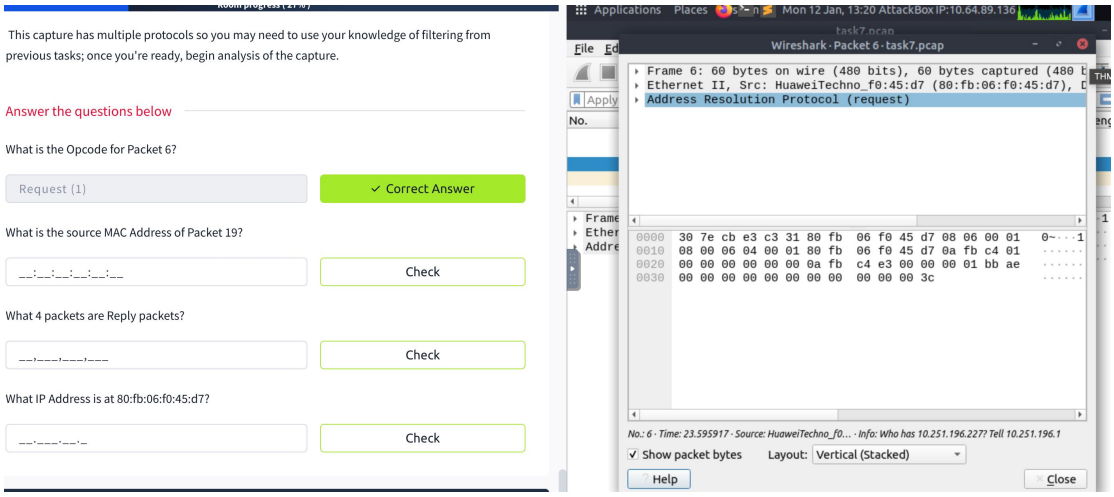
Name : Amr Khaled Elgendy
Group : AMIT - Cyber Security Online 87
Task :Wireshark 101

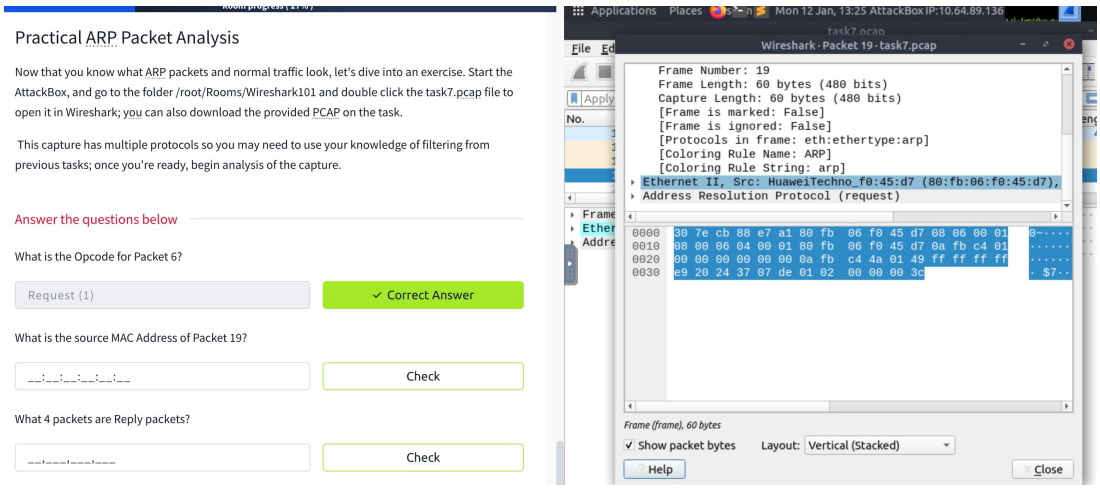
Wireshark, a tool used for creating and analyzing PCAPs (network packet capture files), is commonly used as one of the best packet analysis tools.

