

1/

http						
No.	Time	Source	Destination	Protocol	Length	Info
7	2009-09-21 03:43:01.477175	192.168.1.100	74.125.91.113	HTTP	1035	POST /safebrowsing/downloads?client=navclient-auto-ffox&appver=3.0.14&pver=2.2&wrke
11	2009-09-21 03:43:01.543197	74.125.91.113	192.168.1.100	HTTP	853	HTTP/1.1 200 OK (application/vnd.google.safebrowsing-update)
13	2009-09-21 03:43:01.797783	74.125.91.113	192.168.1.100	HTTP	853	[TCP Spurious Retransmission] HTTP/1.1 200 OK (application/vnd.google.safebrowsing
20	2009-09-21 03:43:01.841450	192.168.1.100	74.125.106.31	HTTP	767	GET /safebrowsing/rd/goog-malware-shavar_s_15361-15365.15361-15365.: HTTP/1.1
39	2009-09-21 03:43:01.946914	74.125.106.31	192.168.1.100	HTTP	651	HTTP/1.1 200 OK (application/vnd.google.safebrowsing-chunk)
41	2009-09-21 03:43:02.246131	192.168.1.100	74.125.106.31	HTTP	772	GET /safebrowsing/rd/goog-malware-shavar_a_14466-14470.14466.14467-14470: HTTP/1.1
42	2009-09-21 03:43:02.269764	74.125.106.31	192.168.1.100	HTTP	881	HTTP/1.1 200 OK (application/vnd.google.safebrowsing-chunk)
43	2009-09-21 03:43:02.283240	192.168.1.100	74.125.106.31	HTTP	776	GET /safebrowsing/rd/goog-phish-shavar_s_48291-48300.48291-48295.48296-48300: HTTP/
44	2009-09-21 03:43:02.307382	74.125.106.31	192.168.1.100	HTTP	526	HTTP/1.1 200 OK (application/vnd.google.safebrowsing-chunk)
45	2009-09-21 03:43:02.313886	192.168.1.100	74.125.106.31	HTTP	776	GET /safebrowsing/rd/goog-phish-shavar_a_67721-67760.67721-67729.67730-67760: HTTP/
> Frame 13: 853 bytes on wire (6824 bits), 853 bytes captured (6824 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: 74.125.91.113, Dst: 192.168.1.100						
0100 .... = Version: 4						
.... 0101 = Header Length: 20 bytes (5)						
> Differentiated Services Field: 0x20 (DSCP: CS1, ECN: Not-ECT)						
Total Length: 839						
Identification: 0x6354 (25428)						
> Flags: 0x00						
Fragment Offset: 0						
Time to Live: 51						
Protocol: TCP (6)						
Header Checksum: 0xb942 [validation disabled]						
[Header checksum status: Unverified]						
Source Address: 74.125.91.113						
Destination Address: 192.168.1.100						
> Transmission Control Protocol, Src Port: 80, Dst Port: 4330, Seq: 1, Ack: 982, Len: 799						
> Hypertext Transfer Protocol						
> Media Type						

IP address: 192.168.1.100

3/

No.	Time	Source	Destination	Protocol	Length	Info
56	2009-09-21 03:43:07.378402	192.168.1.100	64.233.169.104	HTTP	689	GET / HTTP/1.1
60	2009-09-21 03:43:07.427932	64.233.169.104	192.168.1.100	HTTP	814	HTTP/1.1 200 OK (text/html)
62	2009-09-21 03:43:07.550534	192.168.1.100	64.233.169.104	HTTP	719	GET /intl/en_ALL/images/logo.gif HTTP/1.1
73	2009-09-21 03:43:07.618586	64.233.169.104	192.168.1.100	HTTP	226	HTTP/1.1 200 OK (GIF89a)
75	2009-09-21 03:43:07.639320	192.168.1.100	64.233.169.104	HTTP	809	GET /extern_js/f/CgJlbhICdX0rMAo4NUAILCswDjgHLCswFjgQLCswFzgDLCswGDgELCsw
92	2009-09-21 03:43:07.717784	64.233.169.104	192.168.1.100	HTTP	648	HTTP/1.1 200 OK (text/javascript)
94	2009-09-21 03:43:07.761459	192.168.1.100	64.233.169.104	HTTP	695	GET /extern_chrome/ee36edbd3c16a1c5.js HTTP/1.1
100	2009-09-21 03:43:07.806488	64.233.169.104	192.168.1.100	HTTP	870	HTTP/1.1 200 OK (text/html)
107	2009-09-21 03:43:07.921971	192.168.1.100	64.233.169.104	HTTP	712	GET /images/nav_logo7.png HTTP/1.1
112	2009-09-21 03:43:07.951496	192.168.1.100	64.233.169.104	HTTP	806	GET /csi?v=3&s=webho&action=&tran=undefined&e=17259.21588.21766.21920&ei=
> Frame 56: 689 bytes on wire (5512 bits), 689 bytes captured (5512 bits)						
> 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: 64.233.169.104						
✖ Transmission Control Protocol, Src Port: 4335, Dst Port: 80, Seq: 1, Ack: 1, Len: 635						
Source Port: 4335						
Destination Port: 80						
[Stream index: 2]						
[TCP Segment Len: 635]						
Sequence Number: 1 (relative sequence number)						
Sequence Number (raw): 4164040421						
[Next Sequence Number: 636 (relative sequence number)]						
Acknowledgment Number: 1 (relative ack number)						
Acknowledgment number (raw): 3914283157						
0101 .... = Header Length: 20 bytes (5)						
> Flags: 0x018 (PSH, ACK)						
Window: 65044						
[Calculated window size: 260176]						
[Window size scaling factor: 4]						
Checksum: 0xae3 [unverified]						
[Checksum Status: Unverified]						
Urgent Pointer: 0						
> [SEQ/ACK analysis]						
> [Timestamps]						
TCP_nload (635 bytes)						

