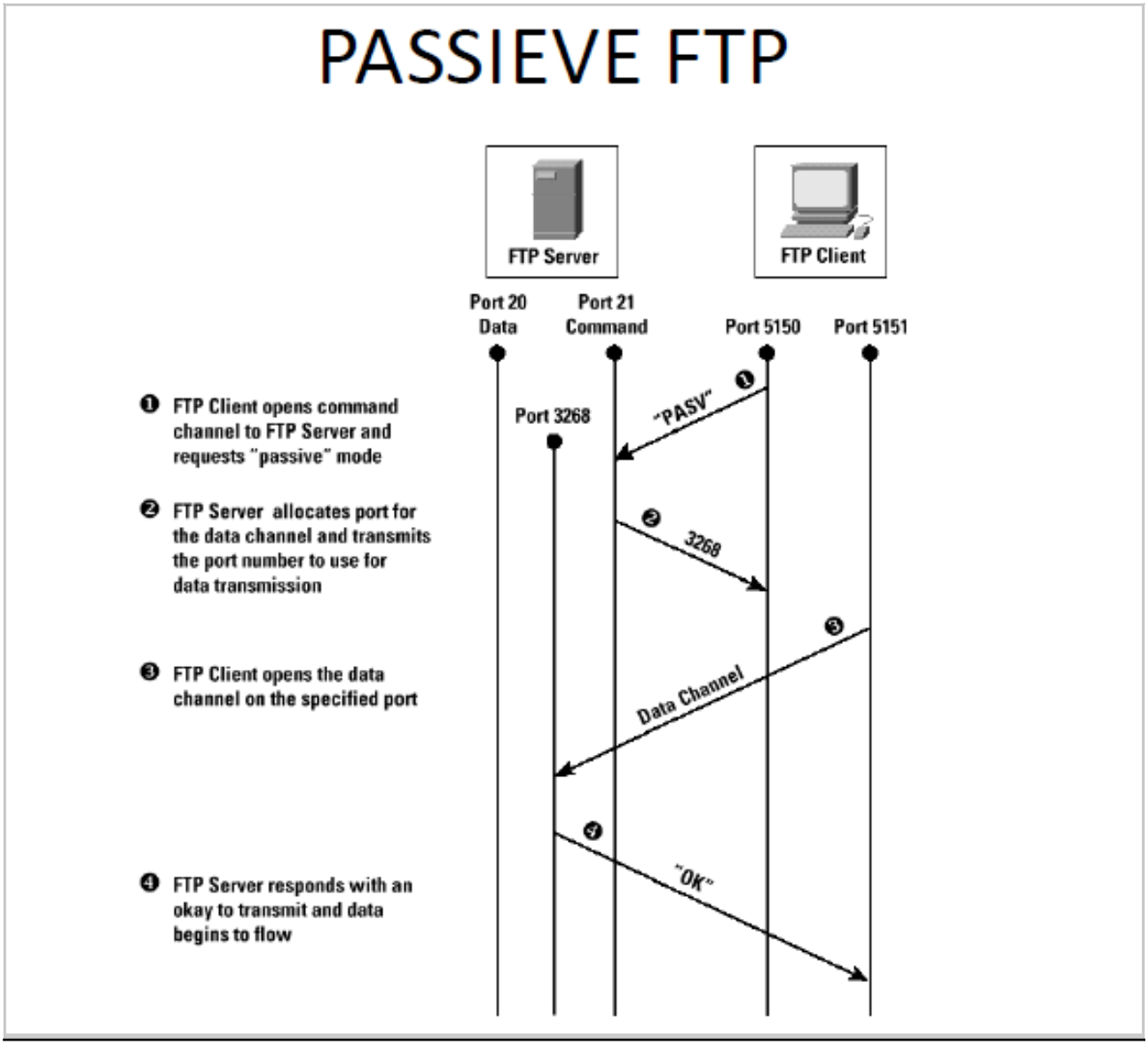


de toegewezen poort en nadat de server dat bevestigt begint de dataflow.

Standaard maakt FTP gebruik van een TCP-verbinding die een gebruikersnaam en wachtwoord nodig heeft om de verbinding te kunnen opzetten. Sommige publieke FTP-servers staan ook toe om anoniem aan te melden, met beperkte mogelijkheden.

FTP is een non-secured protocol. Dit wil zeggen dat alle info, inclusief

gebruikersnaam en wachtwoord onversleuteld wordt verstuurd (in plain text). Er bestaan daarom ook beveiligde FTP-versies, SFTP (Secure Shell FTP) en FTPS (FTP over een Secure Sockets Layer voor encryptie).



Oefeningen

1. Start een Wireshark capture-sessie.
2. Downloadmethet FTP-protocolhetbestandINDEX.TXT uit de

subdirectory SOFTLIB van de FTP-server van Microsoft (ftp.microsoft.com). Maak gebruik van de FTP-clientsoftware van FileZilla.