ARP Traffic

What is the Opcode for Packet 6?
Request (1)



What is the source MAC Address of Packet 19?
80:fb:06:f0:45:d7

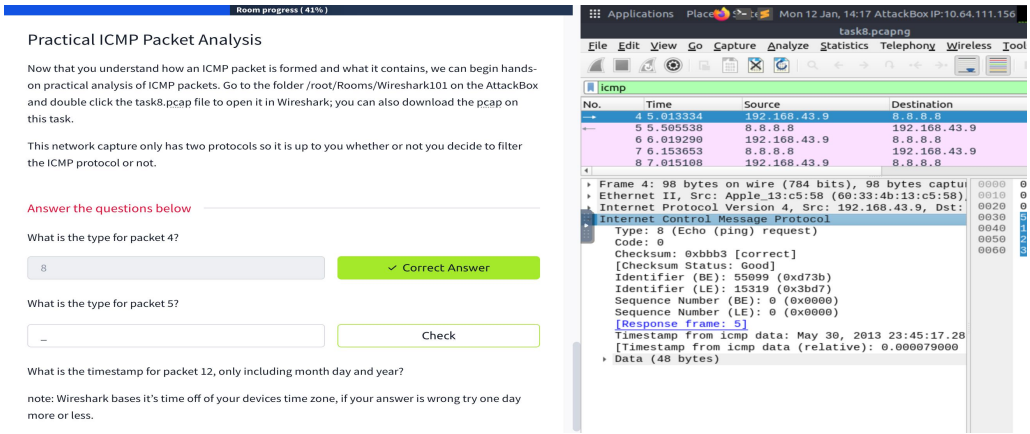


What 4 packets are Reply packets?
76,400,459,520
Explanation :
1st - Filter by Protocol based on "ARP"
2nd - Scroll through each packet and look for "Opcode: reply (2)

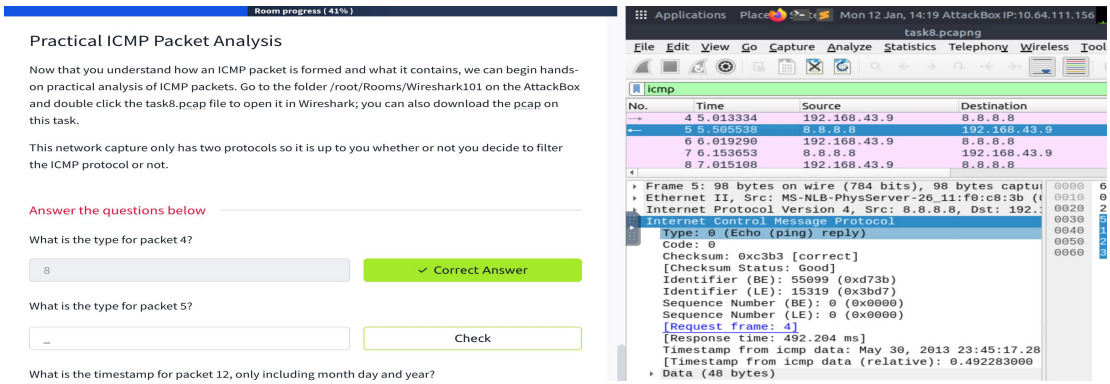
What IP Address is at 80:fb:06:f0:45:d7?
10.251.23.1
Explanation :
1st - Filter by Protocol based on "ARP"
arp && eth.addr == 80:fb:06:f0:45:d7

