Das Domain Name System (DNS)

Tom Gries

Dokumenten URL: http://docs.tx7.de/TT-DNS
Autor: Tom Gries <TT-DNS@tx7.de>
@tomo@chaos.social

Version: 7.2.1 vom 16.01.2025

Namensauflösung:

Das Domain Name System (DNS) ist das zweite Rückgrat des Internets (das Erste sind die Hochgeschwindigkeitsverbindungen und Router zwischen den Providern).

DNS wurde als Nachfolger der lokalen Hosts Datei entwickelt und 1983 veröffentlicht. Die Hauptaufgabe besteht in der Beantwortung von Anfragen zur Namensauflösung, also dem Herausfinden einer IP Adresse zu einem Hostnamen (Forward Lookup) und umgekehrt (Reverse Lookup).

Aufbau des Domain Name Systems:

Das DNS besteht aus hunderttausenden von Nameservern. Eine besondere Stellung nehmen die sogenannten Root Nameserver ein. Diese stehen an der Spitze der Hierarchie und beantworten mehrere Milliarden Anfragen pro Tag.

Der Namensraum wird in sogenannten Zonen verwaltet. Diese können (und sollten) auf mehreren Nameservern verteilt sein.

Das Domain Name System ist technisch gesehen eine verteilte Datenbank. Vorläufer, aber immer nocht genutzt, ist die lokale HOSTS-Datei.

Beispiel einer lokalen HOSTS-Datei:

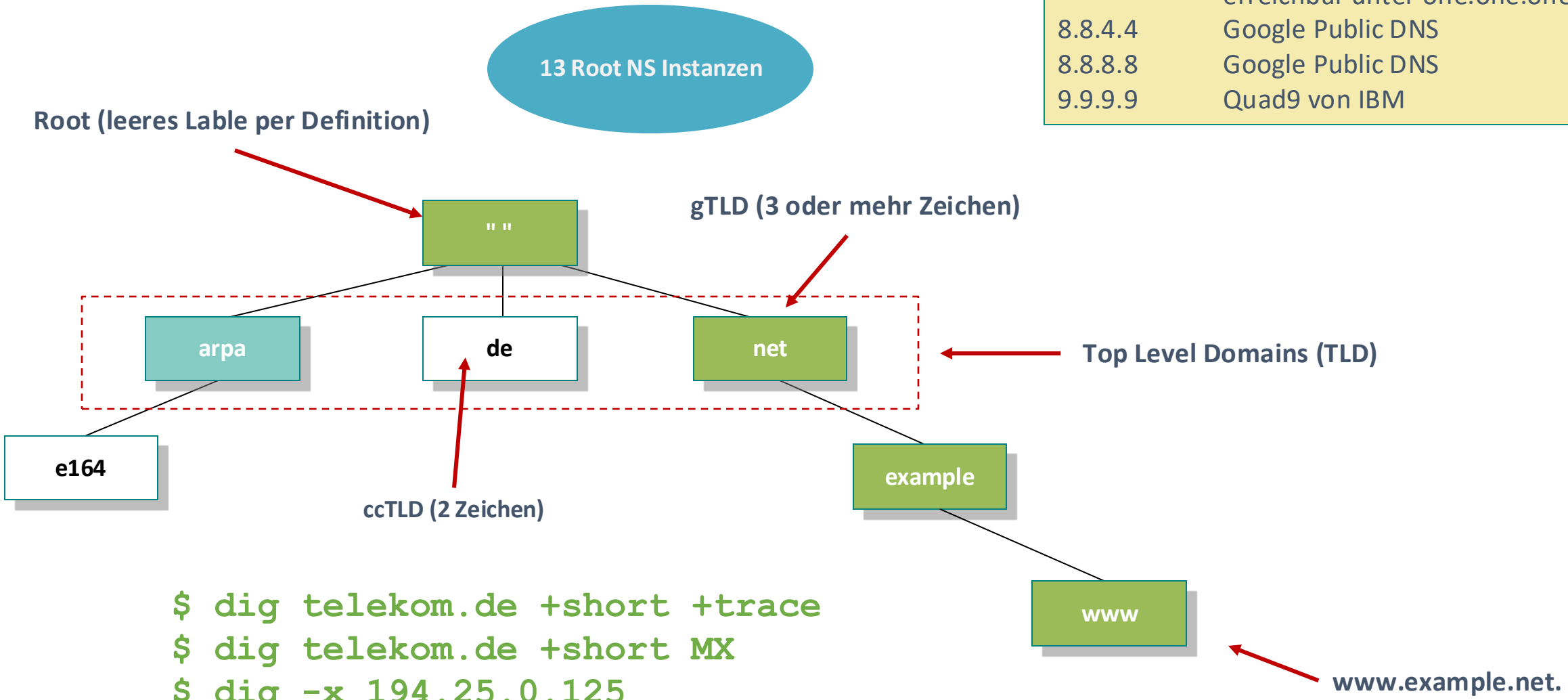
```
# This is a sample HOSTS file.
#
# This file is stored at C:\Windows\System32\drivers\etc\hosts
# on Windows machines and at /etc/hosts on Linux/Unix machines.


127.0.0.7           me
127.0.0.7           laptop.home.local
127.127.127.127     EinsZwoSieben Quad127
```

