

Travaux Dirigés

Etude d'échanges entre machines, protocoles, couches et encapsulation

Observez la capture de trafic ci-dessous faite avec Wireshark (en amphi Ensimag, par une connexion Wifi).

Longueur d'en-tête Ethernet (couche 2) : 14 octets. Le type associé à IP est 0x0800

0	5	6	11	12	13
Adresse MAC Dest	Adresse MAC Src	Type Prot encapsulé			

Longueur d'en-tête IP(v4) : 20 octets (sans options) ; se termine par Adresse IP Source (4 octets) puis Adresse IP Destination (4 octets).

Wireshark 1.6.5 (SVN Rev 40429 from /trunk-1.6)

Filter: Expression... Clear Apply

No.	Time	Source	Destination	Protocol	Info
5	0.028187	130.190.123.77	193.54.188.33	DNS	Standard query A www.ensimag.fr
6	0.029449	193.54.188.33	130.190.123.77	DNS	Standard query response CNAME www-ensimag.imag.fr CNAME w
7	4.160316	130.190.123.77	195.221.228.24	TCP	50064 > http [SYN] Seq=0 Win=65535 Len=0 MSS=1460 WS=8 TS
8	4.164126	195.221.228.24	130.190.123.77	TCP	http > 50064 [SYN, ACK] Seq=0 Ack=1 Win=5792 Len=0 MSS=14
9	4.164252	130.190.123.77	195.221.228.24	TCP	50064 > http [ACK] Seq=1 Ack=1 Win=524280 Len=0 TSval=625
10	4.164383	130.190.123.77	195.221.228.24	HTTP	GET / HTTP/1.1
11	4.165886	195.221.228.24	130.190.123.77	TCP	http > 50064 [ACK] Seq=1 Ack=496 Win=6912 Len=0 TSval=847
12	4.166390	195.221.228.24	130.190.123.77	HTTP	HTTP/1.1 304 Not Modified
13	4.166431	130.190.123.77	195.221.228.24	TCP	50064 > http [ACK] Seq=496 Ack=151 Win=524280 Len=0 TSval:
14	4.166444	195.221.228.24	130.190.123.77	TCP	http > 50064 [FIN, ACK] Seq=151 Ack=496 Win=6912 Len=0 TS
15	4.166460	130.190.123.77	195.221.228.24	TCP	50064 > http [ACK] Seq=496 Ack=152 Win=524280 Len=0 TSval:
16	4.166599	130.190.123.77	195.221.228.24	TCP	50064 > http [FIN, ACK] Seq=496 Ack=152 Win=524280 Len=0
17	4.167799	195.221.228.24	130.190.123.77	TCP	http > 50064 [ACK] Seq=152 Ack=497 Win=6912 Len=0 TSval=8
18	4.174833	130.190.123.77	195.221.228.24	TCP	50065 > http [SYN] Seq=0 Win=65535 Len=0 MSS=1460 WS=8 TS
19	4.175861	195.221.228.24	130.190.123.77	TCP	http > 50065 [SYN, ACK] Seq=0 Ack=1 Win=5792 Len=0 MSS=14
20	4.175919	130.190.123.77	195.221.228.24	TCP	50065 > http [ACK] Seq=1 Ack=1 Win=524280 Len=0 TSval=625

Frame 10: 561 bytes on wire (4488 bits), 561 bytes captured (4488 bits)

Ethernet II, Src: Apple_20:c4:b0 (b8:8d:12:20:c4:b0), Dst: Cisco_da:22:80 (00:25:84:da:22:80)

Internet Protocol Version 4, Src: 130.190.123.77 (130.190.123.77), Dst: 195.221.228.24 (195.221.228.24)

Transmission Control Protocol, Src Port: 50064 (50064), Dst Port: http (80), Seq: 1, Ack: 1, Len: 495

Hypertext Transfer Protocol

0000 00 25 84 da 22 80 b8 8d 12 20 c4 b0 08 00 45 00 .%. "...E.

0010 02 23 8a 14 40 00 40 06 08 bf 82 be 7b 4d c3 dd .#..@.@.{M..

0020 e4 18 c3 90 00 50 37 b8 bc 7f 1e 2c e9 3b 80 18P7. .w.,;..

0030 ff ff 83 b5 00 00 01 01 0c 0a 25 41 ca ef 00 81 %A....