ICMP Traffic

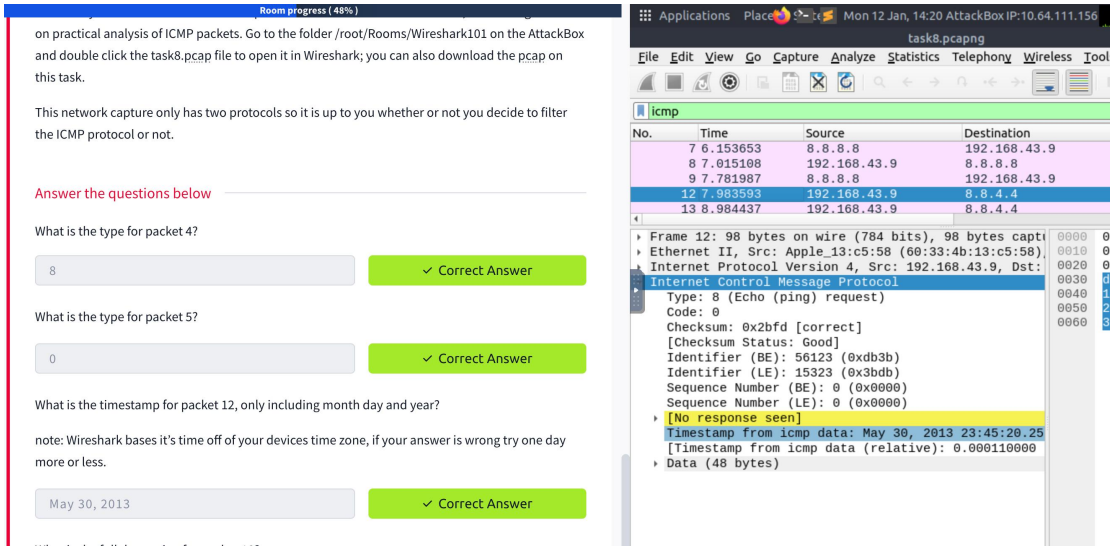
What is the type for packet 4?
8



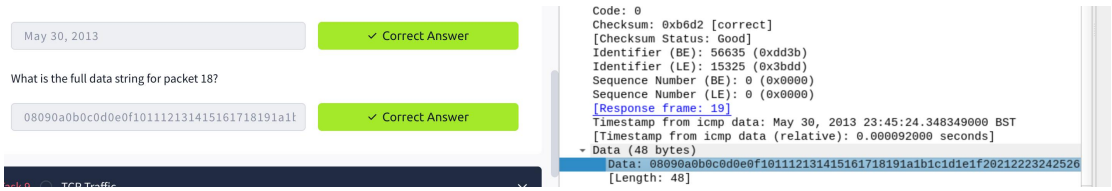
What is the type for packet 5?
0



What is the timestamp for packet 12, only including month day and year? note: Wireshark bases it’s time off of your devices time zone, if your answer is wrong try one day more or less.
May 30,2013

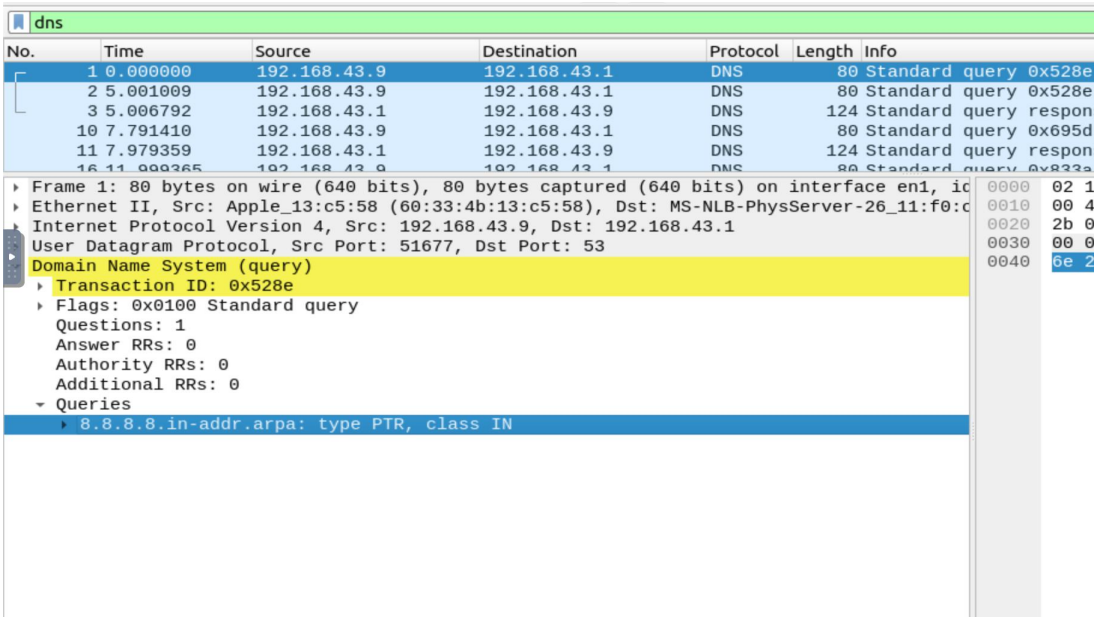


What is the full data string for packet 18?
08090a0b0c0d0e0f101112131415161718191a1b1c1d1e1f202122232425262728292a2b2c2d2e2f3031323334353637

