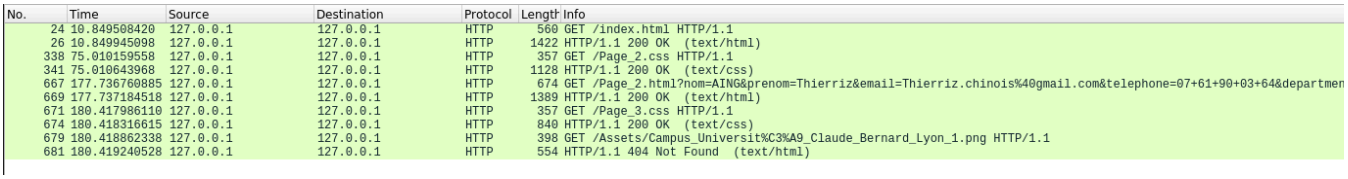
Hugo DA SILVA CARDOSO G5S2
Thierry AING

Saé 2.03 : Analyse de trames

Analyse des trames :

Pour pouvoir analyser les différentes trames nous avons circulé dans les pages du site web.

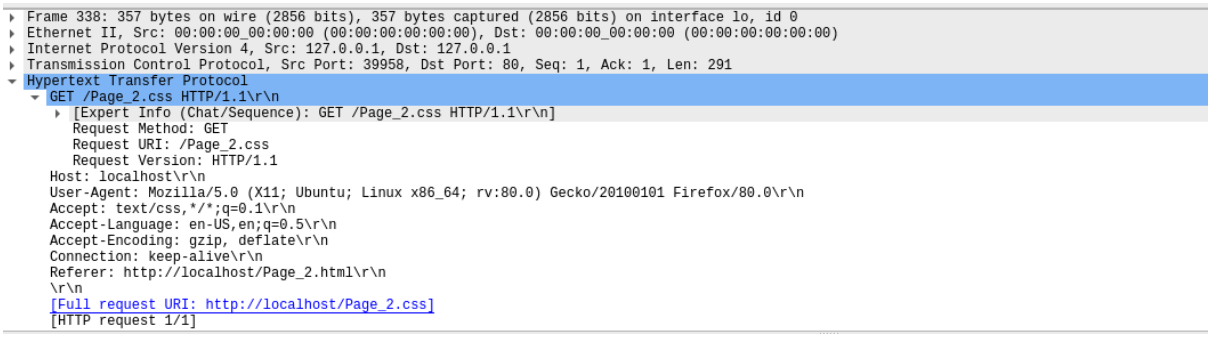
Sur Wireshark nous avons sélectionné les trames avec le Protocol HTTP afin d'avoir seulement les trames nécessaires.



No.	Time	Source	Destination	Protocol	Length	Info
24	10.849508420	127.0.0.1	127.0.0.1	HTTP	560	GET /index.html HTTP/1.1
26	10.849945098	127.0.0.1	127.0.0.1	HTTP	1422	HTTP/1.1 200 OK (text/html)
338	75.010159558	127.0.0.1	127.0.0.1	HTTP	357	GET /Page_2.css HTTP/1.1
341	75.010643968	127.0.0.1	127.0.0.1	HTTP	1128	HTTP/1.1 200 OK (text/css)
667	177.736760885	127.0.0.1	127.0.0.1	HTTP	674	GET /Page_2.html?nom=AING&prenom=Thierriz&email=Thierriz.chinois%40gmail.com&telephone=07+61+90+03+64&departmen
669	177.737184518	127.0.0.1	127.0.0.1	HTTP	1389	HTTP/1.1 200 OK (text/html)
671	180.417986110	127.0.0.1	127.0.0.1	HTTP	357	GET /Page_3.css HTTP/1.1
674	180.418316615	127.0.0.1	127.0.0.1	HTTP	840	HTTP/1.1 200 OK (text/css)
679	180.418862338	127.0.0.1	127.0.0.1	HTTP	398	GET /Assets/Campus_Universit%C3%A9_Claude_Bernard_Lyon_1.png HTTP/1.1
681	180.419240528	127.0.0.1	127.0.0.1	HTTP	554	HTTP/1.1 404 Not Found (text/html)

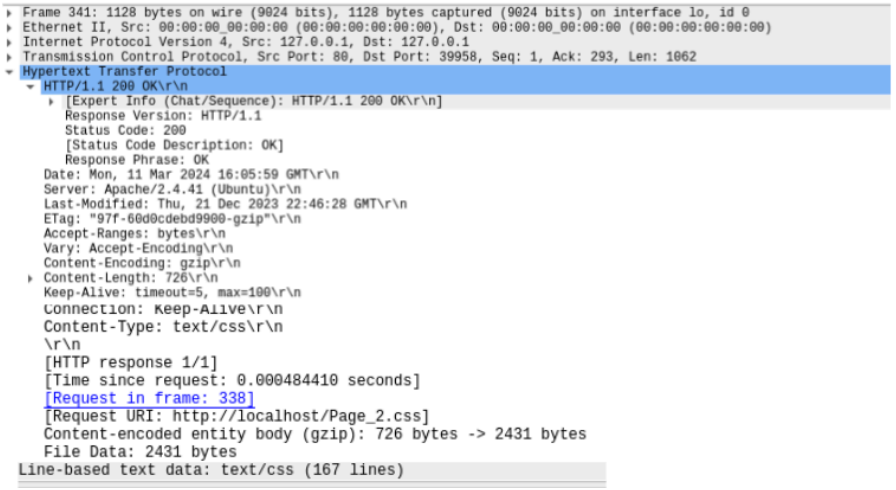
Analyse requête Apache2 port 80:

