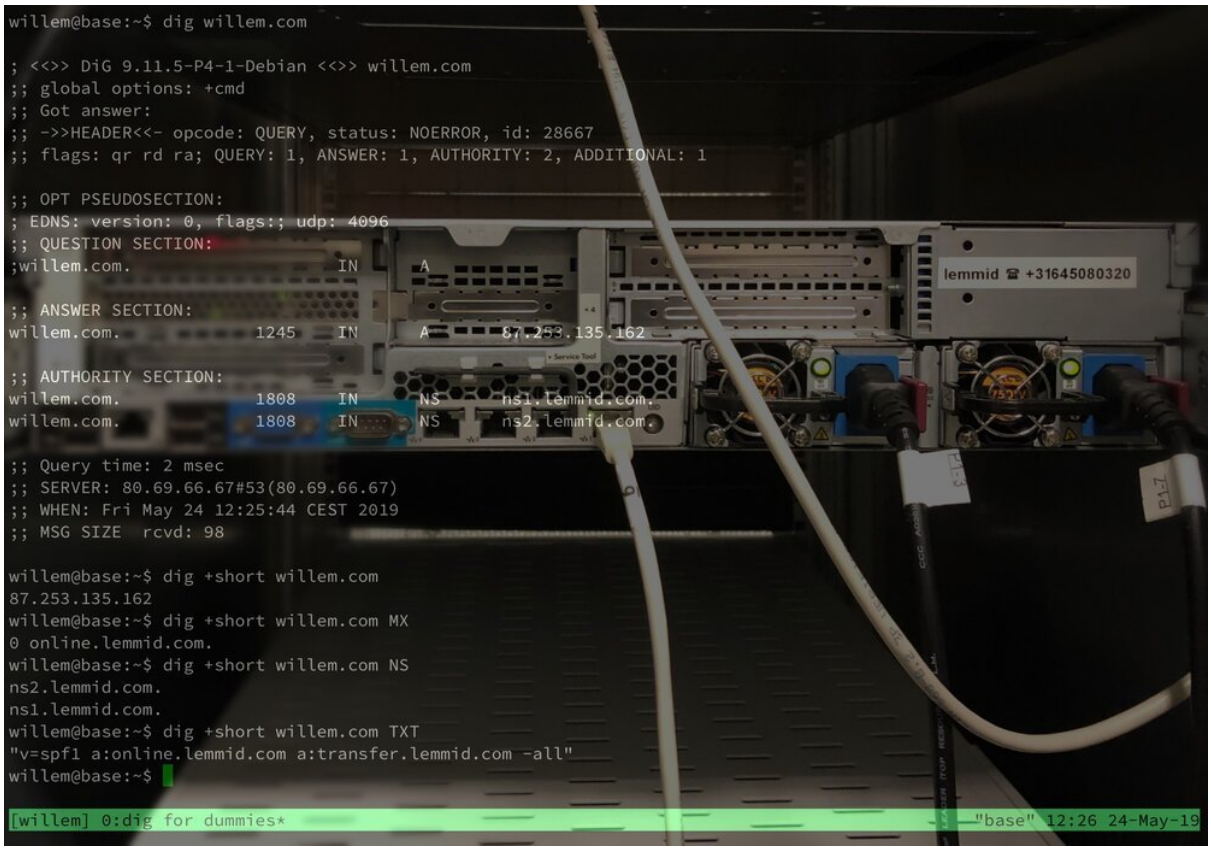
Dig für Dummies

Erläuterung eines äußerst nützlichen Netzwerk-Tools

Willem L. Middelkoop
May 24, 2019



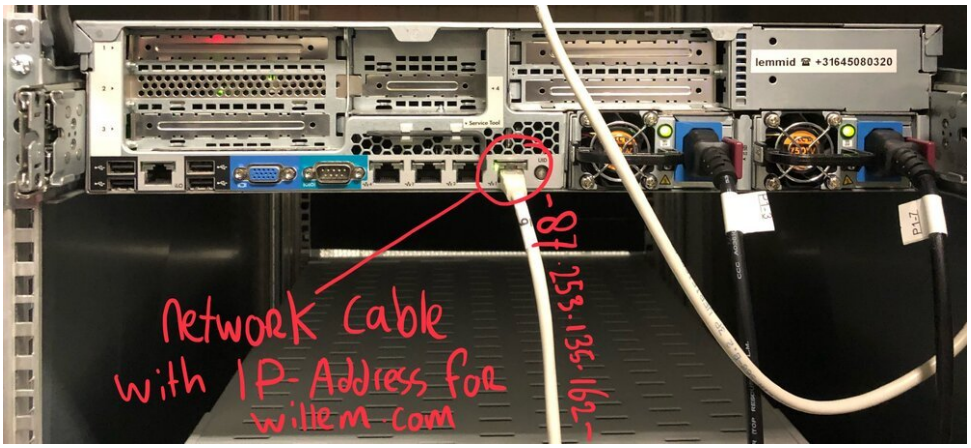
Beim Erstellen von Websites, Apps oder E-Mail-Diensten begegnen Ihnen möglicherweise Domainnamen und deren Konfigurationen. Wenn alles wie vorgesehen funktioniert, bleibt das meiste davon unsichtbar. Aber bei der Fehlerbehebung einer Domainnamenkonfiguration kann es notwendig sein, etwas tiefer zu graben ... lesen Sie weiter, um zu erfahren, wie!

