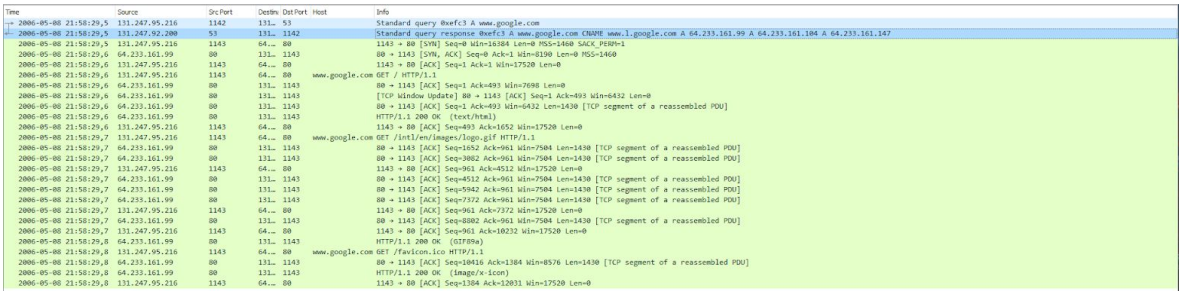
TP4 :

Exercice 1 :

Open “Exercise One.pcap”, you should see 26 packets listed



Time	Source	Src Port	Destin	Dst Port	Host	Info
2006-05-08 21:58:29,5	131.247.95.216	1142	131…	53		Standard query 0xefc3 A www.google.com
2006-05-08 21:58:29,5	131.247.92.200	53	131…	1142		Standard query response 0xefc3 A www.google.com CNAME www.l.google.com A 64.233.161.99 A 64.233.161.104 A 64.233.161.147
2006-05-08 21:58:29,5	131.247.95.216	1143	64.…	80		1143 → 80 [SYN] Seq=0 Win=16384 Len=0 MSS=1460 SACK_PERM=1
2006-05-08 21:58:29,6	64.233.161.99	80	131…	1143		80 → 1143 [SYN, ACK] Seq=0 Ack=1 Win=8190 Len=0 MSS=1460
2006-05-08 21:58:29,6	131.247.95.216	1143	64.…	80		1143 → 80 [ACK] Seq=1 Ack=1 Win=17520 Len=0
2006-05-08 21:58:29,6	131.247.95.216	1143	64.…	80	www.google.com	GET / HTTP/1.1
2006-05-08 21:58:29,6	64.233.161.99	80	131…	1143		80 → 1143 [ACK] Seq=1 Ack=493 Win=7698 Len=0
2006-05-08 21:58:29,6	64.233.161.99	80	131…	1143		[TCP Window Update] 80 → 1143 [ACK] Seq=1 Ack=493 Win=6432 Len=0
2006-05-08 21:58:29,6	64.233.161.99	80	131…	1143		80 → 1143 [ACK] Seq=1 Ack=493 Win=6432 Len=1430 [TCP segment of a reassembled PDU]
2006-05-08 21:58:29,6	64.233.161.99	80	131…	1143		HTTP/1.1 200 OK (text/html)
2006-05-08 21:58:29,6	131.247.95.216	1143	64.…	80		1143 → 80 [ACK] Seq=493 Ack=1652 Win=17520 Len=0
2006-05-08 21:58:29,7	131.247.95.216	1143	64.…	80	www.google.com	GET /intl/en/images/logo.gif HTTP/1.1
2006-05-08 21:58:29,7	64.233.161.99	80	131…	1143		80 → 1143 [ACK] Seq=1652 Ack=961 Win=7504 Len=1430 [TCP segment of a reassembled PDU]
2006-05-08 21:58:29,7	64.233.161.99	80	131…	1143		80 → 1143 [ACK] Seq=3082 Ack=961 Win=7504 Len=1430 [TCP segment of a reassembled PDU]
2006-05-08 21:58:29,7	131.247.95.216	1143	64.…	80		1143 → 80 [ACK] Seq=961 Ack=4512 Win=17520 Len=0
2006-05-08 21:58:29,7	64.233.161.99	80	131…	1143		80 → 1143 [ACK] Seq=4512 Ack=961 Win=7504 Len=1430 [TCP segment of a reassembled PDU]
2006-05-08 21:58:29,7	64.233.161.99	80	131…	1143		80 → 1143 [ACK] Seq=5942 Ack=961 Win=7504 Len=1430 [TCP segment of a reassembled PDU]
2006-05-08 21:58:29,7	64.233.161.99	80	131…	1143		80 → 1143 [ACK] Seq=7372 Ack=961 Win=7504 Len=1430 [TCP segment of a reassembled PDU]
2006-05-08 21:58:29,7	131.247.95.216	1143	64.…	80		1143 → 80 [ACK] Seq=961 Ack=7372 Win=17520 Len=0
2006-05-08 21:58:29,7	64.233.161.99	80	131…	1143		80 → 1143 [ACK] Seq=8802 Ack=961 Win=7504 Len=1430 [TCP segment of a reassembled PDU]
2006-05-08 21:58:29,7	131.247.95.216	1143	64.…	80		1143 → 80 [ACK] Seq=961 Ack=10232 Win=17520 Len=0
2006-05-08 21:58:29,8	64.233.161.99	80	131…	1143		HTTP/1.1 200 OK (GIF89a)
2006-05-08 21:58:29,8	131.247.95.216	1143	64.…	80	www.google.com	GET /favicon.ico HTTP/1.1
2006-05-08 21:58:29,8	64.233.161.99	80	131…	1143		80 → 1143 [ACK] Seq=10416 Ack=1384 Win=8576 Len=1430 [TCP segment of a reassembled PDU]
2006-05-08 21:58:29,8	64.233.161.99	80	131…	1143		HTTP/1.1 200 OK (image/x-icon)
2006-05-08 21:58:29,8	131.247.95.216	1143	64.…	80		1143 → 80 [ACK] Seq=1384 Ack=12031 Win=17520 Len=0