Adressierung - Das DNS

Frei verfügbare Nameserver (Auszug):

1.1.1.1	Cloudflare (schnellster). Auch erreichbar unter one.one.one.one
8.8.4.4	Google Public DNS
8.8.8.8	Google Public DNS
9.9.9.9	Quad9 von IBM



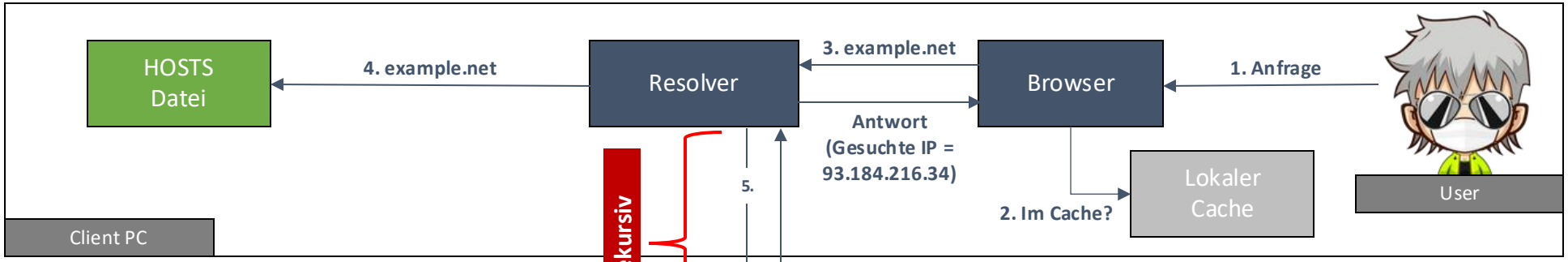

```
$ dig telekom.de +short +trace
$ dig telekom.de +short MX
$ dig -x 194.25.0.125
```

Beispiel einer Nameserver Zonendatei (BIND):

```
example.net. 3600  IN  SOA  ns.icann.org. noc.dns.icann.org.    (
                       2022091355        ; Seriennummer
                       7200              ; Refresh Time
                       3600              ; Retry Time
                       209600            ; Expire Time
                       3600              ; Negative Caching Time   )

example.net.           86400  IN   NS      a.iana-servers.net.
example.net.           86400  IN   NS      b.iana-servers.net.
example.net.           86400  IN   A       93.184.216.34
www.example.net.       86400  IN   A       93.184.216.34
example.net.           86400  IN   MX      10 example.net.
```

DNS Abfrage mit Rekursion und Iteration



Zu 7. (Hint Datei):

F: Wie heißen die Root-NS?

A: a.root-servers.net

A: b.root-servers.net [… bis m = 13]

Zu 8. (z. B. b.root-servers.net):

F: Wer ist zuständig für net.?

A: d.gtld-servers.net [a bis m = 13]

A: IPv4 = 192.31.80.30

Zu 9. (an d.gtld-servers.net):

F: Wer ist zuständig für example.net.?

A: a.iana-servers.net [a oder b]

