

TASHI SONAM AIDOR TSANG		BTSSIO1 12/03/25
----------------------------	--	---------------------

## Étape 1 : Exécution d'un ping

Lancez Wireshark et démarrez la capture.

Dans une invite de commandes (Windows) ou un Terminal (Linux), envoyez la commande ping à une adresse IP, par exemple, 172.20.32.150

Attendez d'obtenir les résultats attendus du ping.

Arrêtez la capture des paquets dans Wireshark.

```
C:\Users\aidor>ping 172.20.32.150

Pinging 172.20.32.150 with 32 bytes of data:
Reply from 172.20.32.150: bytes=32 time<1ms TTL=128

Ping statistics for 172.20.32.150:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
    Approximate round trip times in milli-seconds:
        Minimum = 0ms, Maximum = 0ms, Average = 0ms
```

## Étape 2 : Observation du volet de la liste des paquets

Examinez les paquets similaires aux paquets de la liste fournie (paquets 19, 20, 22, 23, 24 et 25)

Quel protocole est utilisé avec la commande ping

ICMP (Internet Control Message Protocol)

Quel est le nom complet du protocole ?

Internet Control Message Protocol (ICMP)

Quels sont les noms des deux messages ping ?

Echo Request et Echo Reply

Qui envoie les messages ping (précisez qui envoie quel type de message) ?

L'émetteur envoie un Echo Request, et le récepteur renvoie un Echo Reply.

No.	Time	Source	Destination	Protocol	Length	Info
16	22.590889	172.20.32.150	13.107.42.12	TCP	66	50196 → 443 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 WS=256 SACK_PERM
17	22.597324	13.107.42.12	172.20.32.150	TCP	66	443 → 50196 [SYN, ACK] Seq=0 Ack=1 Win=65535 Len=0 MSS=1440 WS=256 SACK_PERM
18	22.597600	172.20.32.150	13.107.42.12	TCP	54	50196 → 443 [ACK] Seq=1 Ack=1 Win=132352 Len=0
19	22.600034	172.20.32.150	13.107.42.12	TLSv1.3	338	Client Hello (SNI=blz04pap001.storage.live.com)
20	22.607841	13.107.42.12	172.20.32.150	TCP	60	443 → 50196 [ACK] Seq=1 Ack=285 Win=4194048 Len=0
21	22.608627	13.107.42.12	172.20.32.150	TLSv1.3	153	Hello Retry Request, Change Cipher Spec
22	22.613240	172.20.32.150	13.107.42.12	TLSv1.3	409	Change Cipher Spec, Client Hello (SNI=blz04pap001.storage.live.com)
23	22.619363	fe80::6f26:8356:196...	ff02::fb	MDNS	105	Standard query 0x0000 PTR _microsoft_mcc_tcp.local, "QU" question
24	22.621181	13.107.42.12	172.20.32.150	TCP	60	443 → 50196 [ACK] Seq=100 Ack=640 Win=4193792 Len=0
25	22.628836	13.107.42.12	172.20.32.150	TLSv1.3	1514	Server Hello
26	22.629345	13.107.42.12	172.20.32.150	TCP	1514	443 → 50196 [ACK] Seq=1560 Ack=640 Win=4193792 Len=1460 [TCP segment of a reassembled PDU]
27	22.629345	13.107.42.12	172.20.32.150	TCP	1514	443 → 50196 [ACK] Seq=3020 Ack=640 Win=4193792 Len=1460 [TCP segment of a reassembled PDU]
28	22.629345	13.107.42.12	172.20.32.150	TCP	2974	443 → 50196 [ACK] Seq=4480 Ack=640 Win=4193792 Len=2920 [TCP segment of a reassembled PDU]
29	22.629501	172.20.32.150	13.107.42.12	TCP	54	50196 → 443 [ACK] Seq=640 Ack=7400 Win=132352 Len=0
30	22.629993	13.107.42.12	172.20.32.150	TCP	1514	443 → 50196 [ACK] Seq=7400 Ack=640 Win=4193792 Len=1460 [TCP segment of a reassembled PDU]
31	22.629993	13.107.42.12	172.20.32.150	TLSv1.3	358	Application Data
32	22.630078	172.20.32.150	13.107.42.12	TCP	54	50196 → 443 [ACK] Seq=640 Ack=9164 Win=132352 Len=0
33	22.633608	172.20.32.150	13.107.42.12	TLSv1.3	128	Application Data
34	22.633949	172.20.32.150	13.107.42.12	TCP	1494	50196 → 443 [ACK] Seq=714 Ack=9164 Win=132352 Len=1440 [TCP segment of a reassembled PDU]
35	22.633949	172.20.32.150	13.107.42.12	TLSv1.3	843	Application Data

