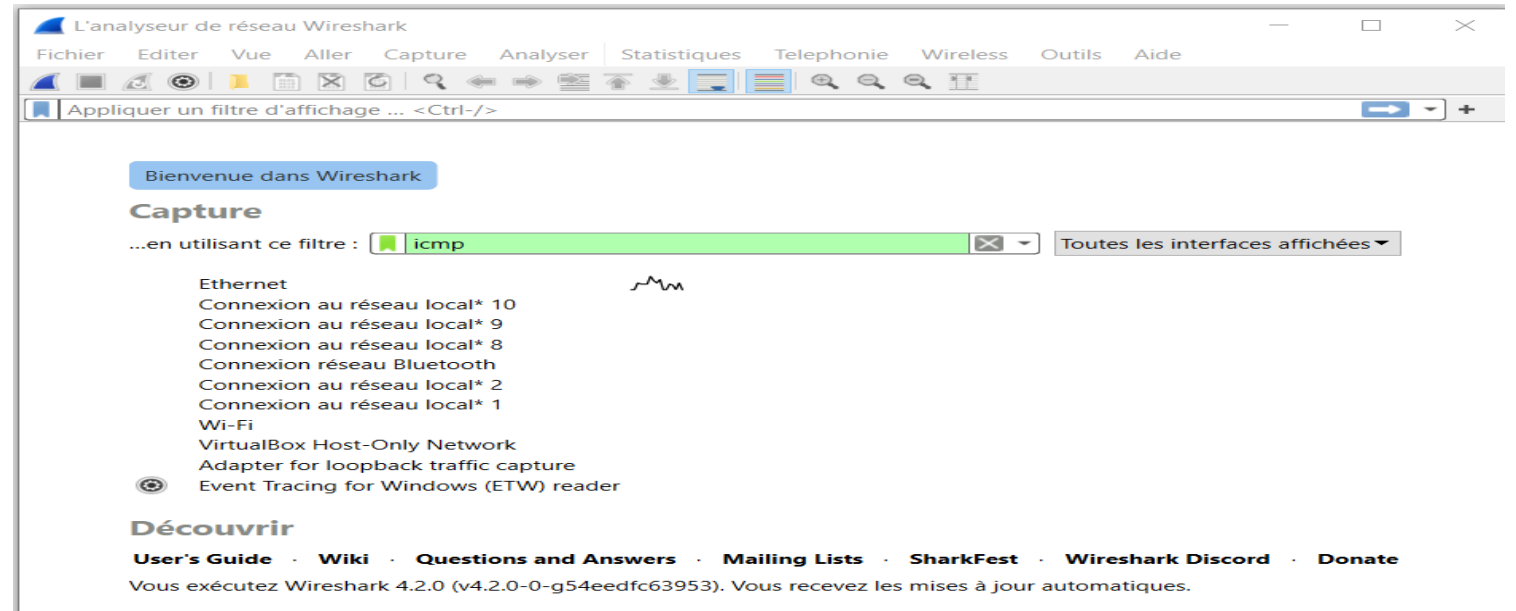
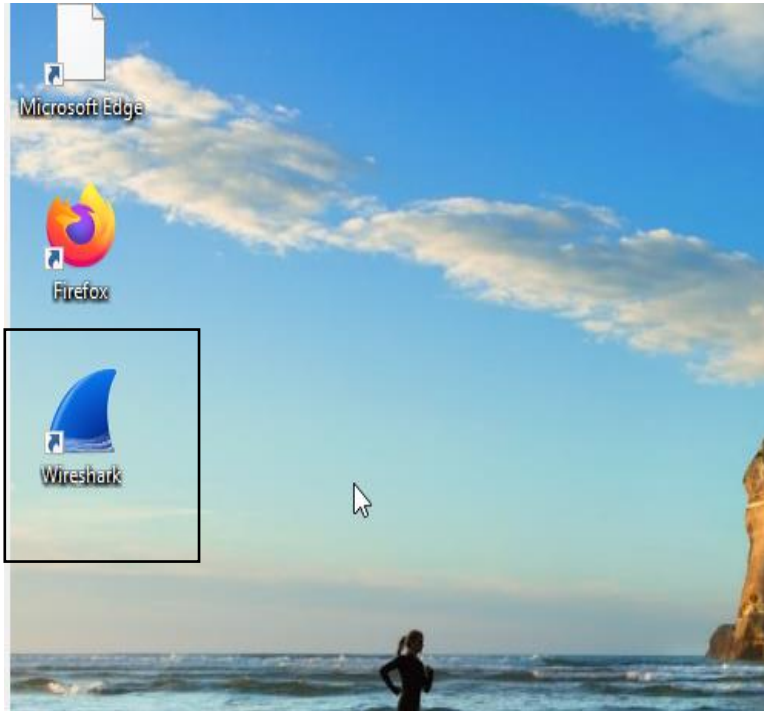


