NIA 2024T CA2 solution

Redes y aplicaciones Internet (Universitat Oberta de Catalunya)

Computer Science, Multimedia and Telecommunications Studies

Networks and Internet Applications
Activity: CA2 – Second Continuous Assessment Test

- The solution must be delivered in a PDF file in the subject classroom.
- You must include references to the resources you consulted to answer the questions.
- The delivery deadline is **December 1st, 2024**

Questions

1. Use the dig program on Linux to obtain DNS protocol information for the domain google.com. If you do not have a Linux system you can use the website http://www.kloth.net, which offers the service for dig (http://www.kloth.net/services/dig.php). For the proposed domain, perform the following queries, attaching a screenshot with the result and explaining the different blocks that appear in the response:

    a. Make a type A query.

Dig

Domain: google.com ... the name of the machine to

Server: localhost ... the DNS nameserver you w (just start with this site's defau better).

Query: A (IPv4 address) Trace Dnssec Look it up

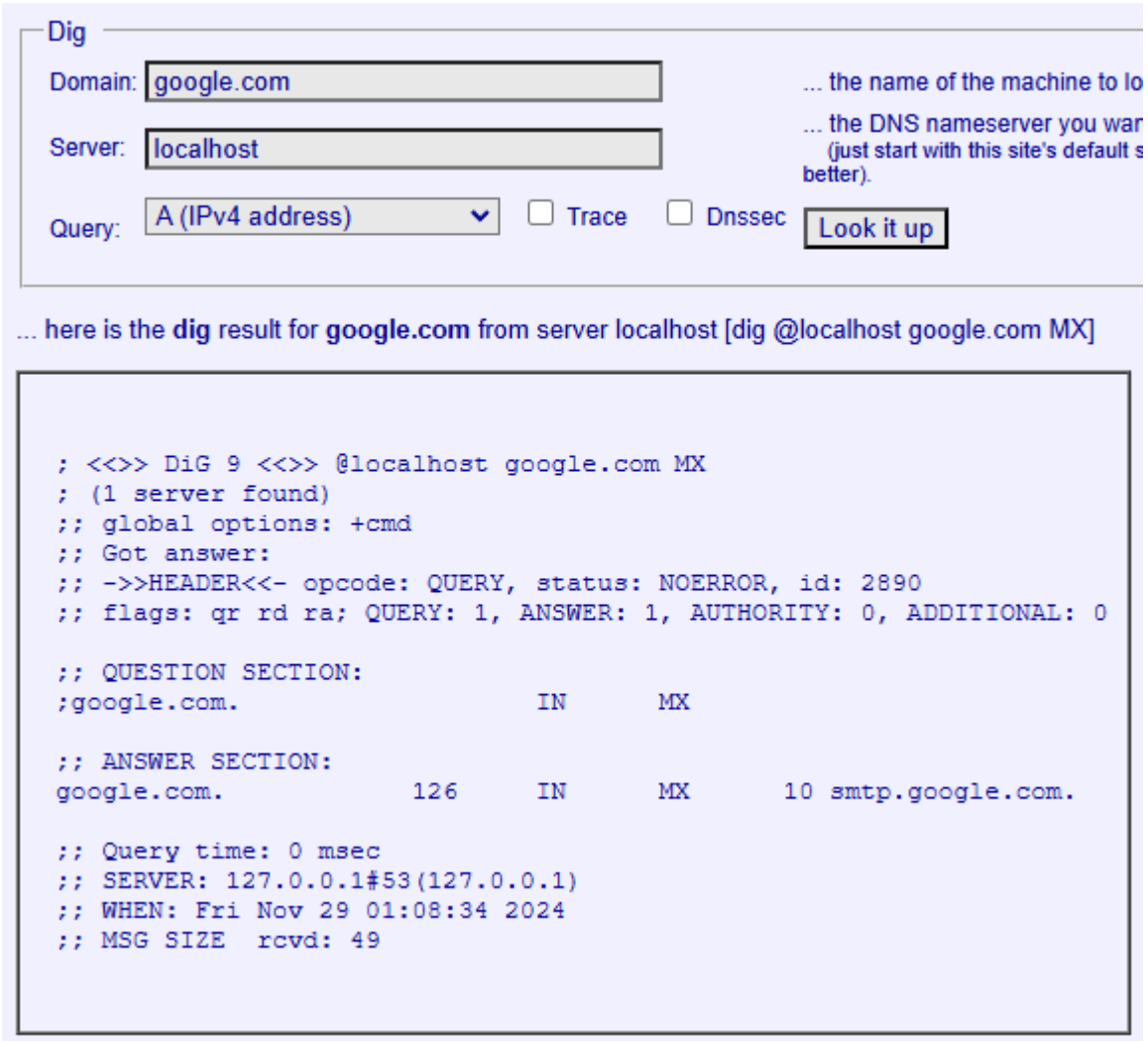
... here is the **dig** result for **google.com** from server localhost [dig @localhost google.com A]

```
; <<>> DiG 9 <<>> @localhost google.com A
; (1 server found)
;; global options: +cmd
;; Got answer:
;; ->>HEADER<<- opcode: QUERY, status: NOERROR, id: 16132
;; flags: qr rd ra; QUERY: 1, ANSWER: 1, AUTHORITY: 0, ADDITIONAL: 0

;; QUESTION SECTION:
;google.com.                    IN      A

;; ANSWER SECTION:
google.com.             47      IN      A       142.250.181.238

;; Query time: 0 msec
;; SERVER: 127.0.0.1#53(127.0.0.1)
;; WHEN: Fri Nov 29 01:08:09 2024
;; MSG SIZE  rcvd: 44
```

