

Laboratoire de téléinformatique Introduction à l'analyseur de réseau Wireshark (Ethereal)

Description

Wireshark est un analyseur de protocole gratuit pour Windows, Unix et ses dérivés. Il permet d'examiner des trames à partir d'un fichier ou directement en les capturant sur le réseau. Pour chaque paquet, il est possible d'obtenir un résumé ainsi qu'un décodage détaillé. Wireshark peut être téléchargée à l'adresse suivante : <u>http://www.wireshark.org/</u>.

En outre, le logiciel possède des fonctionnalités très utiles comme les filtres de capture et d'affichage et la reconstitution du flux d'une session TCP. De plus, le nombre de protocoles reconnus par l'analyseur est très élevé.

Wireshark est un projet *open source* réalisé sous la licence public GNU (GPL). Il est donc possible d'obtenir les programmes sources afin de les modifier.

Ce document, basé sur la version 0.99.0 (windows) du logiciel, est inspiré du User's Guide disponible sous <u>www.ethereal.com</u> (ancien nom de Wireshark : http://www.wireshark.org/docs/).

Pour la manipulation au laboratoire (nous en aurons besoin pour les autres manipulations), il faut suivre la procédure ci-dessous.

Comment commencer ?

Si vous travaillez sur les machines de l'école il faut premièrement vous mettre sur une station de travail (PC) et démarrer sous Linux¹:

Login : labo Password : labo

Ensuite il faut démarrer le programme en cliquant sur l'icône « Wireshark » (bureau du Desktop).

Vous obtiendrez une fenêtre de ce type :

¹ Il faut être administrateur pour utiliser Ethereal, c'est pourquoi vous ne pouvez pas utilier Windows 2k/XP!



© Th	e Eth	ereal	Netw	ork Ana	lyzer													
Eile	⊑dit	⊻iew	<u>G</u> ο	⊆apture	<u>A</u> naly:	ze <u>S</u> ta	tistics	Help										
Ð	ë,	ð,			B		×	¢				Ŵ	T			4	Ð	Q
Eilter:										•	Expr	ession	. ⊆lea	ir <u>A</u> ppl	у			
Ready	to load	d or cap	oture						No F	Packets								/

Ensuite faites une analyse sur le réseau en cliquant « Capture » et « Interfaces » et vous obtenez ceci:

(il faut choisir une carte réseau comme interface et eth0 si vous êtes sur un PC école).





C Ethereal: Capture Interfaces				
Description	IP	Packets	Packets/s	Stop
Generic dialup adapter	unknown	0	0	Capture Prepare Details
Realtek RTL8139/810x Family Fast Ethernet NIC (Microsoft's Packet Scheduler)	192.168.2.118	950	0	Capture Prepare Details
⊆lose				

Faites « capture » et l'analyse commence. Vous obtenez ceci :

G Ethereal:	Capture fro	m Realtek R	
_[Captured Pack	ets		
Total	245	% of total	
SCTP	0		0.0%
тср	203		82.9%
UDP	39		15.9%
ICMP	0		0.0%
ARP	2		0.8%
OSPF	0		0.0%
GRE	0		0.0%
NetBIOS	0		0.0%
IPX	0		0.0%
VINES	0		0.0%
Other	1		0.4%
Running	00:01:23		
	S	top	

Quand vous voulez arrêter l'analyse, faites « STOP ». Vous obtenez une fenêtre qui ressemble à ceci :





