Travaux Pratiques N° 1 : Protocole HTTP

Objectif:

Analyser une requête ainsi qu'une réponse HTTP, en utilisant Wireshark.

Etape 1 : téléchargement & installation de wireshark

Wireshark est un programme de reconnaissance, utilisé par les ingénieurs réseau pour analyser le trafic. Ce logiciel open source est disponible pour de nombreux systèmes d'exploitation, y compris Windows, Mac et Linux.

- a. Télécharger Wireshark depuis https://www.wireshark.org/download.html
- b. Procéder à l'installation de wireshark avec les paramètres par défaut

Etape 2 : récupération des adresses IP source et destination

- Dans ce travail, nous analyserons le trafic web échangé entre le PC local et le site du département d'informatique cs. univ-batna2.dz.
 - a. Commençons par récupérer l'adresse IP de l'adaptateur réseau à utiliser lors de la capture. Pour cela, lancer l'invite de commande en exécutant la commande *cmd*. Exécuter la commande *ipconfig*, votre configuration IP apparaitra comme suit :

C:\Users\elhou>inconfig	
Wireless LAN adapter Wi-Fi:	
Connection-specific DNS Suffix .: Link-local IPv6 Address : fe80::e191:74ff IPv4 Address : 192.168.1.99 Subnet Mask : 255.255.255.0 Default Gateway : 192.168.1.1 b. Le moyen le plus simple pour avoir l'adresse IP du site <i>cs.univ-batna2.dz</i> est correspondante s'affichera entre [].	: f58b : 323%11 d'exécuter la commande ping. L'adresse IP
C:\Users\elhou>ping cs.univ-batna2.dz Pinging ww.univ-batna2.dz [193.194.68.228] with 32 byt Request timed out. Etape 3:lancer la capture wireshark	es of data:
 a. Cliquer sur « démarrer la capture de paquet ». Les informations commences Wireshark. Les lignes de données apparaîtront dans des couleurs différentes 	ront à défiler dans la section supérieure de s selon le protocole.
The Wireshark Network Analyzer Ime Wireshark Network Analyzer File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help Ime D	
Apply a display filter <ctrl-></ctrl->	
Welcome to Wireshark Captureusing this filter:	
Npcap Loopback Adapter	

- Adapter for loopback traffic capture $_{-}$
- Learn User's Guide · Wiki · Questions and Answers · Mailing Lists You are running Wireshark 3.4.0 (v3.4.0-0-g9733f173ea5e). You receive automatic updates Ready to load or capture No Packets Profile: Default

Local Area Connection* 9 Local Area Connection* 1

Ethernet

b. Lancer le navigateur web, dans la barre d'adresse, saisir l'URL : cs. univ-batna2.dz puis appuyer sur entrée. Attendre jusqu'à ce que la page d'accueil du site du département se charge entièrement, puis arrêter la capture wireshark, en cliquant sur le bouton « arrêter la capture de paquets »