Antwoord: Dit kan door in FileZilla bovenaan het ftp-adres in te vullen, met als username "anonymous". Wachtwoord is niet nodig als je inlogt op die naam.

3. Verbreek de FTP-verbinding en stop de capture-sessie.

4. Bekijk het FileZilla-berichtenlogboek om te achterhalen welke FTP- commando's er op de achtergrond hiervoor gebruikt werden en ga hierbij na of er met actieve of passieve FTP gewerkt wordt.
   Antwoord:

5. Filter Wireshark op FTP-pakketten en ga na welke gebruikersnaam en wachtwoord er gebruikt werd om een FTP-connectie te maken.
Antwoord:

Voor het capture-document klikt u hier.

6. Start een nieuwe capture-sessie. Upload daarna in FileZilla een testbestand naar je persoonlijke Howest-webruimte, en verwijder het eens dat gelukt is.

7. Verbreek de verbinding met de FTP-server en stop de capture-sessie.

8. Ga na of je met behulp van Wireshark gebruikersnaam en wachtwoord
   kunt achterhalen waarmee er aangemeld werd en ga na of je de data van je verzonden testbestand kunt lezen. Leg uit!
   Antwoord: De persoonlijke webruimte die we gekregen hebben op Howest gebruikt Secure FTP, we kunnen dus geen data uitlezen. Noch gebruikersnaam en wachtwoord, nog de data van een bestand.
   Het is wel mogelijk de commando's die gebruikt zijn uit te lezen met de filter 'SSH'. Bij info over de pakketten kun je zien dat de pakketten 'encrypted' (versleuteld) zijn. Hier kun je ook zien dat er een Key Exchange is gebeurd tussen de client en server, zodat die de uitgewisselde data terug kunnen vertalen.

Oefensessie 7 - Het HTTP-Protocol

WWW, World Wide Web, is een recente internettoepassing die voor de doorbraak van het internet gezorgd heeft. Het is een gedistribueerd systeem van informatiebronnen, die toegankelijk zijn via hun adres. Dit is ofwel een URI, Uniform Resource Identifier, of URL, Uniform Resource Locator.
URI bestaat uit 3 delen:

- De naam van het mechanisme om toegang te krijgen tot de informatiebron
- De naam van de hostmachine
- De naam van de informatiebron als eer een path gegeven is

HTTP, HyperText Transfer Protocol, is een protocol dat gebruikt wordt in de applicatielaag van het web. Hierbij is er interactie tussen de client, meer bepaald de browser van de client, en de webserver. De client stuurt HTTP-requests naar de server voor het ophalen van objecten op een webpagina, die de server dan beantwoordt met HTTP-responses die de gevraagde objecten bevatten. Bij oudere browsers is er sprake van non persistent connections, die één TCP-connectie gebruiken per op te halen object. Moderne browsers daarentegen maken gebruik van (verschillende gelijktijdige) persistent connections. Deze kunnen via één TCP-connectie verschillende objecten ophalen, zodat de pagina sneller geladen wordt.
HTTP is een stateless protocol, dit wil zeggen dat er geen info wordt bijgehouden over de clients. Een webserver luistert standaard op TCP-poort 80.

