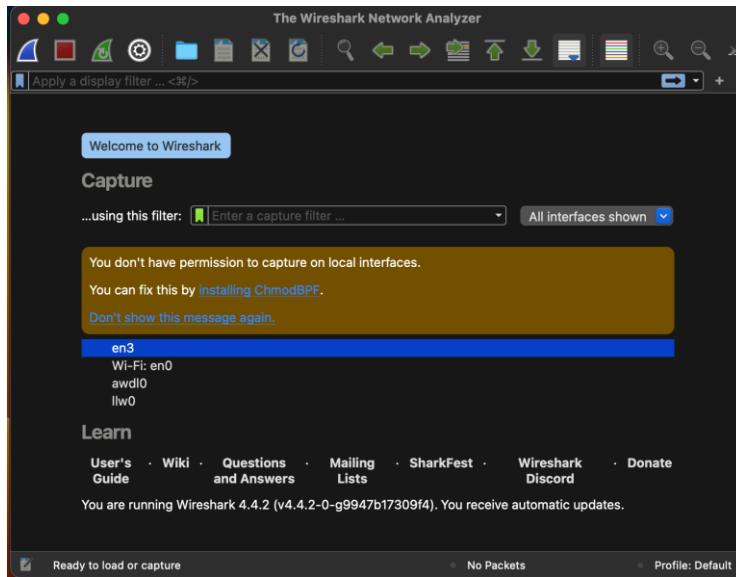


TP wire shark

1) Ci-joint l'installation de wireshark sur ma mac .



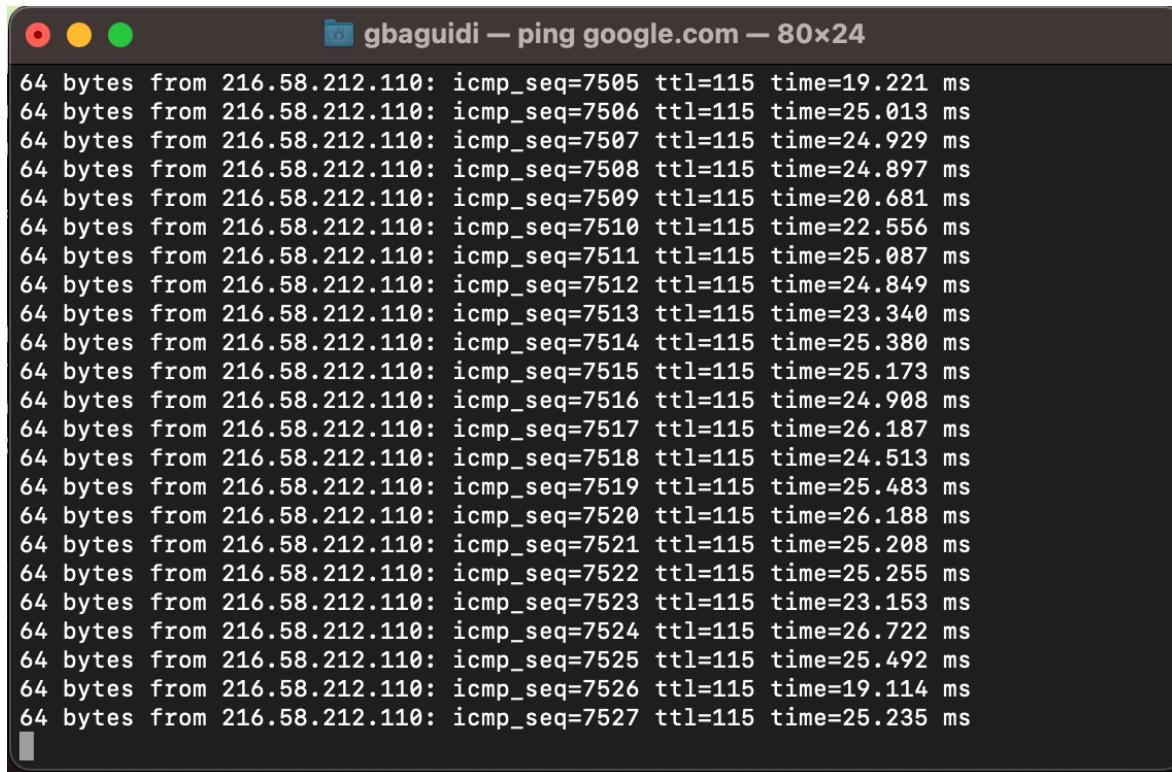
2) ci-joint j'ai choisis l'interface réseaux avec wi-fi .

