

Travaux Pratiques TP N°3 :

Examiner le trafic UDP, DNS et HTTP

YOUSSEF HACHIMI

ARI

GROUP 2

N : 31

2024/2025 EST BM

PARTIE I : Analyser le trafic UDP et DNS

Exercice 1 : Analyser le trafic UDP et DNS

1. Sur Wireshark, appliquer un filtre de capture pour capturer seulement le trafic UDP.

- **Filtre : udp**

Cela capture uniquement les paquets utilisant le protocole UDP.

Capturing from Wi-Fi

File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help

udp

No.	udp	Source	Destination	Protocol	Length	Info
2	udpencap	790	fe80::6c8f:31f7:1ea...	MDNS	101	Standard query 0x0000 A BRWCC6B1E8EE0C9.local, "QM" question
2	udplite	282	100.88.217.159	NBNS	92	Name query NB BRWCC6B1E8EE0C9<00>
2	udplite	282	fe80::283c:1741:b54...	MDNS	101	Standard query 0x0000 ANY DESKTOP-3AG1QIS.local, "QM" question
2425		126.832282	fe80::283c:1741:b54...	LLMNR	95	Standard query 0x9da8 ANY DESKTOP-3AG1QIS
2426		126.832282	fe80::283c:1741:b54...	MDNS	139	Standard query response 0x0000 AAAA fe80::283c:1741:b54f:c4f2 A 100.88.219.54
2427		126.832282	100.88.219.54	MDNS	81	Standard query 0x0000 ANY DESKTOP-3AG1QIS.local, "QM" question
2428		126.832282	100.88.219.54	LLMNR	75	Standard query 0x9da8 ANY DESKTOP-3AG1QIS
2429		126.933019	100.88.217.72	MDNS	154	Standard query 0x0000 PTR _companion-link._tcp.local, "QM" question PTR _rdlink._tcp.local, "QM" question PTR _sleep-proxy
2430		126.933019	fe80::1c0e:d1ce:ada...	MDNS	174	Standard query 0x0000 PTR _companion-link._tcp.local, "QM" question PTR _rdlink._tcp.local, "QM" question PTR _sleep-proxy
2431		127.036545	100.88.219.175	MDNS	568	Standard query response 0x0000 TXT, cache flush PTR _mi-connect._udp.local PTR {"nm":"Redmi Note 10","as":["8194"],"ip":"0
2432		127.036545	fe80::384e:9fff:fef...	MDNS	588	Standard query response 0x0000 TXT, cache flush PTR _mi-connect._udp.local PTR {"nm":"Redmi Note 10","as":["8194"],"ip":"0
2434		127.446624	100.88.217.159	NBNS	92	Name query NB BRWCC6B1E8EE0C9<00>
2435		127.446624	100.88.217.159	MDNS	81	Standard query 0x0000 A BRWCC6B1E8EE0C9.local, "QM" question
2436		127.446624	fe80::6c8f:31f7:1ea...	MDNS	101	Standard query 0x0000 A BRWCC6B1E8EE0C9.local, "QM" question
2437		127.446624	fe80::6c8f:31f7:1ea...	LLMNR	95	Standard query 0x9bde A BRWCC6B1E8EE0C9
2438		127.446624	100.88.217.159	LLMNR	75	Standard query 0x9bde A BRWCC6B1E8EE0C9
2439		128.059431	fe80::6c8f:31f7:1ea...	LLMNR	95	Standard query 0x9bde A BRWCC6B1E8EE0C9
2440		128.059431	100.88.217.159	LLMNR	75	Standard query 0x9bde A BRWCC6B1E8EE0C9
2441		128.059431	100.88.219.60	MDNS	119	Standard query 0x0000 PTR _674A0243._sub._googlecast._tcp.local, "QM" question PTR _8E6C866D._sub._googlecast._tcp.local,
2442		128.469033	100.88.217.159	NBNS	92	Name query NB BRWCC6B1E8EE0C9<00>
2443		128.469033	100.88.217.159	MDNS	81	Standard query 0x0000 A BRWCC6B1E8EE0C9.local, "QM" question
2444		128.469033	fe80::6c8f:31f7:1ea...	MDNS	101	Standard query 0x0000 A BRWCC6B1E8EE0C9.local, "QM" question