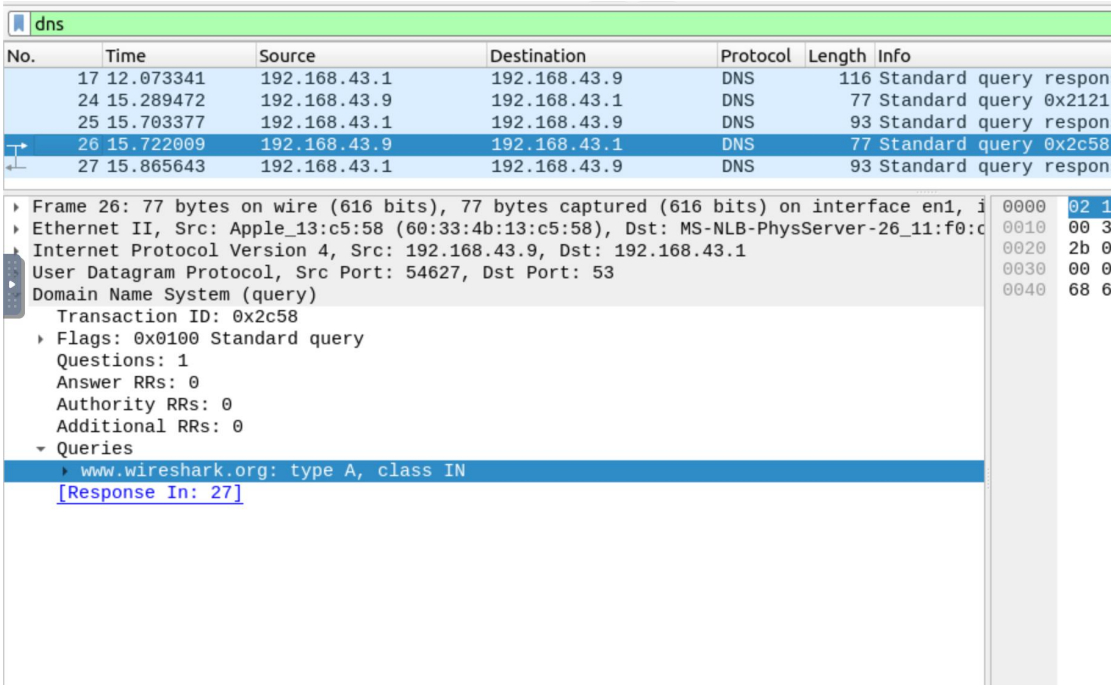


DNS Traffic

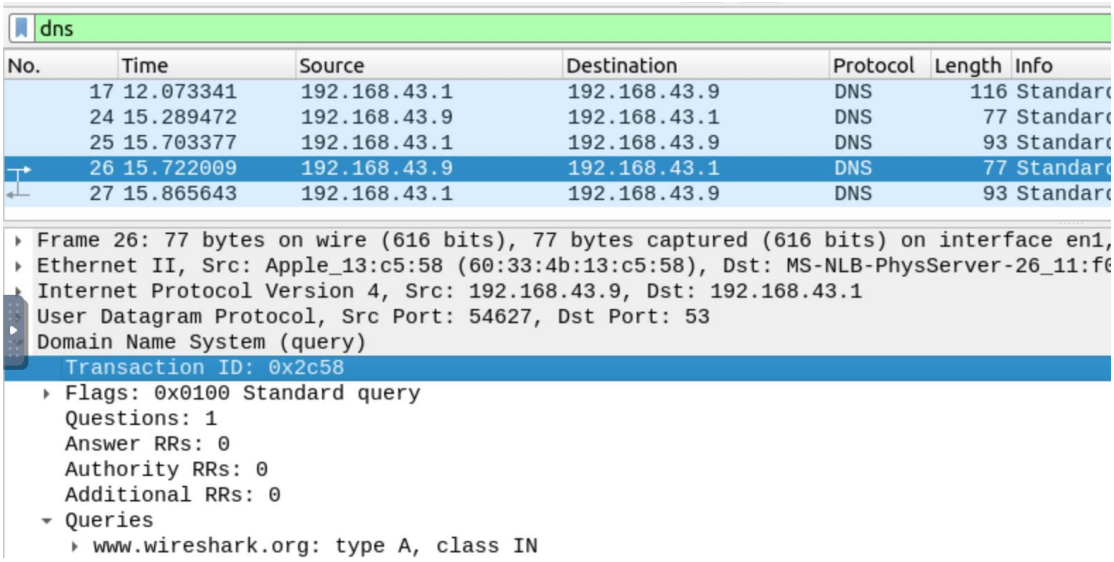
What is being queried in packet 1?
8.8.8.8.in-addr.arpa



