



DECOUVERTE ET UTILISATION DE WIRESHARK

I) Wireshark

Depuis le menu Demarrer, lancer l'appliaction Wireshark. Vous devriez voir apparaître une fenêtre similaire à celle-ci :



Dans le menu capture, sélectionner le sous-menu Interfaces et lancer une capture de trame. sur la carte réseau portant votre adresse IP et appuyer sur Start

🕅 Wireshark: Capture Interfaces				- D ×
Description	IP	Packets	Packets/s	Stop
Broadcom NetXtreme Gigabit Ethernet Driver (Microsoft's Packet Scheduler)	139.124.38.128			Start Options Details
👰 Carte Mini rggs. local sans fil Wireless 1505 Dell 802.11n (projet) (Microsoft's Packet Scheduler)	unknown			Start Immediately start a capture from this interface:
TAP-Win32 Adapter V9 (Microsoft's Packet Scheduler)	unknown			Start Device: \Device\NPF_{952FC1E2-3516-4C95-AC64- A1E728F7AE60}
				Description: Broadcom NetXtreme Gigabit Ethernet Driver (Microsoft's Packet Scheduler) IP: 139.124.38.128

Une fois la capture lancée, ouvrez une fenetre de commande DOS (menu Demarrer -> Exécuter -> cmd), et lancer un ping sur <u>www.google.fr</u>. Quand le ping s'arrête, arrêter la capture en cliquant sur l'icône adéquate (voir image ci-dessous).



Résultat d'une capture

Une fois la capture effectuée, vous obtiendrez la fenêtre suivante :

VY Broadcom NetXtreme	e Gigabit Ethernet Driver (Mic	rosoft's Packet Scheduler) : (apturing - Wire	shark			- B ×
<u>File E</u> dit <u>V</u> iew <u>Go</u> <u>C</u> apt	ture <u>A</u> nalyze <u>S</u> tatistics <u>H</u> elp						
	⊨ 8 × 2 ≜ ९	🗢 🔶 😜 ዥ 👱 🗏		0, 🖭 🌉 🛙	1 💀 💥 🕱	1	
Eilter:		 Expression 	<u>C</u> lear <u>A</u> pply				
No Time	Source	Destination	Protocol Info				<u> </u>
31 15.054620 32 13.097493 33 14.055834 34 14.055834 35 15.056566 36 15.100220 37 16.057568 38 16.099907 39 17.058548 40 17.100895 41 18.059451 42 18.102667 43 19.059628 44 19.101778	192.168.0.13 209.85,229.103 192.168.0.13 209.85,229.103 192.168.0.13 209.85,229.103 192.168.0.13 209.85,229.103 192.168.0.13 209.85,229.103 192.168.0.13 209.85,229.103 192.168.0.13 209.85,229.103	209, 85, 229, 103 192, 168, 0, 13 209, 85, 229, 103 192, 168, 0, 13 201, 85, 229, 103 202, 85, 229, 103 202, 85, 229, 103 203, 85, 229, 103 204, 85, 229, 103 204, 85, 229, 103 205, 85, 205, 105 205, 85, 205 205, 85, 85, 85, 85, 85, 85, 85, 85, 85, 8	ICMP Echi ICMP Echi	 (ping) reque (ping) reply (ping) reque 	st st st st st st	1	-
	es on wire, 74 bytes ca	ptured)	Doll bdib6.7	F (00.21.70.b	1.66.75)		-
Internet Protocol Internet Protocol	, src: 209.85.229.103	(209.85.229.103), Dst:	192.168.0.13	(192.168.0.13	3)		
🗈 Internet Control	Message Protocol						
						2	
0000 00 21 70 bd bd 0010 00 3C eb cd 0 0020 00 0d 00 2 0 0 0 2 0030 67 68 69 6a 61 0 040 77 61 62 63 64	6 75 00 07 cb b6 b9 7 0 00 35 01 22 81 d1 5 6 5c 02 00 2d 00 61 6; b 6c 6d 6e 6f 70 71 7; 4 65 66 67 68 69	5 08 00 45 00 .!pu. 5 e5 67 c0 a8 .<5 2 63 64 65 66&\. 2 73 74 75 76 ghijkim wabcdef	uE. "U.g . –.abcdef in opgrstuv g hi			3	

L'affichage des résultats se décompose en trois parties :

- 1) la liste des paquets capturés disponibles en dessous de la barre de menu avec un affichage synthétique du contenu de chaque paquet.
- 2) la décomposition exacte du paquet actuellement sélectionné dans la liste. Cette décomposition permet de visualiser les champs des entêtes des protocoles ainsi que l'imbrication des différentes couches de protocoles connus.
- 3) La troisième zone contient la capture affichée en hexadécimal et en ASCII.

Chaque ligne de la liste des paquets (premier volet) correspond à une PDU de données capturées. Si vous sélectionnez une ligne dans ce volet, ses détails s'affichent dans les volets du milieu et inférieur.

Le volet du milieu affiche les détails de ce paquet. Les protocoles et les champs de protocole du paquet sélectionné sont indiqués. Ils s'affichent sous la forme d'une arborescence que vous pouvez développer ou réduire.

II) Analyse de la capture du ping

Observez la liste des paquets capturés et réponder aux questions suivantes :

- a) Avez-vous capturé un échange avec le DNS ? Pourquoi votre ordinateur a t-il interrogé le DNS ?
- b) Quels sont les deux types de messages "ping" que vous avez capturés ?