Frame 4: 92 bytes on wire (736 bits), 92 bytes captured (736 bits) on interface \Device\NPF_{921A64D1-...} 0000 ff ff ff ff ff 90 cc df 97 52 20 08 00 45 00 R E

Ethernet II, Src: Intel 97:52:20 (90:cc:df:97:52:20), Dst: Broadcast (ff:ff:ff:ff:ff:ff) 0010 00 4e d1 da 00 00 80 11 e6 74 64 58 d9 9f 64 58 N tdx dx

Internet Protocol Version 4, Src: 100.88.217.159, Dst: 100.88.223.255 0020 df ff 00 89 00 89 00 3a 4a 9c be fc 01 10 00 01 J

User Datagram Protocol, Src Port: 137, Dst Port: 137 0030 00 00 00 00 00 00 20 45 43 46 43 46 48 45 44 45 E CFCFHEDE

NetBIOS Name Service 0040 44 44 47 45 43 44 42 45 46 44 49 45 46 45 46 44 DDGECDBE FDIEFEFD

0050 41 45 44 44 4a 41 41 00 00 20 00 01 AEDDJAA

2. Citer les applications présentes au niveau du filtre, celles qui utilisent le protocole UDP.

- Parmi les applications qui utilisent UDP, vous trouverez :
 - DNS
 - DHCP
 - SNMP
 - VoIP

3. Filtrer seulement le trafic DNS.

- **Filtre :** udp.port == 53
Ce filtre capture uniquement le trafic DNS, qui utilise le port UDP 53.

dns	Source	Destination	Protocol	Length	Info
17 7.673567	100.88.219.154	100.127.255.72	DNS	85	Standard query 0xaa67 A authentication.ducunt.com
18 7.698116	100.88.219.154	100.127.255.72	DNS	85	Standard query 0xfeaf HTTPS authentication.ducunt.com
19 7.698345	100.88.219.154	100.127.255.72	DNS	88	Standard query 0x5c0b A analytics-toolbar.ducunt.com
22 8.059562	100.88.219.154	100.127.255.72	DNS	88	Standard query 0xef61 HTTPS analytics-toolbar.ducunt.com
23 8.059816	100.88.219.154	100.127.255.72	DNS	72	Standard query 0xf2bf A cdn.honey.io
25 8.525419	100.88.219.154	100.127.255.73	DNS	72	Standard query 0xfc52 HTTPS cdn.honey.io
26 8.525702	100.88.219.154	100.127.255.73	DNS	85	Standard query 0x9ec3 A authentication.ducunt.com
27 8.556606	100.88.219.154	100.127.255.73	DNS	85	Standard query 0xdd52 HTTPS authentication.ducunt.com
28 8.556880	100.88.219.154	100.127.255.73	DNS	88	Standard query 0xa4ba A analytics-toolbar.ducunt.com
30 8.918041	100.88.219.154	100.127.255.73	DNS	88	Standard query 0xb38d HTTPS analytics-toolbar.ducunt.com
31 8.918570	100.88.219.154	100.127.255.73	DNS	72	Standard query 0x9b10 A cdn.honey.io
32 9.544406	100.88.219.154	100.127.255.73	DNS	72	Standard query 0x1168 HTTPS cdn.honey.io
33 9.544716	100.88.219.154	100.127.255.72	DNS	85	Standard query 0x5ab0 A authentication.ducunt.com
34 9.575641	100.88.219.154	100.127.255.72	DNS	85	Standard query 0xb074 HTTPS authentication.ducunt.com
35 9.575945	100.88.219.154	100.127.255.72	DNS	88	Standard query 0x0278 A analytics-toolbar.ducunt.com
36 9.932966	100.88.219.154	100.127.255.72	DNS	88	Standard query 0x45d5 HTTPS analytics-toolbar.ducunt.com
37 9.933238	100.88.219.154	100.127.255.72	DNS	72	Standard query 0xb08b A cdn.honey.io
39 11.259182	100.88.219.154	100.127.255.73	DNS	72	Standard query 0xfab5 HTTPS cdn.honey.io
40 11.274777	100.88.219.154	100.127.255.73	DNS	85	Standard query 0xd4c9 HTTPS authentication.ducunt.com
41 11.275042	100.88.219.154	100.127.255.73	DNS	88	Standard query 0xc3cc A analytics-toolbar.ducunt.com
42 11.571750	100.88.219.154	100.127.255.72	DNS	88	Standard query 0x2cc8 HTTPS analytics-toolbar.ducunt.com
			DNS	85	Standard query 0x053c A authentication.ducunt.com

