

Wireshark est un logiciel open source d'analyse des protocoles réseau créé par Gerald Combs en 1998. Il est utilisé par des agences gouvernementales, de grandes entreprises, des organisations à but non lucratif et des établissements pédagogiques pour résoudre des problèmes réseau et assurer des formations.

Wireshark est un outil de capture et d'analyse de paquets. Il capture le trafic du réseau local et stocke les données ainsi obtenues pour permettre leur analyse hors ligne.

Wireshark est capable de capturer le trafic Ethernet, Bluetooth, sans fil (IEEE.802.11), Token Ring, Frame Relay et plus encore. *Remarque : un « paquet » est un message d'un protocole réseau (par ex., TCP, DNS, etc.)*

Quelle est la différence entre une trame et un paquet ?

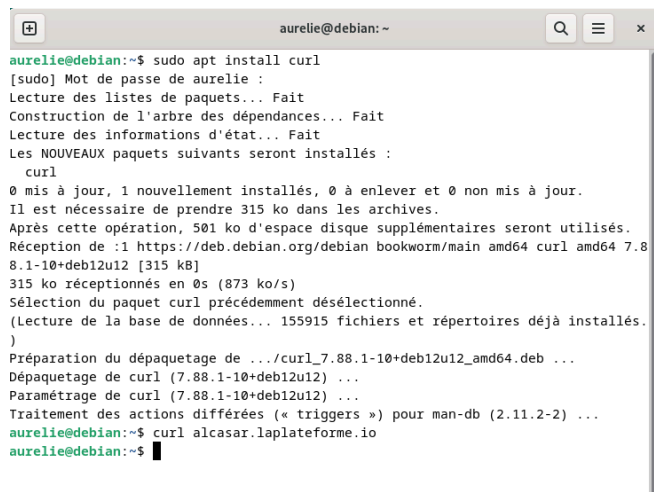
Une trame est un bloc de données envoyé en bloc sur la liaison de données (Ethernet, ATM). **Un paquet** est un bloc de données envoyé en bloc sur la couche supérieure (IP).

Qu'est-ce que le format pcap/pcapng ?

- Une trace de capture de paquets (PCAP) est une capture effectuée à partir d'une interface réseau pour effectuer une analyse et un dépannage du réseau.
- Les fichiers PCAPNG appartiennent principalement à Wireshark de The Wireshark team. PCAPNG est un format utilisé pour enregistrer les traces de paquets réseau capturés dans un fichier.

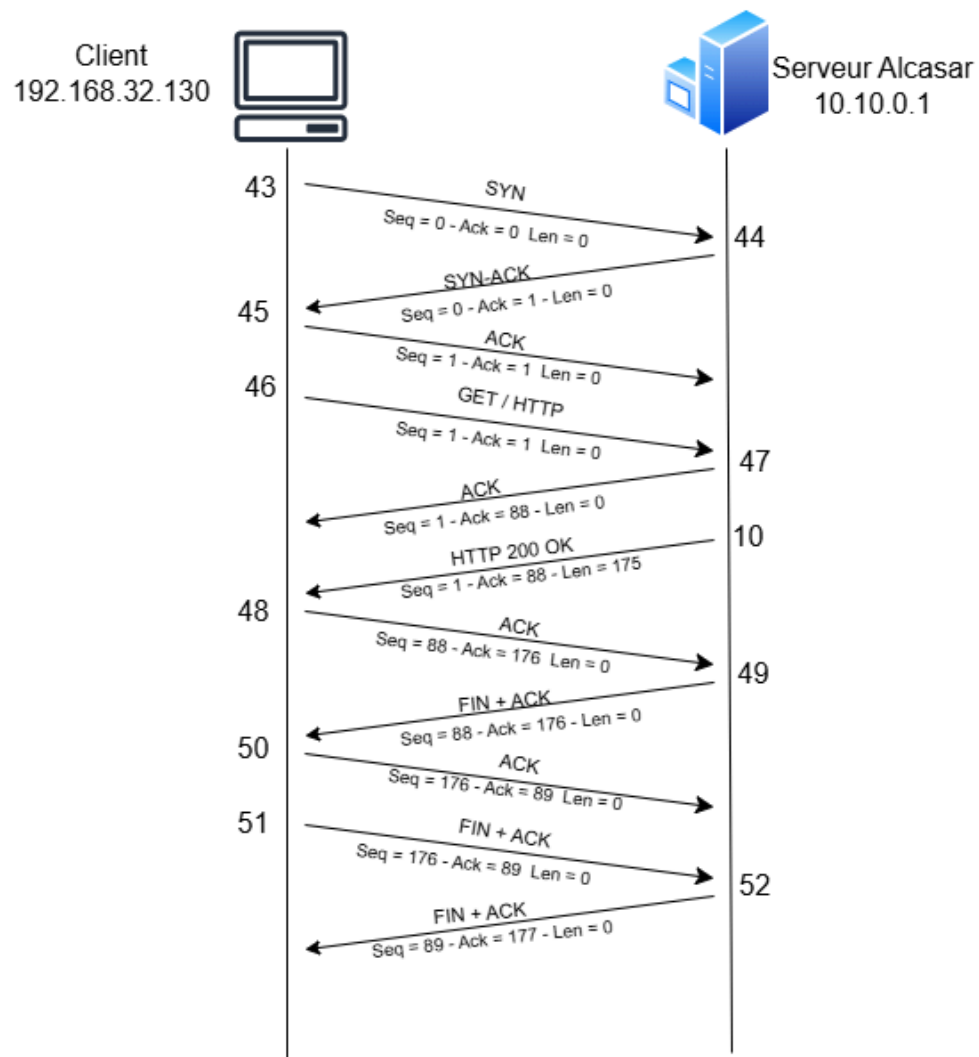
Pour installer Wireshark sur Debian on utilise les commandes suivantes :