Domain Name System (DNS)

Das Internet funktioniert mit numerischen Internetprotokoll-(IP-)Adressen, um Online-Computer, (Cloud-)Dienste und Geräte zu lokalisieren und zu identifizieren. Anstatt sich all diese IP-Adressen zu merken, ist das Domain Name System zum weltweit wichtigsten Verzeichnisdienst geworden, der Namen mit Nummern verknüpft.

Sie lesen dies auf **willem.com**, aber in Wirklichkeit ist dieser Domainname lediglich ein Zeiger auf eine physische Maschine, die mit dem Internet verbunden ist (tatsächlich

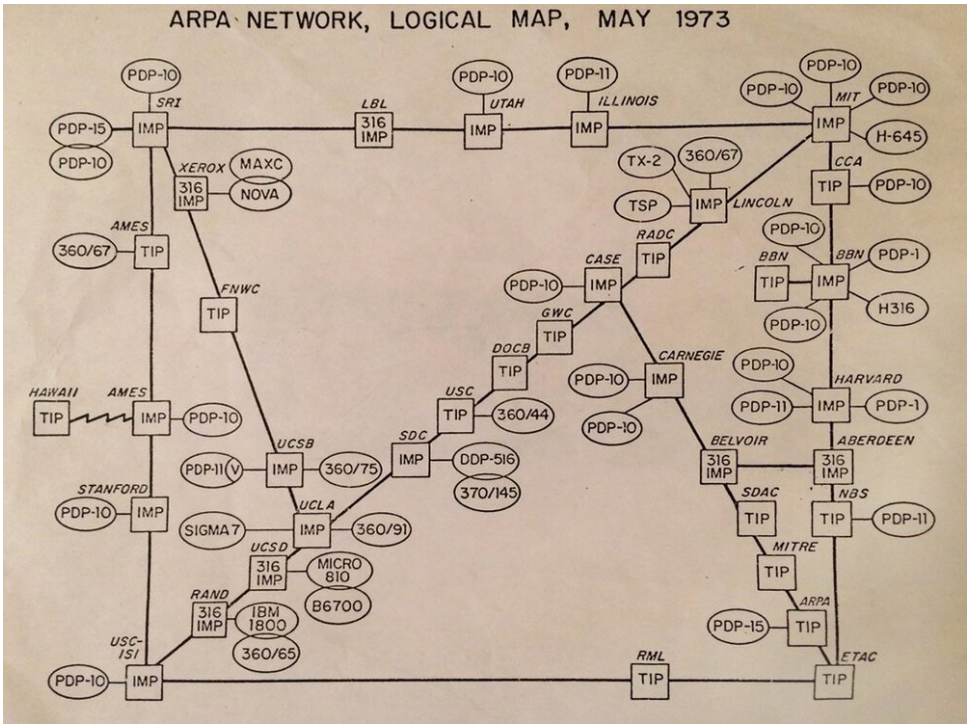
mit Kabeln!). Eines dieser Kabel ist mit der IP-Adresse **87.253.135.162** verbunden. Es liegt in der Verantwortung des DNS-Servers, die richtigen (IP-Adress-)Nummern mit den (Domain-)Namen abzugleichen.



Das Domain Name System (DNS) verknüpft Domainnamen mit IP-Adressen, die wiederum über Kabel geroutet werden. Sie lesen dies - wirklich! - über das Kabel, das mit dem auf diesem Foto gezeigten Server verbunden ist!

Verteilt und dezentralisiert

Als die Amerikaner Anfang der siebziger Jahre ihr ARPANET entwickelten, war eine ihrer militärischen Designanforderungen, dass das Netzwerk Angriffe (von Feinden) überstehen würde. Sie erreichten dies durch die Implementierung von Paketvermittlung, einer Möglichkeit, Netzwerkkabel von mehreren Personen auf verschiedene Weise gemeinsam zu nutzen und wiederzuverwenden. Wenn ein Teil des Netzwerks beschädigt wird, werden Informationspakete über andere Teile des Netzwerks umgeleitet.



