

## Travaux Pratiques N° 1 : Protocole HTTP

### Objectif :

Analyser une requête ainsi qu'une réponse HTTP, en utilisant **Wireshark**.

### Etape 1 : téléchargement & installation de *wireshark*

Wireshark est un programme de reconnaissance, utilisé par les ingénieurs réseau pour analyser le trafic. Ce logiciel *open source* est disponible pour de nombreux systèmes d'exploitation, y compris Windows, Mac et Linux.



- Télécharger Wireshark depuis <https://www.wireshark.org/download.html>
- Procéder à l'installation de **wireshark** avec les paramètres par défaut

### Etape 2 : récupération des adresses IP source et destination

Dans ce travail, nous analyserons le trafic web échangé entre le PC local et le site du département d'informatique *cs.univ-batna2.dz*.

- Commençons par récupérer l'adresse IP de l'adaptateur réseau à utiliser lors de la capture. Pour cela, lancer l'invite de commande en exécutant la commande **cmd**. Exécuter la commande **ipconfig**, votre configuration IP apparaîtra comme suit :

```
C:\Users\elhoul>ipconfig

Wireless LAN adapter Wi-Fi:

Connection-specific DNS Suffix  . : 
Link-local IPv6 Address . . . . . : fe80::e191:74ff:f58b:323%11
IPv4 Address. . . . . : 192.168.1.99
Subnet Mask . . . . . : 255.255.255.0
Default Gateway . . . . . : 192.168.1.1
```