What is the IP address of the client that initiates the conversation?

The IP address of the client that initiates the conversation is 131.247.95.216

Use the first two packets to identify the server that is going to be contacted. List the common name, and three IP addresses that can be used for the server.

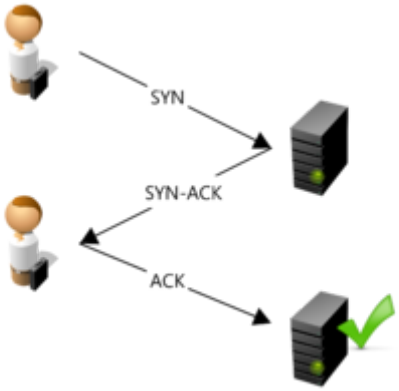
The common name is www.l.google.com
The ip address can be use are :
64.233.161.99
64.233.161.104
64.233.161.147

What is happening in frames 3, 4, and 5?

It’s the Three-way handshake :

In frame 3 , the client who wishes to establish a connection with a server will send a first SYN (synchronized) packet to the server. The sequence number of this packet is a random number A
In frame 4 ,the server will respond to the client using a SYN-ACK (synchronize, acknowledge) packet. The ACK number is equal to the sequence number of the previous packet (SYN) incremented by one (A + 1) while the sequence number of the SYN-ACK packet is a random number B.

In frame 5 , Finally, the client will send an ACK packet to the server which will serve as an acknowledgment. The acknowledgment number of this packet is defined according to the sequence number received previously (for example: A + 1) and the ACK number is equal to the sequence number of the previous packet (SYN-ACK) incremented by one (B + 1).



What is happening in frames 6 and 7?

In frame 6 , the user sends the request and in frame 7 it's the acknowledgement of receipt .

What is happening in frames nine and ten? How are these two frames related?

In frame 9, the server found the url and in frame 10 , the server gave the answer.
Their are linked because the frame 9 is the acknowledgment of receipt of the frame 10

What happens in packet 11?

Packet 11 is the acknowledge to the packets received in frame 10

After the initial set of packets is received, the client sends out a new request in packet 12. This occurs automatically without any action by the user. Why does this occur?

The requested URI contains the image file that the server did not send in Image 10 in text format. Therefore, the client will automatically request the image in another package.

What is occurring in packets 13 through 22?

Packet 13 is acknowledge to packet 12.
For packets 14 to 21 are requests and acknowledge relate by the requested image file.
The image file that is finally sent to the client in package 22.