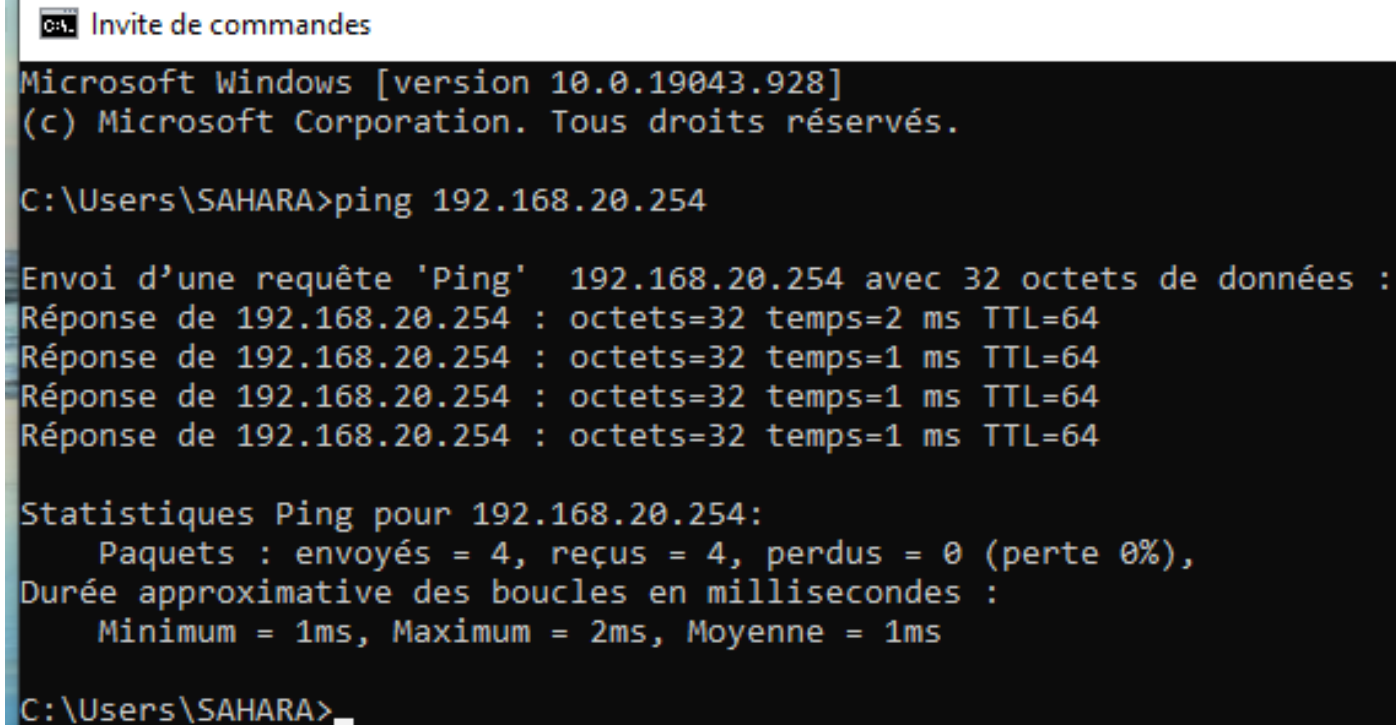
TP initiation wireshark



1- Téléchargement de Wireshark



2- Vérification de la bonne connectivité du réseau



Invite de commandes

Microsoft Windows [version 10.0.19043.928]
(c) Microsoft Corporation. Tous droits réservés.

C:\Users\SAHARA>ping 192.168.20.254

Envoi d'une requête 'Ping' 192.168.20.254 avec 32 octets de données :
Réponse de 192.168.20.254 : octets=32 temps=2 ms TTL=64
Réponse de 192.168.20.254 : octets=32 temps=1 ms TTL=64
Réponse de 192.168.20.254 : octets=32 temps=1 ms TTL=64
Réponse de 192.168.20.254 : octets=32 temps=1 ms TTL=64

Statistiques Ping pour 192.168.20.254:
Paquets : envoyés = 4, reçus = 4, perdus = 0 (perte 0%),
Durée approximative des boucles en millisecondes :
Minimum = 1ms, Maximum = 2ms, Moyenne = 1ms