Source: 192.168.1.100, 4335 Destination: 64.233.169.104, 80

4/

Time: 7.427932

50	2009-09-21 03:43:07.578402	192.168.1.100	64.233.169.104	HTTP	689 GET / HTTP/1.1
60	2009-09-21 03:43:07.427932	64.233.169.104	192.168.1.100	HTTP	814 HTTP/1.1 200 OK (text/html)
62	2009-09-21 03:43:07.556534	192.168.1.100	64.233.169.104	HTTP	719 GET /intl/en_ALL/images/logo.gif HTTP/1.1
73	2009-09-21 03:43:07.618586	64.233.169.104	192.168.1.100	HTTP	226 HTTP/1.1 200 OK (GIF89a)
75	2009-09-21 03:43:07.639320	192.168.1.100	64.233.169.104	HTTP	809 GET /extern_js/f/CgJlbhIcdXMao4NUAILCswDjgHLCswFjgQLCswFzgL
92	2009-09-21 03:43:07.717784	64.233.169.104	192.168.1.100	HTTP	648 HTTP/1.1 200 OK (text/javascript)
94	2009-09-21 03:43:07.761459	192.168.1.100	64.233.169.104	HTTP	695 GET /extern_chrome/ee36edbd3c16alc5.js HTTP/1.1
100	2009-09-21 03:43:07.806488	64.233.169.104	192.168.1.100	HTTP	870 HTTP/1.1 200 OK (text/html)
107	2009-09-21 03:43:07.921971	192.168.1.100	64.233.169.104	HTTP	712 GET /images/nav_logo7.png HTTP/1.1
112	2009-09-21 03:43:07.951496	192.168.1.100	64.233.169.104	HTTP	806 GET /csi?v=3&s=webhn&action=&tran=undefined&e=17259.21588.2176

> Frame 60: 814 bytes on wire (6512 bits), 814 bytes captured (6512 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: 64.233.169.104, Dst: 192.168.1.100  
 > Transmission Control Protocol, Src Port: 80, Dst Port: 4335, Seq: 2861, Ack: 636, Len: 760  
 > [3 Reassembled TCP Segments (3620 bytes): #58(1430), #59(1430), #60(760)]  
 > Hypertext Transfer Protocol  
 > Line-based text data: text/html (12 lines)

Source: 64.233.169.104, 80 Destination: 192.168.1.100, 4335

5/At 7.344792, the client-to-server TCP SYN segment sent that sets up the connection used by the GET TCP SYN segment (Source: 192.168.1.100, 4335 Destination: 64.233.169.104, 80)