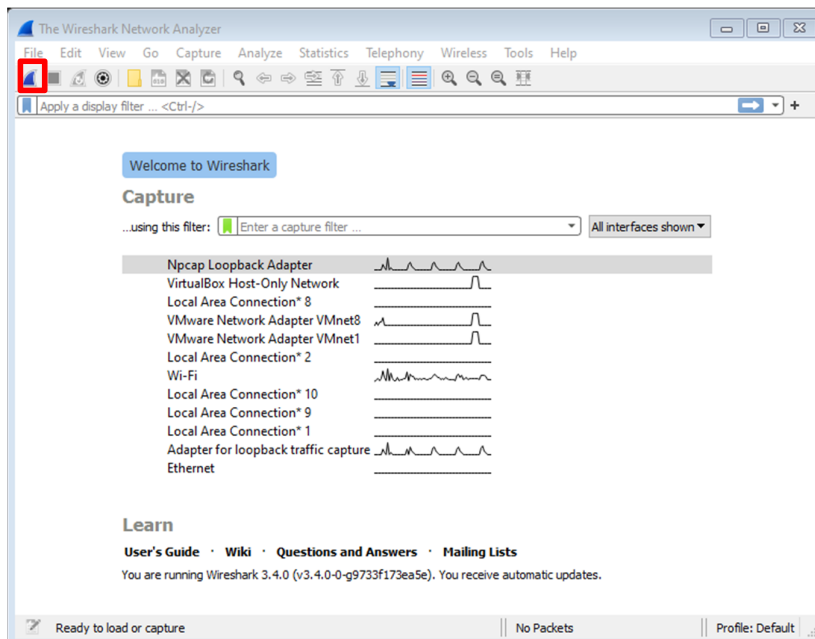
- Le moyen le plus simple pour avoir l'adresse IP du site *cs.univ-batna2.dz* est d'exécuter la commande ping. L'adresse IP correspondante s'affichera entre [ ].

```
C:\Users\elhoul>ping cs.univ-batna2.dz

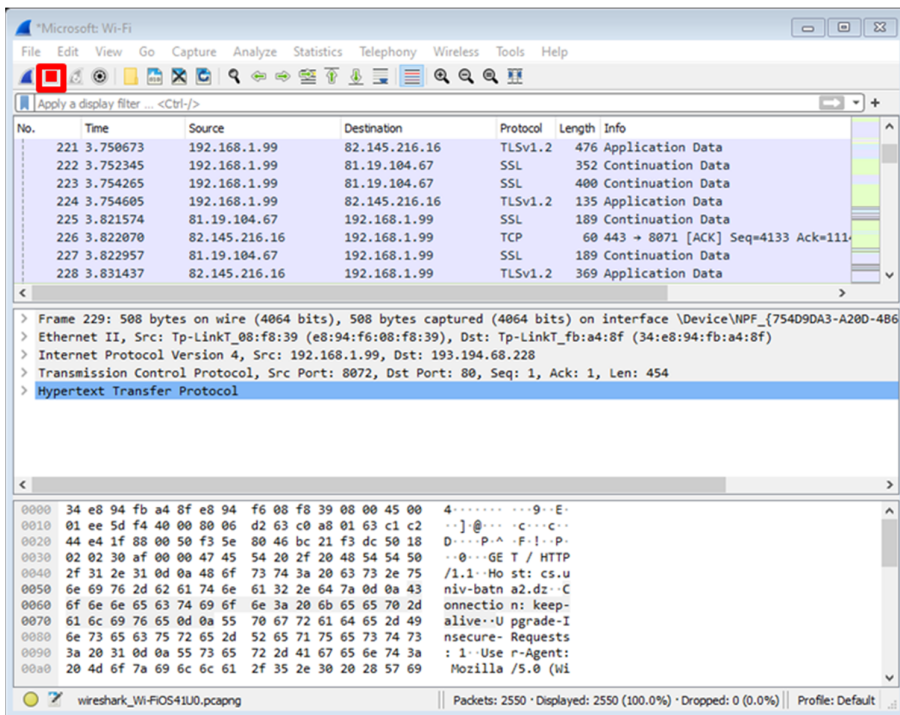
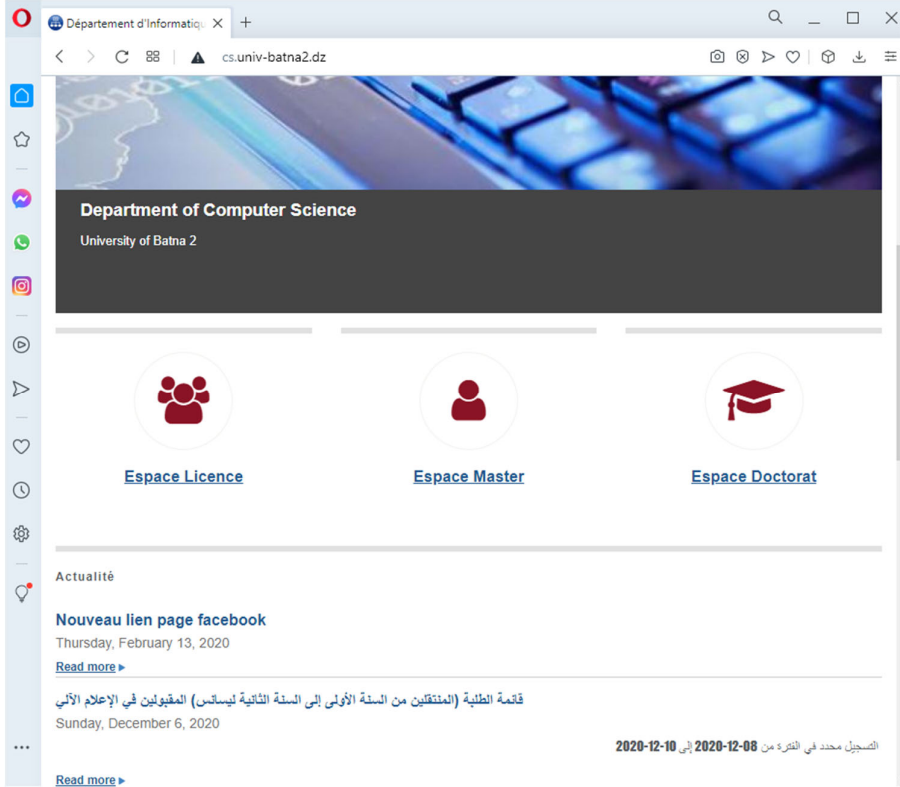
Pinging ww.univ-batna2.dz [193.194.68.228] with 32 bytes of data:
Request timed out.
```

### Etape 3 : lancer la capture *wireshark*

- Cliquer sur « démarrer la capture de paquet ». Les informations commenceront à défiler dans la section supérieure de Wireshark. Les lignes de données apparaîtront dans des couleurs différentes selon le protocole.