Dans la première fenêtre, sélectionner une trame contenant une requête écho (echo ping request). Le volet du milieu affiche des informations détaillées sur le paquet semblables à cellesci :

```
    Frame 3 (74 bytes on wire, 74 bytes captured)
    Ethernet II, Src: Dell_bd:b6:75 (00:21:70:bd:b6:75), Dst: Freeboxs_b6:b9:75 (00:07:cb:b6:b9:75)
    Internet Protocol, Src: 192.168.0.13 (192.168.0.13), Dst: 209.85.229.103 (209.85.229.103)
    Internet Control Message Protocol
```

Cliquez sur les quatre signes « + » pour développer les arborescences correspondantes.



Comme vous pourrez le constater, il est possible de développer encore chaque section et protocole. Consacrez un peu de temps à l'étude de ces informations même si vous ne comprenez pas encore toutes les informations affichées.

a) Localisez deux types d'adresses « Source » et « Destination » différents. A quelles couches ces adresses appartiennent-elles ? b) Parmi les encapsulations suivantes, laquelle correspond à ce que vous voyez dans la capture ? [message ICMP [paquet IP[trame ethernet]]] [paquet IP [trame ethernet [message ICMP]]] [trame ethernet [paquet IP[message ICMP]]] [message ICMP [trame ethernet [paquet IP]]] c) A quelle couche du modèle OSI se situent les protocoles ICMP, IP et Ethernet ?

Sélectionnez maintenant une trame contenant la réponse à votre requête DNS.

- a) Quel est le nom complet du protocole DNS ?
- b) Quel protocole de la couche transport est utilisé par le DNS ?
- c) Ecrire l'encapsulation utilisée pour transporter une requête DNS

III) Analyse d'un trafic ftp

Lancez une capture de trames. Depuis la Console, lancez la commande ftp dl.free.fr (le username est essai@free.fr, et le password est celui que vous voulez). Une fois connecté sur le serveur, tapez la commande quit et arrêtez alors la capture.

Nous allons maintenant utilisez un filtre d'affichage pour n'afficher que les trames relatives au protocole ftp. Pour cela, dans le champ Filter, vous allez saisir ftp puis cliquez sur Apply.

Eile	Edit	⊻iev	v <u>G</u>	<u>o</u> <u>c</u>	apture	<u>A</u> nal	yze	<u>S</u> tatis	tics	Teleph	ony	<u>T</u> ools	<u>H</u> el	P										
	i	0(e í)			×	Z	≞	Q	4	\$		Ŧ	₽		-	Ð	Q	11	++	M	¥	1
Filter	: ftp	I												•	Expres	sion	Clea <u>r</u>	App	У					
No.		Tim	,						5	ource					Dest	ination	1		Appl	y this	filter st	ring to	the di	splay

En observant la première trame du protocole ftp, et en détaillant les PDU dans la deuxième fenêtre, répondez aux questions suivantes :

a) Dans le PDU de la couche réseau, quelle est la valeur du champ Time to Live ? Chercher sur internet à quoi ce champ peut-il servir ?
b) Dans le PDU de la couche réseau, quelle est la valeur du champ Protocol? Chercher sur internet à quoi ce champ peut-il servir ?
c) Quel est le protocole de la couche transport utilisé par ftp ?
d) Existe-t-il dans le PDU de la couche transport, un champ contenant le numéro du segment ?
e) Existe-t-il dans le PDU de la couche transport, un champ nommé Flag ? Quelles sont les valeurs possibles de ce champ ?
f) Examinez la totalité de la capture, en portant votre attention sur l'affichage en ASCII, et retrouver le mot de passe saisi¹.
g) Quel équipement d'infrastructure vous permettrez de capturer, à partir de votre machine, un mot de passe saisi par l'un de vos voisins ? Justifiez.

¹ Si jamais vous n'y arrivez pas, sélectionnez n'importe quelle trame ftp, puis dans le menu Analyse, lancez la commande Follow TCP Stream. Magique non !!!!

IV) Analyse d'un trafic facebook

Lancez une capture de trames. Ouvrez alors un navigateur et connectez vous à votre compte facebook (Attention, il ne s'agit pas d'y passer des heures !!!). Une fois que vous êtes connecté, arrêtez la capture de trame et répondez aux questions suivantes :

- a) Existe t-il dans la capture une trame dont le protocole est TLSv1 ?
- b) En observant cette trame déterminer ?- l'adresse IP du serveur hébergeant facebook ?
 - le protocole de couche réseau utilisé ?
 - le protocole de couche transport utilisé ?
 - le protocole de la couche application utilisé ?
- c) En interrogeant le DNS, vérifiez que l'adresse IP trouvée à la question précédente correspond bien au serveur de facebook ?
- d) Donnez le développé des acronymes SSL et TLS ?
- e) Retrouve t-on, comme dans l'exercice précédent, le mot de passe en clair dans l'échange ? Pourquoi ?

V) Analyse d'un trafic DNS

Lancez une capture de trames. Depuis la Console, lancez la commande nslookup 66.220.153.11. Une fois la réponse obtenue, arrêtez la capture, tapez dans le champ Filter le protocole dns (n'oubliez pas de faire Apply) et répondez aux questions suivantes :

a)	Quelle est l'adresse IP du DNS ?						
b)	Quel est le protocole de la couche transport utilisé par le DNS ?						
c)) Quels sont les deux types de trames possible pour le protocole DNS ?						
d)	Sur la première trame détern	niner la valeur des champs :					
	- @IP Src	@IP Dst					
	- Src Port	Dst Port					
e)) Sur la deuxième trame, déterminer la valeur des champs :						
	- @IP Src	@IP Dst					
	- Src Port	Dst Port					
	Que constatez vous ?						