

# Computer Network 1

LAB 4c

Wireshark lab NAT

Student Name: Alexandre Rousseau

Student ID: 1952001

1) What is the IP address of the client?

IP Address is 192.168.1.100

2) The client communicates with several different Google servers to implement “safe browsing.” (See extra credit section at the end of this lab). The main Google server that will serve up the main Google web page has IP address 64.233.169.104. To display only those frames containing HTTP messages that are sent to/from this Google, server, enter the expression “http && ip.addr == 64.233.169.104” (without quotes) into the Filter: field in Wireshark.

Http doesn’t return any result but ip.addr == 64.233.169.104 returns result.

ip.addr == 64.233.169.104							
No.	Time	Source	Destination	Protocol	Length	Info	Expression
53	16:43:07.344792	192.168.1.100	64.233.169.104	TCP	66	4335→80 [SYN] Seq=0 Win=65535 Len=0 MSS=1460 W...	
54	16:43:07.378121	64.233.169.104	192.168.1.100	TCP	66	80→4335 [SYN, ACK] Seq=0 Ack=1 Win=5720 Len=0 ...	
55	16:43:07.378188	192.168.1.100	64.233.169.104	TCP	54	4335→80 [ACK] Seq=1 Ack=1 Win=260176 Len=0	
56	16:43:07.378402	192.168.1.100	64.233.169.104	TCP	689	4335→80 [PSH, ACK] Seq=1 Ack=1 Win=260176 Len=...	
57	16:43:07.409863	64.233.169.104	192.168.1.100	TCP	60	80→4335 [ACK] Seq=1 Ack=636 Win=7040 Len=0	
58	16:43:07.427567	64.233.169.104	192.168.1.100	TCP	1484	80→4335 [ACK] Seq=1 Ack=636 Win=7040 Len=1430	
59	16:43:07.427896	64.233.169.104	192.168.1.100	TCP	1484	80→4335 [ACK] Seq=1431 Ack=636 Win=7040 Len=14...	
60	16:43:07.427932	64.233.169.104	192.168.1.100	TCP	814	80→4335 [PSH, ACK] Seq=2861 Ack=636 Win=7040 L...	
61	16:43:07.427979	192.168.1.100	64.233.169.104	TCP	54	4335→80 [ACK] Seq=636 Ack=3621 Win=260176 Len=0	
62	16:43:07.550534	192.168.1.100	64.233.169.104	TCP	719	4335→80 [PSH, ACK] Seq=636 Ack=3621 Win=260176...	
63	16:43:07.584154	64.233.169.104	192.168.1.100	TCP	309	80→4335 [PSH, ACK] Seq=3621 Ack=1301 Win=8320 ...	
64	16:43:07.584711	64.233.169.104	192.168.1.100	TCP	1484	80→4335 [ACK] Seq=3876 Ack=1301 Win=8320 Len=1...	
65	16:43:07.584776	192.168.1.100	64.233.169.104	TCP	54	4335→80 [ACK] Seq=1301 Ack=5306 Win=260176 Len...	
66	16:43:07.585055	64.233.169.104	192.168.1.100	TCP	1484	80→4335 [ACK] Seq=5306 Ack=1301 Win=8320 Len=1...	
67	16:43:07.585388	64.233.169.104	192.168.1.100	TCP	1290	80→4335 [PSH, ACK] Seq=6736 Ack=1301 Win=8320 ...	
68	16:43:07.585418	192.168.1.100	64.233.169.104	TCP	54	4335→80 [ACK] Seq=1301 Ack=7972 Win=260176 Len...	
69	16:43:07.617865	64.233.169.104	192.168.1.100	TCP	1484	80→4335 [ACK] Seq=7972 Ack=1301 Win=8320 Len=1...	
70	16:43:07.618238	64.233.169.104	192.168.1.100	TCP	1484	80→4335 [ACK] Seq=9402 Ack=1301 Win=8320 Len=1...	
71	16:43:07.618278	192.168.1.100	64.233.169.104	TCP	54	4335→80 [ACK] Seq=1301 Ack=10832 Win=260176 Le...	
72	16:43:07.618557	64.233.169.104	192.168.1.100	TCP	1484	80→4335 [ACK] Seq=10832 Ack=1301 Win=8320 Len=...	
73	16:43:07.618586	64.233.169.104	192.168.1.100	TCP	226	80→4335 [PSH, ACK] Seq=12262 Ack=1301 Win=8320...	
74	16:43:07.618609	192.168.1.100	64.233.169.104	TCP	54	4335→80 [ACK] Seq=1301 Ack=12434 Win=260176 Le...	
75	16:43:07.639320	192.168.1.100	64.233.169.104	TCP	809	4335→80 [PSH, ACK] Seq=1301 Ack=12434 Win=2601...	
76	16:43:07.683545	64.233.169.104	192.168.1.100	TCP	1484	80→4335 [ACK] Seq=12434 Ack=2056 Win=9856 Len=...	
77	16:43:07.683845	64.233.169.104	192.168.1.100	TCP	1484	80→4335 [ACK] Seq=13864 Ack=2056 Win=9856 Len=...	
78	16:43:07.683891	192.168.1.100	64.233.169.104	TCP	54	4335→80 [ACK] Seq=2056 Ack=15294 Win=260176 Le...	
79	16:43:07.684198	64.233.169.104	192.168.1.100	TCP	1484	80→4335 [ACK] Seq=15294 Ack=2056 Win=9856 Len=...	
80	16:43:07.684217	64.233.169.104	192.168.1.100	TCP	146	80→4335 [PSH, ACK] Seq=16724 Ack=2056 Win=9856...	
81	16:43:07.684240	192.168.1.100	64.233.169.104	TCP	54	4335→80 [ACK] Seq=2056 Ack=16816 Win=260176 Le...	