(Untit	led) - Ethereal				×
<u>Eile E</u> dit	View Go Captur	e Analyze Statistics Help			
	i 🖭 🎱 📦	🕞 🔚 🗙 🖗 📇	🔄 🗢 🗢 不 :		
Eilter:			▼ <u>E</u> xpression <u>C</u> lear	Apply	
No	Time	Source	Destination	Protocol Info	^
	1 0.000000	CompalEl_ba:b3:aa	Broadcast	ARP Who has 192.168.2.1?	
	2 0.002389	olicom_c2:be:ba	CompalEl_ba:b3:aa	ARP 192.168.2.1 is at OC	
	3 0.002407	192.168.2.118	192.168.2.1	DNS Standard query A ima	
	4 0.021335	192.168.2.1	192.168.2.118	DNS Standard query respo	
	6 0 124705	64 233 183 147	107 168 2 118	TCP 2782 > HULD [SYN] 56	
	7 0.125028	192.168.2.118	64,233,183,147	TCP 2782 > http [ACK] SE	
	8 0.130069	192.168.2.118	64.233.183.147	HTTP GET /imahp?ie=UTF-88	
	9 0.187677	64.233.183.147	192.168.2.118	TCP http > 2782 [ACK] Se	
1	.0 0.304721	64.233.183.147	192.168.2.118	HTTP [TCP Previous segmer	
1	1 0.304989	192.168.2.118	64.233.183.147	TCP [TCP Dup ACK 8#1] 27	
1	2 0.309273	64.233.183.147	192.168.2.118	TCP [TCP Fast Retransmis	
1		102 168 2 118	64 222 182 147	TCP 2782 > http [ACK] Sc	
1	5 1 382838	192.108.2.118	64 233 183 147	HTTP GET /intl/fr ALL/ima	
1	6 1.432417	64.233.183.147	192.168.2.118	TCP http > 2782 [ACK] SE	
1	7 1 447005	64 233 183 147	192 168 2 118	TCP [TCP segment of a re	~
<					
🗄 Frame	e 5 (62 bytes o	on wire, 62 bytes captur	ed)		
🗄 Ether	net II, Src: 0	CompalEl_ba:b3:aa (00:02	:3f:ba:b3:aa), Dst: Olio	com_c2:be:ba (00:00:24:c2:be:b	oa)
🗄 Inter	net Protocol,	src: 192.168.2.118 (192	.168.2.118), Dst: 64.233	3.183.147 (64.233.183.147)	
 Trans 	mission Contro	ol Protocol, Src Port: 2	782 (2782), Dst Port: ht	ttp (80), Seq: 0, Len: 0	
<					>
0000 0	0 00 24 c2 be	ba 00 02 3f ba b3 aa 0;	3 00 45 00\$?.	E.	_
0010 0	0 30 78 a5 40	00 80 06 c6 87 c0 a8 0	2 76 40 e9 .0x.0	∨@.	
0020 b 0030 Q	/ 93 Ua de 00 d 80 31 c6 00	50 14 e2 08 20 00 00 0 00 02 04 05 b4 01 01 0	J UU /U UZP	p.	
0030 9	u au ar ca uu	00 02 04 03 D4 01 01 04	· v2 · · · · · · · ·		
					_
Hile: "C:\DC	COME~1\Isabelle\LOC	ALS~1(Temp\etherXXXXN5DMIT" 142 K	B UU: J P: 246 D: 246 M: U Drops: 0		//

Nous remarquons que Wireshark est composé de trois panneaux principaux :

- 1. Ce panneau affiche la liste des paquets ainsi que leurs caractéristiques principales. En cliquant dans ce panneau, on contrôle l'affichage des deux autres.
- 2. Le panneau du milieu montre le détail de la trame sélectionnée dans le panneau 1.
- 3. Le dernier panneau permet de visualiser le contenu brut des trames. Il représente le paquet sélectionné dans le panneau 1 et met en évidence le champ sélectionné dans le panneau 2.

Maintenant revenons un peu plus en détail sur la façon dont on peut capturer les paquets. Après avoir cliqué « Options » (faisons-le, au lieu de cliquer sur Interfaces), nous obtenons cette fenêtre :