Voici ci-dessous, une requête de l'utilisateur au serveur apache. On peut voir que la requête est un GET, qui demande les informations de la page2.css et la version est en HTTP 1.1. Le client qui fait la requête est le navigateur que nous avons utilisé Mozilla. On peut voir qu'il accepte seulement du css pour cette requête et la langue de réponse est l'anglais. La requête indique que la connection entre le serveur et le client est en keep alive.



```
▸ Frame 338: 357 bytes on wire (2856 bits), 357 bytes captured (2856 bits) on interface lo, id 0
▸ Ethernet II, Src: 00:00:00_00:00:00 (00:00:00:00:00:00), Dst: 00:00:00_00:00:00 (00:00:00:00:00:00)
▸ Internet Protocol Version 4, Src: 127.0.0.1, Dst: 127.0.0.1
▸ Transmission Control Protocol, Src Port: 39958, Dst Port: 80, Seq: 1, Ack: 1, Len: 291
▾ Hypertext Transfer Protocol
  ▾ GET /Page_2.css HTTP/1.1\r\n
    ▸ [Expert Info (Chat/Sequence): GET /Page_2.css HTTP/1.1\r\n]
      Request Method: GET
      Request URI: /Page_2.css
      Request Version: HTTP/1.1
    Host: localhost\r\n
    User-Agent: Mozilla/5.0 (X11; Ubuntu; Linux x86_64; rv:80.0) Gecko/20100101 Firefox/80.0\r\n
    Accept: text/css,*/*;q=0.1\r\n
    Accept-Language: en-US,en;q=0.5\r\n
    Accept-Encoding: gzip, deflate\r\n
    Connection: keep-alive\r\n
    Referer: http://localhost/Page_2.html\r\n
    \r\n
    [Full request URI: http://localhost/Page_2.css]
    [HTTP request 1/1]
```

La réponse du serveur à cette requête est la suivante :

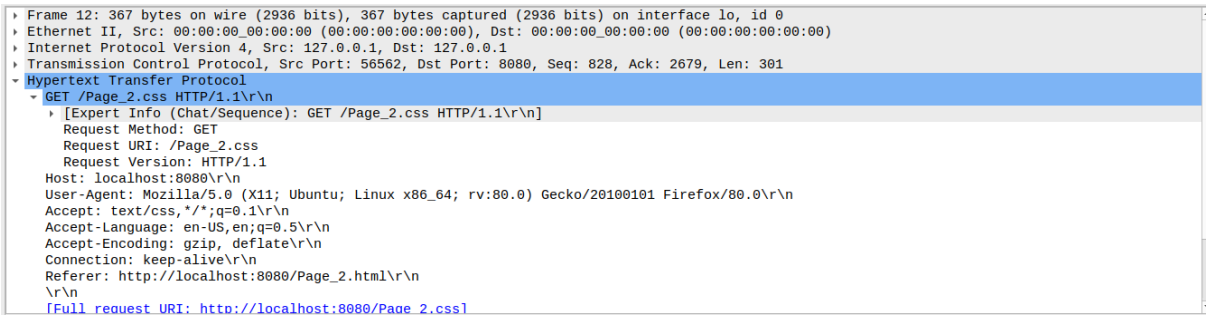


```
▸ Frame 341: 1128 bytes on wire (9024 bits), 1128 bytes captured (9024 bits) on interface lo, id 0
▸ Ethernet II, Src: 00:00:00_00:00:00 (00:00:00:00:00:00), Dst: 00:00:00_00:00:00 (00:00:00:00:00:00)
▸ Internet Protocol Version 4, Src: 127.0.0.1, Dst: 127.0.0.1
▸ Transmission Control Protocol, Src Port: 80, Dst Port: 39958, Seq: 1, Ack: 293, Len: 1062
▾ Hypertext Transfer Protocol
  ▾ HTTP/1.1 200 OK\r\n
    ▸ [Expert Info (Chat/Sequence): HTTP/1.1 200 OK\r\n]
      Response Version: HTTP/1.1
      Status Code: 200
      [Status Code Description: OK]
      Response Phrase: OK
    Date: Mon, 11 Mar 2024 16:05:59 GMT\r\n
    Server: Apache/2.4.41 (Ubuntu)\r\n
    Last-Modified: Thu, 21 Dec 2023 22:46:28 GMT\r\n
    ETag: "97f-60d0cdebd9900-gzip"\r\n
    Accept-Ranges: bytes\r\n
    Vary: Accept-Encoding\r\n
    Content-Encoding: gzip\r\n
  ▸ Content-Length: 726\r\n
    Keep-Alive: timeout=5, max=100\r\n
    Connection: Keep-Alive\r\n
    Content-Type: text/css\r\n
    \r\n
    [HTTP response 1/1]
    [Time since request: 0.000484410 seconds]
    [Request in frame: 338]
    [Request URI: http://localhost/Page_2.css]
    Content-encoded entity body (gzip): 726 bytes -> 2431 bytes
    File Data: 2431 bytes
Line-based text data: text/css (167 lines)
```

Nous allons donc analyser la réponse du serveur, tout d'abord le serveur renvoie le code 200 ce qui signifie que la requête a bien été comprise et réceptionnée. Il envoie la version HTTP qu'il va utiliser pour la réponse (HTTP 1.1), la date de la réponse, le serveur, les paramètres de keep alive, la taille du fichier le nom du fichier réquisitionné(page2.css), la dernière fois que le fichier à été modifié. Ces informations sont nécessaires pour le navigateur Mozilla afin qu'il puisse accéder au fichier du site.

Analyse requête Apache2 port 8080:

Nous avons pris pour exemple, une requête similaire à la précédente, la différence entre cette requête et la précédente est le port de destination qui est le port 8080 (le port source a changé car le jour n'est pas le même que celui d'avant).



Pour la réponse tout est similaire sauf pour le port source qui 8080.