3) Consider now the HTTP GET sent from the client to the Google server (whose IP address is IP address 64.233.169.104) at time 7.109267. What are the source and destination IP addresses and TCP source and destination ports on the IP datagram carrying this HTTP GET?

Source IP Address: 192.168.1.199, Port: 4335

Destination IP Address: 64.233.169.104, Port: 80



- 4) At what time is the corresponding 200 OK HTTP message received from the Google server? What are the source and destination IP addresses and TCP source and destination ports on the IP datagram carrying this HTTP 200 OK message?

Time the corresponding 200 OK HTTP: 7.158432000 seconds

Source IP Address: 64.233.169.104, Port: 80

Destination IP Address: 192.168.1.100, Port: 4335

- 5) Recall that before a GET command can be sent to an HTTP server, TCP must first set up a connection using the three-way SYN/ACK handshake. At what time is the client-to-server TCP SYN segment sent that sets up the connection used by the GET sent at time 7.109267? What are the source and destination IP addresses and source and destination ports for the TCP SYN segment? What are the source and destination IP addresses and source and destination ports of the ACK sent in response to the SYN.? At what time is this ACK received at the client?

SYN Time: 7.075657000 seconds

SYN Source IP Address: 192.168.1.100, Port: 4335

SYN Destination IP Address: 64.233.169.104, Port: 80

ACK Time: 7.108986000 seconds

ACK Source IP Address: 64.233.169.104, Port: 80

ACK Destination IP Address: 192.168.1.100, Port 4335

- 6) In the NAT\_ISP\_side trace file, find the HTTP GET message was sent from the client to the Google server at time 7.109267 (where  $t=7.109267$  is time at which this was sent as recorded in the NAT\_home\_side trace file). At what time does this message appear in the NAT\_ISP\_side trace file? What are the source and destination IP addresses and TCP source and destination ports on the IP datagram carrying this HTTP GET (as recording in the NAT\_ISP\_side trace file)? Which of these fields are the same, and which are different, than in your answer to question 3 above?

Time: 6.069168000 seconds

Source IP Address: 71.192.34.104, Port: 4335

Destination IP Address: 64.233.169.104, Port: 80

Destination IP, source IP and ports are different.

- 7) Are any fields in the HTTP GET message changed? Which of the following fields in the IP datagram carrying the HTTP GET are changed: Version, Header Length, Flags, Checksum? If any of these fields have changed, give a reason (in one sentence) stating why this field needed to change.

GET Message has not changed.

Version is the same.

Source IP changed from 192.168.1.100 to 71.192.34.104 but port is the same.

Header checksum changed from (Home) 0xa94a to (ISP) 0x022f

Header checksum changed because IP Address changed from 192.168.1.100 to 71.192.34.104

No.	Time	Source	Destination	Protocol	Length	Info
82	16:43:07.766539	71.192.34.104	64.233.169.104	TCP	66	4335→80 [SYN] Seq=0 Win=65535 Len=0 MSS=1460 W..
83	16:43:07.798839	64.233.169.104	71.192.34.104	TCP	66	80→4335 [SYN, ACK] Seq=0 Ack=1 Win=5720 Len=0 ..
84	16:43:07.799818	71.192.34.104	64.233.169.104	TCP	60	4335→80 [ACK] Seq=1 Ack=1 Win=260176 Len=0
85	16:43:07.800232	71.192.34.104	64.233.169.104	TCP	689	4335→80 [PSH, ACK] Seq=1 Ack=1 Win=260176 Len=...
86	16:43:07.823819	CiscoInc_bf:6c:01	Broadcast	ARP	60	who has 71.192.35.144? Tell 71.192.32.1
87	16:43:07.830701	64.233.169.104	71.192.34.104	TCP	60	80→4335 [ACK] Seq=1 Ack=636 Win=7040 Len=0