We see the DNS server's address, which would be the local machine
We see the name of the domain and the address we looked up.
This Type A query retrieves the IPv4 address 142.250.181.238 for google.com.

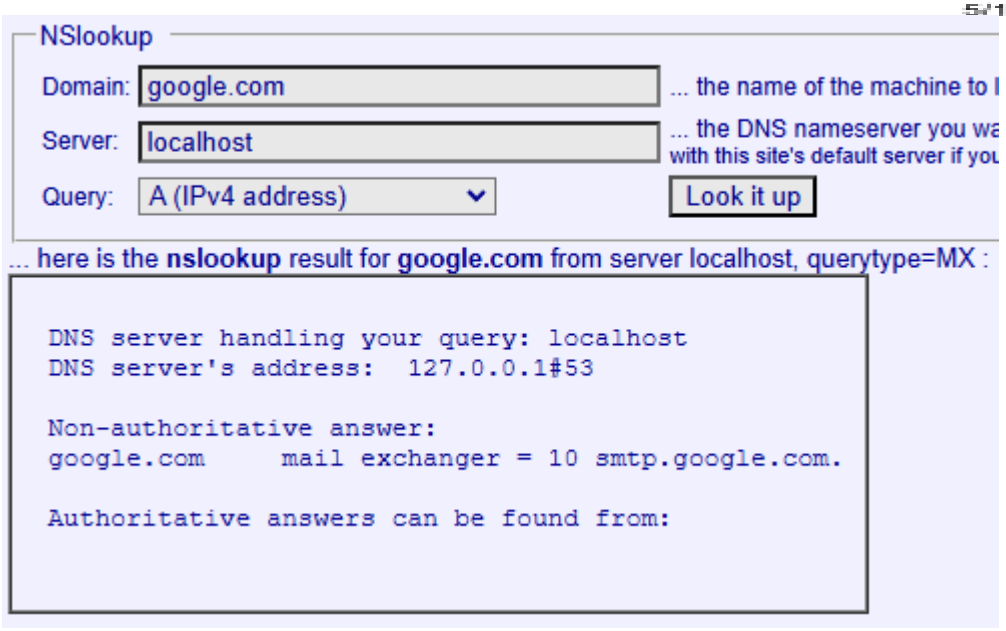
The TTL value (47) indicates the remaining time in seconds before the record expires from DNS cache.

b. Make a type MX query.



We see the smtp servers domain name and the domain name it pertains to
This query retrieves the MX record for google.com. The mail server smtp.google.com is listed with a priority of 10. This indicates that this mail server is the primary one used for handling emails sent to the domain.

c. Now, make the same MX query using nslookup tool. If you do not have a Windows system, you can use the one in http://www.kloth.net/services/nslookup.php.



