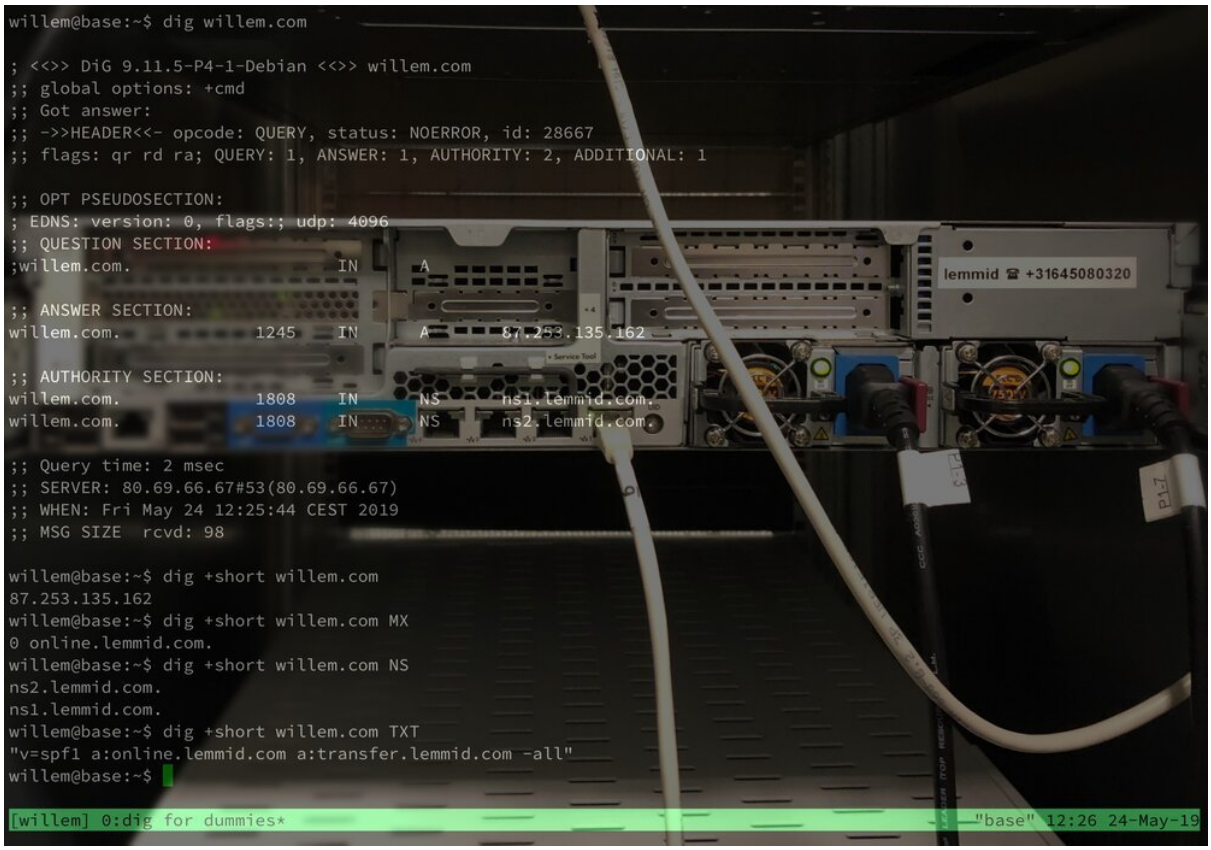
Dig voor Dummies

Uitleg van een zeer nuttige netwerktool

Willem L. Middelkoop
24 mei 2019



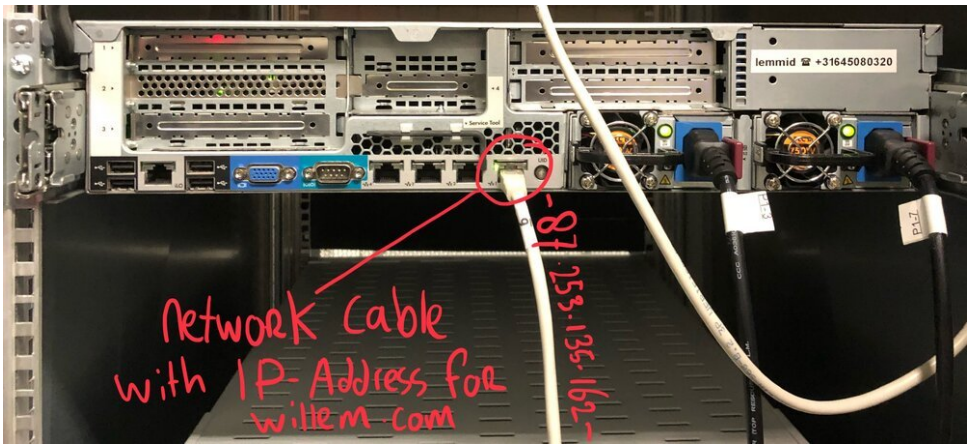
Bij het bouwen van websites, apps of e-mailservices kom je mogelijk domeinnamen en hun configuraties tegen. Wanneer alles werkt zoals het hoort, is het meeste hiervan onzichtbaar. Maar bij het oplossen van problemen met een domeinnaamconfiguratie kan het nodig zijn om wat dieper te graven... lees verder om te leren hoe!

Domain Name System (DNS)

Het internet werkt met numerieke internet protocol (IP) adressen als middel om online computers, (cloud)diensten en apparaten te lokaliseren en te identificeren. In plaats van al deze IP-adressen te