> Frame 85: 689 bytes on wire (5512 bits), 689 bytes captured (5512 bits)

> Ethernet II, Src: Dell\_4f:36:23 (00:08:74:4f:36:23), Dst: CiscoInc\_bf:6c:01 (00:0e:d6:bf:6c:01)

Internet Protocol Version 4, Src: 71.192.34.104, Dst: 64.233.169.104

0100 .... = Version: 4

.... 0101 = Header Length: 20 bytes (5)

> Differentiated Services Field: 0x00 (DSCP: CS0, ECN: Not-ECT)

Total Length: 675

Identification: 0xa2ac (41644)

> Flags: 0x02 (Don't Fragment)

Fragment offset: 0

Time to live: 127

Protocol: TCP (6)

Header checksum: 0x022f [validation disabled]

[Header checksum status: Unverified]

Source: 71.192.34.104

Destination: 64.233.169.104

[Source GeoIP: Unknown]

[Destination GeoIP: Unknown]

> Transmission Control Protocol, Src Port: 4335, Dst Port: 80, Seq: 1, Ack: 1, Len: 635

> Data (635 bytes)

Figure 1: ISP

No.	Time	Source	Destination	Protocol	Length	Info
52	16:43:07.343032	68.87.71.230	192.168.1.100	DNS	158	Standard query response 0xed6a A www.google.co..
53	16:43:07.344792	192.168.1.100	64.233.169.104	TCP	66	4335→80 [SYN] Seq=0 Win=65535 Len=0 MSS=1460 W..
54	16:43:07.378121	64.233.169.104	192.168.1.100	TCP	66	80→4335 [SYN, ACK] Seq=0 Ack=1 Win=5720 Len=0 ..
55	16:43:07.378188	192.168.1.100	64.233.169.104	TCP	54	4335→80 [ACK] Seq=1 Ack=1 Win=260176 Len=0
56	16:43:07.378402	192.168.1.100	64.233.169.104	TCP	689	4335→80 [PSH, ACK] Seq=1 Ack=1 Win=260176 Len=...
57	16:43:07.409863	64.233.169.104	192.168.1.100	TCP	60	80→4335 [ACK] Seq=1 Ack=636 Win=7040 Len=0

> Frame 56: 689 bytes on wire (5512 bits), 689 bytes captured (5512 bits)

> Ethernet II, Src: MonHaiPr\_0d:ca:8f (00:22:68:0d:ca:8f), Dst: Cisco-Li\_45:1f:1b (00:22:6b:45:1f:1b)

Internet Protocol Version 4, Src: 192.168.1.100, Dst: 64.233.169.104

0100 .... = Version: 4

.... 0101 = Header Length: 20 bytes (5)

> Differentiated Services Field: 0x00 (DSCP: CS0, ECN: Not-ECT)

Total Length: 675

Identification: 0xa2ac (41644)

> Flags: 0x02 (Don't Fragment)

Fragment offset: 0

Time to live: 128

Protocol: TCP (6)

Header checksum: 0xa94a [validation disabled]

[Header checksum status: Unverified]

Source: 192.168.1.100

Destination: 64.233.169.104

[Source GeoIP: Unknown]

[Destination GeoIP: Unknown]

> Transmission Control Protocol, Src Port: 4335, Dst Port: 80, Seq: 1, Ack: 1, Len: 635

> Data (635 bytes)

Figure 2: Home

- 8) In the NAT\_ISP\_side trace file, at what time is the first 200 OK HTTP message received from the Google server? What are the source and destination IP addresses and TCP source and destination ports on the IP datagram carrying this HTTP 200 OK message? Which of these fields are the same, and which are different than your answer to question 4 above?

HTTP 200 OK message first time: 6.117078000 seconds.

HTTP 200 OK message Source IP : 64.233.169.104, Port : 80

HTTP 200 OK message Destination IP : 71.192.34.104, Port : 4335

Version is the same, Flag does not change.

Time to live change

Header checksum changed

No.	Time	Source	Destination	Protocol	Length	Info
82	16:43:07.766539	71.192.34.104	64.233.169.104	TCP	66	4335→80 [SYN] Seq=0 Win=65535 Len=0 MSS=1460 W...
83	16:43:07.798839	64.233.169.104	71.192.34.104	TCP	66	80→4335 [SYN, ACK] Seq=0 Ack=1 Win=5720 Len=0 ...
84	16:43:07.799818	71.192.34.104	64.233.169.104	TCP	60	4335→80 [ACK] Seq=1 Ack=1 Win=260176 Len=0
85	16:43:07.800232	71.192.34.104	64.233.169.104	TCP	689	4335→80 [PSH, ACK] Seq=1 Ack=1 Win=260176 Len=...
86	16:43:07.823819	CiscoInc_bf:6c:01	Broadcast	ARP	60	Who has 71.192.35.144? Tell 71.192.32.1
87	16:43:07.830201	64.233.169.104	71.192.34.104	TCP	60	80→4335 [ACK] Seq=1 Ack=636 Win=7040 Len=0
88	16:43:07.848142	64.233.169.104	71.192.34.104	TCP	1484	80→4335 [ACK] Seq=1 Ack=636 Win=7040 Len=1430
89	16:43:07.848471	64.233.169.104	71.192.34.104	TCP	1404	80→4335 [ACK] Seq=1431 Ack=636 Win=7040 Len=14...