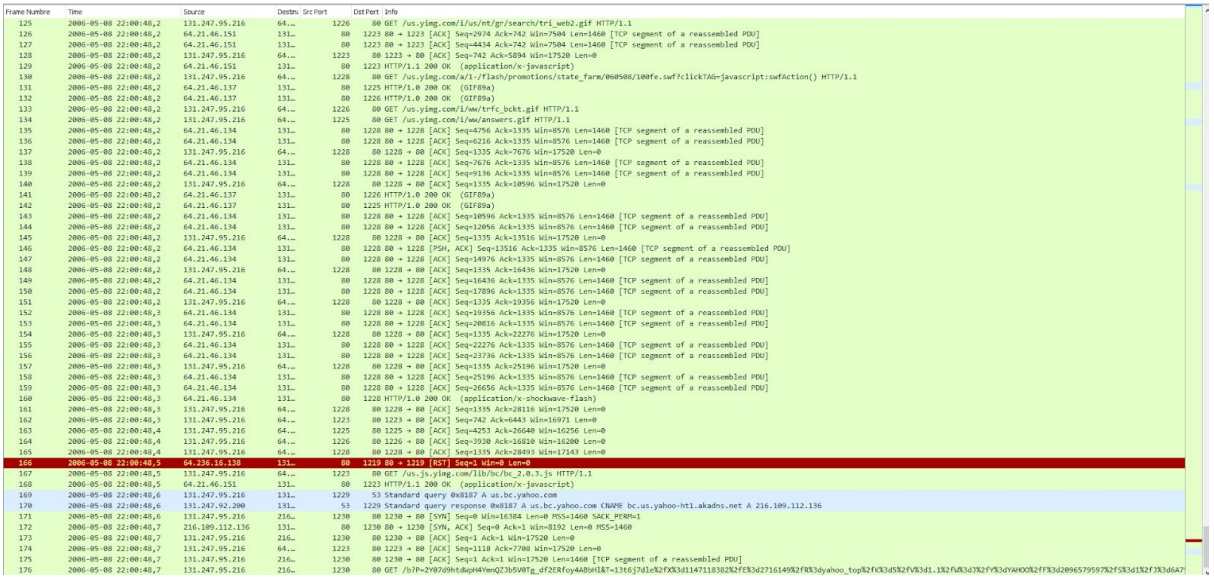
Explain what happens in packets 23 through 26.

The frame 23 is an automatic request sent by the client
In the frame 24 is the acknowledge to frame 23 as usual
At the grame 25, it contains the image file requested by client.
For frame 26 is the acknowledge for received packet in frame 25.

In one sentence describe what the user was doing

The user access to www.google.com

Exercice 2 :