Frame 16: 85 bytes on wire (680 bits), 85 bytes captured (680 bits) on interface \Device\NPF_{921A64D1-0000-e8-ed-d6-07-b3-a4-e8-2a-ea-89-70-15-08-00-45-00} Ethernet II, Src: Intel 89:70:15 (e8:2a:ea:89:70:15), Dst: Fortinet 07:b3:a4 (e8:ed:d6:07:b3:a4)	0000 e8 ed d6 07 b3 a4 e8 2a ea 89 70 15 08 00 45 00*..p...E
Internet Protocol Version 4, Src: 100.88.219.154, Dst: 100.127.255.72	0010 00 47 82 3f 00 00 80 11 14 ac 64 58 db 9a 64 7f	.G?...dX..d.
User Datagram Protocol, Src Port: 57263, Dst Port: 53	0020 ff 48 df af 00 35 00 33 28 53 aa 67 01 00 00 01	H...5:3(Sg....
Domain Name System (query)	0030 00 00 00 00 00 00 0e 61 75 74 68 65 6e 74 69 63a uthentic
	0040 61 74 69 6f 6e 06 64 75 63 75 6e 74 03 63 6f 6d	ation du cunt.com
	0050 00 00 01 00 01

4. Sélectionner une requête DNS et examiner le segment UDP (les différents champs).

Dans le segment UDP

- **Source Port** : Port de l'application qui a initié la requête.
- **Destination Port** : Généralement 53 pour DNS.
- **Length** : Longueur totale du segment UDP.
- **Checksum** : Utilisé pour la vérification des erreurs.

5. Avancer sur la ligne suivante et examiner la requête DNS.

- **a) Examinez les différents champs DNS**
 - **Transaction ID** : Identifiant unique de la requête/réponse.
 - **Flags** : Indique si la requête est récursive, autoritaire, etc.
 - **Questions** : Noms de domaine demandés.

- **Answers** : Réponses fournies par le serveur DNS.
- **b)** Le type d'information demandée est spécifié dans le champ **Query Type** (ex. A, AAAA, MX, NS).
- **c)** Examinez la réponse DNS. Vous verrez les **Resource Records (RR)** contenant des informations comme l'adresse IP, le type de record (A, MX, etc.), et leur TTL.

6. Appliquer un filtre pour afficher les requêtes DNS envoyées pour résoudre le nom de domaine du site demandé.

- **Filtre** : `dns.qry.name == "www.amazon.com"`
Ce filtre affiche uniquement les requêtes DNS pour un domaine spécifique.

Wireshark capture showing DNS queries and responses for `www.amazon.com`. The filter applied is `dns.qry.name contains "www.amazon.com"`.

No.	Time	Source	Destination	Protocol	Length	Info
11348	445.329344	100.88.219.154	100.127.255.72	DNS	74	Standard query 0x6af5 A www.amazon.com
11349	445.329747	100.88.219.154	100.127.255.72	DNS	74	Standard query 0xd241 HTTPS www.amazon.com
11350	445.343598	100.127.255.72	100.88.219.154	DNS	179	Standard query response 0x6af5 A www.amazon.com CNAME tp.47cf2c8c9-frontier.amazon.com CNAME d3ag4hukkh62yn.cloudfront.net A 54.192.104.198
11351	445.343598	100.127.255.72	100.88.219.154	DNS	237	Standard query response 0xd241 HTTPS www.amazon.com CNAME tp.47cf2c8c9-frontier.amazon.com CNAME d3ag4hukkh62yn.cloudfront.net SOA ns-130.awsdn

Frame 11348: 74 bytes on wire (592 bits), 74 bytes captured (592 bits) on interface \Device\NPF_{921A6...}

Ethernet II, Src: Intel_89:70:15 (e8:2a:ea:89:70:15), Dst: Fortinet_07:b3:a4 (e8:ed:d6:07:b3:a4)

Internet Protocol Version 4, Src: 100.88.219.154, Dst: 100.127.255.72

User Datagram Protocol, Src Port: 61627, Dst Port: 53

Domain Name System (query)

0000 e8 ed d6 07 b3 a4 e8 2a ea 89 70 15 00 00 45 00*..p...E
 0010 00 3c 82 bc 00 00 80 11 14 3a 64 58 db 9a 64 7f -<.....:dX...d
 0020 ff 48 f0 bb 00 35 00 28 57 66 6a f5 01 00 00 01 H...5(Wfj.....
 0030 00 00 00 00 00 03 77 77 77 06 61 6d 61 7a 6fw ww amazo
 0040 6e 03 63 6f 6d 00 00 01 00 01 n com... ..