  

Frame 88: 1484 bytes on wire (11872 bits), 1484 bytes captured (11872 bits)

Encapsulation type: Ethernet (1)

Arrival Time: Sep 20, 2009 16:43:07.848142000 Eastern Daylight Time

[Time shift for this packet: 0.000000000 seconds]

Epoch Time: 1253479387.848142000 seconds

[Time delta from previous captured frame: 0.017441000 seconds]

[Time delta from previous displayed frame: 0.017441000 seconds]

[Time since reference or first frame: 6.117078000 seconds]

Frame Number: 88

Frame Length: 1484 bytes (11872 bits)

Capture Length: 1484 bytes (11872 bits)

[Frame is marked: False]

[Frame is ignored: False]

[Protocols in frame: eth:ethertype:ip:tcp:data]

[Coloring Rule Name: HTTP]

[Coloring Rule String: http || tcp.port == 80 || http2]

Ethernet II, Src: CiscoInc bf:6c:01 (00:0e:d6:bf:6c:01), Dst: Dell\_4f:36:23 (00:08:74:4f:36:23)

Internet Protocol Version 4, Src: 64.233.169.104, Dst: 71.192.34.104

Transmission Control Protocol, Src Port: 80, Dst Port: 4335, Seq: 1, Ack: 636, Len: 1430

Data (1430 bytes)

- 9) In the NAT\_ISP\_side trace file, at what time were the client-to-server TCP SYN segment and the server-to-client TCP ACK segment corresponding to the segments in question 5 above captured? What are the source and destination IP addresses and source and destination ports for these two segments? Which of these fields are the same, and which are different than your answer to question 5 above?

SYN:

Time: 6.035475000 seconds

Source IP Address: 71.192.34.104

Destination IP Address: 64.233.169.104

Time to live changed

No.	Time	Source	Destination	Protocol	Length	Info
82	16:43:07.766539	71.192.34.104	64.233.169.104	TCP	66	4335→80 [SYN] Seq=0 Win=65535 Len=0 MSS=1460 W...
83	16:43:07.798839	64.233.169.104	71.192.34.104	TCP	66	80→4335 [SYN, ACK] Seq=0 Ack=1 Win=5720 Len=0 ...
84	16:43:07.799818	71.192.34.104	64.233.169.104	TCP	60	4335→80 [ACK] Seq=1 Ack=1 Win=260176 Len=0
85	16:43:07.800232	71.192.34.104	64.233.169.104	TCP	689	4335→80 [PSH, ACK] Seq=1 Ack=1 Win=260176 Len=...

  

>	Frame 82: 66 bytes on wire (528 bits), 66 bytes captured (528 bits)
>	Ethernet II, Src: Dell_4f:36:23 (00:08:74:4f:36:23), Dst: CiscoInc_bf:6c:01 (00:0e:d6:bf:6c:01)
>	Internet Protocol Version 4, Src: 71.192.34.104, Dst: 64.233.169.104
>	0100 .... = Version: 4
>	.... 0101 = Header Length: 20 bytes (5)
>	Differentiated Services Field: 0x00 (DSCP: CS0, ECN: Not-ECT)
>	Total Length: 52
>	Identification: 0xa2aa (41642)
>	Flags: 0x02 (Don't Fragment)
>	Fragment offset: 0
>	Time to live: 127
>	Protocol: TCP (6)
>	Header checksum: 0x04a0 [validation disabled]
>	[Header checksum status: Unverified]
>	Source: 71.192.34.104
>	Destination: 64.233.169.104
>	[Source GeoIP: Unknown]
>	[Destination GeoIP: Unknown]
>	Transmission Control Protocol, Src Port: 4335, Dst Port: 80, Seq: 0, Len: 0

ACK:

Time: 6.067775000 seconds

Source IP Address: 64.233.169.104

Destination IP Address: 71.192.34.104

Identification, Time to live, Flags, Source and Destination IP changed

No.	Time	Source	Destination	Protocol	Length	Info
82	16:43:07.766539	71.192.34.104	64.233.169.104	TCP	66	4335→80 [SYN] Seq=0 Win=65535 Len=0 MSS=1460 W...
83	16:43:07.798839	64.233.169.104	71.192.34.104	TCP	66	80→4335 [SYN, ACK] Seq=0 Ack=1 Win=5720 Len=0 ...
84	16:43:07.799818	71.192.34.104	64.233.169.104	TCP	60	4335→80 [ACK] Seq=1 Ack=1 Win=260176 Len=0
85	16:43:07.800232	71.192.34.104	64.233.169.104	TCP	689	4335→80 [PSH, ACK] Seq=1 Ack=1 Win=260176 Len=...