0	Département d'Infor	rmatiqu X +			Q _ 🗆 X
	< > C ==	s.univ-batna2.	dz		
		~ ~			
<u> </u>	Sea D				
2	2				
	Departmen	t of Computer Sc	ience		
	University of Da	uia 2			
0					
0					
\triangleright		\mathbf{C}			
\odot					
	Espac	e Licence	Espace	Master	Espace Doctorat
0					
(ĝ)					
0	Actualité				
·	Nouveau lien pa	age facebook			
	Thursday, February Read more	y 13, 2020			
	بولين في الاعلام الآلي	ى السنة الثانية ليسانس) المق	بة (المنتقلين من السنة الأولى إل	قاتمة الطلي	
	Sunday, December	r 6, 2020	,		
•••				2020	-12-10 2020-12-08 the state the state of the
	Read more >				
	Read more ►				
	<u>Read more</u> ► Microsoft: Wi-Fi				
File	Read more ► Microsoft: Wi-Fi Edit View Go	Capture Analyze Stat	istics Telephony Wirele	ss Tools Help	
File	Read more ► Microsoft: Wi-Fi Edit View Go Di C @	Capture Analyze Stat	istics Telephony Wirele	ss Tools Help	
File	Read more ► Microsoft: Wi-Fi Edit View Go © 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0	Capture Analyze Stat Capture Analyze Stat Ctrl-/> Source	istics Telephony Wirele	ss Tools Help	
File	Read more ► Microsoft: Wi-Fi Edit View Go Complexity a display filter <0 Time 2211 3.759673 222 3.752345	Capture Analyze Stat	istics Telephony Wireles	Protocol Length Info TLSV1.2 476 Appli SSL 352 Conti	cation Data
File	Read more ► Microsoft: Wi-Fi Edit View Go Ime 221 3.756673 223 3.754265	Capture Analyze Stat	istics Telephony Wireles	Protocol Length Info TLSV1.2 476 Appli SSL 352 Conti SSL 400 Conti	cation Data nuation Data
File	Read more ► Microsoft: Wi-Fi Edit View Go Image: Comparison of the comparison of	Capture Analyze Stat	istics Telephony Wirele	Protocol Length Info TLSv1.2 476 Appli SSL 352 Conti SSL 400 Conti TLSv1.2 135 Appli	cation Data nuation Data cation Data
File	Read more ► Microsoft: Wi-Fi Edit View Go Go Q Go Ime 221 223 3.752455 224 3.754655 224 3.754655 225 3.821574 226 3.822760	Capture Analyze Stat	istics Telephony Wirele	Protocol Length Info TLSv1.2 476 Appli SSL 352 conti SSL 400 Conti TLSv1.2 135 Appli SSL 189 conti TCP 60 443 +	r • • • • • • • • • • • • • • • • •
File	Read more ► Microsoft: Wi-Fi Edit View Go Ime 221 3.759673 222 3.75245 223 3.754655 224 3.754655 225 3.821574 226 3.822977	Capture Analyze Stat	istics Telephony Wirelet	Protocol Length Info TLSv1.2 476 Appli SSL 352 Conti SSL 400 Conti TLSv1.2 135 Appli SSL 189 Conti TCP 60 443 + SSL 189 Conti	c e S c e S cation Data nuation Data nuation Data Ref 133 Ack=111 (Ack) Seq=4133 Ack=111 nuation Data
File	Read more ► Microsoft: Wi-Fi Edit View Go Ime 221 3.756673 222 3.752345 223 3.754655 224 3.754655 225 3.821574 226 3.822977 228 3.832457	Capture Analyze Stat	istics Telephony Wirele	Protocol Length Info TLSv1.2 476 Appli SSL 352 Conti SSL 400 Conti TLSv1.2 135 Appli SSL 189 Conti TCP 60 443 + SSL 189 Conti TLSv1.2 369 Appli	<pre>cation Data nuation Data 8071 [ACK] Seq=4133 Ack=111 nuation Data cation Data</pre>
File	Read more ► Microsoft: Wi-Fi Edit View Go Image: Comparison of the state of the s	Capture Analyze Stat	istics Telephony Wirele	ss Tools Help Protocol Length Info TLSv1.2 476 Appli SSL 352 Conti SSL 400 Conti TLSv1.2 135 Appli SSL 189 Conti TCP 60 443 → SSL 189 Conti TLSv1.2 369 Appli d (4064 bits) on interd	r m Spices R 00 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0
File	Read more ► Microsoft: Wi-Fi Edit View Go Image: Comparison of the state of the s	Capture Analyze Stat	istics Telephony Wireles	Protocol Length Info TLSv1.2 476 Appli SSL 352 Conti SSL 400 Conti TLSv1.2 135 Appli SSL 189 Conti TCP 60 443 + SSL 189 Conti TLSv1.2 369 Appli ed (4064 bits) on inter ts: Tp-LinkT_fb:a4:8f (1	<pre>cation Data nuation Data nuation Data Ref (754D9DA3-A200-486 41:6:9:4:8f)</pre>
File No.	Read more ► Microsoft: Wi-Fi Edit View Ime Ime 221 3.756673 223 3.754655 223 3.754655 223 3.821574 226 3.822070 227 3.822957 228 3.831437	Capture Analyze Stat	istics Telephony Wirelet	Protocol Length Info TLSv1.2 476 Appli SSL 352 Conti SSL 135 Appli SSL 189 Conti TLSv1.2 135 Appli SSL 189 Conti TLSv1.2 369 Appli sSt 189 Conti TLSv1.2 369 Appli ed (4064 bits) on intert st: TP-LinkT_fb:a4:sf (394.68.228 (4064.68.228)	<pre>cation Data nuation Data nuation Data nuation Data nuation Data fact \Device\NPF_(754D9DA3-A20D-4B6 44:e8:94:fb:a4:8f)</pre>