- **sudo apt-get install wireshark**
- **sudo dpkg-reconfigure wireshark-common** (permet d'ajouter les privilèges utilisateurs)
- **sudo adduser \$USER wireshark** (ajoute l'utilisateur en super utilisateur)



```
aurelie@debian:~$ sudo apt install curl
[sudo] Mot de passe de aurelie :
Lecture des listes de paquets... Fait
Construction de l'arbre des dépendances... Fait
Lecture des informations d'état... Fait
Les NOUVEAUX paquets suivants seront installés :
  curl
0 mis à jour, 1 nouvellement installés, 0 à enlever et 0 non mis à jour.
Il est nécessaire de prendre 315 ko dans les archives.
Après cette opération, 501 ko d'espace disque supplémentaires seront utilisés.
Réception de :1 https://deb.debian.org/debian bookworm/main amd64 curl amd64 7.8
8.1-10+deb12u12 [315 kB]
315 ko réceptionnés en 0s (873 ko/s)
Sélection du paquet curl précédemment désélectionné.
(Lecture de la base de données... 155915 fichiers et répertoires déjà installés.
)
Préparation du dépaquetage de .../curl_7.88.1-10+deb12u12_amd64.deb ...
Dépaquetage de curl (7.88.1-10+deb12u12) ...
Paramétrage de curl (7.88.1-10+deb12u12) ...
Traitement des actions différées (« triggers ») pour man-db (2.11.2-2) ...
aurelie@debian:~$ curl alcasar.laplateforme.io
aurelie@debian:~$
```

On a installé curl avec la commande ci-dessus, ça nous a permis d'avoir accès au tcp de l'url Alcasar la plateforme.io



*ens33

Fichier Editer Vue Aller Capture Analyser Statistiques Telephonie Wireless Outils Aide

arp

No.	Time	Source	Destination	Protocol	Length	Info
3	5.232206485	VMware_eb:0c:ce	VMware_f9:6f:c7	ARP	42	who has 192.168.32.2
4	5.232568902	VMware_f9:6f:c7	VMware_eb:0c:ce	ARP	60	192.168.32.2
7	54.706555541	VMware_c0:00:08	VMware_ff:6b:31	ARP	60	who has 192.168.32.2
8	54.706556367	VMware_ff:6b:31	VMware_c0:00:08	ARP	60	192.168.32.2
12	69.487483980	VMware_eb:0c:ce	VMware_f9:6f:c7	ARP	42	who has 192.168.32.2
13	69.488128442	VMware_f9:6f:c7	VMware_eb:0c:ce	ARP	60	192.168.32.2
17	115.682553462	VMware_c0:00:08	VMware_ff:6b:31	ARP	60	who has 192.168.32.2
18	115.682554336	VMware_ff:6b:31	VMware_c0:00:08	ARP	60	192.168.32.2
34	138.177535422	VMware_c0:00:08	Broadcast	ARP	60	who has 192.168.32.2
35	138.177536161	VMware_c0:00:08	Broadcast	ARP	60	who has 192.168.32.2

Frame 3: 42 bytes on wire (336 bits), 42 bytes captured (336 bits) on interface 0
 Ethernet II, Src: VMware_eb:0c:ce (00:0c:29:00:00:00), Dst: VMware_f9:6f:c7 (08:00:06:04:00:01)
 Address Resolution Protocol (request)