onthouden, is het Domain Name System de essentiële wereldwijde directorydienst geworden, die namen aan nummers koppelt.

Je leest dit op **willem.com**, maar in werkelijkheid is deze domeinnaam simpelweg een verwijzing naar een fysieke machine, verbonden met het internet (met kabels, echt

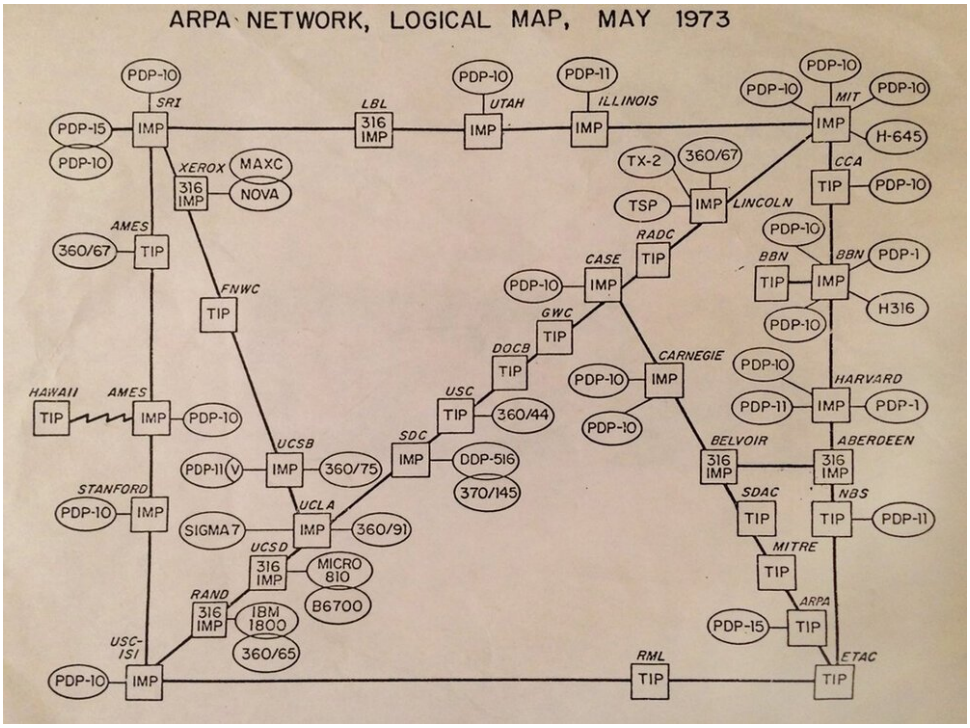
waar!). Een van die kabels is gekoppeld aan IP-adres **87.253.135.162**. Het is de verantwoordelijkheid van de DNS-server om de juiste (IP-adres) nummers te koppelen aan de (domein) namen.



Het Domain Name System (DNS) linkt domeinnamen aan IP-adressen, die op hun beurt via kabels worden gerouteerd. Je leest dit - serieus! - via de kabel die is aangesloten op de server die op deze foto staat!

