### Sommaire

Introduction	3
Objectifs	3
Contexte	3
tcpdump	3
Wireshark	3
Installation	4
Prise en main	5
Mode simple utilisateur	5
Filtrage	6
Encapsulation	9
Outils statistiques	11
Analyse de trames	12
Adressage des protocoles dans le modèle Dod	12
Étude des statistiques	14
Capture de trames	15
Mode super utilisateur	15
Manipulations	17

#### © Copyright 2010 tv <thierry.vaira@orange.fr>

Permission is granted to copy, distribute and/or modify this document under the terms of the GNU Free Documentation License,

Version 1.1 or any later version published by the Free Software Foundation; with no Invariant Sections, with no Front-Cover Texts, and with no Back-Cover.

You can obtain a copy of the GNU General Public License : write to the Free Software Foundation, Inc., 59 Temple Place, Suite 330, Boston, MA 02111-1307 USA

## INTRODUCTION

#### Objectifs

Être capable d'utiliser un analyseur de protocoles.

Découvrir les caractéristiques générales et l'encapsulation des protocoles du modèle "TCP/IP"

#### Contexte

Un ordinateur équipé d'une carte de communication Ethernet fonctionnant sous Windows ou Linux sur lequel est installé un logiciel d'analyse de trames.

On utilisera dans les manipulations **tcpdump** (sous Linux) et **Wireshark** (sous Windows ou Linux).

#### tcpdump

tcpdump est un « *packet sniffer* » en ligne de commande. Il permet d'obtenir le détail du trafic visible depuis une interface réseau. C'est un outil de mise au point apprécié pour sa puissance.

Site officiel : http://www.tcpdump.org/

[Source : http://fr.wikipedia.org/wiki/Tcpdump]

#### Wireshark

Wireshark (anciennement Ethereal) est un logiciel libre d'analyse de protocole, ou « *packet sniffer* », utilisé dans le dépannage et l'analyse de réseaux informatiques, le développement de protocoles, l'éducation et la rétroingénierie, mais aussi le piratage. Wireshark est multi-plates-formes, il fonctionne sous Windows, Mac OS X, Linux, Solaris, ainsi que sous FreeBSD. Wireshark reconnait 759 protocoles.

Site officiel : <u>http://www.wireshark.org/</u>

Documentation : http://www.wireshark.org/docs/wsug\_html\_chunked/index.html

[Source : http://fr.wikipedia.org/wiki/Wireshark]

## INSTALLATION

Vérifier si le logiciel <u>Wireshark</u> est installé sur votre poste.

• Sous Linux (Mandriva 2010) :



```
Ou en mode console :

$ wireshark -help

Wireshark 1.2.10

Interactively dump and analyze network traffic.

See http://www.wireshark.org for more information.
```

Sinon installation (sous le compte root) à partir de la console :

# urpmi wireshark

Remarque : sous Linux, wireshark propose deux modes d'exploitation : le mode simple utilisateur et le mode super utilisateur (root). La différence essentielle entre les deux modes se situe au niveau de la capture de trames à partir des interfaces réseaux permises seulement en mode super utilisateur. Le mode simple utilisateur servira surtout pour l'analyse de trames déjà capturées.

• Sous Ubuntu :

#### Installation (sous le compte root) à partir de la console :

# apt-get install wireshark

• Sous Windows : l'installation se fait à partir d'une version adaptée à son système téléchargée à partir du site http://www.wireshark.org/download.html

## PRISE EN MAIN

## Mode simple utilisateur

Le logiciel s'ouvre sur cette page de menu :

	The Wireshark Network Analyzer	– a ×
File Edit View Go Capture Analyze Statistics Telephony	r Tools Help	
🔜 💐 😫 🕍 🖿 🗷 X C 🖬 🔍 🤄 📎	🗞 a 🗵 🖪 🖪 🗖 🗖 🗹 🖽 📓	¥20 (C)
Filter:	🗧 🖶 Expression 🤞 Clear 🛷 Apply	
WIRE <b>SHARK</b> The World's Most Po	pular Network Protocol Analyzer	
Capture	Files	Online
Interface List Live list of the capture interfaces (counts incoming packets) Start capture on interface:	Open Open a previously captured file Open Recent:	Website Visit the project's website User's Guide
🕮 Capture Options	🗛 Sample Captures	The User's Guide (local version, if installed)
Start a capture with detailed options	A rich assortment of example capture files on the wiki	Security Work with Wireshark as securely as possible
Capture Help		
How to Capture Step by step to a successful capture setup		
Specific information for capturing on: Ethernet, WLAN,		
<ul> <li>Ready to load or capture</li> <li>No Packets</li> </ul>		Profile: Default

On peut vérifier qu'en cliquant sur « Interface List » que l'on possède aucun droit d'accès sur les interfaces réseaux disponibles pour une capture :



Remarque : il faudra donc passer en mode super utilisateur (root) pour réaliser des captures sur ses interfaces réseaux.