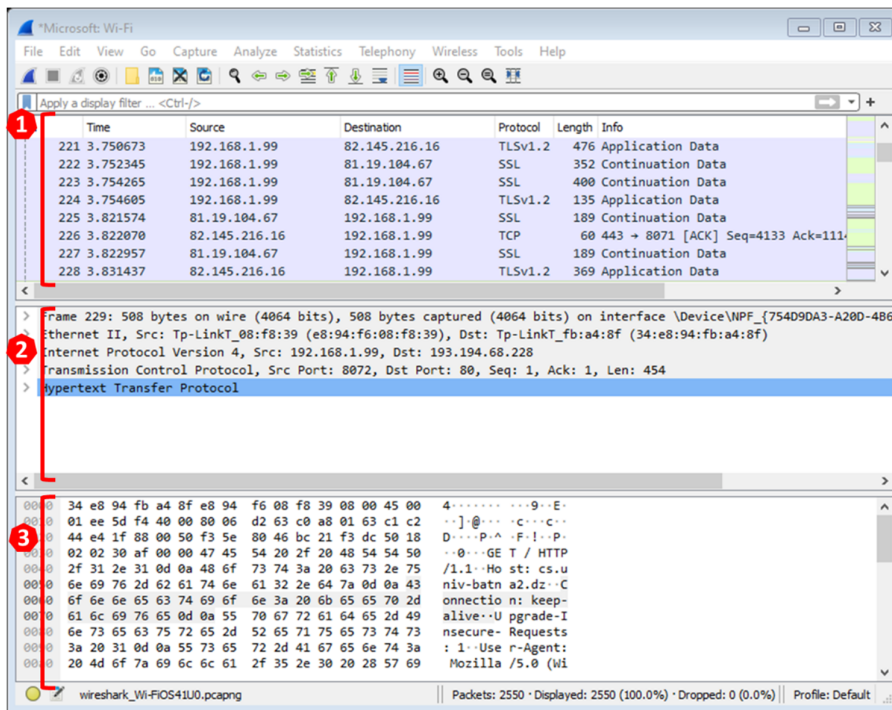
- Lancer le navigateur web, dans la barre d'adresse, saisir l'URL : *cs.univ-batna2.dz* puis appuyer sur **entrée**. Attendre jusqu'à ce que la page d'accueil du site du département se charge entièrement, puis arrêter la capture *wireshark*, en cliquant sur le bouton « arrêter la capture de paquets »



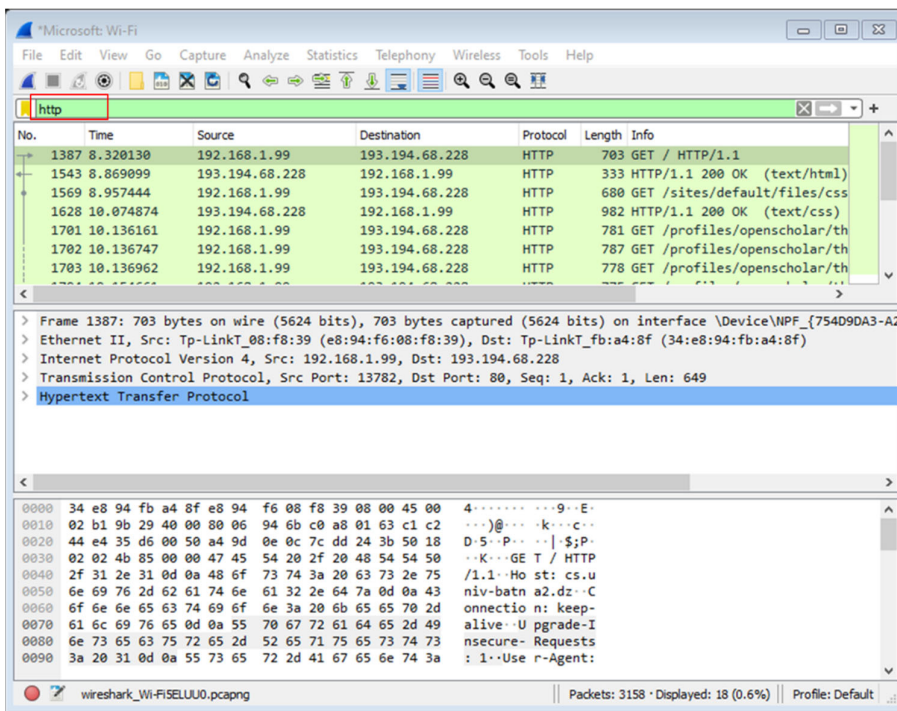
#### Etape 4 : examen des paquets capturés