What site is being queried in packet 26?
www.wireshark.org

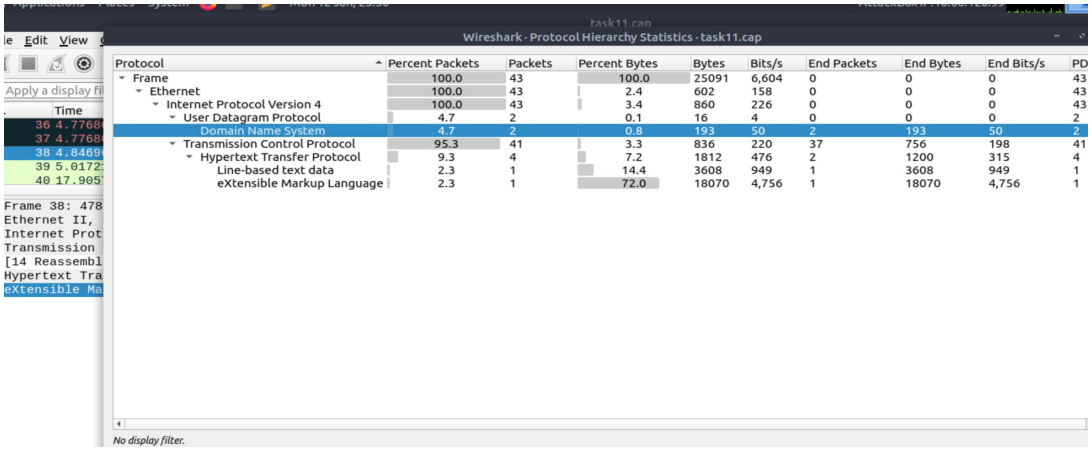


What is the Transaction ID for packet 26?
0x2c58



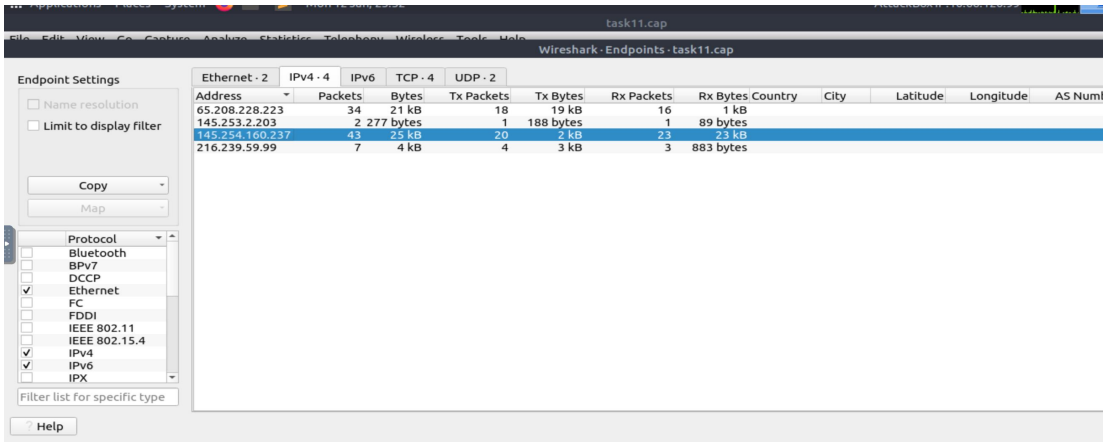
HTTP Traffic

What percent of packets originate from Domain Name System?
4.7
Navigate to "Statistics" > "Protocol Hierarchy"