Address Resolution Protocol: Protocol Paquets: 370 - Affichés: 148 (40.0%) Profil: Default

*ens33

Fichier Editer Vue Aller Capture Analyser Statistiques Telephonie Wireless Outils Aide

udp

No.	Time	Source	Destination	Protocol	Length	Info
267	844.510532130	192.168.32.130	192.168.32.2	DNS	86	Standard query type
270	844.651439891	192.168.32.2	192.168.32.130	DNS	127	Standard query response
271	844.653579924	192.168.32.130	192.168.32.2	DNS	81	Standard query type
272	844.653728963	192.168.32.130	192.168.32.2	DNS	81	Standard query type
273	844.664125576	192.168.32.2	192.168.32.130	DNS	145	Standard query response
274	844.664126186	192.168.32.2	192.168.32.130	DNS	193	Standard query response
339	861.939104960	192.168.32.130	192.168.32.2	DNS	83	Standard query type
340	861.939322571	192.168.32.130	192.168.32.2	DNS	83	Standard query type
341	861.953337457	192.168.32.2	192.168.32.130	DNS	99	Standard query response
342	861.953338197	192.168.32.2	192.168.32.130	DNS	83	Standard query type

Frame 342: 83 bytes on wire (664 bits), 83 bytes captured (664 bits) on interface 0
 Ethernet II, Src: VMware_f9:6f:c7 (08:00:06:04:00:01), Dst: 192.168.32.130 (08:00:06:04:00:01)
 Internet Protocol Version 4, Src: 192.168.32.130, Dst: 192.168.32.2
 User Datagram Protocol, Src Port: 53, Dst Port: 53
 Domain Name System (response)

User Datagram Protocol: Protocol Paquets: 370 - Affichés: 95 (25.7%) Profil: Default

*ens33

Fichier Editer Vue Aller Capture Analyser Statistiques Telephonie Wireless Outils Aide

ip.addr == 10.10.0.1

No.	Time	Source	Destination	Protocol	Length	Info
343	861.954631524	192.168.32.130	10.10.0.1	TCP	74	57810 → 80 [RST] Seq=19216832130 Win=0 Len=0
344	861.961377413	10.10.0.1	192.168.32.130	TCP	60	80 → 57810 [RST] Seq=19216832130 Win=0 Len=0
345	861.961462647	192.168.32.130	10.10.0.1	TCP	54	57810 → 80 [RST] Seq=19216832130 Win=0 Len=0
346	861.961794839	192.168.32.130	10.10.0.1	HTTP	141	GET / HTTP/1.1
347	861.962315215	10.10.0.1	192.168.32.130	TCP	60	80 → 57810 [RST] Seq=19216832130 Win=0 Len=0
348	861.989922511	10.10.0.1	192.168.32.130	HTTP	229	HTTP/1.1 301 Moved Permanently
349	861.989998381	192.168.32.130	10.10.0.1	TCP	54	57810 → 80 [RST] Seq=19216832130 Win=0 Len=0
350	861.990511571	192.168.32.130	10.10.0.1	TCP	54	57810 → 80 [RST] Seq=19216832130 Win=0 Len=0
351	861.991047932	10.10.0.1	192.168.32.130	TCP	60	80 → 57810 [RST] Seq=19216832130 Win=0 Len=0
352	861.997075704	10.10.0.1	192.168.32.130	TCP	60	80 → 57810 [RST] Seq=19216832130 Win=0 Len=0

Frame 343: 74 bytes on wire (592 bits), 74 bytes captured (592 bits) on interface 0
 Ethernet II, Src: VMware_eb:0c:ce (00:0c:29:00:00:00), Dst: 192.168.32.130 (08:00:06:04:00:01)
 Internet Protocol Version 4, Src: 192.168.32.130, Dst: 10.10.0.1
 Transmission Control Protocol, Src Port: 57810, Dst Port: 80, Seq=19216832130, Win=0, Len=0

wireshark_ens33EN2062.pcapng Paquets: 353 - Affichés: 11 (3.1%) Profil: Default

*ens33

Fichier Editer Vue Aller Capture Analyser Statistiques Telephonie Wireless Outils Aide