This shows the MX record for google.com, identifying smtp.google.com as the mail server with priority 10.

"Non-authoritative answer" indicates the response was obtained from a DNS cache rather than directly from an authoritative DNS server.

d. Compare responses from b) and c). Why do you think there are those differences between tools' responses? Respond reasonably to the question.

dig provides detailed, structured output for diagnosing DNS issues or advanced analysis.

nslookup simplifies DNS lookups for quick, essential information.

e. Briefly describe what queries A and MX mean and if the responses you have received from the different tools provide the information associated with them.

Type A Query

Purpose: Retrieves the IPv4 address of a domain name (e.g., google.com).

Usage: This query is essential for mapping domain names to IP addresses, enabling users to connect to websites or services.

Example Response:

IP Address: 142.250.181.238 (for google.com as seen in the outputs).

Information Provided: Both dig and nslookup provided the IPv4 address, confirming the query's success.

Type MX Query

Purpose: Retrieves mail exchanger (MX) records for a domain, which specify the mail servers responsible for receiving email for that domain.

Usage: Email systems use this information to route emails to the correct mail server.

Example Response:

Mail Exchanger: smtp.google.com with a priority of 10.

Information Provided: Both dig and nslookup successfully returned the MX records, including the mail server name and its priority.

f. Make other types of queries (at least two different from the ones done until now) and briefly describe the results received. You can use one of the tools presented above, you do not need to use both of them.

Name Servers for google.com:

ns1.google.com

ns2.google.com

ns3.google.com

ns4.google.com

These are the authoritative name servers responsible for managing the DNS records of the google.com domain.

Domain: google.com

IPv6 Address: 2a00:1450:4001:82f::200e

Non-authoritative Answer: Indicates that the response was retrieved from a cache or intermediate server, not directly from an authoritative DNS server.

g. Make a type A query over www.google.com. Are there differences between this response and the one in a)? Briefly explain the received response and try to give an explanation to the observed differences.

Both tools return the same IPv4 address (142.250.181.238) for google.com.

The responses confirm that the A record resolves to the same IP in both tools.

2. HTTP and SMTP are two well-known application layer protocols which have some commonalities as well as differences. Respond reasonably to the following questions:

   a. Find a common header between both protocols and indicate what it is used for.

      The common header would be Date:

      In HTTP, the Date header indicates when the server generated the response.

      In SMTP, the Date header shows when the email was created and sent by the client.

   b. Now, describe a header unique to each protocol (not shared between them) and indicate what it is used for.

      A unique header for HTTP would be Host:
      Usage: Indicates the domain name of the server being requested

      Purpose: Necessary for virtual hosting, allowing a single server to host multiple websites.

      A unique header for SMTP would be From
      Usage: Specifies the email address of the sender

      Purpose: Identifies the origin of the email message.

   c. Choose a method for each protocol and briefly explain its usage and give an example, including parameters required by the method to properly work.

      HTTP Method: GET: example /getCountries HTTP/1.1 Host: www.example.com

      Parameters:

      Path: Specifies the resource being requested (**/getCountries**).

      Host: Indicates the target server (www.example.com

      SMTP Method: MAIL FROM: example MAIL FROM:<marwane@example.com>
      Parameters:

      <sender@example.com>: Email address of the sender.

3. In this exercise we will use the on-line resources provided by Kurose-Ross book to work with packet scheduling strategies, like FIFO, Round Robin, Priority or WFQ (https://gaia.cs.umass.edu/kurose_ross/interactive/scheduling.php). Select at least three mechanisms and justify the responses given to the different questions provided by the tool.

FIFO (First-In-First-Out):

What it does: Sends packets in the order they arrive, like a line at a cafeteria.
Pros: Easy to implement.
Cons: If a big packet is first, smaller urgent packets might be delayed, causing inefficiencies.

Priority Scheduling:

What it does: Processes important packets (e.g., live video calls) before less critical ones (e.g., emails), no matter when they arrived.
Pros: Ensures critical tasks get priority.
Cons: Low-priority packets might never get sent if high-priority traffic is constant (like always letting VIPs skip the line).

