** Curling wetransfer.com

- curl steps can be outlined as following:

bash-3.2$ curl -svo /dev/null wetransfer.com

*** Trying 34.250.122.178:80...**
*** Connected to wetransfer.com (34.250.122.178) port 80 (#0)**
> GET / HTTP/1.1
> Host: wetransfer.com
> User-Agent: curl/7.77.0
> Accept: */*
>
* Mark bundle as not supporting multiuse
< HTTP/1.1 301 Moved Permanently
< Date: Fri, 08 Jul 2022 13:49:08 GMT
< Content-Length: 0
< Connection: keep-alive
< location: https://wetransfer.com/
<
* Connection #0 to host wetransfer.com left intact

- DNS/Web server IPs for wetransfer.com .

bash-3.2$ dig wetransfer.com

; <<>> DiG 9.10.6 <<>> wetransfer.com
;; global options: +cmd
;; Got answer:
;; ->>HEADER<<- opcode: QUERY, status: NOERROR, id: 49180
;; flags: qr rd ra; QUERY: 1, ANSWER: 3, AUTHORITY: 0, ADDITIONAL: 1

;; OPT PSEUDOSECTION:
; EDNS: version: 0, flags:; udp: 1220
;; QUESTION SECTION:
;wetransfer.com. IN A

;; ANSWER SECTION: >>> DOMAN IPs
wetransfer.com. 39 IN A 34.254.21.56
wetransfer.com. 39 IN A 34.250.122.178
wetransfer.com. 39 IN A 18.202.115.26

;; Query time: 12 msec
;; SERVER: 192.168.100.1#53(192.168.100.1) >> Web Server IP
;; WHEN: Fri Jul 08 03:19:47 EET 2022
;; MSG SIZE rcvd: 91

- Protocols used :

wetransfer.com URL is using various protocols:

1. **Domain Name System (DNS) protocol** to convert a domain name into an IP address.

   Domain Name : wetransfer.com
   3 IPs for the domain :

   wetransfer.com. 39 IN A 34.254.21.56
   wetransfer.com. 39 IN A 34.250.122.178
   wetransfer.com. 39 IN A 18.202.115.26

2. It uses the **HyperText Transfer Protocol (HTTP)** to request the webpage contents from the domain IP address.

3. It also use the **Transport Layer Security (TLS) protocol** to serve the website over a secure, encrypted connection as following:

   *** SSL connection using TLSv1.2 / ECDHE-RSA-AES128-GCM-SHA256**
   * ALPN, server accepted to use h2
   *** Server certificate:**
   *** subject: CN=wetransfer.com**
   * start date: Jul 7 00:00:00 2022 GMT
   * expire date: Aug 5 23:59:59 2023 GMT
   *** subjectAltName: host "wetransfer.com" matched cert's "wetransfer.com"**
   *** issuer: C=US; O=Amazon; OU=Server CA 1B; CN=Amazon**
   * SSL certificate verify ok.
   * Using HTTP2, server supports multi-use
   * Connection state changed (HTTP/2 confirmed)
   * Copying HTTP/2 data in stream buffer to connection buffer after upgrade: len=0

- From above , following explains shortly when executing curl wetransfer.com:

- The first place the operating system is going to check for the address of the URL wetransfer.com is in the hosts file (/etc/hosts in Linux and Mac, c:\windows\system32\drivers\etc\hosts in Windows).
- If the URL is not found inside /etc/hosts file , then the OS will make a

DNS request to find the IP Address of the URL wetransfer.com web page.

- The first step is to ask the DNS Resolver (or Internet Service Provider) server to look up in its cache to see if it knows the IP Address.
- if the Resolver does not know then it asks the root server to ask the .COM TLD (Top Level Domain) server. the TLD server will again check in its cache to see if the requested IP Address is there.
- If not, then it will have at least one of the authoritative name servers associated with that URL, and after going to the Name Server, it will return the IP Address associated with the URL wetransfer.com.
- After the OS has Domain IP Address , it then makes a GET (a type of HTTP Method) to said IP Address.
- When it makes the request to the OS which then, in turn, packs the request in the TCP traffic protocol, and it is sent to the domain IP Address
- On its way, it is checked by both the OS' and the server's firewall to make sure that there are no security violations.
- And upon receiving the request the server (usually a load balancer that directs traffic to all available web servers for the website (wetransfer.com) sends a response with the IP Address of the chosen server along with the SSL (Secure Sockets Layer) certificate to initiate a secure session (HTTPS) https://wetransfer.com
- Finally, the chosen server then sends the HTML, CSS, and Javascript files back to the OS who in turn gives it web server to interpret it. And then you get the website wetransfer.com.