File	Read more ► Microsoft: Wi-Fi Edit View G Image: Comparison of the comparison of	Capture Analyze Stat	istics Telephony Wirelet	Protocol Length Info TLSv1.2 476 Appli SSL SSL 352 Conti SSL SSL 400 Conti TLSv1.2 TLSv1.2 135 Appli SSL SSL 189 Conti TCP TCP 60 443 + SSL SSL 189 Conti TLSv1.2 TLSv1.2 369 Appli SSL ed (4064 bits) on interf st: Tp-LinkT_fb:a4:8f (3) 94.68.228 8, Seq: 1, Ack: 1, Len: SSL	<pre>cation Data nuation Data cation Data nuation Data 8071 [ACK] Seq=4133 Ack=111 nuation Data cation Data 8071 [ACK] Seq=4133 Ack=111 nuation Data face \Device\NPF_(754D9DA3-A200-486 34:e8:94:fb:a4:8f) 454</pre>
File	Read more ► Microsoft: Wi-Fi Edit View Go Image: Ima	Capture Analyze Stat	istics Telephony Wirelet	Image: Source of the	<pre>cation Data nuation Data cation Data nuation Data 8071 [ACK] Seq=4133 Ack=111 nuation Data cation Data face \Device\NPF_{754D9DA3-A20D-486 34:e8:94:fb:a4:8f) 454</pre>
	Read more ► Microsoft: Wi-Fi Edit View Go © © © © © © © Tme 221 3.756673 222 3.752455 223 3.754695 224 3.754695 225 3.821574 226 3.822977 228 3.822957 228 3.831437 Frame 229: 508 byt Ethernet II, Src: Internet Protocol Transmission Contr Hypertext Transfer	Capture Analyze Stat	istics Telephony Wireles	Image: ss Tools Help Protocol Length Info TLSv1.2 476 Appli SSL 352 Conti SSL 352 Conti SSL 189 Conti TLSv1.2 135 Appli SSL 189 Conti TLSv1.2 369 Appli ed (4064 bits) on interf st: Tp-Linkr_fb:a4:8f (1994.68.228 9, Seq: 1, Ack: 1, Len:	<pre>cation Data nuation Data nuation Data nuation Data nuation Data s8071 [ACK] Seq=4133 Ack=111 nuation Data cation Data cat</pre>
	Read more ► Microsoft: Wi-Fi Edit View Go Image: Comparison of the state of the s	Capture Analyze Stat Source 192.168.1.99 192.168.1.99 192.168.1.99 192.168.1.99 192.168.1.99 192.168.1.99 81.19.104.67 82.145.216.16 81.19.104.67 82.145.216.16 tes on wire (4064 bi Tp-LinkT_08:f8:39 (Version 4, Src: 192 rol Protocol, Src Po Protocol	istics Telephony Wirele	ss Tools Help Protocol Length Info TLSv1.2 476 Appli SSL 352 Conti SSL 400 Conti TLSv1.2 135 Appli SSL 189 Conti TCP 60 443 → SSL 189 Conti TLSv1.2 369 Appli ed (4064 bits) on interf st: Tp-LinkT_fb:a4:8f (1) 94.68.228 0, Seq: 1, Ack: 1, Len:	<pre>cation Data nuation Data nuation Data cation Data s8071 [ACK] Seq=4133 Ack=111 nuation Data cation Data catio</pre>
File	Read more ► Microsoft: Wi-Fi Edit View Go Image: Comparison of the state of the s	Capture Analyze Stat Capture Analyze Stat Capture 192.168.1.99 192.	istics Telephony Wirele	ss Tools Help Protocol Length Info TLSv1.2 476 Appli SSL 352 Conti SSL 400 Conti TLSv1.2 135 Appli SSL 189 Conti TCP 60 443 → SSL 189 Conti TLSv1.2 369 Appli ed (4064 bits) on interf st: Tp-LinkT_fb:a4:8f (1 94.68.228 0, Seq: 1, Ack: 1, Len:	<pre>cation Data nuation Data cation Data nuation Data cation Data s8071 [ACK] Seq=4133 Ack=111 nuation Data cation Data catio</pre>
File No. > > > > > 0000 0010 0010	Read more ► Microsoft: Wi-Fi Edit View Go Image: Constraint of the state of the s	Capture Analyze Stat Source 192.168.1.99 192.168 193.168 192.168 192.168 193.168 1	istics Telephony Wirele	ss Tools Help Protocol Length Info TLSv1.2 476 Appli SSL 352 Conti SSL 400 Conti SSL 400 Conti TLSv1.2 135 Appli SSL 189 Conti TCP 60 443 → SSL 189 Conti TLSv1.2 369 Appli ed (4064 bits) on interf st: Tp-LinkT_fb:a4:8f (1 94.68.228 8, Seq: 1, Ack: 1, Len:	<pre>cation Data nuation Data nuation Data cation Data</pre>
File File No. > 1 > 2 > 1 > 2 000 001 002 002 003 004	Read more ► Microsoft: Wi-Fi Edit View Go Image: State Sta	Capture Analyze Stat Capture Analyze Stat Source 192.168.1.99 192.168.1.99 192.168.1.99 192.168.1.99 192.168.1.99 192.168.1.99 192.168.1.99 12.164.67 82.145.216.16 81.19.104.67 82.145.216.16 troid and a state of the sta	istics Telephony Wirele Telephony Wirele Destination 82.145.216.16 81.19.104.67 81.19.104.67 81.19.104.67 81.19.104.67 81.19.104.67 81.19.104.67 91.2168.1.99 192.168.1.99	Tools Help Protocol Length Info TLSv1.2 476 Appli SSL 352 Conti TLSv1.2 135 Appli SSL 189 Conti TLSv1.2 135 Appli SSL 189 Conti TLSv1.2 369 Appli ded (4064 bits) on interf t: Tp-LinkT_fb:a4:8f (1 94.68.228 0, Seq: 1, Ack: 1, Len:	<pre>cation Data nuation Data cation Data cation Data saving a state of the state o</pre>