Gedistribueerd en gedecentraliseerd

Toen de Amerikanen begin jaren zeventig hun ARPANET ontwierpen, was een van hun militaire ontwerpeisen dat het netwerk aanvallen (van vijanden) zou overleven. Ze bereikten dit door packet switching te implementeren, een manier om netwerkkabels te delen en te hergebruiken door meerdere mensen op meerdere manieren. Als een deel van het netwerk beschadigd raakt, worden pakketten met informatie omgeleid via andere delen van het netwerk.



[image]

Om maximale overlevingskansen te bereiken, is er geen enkele root-DNS-server. In plaats daarvan delegeert het Domain Name System de verantwoordelijkheid voor het toewijzen van domeinnamen en mappings aan die namen door een gezaghebbende naamserver aan te wijzen voor elke domeinnaam.

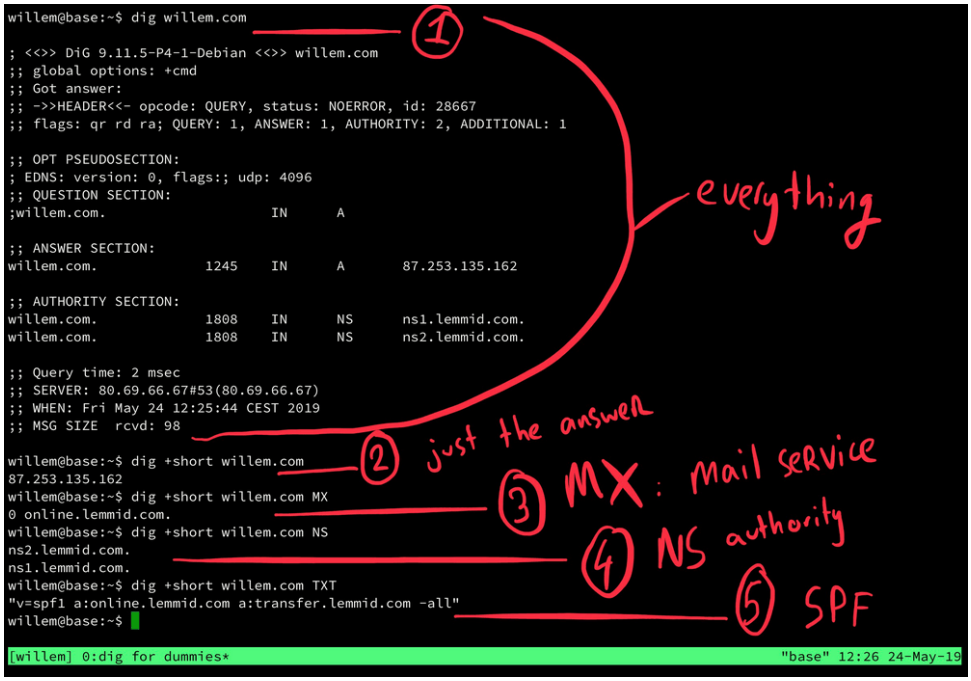
Dit is waarom er zoveel verschillende DNS-servers en configuraties zijn. Met zoveel manieren en plaatsen waarop dingen fout kunnen gaan, heb je een tool nodig om rond te neuzen.

dig (domain information groper)

Het 'dig'-commando is een tool om DNS-naamservers te bevragen voor informatie over IP-adressen, hostnamen, mailservers en andere soorten netwerkinstellingen. Het dig-commando is beschikbaar op Unix, macOS, GNU/Linux en Windows.

Dig gebruiken om domeinnaamservers te bevragen

Je kunt dig gebruiken om informatie over een bepaalde domeinnaam te krijgen door simpelweg te typen: 'dig willem.com'. Zie de volgende schermafbeelding met uitleg:



Een kaart van het ARPANET in 1973... stel je voor om het internet van vandaag in kaart te brengen! (Publiek domein)