WFQ (Weighted Fair Queuing):

What it does: Divides traffic into classes and gives each class a fair share of bandwidth based on their importance, like splitting a group project workload fairly.
Pros: Balances fairness and efficiency so no traffic class is ignored.
Cons: More complicated to manage than FIFO or Priority.

4. Look at an email message that you received at the UOC throughout this year and provide a screenshot showing the original header of the message, **in raw format**. In Gmail, for example, you have the option in each message to display the menu on the right and click on Show original. Explain each part of the message, field by field. Relate the contents of the email with the information described in chapter 2.3 - Electronic Mail in the Internet from the Kurose-Ross book. You have to see, among others, the following fields: date, message-ID, subject, from, to, content-type…

Delivered-To: moukhaoucha@uoc.edu

Explanation: Specifies the recipient's email address, confirming delivery.

Relevance: Part of the destination specification process, as described in the SMTP delivery chain.

Received: by [SMTP server details]

Explanation: Tracks each mail server the email passes through.

Relevance: Reflects the path taken by the email across the internet, demonstrating the working of the **SMTP protocol**.

Return-Path: 0102019378685e98-...@eu-west-1.amazonses.com

Explanation: Indicates where bounce-back messages will be sent if delivery fails.

Relevance: Used in error reporting, which is essential for ensuring reliability in SMTP.

Authentication-Results: mx.google.com

Explanation: Shows authentication checks like DKIM (DomainKeys Identified Mail), SPF (Sender Policy Framework), and DMARC (Domain-based Message Authentication, Reporting, and Conformance).

Relevance: Demonstrates email security measures to prevent spoofing.

DKIM-Signature:

Explanation: A cryptographic signature added by the sender's domain to verify message integrity.

Relevance: Essential for preventing tampering during transmission.

From: Info UOC infouoc@uoc.edu

Explanation: Specifies the sender's address.

Relevance: Part of the **user agent** responsible for initiating the email.

To: moukhaoucha@uoc.edu

Explanation: Recipient's address.

Relevance: Reflects how the email is targeted to a specific user.

Subject: ¡Defiende tus trabajos (y tus ideas) con seguridad!

Explanation: The topic of the email.

Relevance: User-friendly metadata for categorization and preview.

Date: Fri, 29 Nov 2024 14:52:06 +0000

Explanation: Timestamp when the email was sent.

Relevance: Synchronizes time for email organization and tracking.

Message-ID: 0102019378685e98-...@eu-west-1.amazonses.com

Explanation: A unique identifier for this specific email.

Relevance: Helps in email threading and deduplication.

MIME-Version: 1.0

Explanation: Specifies the version of the MIME protocol used.

Relevance: Indicates support for multimedia content (e.g., HTML formatting).

Content-Type: text/html; charset=utf-8

Explanation: Specifies that the email content is HTML and encoded in UTF-8.

Relevance: Enables rich formatting, as discussed under **MIME extensions in email.**

Content-Transfer-Encoding: quoted-printable

Explanation: Defines how the email content is encoded for safe transport.

Relevance: Ensures compatibility across different email servers.

Original Message

Message ID	<0102019378685e98-322e2fa5-3001-4280-ab39-cc535d9a3890-000000@eu-west-1.amazonses.com>
Created at:	Fri, Nov 29, 2024 at 3:52 PM (Delivered after 0 seconds)
From:	Info UOC <infouoc@uoc.edu>
To:	moukhaoucha@uoc.edu
Subject:	¡Defiende tus trabajos (y tus ideas) con seguridad!
SPF:	PASS with IP 54.240.3.30 Learn more
DKIM:	'PASS' with domain uoc.edu Learn more
DMARC:	'PASS' Learn more

Download Original

Copy to clipboard

5. Read the chapter 2.5 - Peer-to-Peer (P2P) file distribution and search for other P2P mechanisms or P2P applications different from the ones described in the book and describe their main features, current usage and network coverage (local, worldwide, etc.). Reference the source of the information

IPFS (InterPlanetary File System):

What it does: A decentralized way to share and access files using a global system that relies on file content (not location).
Where it's used: Decentralized apps, Web3, and science data sharing.
Scope: Worldwide.
Why it matters: Makes internet content more reliable and independent of central servers.