  

>	Frame 83: 66 bytes on wire (528 bits), 66 bytes captured (528 bits)
>	Ethernet II, Src: CiscoInc_bf:6c:01 (00:0e:d6:bf:6c:01), Dst: Dell_4f:36:23 (00:08:74:4f:36:23)
>	Internet Protocol Version 4, Src: 64.233.169.104, Dst: 71.192.34.104
>	0100 .... = Version: 4
>	.... 0101 = Header Length: 20 bytes (5)
>	Differentiated Services Field: 0x20 (DSCP: CS1, ECN: Not-ECT)
>	Total Length: 52
>	Identification: 0xf61a (63002)
>	Flags: 0x00
>	Fragment offset: 0
>	Time to live: 51
>	Protocol: TCP (6)
>	Header checksum: 0x3d10 [validation disabled]
>	[Header checksum status: Unverified]
>	Source: 64.233.169.104
>	Destination: 71.192.34.104
>	[Source GeoIP: Unknown]
>	[Destination GeoIP: Unknown]
>	Transmission Control Protocol, Src Port: 80, Dst Port: 4335, Seq: 0, Ack: 1, Len: 0



- 10) Using your answers to 1-8 above, fill in the NAT translation table entries for HTTP connection considered in questions 1-8 above.

In the WAN, the outside world can see only one client IP address which is the NAT router's IP – 71.192.34.104. Internal LAN IP Address of the client is 192.168.1.100. The router will use the port number after its IP, 71.192.34.104:4335 to forward the packets to the actual client IP – 192.168.1.100:4335.

WAN (Outside)		LAN (Local)	
IP	Port	IP	Port
71.192.34.104	4335	192.168.1.100	4335

**Extra Credit:** The trace files investigated above have additional connections to Google servers above and beyond the HTTP GET, 200 OK request/response studied above. For example, in the NAT\_home\_side trace file, consider the client-to-server GET at time 1.572315, and the GET at time 7.573305. Research the use of these two HTTP messages and write a half page explanation of the purpose of each of these messages.

Before answering the question about google safe browsing, I visited the official website and read about detailed information on Google safe browsing. Based on the description, the Google safe browsing protects clients from malware or unwanted software. When a client clicks on a link from Google's search results, safe browsing automatically checks the website for the client through Google's latest update list of unsafe website list. If client visit an unsafe website that contains suspicious software or malware, client gets a warning page. The HTTP request and response in the NAT\_home\_side trace file shows safe browsing in work.

- 1) In HTTP GET at frame 20 at time 1.572315 the header includes the request URL "safebrowsing cache.google.com/safebrowsing/rd/googlemalware-shaver\_s\_15361-15365.15661-15365".
- 2) In HTTP GET at frame 104 at time 7.573305 the header includes the request URL "google.com/generate\_204"