No.	Time	Source	Destination	Protocol	Length	Info
5430	37.062135	2001:4860:4864:5:4...	2001:861:80:a500:a...	UDP	772	3478 → 55023 L
5430	37.072572	2001:861:80:a500:a...	2001:4860:4864:5:4...	UDP	106	55023 → 3478 L
5440	37.094055	SagemcomBroa_f3:ff:fc	Broadcast	0x7373	121	Ethernet II
5441	37.121875	2001:4860:4864:5:4...	2001:861:80:a500:a...	UDP	1068	3478 → 55023 L
5442	37.137994	2001:861:80:a500:a...	2001:4860:4864:5:4...	UDP	106	55023 → 3478 L
5443	37.152130	2001:4860:4864:5:4...	2001:861:80:a500:a...	UDP	812	3478 → 55023 L
5444	37.169571	2001:861:80:a500:a...	2001:4860:4864:5:4...	RTCP	110	Receiver Report
5445	37.198455	2001:861:80:a500:a...	2001:4860:4864:5:4...	UDP	106	55023 → 3478 L
5446	37.198894	2001:4860:4864:5:4...	2001:861:80:a500:a...	UDP	1055	3478 → 55023 L
5447	37.234814	2001:4860:4864:5:4...	2001:861:80:a500:a...	UDP	936	3478 → 55023 L
5448	37.234815	2001:4860:4864:5:4...	2001:861:80:a500:a...	UDP	174	3478 → 55023 L
5449	37.256079	2001:4860:4864:5:4...	2001:861:80:a500:a...	UDP	111	3478 → 55023 L

> Frame 1: 841 bytes on wire (6728 bits), 841 bytes captured (55023 bits) on interface en0
> Ethernet II, Src: SagemcomBroa_f3:ff:fc (38:00:00:00:00:00), Dst: Broadcast (ff:ff:ff:ff:ff:ff)
> Internet Protocol Version 6, Src: 2001:4860:4864:5:4..., Dst: 2001:861:80:a500:a0
> User Datagram Protocol, Src Port: 3478, Dst Port: 55023
> Data (779 bytes)

Wi-Fi: en0: <live capture in progress>

3) Ci-joint j'ai lancé la commande ping pour tester la connectivité entre ma machine et le serveur , ensuite cela permet de mesurer la latence et de vérifier les pertes de paquets , pour finir elle permet de capturer les paquets ICMP .