0040 5d 9f 47 45 54 20 2f 20 48 54 54 50 2f 31 2e 31].GET / HTTP/1.1

0050 0d 0a 48 6f 73 74 3a 20 77 65 62 2e 65 6e 73 69 ..Host: web.ensi

0060 6d 61 67 2e 66 72 0d 0a 55 73 65 72 2d 41 67 65 mag.fr.. User-Age

0070 6a 71 3a 20 4d 6f 7a 69 6c 6c 61 2f 35 2a 30 20 nt: Mozilla/5.0

File: "/Users/groz/... Packets: 78 Displayed: 78 Marked: 0 Load time: 0:00.078

Diagramme de couches (statique)

Question 1. Repérez les machines (hôtes) qui interviennent dans les échanges capturés. Pour chaque machine impliquée, identifiez les protocoles qu'elle a utilisés dans cet échange. Puis dessinez l'empilement des couches avec les protocoles présents (et utilisés par la machine dans l'échange) dans chaque couche.

Diagramme temporel (dynamique)

Question 2. Tracez autant de lignes de vie parallèles que nécessaire et représentez les échanges ci-dessus sur un diagramme temporel.

Question 3. Expliquez en français les phases du dialogue telles que vous pouvez les observer sur cette succession de 16 messages.

Analyse d'en-tête UDP

On s'intéresse maintenant au contenu de l'en-tête du PDU UDP dans lequel est encapsulée la requête DNS initiale (trame 3). Les octets surlignés sont ceux de l'en-tête IP.

Wireshark 1.6.5 (SVN Rev 40429 from /trunk-1.6)

Filter: Expression... Clear Apply

No.	Time	Source	Destination	Protocol	Info
3	0.004187	130.190.123.77	193.54.188.33	DNS	Standard query A web.ensimag.fr
4	0.007218	193.54.188.33	130.190.123.77	DNS	Standard query response CNAME web-ensimag.imag.fr A 195.22
5	0.028187	130.190.123.77	193.54.188.33	DNS	Standard query A www.ensimag.fr
6	0.029449	193.54.188.33	130.190.123.77	DNS	Standard query response CNAME www-ensimag.imag.fr CNAME we
7	4.160316	130.190.123.77	195.231.228.34	TCP	50064 → http [SYN] Seq=0 Win=65535 Len=0 MSS=1460 WS=8 TS=

Frame 3: 74 bytes on wire (592 bits), 74 bytes captured (592 bits)

Ethernet II, Src: Apple_20:c4:b0 (b8:8d:12:20:c4:b0), Dst: Cisco_da:22:80 (00:25:84:da:22:80)

Internet Protocol Version 4, Src: 130.190.123.77 (130.190.123.77), Dst: 193.54.188.33 (193.54.188.33)

User Datagram Protocol, Src Port: 50522 (50522), Dst Port: domain (53)

Source port: 50522 (50522)

Destination port: domain (53)

Length: 40

Checksum: 0x0157 [correct]

Domain Name System (query)

[Response In: 4]

Transaction ID: 0x9e63

Flags: 0x0100 (Standard query)

Questions: 1

Answer RRs: 0

Authority RRs: 0

Additional RRs: 0

Queries

web.ensimag.fr: type A, class IN

Name: web.ensimag.fr

Type: A (Host address)

Class: IN (0x0001)

0000 00 25 84 da 22 80 b8 8d 12 20 c4 b0 08 00 45 00E.
0010 00 3c 85 1d 00 00 ff 11 bb 2f 82 be 7b 4d c1 36 .<...../..{M.6
0020 bc 21 c5 5a 00 35 00 28 01 57 9e 63 01 00 00 01 ..Z.5.(.W.c....
0030 00 00 00 00 00 00 03 77 65 62 07 65 6e 73 69 6dw eb.ensim
0040 61 67 02 66 72 00 00 01 00 01 ag.fr... ..

Internet Protocol V... : Packets: 78 Displayed: 78 Marked: 0 Load time: 0:00.079

Question 4. Quelle est la longueur de l'en-tête UDP ?

Question 5. Où apparaît dans la trame le port source (50522) ? Convertissez 53 et 50522 en hexadécimal (aucun calcul n'est nécessaire).

Question 6. Wireshark a décodé dans cet en-tête une longueur de 40 (en décimal). Où apparaît cette longueur dans la trame ? Que mesure-t-elle ?

Question 7. Comment Wireshark sait-il où finit l'en-tête UDP et où commence la requête DNS ?