7. Examiner les requêtes DNS envoyées.

- Vérifiez les champs comme **Query Name** et **Query Type**

8. Examiner aussi les réponses DNS correspondantes.

- Vérifiez les champs **Answer Name**, **Answer Type**, et **Answer Address** pour les réponses DNS.

```
Queries
Answers
  www.amazon.com: type CNAME, class IN, cname tp.47cf2c8c9-frontier.amazon.com
  tp.47cf2c8c9-frontier.amazon.com: type CNAME, class IN, cname d3ag4hukkh62yn.cloudfront.net
  d3ag4hukkh62yn.cloudfront.net: type A, class IN, addr 54.192.104.198
[Request In: 11348]
[Time: 0.014254000 seconds]
```

Exercice 2 : Analyse des requêtes DNS

9. Sur Wireshark, appliquer un filtre de capture du trafic DNS.

- **Filtre : dns**

No.	dns dnsserver	Source	Destination	Protocol	Length	Info
17	100.88.219.154	100.88.219.154	100.127.255.72	DNS	85	Standard query 0xaa67 A authentication.ducunt.com
18	100.88.219.154	100.88.219.154	100.127.255.72	DNS	85	Standard query 0xfeaf HTTPS authentication.ducunt.com
19	100.88.219.154	100.88.219.154	100.127.255.72	DNS	88	Standard query 0x5c0b A analytics-toolbar.ducunt.com
22	100.88.219.154	100.88.219.154	100.127.255.72	DNS	88	Standard query 0xef61 HTTPS analytics-toolbar.ducunt.com
23	100.88.219.154	100.88.219.154	100.127.255.72	DNS	72	Standard query 0xf2bf A cdn.honey.io
25	100.88.219.154	100.88.219.154	100.127.255.72	DNS	72	Standard query 0xfc52 HTTPS cdn.honey.io
26	100.88.219.154	100.88.219.154	100.127.255.72	DNS	85	Standard query 0x9ec3 A authentication.ducunt.com
27	100.88.219.154	100.88.219.154	100.127.255.72	DNS	85	Standard query 0xdd52 HTTPS authentication.ducunt.com
28	100.88.219.154	100.88.219.154	100.127.255.72	DNS	88	Standard query 0xa4ba A analytics-toolbar.ducunt.com
30	100.88.219.154	100.88.219.154	100.127.255.72	DNS	88	Standard query 0xb38d HTTPS analytics-toolbar.ducunt.com
31	100.88.219.154	100.88.219.154	100.127.255.72	DNS	72	Standard query 0x9b10 A cdn.honey.io
32	100.88.219.154	100.88.219.154	100.127.255.72	DNS	72	Standard query 0x1168 HTTPS cdn.honey.io
33	100.88.219.154	100.88.219.154	100.127.255.72	DNS	85	Standard query 0x5ab0 A authentication.ducunt.com
34	100.88.219.154	100.88.219.154	100.127.255.72	DNS	85	Standard query 0xb074 HTTPS authentication.ducunt.com
35	100.88.219.154	100.88.219.154	100.127.255.72	DNS	88	Standard query 0x0278 A analytics-toolbar.ducunt.com
36	100.88.219.154	100.88.219.154	100.127.255.72	DNS	88	Standard query 0x45d5 HTTPS analytics-toolbar.ducunt.com
37	100.88.219.154	100.88.219.154	100.127.255.72	DNS	72	Standard query 0xb08b A cdn.honey.io
39	100.88.219.154	100.88.219.154	100.127.255.72	DNS	72	Standard query 0xfab5 HTTPS cdn.honey.io
40	100.88.219.154	100.88.219.154	100.127.255.72	DNS	85	Standard query 0xd4c9 HTTPS authentication.ducunt.com
41	100.88.219.154	100.88.219.154	100.127.255.72	DNS	88	Standard query 0xc3cc A analytics-toolbar.ducunt.com
42	100.88.219.154	100.88.219.154	100.127.255.72	DNS	88	Standard query 0x2cc8 HTTPS analytics-toolbar.ducunt.com
43	100.88.219.154	100.88.219.154	100.127.255.72	DNS	85	Standard query 0x053c A authentication.ducunt.com