The screenshot shows a terminal window titled "gbaguidi — ping google.com — 80x24". The window displays the results of a ping command to the IP address 216.58.212.110. The output lists 30 ICMP echo requests (bytes from 216.58.212.110) with their sequence numbers (icmp_seq), Time-to-Live (ttl), and round-trip time (time). The times range from 19.221 ms to 25.492 ms.

```
64 bytes from 216.58.212.110: icmp_seq=7505 ttl=115 time=19.221 ms
64 bytes from 216.58.212.110: icmp_seq=7506 ttl=115 time=25.013 ms
64 bytes from 216.58.212.110: icmp_seq=7507 ttl=115 time=24.929 ms
64 bytes from 216.58.212.110: icmp_seq=7508 ttl=115 time=24.897 ms
64 bytes from 216.58.212.110: icmp_seq=7509 ttl=115 time=20.681 ms
64 bytes from 216.58.212.110: icmp_seq=7510 ttl=115 time=22.556 ms
64 bytes from 216.58.212.110: icmp_seq=7511 ttl=115 time=25.087 ms
64 bytes from 216.58.212.110: icmp_seq=7512 ttl=115 time=24.849 ms
64 bytes from 216.58.212.110: icmp_seq=7513 ttl=115 time=23.340 ms
64 bytes from 216.58.212.110: icmp_seq=7514 ttl=115 time=25.380 ms
64 bytes from 216.58.212.110: icmp_seq=7515 ttl=115 time=25.173 ms
64 bytes from 216.58.212.110: icmp_seq=7516 ttl=115 time=24.908 ms
64 bytes from 216.58.212.110: icmp_seq=7517 ttl=115 time=26.187 ms
64 bytes from 216.58.212.110: icmp_seq=7518 ttl=115 time=24.513 ms
64 bytes from 216.58.212.110: icmp_seq=7519 ttl=115 time=25.483 ms
64 bytes from 216.58.212.110: icmp_seq=7520 ttl=115 time=26.188 ms
64 bytes from 216.58.212.110: icmp_seq=7521 ttl=115 time=25.208 ms
64 bytes from 216.58.212.110: icmp_seq=7522 ttl=115 time=25.255 ms
64 bytes from 216.58.212.110: icmp_seq=7523 ttl=115 time=23.153 ms
64 bytes from 216.58.212.110: icmp_seq=7524 ttl=115 time=26.722 ms
64 bytes from 216.58.212.110: icmp_seq=7525 ttl=115 time=25.492 ms
64 bytes from 216.58.212.110: icmp_seq=7526 ttl=115 time=19.114 ms
64 bytes from 216.58.212.110: icmp_seq=7527 ttl=115 time=25.235 ms
```

4) Analyser la couche transport (TCP) : ci –joint ont peut trouvé la Source port qui : 50179

On peut également voir la destination port qui est : 443 – port standard pour Https (communication sécurisé)

On peut voir la sequence Number qui est : 90026 (elle indique la position du 1er octet des données envoyées)

On a aussi le Acknowledgment Number qui est : 17630 (il confirme la bonne réception des données du coté opposé)

On retrouve le flag TCP qui est le suivant : ACK (ce flag confirme que les données précédentes ont été reçu .

Capturing from Wi-Fi: en0						
No.	Time	Source	Destination	Protocol	Length	Info
198...	1292.459595	2001:861:80:a500:a...	2603:1063:2206:24:...	TCP	74	50179 → 443 [A]
198...	1292.481330	2603:1063:2206:24:...	2001:861:80:a500:a...	TCP	74	443 → 50179 [A]
199...	1300.651794	2001:861:80:a500:a...	2603:1026:2400:1::2	TCP	74	[TCP Keep-Alive]
199...	1301.152916	2001:861:80:a500:a...	2603:1063:2000:1::...	TCP	74	[TCP Keep-Alive]
199...	1301.153000	2001:861:80:a500:a...	2603:1063:2206:24:...	TCP	74	[TCP Keep-Alive]
199...	1301.173967	2603:1063:2000:1::...	2001:861:80:a500:a...	TCP	74	[TCP Keep-Alive]
199...	1301.174890	2603:1063:2206:24:...	2001:861:80:a500:a...	TCP	74	[TCP Keep-Alive]
199...	1305.145097	2001:861:80:a500:a...	2603:1026:700:14::2	TCP	74	[TCP Keep-Alive]
199...	1307.157815	2001:861:80:a500:a...	2603:1063:2000:1::...	TCP	74	[TCP Keep-Alive]
199...	1307.178614	2603:1063:2000:1::...	2001:861:80:a500:a...	TCP	74	[TCP Keep-Alive]
199...	1308.394636	2001:861:80:a500:a...	2603:1063:2206:24:...	TCP	74	50179 → 443 [A]
199...	1308.416505	2603:1063:2206:24:...	2001:861:80:a500:a...	TCP	74	443 → 50179 [A]

> Frame 199961: 74 bytes on wire (592 bits), 7 Ethernet II, Src: Apple_70:ce:48 (14:7d:da:7) Internet Protocol Version 6, Src: 2001:861:8 Transmission Control Protocol, Src Port: 501 Source Port: 50179 Destination Port: 443 [Stream index: 190] > [Conversation completeness: Incomplete, D [TCP Segment Len: 0] Sequence Number: 90026 (relative sequen Sequence Number (raw): 3698444713 [Next Sequence Number: 90026 (relative Acknowledgment Number: 17630 (relative