Donc, on utilisera essentiellement le menu « **Open** » qui permettra de charger un fichier de capture pour analyse.

Ouvrir le fichier http.cap disponible sur le serveur ou sur le site <u>http://wiki.wireshark.org/SampleCaptures</u> (HTTP).

L'affichage se décompose en trois cadres :

1	http.cap - Wireshark — 🗁 🗙							
File Ed	File Edit View Go Capture Analyze Statistics Telephony Tools Help							
	li 🔐 🐏 🐏 💶 🚾 🗙 C 🖅 🔍 🗇 🤣 🛣 🖄 🗐 🔲 💷 😐 🗉 📅 🕍 🔀 🍽 🐻							
			Cadre 1 : trames ca	apturées (capture en temp	ps réel possi	ble)		
No	Time		Source	Destination	Protocol	Info	A	
	1 0.000000		145.254.160.237	65.208.228.223	ТСР	tip2 > http [SYN	] Seq=0 Win=8760 Len=0	
	2 0.911310		65.208.228.223	145.254.160.237	ТСР	http > tip2 [SYN	I, ACK] Seq=0 Ack=1 Win=	
	3 0.911310		145.254.160.237	65.208.228.223	ТСР	tip2 > http [AC	<pre>K] Seq=1 Ack=1 Win=9660</pre>	
	4 0.911310		145.254.160.237	65.208.228.223	HTTP	GET /download.ht	tml HTTP/1.1	
	5 1.472116		65.208.228.223	145.254.160.237	ТСР	http > tip2 [AC	<pre>{] Seq=1 Ack=480 Win=643</pre>	
	6 1.682419		65.208.228.223	145.254.160.237	TCP	[TCP segment of	a reassembled PDU]	
	7 1.812606		145.254.160.237	65.208.228.223	TCP	tip2 > http [ACH	<pre>{] Seq=480 Ack=1381 Win=</pre>	
	8 1.812606		65.208.228.223	145.254.160.237	TCP	[TCP segment of	a reassembled PDU]	
	9 2.012894		145.254.160.237	65.208.228.223	TCP	tip2 > http [ACH	<pre>{] Seq=480 Ack=2761 Win=</pre>	
1	0 2.443513		65.208.228.223	145.254.160.237	TCP	[TCP segment of	a reassembled PDU]	
1	1 2.553672		65.208.228.223	145.254.160.237	ТСР	[TCP segment of	a reassembled PDU] 🚽	
٩								
▶ Frame	e 1 (62 byte	s on wire, 62	bytes captured)					
▶ Ethe	rnet II, Src	: Xerox 00:00:	00 (00:00:01:00:00:0	0), Dst: fe:ff:20:00:01	L:00 (fe:ff:	20:00:01:00)		
▶ Inte	rnet Protoco	L. Src: 145.25	4,160,237 (145,254,1	60.237), Dst: 65.208.22	28,223 (65,2	208,228,223)		
Trans	smission Con	trol Protocol,	Src Port: tip2 (337	2), Dst Port: http (80)	), Sea: 0, L	en: 0		
			. 10 100 1	1 2 1 1 2	a	1 1 1 4		
		Cadre 2 : col	ntenu decode (couche	par couche) de la trame	selectionnee	e dans le cadre 1		
0000	fe ff 20 00	91 00 00 00 0	1 00 00 00 08 00 45	00E.				
0010 (	00 30 Of 41	40 00 80 06 9	1 eb 91 fe a0 ed 41	d0 .0.A@A.				
0020	e4 df 0d 2c	005038af f	e 13 00 00 00 00 70	02,.P8p.				
0030 2	22 38 c3 0c	00 00 02 04 0	5 b4 01 01 04 02	"8				
	Cadre 3 : "dump" en hexadécimale du protocole sélectionné dans le cadre 2							
🔾 File: "/	/home/tv/Télécha	rgement• Packet	ts: 43 Displayed: 43 Marked	d: O			• Profile: Default	

## Filtrage

Il est possible (indispensable !) de créer des filtres d'affichage qui ne montrent que les trames conformes à la règle de filtrage. Cela permettra d'isoler un échange en particulier ou l'analyse d'un protocole spécifique.