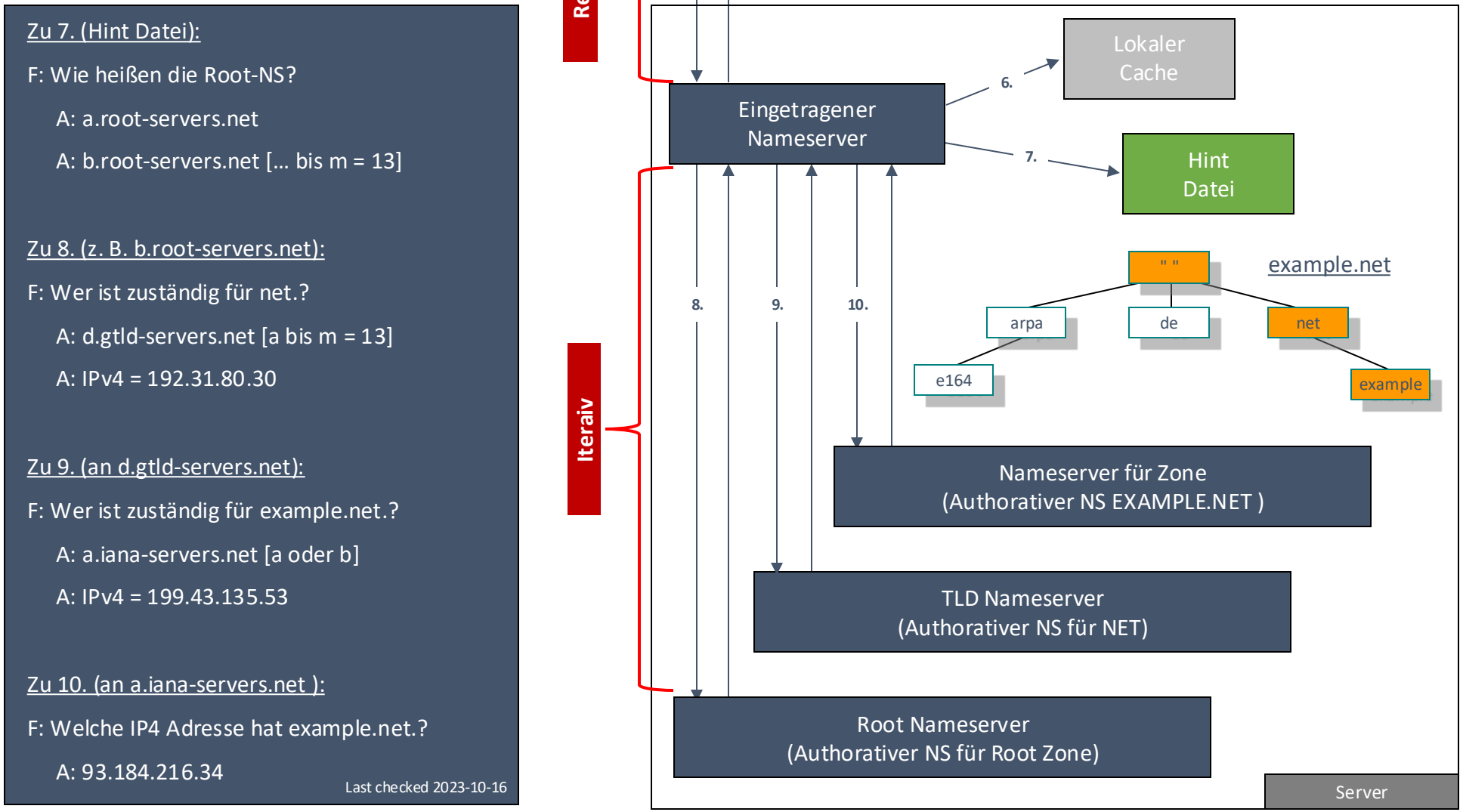
A: IPv4 = 199.43.135.53

Zu 10. (an a.iana-servers.net):

F: Welche IP4 Adresse hat example.net.?

A: 93.184.216.34

Last checked 2023-10-16



Beschreibung der Namensauflösung

01: Der User gibt http://example.net in seinen Browser ein.

02: Der Browser übergibt die Anfrage zur Namensauflösung an den Resolver des Betriebssystems (der Browser übernimmt diese Aufgabe nicht selbst).

03: Der Resolver schaut in der lokalen hosts-Datei nach, ob für den Domainname bereits eine IP-Adresse eingetragen ist. Falls der Domainname in der hosts-Datei eingetragen ist, wird das Ergebnis (die IP-Adresse) an den Browser gesendet.

04: Falls der Domainname nicht in der hosts-Datei eingetragen ist, wird der im Betriebssystem eingetragene Nameserver (der Zugewiesene) mit der Auflösung beauftragt (rekursiv) oder er antwortet mit einen Verweis auf einen anderen Nameserver (iterative). Das Verhalten ist abhängig von der Konfiguration des befragten Nameservers. Normalerweise wird die Anfrage rekursiv bearbeitet.

Beschreibung der Namensauflösung

05: Der eingetragene Nameserver schaut in seinem Cache nach, ob er die Antwort bereits kennt. Falls ja, wird diese an den Resolver zurück geliefert. Der Resolver wiederum liefert die Antwort an den Browser.

06: Ist die Antwort nicht im lokalen Cache vorhanden, wird der zuständige (autorative) Nameserver gesucht und befragt. Hierzu wird als erstes in der lokalen hint-Datei nachgeschaut, wie die Root-Nameserver heißen und wo (unter welchen IP-Adresse) sie zu finden sind.

07: Aus der Ergebnisliste wird ein Root-Nameserver herausgesucht und befragt, wer für die TLD .NET zuständig ist.