heig-vd

Haute Ecole d'Ingénierie et de Gestion du Canton de Vaud



left Capture C	e Options		
Capture			
Interface: Realtek	RTL8139/810× Family	Fast Ethernet NIC	: (Microsoft's Packet Scheduler) : 💌
IP address: 192.168.	2.118		
Link-layer header typ	e: Ethernet 📐 Bu	ıffer size: 1	🗢 megabyte(s)
🔽 Capture packets ir	promiscuous mode		
📃 Limit each packet t	o 68 🔷 🗘 by	tes	
Capture Filter:	tcp port 3389		•
Capture File(s)			Display Options
File:		Browse	Update list of packets in real time
Use <u>m</u> ultiple files			
Next file every	1 🗘 m	egabyte(s) 💌	Automatic scrolling in live capture
Next file every	1 🗘 mi	nute(s) 🗸 🗸	Hide capture info dialog
🗹 Ring buffer with	2 🗘 files	;	-Name Decolution
Stop capture after	1 🗘 file(s)	
Stop Capture			Enable MAC name resolution
🔲 after 🛛 1	🗘 packeti	(5)	Enable network name resolution
🔲 after 🛛 1	🗘 mega	byte(s) 🛛 🗸	
🔲 after 🛛 1	minut	e(s) 🗸	Enable transport name resolution
Help			Start Cancel

La capture peut être personnalisée avec les paramètres suivants :

Interface : L'interface réseau sur laquelle la capture est effectuée. Laissez l'interface par défaut proposée, sous Windows. Pour Linux, utilisée ethX, où X est le numéro de l'interface (en général eth0).

Limit each packet to : Spécifie le nombre maximum de données à capturer pour chaque paquet. La valeur par défaut est généralement suffisante pour les protocoles usuels. Il faut cependant que le nombre corresponde au MTU (*Maximum Transfer Unit*) de l'interface de capture.

Capture packets in promiscuous mode : L'option *promiscious* permet de capturer des paquets qui ne nous sont pas destinés. Ceci est évidemment dépendant de la structure du réseau.

Capture Filter : La zone de texte permet d'entrer ou de modifier le filtre de capture. Le bouton ouvre la boîte de dialogue contenant les filtres enregistrés. La conception d'un filtre de capture est présentée au point « Filtres de capture».



File : Ce champ vous permet de spécifier le nom du fichier qui sera utilisé pour la capture quand vous choisirez plus tard « Save » ou « Save as... » dans le menu « File » d'Ethereal.

Update list of packets in real time : Affichage des paquets en cours de capture. Il est préférable de ne pas activer cette option.

Capture limits : Il est possible d'arrêter la capture suivant différents critères : nombre de paquets, de kB, de secondes.

Enable MAC name resolution : Permet de traduire les trois premiers octets des adresses MAC avec le nom du constructeur.

Enable network name resolution : Permet de traduire les adresses IP avec le nom de machine équivalent.

Enable transport name resolution : Permet d'indiquer le nom du protocole, ceci pour les numéros de ports connus.

Lorsque toutes les options sont choisies, cliquer sur "Start" pour démarrer une nouvelle capture. Une nouvelle boîte de dialogue s'ouvre alors et indique l'évolution de la capture. Cliquer sur le bouton "Stop" pour terminer la session de capture.

L'affichage peut être modifié à souhait à l'aide des filtres d'affichage dont nous allons parler plus loin.

Filtres de capture

Ethereal utilise les filtres de capture basés sur le langage libpcap. Le détail complet de la syntaxe est expliqué dans le manuel tcpdump (man tcpdump sous Unix/Linux).

Les filtres de capture sont indiqués dans le zone de texte prévue à cet effet dans la boîte de dialogue des options de capture. Il est possible de stocker différents filtres. Pour cela, il faut ouvrir la boîte de dialogue d'édition de filtres de capture en cliquant sur le menu "Capture" / "Capture Filters...". Cette boîte peut également être affichée depuis les options de capture à l'aide du bouton "Filter".





C Ethere	al: Capture Filter 📃 🗖 🔀
Edit	Filter
	No Broadcast and no Multicast No ARP
New	IP only IP address 192.168.0.1
	TCP only UDP only
	TCP or UDP port 80 (HTTP) HTTP TCP port (80)
Delete	No ARP and no DNS Non-HTTP and non-SMTP to/from www.ethereal.com
	New filter
Properties	
Filter name	e: mon filtre
Filter string	g: src port 80
Help	<u>OK</u> <u>Save</u> <u>Close</u>

La conception d'un nouveau filtre est la suivante :

- Donner un nom au filtre dans la zone de texte "Filter name" (mon filtre ici).
- Ecrire le filtre dans la zone de texte "Filter string", en respectant la syntaxe ci-dessous.
- Ajouter le filtre en cliquant sur le bouton "New".
- Sauvegarder la liste de filtres à l'aide du bouton "Save".