On renseignera alors le cadre Filter dans la barre du haut du cadre 1 :

	🗹 Filter:		🖶 Expression	od Clear	n Apply
--	-----------	--	--------------	----------	---------

Le bouton « **Expression** » permet d'accéder à un assistant pour créer une règle de filtrage. Une règle de filtrage s'appuie sur les champs des en-têtes (*header*) des protocoles connus du logiciel Wireshark :



En cliquant sur « Valider » puis sur « Apply », on obtient alors :

Filter: ip.ds	st == 145.254.160.237	:	₹ 🕂 Express	ion 🦪 (	Clear	n Apply
No Tim	e	Source		Destinatio	n	
2 0.9	911310	65.208.228.	223	145.254	. 160	.237
5 1.4	472116	65.208.228.	223	145.254	. 160	.237
6 1.6	582419	65.208.228.	223	145.254	. 160	.237
8 1.8	312606	65.208.228.	223	145.254	. 160	.237
10 2.4	443513	65.208.228.	223	145.254	. 160	.237
11 2.5	553672	65.208.228.	223	145.254	. 160	. 237
14 2.6	633787	65.208.228.	223	145.254	. 160	.237
16 2.8	394161	65.208.228.	223	145.254	. 160	.237
17 2.9	914190	145.253.2.2	203	145.254	. 160	. 237
20 3 3	374852	65.208.228.	223	145.254	. 160	.237
21 3.4	495025	65.208.228.	223	145.254	. 160	.237

On peut créer des règles de filtrage en combinant plusieurs expressions avec des opérateurs && (ET), || (OU) et ! (INVERSEUR), par exemple :

Toutes les trames dont l'adresse ip destination est égale à 145.254.160.237 et dont le port source ou destination n'est pas 80:

ip.dst == 145.254.160.237 && !tcp.port == 80

Remarque : en tapant directement dans la zone de saisie « **Filter** », Wireshark propose une complétion bien pratique.



On sélectionne la trame n°4 dans le cadre 1. Cette trame encapsule les protocoles visibles dans le cadre 2:

