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.

a. Télécharger Wireshark depuis https://www.wireshark.org/download.html
b. 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* .

a. 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 apparaitra comme suit :

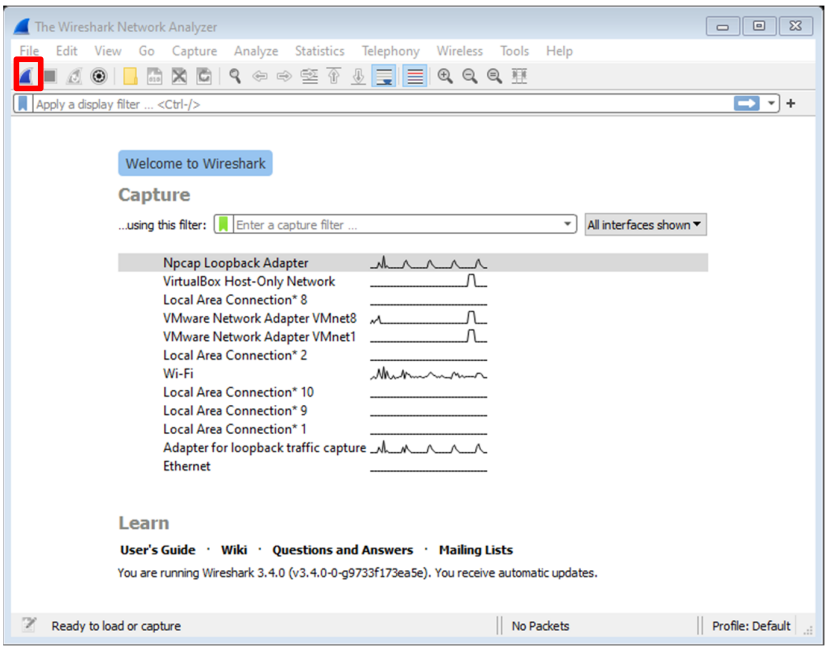
```
C:\Users\elhou>ipconfig
Wireless LAN adapter Wi-Fi:

   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
```

b. 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 [ ].

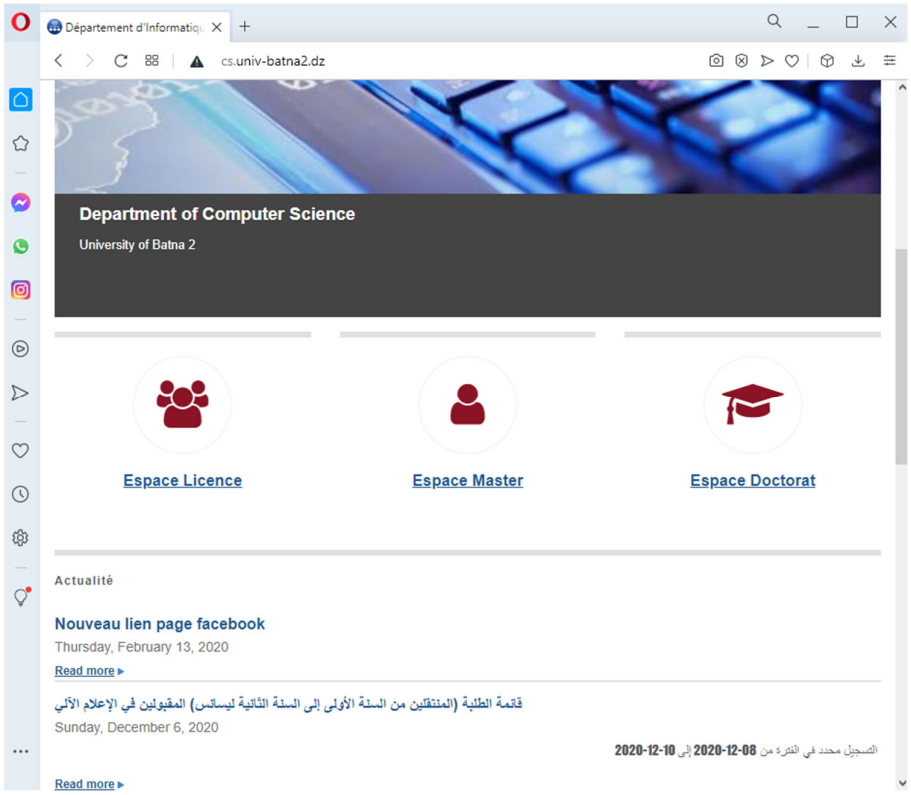