Frame 17: 66 bytes on wire (528 bits), 66 bytes captured (528 bits) on interface DeviceNPF\_{C5836FFB-6...} 0000 82 30 1f 74 d3 81 b8 d4 e7 72 aa 80 08 00 45 00 0 t ... n E  
Ethernet II, Src: ArubaHewlett\_72:aa:80 (b8:d4:e7:72:aa:80), Dst: 82:30:1f:74:d3:81 (82:30:1f:74:d3:81) 0010 00 34 fa 54 40 00 f9 06 83 4d 0d 6b 2a 0c ac 14 4 T@ ... M k\*  
Internet Protocol Version 4, Src: 13.107.42.12, Dst: 172.20.32.150 0020 20 96 01 bb c4 14 a6 02 cd 31 5f 22 d9 f3 80 12 ... 1"  
Transmission Control Protocol, Src Port: 443, Dst Port: 50196, Seq: 0, Ack: 1, Len: 0 0030 ff ff f8 d8 00 00 02 04 05 a0 01 03 03 08 01 01 ... ..  
0040 04 02

## Étape 3: Visualisation des protocoles de chaque couche TCP/IP

Sélectionnez le premier paquet de requête d'écho (Request).

Regardez le détail des informations obtenues.

Quels sont les protocoles inclus dans la trame Ethernet ?

Protocoles incluent IPv4 et ICMP.

Wireshark capture of an HTTP POST request. The packet list shows a POST to /StableMSDiscoveryEndpoint/schemas-xmlsoap-org\_ws\_2005\_04\_discovery HTTP/1.1. The packet details pane shows the request body as XML. The packet bytes pane shows the raw data.

Wireshark capture of ICMP ping requests. The packet list shows multiple Echo (ping) requests to 172.20.32.159. The packet details pane shows the ICMP Echo (ping) request structure.

# Étape 4: Fermer la capture (sans sauvegarder)

## 2. Capture des PDU associées au protocole http

### Étape 1: Lancement de la capture des paquets

Lancez Wireshark.

Ouvrez un navigateur Web et saisissez l'URL d'un site web interne du réseau.

Attendez que la page Web soit téléchargée.

Arrêtez la capture des paquets dans Wireshark.

### Étape 2: Agrandissement du volet de la liste des paquets de Wireshark

Localisez et identifiez les paquets TCP et HTTP associés au téléchargement de la page Web.

Réponses aux questions :

Quel est l'adresse IP du serveur web ?

Recherchez l'adresse IP dans les paquets TCP/HTTP.

Identifiez les types de messages échangés. Quels sont-ils ?

Types de messages incluent TCP pour la gestion de la connexion et HTTP pour le transfert de données.

### Étape 3: Mise en surbrillance d'un paquet HTTP

Sélectionnez un paquet HTTP du volet supérieur portant la mention « (text/html) ».

Dans le volet des détails de paquet, cliquez sur le signe « + » en regard de Linebased text data: html.

Réponses aux questions :

Quel type d'informations s'affiche-t-il lorsque vous développez cet élément ?

Des données HTML.

Examinez la partie mise en surbrillance dans le volet des octets. Elle indique les données HTML transportées par le paquet.

Informations correspondantes aux couches du modèle TCP/IP

Les informations d'encapsulation capturées correspondent aux couches suivantes du modèle TCP/IP :

Ethernet: Couche d'accès au réseau

IPv4: Couche réseau

TCP: Couche transport

HTTP: Couche application

3. Capture des PDU associées au protocole HTTPS

Lancez une capture lors de l'accès à un site web utilisant le protocole HTTPS.

Comparez les différences avec les échanges d'un site Web en utilisant le protocole HTTP.