- 1) **dig willem.com** retourneert alle informatie over de vraag, het antwoord, de autoriteit (degene die de vraag beantwoordde) en statistieken van de daadwerkelijke query (zoals hoe lang het duurde om een antwoord te krijgen).
- 2) **dig +short willem.com** laat alle extra informatie weg en retourneert alleen het antwoord. Hier zie je dat **willem.com** verwijst naar IP-adres **87.253.135.162**.
- 3) **dig +short willem.com MX** laat de mail exchange (MX) records zien. MX-records zijn cruciaal om e-mail op de juiste server te laten aankomen. In principe is het de aanduiding van het postkantoor dat verantwoordelijk is voor e-mail gekoppeld aan de domeinnaam. Voor **willem.com** is dit een e-maildienst genaamd **online.lemmid.com**. Andere populaire e-maildiensten zijn Office365 en Google Gmail. Met dig kun je erachter komen welke e-maildienst iemand gebruikt.
- 4) **dig +short willem.com NS** toont de naamservers die verantwoordelijk zijn voor het afhandelen van queries voor deze domeinnaam. Meestal zijn dit de servers die worden beheerd door het domeinnaamregister, jouw domeinnaamprovider. Met dig kun je achterhalen wat voor soort domeinnaamprovider iemand gebruikt (in het geval van **willem.com** is dat **Lemmid**).
- 5) **dig +short willem.com TXT** retourneert het tekstrecord gekoppeld aan de domeinnaam, hier vind je het zogenaamde SPF-record. Het SPF-record is een ander cruciaal onderdeel van e-mail, het is nuttig om wat dieper in te gaan op SPF.

Sender Policy Framework (SPF)

Om vervalste afzenderadressen in e-mails te detecteren (zogenaamde e-mail spoofing), werd de SPF-standaard in 2004 gedefinieerd. Oorspronkelijk "Sender Permitted From" genoemd, is SPF een manier om te controleren of iemand namens een bepaalde domeinnaam e-mail mag versturen. SPF staat de eigenaar van een domeinnaam toe om te specificeren welke computers bevoegd zijn om e-mail te versturen met VAN-adressen van

dat domein.

Als een domeinnaameigenaar een SPF-record publiceert, is de kans kleiner dat spammers en phishers de domeinnaam (mis)bruiken om vervalste e-mails te versturen, waarbij ze zich voordoen als afkomstig van dat domein. Een SPF-beschermd domein heeft daarom minder kans om op de zwarte lijst van spamfilters te komen, waardoor de kans groter is dat legitieme e-mail van het domein wordt doorgelaten. Een verkeerd geconfigureerd SPF-record kan echter de e-mailbezorging verstoren.

Dig gebruiken om SPF-records te bevragen

Met het dig-commando kun je een SPF-record opvragen en zien wat het exacte afzenderbeleid is. Zie de volgende schermafbeelding met uitleg:

[image]

- 1) **dig +short TXT google.com** laat ons het TXT-record zien dat is geconfigureerd voor google.com, de plaats waar je het SPF-record kunt vinden (onder andere). Het SPF-record voor **google.com** is **"v=spf1 include:_spf.google.com ~all"**. Het **include:**-gedeelte betekent dat voor deze domeinnaam ook externe SPF-waarden moeten worden geladen.
- 2) **dig +short TXT _spf.google.com** laat zien wat die externe SPF-waarden voor **google.com** daadwerkelijk zijn. In dit geval onthult het nog drie includes: "_netblocks.google.com", "_netblocks2.google.com" en (hoe origineel..) "_netblocks3.google.com".
- 3) **dig +short TXT _netblocks.google.com** (en de 2 + 3 varianten) specificeren de daadwerkelijke IP-adressen die namens **google.com** e-mail mogen versturen. Omdat Google een groot internetbedrijf is, staan er veel IP-adressen in deze lijsten. Als je goed kijkt, zie je dat sommige van deze adressen een "/"-achtervoegsel hebben, zoals "/24". Dit is de manier om een heel blok (bijv. straat) IP-adressen te noteren.

IP-blokken uitgelegd

De eenvoudigste manier om IP-adresblok notatie te begrijpen is door de volgende voorbeelden:

- **/8 = 255.0.0.0**
- **/16 = 255.255.0.0**
- **/24 = 255.255.255.0**
- **/32 = 255.255.255.255**

Waar je '0' ziet in de bovenstaande adressen, zijn andere waarden inbegrepen. Dus bijvoorbeeld, de 173.194.0.0/16 betekent eigenlijk "alle adressen die beginnen met '173.194' ". Gegeven 255 mogelijke posities op elk octet, dat is 255x255=65025 verschillende adressen!

Conclusie

Om problemen op te lossen moet je weten waar het probleem zit. Met behulp van het dig-commando kun je meer te weten komen over een bepaalde netwerk- en domeinconfiguratie.

Antwoorden van het ene commando naar het andere stellen je in staat om diep in de ingewanden van het geweldige internet te graven. Succes!