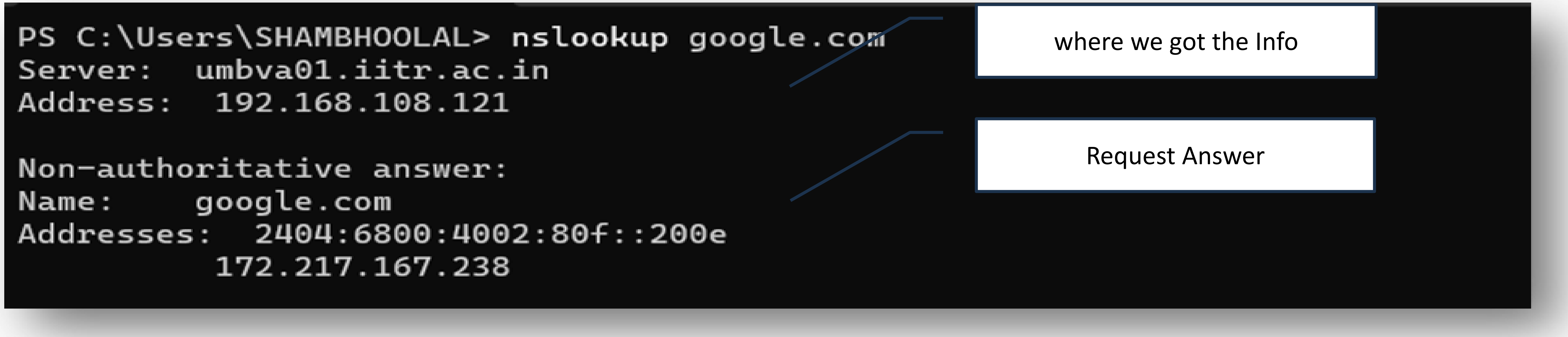
DNS Over HTTPS

Domain Name System Works

Take the domain name www.google.com, for example; using the tool nslookup, we can perform a DNS query to look up the associated IP address, in this case, 172.217.167.238.



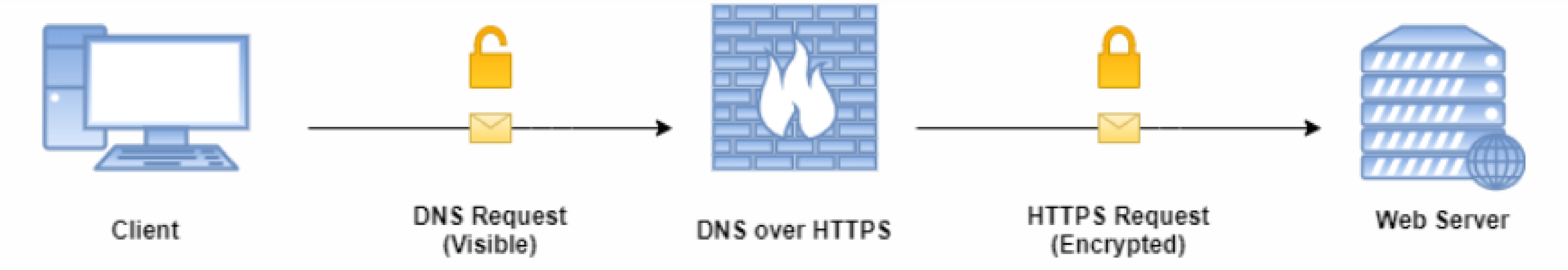
```
PS C:\Users\SHAMBHOOLAL> nslookup google.com
Server:  umbva01.iitr.ac.in
Address:  192.168.108.121

Non-authoritative answer:
Name:    google.com
Addresses:  2404:6800:4002:80f::200e
          172.217.167.238
```

Privacy Concerns

Privacy concerns arise as DNS queries, which occur over plain text, can be viewed by anyone between your computer and the server, including ISPs, governments, and eavesdroppers. Domain names were created to make it easier for computers to remember the IP address of a server. A Domain Name Server is used to map this easy-to-remember domain name to the associated IP address.

What is DOH - DNS Over HTTPS?

DNS over HTTPS (DoH) enables Domain Name System (DNS) resolution via the HTTPS protocol. The classic DNS protocol transmits information in plaintext and, therefore, does not protect against network eavesdroppers. The primary goal of DoH is to incrementally improve user privacy by using HTTPS to encrypt the data between the DoH client and the DoH server. This hides, in effect, the name of websites that users are accessing using their web browsers from public or private network owners or users, including from ISPs or guest Wi-Fi networks.