C:\Users\SAHARA>_

3- Utilisation de Wireshark

icmp							
No.	Time	Source	Destination	Protocol	Length	Info	
106	56.753927	192.168.60.95	192.168.20.254	ICMP	74	Echo (ping) request	id=0x0001, seq=9/2304, ttl=128 (reply in 107)
107	56.754310	192.168.20.254	192.168.60.95	ICMP	74	Echo (ping) reply	id=0x0001, seq=9/2304, ttl=64 (request in 106)
110	57.760395	192.168.60.95	192.168.20.254	ICMP	74	Echo (ping) request	id=0x0001, seq=10/2560, ttl=128 (reply in 111)
111	57.760925	192.168.20.254	192.168.60.95	ICMP	74	Echo (ping) reply	id=0x0001, seq=10/2560, ttl=64 (request in 110)
112	58.768337	192.168.60.95	192.168.20.254	ICMP	74	Echo (ping) request	id=0x0001, seq=11/2816, ttl=128 (reply in 113)
113	58.769152	192.168.20.254	192.168.60.95	ICMP	74	Echo (ping) reply	id=0x0001, seq=11/2816, ttl=64 (request in 112)
115	59.775563	192.168.60.95	192.168.20.254	ICMP	74	Echo (ping) request	id=0x0001, seq=12/3072, ttl=128 (reply in 116)
116	59.776382	192.168.20.254	192.168.60.95	ICMP	74	Echo (ping) reply	id=0x0001, seq=12/3072, ttl=64 (request in 115)
340	46.175426	192.168.60.95	192.168.60.254	ICMP	74	Echo (ping) request	id=0x0001, seq=21/5376, ttl=128 (reply in 341)
341	46.175703	192.168.60.254	192.168.60.95	ICMP	74	Echo (ping) reply	id=0x0001, seq=21/5376, ttl=64 (request in 340)
401	47.182189	192.168.60.95	192.168.60.254	ICMP	74	Echo (ping) request	id=0x0001, seq=22/5632, ttl=128 (reply in 402)
402	47.182463	192.168.60.254	192.168.60.95	ICMP	74	Echo (ping) reply	id=0x0001, seq=22/5632, ttl=64 (request in 401)
405	48.187166	192.168.60.95	192.168.60.254	ICMP	74	Echo (ping) request	id=0x0001, seq=23/5888, ttl=128 (reply in 406)
406	48.187503	192.168.60.254	192.168.60.95	ICMP	74	Echo (ping) reply	id=0x0001, seq=23/5888, ttl=64 (request in 405)
408	49.193497	192.168.60.95	192.168.60.254	ICMP	74	Echo (ping) request	id=0x0001, seq=24/6144, ttl=128 (reply in 409)
409	49.193727	192.168.60.254	192.168.60.95	ICMP	74	Echo (ping) reply	id=0x0001, seq=24/6144, ttl=64 (request in 408)

Requête de 192.168.60.95

Réponse de
192.168.60.254

Liste des trames

```
> Frame 341: 74 bytes on wire (592 bits), 74 bytes captured (592 bits) on interface \Device\NPF_{56810784-C1A7-41D0-B7E3-6FEA2A242092}, id 0
  > Ethernet II, Src: HewlettPacka_14:b7:1d (e8:39:35:14:b7:1d), Dst: Dell_4b:e9:e9 (18:db:f2:4b:e9:e9)
    > Destination: Dell_4b:e9:e9 (18:db:f2:4b:e9:e9)
    > Source: HewlettPacka_14:b7:1d (e8:39:35:14:b7:1d)
    Type: IPv4 (0x0800)
  > Internet Protocol Version 4, Src: 192.168.60.254, Dst: 192.168.60.95
  > Internet Control Message Protocol
    Type: 0 (Echo (ping) reply)
    Code: 0
    Checksum: 0x5546 [correct]
    [Checksum Status: Good]
    Identifier (BE): 1 (0x0001)
    Identifier (LE): 256 (0x0100)
    Sequence Number (BE): 21 (0x0015)
    Sequence Number (LE): 5376 (0x1500)
    [Request frame: 340]
    [Response time: 0,277 ms]
  > Data (32 bytes)
```

Détaille des trames

- L'adresse MAC source :18:db:f2:4b:e9:e9
- L'adresse MAC destinataire: e8: 39:35:14:b7:1d
- L'adresse IP source : 192.168.60.95
- L'adresse IP destinataire:192.168.60.254
- Le Time To Live:64
- Le numéro de trame:341
- La taille de la trame:74bytes((592bits)
- La taille des données:32bytes
- Le code type ICMP:1

4- Modification des paramètres IP

- Les machine n'étant pas sur le même réseau on ne peut pas effectuer un ping vers la machine 172.16.45.36 donc le wireshark en filtre icmp ne chargera pas

Propriétés de : Protocole Internet version 4 (TCP/IPv4) X

Général

Les paramètres IP peuvent être déterminés automatiquement si votre réseau le permet. Sinon, vous devez demander les paramètres IP appropriés à votre administrateur réseau.