The first URL directs the client to the safebrowsing cache site, while the second URL directs the client to the target website, which means that the website is safe to visit. After looking at the two HTTP GET messages, I found some interesting results. The Destination IP changed from 74.125.106.31 in frame 20 to 74.125.91.113 in frame 104. Additionally, the identification in the header changed because each one is a uniquely assigned number, and the Header checksums changed because the destination address changed. Between frame 20 and 104, the source IP transition twice – once at frame 52 from 74.125.106.31 (safebrowsing cache.google.com) to 64.233.169.104 (www.google.com) and again at frame 96 from 64.233.169.104 (www.google.com) to 74.125.106.31 (clients1.google.com). Both times, there are DNS queries and query answer. Maybe we can guess that there was a Google Search query at frame 96. I tried safebrowsing in real like using Wireshark to capture activities while visiting a website through Google search engine. However, I could not find safebrowsing frame at all. Instead of that, I found TLSv1.2 protocol with handshakes and encrypted DNS protocol.



```

▼ Frame 20: 767 bytes on wire (6136 bits), 767 bytes captured (6136 bits)
  Encapsulation type: Ethernet (1)
  Arrival Time: Sep 20, 2009 16:43:01.841450000 Eastern Daylight Time
  [Time shift for this packet: 0.000000000 seconds]
  Epoch Time: 1253479381.841450000 seconds
  [Time delta from previous captured frame: 0.000087000 seconds]
  [Time delta from previous displayed frame: 0.000087000 seconds]
  [Time since reference or first frame: 1.572315000 seconds]
  Frame Number: 20
  Frame Length: 767 bytes (6136 bits)
  Capture Length: 767 bytes (6136 bits)
  [Frame is marked: False]
  [Frame is ignored: False]
  [Protocols in frame: eth:ethertype:ip:tcp:data]
  [Coloring Rule Name: HTTP]
  [Coloring Rule String: http || tcp.port == 80 || http2]
  > Ethernet II, Src: HonHaiPr_0d:ca:8f (00:22:68:0d:ca:8f), Dst: Cisco-Li_45:1f:1b (00:22:6b:45:1f:1b)
  ▼ Internet Protocol Version 4, Src: 192.168.1.100, Dst: 74.125.106.31
    0100 .... = Version: 4
    .... 0101 = Header Length: 20 bytes (5)
    > Differentiated Services Field: 0x00 (DSCP: CS0, ECN: Not-ECT)
    Total Length: 767
    Identification: 0xa27e (41598)
    > Flags: 0x02 (Don't Fragment)
    Fragment offset: 0
    Time to live: 128
    Protocol: TCP (6)
    Header checksum: 0xdedf [validation disabled]
    [Header checksum status: Unverified]
    Source: 192.168.1.100
    Destination: 74.125.106.31
    [Source GeoIP: Unknown]
    [Destination GeoIP: Unknown]
  ▼ Transmission Control Protocol, Src Port: 4331, Dst Port: 80, Seq: 1, Ack: 1, Len: 713
    Source Port: 4331
    Destination Port: 80

0000  00 22 6b 45 1f 1b 00 22 68 0d ca 8f 08 00 45 00  .".kE... h....E.
0010  02 f1 a2 7e 40 00 80 06 de df c0 a8 01 64 4a 7d  ...~@... ..dJ}
0020  6a 1f 10 eb 00 50 57 e8 78 a1 b3 bf 8a 9b 50 18  i....PW. x....P.
0030  fe 14 79 8c 00 00 47 45 54 20 2f 73 61 66 65 62  ..y...GE T /safeb
0040  72 6f 77 73 69 6e 67 2f 72 64 2f 67 6f 6f 67 2d  rowsing/ rd/goog-
0050  6d 61 6c 77 61 72 65 2d 73 68 61 76 61 72 5f 73  malware- shavar_s
0060  5f 31 35 33 36 31 2d 31 35 33 36 35 2e 31 35 33  _15361-1 5365.153
0070  36 31 2d 31 35 33 36 35 2e 3a 20 48 54 54 50 2f  61-15365 .: HTTP/
0080  31 2e 31 0d 0a 40 6f 73 74 3a 20 73 61 66 65 62  1.1..Mos t: safeb
0090  72 6f 77 73 69 6e 67 2d 63 61 63 68 65 2e 67 6f  rowsing- cache.go
00a0  6f 67 6c 65 2e 63 6f 6d 0d 0a 55 73 65 72 2d 41  ogle.com ..User-A
00b0  67 65 6e 74 3a 20 4d 6f 7a 69 6c 6c 61 2f 35 2e  gent: Mo zilla/S.
00c0  30 20 28 57 69 6e 64 6f 77 73 3b 20 55 3b 20 57  0 (windo ws; U; W
00d0  69 6e 64 6f 77 73 20 4e 54 20 35 2e 31 3b 20 65  indows N T 5.1; e
00e0  6e 2d 55 53 3b 20 72 76 3a 31 2e 39 2e 30 2e 31  n-US; rv :1.9.0.1
00f0  34 29 20 47 65 63 6b 6f 2f 32 30 30 39 30 38 32  4) Gecko /2009082
0100  37 30 37 20 46 69 72 65 66 6f 78 2f 33 2e 30 2e  707 Fire fox/3.0.
0110  31 34 20 28 2e 4e 45 54 20 43 4c 52 20 33 2e 35  14 (.NET CLR 3.5