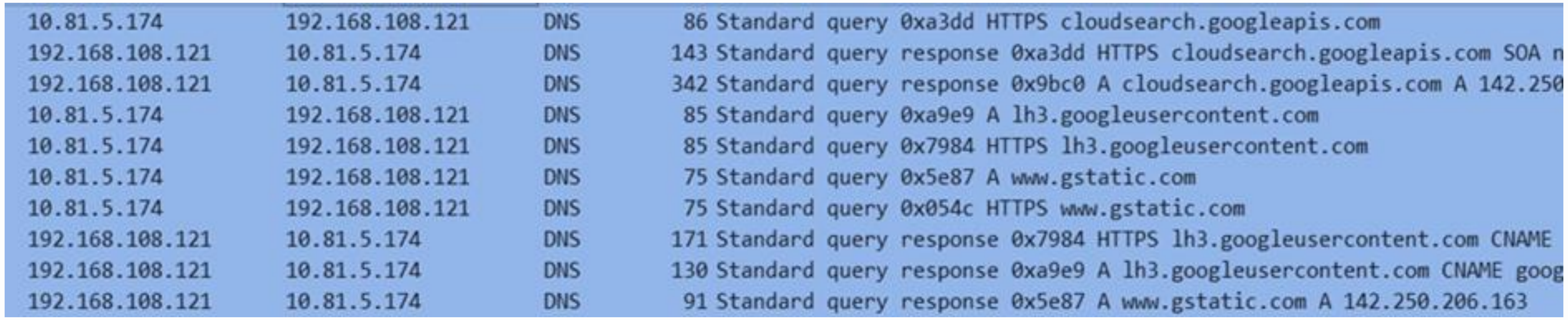


The route of a DNS query when DoH is enabled.

Demonstration

1.Simple DNS Query

As I mentioned before, this DNS query takes place over plain text. Below is an illustration of a DNS query when navigating to https://www.google.com. This was taken from a tool called Wireshark, which allows me to sniff all the packets being sent to and from my system, essentially doing what the government, ISP, eavesdropper, etc, would potentially do.



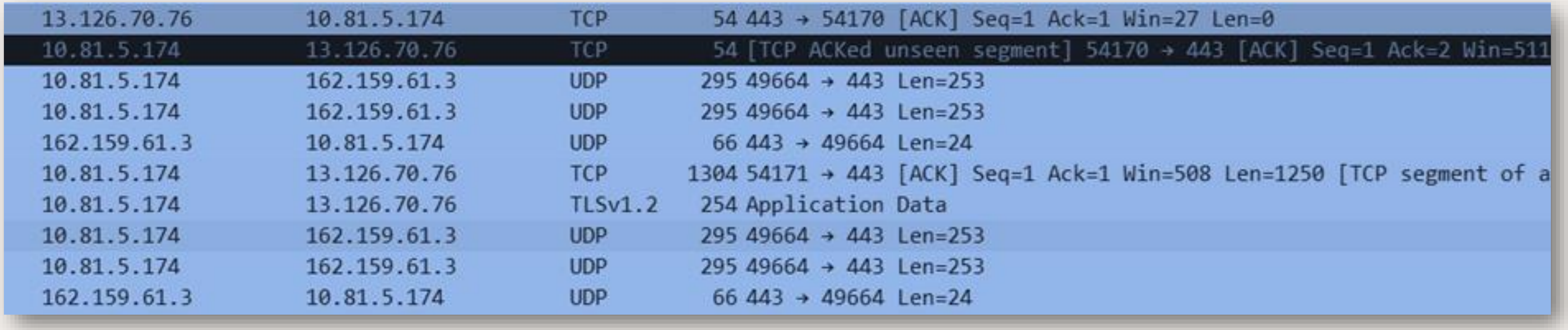
```
10.81.5.174        192.168.108.121   DNS     86 Standard query 0xa3dd HTTPS cloudsearch.googleapis.com
192.168.108.121    10.81.5.174       DNS    143 Standard query response 0xa3dd HTTPS cloudsearch.googleapis.com SOA n
192.168.108.121    10.81.5.174       DNS    342 Standard query response 0x9bc0 A cloudsearch.googleapis.com A 142.250
10.81.5.174        192.168.108.121   DNS     85 Standard query 0xa9e9 A lh3.googleusercontent.com
10.81.5.174        192.168.108.121   DNS     85 Standard query 0x7984 HTTPS lh3.googleusercontent.com
10.81.5.174        192.168.108.121   DNS     75 Standard query 0x5e87 A www.gstatic.com
10.81.5.174        192.168.108.121   DNS     75 Standard query 0x054c HTTPS www.gstatic.com
192.168.108.121    10.81.5.174       DNS    171 Standard query response 0x7984 HTTPS lh3.googleusercontent.com CNAME
192.168.108.121    10.81.5.174       DNS    130 Standard query response 0xa9e9 A lh3.googleusercontent.com CNAME goog
192.168.108.121    10.81.5.174       DNS     91 Standard query response 0x5e87 A www.gstatic.com A 142.250.206.163
```