```
C:\Users\elhou>ping cs.univ-batna2.dz

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

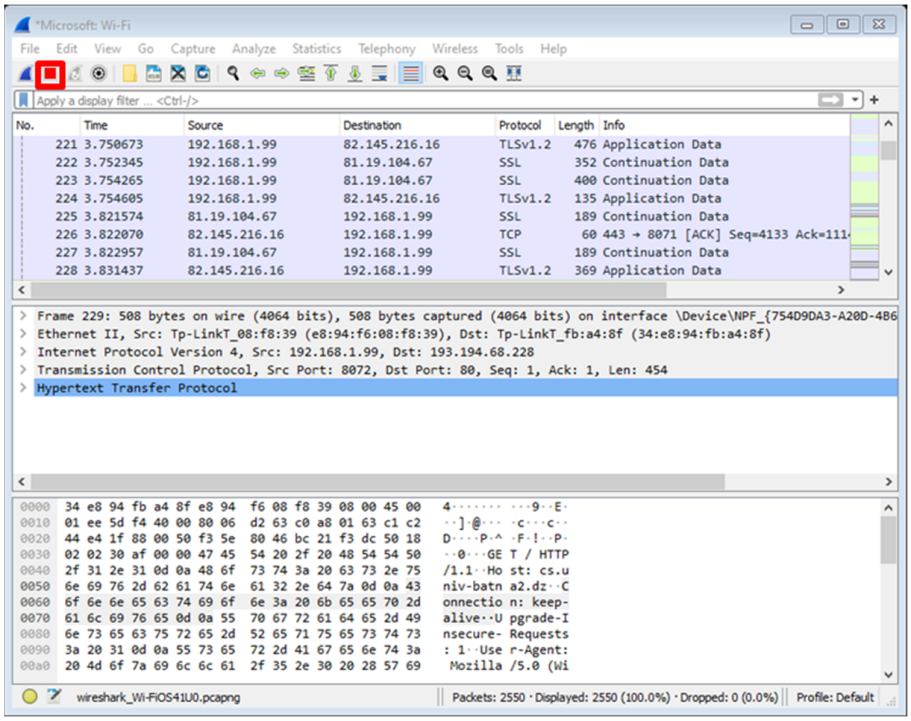
Etape 3 : lancer la capture *wireshark*

a. 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.



b. 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 »

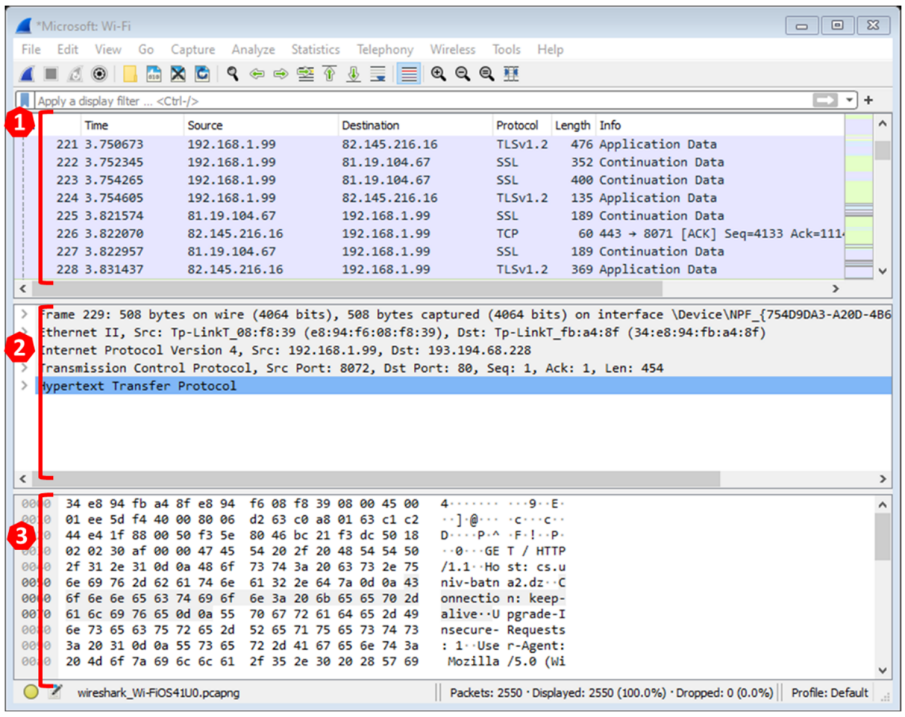




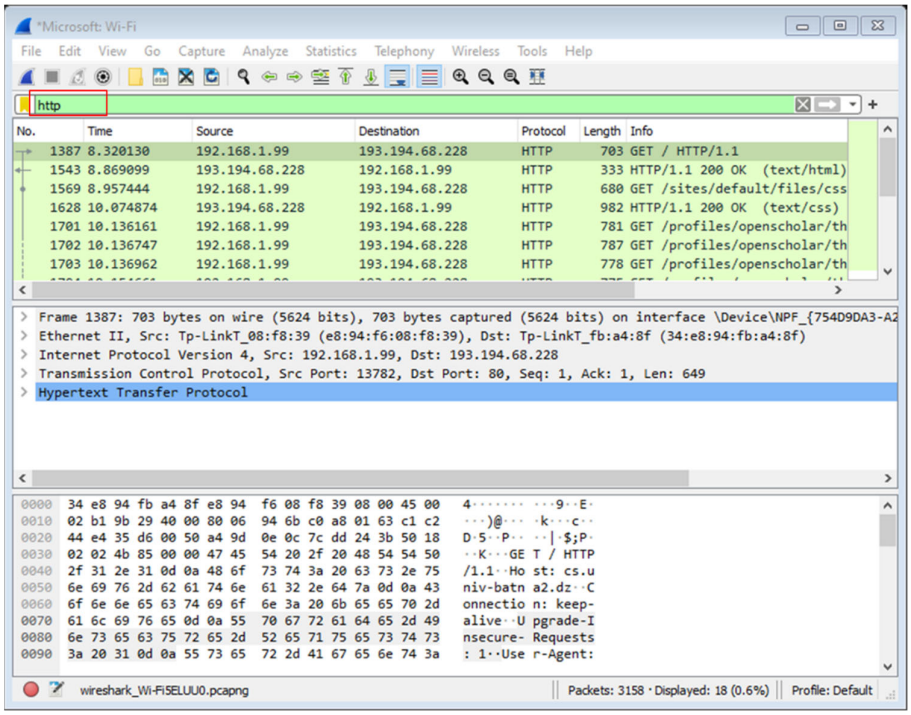
Etape 4 : examen des paquets capturés

Les données collectées par Wireshark sont affichées en trois sections :