```

Figure 3: Client to server GET at time 1.572315

```

> Frame 52: 158 bytes on wire (1264 bits), 158 bytes captured (1264 bits)
> Ethernet II, Src: Cisco-Li_45:1f:1b (00:22:6b:45:1f:1b), Dst: MonHaiPr_0d:ca:8f (00:22:68:0d:ca:8f)
> Internet Protocol Version 4, Src: 68.87.71.230, Dst: 192.168.1.100
  0100 .... = Version: 4
  .... 0101 = Header Length: 20 bytes (5)
  > Differentiated Services Field: 0x00 (DSCP: CS0, ECN: Not-ECT)
    Total Length: 144
    Identification: 0x0000 (0)
  > Flags: 0x02 (Don't Fragment)
    Fragment offset: 0
    Time to live: 56
  Protocol: UDP (17)
  Header checksum: 0xf413 [validation disabled]
  [Header checksum status: Unverified]
  Source: 68.87.71.230
  Destination: 192.168.1.100
  [Source GeoIP: Unknown]
  [Destination GeoIP: Unknown]
> User Datagram Protocol, Src Port: 53, Dst Port: 49200
> Domain Name System (response)
  [Request In: 51]
  [Time: 0.013628000 seconds]
  Transaction ID: 0xed6a
  > Flags: 0x8180 Standard query response, No error
  Questions: 1
  Answer RRs: 5
  Authority RRs: 0
  Additional RRs: 0
  > Queries
    > www.google.com: type A, class IN
  > Answers
    > www.google.com: type CNAME, class IN, cname www.l.google.com
    > www.l.google.com: type A, class IN, addr 64.233.169.104
    > www.l.google.com: type A, class IN, addr 64.233.169.147
    > www.l.google.com: type A, class IN, addr 64.233.169.99
    > www.l.google.com: type A, class IN, addr 64.233.169.103
0000 00 22 68 0d ca 8f 00 22 6b 45 1f 1b 08 00 45 00  .".h...." kE...E.
0010 00 90 00 00 40 00 38 11 f4 13 44 57 47 e6 c0 a8  ....@.8. ..DWG...
0020 01 64 00 35 c0 30 00 7c 1a 34 ed 6a 81 80 00 01  .d.5.0.| .4.j....
0030 00 05 00 00 00 00 03 77 77 77 06 67 6f 6f 67 6c  ....w ww.googl
0040 65 03 63 6f 6d 00 00 01 00 01 c0 0c 00 05 00 01  e.com... ....
0050 00 09 31 d0 00 08 03 77 77 77 01 6c c0 10 c0 2c  .l....w ww.l...
0060 00 01 00 01 00 00 00 39 00 04 40 e9 a9 68 c0 2c  ....9 ..@..h.,
0070 00 01 00 01 00 00 00 39 00 04 40 e9 a9 93 c0 2c  ....9 ..@....,
0080 00 01 00 01 00 00 00 39 00 04 40 e9 a9 63 c0 2c  ....9 ..@..C.,

```

Figure 4: Transition to Source IP: 64.233.169.104, Home\_side\_Frame 52



```

> Frame 96: 199 bytes on wire (1592 bits), 199 bytes captured (1592 bits)
> Ethernet II, Src: Cisco-Li_45:1f:1b (00:22:6b:45:1f:1b), Dst: HonHaiPr_0d:ca:8f (00:22:68:0d:ca:8f)
> Internet Protocol Version 4, Src: 68.87.71.230, Dst: 192.168.1.100
  0100 .... = Version: 4
  .... 0101 = Header Length: 20 bytes (5)
  > Differentiated Services Field: 0x00 (DSCP: CS0, ECN: Not-ECT)
    Total Length: 185
    Identification: 0x0000 (0)
  > Flags: 0x02 (Don't Fragment)
    Fragment offset: 0
    Time to live: 64
  Protocol: UDP (17)
  Header checksum: 0xf3ea [validation disabled]
  [Header checksum status: Unverified]
  Source: 68.87.71.230
  Destination: 192.168.1.100
  [Source GeoIP: Unknown]
  [Destination GeoIP: Unknown]
> User Datagram Protocol, Src Port: 53, Dst Port: 57244
> Domain Name System (response)
  [Request In: 95]
  [Time: 0.015247000 seconds]
  Transaction ID: 0x0041
  > Flags: 0x8180 Standard query response, No error
  Questions: 1
  Answer RRs: 7
  Authority RRs: 0
  Additional RRs: 0
  > Queries
    > clients1.google.com: type A, class IN
  > Answers
    > clients1.google.com: type CNAME, class IN, cname clients.l.google.com
    > clients.l.google.com: type A, class IN, addr 74.125.91.113
    > clients.l.google.com: type A, class IN, addr 74.125.91.139
    > clients.l.google.com: type A, class IN, addr 74.125.91.138
    > clients.l.google.com: type A, class IN, addr 74.125.91.101
    > clients.l.google.com: type A, class IN, addr 74.125.91.102
    > clients.l.google.com: type A, class IN, addr 74.125.91.100
0000 00 22 68 0d ca 8f 00 22 6b 45 1f 1b 08 00 45 00  .".h...." kE....E.
0010 00 b9 00 00 40 00 38 11 f3 ea 44 57 47 e6 c0 a8  ....@.8. ..DWG...
0020 01 64 00 35 df 9c 00 a5 cb c7 08 41 81 80 00 01  .d.5.... ..A....
0030 00 07 00 00 00 00 08 63 6c 69 65 6e 74 73 31 06  ....c lients1.
0040 67 6f 6f 67 6c 65 03 63 6f 6d 00 00 01 00 01 c0  google.c om.....
0050 0c 00 05 00 01 00 00 00 af 00 0c 07 63 6c 69 65  .... ..clie
0060 6e 74 73 01 6c c0 15 c0 31 00 01 00 01 00 00 00  nts.l... 1.....