Les données collectées par Wireshark sont affichées en trois sections :

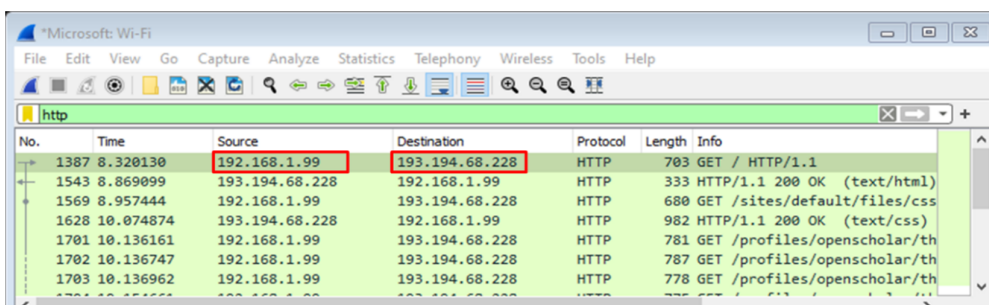
- **La section supérieure** affiche la liste des trames PDU capturées avec un résumé des informations sur les paquets IP répertoriés,
- **La section du milieu** énumère les informations PDU pour la trame sélectionnée dans la partie supérieure de l'écran et détaille une trame PDU capturée selon les couches de protocole
- **La section inférieure** affiche les données brutes de chaque couche. Les données brutes sont affichées à la fois sous forme hexadécimale et décimale.



- a. Appliquer un filtre pour n'afficher que les messages http. Taper http dans la case **Filtre** en haut de Wireshark et appuyez sur **Entrée**



- b. Cliquer sur la première trame de requête http dans la section supérieure de Wireshark. Remarquez que la colonne **Source** contient l'adresse IP de votre PC, et la colonne **Destination** contient l'adresse IP site *cs.univ-batna2.dz*.



- c. La trame étant toujours sélectionnée dans la partie supérieure, passer à la partie centrale et cliquer sur le signe « plus » (+) à gauche de la ligne **Hypertext Transfer Protocol**, pour afficher la requête http.

```

> Frame 1387: 703 bytes on wire (5624 bits), 703 bytes captured (5624 bits) on interface \Device\NPF_{754D9DA3-A208-8000-0000-000000000000}
> Ethernet II, Src: Tp-LinkT_08:f8:39 (e8:94:f6:08:f8:39), Dst: Tp-LinkT_fb:a4:8f (34:e8:94:fb:a4:8f)
> Internet Protocol Version 4, Src: 192.168.1.99, Dst: 193.194.68.228
> Transmission Control Protocol, Src Port: 13782, Dst Port: 80, Seq: 1, Ack: 1, Len: 649
+ Hypertext Transfer Protocol
  > GET / HTTP/1.1\r\n
  Host: cs.univ-batna2.dz\r\n
  Connection: keep-alive\r\n
  Upgrade-Insecure-Requests: 1\r\n
  User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/86.0.4240.0
  Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,image/apng,*/*;q=0.8,application/signed-exchange;v=b3;q=0.9\r\n
  Accept-Encoding: gzip, deflate\r\n
  Accept-Language: en-US,en;q=0.9\r\n
  > Cookie: has_js=1; __atuvc=1%7C49; __utma=154703530.1713542590.1607007658.1607007658.1607007658.1; __utmc=154703530
  \r\n
  [Full request URI: http://cs.univ-batna2.dz/]
  [HTTP request 1/2]
  [Response in frame: 1543]
  [Next request in frame: 1569]

```

d. Répondre aux questions suivantes :

- Quelle méthode http faisant l'objet de cette requête ? \_\_\_\_\_
- Quelle est la requête URI de l'objet demandé ? \_\_\_\_\_. Prévoir le nom du fichier demandé \_\_\_\_\_
- Quelle est la version du protocole http ? \_\_\_\_\_
- Quelle est la signification de « keep-alive » ? \_\_\_\_\_

- Que signifie « q=0.9 » ? \_\_\_\_\_

- Quel type de donnée le client préfère recevoir le plus dans la réponse http ? \_\_\_\_\_

e. Cliquez sur la deuxième trame dans la section supérieure de Wireshark. Cette trame représente une réponse http, la colonne **Destination** contient l'adresse IP du site cs.univ-batna2.dz. La colonne **Source** contient l'adresse IP de votre PC.