Frame Numbre	Time	Source	Destin	Src Port	Dst Port	Info
125	2006-05-08 22:00:48,2	131.247.95.216	64.…	1226	80	GET /us.yimg.com/i/us/nt/gr/search/tri_web2.gif HTTP/1.1
126	2006-05-08 22:00:48,2	64.21.46.151	131.…	80	1223	80 → 1223 [ACK] Seq=2974 Ack=742 Win=7504 Len=1460 [TCP segment of a reassembled PDU]
127	2006-05-08 22:00:48,2	64.21.46.151	131.…	80	1223	80 → 1223 [ACK] Seq=4434 Ack=742 Win=7504 Len=1460 [TCP segment of a reassembled PDU]
128	2006-05-08 22:00:48,2	131.247.95.216	64.…	1223	80	1223 → 80 [ACK] Seq=742 Ack=5894 Win=17520 Len=0
129	2006-05-08 22:00:48,2	64.21.46.151	131.…	80	1223	HTTP/1.1 200 OK (application/x-javascript)
130	2006-05-08 22:00:48,2	131.247.95.216	64.…	1228	80	GET /us.yimg.com/a/1-/flash/promotions/state_farm/060508/100fe.swf?clickTAG=javascript:swfAction() HTTP/1.1
131	2006-05-08 22:00:48,2	64.21.46.137	131.…	80	1225	HTTP/1.0 200 OK (GIF89a)
132	2006-05-08 22:00:48,2	64.21.46.137	131.…	80	1226	HTTP/1.0 200 OK (GIF89a)
133	2006-05-08 22:00:48,2	131.247.95.216	64.…	1226	80	GET /us.yimg.com/i/ww/trfc_bckt.gif HTTP/1.1
134	2006-05-08 22:00:48,2	131.247.95.216	64.…	1225	80	GET /us.yimg.com/i/ww/answers.gif HTTP/1.1
135	2006-05-08 22:00:48,2	64.21.46.134	131.…	80	1228	80 → 1228 [ACK] Seq=4756 Ack=1335 Win=8576 Len=1460 [TCP segment of a reassembled PDU]
136	2006-05-08 22:00:48,2	64.21.46.134	131.…	80	1228	80 → 1228 [ACK] Seq=6216 Ack=1335 Win=8576 Len=1460 [TCP segment of a reassembled PDU]
137	2006-05-08 22:00:48,2	131.247.95.216	64.…	1228	80	1228 → 80 [ACK] Seq=1335 Ack=7676 Win=17520 Len=0
138	2006-05-08 22:00:48,2	64.21.46.134	131.…	80	1228	80 → 1228 [ACK] Seq=7676 Ack=1335 Win=8576 Len=1460 [TCP segment of a reassembled PDU]
139	2006-05-08 22:00:48,2	64.21.46.134	131.…	80	1228	80 → 1228 [ACK] Seq=9136 Ack=1335 Win=8576 Len=1460 [TCP segment of a reassembled PDU]
140	2006-05-08 22:00:48,2	131.247.95.216	64.…	1228	80	1228 → 80 [ACK] Seq=1335 Ack=10596 Win=17520 Len=0
141	2006-05-08 22:00:48,2	64.21.46.137	131.…	80	1226	HTTP/1.0 200 OK (GIF89a)
142	2006-05-08 22:00:48,2	64.21.46.137	131.…	80	1225	HTTP/1.0 200 OK (GIF89a)
143	2006-05-08 22:00:48,2	64.21.46.134	131.…	80	1228	80 → 1228 [ACK] Seq=10596 Ack=1335 Win=8576 Len=1460 [TCP segment of a reassembled PDU]
144	2006-05-08 22:00:48,2	64.21.46.134	131.…	80	1228	80 → 1228 [ACK] Seq=12056 Ack=1335 Win=8576 Len=1460 [TCP segment of a reassembled PDU]
145	2006-05-08 22:00:48,2	131.247.95.216	64.…	1228	80	1228 → 80 [ACK] Seq=1335 Ack=13516 Win=17520 Len=0
146	2006-05-08 22:00:48,2	64.21.46.134	131.…	80	1228	80 → 1228 [PSH, ACK] Seq=13516 Ack=1335 Win=8576 Len=1460 [TCP segment of a reassembled PDU]
147	2006-05-08 22:00:48,2	64.21.46.134	131.…	80	1228	80 → 1228 [ACK] Seq=14976 Ack=1335 Win=8576 Len=1460 [TCP segment of a reassembled PDU]
148	2006-05-08 22:00:48,2	131.247.95.216	64.…	1228	80	1228 → 80 [ACK] Seq=1335 Ack=16436 Win=17520 Len=0
149	2006-05-08 22:00:48,2	64.21.46.134	131.…	80	1228	80 → 1228 [ACK] Seq=16436 Ack=1335 Win=8576 Len=1460 [TCP segment of a reassembled PDU]
150	2006-05-08 22:00:48,2	64.21.46.134	131.…	80	1228	80 → 1228 [ACK] Seq=17896 Ack=1335 Win=8576 Len=1460 [TCP segment of a reassembled PDU]