Syntaxe des filtres de capture

Un filtre de capture est composé d'une suite d'instructions reliées entre elles par des opérateurs and ou or. On peut inverser le sens des instructions en ajoutant un not. Il est possible de grouper les expressions avec des parenthèses.

• [not] primitive [and|or [not] primitive ...]

Ceci est la forme générale d'un filtre. Une primitive est l'une de celles présentées ci-dessous.

• [src|dst] host <host> (exemple: src host 192.169.1.37)

Filtre sur une adresse IP ou un nom d'hôte. Les mots clés src, dst permettent de se concentrer sur l'adresse IP source, respectivement destination. Sans ces mots clés, tous les paquets liés à l'adresse IP spécifiée sont pris en compte.

ether [src|dst] host <ehost>



Ce filtre suit exactement les principes cités ci-dessus mais s'applique cette fois sur les adresses MAC.

[tcp|udp] [src|dst] port <port>

Filtre sur un port et, par corollaire, un service précis. Délimite la capture aux trames correspondants à un certain numéro de port. De plus, l'on peut spécifier le type de protocole ou encore s'il s'agit d'un port source ou destination.

• [src|dst] net <net> [{mask <mask>}|{len <len>}]

Filtre sur un réseau ou un sous-réseau. La capture peut être limitée avec les paramètres src et dst de la même manière que pour les primitives précédentes. Le masque de sous-réseau ou le préfixe CIDR² peut être indiqué s'il est différent de la machine sur laquelle se trouve l'analyseur.

less|greater <length>

Filtre sur le paquets dont la longueur est plus petite ou égale, ou respectivement, plus grande ou égale à la longueur spécifiée.

• [ip|ether] proto <protocol>

Filtre sur un protocole spécifique au niveau IP respectivement au niveau MAC. Le paramètre protocol correspond au numéro du protocole ou un nom reconnu. Quelques exemples : Un datagramme IP encapsulant un message ICMP à la valeur du champ protocol ID à 1. De même, on reconaît une requête ARP à la valeur 0x0806 du champ type de la trame ethernet.

• [ether|ip] broadcast|multicast

Filtre sur du *broadcast* ou du *multicast* IP ou au niveau MAC.

• <expr> relop <expr>

Permet de créer des expressions complexes. Les détails sont donnés dans les pages du manuel tcpdump.

Exemples

Les deux filtres ci-dessous sont équivalents : capture du trafic FTP.

• (src port 21) or (dst port 21) ou port 21

Un filtre pour capturer tout le trafic telnet concernant un hôte IP particulier.

• tcp port 23 and host 10.192.73.1

Un filtre de capture concernant le trafic telnet visible sans inclure celui générer vers et à partir un hôte IP particulier.

• tcp port 23 and not host 10.192.73.1

Maintenant que nous savons comment faire un filtre, il suffit de relancer l'analyseur et maintenant nous n'obtenons que les paquets http:

2

CIDR, Classless Inter-Domain Routing

heig-vd

Haute Ecole d'Ingénierie et de Gestion du Canton de Vaud



(U) 🔘	Intitle	d) - E	ther	eal																			×
File	Edit	View	Go	Capt		Analys		atistics	Halo														
Elle	Eair	View	<u>G</u> 0	Cahr	ure.	Analyz	e <u>p</u> u	ausuus	Deih														
	ĕ,	Ø		[💼	ji j	6		x	¢		5 [[<u>}</u> (þ		¢)	T	₽ [Ð	. E	ζ 🤅	I)	
Eilter	:												Ŧ	Expre	ession	⊆lea	r <u>A</u> pply						
No		Time			Sou	urce					Des	tinatior	1				Protocol	Info					^
	1	0.0	0000	0	64	.233	.183	.147			192	2.168	3.2.	118			TCP	http	> 13	32	FIN	, AC	Ξ
	2	0.0	1190)7	64	.233	.183	.147			192	2.168	3.2.	118			TCP	http	> 25	13	[SYN	, AC	
	3	0.0	6306	i9 –	64	.233	.183	.147			192	2.168	3.2.	118			TCP	http	> 25	13	[АСК] Se	
	4	0.0	8731	.9	64	.233	.183	.147			192	2.168	3.2.	118			TCP	[TCP	segm	ent	of	a ne	
	5	0.0	9022	:9	64	.233	.183	.147			192	2.168	3.2.	118			TCP	[TCP	segm	ent	of	a ne	
	6	0.0	9421	.0	64	.233	.183	.147			192	2.168	3.2.	118			TCP	[TCP	segm	ent	ot	a ne	
		0.1	2285	9	64	.233	.183	.147			19,	2.168	<u>s. 2.</u>	118			HTTP		Prev	nous	s se	gmer	
	8	0.1	5152 0222	8	64	.233	102	.147			101	2.168	s. Z.	110			TCP	LICH	Retr	ansr	1155	ion	
	10	0.2	0333)上)1	64	.233	.183	.147			102	2.100 1.40	s. <u>z</u> .	110			HITP	Cont	inuat	ion	on	non-	
	11	0.2	1126	/L :1	64	.233	107	.147			102	2.100 1.60	<u></u>	110			HITP	Cont	inuat	ion	on	non-	
	12	0.2	4770	10 11	64	.200	192	.147			192	2.100 2.169	2.5	11 Q				Cont	inuat	ion	on	non-	
	13	0.2	4723 5040	,9 17	64	.233	183	147			107	2.168	2.2.	118			HTTD	Cont	inuat	ion	on	non-	
	14	0.2	5420	12	64	233	183	147			192	2 168	2.5	118			HTTP	Cont	inuat	ion	on	non-	
	15	0.2	5734	0	64	.233	.183	.147			192	2.168	3. 2.	118			HTTP	Cont	inuat	ion	on	non-	
	16	0.2	5753	1	64	.233	.183	.147			192	2.168	3.2.	118			TCP	http	> 25	15	Γ <u>S</u> ΥN	. AC	
	17	0.2	6120	13	64	233	183	147			193	2 168	2.2	118			HTTP	Cont	inuat	ion	or	non-	*
<																						>	
		1 60	0 k.					. I.,															_
	ame	I (6	ίαυ	/tes	on	wire	2, 60	ι ογτ	es c	apti	urea)						7-7 66						
E E	thern	et I	1, 1	snc:	011	COM_	_CZ:D	e:pa	2 14	:00	:24:C	2:De	:ba,	, D	St: U	ompa 100	160 D 1	10 (1)	00:02	2:31	:pa 110	:bs:a	.a,
	ncern	ес Р • • • •	rutt		, Sr	C: 0	04.23	3.18	3.14	7.0	04.23	3.18	3.I4 \	·/),	DSU:	192	.168.2.1	18 (1	92.100	3.Z.	TT9.		
	ransm	1551	on (.onτ	roi	Prot	:0C01	, sr	C POI	rτ:	ηττρ	(80)), ι	sτ	Port:	ک ک ⊥	2 (1332)	, seq	: 0, /	чск:	υ,	Len:	Ľ
																							_
<																							>
0000	00	02 3	af b	a hi	2 2 2	00	00	24 c	2 ha	ha	08.00	0.45	00		2	¢							_
0010	i ŏŏ	28 3	3e 2	8 0	0 00	ef	ŏĕ i	d2 0	- 40	р9 29	h7 93	3 <u>-</u> 0	ă8		66	• •	.a						
0020	02	76 (20 5	õ õ	5 34	9c	6d i	6d 2	d 7c	8e	0d 61	Ē 50	11		,́.Р.4.	m m	- oP.						
0030) 1f	fe 3	3b 1	e 0	0 00	ff	ff ·	ff f	F ff	ff					.;								
l Filou "	<u>cupoc</u>	I IME 1	Uteab) اذهاله			molath	~~~~~~	47500	T" 04	VP 00-0		100.0	N. 100		onci 0							_
Tue:	capoe	OWENI	usab	enertr	CALD	~ r(rei	mptern	CIVVVV	Песерт	1 24	VD 00:0	JP:	1001	7, 100	THE O DR	ops: 0							11

Fantastique, non ? A vous de jouer maintenant...