0000 38 35 fb f3 ff fc 14 7d da 70 ce 48 86 0010 0a 00 00 14 06 40 20 01 08 61 00 80 a5 0020 38 ce 11 78 06 84 26 03 10 63 22 06 00 0030 00 00 00 00 05 c4 03 01 bb dc 71 c9 0040 a8 67 50 10 10 00 bb a1 00 00

Transmission Control Protocol (tcp), 20 bytes Packets: 323276 Profile: Default

On retrouve un protocol ICMP avec une taille total de 84 octet , ensuite pour l'adresse ip source on retrouve : 216.58.212.118 et l'adresse de destination : 192.168.1.1 .

Capturing from Wi-Fi: en0

No. | Time | Source | Destination | Protocol | Length | Info

458...	3843.172424	216.58.212.110	192.168.1.1	ICMP	98	Echo (ping) re
459...	3844.156952	192.168.1.1	216.58.212.110	ICMP	98	Echo (ping) re
459...	3844.176324	216.58.212.110	192.168.1.1	ICMP	98	Echo (ping) re
→ 459...	3845.160746	192.168.1.1	216.58.212.110	ICMP	98	Echo (ping) re
459...	3845.161992	192.168.1.123	224.0.0.251	IGMPv2	46	Membership Rep
← 459...	3845.179826	216.58.212.110	192.168.1.1	ICMP	98	Echo (ping) re
459...	3846.165437	192.168.1.1	216.58.212.110	ICMP	98	Echo (ping) re
459...	3846.185080	216.58.212.110	192.168.1.1	ICMP	98	Echo (ping) re
460...	3847.168345	192.168.1.1	216.58.212.110	ICMP	98	Echo (ping) re
460...	3847.188421	216.58.212.110	192.168.1.1	ICMP	98	Echo (ping) re
460...	3848.172621	192.168.1.1	216.58.212.110	ICMP	98	Echo (ping) re
460...	3848.181632	216.58.212.110	192.168.1.1	TCMP	98	Echo (ping) re

```

> Frame 459603: 98 bytes on wire (784 bits), 9 0000 14 7d da 70 ce 48 38 35 fb f3 ff fc 08
> Ethernet II, Src: SagemcomBroa_f3:ff:fc (38:00:54:00:00:00)
-> Internet Protocol Version 4, Src: 216.58.212.0100 .... = Version: 4
  .... 0101 = Header Length: 20 bytes (5)
-> Differentiated Services Field: 0x00 (DSCP: 0000) Total Length: 84
  Identification: 0x0000 (0)
-> 000. .... = Flags: 0x0
  ...0 0000 0000 0000 = Fragment Offset: 0
  Time to Live: 115
  Protocol: ICMP (1)
  Header Checksum: 0xd956 [validation disabled]

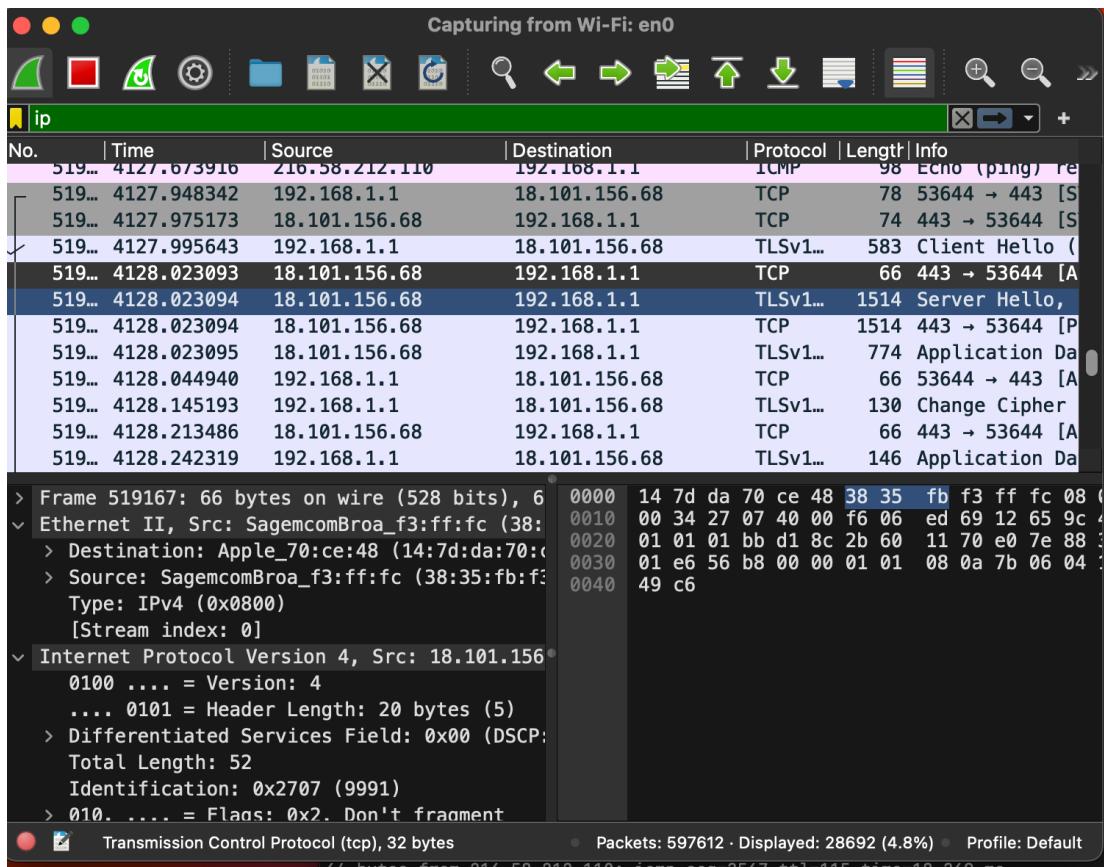
```