Frame 16: 85 bytes on wire (680 bits), 85 bytes captured (680 bits) on interface \Device\NPF{921A64D1-0000-0000-0000-000000000000} on 00000000000000000000000000000000
Ethernet II, Src: Intel_B9:70:15 (e8:2a:ea:89:70:15), Dst: Fortinet_07:b3:a4 (e8:ed:d6:07:b3:a4) 0010 00 47 82 3f 00 00 80 11 14 ac 64 58 db 9a 64 7f G ? dx d
Internet Protocol Version 4, Src: 100.88.219.154, Dst: 100.127.255.72 0020 ff 48 df af 00 35 00 33 28 53 aa 67 01 00 00 01 H...5 3 (S g...
User Datagram Protocol, Src Port: 57263, Dst Port: 53 0030 00 00 00 00 00 0e 61 75 74 68 65 6e 74 69 63a uthentic
Domain Name System (query) 0040 61 74 69 6f 6e 06 64 75 63 75 6e 74 03 63 6f 6d ation du cunt.com
0050 00 00 01 00 01

10. Appliquer la commande pour chercher les serveurs DNS d'un domaine dans le terminal :

- **Commande :** nslookup ebay.com

Cela affichera les adresses IP des serveurs DNS qui répondent pour ce domaine.

```
Command Prompt
Microsoft Windows [Version 10.0.22000.2538]
(c) Microsoft Corporation. All rights reserved.

C:\Users\Youssef Hachimi>ping www.ebay.com

Pinging e9428.a.akamaiedge.net [2.23.189.84] with 32 bytes of data:
Reply from 2.23.189.84: bytes=32 time=44ms TTL=56
Reply from 2.23.189.84: bytes=32 time=2397ms TTL=56
Reply from 2.23.189.84: bytes=32 time=443ms TTL=56
Reply from 2.23.189.84: bytes=32 time=63ms TTL=56

Ping statistics for 2.23.189.84:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
    Approximate round trip times in milli-seconds:
        Minimum = 44ms, Maximum = 2397ms, Average = 736ms

C:\Users\Youssef Hachimi>nslookup ebay.com
Server:  UnKnown
Address:  100.127.255.72

Non-authoritative answer:
Name:     ebay.com
Addresses: 2.21.67.51
           2.21.67.41
```

11. Appliquer la commande pour chercher les serveurs de messagerie (enregistrement MX) :

- **Commande :** nslookup -query=mx ebay.com

Cela liste les serveurs MX (Mail Exchange) du domaine.

12. Appliquer la commande pour chercher les serveurs de noms (enregistrement NS) :

- **Commande :** `nslookup -query=ns ebay.com`

Cela liste les serveurs de noms (Name Servers) du domaine.

```
C:\Users\Youssef Hachimi>nslookup -type=MX ebay.com
Server:  UnKnown
Address:  100.127.255.72

Non-authoritative answer:
ebay.com      MX preference = 10, mail exchanger = mx1.hc2186-24.iphmx.com
ebay.com      MX preference = 10, mail exchanger = mx2.hc2186-24.iphmx.com
C:\Users\Youssef Hachimi>
```

13. Sur Wireshark, appliquer les filtres nécessaires pour afficher les requêtes DNS des questions 10, 11 et 12 :

- Pour afficher les requêtes DNS :
 - **Filtre pour A :** `dns.qry.type == 1`
 - **Filtre pour MX :** `dns.qry.type == 15`
 - **Filtre pour NS :** `dns.qry.type == 2`Examinez ensuite les réponses pour chaque type d'enregistrement.