TCP

No.	Time	Source	Destination	Protocol	Length	Info
14	61.931632239	192.168.171.1	192.168.171.128	TCP	66	57211 → 22 [SYN] Seq=0 Win=65535 Len=0
15	61.931822576	192.168.171.128	192.168.171.1	TCP	66	22 → 57211 [SYN, ACK] Seq=0 Ack=1 Win=65535 Len=0
16	61.932017983	192.168.171.1	192.168.171.128	TCP	60	57211 → 22 [ACK] Seq=1 Ack=1 Win=65535 Len=0

tcp.port == 80					
No.	Time	Source	Destination	Protocol	Length Info
7	25.488734	192.168.32.1	192.168.32.130	TCP	54 59193 → 80 [FIN, ACK] Seq=1 Ack=1 Win=255 Len=0
8	25.489066	192.168.32.130	192.168.32.1	TCP	60 80 → 59193 [ACK] Seq=1 Ack=2 Win=501 Len=0
9	25.489333	192.168.32.1	192.168.32.130	TCP	66 59203 → 80 [SYN] Seq=0 Win=65535 Len=0 MSS=1460 WS=256 SACK_PERM
10	25.489557	192.168.32.130	192.168.32.1	TCP	66 80 → 59203 [SYN, ACK] Seq=0 Ack=1 Win=64240 Len=0 MSS=1460 SACK_PERM WS=128
11	25.489773	192.168.32.1	192.168.32.130	TCP	54 59203 → 80 [ACK] Seq=1 Ack=1 Win=65280 Len=0
12	25.490291	192.168.32.1	192.168.32.130	HTTP	189 GET / HTTP/1.1
13	25.491878	192.168.32.130	192.168.32.1	TCP	60 80 → 59203 [ACK] Seq=1 Ack=136 Win=64128 Len=0
14	25.492725	192.168.32.130	192.168.32.1	TCP	1514 80 → 59203 [ACK] Seq=1 Ack=136 Win=64128 Len=1460 [TCP PDU reassembled in 21]
15	25.492761	192.168.32.130	192.168.32.1	TCP	1514 80 → 59203 [ACK] Seq=1461 Ack=136 Win=64128 Len=1460 [TCP PDU reassembled in 21]
16	25.492777	192.168.32.130	192.168.32.1	TCP	1514 80 → 59203 [ACK] Seq=2921 Ack=136 Win=64128 Len=1460 [TCP PDU reassembled in 21]
17	25.492787	192.168.32.130	192.168.32.1	TCP	1514 80 → 59203 [ACK] Seq=4381 Ack=136 Win=64128 Len=1460 [TCP PDU reassembled in 21]
18	25.492792	192.168.32.130	192.168.32.1	TCP	1514 80 → 59203 [PSH, ACK] Seq=5841 Ack=136 Win=64128 Len=1460 [TCP PDU reassembled in 21]
19	25.492875	192.168.32.130	192.168.32.1	TCP	1514 80 → 59203 [ACK] Seq=7301 Ack=136 Win=64128 Len=1460 [TCP PDU reassembled in 21]
20	25.492883	192.168.32.130	192.168.32.1	TCP	1514 80 → 59203 [ACK] Seq=8761 Ack=136 Win=64128 Len=1460 [TCP PDU reassembled in 21]
21	25.492907	192.168.32.130	192.168.32.1	HTTP	790 HTTP/1.1 200 OK (text/html)

tcp.port == 21					
No.	Time	Source	Destination	Protocol	Length Info
4906	1693.1355122...	192.168.32.1	192.168.32.130	TCP	66 53181 → 21 [SYN] Seq=0 Win=65535 Len=0 MSS=1460
4907	1693.1355404...	192.168.32.130	192.168.32.1	TCP	66 21 → 53181 [SYN, ACK] Seq=0 Ack=1 Win=64240 Len=0
4908	1693.1357671...	192.168.32.1	192.168.32.130	TCP	60 53181 → 21 [ACK] Seq=1 Ack=1 Win=65280 Len=0
4913	1693.1517637...	192.168.32.130	192.168.32.1	FTP	107 Response: 220 ProFTPD Server (Debian) [::ffff:192.168.32.130]
4914	1693.1526486...	192.168.32.1	192.168.32.130	FTP	64 Request: AUTH TLS
4915	1693.1526664...	192.168.32.130	192.168.32.1	TCP	54 21 → 53181 [ACK] Seq=54 Ack=11 Win=64256 Len=0
4916	1693.1529354...	192.168.32.130	192.168.32.1	FTP	86 Response: 500 commande AUTH non comprise
4917	1693.1531375...	192.168.32.1	192.168.32.130	FTP	64 Request: AUTH SSL
4918	1693.1531957...	192.168.32.130	192.168.32.1	FTP	86 Response: 500 commande AUTH non comprise
4919	1693.2091988...	192.168.32.1	192.168.32.130	TCP	60 53181 → 21 [ACK] Seq=21 Ack=118 Win=65280 Len=0
4929	1698.7108493...	192.168.32.1	192.168.32.130	FTP	68 Request: USER testftp
4930	1698.7114046...	192.168.32.130	192.168.32.1	FTP	92 Response: 331 Mot de passe requis pour testftp
4931	1698.7117331...	192.168.32.1	192.168.32.130	FTP	65 Request: PASS 1234
4932	1698.7490201...	192.168.32.130	192.168.32.1	FTP	92 Response: 230 Utilisateur testftp authentifié
4933	1698.7494009...	192.168.32.1	192.168.32.130	FTP	60 Request: SYST
4934	1698.7495607...	192.168.32.130	192.168.32.1	FTP	73 Response: 215 UNIX Type: LB
4935	1698.7499026...	192.168.32.1	192.168.32.130	FTP	60 Request: FEAT