Nous vous encourageons néanmoins à consulter l'aide d'Ethereal.

Enregistrer les captures

Il est possible de sauvegarder les captures pour les importer dans un certain nombre d'analyseurs de protocoles. Cependant, il ne s'agit pas de fichiers textes lisibles. De plus le passage du logiciel de Unix à Windows n'a pas permis de gérer l'impression correctement.

Le meilleur moyen pour sauvegarder et imprimer une capture est l'impression dans un fichier à l'aide du menu "File" / "Print...".

Une boîte de dialogue s'ouvre

Choisir l'option "Plain Text" (par exemple)





C Ethereal: Print			
Printer			
💿 Plain <u>t</u> ext			
O PostScript			
Output to file:	CALS~1\Te	emp\ethprint>	XXXM59IIT Browse
Packet Range			Packet Format
	⊆aptured	Displayed	Packet summary line
 All packets 	100	100	Packet details:
Selected packet only	1	1	🔘 All coļlapsed
Marked packets only	0	0	 As displayed
 From first to last marked packet 			◯ All expanded
Specify a packet range:	0		Packet bytes
			Each packet on a new page
			Print Cancel

L'impression sous Linux ne pose pas de problème praticulier. En utilisant la commande lpr, l'impression est envoyé vers l'imprimante par défaut.

Le bouton "File" permet de choisir le fichier destination (par défault il se place dans le répertoire d'Ethereal chez moi). Vous pouvez aussi sauver un fichier en format .cap :





Ethereal: Save file	e as	? 🛛
Enregistrer <u>d</u> ans :	🥯 System (C:) 🔽 🔇 🤌 📂 🛄 🗸	
AddOn coktel Documents and Se emme i386 Isabelle	Image: Section 2013 Image: Section 2013 Image: Section 2014 Image: Section 2014 Image: Section 2014 Image: Section 2014 <td></td>	
Nom <u>d</u> u fichier : <u>T</u> ype :	ma-capture.cap Ethereal/tcpdump (*.cap, *.pcap)	Enregistrer Annuler
File format: libpca	ap (topdump, Ethereal, etc.)	
Packet Range		
	💽 Captured 🛛 🔘 Displayed	
 All packets 	100 100	
Selected pack	et 1 1	
O Marked packet	s 0 0	
First to last mar		
C Range:	U	.::

Il est aussi utile de savoir que nous pouvons exporter les données en fichier .txt, .ps,...

Filtres d'affichage

Après avoir effectué une capture, il est toujours possible de modifier l'affichage des paquets en spécifiant un filtre d'affichage (ou filtre de post-capture).

Les filtres d'affichage offrent un nombre d'options et de protocoles reconnus nettement plus grand que celui des filtres de capture. La sélection peut se faire sur :

- un protocole ;
- la présence d'un champ ;
- les valeurs des champs ;
- la comparaison de champs.





C Ethere	al: Display Filter	×
Edit	Filter	
	Ethernet address 00:08:15:00:08:15	
	Ethernet type 0x0806 (ARP)	
	Ethernet broadcast	
New	No ARP	
	IP only	
	IP address 192.168.0.1	
	IP address isn't 192.168.0.1, don't use != for this!	
	IPX only	
	TCP only	
Delete	UDP only	
Perce	UDP port isn't 53 (not DNS), don't use != for this!	
	TCP or UDP port is 80 (HTTP)	
	НТТР	
Properties -		4
Filter name	TCP only	1
Filter string	g: tcp	Ĵ
Help	OK Apply Save Close	