[image]

Um maximale Überlebensfähigkeit zu erreichen, gibt es keinen einzigen Root-DNS-Server. Stattdessen delegiert das Domain Name System die Verantwortung für die Zuweisung von Domainnamen und die Zuordnung zu diesen Namen, indem es für jeden Domainnamen einen autoritativen Nameserver bestimmt.

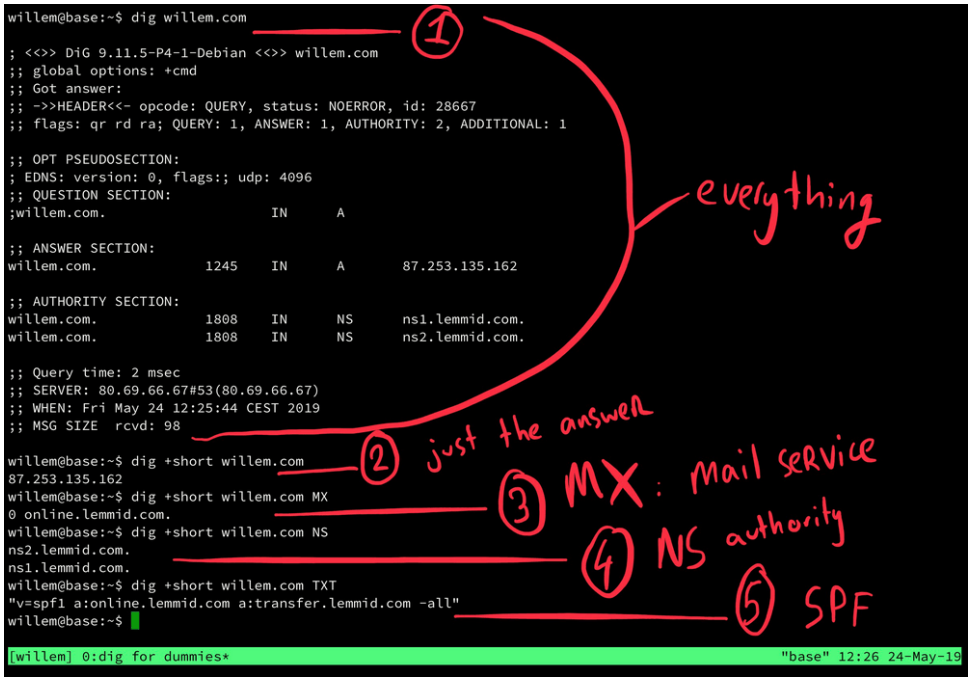
Deshalb gibt es viele verschiedene DNS-Server und -Konfigurationen. Bei so vielen Möglichkeiten und Orten, an denen etwas schief gehen kann, benötigt man ein Werkzeug, um nachzuforschen.

dig (domain information groper)

Der Befehl 'dig' ist ein Werkzeug, um DNS-Nameserver nach Informationen über IP-Adressen, Hostnamen, Mailserver und andere Arten von Netzwerkeinstellungen abzufragen. Der Befehl dig ist unter Unix, macOS, GNU/Linux und Windows verfügbar.

Verwendung von dig zur Abfrage von Domain-Nameservern

Sie können dig verwenden, um Informationen über einen bestimmten Domainnamen zu erhalten, indem Sie einfach Folgendes eingeben: 'dig willem.com'. Siehe den folgenden Screenshot mit Erklärung:



Eine Karte des ARPANET von 1973... stellen Sie sich vor, das heutige Internet abzubilden! (Public Domain)