File File No. > 1 > 2 > 1 > 2 0000 0010	Read more ► Microsoft: Wi-Fi Edit View Go Image: Comparison of the state of the	Capture Analyze Stat Capture Analyze Stat Capture Analyze Stat Source 192.168.1.99 192.168.1.	istics Telephony Wirele Telephony Wirele Destination 82.145.216.16 81.19.104.67 81.19.104.67 81.19.104.67 81.19.104.67 81.19.104.67 81.19.104.67 91.2168.1.99 192.168.1.99	Tools Help Protocol Length Info TLSv1.2 476 Appli SSL 352 Conti SSL 352 Conti TLSv1.2 135 Appli SSL 189 Conti TLSv1.2 369 Appli ded (4064 bits) on interf st: Tp-LinkT_fb:a4:8f (3 4.68.228 B, Seq: 1, Ack: 1, Len: """ ""	<pre>cation Data nuation Data cation Data Roy Seq=4133 Ack=111 nuation Data cation Data ca</pre>
File File File No. </th <th>Read more ► Microsoft: Wi-Fi Edit View Go Image: Construction of the state of the</th> <th>Capture Analyze Stat Capture Analyze Stat Capture Analyze Stat Source 192.168.1.99 192.168.1.</th> <th>istics Telephony Wirele Telephony Wirele Destination 82.145.216.16 81.19.104.67 81.19.104.67 81.19.104.67 81.19.104.67 81.19.104.67 81.19.104.67 91.2168.1.99 192.168.1.99</th> <th><pre>ss Tools Help Protocol Length Info TLSv1.2 476 Appli SSL 352 Conti SSL 400 Conti SSL 400 Conti TLSv1.2 135 Appli SSL 189 Conti TLSv1.2 369 Appli d (4064 bits) on interf st: Tp-LinkT_fb:a4:8f (: 94.68.228 B, Seq: 1, Ack: 1, Len: </pre></th> <th><pre>cation Data nuation Data nuation Data cation Data</pre></th>	Read more ► Microsoft: Wi-Fi Edit View Go Image: Construction of the state of the	Capture Analyze Stat Capture Analyze Stat Capture Analyze Stat Source 192.168.1.99 192.168.1.	istics Telephony Wirele Telephony Wirele Destination 82.145.216.16 81.19.104.67 81.19.104.67 81.19.104.67 81.19.104.67 81.19.104.67 81.19.104.67 91.2168.1.99 192.168.1.99	<pre>ss Tools Help Protocol Length Info TLSv1.2 476 Appli SSL 352 Conti SSL 400 Conti SSL 400 Conti TLSv1.2 135 Appli SSL 189 Conti TLSv1.2 369 Appli d (4064 bits) on interf st: Tp-LinkT_fb:a4:8f (: 94.68.228 B, Seq: 1, Ack: 1, Len: </pre>	<pre>cation Data nuation Data nuation Data cation Data</pre>
File File File No. </th <th>Read more ► Microsoft: Wi-Fi Edit View Go Image: Construction of the state of t</th> <th>Capture Analyze Stat Capture Analyze Stat Capture Analyze Stat Source 192.168.1.99 192.168.1.99 192.168.1.99 192.168.1.99 192.168.1.99 19.168.1.99</th> <th>istics Telephony Wirele Telephony Wir</th> <th>ss Tools Help Protocol Length Info TLSv1.2 476 Appli SSL 352 Conti SSL 352 Conti SSL 352 Conti SSL 189 Conti TLSv1.2 135 Appli SSL 189 Conti TLSv1.2 369 Appli continue 189 Conti TLSv1.2 369 Appli ed (4064 bits) on intert st: Tp-LinkT_fb:a4:8f (1994) 94.68.228 8, Seq: 1, Ack: 1, Len: Content Content Content Content Total Content TLSv1.2 SSL SSL SSL SSL SSL SSL 1, Ack: 1, Len: SSL SSL SSL TLSv1.2 TLSv1.2 SSL SSL SSL SSL SSL SSL SSL SS</th> <th><pre>cation Data nuation Data nuation Data cation Data</pre></th>	Read more ► Microsoft: Wi-Fi Edit View Go Image: Construction of the state of t	Capture Analyze Stat Capture Analyze Stat Capture Analyze Stat Source 192.168.1.99 192.168.1.99 192.168.1.99 192.168.1.99 192.168.1.99 19.168.1.99	istics Telephony Wirele Telephony Wir	ss Tools Help Protocol Length Info TLSv1.2 476 Appli SSL 352 Conti SSL 352 Conti SSL 352 Conti SSL 189 Conti TLSv1.2 135 Appli SSL 189 Conti TLSv1.2 369 Appli continue 189 Conti TLSv1.2 369 Appli ed (4064 bits) on intert st: Tp-LinkT_fb:a4:8f (1994) 94.68.228 8, Seq: 1, Ack: 1, Len: Content Content Content Content Total Content TLSv1.2 SSL SSL SSL SSL SSL SSL 1, Ack: 1, Len: SSL SSL SSL TLSv1.2 TLSv1.2 SSL SSL SSL SSL SSL SSL SSL SS	<pre>cation Data nuation Data nuation Data cation Data</pre>
File File No. > E > 1 > 2 000 001 002 003 004 005 006 007 008 009 009 009 009 009 009 009 009 009 009 009	Read more ► Microsoft: Wi-Fi Edit View Go Image: Second S	Capture Analyze Stat Capture Analyze Stat Source 192.168.1.99	istics Telephony Wirele Telephony Wirele Destination B2.145.216.16 81.19.104.67 81.19.104.67 81.19.104.67 81.19.104.67 81.19.104.67 81.19.104.67 91.2168.1.99 192.168.1.99	Image: Solution of the second secon	<pre>cation Data nuation Data cation Data Roy Less A data cation Data Roy Less A data cation Data cati</pre>

