IP-Recherchen

Die Wurzeln ausgraben - Recherchen nach und mit IPs

Wer steckt hinter den Adressen im Netz?

Albrecht Ude

freier Journalist | Rechercheur | Recherche-Trainer

www.ude.de | albrecht@ude.de

Wichtige Quellen:

Request for Comments (RFC)
http://www.rfc-editor.org/

- Die "Bitte um Kommentierung" sind quasi die 'Gesetze' des Internet.
- Autoritative Dokumente, aber staubtrocken.

Dachorganisationen des Internet:

IANA, IETF, IEEE

Adressierungen in Computernetzen

Wie wird eigentlich ein Computer identifiziert (adressiert)
so dass er Daten(-pakete) erhalten kann?

MAC-Adresse

- Jede Netzwerkkarte (NIC) hat eine **eindeutige**, abrufbare **Seriennummer** (MAC-Adresse, LAN-ID, NIC-Nummer, physikalische Adresse, Airport-ID, Ethernet-ID, Wi-Fi-Adresse).
- Besteht aus **Hersteller-ID** (Organizationally Unique Identifier OUI und **laufender Nummer** (Individual Address Block IAB)
- 48 Bit (sechs Bytes) normalerweise hexadezimal (z.B. 00:07:E9:a3:e4:8a)
- ein-eindeutig für jedes Gerät (aber: MAC-Spoofing)
- eingesetzt als Zugangscode in WLANs

Adressierungen in Computernetzen

Wie wird eigentlich ein Computer identifiziert (adressiert)
so dass er Daten(-pakete) erhalten kann?

IP-Adresse (IPv4)

- Jedes mit dem Internet verbundene Gerät hat eine IP-Adresse.
- 4 x 3 Ziffern, Netzwerkbereich und Hostbereich, ergänzt durch Portnummer (z.B. 81.169.145.90)
- eindeutig für jedes Gerät / Subnetz zu einer Zeit, änderbar
- aber: IP-Spoofing, Anonymisierung. VDS zielte auf IP-Adressen

Adressierungen in Computernetzen

Wie wird eigentlich ein Computer identifiziert (adressiert)
so dass er Daten(-pakete) erhalten kann?

Domain Name System

- Gestaffelte Domainnamen (z.B. http://www.netzwerkrecherche.de)
- memorierbare Zeichenketten, aufgeteilt in

Protokoll	http://
Subdomain(s)	www
Domain	netzwerkrecherche
TLD	de

- verschiedenste Möglichkeiten der Manipulation

Woher kommen die Nummern / Adressen?

MAC-Adresse

- Herstellerkontingente (erste drei Blöcke)

Datenbank der Herstellerkennungen (OUI):
http://standards.ieee.org/develop/regauth/oui/public.html

Woher kommen die Nummern / Adressen?

IP-Adresse (IPv4)

- Vergabe durch IANA in Blöcken an 5 Regional Internet Registries (RIR)
  - Réseaux IP Européens Network Coordination Centre (RIPE NCC)
  - American Registry for Internet Numbers (ARIN)
  - Asia-Pacific Network Information Centre (APNIC)
  - Latin American and Caribbean Internet Addresses Registry (LACNIC)
  - African Network Information Centre (AfriNIC)
- Diese bedienen die Local Internet Registries (LIR) "Provider"

Übersicht:
IANA IPv4 Address Space Registry
http://www.iana.org/assignments/ipv4-address-space/ipv4-address-space.xml

Woher kommen die Nummern / Adressen?

Domains

- Domains: Vergabe durch NICs je TLD

Übersicht:
IANA Root Zone Database
http://www.iana.org/domains/root/db/

Von dort ausgehend die Whois-Datenbanken der NICs,
z.B. Denic
http://www.denic.de/

Was kann man damit rauskriegen?

Eigene IP-Nummer ermitteln

Ping:
Programm, das feststellt, ob ein bestimmter Rechner im Netz ist
Diverse Programme, normalerweise Konsolenbefehl, aber auch Webservices:

Online web-based ping: Free online ping from 50 locations worldwide
http://www.just-ping.com/index.php

IP Check
http://ip-check.info/?lang=de

Firefox Addon "Show MyIP"
https://addons.mozilla.org/de/firefox/addon/show-myip/

Was kann man damit rauskriegen?

Weg der Datenpakete ermitteln mit Traceroute (u.ä.)

Traceroute (traceroute6, tracert, mtr) stellen den Weg der Datenpakete dar.

Übersicht über webbasierte traceroutes:
http://www.traceroute.org/

YouGetGignal Visual Traceroute
http://www.yougetsignal.com/tools/visual-tracert/

Was kann man damit rauskriegen?

Wo ist die IP?

YouGetSignal
http://www.yougetsignal.com/tools/network-location/

IP-Adres.eu
http://adres-ip.eu/

IP-address.com - IP Tracer and IP Locator
http://www.ip-adress.com/ip_lokalisieren/

Was kann man damit rauskriegen?

Welche Domains mappen darauf?

YouGetSignal Reverse IP Somain Check
http://www.yougetsignal.com/tools/web-sites-on-web-server/

OnSameHost
http://www.onsamehost.org/

Domains by IP
http://domainsbyip.com/

Vielen Dank für die Aufmerksamkeit

Albrecht Ude
albrecht@ude.de
www.ude.de
https://privacybox.de/aude.msg