ssl					
No.	Time	Source	Destination	Protocol	Length Info
4554	1096.5653897...	194.177.211.216	192.168.32.130	TLSv1.3	377 Application Data
4555	1096.5655896...	192.168.32.130	194.177.211.216	TLSv1.3	89 Application Data
4557	1096.5660284...	192.168.32.130	194.177.211.216	TLSv1.3	185 Application Data
4559	1096.8273186...	194.177.211.216	192.168.32.130	TLSv1.3	377 Application Data
4560	1096.8275431...	192.168.32.130	194.177.211.216	TLSv1.3	89 Application Data
4563	1101.9465402...	194.177.211.216	192.168.32.130	TLSv1.3	117 Application Data, Application Data
4564	1101.9470379...	192.168.32.130	194.177.211.216	TLSv1.3	93 Application Data
4571	1102.8357752...	192.168.32.130	194.177.211.216	TLSv1.3	571 Client Hello
4573	1102.9239388...	194.177.211.216	192.168.32.130	TLSv1.3	4325 Server Hello, Change Cipher Spec, Application Data
4575	1102.9250822...	192.168.32.130	194.177.211.216	TLSv1.3	60 Change Cipher Spec
4577	1102.9285102...	192.168.32.130	194.177.211.216	TLSv1.3	128 Application Data
4579	1102.9288972...	192.168.32.130	194.177.211.216	TLSv1.3	100 Application Data
4581	1102.9290108...	192.168.32.130	194.177.211.216	TLSv1.3	103 Application Data
4583	1102.9292543...	192.168.32.130	194.177.211.216	TLSv1.3	89 Application Data
4585	1102.9296988...	192.168.32.130	194.177.211.216	TLSv1.3	218 Application Data
4587	1103.1769005...	194.177.211.216	192.168.32.130	TLSv1.3	791 Application Data, Application Data, Application Data
4588	1103.1770987...	192.168.32.130	194.177.211.216	TLSv1.3	85 Application Data

dhcp					
No.	Time	Source	Destination	Protocol	Length Info
294	567.011411154	192.168.32.130	192.168.32.254	DHCP	326 DHCP Request - Transaction ID 0xc1fa4fd3
295	567.012589984	192.168.32.254	192.168.32.130	DHCP	342 DHCP ACK - Transaction ID 0xc1fa4fd3
2715	764.012666396	192.168.32.1	192.168.32.254	DHCP	358 DHCP Request - Transaction ID 0xb6569254
2716	764.012713231	192.168.32.254	192.168.32.1	DHCP	342 DHCP ACK - Transaction ID 0xb6569254
4775	1467.0124366...	192.168.32.130	192.168.32.254	DHCP	326 DHCP Request - Transaction ID 0xeb3b10d6
4776	1467.0131763...	192.168.32.254	192.168.32.130	DHCP	342 DHCP ACK - Transaction ID 0xeb3b10d6
4858	1674.2788431...	192.168.32.1	192.168.32.254	DHCP	358 DHCP Request - Transaction ID 0xed4422df
4859	1674.2788436...	192.168.32.254	192.168.32.1	DHCP	342 DHCP ACK - Transaction ID 0xed4422df