Internet Protocol Version 4: Protocol ● Packets: 519484 · Displayed: 20875 (4.0%) ● Profile: Default

Ci-joint on retrouve l'adresse **MAC** de l'émetteur :
38:35:f8:f3:ff:fc

On peut également voir l'adresse **MAC** destination :
apple_70:ce:48

Ipv4 type 0*0800 .



ci- joint le **Protocole : HTTP (Hypertext Transfer Protocol)**, utilisé pour les échanges web.

Source et destination avec pour **source IP** : 141.95.154.189 (serveur web). **Destination IP** : 192.168.1.1 (client ou routeur). **Port source** : 80 (port HTTP standard). **Port destination** : Dynamique, attribué par le client.

Transport sous-jacent :

Protocole TCP pour un transfert fiable.

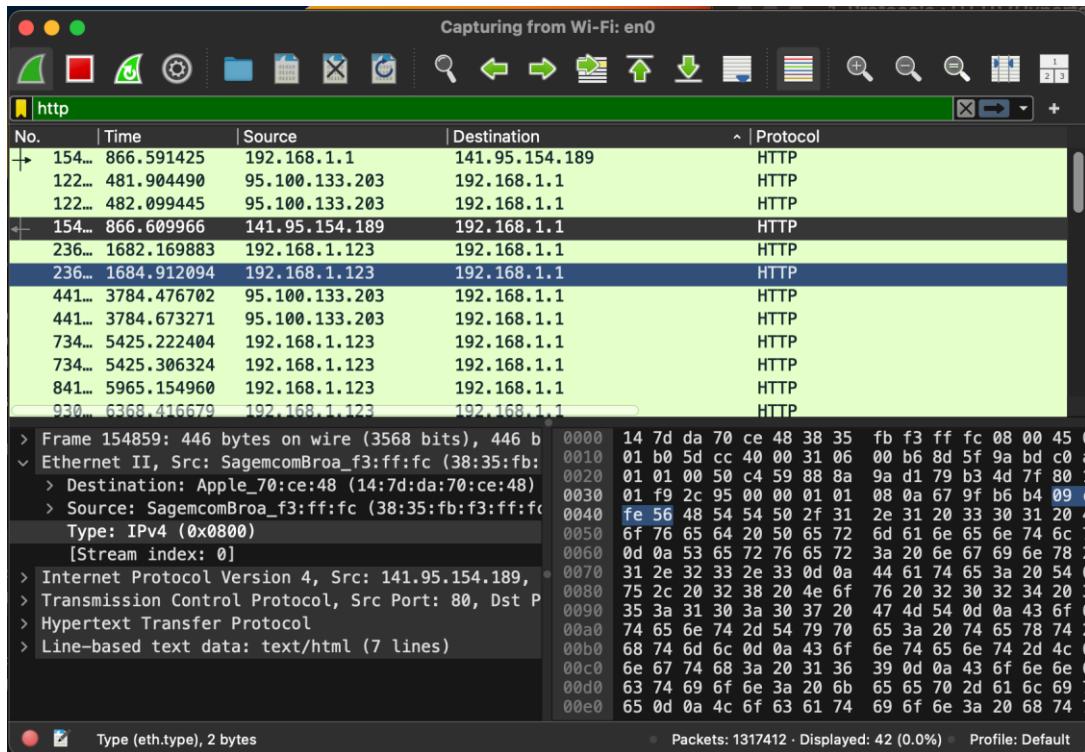
Couches impliquées :