Shareaza:
What it does: A tool to share files across multiple P2P networks like Gnutella and BitTorrent.
Where it's used: Sharing all kinds of files.
Scope: Worldwide.
Why it matters: It connects to many P2P systems, letting users get files from multiple sources.

Perfect Dark:
What it does: A Japan-based app for sharing large files, focusing on privacy and efficiency.
Where it's used: Mostly Japan.
Scope: Local to Japan, some international users.
Why it matters: Ideal for securely sharing large media files.

BitComet:
What it does: A popular app for downloading big files like movies, using BitTorrent.
Where it's used: Global file-sharing.
Scope: Worldwide.
Why it matters: Allows previews and efficient downloads.

gtk-gnutella:
What it does: A lightweight file-sharing app for the Gnutella network.
Where it's used: By people looking for a simple, efficient tool for downloading files.
Scope: Worldwide.
Why it matters: Uses fewer resources and is secure with encrypted connections.

Sources:
https://en.wikipedia.org/wiki/Gtk-gnutella
https://en.wikipedia.org/wiki/BitComet
https://en.wikipedia.org/wiki/Perfect_Dark_%28P2P%29
https://en.wikipedia.org/wiki/Shareaza
https://en.wikipedia.org/wiki/InterPlanetary_File_System

6. Look for updated information regarding Netflix CDN that complements the explanation in the Kurose-Ross book. Specifically, describe in more detail how the content is replicated on the different servers and how it is delivered to the client. Moreover, describe the differences, if any, between Netflix and other streaming services providers in terms of CDN usage. Reference the source of the information.

Netflix's Open Connect:

How Content is Stored and Replicated:
Netflix encodes its shows and movies in multiple quality levels.
Popular content is copied to Open Connect Appliances (OCAs)—special servers placed in ISP networks worldwide. This ensures the content is closer to users, reducing delays.

How Content is Delivered:
When you stream, Netflix directs you to the nearest OCA based on your location,network quality, and server load.
If the local OCA doesn't have the video, Netflix fetches it from another nearby server or its central database to keep your stream smooth.

Differences from Other Streaming Services:
Netflix: Uses its own CDN (Open Connect), giving it full control to optimize streaming quality.
Others: Rely on shared third-party CDNs like Akamai or Cloudflare, which may not be as customized or efficient.
Netflix Advantage: Has over 8,000 dedicated servers inside ISP networks, ensuring faster, more reliable streaming.

https://about.netflix.com/en/news/how-netflix-works-with-isps-around-the-globe-to-deliver-a-great-viewing-experience

https://www.theverge.com/22787426/netflix-cdn-open-connect

7. In practice 2 we have proposed implementing web services based on REST. Find information on two real examples of web services implemented with REST. For each of them, clearly indicate what service it offers and what the format of the requests and responses of one of its operations is like. Show a screenshot and explain some interaction. Do you know of any other mechanism to implement web services other than REST? Find information about what other types of web services exist (at least two) and briefly describe their features. Reference the source of the information.

8. HTTP/3 has been already published as RFC (https://www.rfc-editor.org/rfc/rfc9114). Respond reasonably to the following questions:

   a. Identify its network protocol stack and compare it with the ones in HTTP/1.1 and HTTP/2.

HTTP/1.1:

Application Layer: HTTP/1.1
Transport Layer: Transmission Control Protocol (TCP)
Security Layer: Optional Transport Layer Security (TLS)

HTTP/2:

Application Layer: HTTP/2
Transport Layer: TCP
Security Layer: Typically used with TLS

HTTP/3:

Application Layer: HTTP/3
Transport Layer: QUIC (Quick UDP Internet Connections)
Security Layer: TLS 1.3 integrated within QUIC

b. Are there any changes in HTTP commands or headers used? Which do you think is the reason for that?

HTTP/3 maintains the same HTTP semantics, including request methods, status codes, and headers, consistent with HTTP/1.1 and HTTP/2.

c. Provide two examples of websites supporting HTTP/3 protocol. How have you found out that they use the protocol? Indicate the references.