PARTIE II : Examiner le trafic HTTP

Exercice 1 : Examiner le trafic HTTP

Si tu utilises le site www.ebay.com pour analyser le trafic HTTP, voici comment répondre aux questions dans la PARTIE II : Examiner le trafic HTTP :

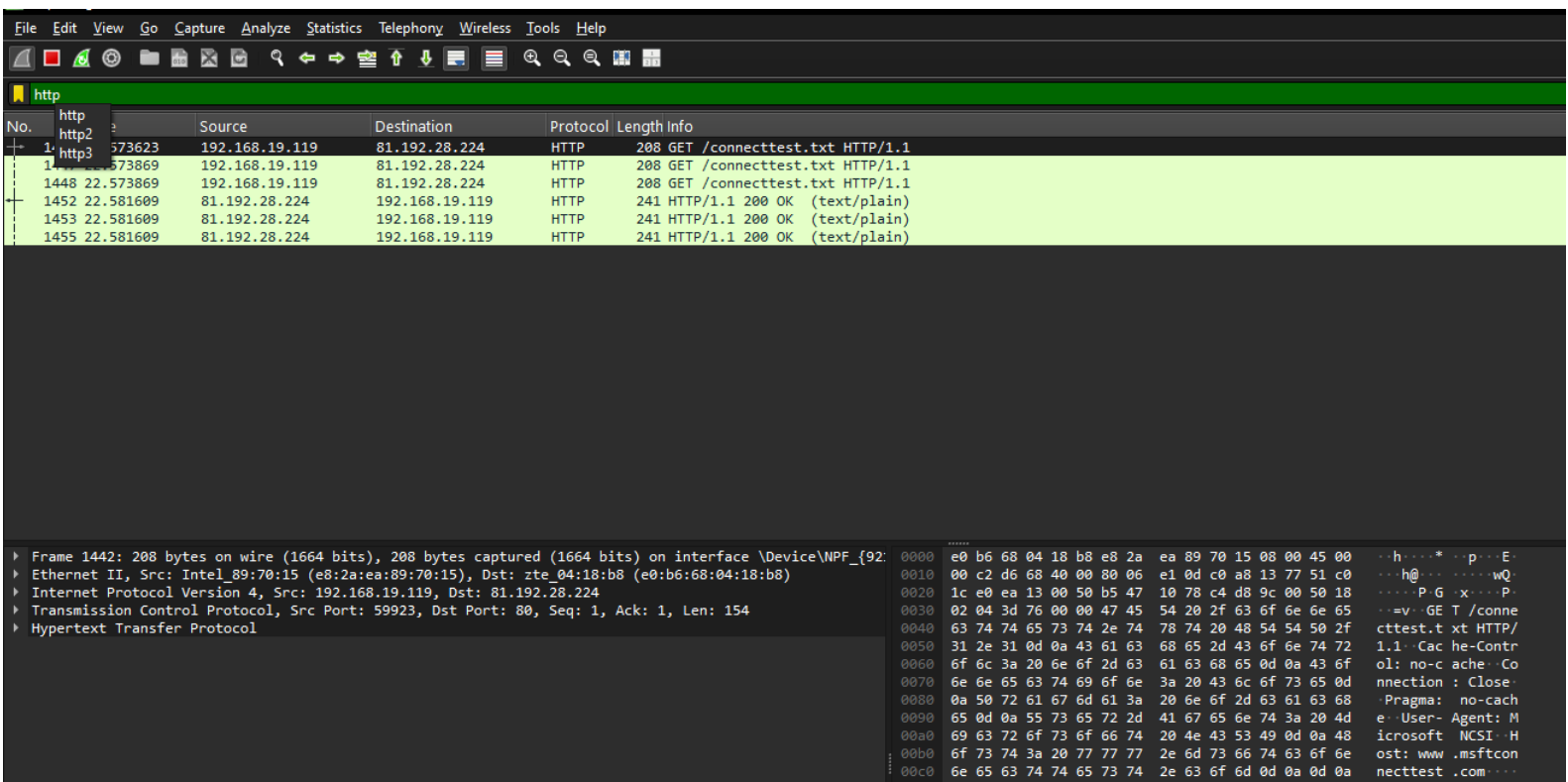
Exercice 1 : Examiner le trafic HTTP avec www.ebay.com

1. Connectez-vous au site <https://www.ebay.com/>

- Ouvre ton navigateur, accède à eBay et laisse les données se charger complètement.