No	Time	Source	Destination	Protocol Info
	4 0.911310	145.254.160.237	65.208.228.223	HTTP GET /download.html HTTP/1.1
•			* * *	•
▶ ⊢ra	ame 4 (533 bytes on wire, 533	bytes captured)		
• Eth	nernet II, Src: Xerox_00:00:00	(00:00:01:00:00:00),	Dst: fe:ff:20:00:01:00	0 (fe:ff:20:00:01:00)
- D	estination: fe:ff:20:00:01:00	(fe:ff:20:00:01:00)		
	Address: fe:ff:20:00:01:00 (1	fe:ff:20:00:01:00)		
		. = IG bit: Individual	address (unicast)	
	1	. = LG bit: Locally ad	ministered address (th	is is NOT the factory default)
▶ S	ource: Xerox_00:00:00 (00:00:	01:00:00:00)		
T	ype: IP (0x0800)			
Int	ternet Protocol, Src: 145.254.	160.237 (145.254.160.3	237), Dst: 65.208.228.2	223 (65.208.228.223)
▶ Tra	ansmission Control Protocol, S	orc Port: tip2 (3372),	Dst Port: http (80), S	Seg: 1, Ack: 1, Len: 479
▶ Нур	pertext Transfer Protocol		• • • •	• • •
0000		00 00 00 08 00 45 00		
0010	02 07 0f 45 40 00 80 06 90	10 91 fe a0 ed 41 d0	E.	
0020	e4 df 0d 2c 00 50 38 af fe	14 11 4c 61 8c 50 18	P8La.P.	
0030	25 bc a9 58 00 00 47 45 54	20 2f 64 6f 77 6e 6c	%XGE T /downl	
0040	6f 61 64 2e 68 74 6d 6c 20	48 54 54 50 2f 31 2e	oad.html HTTP/1.	
0050	31 0d 0a 48 6f 73 74 3a 20	77 77 77 2e 65 74 68	1Host: www.eth	
0060	65 72 65 61 6c 2e 63 6f 6d	0d 0a 55 73 65 72 2d	ereal.co mUser-	
0070	41 67 65 6e 74 3a 20 4d 6f	7a 69 6c 6c 61 2f 35	Agent: M ozilla/5	
0080	2e 30 20 28 57 69 6e 64 6f	77 73 3b 20 55 3b 20	.0 (Wind ows; U;	
0090	57 69 6e 64 6f 77 73 20 4e	54 20 35 2e 31 3b 20	Windows NT 5.1;	
00a0	65 6e 2d 55 53 3b 20 72 76	3a 31 2e 36 29 20 47	en-US; r v:1.6) G	
00b0	65 63 6b 6f 2f 32 30 30 34	30 31 31 33 0d 0a 41	ecko/200 40113.A	
00c0	63 63 65 70 74 3a 20 74 65	78 74 2f 78 6d 6c 2c	ccept: t ext/xml,	
00d0	61 70 70 6c 69 63 61 74 69	6f 6e 2f 78 6d 6c 2c	applicat ion/xml,	
00e0	61 70 70 6c 69 63 61 74 69	6f 6e 2f 78 68 74 6d	applicat ion/xhtm	
00f0	6c 2b 78 6d 6c 2c 74 65 78	74 2f 68 74 6d 6c 3b	l+xml,te xt/html;	
0100	71 3d 30 2e 39 2c 74 65 78	74 2f 70 6c 61 69 6e	q=0.9,te xt/plain	
0110	3b 71 3d 30 2e 38 2c 69 6d	61 67 65 2f 70 6e 67	;q=0.8,i mage/png	
0120	2c 69 6d 61 67 65 2f 6a 70	65 6/ 2c 69 6d 61 6/	,image/j peg,imag	
0130	65 21 6/ 69 66 3b /1 3d 30	2e 32 2c 2a 2t 2a 3b	e/git;q= 0.2,*/*;	
0140	/1 30 30 2e 31 0d 0a 41 63	63 65 70 74 20 4c 61	q=⊍.1A ccept-La	
0160	oe o/ /5 ol o/ o5 3a 20 65	be 20 /5 /3 20 05 be	nguage: en-us,en	
0170			;q=0.5., Accept-E	
0110	0e 05 01 04 09 0e 07 3a 20	07 7a 09 70 20 04 05	ncourng: gzip,de	

Wireshark est capable de décoder les champs des différents en-tête de protocoles présents dans la trame capturée.

Remarque : mais sans connaissances théoriques, l'utilisation de wireshark s'avère très vite limitée ! C'est un outil de spécialiste. En effet, qu'est-ce qu'une « address unicast » ? « Seq » ? etc ...

### Encapsulation

Le cadre 2 illustre le principe de l'encapsulation des protocoles utilisées dans l'échange d'une trame. On fait souvent référence à un modèle pour représenter cette communication. Ici, le modèle est celui qui implémente les protocoles de la famille « TCP/IP » appelée aussi DoD (*Department of Defense*) :

Couche application HTTP	
Couche transport TCP	
Couche réseau IP	
Couche interface Ethernet_II	
Modèle Dol	)

En sachant qu'une couche se décomposera en deux parties comprenant un en-tête (*header*) appelé aussi PCI (*Protocol Control Information*) et un champ DATA (au sens « *network data* »). En fait, cela représente les protocoles présents dans la trame de la manière suivante :



On comprend alors que le champ DATA d'une couche contient le bloc de la couche supérieure (Header + DATA). C'est le principe de l'encapsulation.



Une fois le rapprochement fait avec le modèle « TCP/IP », on obtient la « vision suivante » :

## trame

Remarques : certaines couches ou certains champs DATA peuvent être vides. Par exemple, la trame  $n^{\circ}1$  n'encapsule que les protocoles Ethernet\_II, IP et TCP. La couche application est donc vide.