The screenshot shows the Wireshark interface with the following details:

- Packet List:**

No.	Time	Source	Destination	Protocol	Length	Info
1387	8.320130	192.168.1.99	193.194.68.228	HTTP	703	GET / HTTP/1.1
1543	8.869099	193.194.68.228	192.168.1.99	HTTP	333	HTTP/1.1 200 OK (text/html)
1569	8.957444	192.168.1.99	193.194.68.228	HTTP	680	GET /sites/default/files/css/cs...
1628	10.074874	193.194.68.228	192.168.1.99	HTTP	982	HTTP/1.1 200 OK (text/css)
1701	10.136161	192.168.1.99	193.194.68.228	HTTP	781	GET /profiles/openscholar/theme...
- Packet Details (Frame 1543):**
  - Ethernet II, Src: Tp-LinkT\_fb:a4:8f (34:e8:94:fb:a4:8f), Dst: Tp-LinkT\_08:f8:39 (e8:94:f6:08:f8:39)
  - Internet Protocol Version 4, Src: 193.194.68.228, Dst: 192.168.1.99
  - Transmission Control Protocol, Src Port: 80, Dst Port: 13782, Seq: 26601, Ack: 650, Len: 279
  - Hypertext Transfer Protocol
    - Line-based text data: text/html (281 lines)
    - Content-Type: text/html
    - HTML Content:
 

```

<!DOCTYPE html>\n
<!--[if IEMobile 7]><html class="iem7" lang="en" dir="ltr"><![endif]-->\n
<!--[if lte IE 6]><html class="lt-ie9 lt-ie8 lt-ie7" lang="en" dir="ltr"><![endif]-->\n
<!--[if (IE 7)&(!IEMobile)]><html class="lt-ie9 lt-ie8" lang="en" dir="ltr"><![endif]-->\n
<!--[if IE 8]><html class="lt-ie9" lang="en" dir="ltr"><![endif]-->\n
<!--[if (gte IE 9)](gt IEMobile 7)><!--><html lang="en" dir="ltr"><!--><![endif]-->\n
<head>\n
<meta charset="utf-8" />\n
<meta name="generator" content="OpenScholar for Drupal 7 (http://theopenscholar.org)" />\n
              
```
- Packet Bytes:**

```

0000 e8 94 f6 08 f8 39 34 e8 94 fb a4 8f 08 00 45 00 .....94.....E
0010 01 3f 44 01 40 00 33 06 3a 06 c1 c2 44 e4 c0 a8 ..?D@3:..D...
0020 01 63 00 50 35 d6 7c dd 8c 23 a4 9d 10 95 50 18 ..c-P5|.#...P-
0030 01 10 18 d1 00 00 74 74 70 3a 2f 2f 63 73 2e 75 .....tt p://cs.u
0040 6e 69 76 2d 62 61 74 6e 61 32 2e 64 7a 2f 73 69 niv-batn a2.dz/si
0050 74 65 73 2f 64 65 66 61 75 6c 74 2f 66 69 6c 65 tes/defa ult/file
0060 73 2f 6a 73 2f 6a 73 5f 64 6f 51 37 4b 4f 64 37 s/js/js_ doQ7Kod7
0070 4c 32 34 66 74 64 55 54 4e 63 55 47 34 44 58 72 L24ftdUT NcUG4DXr
0080 74 53 43 6c 41 38 54 65 57 52 47 78 62 48 7a 47 tSCLa8TE WRGxbHzG
0090 36 65 41 2e 6a 73 3f 6d 3d 31 36 30 36 30 34 35 6eA.js?m =1606045
00a0 34 35 38 22 3e 3c 2f 73 63 72 69 70 74 3e 0a 3c 458"></s cript><<