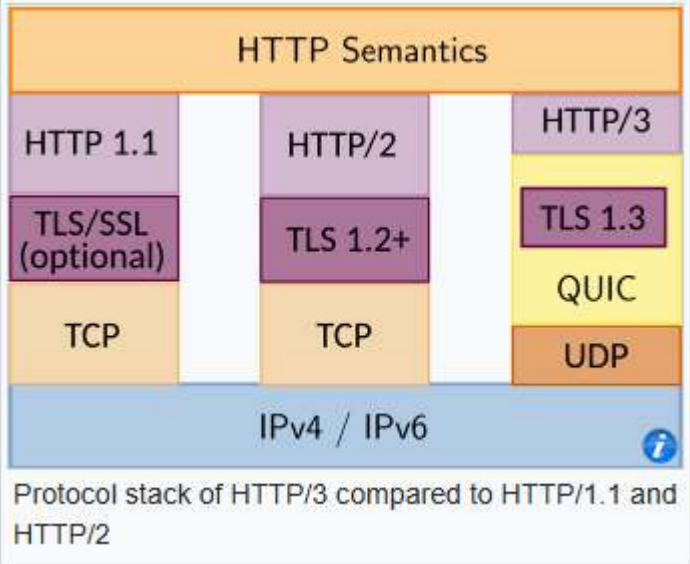
Examples of Websites Supporting HTTP/3:

Google Services (e.g., www.google.com):

Facebook (www.facebook.com):

We can find out they're using HTTP/3 by checking this website's tool **https://http3check.net/**

d. Find an image that synthesises the differences between different HTTP versions. Indicate the source of the image.



Protocol stack of HTTP/3 compared to HTTP/1.1 and HTTP/2

https://en.wikipedia.org/wiki/HTTP/3

9. Use the programmer mode from your browser (usually it appears pressing F12 key) and try to identify the headers in an HTTP request and response, the HTTP method used and also if cookies have been added to the HTTP interchange. Paste some screenshots showing the information you have found and briefly describe its content.

We can see an api request in which
The request sends form data to api.viglink.com using the POST method, likely part of a user interaction with the referring website (https://thestreamable.com).
The server responds with JavaScript content and specifies caching and cross-origin policies to control access and optimize delivery.

We can see the request headers and the cookies stored

Request Headers (Client to Server)
Host: api.viglink.com
Specifies the server that is being contacted.