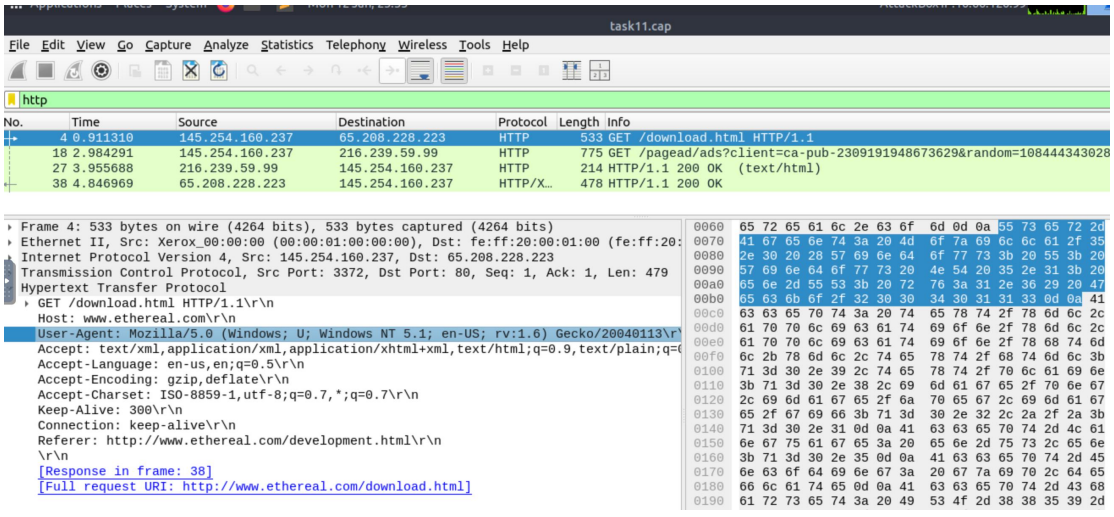


What endpoint ends in .237?
145.254.160.237

Navigate to "Statistics" > "Endpoints" > "IPv4•4



What is the user-agent listed in packet 4?
Mozilla/5.0 (Windows; U; Windows NT 5.1; en-US; rv:1.6) Gecko/20040113\r\n



Looking at the data stream what is the full request URI from packet 18?
http://pagead2.googlesyndication.com/pagead/ads?client=ca-pub-2309191948673629&random=1084443430285&lmt=1082467020&format=468x60_as&output=html&url=http%3A%2F%2Fwww.ethereal.com%2Fdownload.html&color_bg=FFFFFF&color_text=333333&color_link=000000&color_url=666633&color_border=666633

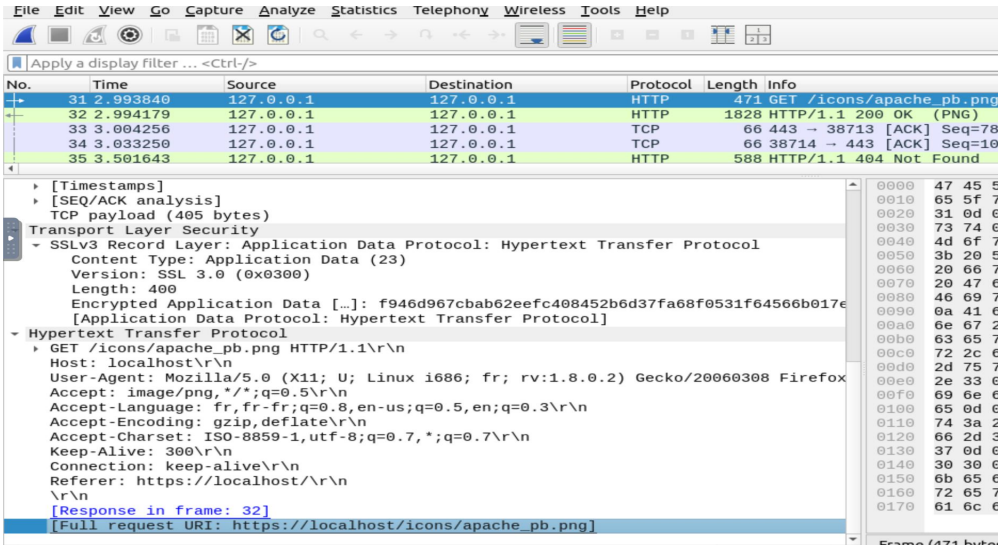
What domain name was requested from packet 38?

Looking at the data stream what is the full request URI from packet 38?
http://www.ethereal.com/download.htm

HTTPS Traffic

Looking at the data stream what is the full request URI for packet 31?
https://localhost/icons/apache_pb.png

Navigate to "Edit" > "Preferences" > "Protocols" > "TLS" > RSA Keys List [Edit]IP Address: 127.0.0.1
Port: start_tls
Protocol: http
Key File: The file location of rsasnakeoil2.key



Looking at the data stream what is the full request URI for packet 50?
https://localhost/icons/back.gif

What is the User-Agent listed in packet 50?
Mozilla/5.0 (X11; U; Linux i686; fr; rv:1.8.0.2) Gecko/20060308 Firefox/1.5.0.2\r\n