2. Sur Wireshark, appliquer un filtre pour afficher le trafic HTTP.

- **Filtre : http**



The screenshot shows the Wireshark network protocol analyzer interface. The top menu bar includes File, Edit, View, Go, Capture, Analyze, Statistics, Telephony, Wireless, Tools, and Help. Below the menu is a toolbar with various icons for file operations, capture control, and analysis. The main display area is divided into three panes. The top pane shows a list of captured packets, with the first three packets highlighted in green. The middle pane shows the details of the selected packet (No. 1, http2), displaying the source and destination IP addresses, the protocol (HTTP), and the length of the packet. The bottom pane shows the raw packet data in hexadecimal and ASCII format.

No.	Time	Source	Destination	Protocol	Length	Info
1	0.000000	192.168.19.119	81.192.28.224	HTTP	208	GET /connecttest.txt HTTP/1.1
2	0.000000	192.168.19.119	81.192.28.224	HTTP	208	GET /connecttest.txt HTTP/1.1
3	0.000000	192.168.19.119	81.192.28.224	HTTP	208	GET /connecttest.txt HTTP/1.1
1448	22.573869	192.168.19.119	81.192.28.224	HTTP	241	HTTP/1.1 200 OK (text/plain)
1452	22.581609	81.192.28.224	192.168.19.119	HTTP	241	HTTP/1.1 200 OK (text/plain)
1453	22.581609	81.192.28.224	192.168.19.119	HTTP	241	HTTP/1.1 200 OK (text/plain)
1455	22.581609	81.192.28.224	192.168.19.119	HTTP	241	HTTP/1.1 200 OK (text/plain)

Frame 1442: 208 bytes on wire (1664 bits), 208 bytes captured (1664 bits) on interface \Device\NPF_{92...} Ethernet II, Src: Intel_89:70:15 (e8:2a:ea:89:70:15), Dst: zte_04:18:b8 (e0:b6:68:04:18:b8) Internet Protocol Version 4, Src: 192.168.19.119, Dst: 81.192.28.224 Transmission Control Protocol, Src Port: 59923, Dst Port: 80, Seq: 1, Ack: 1, Len: 154 Hypertext Transfer Protocol

3. En se basant sur les informations transportées par la méthode GET et sa réponse, répondez :

- **a) Quelle est la version du protocole HTTP que votre navigateur utilise ? Quelle version est utilisée par le serveur ?**
 - Pour le voir :
 - Sélectionne un paquet HTTP dans Wireshark.
 - Dans le volet **Packet Details**, vérifie le champ **HTTP Version**
 - Cela indiquera également la version utilisée par le serveur dans la réponse.
- **b) Quelle(s) langue(s) votre navigateur supporte-t-il ?**
 - Dans les en-têtes de la requête GET, vérifie le champ **Accept-Language**.
 - Exemple : Accept-Language: en-US,en;q=0.9,fr;q=0.8.
- **c) Quelle est la taille en octets du contenu retourné vers votre navigateur ?**

- Dans la réponse HTTP **Content-Length**, qui indique la taille des données envoyées au navigateur.
- **d) Quelle est la version du serveur Web ?**
 - Dans les en-têtes de la réponse HTTP, cherche le champ **Server**.

Server: Apache/2.4.41.

4. Examiner les différents messages envoyés :

- **a) Combien de requêtes GET ont été envoyées par votre navigateur ?**
 - Compte le nombre de requêtes GET dans le trafic capturé (filtrage HTTP).
- **b) Combien de segments TCP (transportant les données) sont nécessaires pour transmettre le message réponse HTTP ?**
 - examine les segments TCP associés dans le **Stream**.
 - Pour chaque réponse, tu peux voir les numéros de séquence dans les paquets TCP pour calculer combien de segments sont utilisés.

de Réponses avec eBay :

a) Version HTTP :

- Navigateur : HTTP/1.1.
- Serveur : HTTP/1.1.

b) Langues supportées par le navigateur :

- Exemple : en-US,fr-FR.

c) Taille en octets du contenu retourné :

- Exemple : Content-Length: 6845 octets.

d) Version du serveur Web :

- Exemple : Server: Apache.

Nombre de requêtes GET :

- Exemple : Environ 30 requêtes GET pour eBay, incluant la page principale et les ressources (images, scripts, etc.).

Nombre de segments TCP nécessaires :

- Exemple : 3 à 5 segments TCP peuvent être nécessaires, selon la taille de la réponse HTTP.