D'autre part les couches du modèle DoD offre l'utilisation d'autres protocoles. Par exemple, les trames  $n^{\circ}13$  et 17 encapsulent les protocoles Ethernet\_II, IP, UDP et DNS :

🛛 Filter	udp.port	== 53					₹	🕂 Exp	ressio	on 🦪 Cle	ar 🧹 Apply					
No	Time				Sou	rce			0	Destination		Protocol	Info			
1	3 2.55367	72			145	.254.3	160.2	37		145.253.2	2.203	DNS	Standard	query	A pagead2.googlesy	ndicat
1	17 2.91419	90			145	.253.2	2.203			145.254.1	160.237	DNS	Standard	query	response CNAME pag	ead2.g
<ul> <li>Frame</li> <li>Ethen</li> <li>Inten</li> <li>User</li> </ul>	e 17 (188 rnet II, rnet Prot Datagram	3 bytes Src: f tocol, S Proto	on wi e:ff:2 Src: 1 col. 9	ire, 18 20:00:0 145.253 Src Por	8 byt 1:00 .2.20 t: do	es ca (fe:f 3 (14) main	oture f:20: 5.253 (53).	d) 00:01 .2.20 Dst	.:00) 3), Port	, Dst: X Dst: 145 : pxc-nt	erox_00:00 .254.160.23 fv (3009)	:00 (00:00: 37 (145.254	01:00 4.160.2	Couc	he application	2
Doma:	in Name S	System	(respo	onse)			(00))	000		, pae ne	., (0000)					
0000         0           0010         0           0020         0           0030         0           0040         0           0050         0           0050         0           0070         0           0090         0           0090         0           0040         0	00       00       01         00       ae       15         a0       ed       00         00       04       00         6f       67         00       bc       c1         6f       67       6c         00       bc       c1         6f       67       6c         00       bc       c1         6f       67       6c         00       1a       06         06       61       6b         00       01       00         00       01       00	00         00           95         40           35         0b           00         00           6c         65           6d         00           00         11           65         c0           70         61           61         64           00         00           00         00	00 fe 00 f9 c1 00 00 07 73 79 00 01 07 70 26 c0 67 65 6e 73 7b 00 7b 00	ff         20           11         a3           9a         30           70         61           6e         64           00         01           61         67           3b         00           61         64           03         6e           04         d8           04         d8	00 0 15 9 02 0 67 6 69 6 65 6 05 0 05 0 65 7 ef 3 ef 3	1 00 ( 1 fd ( 0 23 ( 5 61 ( 3 61 ( 3 61 ( 1 64 (	08 00 02 cb 31 80 54 32 74 69 05 00 32 06 00 00 5f 67 c0 58 c0 58	45 6 91 f 00 6 11 6 6f 6 01 6 67 6 00 7 6c 6 00 6 00 6	00 91 97 90 96 97 95 91 91		0E. agead2.g dication z gead2.go z d.google net.X ;c			Coud	che transport UDP uche réseau IP	
														Cou Eth	che interface nernet_I	

## **Outils statistiques**

Wireshark fournit des outils pour l'analyse et les statistiques du trafic capturé.

- Summary : statistiques générales sur la capture actuelle
- Protocol Hierarchy : statistiques sur la pile de protocoles utilisé dans l'échange
- Conversations : statistiques des conversations saisies. Une conversation est le trafic entre deux points de terminaison spécifique. Par exemple, une conversation IP est tout le trafic entre deux adresses IP.
- Endpoints : statistiques des points de terminaison. Un point de terminaison réseau est la terminaison logique d'un protocole d'une couche spécifique.

Sta	atistics
1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1	Summary Protocol Hierarchy Conversations Endpoints Packet Lengths IO Graphs
	Conversation ListEndpoint ListService Response Time
3	BOOTP-DHCP Compare Flow Graph HTTP IP Addresses IP Destinations IP Protocol Types ONC-RPC Programs
	UDP Multicast Streams WLAN Traffic

Il y a deux aspects à prendre en compte dans un échange :

- le transfert physique de trames contenant des protocoles encapsulés (fabrication à l'émission et décodage à la réception : parcours vertical du modèle)
- un dialogue logique entre protocole de couche spécifique (dialogue virtuel horizontal entre deux modèles)



## ANALYSE DE TRAMES

Ouvrir le fichier http.cap disponible sur le serveur ou sur le site <u>http://wiki.wireshark.org/SampleCaptures</u> (HTTP).

## Adressage des protocoles dans le modèle Dod

Un protocole utilise des numéros (les *assigned numbers*) identifiant les protocoles de niveau supérieur qu'il transporte.

Sélectionnez une trame transportant des données http.

Le champ de l'en-tête Ethernet identifiant le protocole de niveau réseau est **Type**.