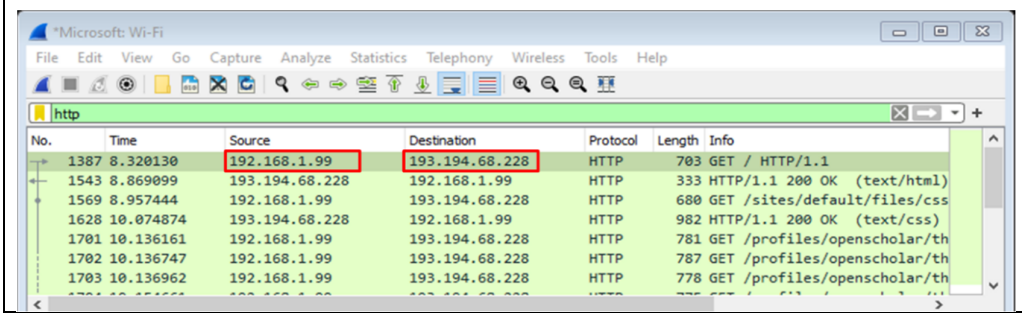
- **La section supérieure** affiche la liste des trames PDU capturées avec un résumé des informations sur les paquets IP répertoriés,
- **La section du milieu** énumère les informations PDU pour la trame sélectionnée dans la partie supérieure de l'écran et détaille une trame PDU capturée selon les couches 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-A20
> 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
v 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.
    Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,image/apng,*/*;q=0.8,appli
    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=1547
    \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 » ?

_____ _____ _____ _____ _____ _____ _____ _____ _____ _____ _____ _____ _____ _____

_____ _____ _____ _____ _____ _____ _____ _____ _____ _____ _____ _____ _____ _____

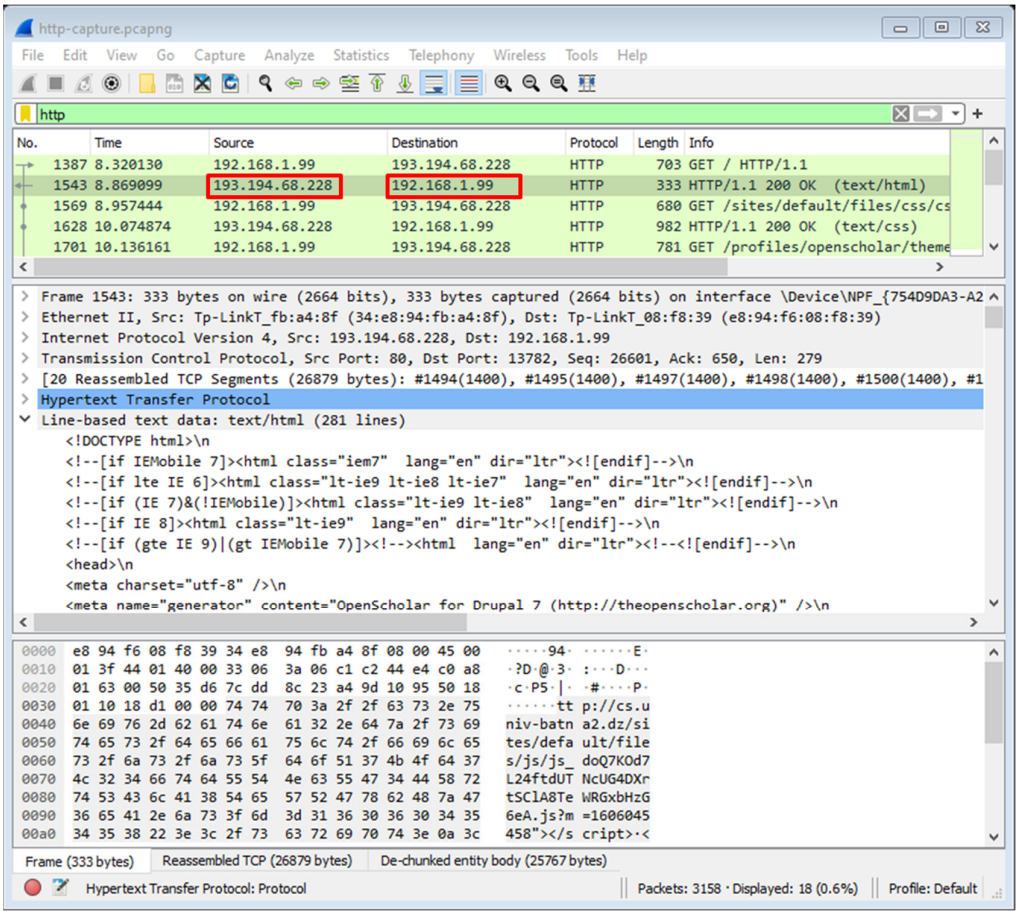
- Que signifie « q=0.9 » ?

_____ _____ _____ _____ _____ _____ _____ _____ _____ _____ _____ _____ _____ _____

- 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.



```
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&#039;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-481GCsCEM8LQ3b
```

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 ? _____