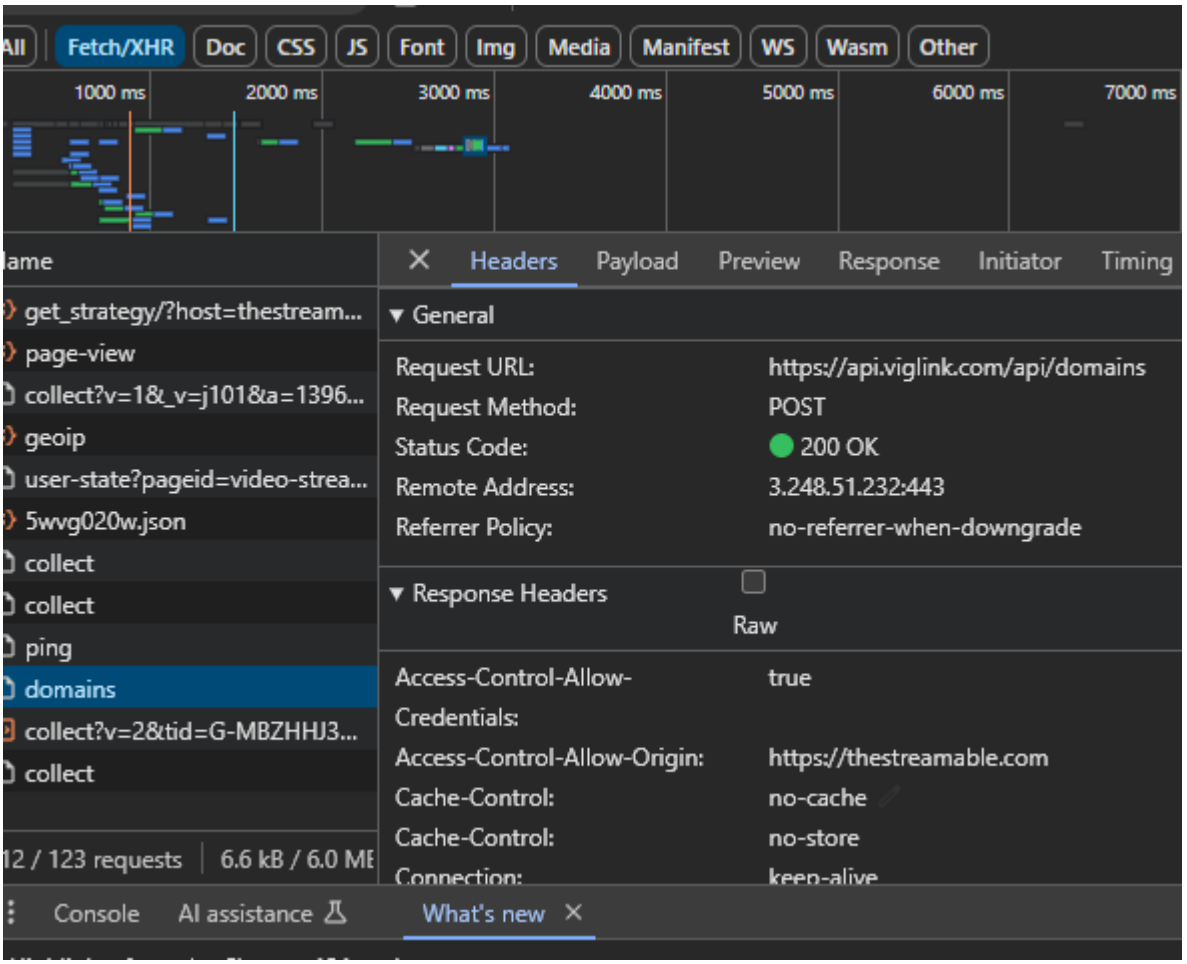
Content-Type: application/x-www-form-urlencoded
Indicates the format of the data being sent in the request body (URL-encoded key-value pairs).

Accept: */*
Specifies that the client can handle any type of response content.

Accept-Encoding: gzip, deflate, br
Indicates the compression formats the client can handle.

Referer: https://thestreamable.com/video-streaming
Shows the origin of the request, useful for tracking where the request is coming from.

User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64)...
Identifies the browser and operating system used for the request.