#### 1) Quelle est la valeur de ce champ pour le protocole IP ?

Dans l'en-tête IP, le protocole de niveau transport est identifié par le champ **Protocol**.

#### 2) Quelle est la valeur du champ Protocol pour le protocole TCP ?

Sous Linux seulement, vérifier le numéro de protocole assigné à TCP en consultant le fichier /etc/protocols

\$ grep 'tcp' /etc/protocols

Dans l'en-tête de niveau transport, le nombre identifiant le processus applicatif est appelé **port**. Les processus client et serveur utilisent un numéro de port chacun : le numéro de port du client est généralement choisi par la machine, tandis que le numéro de port des applications exécutées sur le serveur est normalisé.

3) Quel est le numéro de port utilisé par le service HTTP ?

4) Quel est le numéro de port choisi par votre client ?

5) Sur combien d'octets sont codés les numéros de ports en TCP ? Combien de processus simultanés peuvent théoriquement communiqués via TCP sur une machine ?

Sous Linux seulement, vérifier le numéro de port utilisé par le service HTTP en consultant le fichier /etc/services

\$ grep 'http' /etc/services

# 6) Les en-têtes des protocoles Ethernet\_II, IP et TCP sont-ils encodées en ASCII ?

#### 7) L'en-tête du HTTP est-il encodé en ASCII ?

Sélectionnez une trame transportant des données dns.

#### 8) Quelle est la valeur du champ Protocol pour le protocole UDP ?

Sous Linux seulement, vérifier le numéro de protocole assigné à UDP en consultant le fichier /etc/protocols

\$ grep 'udp' /etc/protocols

#### 9) Quel est le numéro de port utilisé par le service DNS ?

Sous Linux seulement, vérifier le service associé par défaut au numéro de port 53 en consultant le fichier /etc/services

\$ grep '53' /etc/services

10) Sur combien d'octets sont codés les numéros de ports en UDP ? Combien de processus simultanés peuvent théoriquement communiqués via UDP sur une machine ?

## Étude des statistiques

Sélectionner le menu Summary.

#### 11) Quel est le débit moyen mesuré par Wireshark ?

Sélectionner l'outil Protocol Hierarchy qui permet de visualiser la pile de protocoles, le pourcentage de bande passante consommé par chaque protocole, le débit, à chaque niveau etc.

12) Des deux protocoles de niveau transport utilisés, lequel est prépondérant ?

13) Pour le protocole TCP les valeurs indiquées dans colonnes Packets et End packets diffèrent. Pourquoi la colonne End packets contient-elle moins de paquets ? Est-ce aussi le cas pour le protocole UDP ?

14) À quoi servent les paquets qui ne sont pas comptabilisés dans la colonne End packets ?

15) Pourquoi le débit affiché pour les couches hautes est-il inférieur à celui des couches basses ?

## CAPTURE DE TRAMES

## Mode super utilisateur

Le logiciel s'ouvre alors sur cette page de menu :

Eila Edit View Ga Captura Apolyza Statistica Telephony		
	🖇 🛆 📃 🖪 🖪 🕒 🖸 🛅 🎬 🛄 🔯	YEG (C)
▼ Filter:	🖶 Expression 🤞 Clear 🖋 Apply	
WIRE <b>SHARK</b> The World's Most Pop	oular Network Protocol Analyzer	
Capture	Files	Online
Interface List Live list of the capture interfaces (counts incoming packets)	Open Open a previously captured file	Website Visit the project's website
Start capture on interface:	Open Recent: /home/tv/Téléchargements/http.cap (25 KB)	User's Guide     The User's Guide (local version, if installed)
<ul> <li>Pseudo-device that captures on all interfaces</li> <li>lo</li> </ul>	🚙 Sample Captures	🚙 Security
Capture Options	• A rich assortment of example capture files on the wiki	Work with Wireshark as securely as possible
Capture Help         Image: Step by step to a successful capture setup         Image: Step by step to a		
O Ready to load or capture • No Packets		Profile: Default

On peut vérifier qu'en cliquant sur « Interface List » que l'on possède les droits d'accès sur les interfaces réseaux disponibles pour une capture :

R	Wireshark: Capture Interfaces								
Device	Description	IP	Packets	Packets/s		Stop			
🔊 eth0		192.168.52.2	19	4	🖭 Start	🍯 Options			
🔊 any	Pseudo-device that captures on all interfaces		67	4	🖳 Start	🍯 Options			
🔊 lo		127.0.0.1	48		💐 Start	🍯 Options			
👩 Aide						💥 Fermer			