151	2006-05-08 22:00:48,2	131.247.95.216	64.…	1228	80	1228 → 80 [ACK] Seq=1335 Ack=19356 Win=17520 Len=0
152	2006-05-08 22:00:48,3	64.21.46.134	131.…	80	1228	80 → 1228 [ACK] Seq=19356 Ack=1335 Win=8576 Len=1460 [TCP segment of a reassembled PDU]
153	2006-05-08 22:00:48,3	64.21.46.134	131.…	80	1228	80 → 1228 [ACK] Seq=20816 Ack=1335 Win=8576 Len=1460 [TCP segment of a reassembled PDU]
154	2006-05-08 22:00:48,3	131.247.95.216	64.…	1228	80	1228 → 80 [ACK] Seq=1335 Ack=22276 Win=17520 Len=0
155	2006-05-08 22:00:48,3	64.21.46.134	131.…	80	1228	80 → 1228 [ACK] Seq=22276 Ack=1335 Win=8576 Len=1460 [TCP segment of a reassembled PDU]
156	2006-05-08 22:00:48,3	64.21.46.134	131.…	80	1228	80 → 1228 [ACK] Seq=23736 Ack=1335 Win=8576 Len=1460 [TCP segment of a reassembled PDU]
157	2006-05-08 22:00:48,3	131.247.95.216	64.…	1228	80	1228 → 80 [ACK] Seq=1335 Ack=25196 Win=17520 Len=0
158	2006-05-08 22:00:48,3	64.21.46.134	131.…	80	1228	80 → 1228 [ACK] Seq=25196 Ack=1335 Win=8576 Len=1460 [TCP segment of a reassembled PDU]
159	2006-05-08 22:00:48,3	64.21.46.134	131.…	80	1228	80 → 1228 [ACK] Seq=26656 Ack=1335 Win=8576 Len=1460 [TCP segment of a reassembled PDU]
160	2006-05-08 22:00:48,3	64.21.46.134	131.…	80	1228	HTTP/1.0 200 OK (application/x-shockwave-flash)
161	2006-05-08 22:00:48,3	131.247.95.216	64.…	1228	80	1228 → 80 [ACK] Seq=1335 Ack=28116 Win=17520 Len=0
162	2006-05-08 22:00:48,3	131.247.95.216	64.…	1223	80	1223 → 80 [ACK] Seq=742 Ack=6443 Win=16971 Len=0
163	2006-05-08 22:00:48,4	131.247.95.216	64.…	1225	80	1225 → 80 [ACK] Seq=4253 Ack=26640 Win=16256 Len=0
164	2006-05-08 22:00:48,4	131.247.95.216	64.…	1226	80	1226 → 80 [ACK] Seq=3930 Ack=16010 Win=16200 Len=0
165	2006-05-08 22:00:48,4	131.247.95.216	64.…	1228	80	1228 → 80 [ACK] Seq=1335 Ack=28493 Win=17143 Len=0
166	2006-05-08 22:00:48,5	64.236.16.138	131.…	80	1219	80 → 1219 [RST] Seq=1 Win=0 Len=0
167	2006-05-08 22:00:48,5	131.247.95.216	64.…	1223	80	GET /us.js.yimg.com/lib/bc/bc_2.0.3.js HTTP/1.1
168	2006-05-08 22:00:48,5	64.21.46.151	131.…	80	1223	HTTP/1.1 200 OK (application/x-javascript)
169	2006-05-08 22:00:48,6	131.247.95.216	131.…	1229	53	Standard query 0x8187 A us.bc.yahoo.com
170	2006-05-08 22:00:48,6	131.247.92.200	131.…	53	1229	Standard query response 0x8187 A us.bc.yahoo.com CNAME bc.us.yahoo-ht1.akadns.net A 216.109.112.136
171	2006-05-08 22:00:48,6	131.247.95.216	216.…	1230	80	1230 → 80 [SYN] Seq=0 Win=16384 Len=0 MSS=1460 SACK_PERM=1
172	2006-05-08 22:00:48,7	216.109.112.136	131.…	80	1230	80 → 1230 [SYN, ACK] Seq=0 Ack=1 Win=8192 Len=0 MSS=1460
173	2006-05-08 22:00:48,7	131.247.95.216	216.…	1230	80	1230 → 80 [ACK] Seq=1 Ack=1 Win=17520 Len=0
174	2006-05-08 22:00:48,7	131.247.95.216	64.…	1223	80	1223 → 80 [ACK] Seq=1118 Ack=7708 Win=17520 Len=0
175	2006-05-08 22:00:48,7	131.247.95.216	216.…	1230	80	1230 → 80 [ACK] Seq=1 Ack=1 Win=17520 Len=1460 [TCP segment of a reassembled PDU]
176	2006-05-08 22:00:48,7	131.247.95.216	216.…	1230	80	GET /b?P=2Y07d9htdapH4YmvQZJb5V8Tg_df2ERfoy4ABbH1&T=13t6j7dle%2fX%3d1147113382%2fE%3d2716149%2fR%3dyahoo_top%2fK%3d5%2fV%3d1.1%2fW%3d3%2fY%3dYAHOO%2fF%3d2096579597%2fS%3d1%2fJ%3d6A7