```

Figure 5: Transition to Source IP Address: 74.125.91.113, Home\_side\_Frame 96

```

▼ Frame 104: 709 bytes on wire (5672 bits), 709 bytes captured (5672 bits)
  Encapsulation type: Ethernet (1)
  Arrival Time: Sep 20, 2009 16:43:07.842440000 Eastern Daylight Time
  [Time shift for this packet: 0.000000000 seconds]
  Epoch Time: 1253479387.842440000 seconds
  [Time delta from previous captured frame: 0.000122000 seconds]
  [Time delta from previous displayed frame: 0.000122000 seconds]
  [Time since reference or first frame: 7.573305000 seconds]
  Frame Number: 204
  Frame Length: 709 bytes (5672 bits)
  Capture Length: 709 bytes (5672 bits)
  [Frame is marked: False]
  [Frame is ignored: False]
  [Protocols in frame: eth:ethertype:ip:tcp:data]
  [Coloring Rule Name: HTTP]
  [Coloring Rule String: http || tcp.port == 80 || http2]
  > Ethernet II, Src: MonHsiPr_0d:ca:8f (00:22:68:0d:ca:8f), Dst: Cisco-Li_45:1f:1b (00:22:6b:45:1f:1b)
  ▼ Internet Protocol Version 4, Src: 192.168.1.100, Dst: 74.125.91.113
    0100 .... = Version: 4
    .... 0101 = Header Length: 20 bytes (5)
    > Differentiated Services Field: 0x00 (DSCP: CS0, ECN: Not-ECT)
    Total Length: 655
    Identification: 0xa2d7 (41687)
    > Flags: 0x02 (Don't Fragment)
    Fragment offset: 0
    Time to live: 128
    Protocol: TCP (6)
    Header checksum: 0xed6e [validation disabled]
    [Header checksum status: Unverified]
    Source: 192.168.1.100
    Destination: 74.125.91.113
    [Source GeoIP: Unknown]
    [Destination GeoIP: Unknown]
  ▼ Transmission Control Protocol, Src Port: 4336, Dst Port: 80, Seq: 1, Ack: 1, Len: 655
    Source Port: 4336
    Destination Port: 80

0000  00 22 6b 45 1f 1b 00 22 68 0d ca 8f 08 00 45 00  . "kE... " h.....E.
0010  02 b7 a2 d7 40 00 80 06 ed 6e c0 a8 01 64 4a 7d  ....@... .n...d}
0020  5b 71 10 f0 00 50 e7 b7 8e cf 70 5f 64 ff 50 18  [a...P... n...d P
0030  fe 14 6a a4 00 00 47 45 54 20 2f 67 65 6e 65 72  ..j...GE T /gener
0040  61 74 65 5f 32 30 34 20 48 54 54 50 2f 31 2e 31  ate_204 HTTP/1.1
0050  0d 0a 48 6f 73 74 3a 20 63 6c 69 65 6e 74 73 31  ..Host: clients1
0060  2e 67 6f 6f 67 6c 65 2e 63 6f 6d 0d 0a 55 73 65  .google. com..Use
0070  72 2d 41 67 65 6e 74 3a 20 4d 6f 7a 69 6c 6c 61  r-Agent: Mozilla
0080  2f 35 2e 30 20 28 57 69 6e 64 6f 77 73 20 4e 54 20 35 2e 31  /5.0 (Wi ndows; U
0090  3b 20 57 69 6e 64 6f 77 73 20 4e 54 20 35 2e 31  , window S W 3.1
00a0  3b 20 65 6e 2d 55 53 3b 20 72 76 3a 31 2e 39 2e  ; en-US; rv:1.9.
00b0  30 2e 31 34 29 20 47 65 63 6b 6f 2f 32 30 30 39  0.14) Ge cko/2009
00c0  30 38 32 37 30 37 20 46 69 72 65 66 6f 78 2f 33  002707 F irefox/3
00d0  2e 30 2e 31 34 20 28 2e 4e 45 54 20 43 4c 52 20  .0.14 (. NET CLR
00e0  33 2e 35 2e 33 30 37 32 39 29 0d 0a 41 63 63 65  3.5.3072 9)..Acce
00f0  70 74 3a 20 69 6d 61 67 65 2f 70 6e 67 2c 69 6d  pt: imag e/png,im
0100  61 67 65 2f 2a 3b 71 3d 30 2e 38 2c 2a 2f 2a 3b  age/*;q= 0.8,*/*;
0110  71 3d 30 2e 35 0d 0a 41 63 63 65 70 74 2d 4c 61  q=0.5..A ccept-La

```

Figure 6: Client to server GET at time 7.573305