- 1) **dig willem.com** gibt alle Informationen über die Frage, die Antwort, die Autorität (die die Frage beantwortet hat) und Statistiken der eigentlichen Abfrage zurück (z. B. wie lange es gedauert hat, eine Antwort zu erhalten).
- 2) **dig +short willem.com** lässt alle zusätzlichen Informationen weg und gibt nur die Antwort zurück. Hier sehen Sie, dass **willem.com** auf die IP-Adresse **87.253.135.162** verweist.
- 3) **dig +short willem.com MX** zeigt Ihnen die Mail-Exchange-(MX-)Einträge an. MX-Einträge sind entscheidend dafür, dass E-Mails beim richtigen Server ankommen. Im Grunde ist es die Bezeichnung der Poststelle, die für E-Mails zuständig ist, die mit dem Domainnamen verknüpft sind. Für **willem.com** ist dies ein Maildienst namens **online.lemmid.com**. Andere beliebte Maildienste sind Office365 und Google Gmail. Mit dig können Sie herausfinden, welchen Maildienst jemand verwendet.
- 4) **dig +short willem.com NS** zeigt Ihnen die Nameserver an, die für die Bearbeitung von Anfragen für diesen Domainnamen zuständig sind. In der Regel sind dies die Server, die von der Domainnamen-Registrierungsstelle, Ihrem Domainnamen-Provider, betrieben werden. Mit dig können Sie herausfinden, welche Art von Domainnamen-Provider jemand verwendet (im Fall von **willem.com** ist das **Lemmid**).
- 5) **dig +short willem.com TXT** gibt den mit dem Domainnamen verknüpften Texteintrag zurück. Hier finden Sie den sogenannten SPF-Eintrag. Der SPF-Eintrag ist ein weiterer wichtiger Bestandteil von E-Mails. Es ist nützlich, sich etwas genauer mit SPF zu befassen.

Sender Policy Framework (SPF)

Um gefälschte Absenderadressen in E-Mails zu erkennen (sogenanntes E-Mail-Spoofing), wurde 2004 der SPF-Standard definiert. Ursprünglich "Sender Permitted From" genannt, ist SPF eine Möglichkeit zu überprüfen, ob jemand berechtigt ist, E-Mails im Namen eines bestimmten Domainnamens zu versenden. SPF ermöglicht es dem Eigentümer eines Domainnamens, anzugeben, welche Computer berechtigt sind, E-Mails mit FROM-Adressen dieser Domain zu versenden.

Wenn ein Domainnamen-Inhaber einen SPF-Eintrag veröffentlicht, ist es weniger wahrscheinlich, dass Spammer und Phisher den Domainnamen (miss)brauchen, um gefälschte E-Mails zu versenden und so zu tun, als kämen sie von dieser Domain. Eine SPF-geschützte Domain wird daher weniger wahrscheinlich von Spamfiltern auf die schwarze Liste gesetzt, wodurch es wahrscheinlicher wird, dass legitime E-Mails von der Domain durchkommen. Ein falsch konfigurierter SPF-Eintrag kann jedoch die E-Mail-Zustellung stören.

Verwendung von dig zur Abfrage von SPF-Einträgen

Mit dem Befehl dig können Sie einen SPF-Eintrag abfragen und sehen, wie die genaue Senderrichtlinie lautet. Siehe den folgenden Screenshot mit Erklärung:

[image]

- 1) **dig +short TXT google.com** zeigt uns den TXT-Eintrag, der für google.com konfiguriert ist, den Ort, an dem Sie den SPF-Eintrag finden können (neben anderen Dingen). Der SPF-Eintrag für **google.com** ist **"v=spf1 include:_spf.google.com ~all"**. Der **include:**-Teil bedeutet, dass für diesen Domainnamen auch externe SPF-Werte geladen werden sollen.
- 2) **dig +short TXT _spf.google.com** zeigt, was diese externen SPF-Werte für **google.com** tatsächlich sind. In diesem Fall werden drei weitere Includes angezeigt:

"_netblocks.google.com", "_netblocks2.google.com" und (wie originell..) "_netblocks3.google.com".

- 3) **dig +short TXT _netblocks.google.com** (und die 2 + 3 Varianten) geben die tatsächlichen IP-Adressen an, die berechtigt sind, E-Mails im Namen von **google.com** zu versenden. Da Google ein großes Internetunternehmen ist, gibt es viele IP-Adressen in diesen Listen. Wenn Sie genau hinschauen, werden Sie feststellen, dass einige dieser Adressen ein "/"-Suffix haben, wie "/24". Dies ist die Art und Weise, einen ganzen Block (z. B. Straße) von IP-Adressen zu notieren.

IP-Blöcke erklärt

Die einfachste Art, die Notation von IP-Adressblöcken zu verstehen, ist anhand der folgenden Beispiele:

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

Wo Sie oben '0' in den Adressen sehen, sind andere Werte enthalten. So bedeutet beispielsweise 173.194.0.0/16 tatsächlich "alle Adressen, die mit '173.194' beginnen". Bei 255 möglichen Positionen auf jedem Oktett sind das 255x255=65025 verschiedene Adressen!

Schlussfolgerung

Um Probleme zu lösen, müssen Sie wissen, wo das Problem liegt. Mit dem Befehl dig können Sie etwas über ein bestimmtes Netzwerk und die Domänenkonfiguration erfahren.

Die Antworten von einem Befehl zum anderen ermöglichen es Ihnen, tief in die Eingeweide des erstaunlichen Internets einzutauchen. Viel Glück!