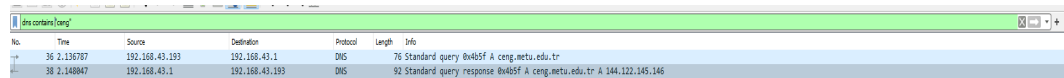


Network THE 1 Report

Uygar Yaşar / 2310613

November 3, 2022

1 HTTP

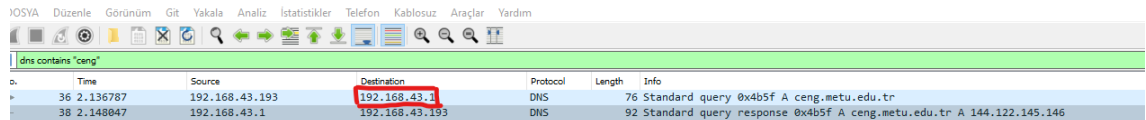


A screenshot of a Wireshark packet capture window. The filter bar at the top shows 'dns contains "ceng"'. The packet list below shows two packets:

No.	Time	Source	Destination	Protocol	Length	Info
36	2.136787	192.168.43.193	192.168.43.1	DNS	76	Standard query 0x4b5f A ceng.metu.edu.tr
38	2.148847	192.168.43.1	192.168.43.193	DNS	92	Standard query response 0x4b5f A ceng.metu.edu.tr A 144.122.145.146

Figure 1: DNS queries of my capture

1- There is just one query were sent from my computer to the DNS server to get the <http://ceng.metu.edu.tr>'s address.



A screenshot of a Wireshark packet capture window with a menu bar and toolbar. The filter bar shows 'dns contains "ceng"'. The packet list below shows two packets, with the destination IP address '192.168.43.1' in the first packet highlighted by a red box:

No.	Time	Source	Destination	Protocol	Length	Info
36	2.136787	192.168.43.193	192.168.43.1	DNS	76	Standard query 0x4b5f A ceng.metu.edu.tr
38	2.148847	192.168.43.1	192.168.43.193	DNS	92	Standard query response 0x4b5f A ceng.metu.edu.tr A 144.122.145.146

Figure 2: DNS queries with annotation of IP address.

2- One server were queried for the DNS request.

3- The queried IP address of the queried DNS server is 192.168.43.1 (figure 1 and figure 2).

1 Answer

Active Oldest Votes

▲
1
▼

✓


Are you talking about the authority section in the DNS response? If that section contains any servers (it need not contain any) then they all supposed to be able to give you authoritative answers to the query in question. The (recursive) nameserver that generated the response need not (can not) guarantee that, though, nor does it tell you which one it queried to get the response: it might even have queried more than one, or none at all (if it answered from its cache).

🔄

If you just want to get a list of authoritative servers for a domain, query that domain for `NS` records and look at the answer section (not the authority section). That's the published information prescribed by the zone's author about which nameservers one is supposed to use to get authoritative responses for that domain.

Share Improve this answer Follow

answered Jan 26 '13 at 17:11

 Celada

20.5k 3 58 73

Add a comment

Figure 3: Stackoverflow answer on caches.
<https://stackoverflow.com/questions/14538770/dns-authoritative-name-server>

4- Internet service provider probably caches the response (Since the destination address is the address of ISP). However, the response was not cached by my own computer. (If it was cached locally, there would be authoritative nameservers part in figure 4)

```
> Frame 38: 92 bytes on wire (736 bits), 92 bytes captured (736 bits)
> Ethernet II, Src: XiaomiCo_ac:5a:18 (28:16:7f:ac:5a:18), Dst: IntelCor_ca:35:1e (3c:6a:a7:ca:35:1e)
> Internet Protocol Version 4, Src: 192.168.43.1, Dst: 192.168.43.193
> User Datagram Protocol, Src Port: 53, Dst Port: 50444
▼ Domain Name System (response)
  Transaction ID: 0x4b5f
  > Flags: 0x8180 Standard query response, No error
    Questions: 1
    Answer RRs: 1
    Authority RRs: 0
    Additional RRs: 0
  > Queries
  > Answers
    [Request In: 36]
    [Time: 0.011260000 seconds]
```

Figure 4: DNS response.