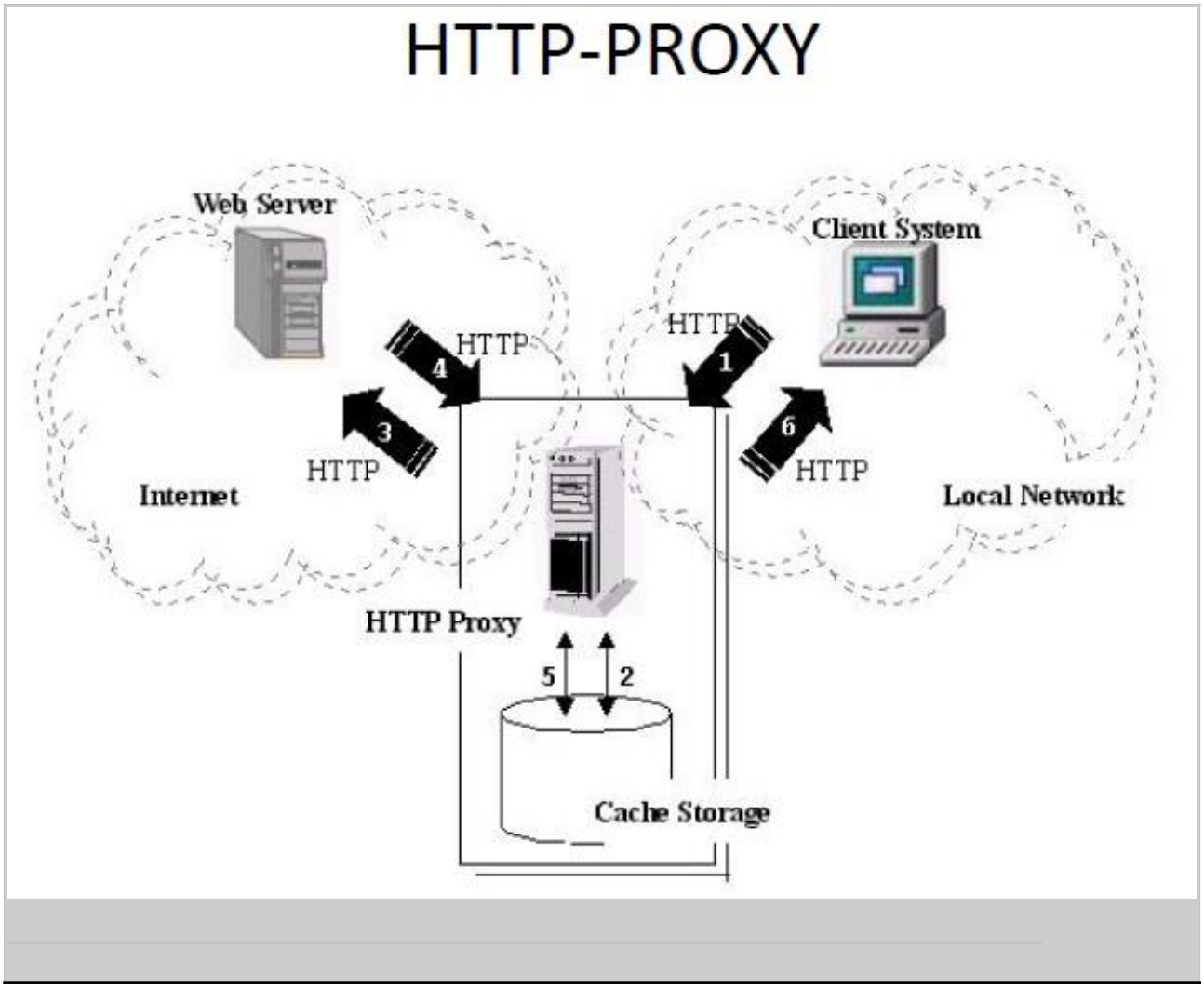
Een andere manier om de pagina sneller te kunnen laden als client (of sneller kunnen aanbieden als server), is gebruik maken van een proxyserver of webcache. Deze behandelt de HTTP requests namens

de webserver waar het verzoek naar verstuurd werd. De resources die deze proxyserver ophaalt worden op die server gecachet. Voorbeelden van proxyserversoftware zijn Microsoft Forefront Threat Management Gateway en SQUID.

HTTPS, HTTP Secure, is een uitbreiding op HTTP om veilige uitwisseling van gegevens te verzekeren. Dit is belangrijk voor bv. webbanking en webmail. Het luistert op poort 443.
Het maakt gebruik van verschillende encryptieprotocollen om de data versleuteld te versturen. Voorbeelden zijn SSL (Secure Sockets Layer) en TLS (Transport Layer Security).

Hiervoor moet op de webserver een certificaat geÏnstalleerd worden dat ondertekend moet worden door een Certificate Authority.

De gebruiker kan aan de hand van dat certificaat aan authenticatie van de webserver doen. Hierdoor is hij zeker dat de gevonden server ook inderdaad de juiste server is. Daarna wisselen de client en server een zogenaamde session/private key uit waarmee de verdere communicatie zal gecodeerd en gedecodeerd worden.



Oefeningen

9. Start een nieuwe Wireshark capture-sessie.

10. Surf naar de website van de hogeschool en stop daarna je capture-sessie.

11. Filter op het HTTP-protocol.
    Antwoord:

12. Open de eerste HTTP-request en leid er onderstaande zaken uit af:
    Antwoord:

5. Open de HTTP-response op deze request en leid er onderstaande zaken

uit af:

- De statuscode: 200
- De gebruikte HTTP-server: Microsoft-IIS
- De HTML-code van de opgevraagde pagina: Staat onder Line-based text data

6. Ga na welk 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?
Antwoord:

7. Start een nieuwe capture-sessie en surf vervolgens naar https://mail.howest.be en meld je aan. Stop daarna de capture-sessie.

8. Met behulp van welke "expression" kan je HTTPS-verkeer (die gebruikmaakt van TLSV1) filteren?
   Antwoord:

9. Welke informatie over het certificaat dat door de webmailserver met je browser uitgewisseld wordt, kun je terugvinden? Normaliter moet je die info ook via je browser kunnen opvragen...
   Antwoord:

Open in de tab Certificeringspad het certificaat van de verlener en kijk daar bij serienummer.