☐ Obtenir une adresse IP automatiquement

☒ Utiliser l'adresse IP suivante :

Adresse IP : 172 . 16 . 45 . 36

Masque de sous-réseau : 255 . 255 . 0 . 0

Passerelle par défaut : . . .

☐ Obtenir les adresses des serveurs DNS automatiquement

☒ Utiliser l'adresse de serveur DNS suivante :

Serveur DNS préféré : . . .

Serveur DNS auxiliaire : . . .

☒ Valider les paramètres en quittant

Avancé...

OK Annuler

```
C:\Users\Sarah>ping 172.16.45.36
```

```
Envoi d'une requête 'Ping' 172.16.45.36 avec 32 octets de données :  
Réponse de 192.168.60.95 : Impossible de joindre l'hôte de destination.  
Réponse de 192.168.60.95 : Impossible de joindre l'hôte de destination.  
Réponse de 192.168.60.95 : Impossible de joindre l'hôte de destination.  
Réponse de 192.168.60.95 : Impossible de joindre l'hôte de destination.
```

```
Statistiques Ping pour 172.16.45.36:
```

```
Paquets : envoyés = 4, reçus = 4, perdus = 0 (perte 0%),
```

5-Analyse du protocole http et https

http						
No.	Time	Source	Destination	Protocol	Length	Info
67	3.868302	142.250.75.227	192.168.60.95	OCSP	526	Response
260	20.039561	192.168.60.95	87.98.154.146	HTTP	474	GET / HTTP/1.1
279	20.799625	87.98.154.146	192.168.60.95	HTTP	60	HTTP/1.1 200 OK (text/html)
282	20.878076	192.168.60.95	87.98.154.146	HTTP	497	GET /theme/adaptable/style/font-awesome.min.css HTTP/1.1
284	20.880790	87.98.154.146	192.168.60.95	HTTP	384	HTTP/1.1 304 Not Modified
306	21.010020	192.168.60.95	87.98.154.146	HTTP	464	GET /pluginfile.php/3879/user/icon/adaptable/f1?rev=45376 HTTP/1.1
311	21.016482	192.168.60.95	87.98.154.146	HTTP	464	GET /pluginfile.php/3876/user/icon/adaptable/f1?rev=45447 HTTP/1.1
334	21.128700	87.98.154.146	192.168.60.95	HTTP	147	HTTP/1.1 200 OK (JPEG JFIF image)
340	21.149060	87.98.154.146	192.168.60.95	HTTP	688	HTTP/1.1 200 OK (JPEG JFIF image)
379	21.530305	192.168.60.95	87.98.154.146	HTTP/J...	732	POST /lib/ajax/service.php?sesskey=4YFNKxWxPv&info=create_message_get_unread_conversations_count HTTP/1.1 , JSON (application/json)
382	21.542352	192.168.60.95	87.98.154.146	HTTP/J...	745	POST /lib/ajax/service.php?sesskey=4YFNKxWxPv&info=message_popup_get_unread_popup_notification_count HTTP/1.1 , JSON (application/json)
392	21.645644	87.98.154.146	192.168.60.95	HTTP/J...	60	HTTP/1.1 200 OK , JSON (application/json)
396	21.662133	87.98.154.146	192.168.60.95	HTTP/J...	60	HTTP/1.1 200 OK , JSON (application/json)
508	26.543507	192.168.60.95	34.107.221.82	HTTP	378	GET /canonical.html HTTP/1.1
517	26.552060	34.107.221.82	192.168.60.95	HTTP	144	HTTP/1.1 200 OK (text/html)
520	26.557513	192.168.60.95	34.107.221.82	HTTP	380	GET /success.txt?ipv4 HTTP/1.1
523	26.565478	34.107.221.82	192.168.60.95	HTTP	62	HTTP/1.1 200 OK (text/plain)

Clés de session

Composition du site (architecture du site)

> Frame 284: 384 bytes on wire (3072 bits), 384 bytes captured (3072 bits) on interface \Device\NPF_{56810784-C1A7-41D0-B7E3-6FEA2A242092}, id 0