Etape 4 : examen des paquets capturés

Les données collectées par Wireshark sont affichées en trois sections :

- La section supérieure affiche la liste des trames PDU capturées avec un résumé des informations sur les paquets IP répertoriés,
- La section du milieu énumère les informations PDU pour la trame sélectionnée dans la partie supérieure de l'écran et détaille une trame PDU capturée selon les couches de protocole
- La section inférieure affiche les données brutes de chaque couche. Les données brutes sont affichées à la fois sous forme hexadécimale et décimale.

1 m 1																	
Microso	oft: WI-FI																~~~~
ile Edit	View	Go	Capture	Ana	lyze	Statistics	lele	phony	Wirele	ess lo	ols H	elp					
	•	610		۹ (⊨ ⇔	2 1	<u>*</u> =		Θ		墅						
Apply a d	lisplay filte	er <c< td=""><td>trl-/></td><td></td><td></td><td></td><td></td><td></td><td></td><td></td><td></td><td></td><td></td><td></td><td></td><td></td><td>• +</td></c<>	trl-/>														• +
	Time		Source	ce			Destina	tion		P	rotocol	Length	Info				^
221	3.75067	73	192.	168.1	.99		82.14	5.216	.16	Т	LSv1.2	476	5 Applicati	on Data			
222	3.75234	45	192.	168.1	.99		81.19	.104.	67	S	SL	352	2 Continuat	ion Data			
223	3.75426	55	192.	168.1	.99		81.19	.104.	67	S	SL	400	<pre>Ocontinuat</pre>	ion Data			
224	3.75460	95	192.	168.1	.99		82.14	5.216	.16	Т	LSv1.2	135	5 Applicati	on Data			_
225	3.82157	74	81.1	19.104	.67		192.1	68.1.	99	S	SL	189	9 Continuat	ion Data			_
226	3.82207	70	82.1	145.21	6.16		192.1	68.1.	99	т	CP	60	0 443 → 807	1 [ACK] 9	Seq=4133	Ack=111	
227	3.82295	57	81.1	19.104	.67		192.1	68.1.	99	S	SL	189	Ocontinuat	ion Data			
228	3.83143	37	82.1	145.21	6.16		192.1	68.1.	99	Т	LSv1.2	369	Application	on Data			~
_																>	
Transm Typert	et Prot ission ext Tra	Contro Contro Insfer	Versio ol Pro Proto	n 4, 9 tocol	Src: 1 , Src	192.168 Port:	.1.99 8072,	, Dst Dst	: 193.1 Port: 8	194.68 30, Se	,228 q: 1, /	Ack: 1	, Len: 454		4.01)		
iransm Hypert	et Prot ission ext Tra	cocol Contro insfer	Versio ol Pro Proto	n 4, 9 tocol	Src: 1 , Src	192.168 Port:	.1.99 8072,	, Dst Dst	: 193.1 Port: 8	JST: 1 194.68 30, Se	,228 q: 1, /	Ack: 1	, Len: 454				
Transm Hypert	et Prot ission ext Tra	cocol N Contro Insfer	Versio ol Pro Proto	n 4, 9 otocol	Src: 1	192.168 Port:	.1.99 8072,	, Dst Dst	: 193.1 Port: 8	JST: 1 194.68 30, Se	,228 q: 1, 4	Ack: 1	, Len: 454				1
Transm typert	ext Tra	Contro Contro Insfer	Versio ol Pro Proto 8f e8	on 4, stocol, ocol	5rc: 1 , Src	192.168 Port:	.1.99 8072,	, Dst Dst 45 0	2 4	JST: 1 L94.68 30, Se	.228 q: 1, /	Ack: 1	, Len: 454				2
iransm Hypert	et Prot ission ext Tra e8 94 ee 5d	fb a4	Versio ol Pro Proto 8f e8 00 80	94 f	5rc: 1 , Src 6 08 12 63	192.168 Port: f8 39 (c0 a8 (.1.99 8072, 808 00 80 00	, Dst Dst 45 00 c1 c2	2 ···]	194.68 30, Se	.228 q: 1, /	Ack: 1	, Len: 454				2
Transm Hypert 10 34 10 01 10 44	e8 94 ee 5d e4 1f	fb a4 f4 40 88 00	Versio pl Pro Proto 8f e8 00 80 50 f3	94 f 06 c 5e 8	5rc: 1 , Src 76 08 12 63 30 46	192.168 Port: f8 39 (c0 a8 (bc 21)	.1.99 8072, 8072, 08 00 01 63 f3 dc	45 0 c1 c 50 1	0 4	JST: 1 L94.68 30, Se 30, Se	.228 q: 1, /	E- P-	, Len: 454				>