Les filtres d'affichage s'écrivent dans la zone de texte située au bas de la fenêtre d'Ethereal (zone B du panneau d'Ethereal). Le bouton "Filter" permet de charger un filtre enregistré préalablement. La création d'un nouveau filtre d'affichage est identique à celle des filtres de capture. Pour sélectionner un protocole particulier, vous pouvez simplement taper le nom du protocole dans la zone B (page 3) et ensuite « Apply » ou « return » pour obtenir ce que vous voulez :





© m	a-capt	ure.c	ap - I	there	eal																			X
File	Edit	View	Go	Cantur	e 4	Analyz	e Sta	tistics	Help															
									<u> </u>	_		_						_	_			_		
	ë.	ð.			. (B	H	×	¢	Ľ	5 [9			ŝ	$\overline{\mathbf{v}}$			ŝ	Ð	Θ	ζ 🖲	l,	
Eilter:	tcp												•	Ē×Þ	ression	⊆le	ear <u>A</u> pply							
No. +		Time			Sou	rce					De	stinat	tion				Protoco	ol I	info					^
	1	0.0	00000)	64.	.233	.183.	147			19	92.1	.68.2	2.118	3		TCP	ł	nttp	> 133	32	FIN,	AC	
	2	0.01	11907	7	64.	.233	.183.	147			19	92.1	.68.2	2.118	3		TCP	ł	nttp	> 251	L3 [SYN,	, AC	
	3	0.0	63069	9	64.	.233	.183.	147			- 19	2.1	.68.2	2.118	3		TCP	ł	nttp	> 251	13 [ACK.	Se	
	4	0.0	37319	9	64.	.233	.183.	147			19	92.1	.68.2	2.118	3		TCP		TCP	segme	ent	of a	i ne	
		0.0	90225 54517	9 \	64.	.233	.183. 197	147			10	12.1 17 1	.68.2	(.11) (.11)	5		TCP		ГТСР	segme	ent	of a	i ne	
	7	0.0	94 Z I (7 7 8 5 () 3	64.	. 233	.103. 192	147			10	2.1 21	68.2	. 119	2		TCP		TCP	Drom	enu		1 FE	
	- 8	0.1	31328	3	64.	. 233	.183.	147			10)2.1	68.7	2.118	3		TCP		TCP	Retra	ansm	, <u>36</u> 0	ionl	
	9	0.20	03331		64.	. 233	.183.	147			19	92.1	.68.2	2.118	3		TCP		ТСР	seame	ent	of a	a ne	
	10	0.2	08201	L	64.	.233	.183.	147			- 19	92.1	.68.2	2.118	3		TCP		TCP	segme	ent	of a	a ne	
	11	0.23	11351	L	64.	.233	.183.	147			- 19	92.1	.68.2	2.118	3		TCP		TCP	segme	ent	of a	a ne	
	12	0.24	47299	9	64.	.233	.183.	147			19	92.1	.68.2	2.118	3		TCP		[TCP	segme	ent	ofa	a ne	
	13	0.2	50402	2	64.	.233	.183.	147			19	92.1	.68.2	2.118	3		TCP		TCP	segme	ent	ofa	a ne	
	14	0.2	54202	2	64.	. 233	.183.	147			19	92.1	.68.2	2.118	3		TCP		TCP	segme	ent	of a	a ne	
	10	0.2	5734U 57521) 	64.	.233	.183.	147			19	12.I	.68.2	. 110	5		TCP		LICP.	segme	ent	OT 8	i ne	
	17	0.2	07 0 5 J 61 7 0 3	2	64.	.233	.183. 192	147			10	92.1 92.1	68.2	(.11) (.11)	2		тсе	ı I	поср. Гтар	> 20. Secmi	LD [ent	of :	, AC	~
						~ ` `														SELIN				
																								,
∃ Fr	ame	1 (6	0 byt	tes (on י	wire	, 60	byt	es c	apt	ured)												
🛨 Et	hern	et I	I, SM	nc: (oli	com_	.c2 : b	e:ba	(00	:00	:24:	c2:k	pe:b	a),	Dst:	Comp	balEl_ba	:b3:	aa (00:02	::3f	:ba:	b3:a	aa)
🛨 Ir	itern	et Pi	roto	col,	Sr	c: 6	4.23	3.183	3.14	7 (64.23	33.1	183.3	147)	, Dsi	t: 19	2.168.2	.118	(19	2.168	3.2.	118)		
∃ Tr	ansm	issi	on Ci	ontro	ו וס	Prot	ocol	, sr	c Po	rt:	http	p (8	30),	Dst	Port	t: 13	32 (133	2),	seq:	О, А	kck :	0,	Len	: (
<																								>
0000	00	02 3	sf ba	b3	aa	00	00 7	·4 c2	, pe	ha	08.0	0 4	5 00)	. 7		\$F							_
0010	ŐŐ	28 3	Se 28	00	õõ	ef (06 c	12 00	40	ē9	b7 9	93 c	:0 a8	3.	66									
0020	02	<u>7</u> 6 (0 50	05	34	9c (6d 6	id 20	1 7 C	8e	0d 6	if 5	0 11		v.P.	4.m	m− oP							
0030	1f	te 3	3b 1e	2 00	00	tt 1	rt f	t ff	- ff	ŦŤ					;	• • •								
File: "]:\ma-c	apture	.cap" 9	4 KB 00	0:00:	:02							P: 10	0 D: 1	00 M: 0									//