dns					
No.	Time	Source	Destination	Protocol	Length Info
2677	762.753249694	170.247.170.2	192.168.32.130	DNS	70 Standard query response 0x439c Refused DNSKEY <R>
2678	762.753249991	192.112.36.4	192.168.32.130	DNS	70 Standard query response 0x113b Refused NS <Root>
2679	762.753859563	192.168.32.130	192.112.36.4	DNS	82 Standard query 0x29db DNSKEY <Root> OPT
2680	762.753931859	192.168.32.130	192.58.128.30	DNS	82 Standard query 0x03b5 NS <Root> OPT
2681	762.762070539	192.112.36.4	192.168.32.130	DNS	70 Standard query response 0x29db Refused DNSKEY <R>
2682	762.762070981	192.58.128.30	192.168.32.130	DNS	70 Standard query response 0x03b5 Refused NS <Root>
2683	762.762651842	192.168.32.130	192.58.128.30	DNS	82 Standard query 0x3d06 DNSKEY <Root> OPT
2684	762.762759019	192.168.32.130	192.36.148.17	DNS	82 Standard query 0x9e17 NS <Root> OPT
2685	762.777328367	192.58.128.30	192.168.32.130	DNS	70 Standard query response 0x3d06 Refused DNSKEY <R>
2686	762.777328620	192.36.148.17	192.168.32.130	DNS	70 Standard query response 0x9e17 Refused NS <Root>
2687	762.777895639	192.168.32.130	192.36.148.17	DNS	82 Standard query 0x0429 DNSKEY <Root> OPT
2688	762.777970343	192.168.32.130	192.203.230.10	DNS	82 Standard query 0xd357 NS <Root> OPT
2689	762.792179967	192.36.148.17	192.168.32.130	DNS	70 Standard query response 0x0429 Refused DNSKEY <R>
2690	762.792180254	192.203.230.10	192.168.32.130	DNS	70 Standard query response 0xd357 Refused NS <Root>
2691	762.792687882	192.168.32.130	192.203.230.10	DNS	82 Standard query 0x0235 DNSKEY <Root> OPT
2692	762.792770322	192.168.32.130	202.12.27.33	DNS	82 Standard query 0xc652 NS <Root> OPT
2693	762.802372231	192.203.230.10	192.168.32.130	DNS	70 Standard query response 0x0235 Refused DNSKEY <R>

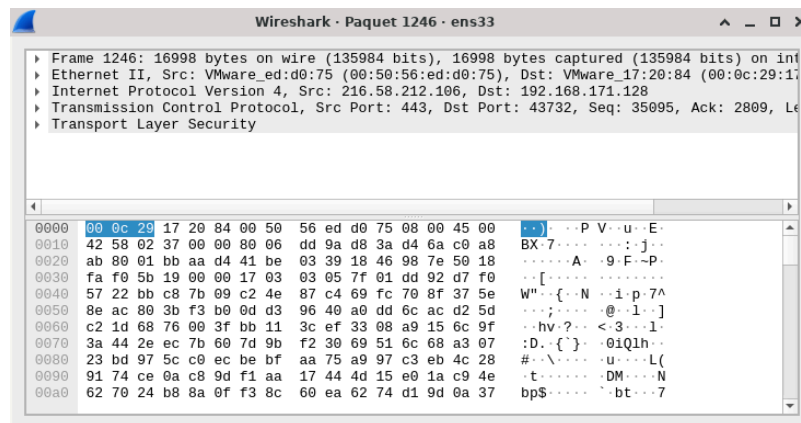
No.	Time	Source	Destination	Protocol	Length	Info
274	534.129903824	192.168.32.1	224.0.0.251	MDNS	93	Standard query 0x0000 ANY LAPTOP-SSB612HH._dosvc
275	534.131059583	fe80::caea:92cd:6f7...	ff02::fb	MDNS	113	Standard query 0x0000 ANY LAPTOP-SSB612HH._dosvc
276	534.392470069	192.168.32.1	224.0.0.251	MDNS	299	Standard query response 0x0000 PTR, cache flush
277	534.393290312	fe80::caea:92cd:6f7...	ff02::fb	MDNS	319	Standard query response 0x0000 PTR, cache flush
278	534.393980894	192.168.32.1	224.0.0.251	MDNS	235	Standard query response 0x0000 SRV, cache flush
279	534.395213400	fe80::caea:92cd:6f7...	ff02::fb	MDNS	255	Standard query response 0x0000 SRV, cache flush
520	654.401580019	192.168.32.1	224.0.0.251	MDNS	234	Standard query response 0x0000 PTR LAPTOP-SSB612
521	654.404665103	fe80::caea:92cd:6f7...	ff02::fb	MDNS	254	Standard query response 0x0000 PTR LAPTOP-SSB612
522	654.407262387	192.168.32.1	224.0.0.251	MDNS	93	Standard query 0x0000 ANY LAPTOP-SSB612HH._dosvc
523	654.408565255	fe80::caea:92cd:6f7...	ff02::fb	MDNS	113	Standard query 0x0000 ANY LAPTOP-SSB612HH._dosvc
524	654.660808927	192.168.32.1	224.0.0.251	MDNS	93	Standard query 0x0000 ANY LAPTOP-SSB612HH._dosvc
525	654.661912337	fe80::caea:92cd:6f7...	ff02::fb	MDNS	113	Standard query 0x0000 ANY LAPTOP-SSB612HH._dosvc
526	654.925661935	192.168.32.1	224.0.0.251	MDNS	93	Standard query 0x0000 ANY LAPTOP-SSB612HH._dosvc
527	654.928224209	fe80::caea:92cd:6f7...	ff02::fb	MDNS	113	Standard query 0x0000 ANY LAPTOP-SSB612HH._dosvc
528	655.184852546	192.168.32.1	224.0.0.251	MDNS	299	Standard query response 0x0000 PTR, cache flush
529	655.186029794	fe80::caea:92cd:6f7...	ff02::fb	MDNS	319	Standard query response 0x0000 PTR, cache flush
530	655.187218533	192.168.32.1	224.0.0.251	MDNS	235	Standard query response 0x0000 SRV, cache flush