```

```

Hypertext Transfer Protocol
> HTTP/1.1 200 OK\r\n
Server: nginx/1.15.6\r\n
Date: Sun, 06 Dec 2020 17:01:03 GMT\r\n
Content-Type: text/html; charset=utf-8\r\n
Transfer-Encoding: chunked\r\n
Connection: keep-alive\r\n
X-Powered-By: PHP/5.6.40\r\n
Expires: Sun, 19 Nov 1978 05:00:00 GMT\r\n
Cache-Control: no-cache, must-revalidate\r\n
X-Content-Type-Options: nosniff\r\n
Access-Control-Allow-Origin: *\r\n
Access-Control-Allow-Credentials: true\r\n
Access-Control-Allow-Headers: Authorization, access-token\r\n
Content-Language: en\r\n
X-Frame-Options: SAMEORIGIN\r\n
x-drupal-cache-os-boxes-plugin: os_boxes_html,os_boxes_html,os_sv_list_box,os_slideshow_box,os_boxes_html,os_boxes_html,os_boxe
[truncated]x-drupal-cache-os-boxes-cache-id: os_boxes_cache:45:hwp_personal_contact_html:0,os_boxes_cache:45:1512901820:0,os_b
X-Generator: OpenScholar for Drupal 7 (http://theopenscholar.org)\r\n
Link: <http://cs.univ-batna2.dz/home>; rel="canonical",<http://cs.univ-batna2.dz/home>; rel="shortlink"\r\n
\r\n
[HTTP response 1/3]
[Time since request: 0.548969000 seconds]
[Request in frame: 1387]
[Next request in frame: 1569]
[Next response in frame: 1628]
[Request URI: http://cs.univ-batna2.dz/profiles/openscholar/themes/hwpi_basetheme/images/hwpi_basesprite.png]

```

```

Line-based text data: text/html (281 lines)
<!DOCTYPE html>\n
<!--[if IEMobile 7]><html class="iem7" lang="en" dir="ltr"><![endif]-->\n
<!--[if lte IE 6]><html class="lt-ie9 lt-ie8 lt-ie7" lang="en" dir="ltr"><![endif]-->\n
<!--[if (IE 7)&(!IEMobile)]><html class="lt-ie9 lt-ie8" lang="en" dir="ltr"><![endif]-->\n
<!--[if IE 8]><html class="lt-ie9" lang="en" dir="ltr"><![endif]-->\n
<!--[if (gte IE 9)|(gt IEMobile 7)]><!--><html lang="en" dir="ltr"><!--><![endif]-->\n
<head>\n
<meta charset="utf-8" /\n
<meta name="generator" content="OpenScholar for Drupal 7 (http://theopenscholar.org)" /\n
<link rel="canonical" href="http://cs.univ-batna2.dz/home" /\n
<link rel="shortlink" href="http://cs.univ-batna2.dz/home" /\n
<link rel="shortcut icon" href="http://cs.univ-batna2.dz/sites/default/files/web/files/network-blue-64-77371.png?m=1510674707"
<meta name="twitter:card" content="summary" /\n
<meta property="og:title" content="Département d&#39;Informatique" /\n
<meta name="description" content="Université Batna 2" /\n
<meta property="og:type" content="university" /\n
<meta property="og:image" content="http://cs.univ-batna2.dz/sites/default/files/web/files/logo-informatique_0.png?m=1511182042"
<meta name="twitter:image" content="http://cs.univ-batna2.dz/sites/default/files/web/files/logo-informatique_0.png?m=1511182042"
<title>Département d'Informatique </title>\n
<meta http-equiv="x-ua-compatible" content="IE=edge">\n
<meta name="viewport" content="width=device-width, initial-scale=1.0" /\n
<link type="text/css" rel="stylesheet" href="http://cs.univ-batna2.dz/sites/default/files/css/css_xE-rWrJf-fncB6ztZfd2huxqgxu
<link type="text/css" rel="stylesheet" href="http://cs.univ-batna2.dz/sites/default/files/css/css_raUrXnSCPh_IEA-481GCsCEM8LQ3t

```

f. Répondre aux questions suivantes :

- Que signifie la valeur 200 ? \_\_\_\_\_
- Quel serveur est responsable de fournir la réponse http ? \_\_\_\_\_
- Comment le corps de la réponse http est-il séparé de son en-tête ? \_\_\_\_\_
- Quel est le type des données renvoyées par le serveur dans le corps de la réponse http ? \_\_\_\_\_
- Combien de lignes de code comporte le document retourné ? \_\_\_\_\_