Essayez de faire un ping (ping <u>www.epfl.ch</u>) et de filtrer que ces paquets avec un filtre de d'affichage (en bas à gauche dans cette version d'Ethereal). Le protocole utilisé pour les pings est ICMP.

Flux TCP

La recomposition d'un flux de données n'est disponible que pour le TCP. En effet, les protocoles comme UDP, ICMP, etc. n'établissent pas de connexion et n'ont donc pas de session. Ethereal permet donc de rassembler un flux TCP et d'y appliquer un décodage.

Pour suivre un flux TCP, il faut premièrement sélectionner un paquet faisant parti du flux puis cliquer sur le menu "Statistics" / "Follow TCP Stream". Il est possible d'analyser le comportement de la liaison avec cette option : Timesequence, débit, RTT,.... Essayez... Ne pas oublier que l'utilisation de cette option applique un filtre d'affichage afin de ne prendre en compte que les paquets en relation à la session sélectionnée. Pour supprimer le filtre d'affichage, il suffit d'appuyer sur le bouton "clear" dans la fenêtre.

heig-vd

Haute Ecole d'Ingénierie et de Gestion du Canton de Vaud



🥝 Follow TCP stream
Stream Content
GET / HTTP/1.1 Accept: image/gif, image/x-xbitmap, image/jpeg, image/pjpeg, application/vnd.ms- powerpoint, application/vnd.ms-excel, application/msword, application/x-shockwave- flash, */* Accept-Language: fr-ch
User-Agent: Mozilla/4.0 (compatible; MSIE 6.0; Windows NT 5.1; SV1; .NET CLR 1.0.3705) Host: ic.epfl.ch Connection: Keep-Alive
HTTP/1.1 200 OK Date: wed, 01 Nov 2006 11:21:00 GMT Server: Apache-Coyote/1.1 Set-Cookie: JSESSIONID=BF2BAF52C9ED25F8540F0B8D08236A50; Path=/ Content-Type: text/html; charset=ISO-8859-1 Connection: close Transfer-Encoding: chunked
1e71 html PUBLIC "-//W3C//DTD HTML 4.0 Transitional//EN" "http://www.w3.org/TR/<br html4/loose.dtd">
This code was generated automatically so it is not well formatted, and it can
In order to see the formatted HTML, submit the URL of this page to TIDY at http:// infohound.net/tidy/. We apologize for that.
Ce code a .t. g.n.r. automatiquement, il n'est donc pas bien format. et peut contenir des lignes vides. Afin de formater le code HTML, soumettez l'URL de cette page . TIDY sur http://
Save As Print Entire conversation (19221 bytes)
Filter out this stream



Référence

• Manuel de l'utilisateur : <u>www.wireshark.com</u> (ou <u>www.ethereal.com</u>). Si vous avez besoin de plus de connaissances sur l'analyseur il est vivement recommandé de consulter ce manuel qui est bien fait.