No.	Time	Source	Destination	Protocol	Length	Info
2792	769.836456987	192.168.32.130	192.168.32.255	BROWSER	263	Host Announcement DEBIAN, workstation, Server, Print
2911	776.856217202	192.168.32.130	192.168.32.255	BROWSER	231	Browser Election Request
2942	778.859624845	192.168.32.130	192.168.32.255	BROWSER	231	Browser Election Request
2945	780.862417445	192.168.32.130	192.168.32.255	BROWSER	231	Browser Election Request
2948	782.865875707	192.168.32.130	192.168.32.255	BROWSER	231	Browser Election Request
2957	784.869064153	192.168.32.130	192.168.32.255	BROWSER	231	Browser Election Request
2971	792.891639922	192.168.32.130	192.168.32.255	BROWSER	219	Request Announcement
2972	792.891980515	192.168.32.130	192.168.32.255	BROWSER	263	Local Master Announcement DEBIAN, Workstation, Server,
2973	792.892179935	192.168.32.130	192.168.32.255	BROWSER	249	Domain/Workgroup Announcement WORKGROUP, NT Workstati
3021	923.021551418	192.168.32.130	192.168.32.255	BROWSER	263	Local Master Announcement DEBIAN, Workstation, Server,
3022	923.021929593	192.168.32.130	192.168.32.255	BROWSER	249	Domain/Workgroup Announcement WORKGROUP, NT Workstati
4594	1103.1871966...	192.168.32.130	192.168.32.255	BROWSER	263	Local Master Announcement DEBIAN, Workstation, Server,
4595	1103.1873435...	192.168.32.130	192.168.32.255	BROWSER	249	Domain/Workgroup Announcement WORKGROUP, NT Workstati
4743	1343.3964308...	192.168.32.130	192.168.32.255	BROWSER	263	Local Master Announcement DEBIAN, Workstation, Server,
4744	1343.3972634...	192.168.32.130	192.168.32.255	BROWSER	249	Domain/Workgroup Announcement WORKGROUP, NT Workstati
4855	1643.6836496...	192.168.32.130	192.168.32.255	BROWSER	263	Local Master Announcement DEBIAN, Workstation, Server,
4856	1643.6845929...	192.168.32.130	192.168.32.255	BROWSER	249	Domain/Workgroup Announcement WORKGROUP, NT Workstati

La différence entre FTP et TLS lors de la capture des paquets: On voit bien que le protocole FTP n'est pas sécurisé car il affiche quasi toute l'opération qui a été effectuée alors que pour le TLS, les informations sont scriptées.

Wireshark · Paquet 1110 · ens33		
▶ Frame 1110: 102 bytes on wire (816 bits), 102 bytes captured (816 bits) on interface ens3 ▶ Ethernet II, Src: VMware_17:20:84 (00:0c:29:17:20:84), Dst: VMware_c0:00:08 (00:50:56:c0:00:08) ▶ Internet Protocol Version 4, Src: 192.168.171.128, Dst: 192.168.171.1 ▶ Transmission Control Protocol, Src Port: 21, Dst Port: 58390, Seq: 599, Ack: 94, Len: 46 ▶ File Transfer Protocol (FTP) [Current working directory: /home/ftppuser]		
0000	00 50 56 c0 00 08 00 29 17 20 84 08 00 45 00	.PV....). ...E-
0010	00 58 96 94 00 00 40 06 cc 38 c0 a8 ab 80 c0 a8	.X..@.@.8.....
0020	ab 01 00 15 e4 16 b6 ee 62 ad 59 b4 f3 b3 50 18b.Y...P-
0030	01 f6 d8 1d 00 00 32 35 37 20 22 2f 68 6f 6d 6525 7 "/home
0040	2f 66 74 70 75 73 65 72 22 20 65 73 74 20 6c 65	/ftppuser " est le
0050	20 72 c3 a9 70 65 72 74 6f 69 72 65 20 63 6f 75	r·pert oire cou
0060	72 61 6e 74 0d 0a	rant·