As you quite clearly see, the hostname is www.gstatic.com, so I know you visited www.google.com. Now, Google is a benign example but imagine a more sensitive site. ISPs, governments, and other organizations could also use this information to form a picture of users' browsing habits.

2. DNS Over HTTPS?

Cloudflare's new DNS service tries to combat this by supporting DNS-over-HTTPS, which sends the DNS query over an encrypted channel. This means those wishing to obtain which sites you visit can no longer do so by viewing your DNS queries.

The first browser is set on a secure connection using Cloudflare (1.1.1.1). Below is an example of a DNS-over-HTTPS query performed with the tool Wireshark:



```
13.126.70.76    10.81.5.174     TCP        54 443 → 54170 [ACK] Seq=1 Ack=1 Win=27 Len=0
10.81.5.174     13.126.70.76    TCP        54 [TCP ACKed unseen segment] 54170 → 443 [ACK] Seq=1 Ack=2 Win=511
10.81.5.174     162.159.61.3    UDP       295 49664 → 443 Len=253
10.81.5.174     162.159.61.3    UDP       295 49664 → 443 Len=253
162.159.61.3    10.81.5.174     UDP        66 443 → 49664 Len=24
10.81.5.174     13.126.70.76    TCP      1304 54171 → 443 [ACK] Seq=1 Ack=1 Win=508 Len=1250 [TCP segment of a
10.81.5.174     13.126.70.76    TLSv1.2   254 Application Data
10.81.5.174     162.159.61.3    UDP       295 49664 → 443 Len=253
10.81.5.174     162.159.61.3    UDP       295 49664 → 443 Len=253
162.159.61.3    10.81.5.174     UDP        66 443 → 49664 Len=24
```

When viewing the associated traffic in Wireshark, we can see that the DNS query now takes place over HTTPS, and as a result, I no longer have the ability to see the domain name, in this case, www.google.com

Impact On User Experience.

1. **Privacy and Security**:
Positive Impact: DoH protects individual users’ privacy by encrypting DNS queries, potentially preventing eavesdropping and manipulation from man-in-the-middle attacks.

2. **Control Over Online Experiences**:
Positive Impact: Encrypting DNS queries enables users to better control their online experiences and keep their communication private.

3. **Minimal Impact on Web Browsing**:
Negative Impact: Research has found that DoH has a minimal impact or even improves the total time it takes to get a response from the resolver and fetch a web page. **DoT performs better than DoH and Do53 in terms of page load times.**

4. **Potential Issues**:
Negative: Some experts argue that DoH causes more problems than it solves, and that efforts should be focused on implementing better ways to encrypt DNS traffic, such as DNS-over-TLS. Additionally, the technology is dominated by US-based companies, over whom most governments feel they have little control.

Impact On Web Application.

Traffic originating from a DoH client passes through an Application Delivery Controller (ADC) and goes to a DoH-capable DNS resolver –

1. Performance and scalability impact on the ADC while handling traditional DNS requests vs. DoH as the ADC does TCP termination, filtering, security, etc.
2. Measure the latency and delay in the network for handling DoH requests instead of traditional DNS.
3. DoH handling capacity of the ADC for application mixes combined with HTTP, HTTP/2, and other IMIX traffic.
4. As all modern ADCs generally intercepts the encrypted packets, this test also enables DPI and IPS for DoH packets.

Increased Level of Encryption: DoH increases the level of encryption, which can impact the performance of network infrastructure elements and content-aware devices.

Increased Number of New Encrypted Connections: DNS transactions are small, which increases the number of new encrypted connections per second (DNS queries per second).

Mixed Performance Impact: The impact on speed is different for different users, with some experiencing slower response times and others seeing faster ones.