38	2.148047	192.168.43.1	192.168.43.193	DNS	92 Standard query response 0x4b5f A ceng.metu.edu.tr A 144.122.145.146
39	2.148684	192.168.43.193	144.122.145.146	TCP	66 53862 → 80 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 WS=256 SACK_PERM
40	2.148937	192.168.43.193	144.122.145.146	TCP	66 53863 → 80 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 WS=256 SACK_PERM
41	2.149253	192.168.43.1	192.168.43.193	DNS	100 Standard query response 0x0d34 A www.googletagmanager.com A 172.217.17.104
42	2.149860	192.168.43.193	192.168.43.1	DNS	80 Standard query 0x46d0 A platform.twitter.com
43	2.152122	192.168.43.1	192.168.43.193	DNS	299 Standard query response 0x46d0 A platform.twitter.com CNAME cs472.wac.edge
44	2.189303	192.168.43.1	192.168.43.193	DNS	100 Standard query response 0x08b3 A www.google-analytics.com A 172.217.17.110
45	2.192834	144.122.145.146	192.168.43.193	TCP	62 80 → 53862 [SYN, ACK] Seq=0 Ack=1 Win=29200 Len=0 MSS=1339 WS=1024

Figure 5: All request/responses without any filtering.

5- The protocol of the first request is TCP because open socket and connection is needed before creating HTTP request/response pair. The pair is in 39th and 45th lines. the time difference is 0.04415.

46	2.192898	192.168.43.193	144.122.145.146	TCP	54 53862 → 80 [ACK] Seq=1 Ack=1 Win=6
47	2.193054	144.122.145.146	192.168.43.193	TCP	54 [TCP ACKed unseen segment] 80 → 53
48	2.193085	192.168.43.193	144.122.145.146	TCP	54 53863 → 80 [RST] Seq=554832586 Win
49	2.193329	192.168.43.193	144.122.145.146	HTTP	785 GET / HTTP/1.1
50	2.229693	144.122.145.146	192.168.43.193	TCP	54 80 → 53862 [ACK] Seq=1 Ack=732 Win
51	2.361610	144.122.145.146	192.168.43.193	TCP	5410 80 → 53862 [ACK] Seq=1 Ack=732 Win
52	2.361662	192.168.43.193	144.122.145.146	TCP	54 53862 → 80 [ACK] Seq=732 Ack=5357

```

> Frame 49: 785 bytes on wire (6280 bits), 785 bytes captured (6280 bits)
> Ethernet II, Src: IntelCor_ca:35:1e (3c:6a:a7:ca:35:1e), Dst: XiaomiCo_ac:5a:18 (28:16:7f:ac:5a:18)
> Internet Protocol Version 4, Src: 192.168.43.193, Dst: 144.122.145.146
> Transmission Control Protocol, Src Port: 53862, Dst Port: 80, Seq: 1, Ack: 1, Len: 731
▼ Hypertext Transfer Protocol
  > GET / HTTP/1.1\r\n
    Host: ceng.metu.edu.tr\r\n
    Connection: keep-alive\r\n
    Pragma: no-cache\r\n
    Cache-Control: no-cache\r\n
    Upgrade-Insecure-Requests: 1\r\n
    User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/106.0.0.0 Safari/537.36\r\n
    Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,image/apng,*/*;q=0.8,application/signed-exch...
    Accept-Encoding: gzip, deflate\r\n
    Accept-Language: tr-TR,tr;q=0.9,en-US;q=0.8,en;q=0.7\r\n
    Cookie: _fbp=fb.2.1664276623132.958327522; _ga=GA1.3.303919058.1664276623; _APP_LOCALE=EN; _gid=GA1.3.1062275186.1667046616; SE...
    \r\n
    [Full request URI: http://ceng.metu.edu.tr/]
    [HTTP request 1/1]
    [Response in frame: 72]

```

Figure 6: Cookies and user-agent of the first HTTP request.

6- Yes there were cookies, It can be seen from figure 6.

7-

a) User-agent string can be seen from figure 6.
(Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/106.0.0.0 Safari/537.36\r\n)

b) The user-agent string is the string that identifies the operating system, browser and application. It includes all the compatible browsers. For example, I used Google Chrome as browser it is also compatible on safari.

2 DNS

DNSs are responsible for connecting domain names to web servers and gives requested IP address to the user by translating domain into the host IP address.

There are some record types. For this case mail exchange (MX) records must be used. MX records specify the incoming mail servers that receive email messages to a domain name. Receiving servers checks the DNS records and permissions.

Sending server: Hello, I have an email for bob@yourcompany.com
Receiving server: yourcompany.com? Let me check DNS records. You do not have permission to send email on behalf of yourcompany.com. I'm rejecting you.
Sending server: Ugh. I guess I need to fix my DNS so you will accept it. (from <https://www.godaddy.com/garage/configuring-dns-for-email-a-quick-beginners-guide/>)

So, we can basically send email behalf of somebody else by arranging DNS.

In merkel@de case, probably she would never read our email. However, if we send mail acting like Olaf Scholz (chancellor of Germany) (if there is no checking mechanism it is possible.) and sending email by using scholz@de impact will become higher and probably we can reach Angela Merkel just using her DNS and configuring ours.

Also, domain names should have matched with "@de" part, so just matching the IP of Merkel is enough to sending these news to her.