No.: 1110 · Time: 203.235895926 · Source: 192.168.171.128 · Destination: 192.168.171.1 · Info: 257 "/home/ftppuser" est le répertoire courant



Pour la partie *tshark*, on doit d'abord l'installer avec la commande :

```
sudo apt install tshark
```

Ensuite nous pouvons depuis le terminal prendre une capture de paquets :

```
sudo tshark -i ens33 -f "port 21" -w ftp_capture.pcapng
```

```
aurelie@debian:~$ su -
Mot de passe :
root@debian:~# sudo tshark -i ens33 -f "port 21" -w ftp_capture.pcapng
Running as user "root" and group "root". This could be dangerous.
Capturing on 'ens33'
** (tshark:2803) 09:24:54.544657 [Main MESSAGE] -- Capture started.
** (tshark:2803) 09:24:54.544994 [Main MESSAGE] -- File: "ftp_capture.pcapng"
^C
tshark:
root@debian:~# ^C
root@debian:~# ^C
root@debian:~# sudo tshark -i ens33 -f "udp port 53" -w dns_capture.pcapng
Running as user "root" and group "root". This could be dangerous.
Capturing on 'ens33'
** (tshark:2890) 09:34:45.047753 [Main MESSAGE] -- Capture started.
** (tshark:2890) 09:34:45.047849 [Main MESSAGE] -- File: "dns_capture.pcapng"
```

Comme la capture s'enregistre dans le mode *root* pour la déplacer dans un fichier du bureau on utilise la commande :

```
sudo mv /root/ftp_capture.pcapng /home/aurelie/
```

Une fois déplacé on ne pourra pas l'ouvrir, donc on devra autoriser l'accès à l'utilisateur avec la commande suivante :

```
sudo chown aurelie:aurelie /home/aurelie/ftp_capture.pcapng
```

Pour sélectionner un certain nombre de ligne pour la capture, on peut utilise l'option **-c**

```
leonce@debian:~$ tshark -f "icmp" -c 10
Capturing on 'ens33'
** (tshark:12402) 00:02:55.963490 [Main MESSAGE] -- Capture started.
** (tshark:12402) 00:02:55.964608 [Main MESSAGE] -- File: "/tmp/wireshark_ens33
T9EP62.pcapng"
  1 0.000000000 192.168.171.128 → 192.168.171.1 ICMP 98 Echo (ping) request
id=0x308f, seq=1/256, ttl=64
  2 0.000358178 192.168.171.1 → 192.168.171.128 ICMP 98 Echo (ping) reply
id=0x308f, seq=1/256, ttl=128 (request in 1)
  3 1.005876561 192.168.171.128 → 192.168.171.1 ICMP 98 Echo (ping) request
id=0x308f, seq=2/512, ttl=64
  4 1.006567658 192.168.171.1 → 192.168.171.128 ICMP 98 Echo (ping) reply
id=0x308f, seq=2/512, ttl=128 (request in 3)
  5 9.477318247 192.168.171.128 → 192.168.171.1 ICMP 98 Echo (ping) request
id=0x3090, seq=1/256, ttl=64
  6 9.477723137 192.168.171.1 → 192.168.171.128 ICMP 98 Echo (ping) reply
id=0x3090, seq=1/256, ttl=128 (request in 5)
  7 10.479007306 192.168.171.128 → 192.168.171.1 ICMP 98 Echo (ping) request
id=0x3090, seq=2/512, ttl=64
  8 10.479582862 192.168.171.1 → 192.168.171.128 ICMP 98 Echo (ping) reply
id=0x3090, seq=2/512, ttl=128 (request in 7)
  9 11.480469398 192.168.171.128 → 192.168.171.1 ICMP 98 Echo (ping) request
id=0x3090, seq=3/768, ttl=64
 10 11.481049704 192.168.171.1 → 192.168.171.128 ICMP 98 Echo (ping) reply
id=0x3090, seq=3/768, ttl=128 (request in 9)
tshark:
10 packets captured
```