Application : HTTP pour les requêtes/réponses web.

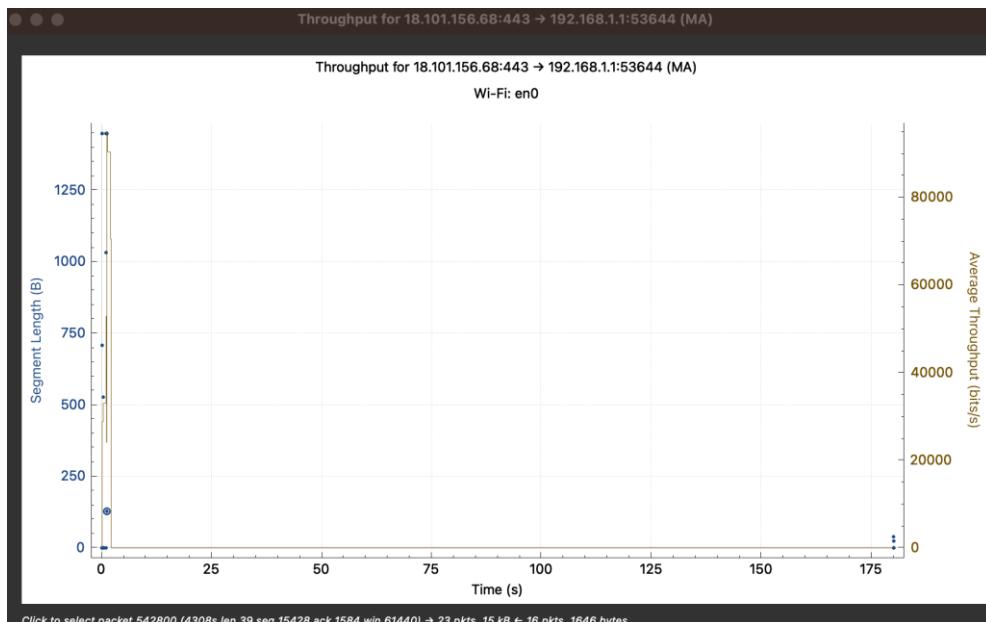
Transport : TCP pour la fiabilité.

Internet : IPv4 pour l'adressage.

Accès réseau : Ethernet pour la transmission physique.



ci-joint l'analyse graphique du **débit** qui montre l'évolution du débit réseau dans le temps pour analyser la performance et la stabilité du réseaux .



Compte rendu : L'analyse des trames Ethernet (couche d'accès réseau) a montré l'encapsulation des données via les adresses MAC et le type EtherType (IPv4, IPv6). Au niveau Internet, les paquets IP ont révélé l'adressage, le routage, et le TTL. Dans la couche transport, les échanges TCP/UDP ont illustré la fiabilité des communications (TCP) et la rapidité des requêtes DNS (UDP). Enfin, la couche application a permis d'étudier DNS, HTTP et ICMP, mettant en lumière les

interactions réseau des applications, la résolution des noms de domaine et les mesures de latence.