ransm iypert	e8 94 ee 5d e4 1f 02 30	fb a4 f4 40 88 00 af 00	Versio pl Proto Proto 8f e8 00 80 50 f3 00 47	94 f 06 c 5e 8	5rc: 1 , Src , Src 6 08 12 63 30 46 54 20	f8 39 (c0 a8 (bc 21) 2f 20 4	.1.99 8072, 8072, 08 00 01 63 f3 dc 48 54	45 0 c1 c 50 1 54 50	0 4. 2] 8 D. 0 .0	194.68 30, Se	.228 q: 1, /	Ack: 1	, Len: 454				2
ransm iypert 0 0 34 0 01 0 44 0 02 0 2f	e8 94 ee 5d e4 1f 02 30 31 2e	fb a4 f4 40 af 00 31 0d 62	Versio pl Proto Proto 8f e8 00 80 50 f3 00 47 0a 48 61 2	94 f 06 c 5e 8 6f 7	6 08 6 2 63 6 46 64 20 73 74	f8 39 (c0 a8 (bc 21 1 2f 20 4 3a 20 (.1.99 8072, 8072, 08 00 01 63 f3 dc 48 54 63 73 73 04	45 00 c1 c2 50 12 54 50 2e 7	0 4 2] 8 D 00 5 /1.			E- P- TP	, Len: 454				3
ransm iypert 0 0 34 0 01 0 44 0 02 0 0 2f 0 0 6e 0 6e	e8 94 ee 5d e4 1f 02 30 31 2e 69 76	fb a4 f4 40 88 00 af 00 31 0d 2d 62 65 63	Versio pl Proto Proto 8f e8 00 80 50 f3 00 47 0a 48 61 74 74 69	94 f 06 c 5e 8 45 5 6f 7 6e 6	5rc: 1 , Src , Src 2 63 30 46 54 20 73 74 51 32	f8 39 0 c0 a8 0 bc 21 2f 20 4 3a 20 0 2e 64 2 29 6b	.1.99 8072,	45 0 c1 c 50 1 54 5 0 2e 7 0a 4	0 4 0 4 2] 8 D 0 .			E- F- F- F- F- F- F- F- F- F- F	, Len: 454				2
ransm iypert 0 0 34 0 01 0 44 0 02 0 0 2f 0 0 6e 0 0 6f 0 0 6f	e8 94 ee 5d e4 1f 02 30 31 2e 69 76 6e 6e 6c 69	fb a4 f4 40 88 00 af 00 31 0d 2d 62 65 63 76 65	Versio ol Proto Proto 8f e8 00 80 50 f3 00 47 0a 48 61 74 74 69 0d 0a	94 f 06 c 5e 8 6f 7 6e 6 6f 6	5rc: 1 , Src , Src 26 08 12 63 30 46 54 20 73 74 51 32 56 3a 70 67	f8 39 0 c0 a8 0 bc 21 2f 20 4 3a 20 0 2e 64 2 20 6b 0	.1.99 8072,	45 00 c1 c2 50 12 54 50 2e 79 0a 4 70 20 2d 40	0 4 0 4 0 2] 8 D 0	L94.68 30, Se 30, Se 0.0	.228 q: 1, / 	E- P- TP p- p- 	, Len: 454				>
ransm Hypert Hypert H 0 01 0 44 0 02 0 2f 0 0 6e 0 0 6f 0 0 61 0 0 61	e8 94 ee 5d ee 5d e4 1f 02 30 31 2e 69 76 6e 6e 6c 69 73 65	fb a4 fb a4 f4 40 88 00 af 00 31 0d 2d 62 65 63 76 65 63 75	Versio ol Proto Proto 8f e8 00 80 50 f3 00 47 0a 48 61 74 74 69 0d 0a 72 65	94 f 06 c 5e 8 6f 7 6e 6 6f 6 2d 5	5 c : 1 5 c	f8 39 (c0 a8 (bc 21) 2f 20 4 3a 20 (2e 64) 20 6b (72 61 (71 75 (.1.99 8072,	45 00 c1 c 54 50 c2e 7 0a 42 70 22 20 40 74 7	0 4 0 4 2] 8 D 00 5 /1. 3 niv d onn 9 ali 3 nse	1. Ho 	.228 q: 1, / q: 1, / .cc. F. ! T / HT st: cs a2.dz pgrade Reques	E- P- TP p- TP 	, Len: 454			_	>
Transm Hypert Hy	e8 94 ee 5d e4 1f 69 76 6e 6e 6c 69 73 65 20 31	fb a4 fb a4 f4 40 88 00 af 00 31 0d 2d 62 65 63 76 65 63 75 0d 0a	Versio ol Pro Proto 8f e8 00 80 50 f3 00 47 0a 48 61 74 74 69 0d 0a 72 65 55 73	94 f 96 f 58 8 45 5 66 6 55 7 24 5 65 7	5 c : 1 5 c : 2 5 c	f8 39 (c0 a8 (bc 21) 2f 20 (2e 64) 20 6b (72 61 (71 75 (41 67 (.1.99 8072,	45 00 c1 c2 50 10 54 50 00 4 70 2 2d 47 77 3	0 4 0 4 2] 8 D 0 0 0 0 0 0 0 0 0 0 0 0 1 1 1 1 2] 8 D 0 0 1 .	251: 1 194.68 30, Se 30, Se	····9·································	E- 	4.00 (34.00				>
Transm Hypert Hy	e8 94 ee 5d e4 1f 62 30 31 2e 69 76 6c 69 73 65 20 31 4d 6f	fb a4 f4 40 88 00 31 0d 2d 62 65 63 76 65 0d 0a 7a 69	Versio ol Pro Proto 8f e8 00 80 50 f3 00 47 0a 48 61 74 74 69 0d 0a 72 65 55 73 6c 6c	94 f 94 f 96 d 5e 8 45 5 6f 7 6e 6 6f 7 2d 5 55 7 61 2	5rc: 1 , Src , Sr	f8 39 0 c0 a8 0 bc 21 2 f2 20 4 26 4 20 6b 7 2 61 0 71 75 0 41 67 0 2 2 30 2	.1.99 8072,	45 00 cl cl cl 50 11 54 50 2e 7 0a 44 70 2 2d 44 74 7 57 6	0 4 Port: 8 0 4 2] 8 D 0 0 0 0 0 1 1 1 1 1 2] 8 D 0 0 1	251: 1 194.68 30, Se 30, Se 30, Se 30, Se 20, Se		E· P· TP P· TP Wi	4.00 (34.00				>