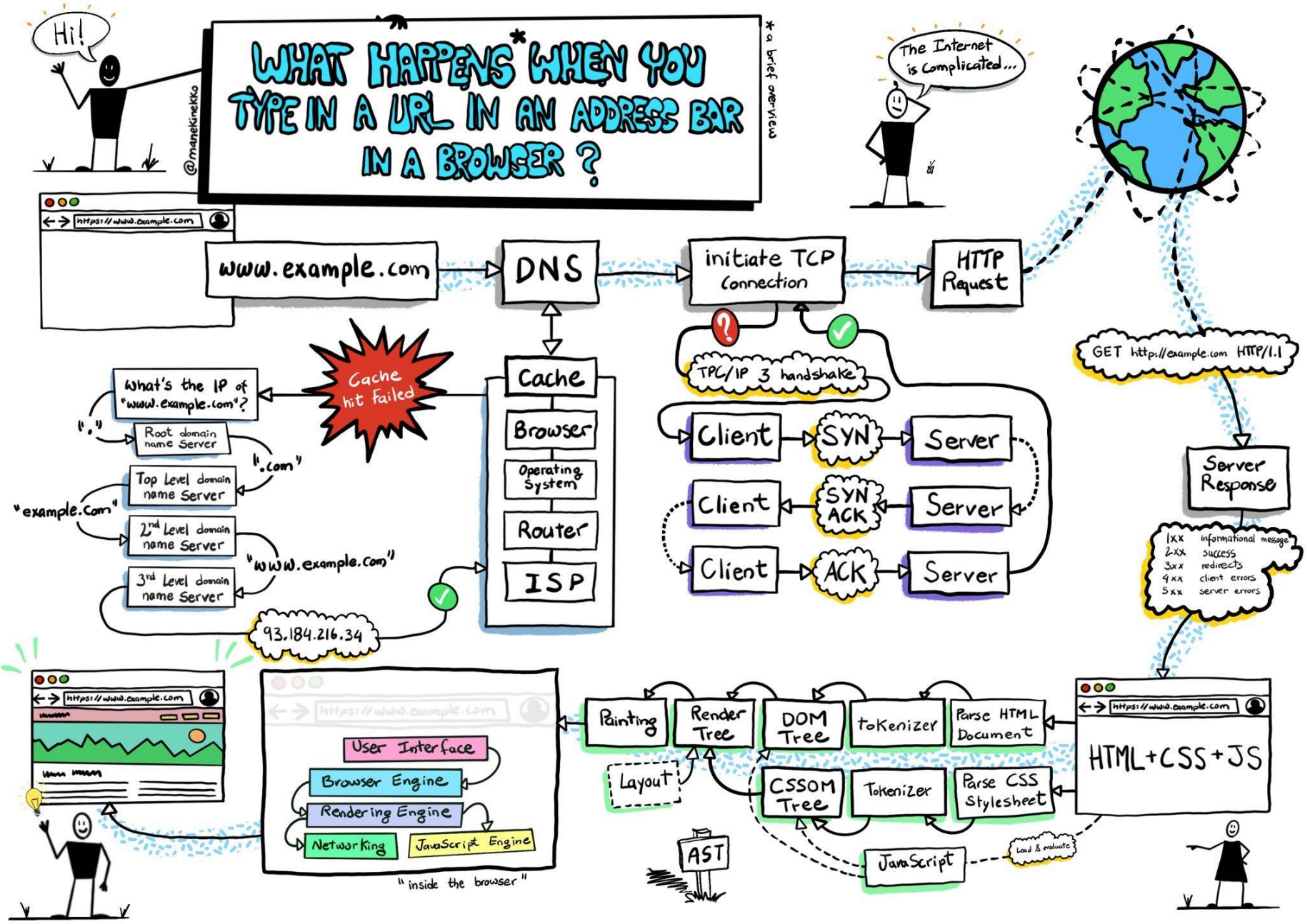
08: Aus dieser Ergebnisliste wiederum wird ein Nameserver herausgesucht und nach der Zone EXAMPE.NET befragt.

Beschreibung der Namensauflösung

09: Der Nameserver aus der Antwort zuvor ist der Autorative und gibt die IP-Adresse als Antwort an den anfragenden Nameserver (unser eingetragener Nameserver von unserem Provider) zurück. Dieser wiederum reicht die Antwort an den anfragenden Resolver weiter, der das Ergebnis an den Browser übergibt.

Auf welche Art auch immer - der Browser hat jetzt eine Antwort. Entweder eine IP-Adresse oder den Hinweis, dass keine IP-Adresse gefunden wurde. Wenn eine Antwort gefunden wurde ist sie entweder autorativ (der tatsächlich zuständige Nameserver hat die Antwort selbst geliefert) oder nicht-autorativ - dann hat ein anderer Nameserver (zum Beispiel aus dem Cache) die Antwort bereitgestellt.

Als Ergebnis der Auflösung hat der Browser jetzt eine IP-Adresse, an die er seine eigentliche Anfrage (HTTP-Request) senden kann.



 Quelle: https://github.com/manekinekko

Anmerkungen oder Fragen?