Task 4 : HTTP based.

1. What is the name of website?

- ctldl.windowsupdate.com

2. Find the packet that contains the first GET request for the website you have accessed.

- Frame 168
- 168
- 4.856837
- 10.1.37.200 213.202.3.240
- HTTP
- 299
- GET/msdownload/update/v3/static/trustedr/en/disallowedcertstl.cab?9e27 5c40f8bffea1 HTTP/1.1

3. Describe all headers and their values in this GET request message.

- **Cache-Control: no-cache**
  Forces caches to revalidate with the server, i.e. don't serve from cache.
- **Connection: Keep-Alive**
  Requests that the TCP connection stay open for multiple requests/responses.
- **Pragma: no-cache**
  Similar to Cache-Control, older HTTP/1.0 backward compatibility.
- **Accept: *\/****
  Client can accept any type of content.
- **User-Agent: Microsoft-CryptoAPI/10.0**
  Identifies the client application making the request (Windows Update in this case).

- **Host: ctldl.windowsupdate.com**
  The actual host/domain being contacted.

```
GET /msdownload/update/v3/static/trustedr/en/disallowedcertstl.cab?9e275c40f8bffea1 HTTP/1.1
Cache-Control: no-cache
Connection: Keep-Alive
Pragma: no-cache
Accept: */*
User-Agent: Microsoft-CryptoAPI/10.0
Host: ctldl.windowsupdate.com
```

4. Identify the status code in the first server response.

- Status code: 200

5. How many HTTP response messages are exchanged in total?

- 10

6. Determine whether the connection is persistent or not. Justify with evidence from packet captures.

- The connection is **non-persistent**.
  Evidence:
- Although the client requested “Connection: Keep-Alive”, the server’s response contains “Connection: close”.