Il existe des options intéressantes avant de démarrer une capture :

7	☑ Wireshark: Capture Options — □ ×							
Capture								
Interface: eth	Interface: eth0							
IP address: 19	2.168.52.2, f	e80::92e6:baff:fe25:8	310a					
Link-layer hea	der type: Eth	ernet 💲						
🗹 Capture pao	ckets in promis	scuous mode						
Capture pa	ckets in pcap-r	ig format (experiment	al)					
Limit each p	backet to 1	bytes						
🕁 Capture Fi	lter:		₹					
Capture File(s)			Display Options					
File:		Browse	Update list of packets in real time					
🗌 Use multiple	e files							
🗹 Next file ev	ery 1	🛊 megabyte(s) 💲	Automatic scrolling in live capture					
🗆 Next file ev	ery 1	🗘 minute(s) 🛛 🗘	Hide capture info dialog					
🗹 Ring buffer	with 2	🛊 files	Name Recolution					
🗆 Stop captur	re after 1	🛊 file(s)	Name Resolution					
Stop Capture .			Enable MAC name resolution					
🗆 after	1	packet(s)	Enable network name resolution					
🗆 after	1	megabyte(s) 😫						
🗆 after	1	minute(s) 🗘	Enable transport name resolution					
👩 Aide			Annuler 🛛 🚉 Start					

- Update list of packets in real time : affiche en temps réel à l'écran les trames capturées.
- *Enable MAC name resolution* : affiche le nom de la machine ou son adresse IP à la place de l'adresse MAC.
- *Enable network name resolution* : affiche le nom d'hôte de la machine à la place de l'adresse IP.
- *Enable transport name resolution* : remplace les numéros de port TCP et UDP par le nom du protocole applicatif associé.

Il est évidemment possible de créer des filtres de capture (qui n'enregistrent que les trames conformes à la règle) et d'enregistrer une capture dans un fichier. Il y a aussi des options pour afficher une capture en temps réel.

Remarque : on laissera généralement l'activation du <u>mode promiscuous</u> qui permet à une carte réseau d'accepter tous les paquets qu'elle reçoit, même si ceux-ci ne lui sont pas adressés. Ce mode est une fonctionnalité utilisée pour écouter tout le trafic réseau.

## Manipulations

Capturer le trafic d'une communication vers un site Internet que vous n'avez pas consulté depuis le démarrage de votre machine.

Proposer une règle de filtrage pour isoler dans la capture la communication avec ce site Internet.

Vous devez visualiser des paquets DNS de type query et response. Observez le contenu de ces paquets DNS.

16) Déduisez-en leur rôle.

17) Quelle est l'adresse IP du serveur auquel votre machine a envoyé la requête DNS ?

18) À votre avis, à qui appartient ce serveur ?

19) À votre avis, l'adresse physique destination de la trame Ethernet\_II contenant la requête DNS est-elle celle du serveur DNS ? Si non, à qui appartient-elle ?

Sélectionnez une trame contenant l'indication HTTP dans la colonne Info. Avec le bouton droit de la souris, choisissez l'option Follow TCP stream. Le dialogue entre votre navigateur et le serveur web apparaît.



20) Par quelle primitive commence la requête HTTP ?

21) Quelle version du protocole HTTP est utilisée par votre navigateur ?

22) La requête HTTP émise par le navigateur contient-elle des données ?

23) Quelle est la version du protocole HTTP utilisée par le serveur dans sa réponse ?

24) Quelle est le type de données renvoyées par le serveur ?

25) A votre avis, quel code réponse aurait renvoyé le serveur si le document demandé dans la requête était introuvable ? Tester avec un document inexistant.

Remarque : lorsque vous fermez la fenêtre ouverte par cette option, il reste un filtre d'affichage : il faut l'effacer en cliquant sur clear.

# 26) Enregistrer la capture réalisée dans un fichier capture\_votreNom au format Wireshark/tcpdump.

Vous m'enverrait <u>votre compte-rendu</u> (réponses aux questions en précisant leur numéro) au **format txt ou rtf** (aucun autre format accepté) ainsi que le <u>fichier de capture</u> à cette adresse : <u>tvaira@free.fr</u>.