> Ethernet II, Src: HewlettPacka_14:b7:1d (e8:39:35:14:b7:1d), Dst: Dell_4b:e9:e9 (18:db:f2:4b:e9:e9)

> Internet Protocol Version 4, Src: 87.98.154.146, Dst: 192.168.60.95

> Transmission Control Protocol, Src Port: 80, Dst Port: 52727, Seq: 14821, Ack: 865, Len: 330

> Hypertext Transfer Protocol

0000 18 db f2 4b e9 e9 e8 39 35 14 b7 1d 08 00 45 00 ... ^

0010 01 72 00 00 40 00 40 06 4a 8a 57 62 9a 92 c0 a8 ... r

0020 3c 5f 00 50 cd f7 c7 d1 d1 5c b2 eb 99 da 50 18 < _

0030 02 02 8b 79 00 00 48 54 54 50 2f 31 2e 31 20 33 ...

0040 30 34 20 4e 6f 74 20 4d 6f 64 69 66 69 65 64 0d 04

0050 0a 44 61 74 65 3a 20 57 65 64 2c 20 32 32 20 4e .De

6-Analyse du protocole FTP

The image shows a Wireshark packet capture of an FTP session. The packet list on the left shows several packets, with packet 66 selected. The packet details pane on the right shows the FTP protocol structure. The 'Request' field is expanded, showing the 'USER Admin' command. The 'Response' field shows the '331 Password required for Admin' message. The 'Request' field is further expanded, showing the 'PASS Root' command. The 'Response' field shows the '230 User Admin logged in.' message. The packet bytes pane at the bottom shows the raw data of the selected packet.

No.	Time	Source	Destination	Protocol	Length	Info
53	18.916836	192.168.60.197	192.168.60.95	FTP	92	Response: 220 TYPSoft FTP Server 1.10 ready...
54	18.923964	192.168.60.95	192.168.60.197	FTP	64	Request: AUTH TLS
55	18.924805	192.168.60.197	192.168.60.95	FTP	91	Response: 500 'AUTH': command not understood
56	18.928945	192.168.60.95	192.168.60.197	FTP	64	Request: AUTH SSL
57	18.931653	192.168.60.197	192.168.60.95	FTP	91	Response: 500 'AUTH': command not understood.
58	18.937210	192.168.60.95	192.168.60.197	FTP	66	Request: USER Admin
59	18.938254	192.168.60.197	192.168.60.95	FTP	88	Response: 331 Password required for Admin
60	18.939567	192.168.60.95	192.168.60.197	FTP	65	Request: PASS Root
61	18.951161	192.168.60.197	192.168.60.95	FTP	81	Response: 230 User Admin logged in.
63	19.016133	192.168.60.95	192.168.60.197	FTP	60	Request: PWD
64	19.019085	192.168.60.197	192.168.60.95	FTP	100	Response: 257 "/C:/Serveur FTP/" is current directory.

Identifiant de l'utilisateur

Mot de passe de Admin

The image shows the TYPSoft FTP Server log window. The log displays the following messages:

```
[09:44:41] - Server Started
[09:44:41] - FTP Port: 21
[09:45:25] - [1] Connect to 192.168.60.95. Get Username.
[09:45:28] - [1] User ADMIN Connected
[09:45:28] - [1] ADMIN: Current Directory: C:\Serveur FTP\
[09:45:39] - [2] Connect to 192.168.60.95. Get Username.
[09:45:39] - [2] User ADMIN Connected
[09:45:39] - [2] ADMIN: Current Directory: C:\Serveur FTP\
[09:47:29] - [3] Connect to 192.168.60.95. Get Username.
[09:47:29] - [3] User ADMIN Connected
[09:47:29] - [3] ADMIN: Current Directory: C:\Serveur FTP\
[09:49:08] - [1] Client ADMIN, 192.168.60.95 Disconnected (00:03:42 Min)
[09:49:08] - [2] Client ADMIN, 192.168.60.95 Disconnected (00:03:28 Min)
[09:49:08] - [3] Client ADMIN, 192.168.60.95 Disconnected (00:01:38 Min)
```

La sécurité du protocole FTP très est faible .

Pour améliorer la sécurité du protocole FTP je propose:

1. Désactiver le FTP standard: Si votre serveur exécute FTP par défaut, vous devriez le désactiver dès que possible.
2. Utiliser des mots de passe forts : Les mots de passe doivent comporter au moins 8 caractères.
3. Utiliser la sécurité des fichiers. Sécuriser votre administrateur.
4. Sécuriser votre administrateur.