a. Appliquer un filtre pour n'afficher que les messages http. Taper http dans la case *Filtre* en haut de Wireshark et appuyez sur *Entrée*

																																_
4 *M	licroso	oft: V	Vi-Fi																									(-			8
File	Edit	Vie	ew	Go		Cap	ture	A	nalyz	e	Stat	stic	s	Tele	pho	ny	Wire	eless	Т	ols	Hel	р										
	l Ø	۲				×	C	٩	æ	۲	2	Ŷ					€.	Q		₩.												
htt	p																												X		•	÷
No.		Time				s	ourc	e					De	stina	tion				P	rotoco	al I	ength	Info									^
T* 1	1387	8.3	2013	30		1	92.	168	.1.9	9			19	3.1	94.	68.	228		H	ITTP		703	GET	1 1	ITTP,	/1.1						
- 1	1543	8.8	6909	99		1	93.	194	.68.	228			19	2.1	68.	1.9	9		H	ITTP		333	HTT	P/1.	1 20	00 0	к	(te)	kt/h	tml)		
+ 1	1569	8.9	5744	14		1	92.	168	.1.9	9			19	3.1	94.	68.	228		H	ITTP		680	GET	/si	tes	/def	ault	t/fi	iles	/css		
1	1628	10.	0748	374		1	93.	194	.68.	228			19	2.1	68.	1.9	9		H	ITTP		982	нтт	P/1.	1 20	00 0	к	(te)	kt/c	:ss)		
1	1701	10.	1361	161		1	92.	168	.1.9	9			19	3.1	94.	68.	228		H	ITTP		781	GET	/pr	ofi	les/	oper	isch	nola	ar/th		
1 1	1702	10.	1367	747		1	92.	168	.1.9	9			19	3.1	94.	68.	228		H	ITTP		787	GET	/pr	ofi	les	oper	nsch	nola	ar/th		
1	1703	10.	1369	962		1	92.	168	.1.9	9			19	3.1	94.	68.	228		H	ITTP		778	GET	/pr	ofi	les	oper	nsch	nola	ar/th		
							~~			~					~ •											•			•			
•																																_
> Tr > Hy	pert	ext	Tra	Cor	fer	Pro	oto	col	ol,	Src	Por	't:	13	782	, D	st F	Port	: 80	, S	eq: :	1, 4	Ack:	ι, ι	en:	649							
<																																>
0000	34	e8	94	fb	a4	8f	e8	94	f6	08	f8	39	08	00	45	00	4			9) - · E											^
0010	02	b1	9b	29	40	00	80	06	94	6b	c0	a8	01	63	c1	c2	-)@		·k··	· c ·											
0020	44	e4	35	d6	00	50	a4	9d	0e	0c	7c	dd	24	Зb	50	18	D	5	.		\$;P	-										
0030	02	02	4b	85	00	00	47	45	54	20	2f	20	48	54	54	50		٠K	GE	т/	HTT	P										
0040	2f	31	2e	31	Ød	0a	48	6f	73	74	3a	20	63	73	2e	75	/1	1.1	Но	st:	cs.	u										
0050	6e	69	76	2d	62	61	74	6e	61	32	2e	64	7a	Ød	0a	43	n	iv-b	atn	a2.0	z	C										
0060	6f	6e	бе	65	63	74	69	6f	6e	3a	20	6b	65	65	70	2d	or	nnec	tio	n: k	ceep	-										
0070	61	50	69	/6	55	00	0a	55	70	67	72	61	64	65	20	49	a.	live		pgra	ade-	1										
0800	6e	13	21	63	15	/2	05	20	52	24	/1	15	65	13	74	/3	n	secu	re-	кери	lest	s										
0090	28	20	31	ou	oa	22	13	00	12	20	41	07	00	06	14	20	-	1	se	r-Ag	sent	•										~
•	× ,	iresh	hark	Wi-F	FISEL).pca	png													Pac	kets: 3	158 -	Displa	aved:	18 (0.6%		Prof	file: De	fault	

b. Cliquer sur la première trame de requête http dans la section supérieure de Wireshark. Remarquez que la colonne *Source* contient l'adresse IP de votre PC, et la colonne *Destination* contient l'adresse IP site *cs.univ-batna2.dz.*

	*Micros	oft: Wi-Fi					
F	ile Edit	View Go	Capture Analyze Statistic	cs Telephony Wireless	Tools H	Help	
1	(🔳 🖉	0 💽 📑	🗙 🖆 । ९ 👄 🔿 鼞 🗿	§ 👲 📃 📃 🔍 Q 🖉			
	http					+	
No	.	Time	Source	Destination	Protocol	Length Info	^
-	1387	8.320130	192.168.1.99	193.194.68.228	HTTP	703 GET / HTTP/1.1	
4	1543	8.869099	193.194.68.228	192.168.1.99	HTTP	333 HTTP/1.1 200 OK (text/html)	
+	1569	8.957444	192.168.1.99	193.194.68.228	HTTP	680 GET /sites/default/files/css	
	1628	10.074874	193.194.68.228	192.168.1.99	HTTP	982 HTTP/1.1 200 OK (text/css)	
	1701	10.136161	192.168.1.99	193.194.68.228	HTTP	781 GET /profiles/openscholar/th	
	1702	10.136747	192.168.1.99	193.194.68.228	HTTP	787 GET /profiles/openscholar/th	
	1703	10.136962	192.168.1.99	193.194.68.228	HTTP	778 GET /profiles/openscholar/th	~
4	1701		*** *** * **	102 101 62 000			

c. La trame étant toujours sélectionnée dans la partie supérieure, passer à la partie centrale et cliquer sur le signe « plus » (+) à gauche de la ligne *Hypertext Transfer Protocol*, pour afficher la requête http.



 e. Cliquez sur la deuxième trame dans la section supérieure de Wireshark. Cette trame représente une réponse http, la colonne Destination contient l'adresse IP du site cs.univ-batna2.dz. La colonne Source contient l'adresse IP de votre PC.