▼ Response Headers

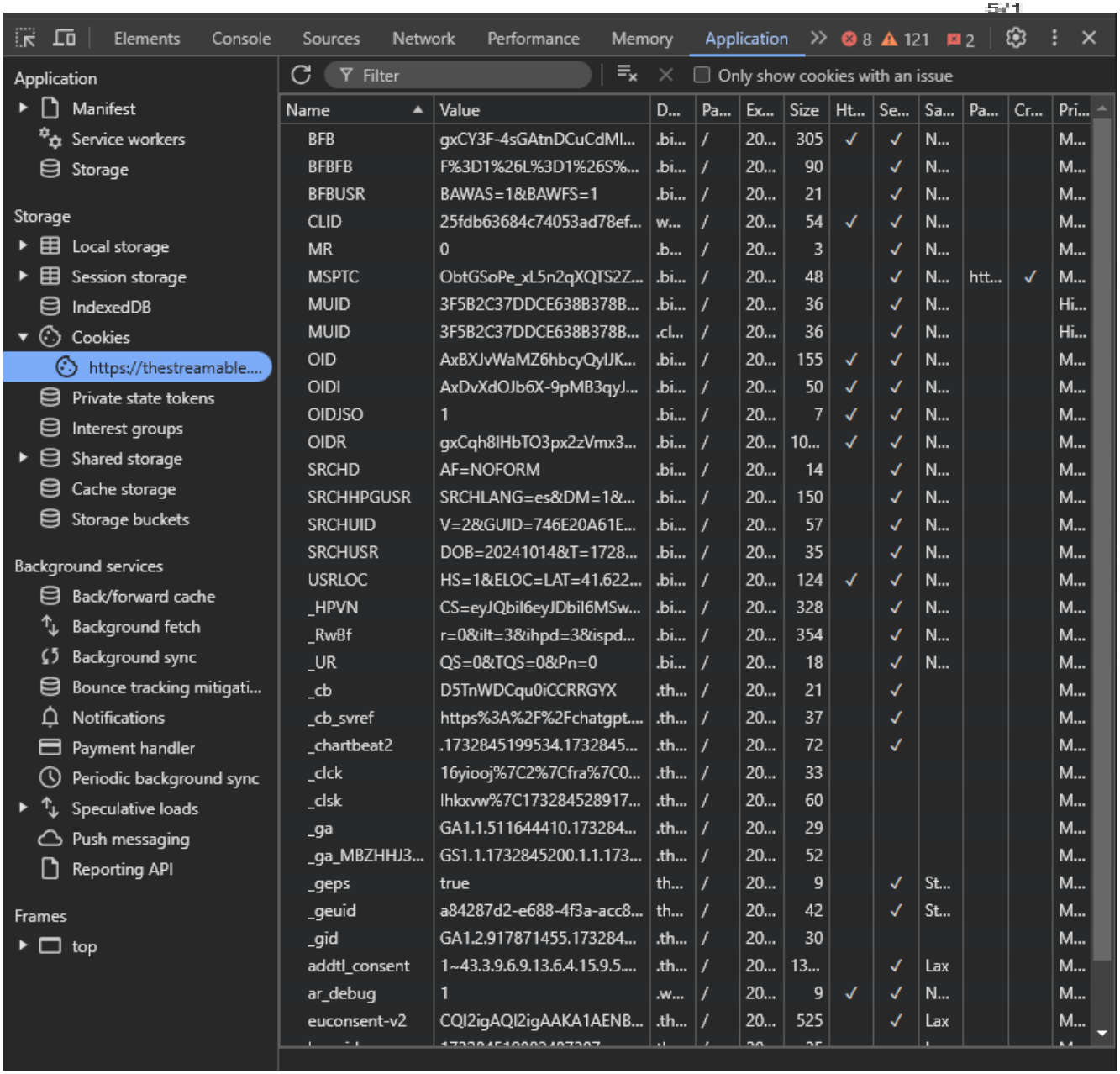
Raw

Access-Control-Allow-Credentials:	true
Access-Control-Allow-Origin:	https://thestreamable.com
Cache-Control:	no-cache
Cache-Control:	no-store
Connection:	keep-alive
Content-Length:	64
Content-Type:	text/javascript;charset=UTF-8
Date:	Fri, 29 Nov 2024 01:54:49 GMT
Expires:	Thu, 01 Jan 1970 00:00:00 GMT
P3p:	CP="ALL IND DSP COR CUR ADM TAIo PSDo OUR COM INT NAV PUR STA UNI"
Pragma:	no-cache
Server:	Apache-Coyote/1.1

▼ Request Headers

Raw

Accept:	*/*
Accept-Encoding:	gzip, deflate, br, zstd
Accept-Language:	es-ES,es;q=0.9,en;q=0.8,ca;q=0.7
Connection:	keep-alive
Content-Length:	271
Content-Type:	application/x-www-form-urlencoded
Host:	api.viglink.com
Origin:	https://thestreamable.com
Referer:	https://thestreamable.com/video-streaming
Sec-Ch-Ua:	"Google Chrome";v="131", "Chromium";v="131", "Not_A Brand";v="24"
Sec-Ch-Ua-Mobile:	?0
Sec-Ch-Ua-Platform:	"Windows"
Sec-Fetch-Dest:	empty
Sec-Fetch-Mode:	cors
Sec-Fetch-Site:	cross-site
User-Agent:	Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/131.0.0.0 Safari/537.36



10. Look for information regarding streaming protocols used by two streaming services providers, different from Netflix or Youtube. Specifically, indicate if those services make use of DASH or other proprietary streaming protocols. Reference the source of the information.

I'll use HBO and Disney+ since those are the ones I use.

Both Disney+ and HBO Max utilize adaptive streaming protocols—HLS and DASH, respectively—to provide optimal viewing experiences. They also implement Widevine DRM to safeguard their content across various platforms.

https://en.wikipedia.org/wiki/Adaptive_bitrate_streaming
https://en.wikipedia.org/wiki/Widevine
https://thestreamable.com/video-streaming/comparison