📕 ht	tp-capture.pcapng					
File	Edit View Go	Capture Analyze Statis	tics Telephony Wirele	s Tools H	lelp	
1		🗙 🛅 🍳 👄 👄 🚭	₩	Q II		
				· -•		
	τφ					
No.	Time	Source	Destination	Protocol	Length Info	^
_*	1387 8.320130	192.168.1.99	193.194.68.228	HTTP	703 GET / HTTP/1.1	
-	1543 8.869099	193.194.68.228	192.168.1.99	HTTP	333 HTTP/1.1 200 OK (te	xt/html)
†	1569 8.957444	192.168.1.99	193.194.68.228	HTTP	680 GET /sites/default/f	iles/css/cs
t –	1628 10.074874	193.194.68.228	192.168.1.99	HTTP	982 HTTP/1.1 200 OK (te	xt/css)
	1701 10.136161	192.168.1.99	193.194.68.228	HTTP	781 GET /profiles/opensc	holar/theme∨
<						>
> Ir > Tr > [: > Hy > Li	nternet Protocol ransmission Contr 20 Reassembled TC ypertext Transfer ine-based text da html	Version 4, Src: 193. col Protocol, Src Por P Segments (26879 by Protocol tta: text/html (281 l \n	194.68.228, Dst: 192 t: 80, Dst Port: 137 tes): #1494(1400), # ines)	.168.1.99 32, Seq: 26 1495(1400),	601, Ack: 650, Len: 279 #1497(1400), #1498(1400), #	#1500(1400), #1
	<pre><?if lteHobII <![if lte IE
<![if (IE 7)&
<![if IE 8?>< <?if (gte IE <head>\n <meta """"""""""""""""""""""""""""""""""<="" charset="utf-8" td=""/><td><pre>c);</pre>/c) Class= let c);</td></head></pre> /c) Class="lt-id (!IEMobile)?>/chml class="lt-ide" 9) (gt IEMobile 7)] utf-8" />\n	<pre>c);</pre> /c) Class= let c);	<pre>#/ lang= en ulr= e9 lt-ie8 lt-ie7" l lass="lt-ie9 lt-ie8" lang="en" dir="ltr" ><!----><html <="" lang="en" pre=""></html></pre>	ing="en" di lang="en" dir="ltr 	l]>\n dir="ltr"> endif? \n dir="ltr"> endif? \n ->\n "> <![endif] \n	
/	<meta content="Ope</th><th>nScholar for Drupal</th><th>(http://t</th><th>heopenscholar.org)" name="gen</th><th>erator"/> \n	Ň				
•						
0000	e8 94 f6 08 f8	39 34 e8 94 fb a4 1	Sf 08 00 45 00 ····	.94	• E •	^
0010	01 57 44 01 40	d6 7c dd 8c 23 a4 0		@	. D.	
0030	01 10 18 d1 00	00 74 74 70 3a 2f	of 63 73 2e 75	tt n://c	5.0	
0040	6e 69 76 2d 62	61 74 6e 61 32 2e	54 7a 2f 73 69 niv	bath a2.dz	/si	
0050	74 65 73 2f 64	65 66 61 75 6c 74	2f 66 69 6c 65 tes	defa ult/f	ile	
0060	73 2f 6a 73 2f	6a 73 5f 64 6f 51	37 4b 4f 64 37 s/j	/js_ doQ7K	0d7	
0070	4c 32 34 66 74	64 55 54 4e 63 55 4	47 34 44 58 72 L24	tdUT NcUG4	DXr	
0080	74 53 43 6c 41	38 54 65 57 52 47	78 62 48 7a 47 tSC	A8Te WRGxb	HzG	
0090	36 65 41 2e 6a	73 3f 6d 3d 31 36	30 36 30 34 35 6eA	js?m =1606	045	
00a0	34 35 38 22 3e	3c 2f 73 63 72 69	70 74 3e 0a 3c 458	> <td>>.<</td> <td>~</td>	>.<	~
Fram	ne (333 bytes) Reas	sembled TCP (26879 bytes)	De-chunked entity body (2	5767 bytes)		
•	Hypertext Transfe	r Protocol: Protocol			Packets: 3158 • Displayed: 18 (0.6%)	Profile: Default

>	HTTP/1.1 200 OK/r/n
	Server: NBINX/1.15.0/r/N
	Date: Suit, do Dec 2000 17:01:05 GH (1/1)
	Connect in tearing, chained in the
	X-Powered-By: PHP/5.6.40\r\n
	Expires: Sun, 19 Nov 1978 05:00:00 GMT\r\n
	Cache-Control: no-cache, must-revalidate\r\n
	X-Content-Type-Options: nosniff/r/n
	Access-Control-Allow-Origin: *\r\n
	Access-Control-Allow-Credentials: true\r\n
	Access-Control-Allow-Headers: Authorization, access-token\r\n
	Content-Language: en\r\n
	X-Frame-Options: SAMEORIGIN\r\n
	<pre>x-drupal-cache-os-boxes-plugin: os_boxes_html,os_boxes_html,os_sv_list_box,os_slideshow_box,os_boxes_html,os_boxes_html,os_b [truncated]x-drupal-cache-os-boxes-cache-id: os_boxes_cache:45:hwp_personal_contact_html:0,os_boxes_cache:45:1512901820:0,o</pre>
	X-Generator: OpenScholar for Drupal 7 (http://theopenscholar.org)\r\n
	Link: <http: cs.univ-batna2.dz="" home="">; rel="canonical",<http: cs.univ-batna2.dz="" home="">; rel="shortlink"\r\n</http:></http:>
	[HTTP response 1/3]
	[lime since request: 0.548969000 seconds]
	[Request in Trame: 1567]
	[Next response in frame: 102]
	<pre>Image responds in rooms, ison and include a second and include a second and include a second a se</pre>
	<pre><?If (If /)&(!Lewobile)?><html class="it-ley" it-le<="" it-ley="" th=""></html></pre>
	<pre>k type="text/css" rel="stylesheet" href="http://cs.univ-batna2.dz/sites/default/files/css/css_raUrXnSCPh_IEA-481GCsCEM8L</pre> Répondre aux questions suivantes : Oue signifie la valeur 200 ?
	Ouel serveur est responsable de fournir la rénonse bttp ?
	Commont la corne de la rénonce http est il cénaré de con en tête 2
	Quel est le type des données renyoyées par le serveur dans le corps de la réponse http?