53	2009-09-21 03:43:07.344792	192.168.1.100	64.233.169.104	TCP	66 4335 → 80 [SYN] Seq=0 Win=65535 Len=0 MSS=1460 WS=4 SACK_PERM=1
54	2009-09-21 03:43:07.378121	64.233.169.104	192.168.1.100	TCP	66 80 → 4335 [SYN, ACK] Seq=0 Ack=1 Win=5720 Len=0 MSS=1430 SACK_PERM=1 WS=64
55	2009-09-21 03:43:07.378188	192.168.1.100	64.233.169.104	TCP	54 4335 → 80 [ACK] Seq=1 Ack=1 Win=260176 Len=0
56	2009-09-21 03:43:07.378402	192.168.1.100	64.233.169.104	HTTP	689 GET / HTTP/1.1
57	2009-09-21 03:43:07.409863	64.233.169.104	192.168.1.100	TCP	60 80 → 4335 [ACK] Seq=1 Ack=636 Win=7040 Len=0
58	2009-09-21 03:43:07.427567	64.233.169.104	192.168.1.100	TCP	1484 80 → 4335 [ACK] Seq=1 Ack=636 Win=7040 Len=1430 [TCP segment of a reassembled PDU]
59	2009-09-21 03:43:07.427896	64.233.169.104	192.168.1.100	TCP	1484 80 → 4335 [ACK] Seq=1431 Ack=636 Win=7040 Len=1430 [TCP segment of a reassembled PDU]
60	2009-09-21 03:43:07.427932	64.233.169.104	192.168.1.100	HTTP	814 HTTP/1.1 200 OK (text/html)
61	2009-09-21 03:43:07.427979	192.168.1.100	64.233.169.104	TCP	54 4335 → 80 [ACK] Seq=636 Ack=3621 Win=260176 Len=0

> Frame 53: 66 bytes on wire (528 bits), 66 bytes captured (528 bits)  
 > 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: 64.233.169.104  
 > Transmission Control Protocol, Src Port: 4335, Dst Port: 80, Seq: 0, Len: 0

ACK sent in response to the SYN(Source: 64.233.169.104, 80 Destination: 192.168.1.100, 4335) at time 7.378121

54	2009-09-21 03:43:07.378121	64.233.169.104	192.168.1.100	TCP	66 80 → 4335 [SYN, ACK] Seq=0 Ack=1 Win=5720 Len=0 MSS=1430 SACK_PERM=1 WS=64
55	2009-09-21 03:43:07.378188	192.168.1.100	64.233.169.104	TCP	54 4335 → 80 [ACK] Seq=1 Ack=1 Win=260176 Len=0
56	2009-09-21 03:43:07.378402	192.168.1.100	64.233.169.104	HTTP	689 GET / HTTP/1.1
57	2009-09-21 03:43:07.409863	64.233.169.104	192.168.1.100	TCP	60 80 → 4335 [ACK] Seq=1 Ack=636 Win=7040 Len=0
58	2009-09-21 03:43:07.427567	64.233.169.104	192.168.1.100	TCP	1484 80 → 4335 [ACK] Seq=1 Ack=636 Win=7040 Len=1430 [TCP segment of a reassembled PDU]
59	2009-09-21 03:43:07.427896	64.233.169.104	192.168.1.100	TCP	1484 80 → 4335 [ACK] Seq=1431 Ack=636 Win=7040 Len=1430 [TCP segment of a reassembled PDU]
60	2009-09-21 03:43:07.427932	64.233.169.104	192.168.1.100	HTTP	814 HTTP/1.1 200 OK (text/html)
61	2009-09-21 03:43:07.427979	192.168.1.100	64.233.169.104	TCP	54 4335 → 80 [ACK] Seq=636 Ack=3621 Win=260176 Len=0

> Frame 54: 66 bytes on wire (528 bits), 66 bytes captured (528 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: 64.233.169.104, Dst: 192.168.1.100  
 > Transmission Control Protocol, Src Port: 80, Dst Port: 4335, Seq: 0, Ack: 1, Len: 0

6/

No.	Time	Source	Destination	Protocol	Length	Info
85	2009-09-21 03:43:07.800232	71.192.34.104	64.233.169.104	HTTP	689	GET / HTTP/1.1
86	2009-09-21 03:43:07.823819	Cisco_bf:6c:01	Broadcast	ARP	60	Who has 71.192.35.144? Tell 71.192.32.1
87	2009-09-21 03:43:07.830701	64.233.169.104	71.192.34.104	TCP	60	80 → 4335 [ACK] Seq=1 Ack=636 Win=7040 Len=0
88	2009-09-21 03:43:07.848142	64.233.169.104	71.192.34.104	TCP	1484	80 → 4335 [ACK] Seq=1 Ack=636 Win=7040 Len=1430 [TCP segment of a reassembled PDU]
89	2009-09-21 03:43:07.848471	64.233.169.104	71.192.34.104	TCP	1484	80 → 4335 [ACK] Seq=1431 Ack=636 Win=7040 Len=1430 [TCP segment of a reassembled PDU]
90	2009-09-21 03:43:07.848634	64.233.169.104	71.192.34.104	HTTP	814	HTTP/1.1 200 OK (text/html)
91	2009-09-21 03:43:07.849579	71.192.34.104	64.233.169.104	TCP	60	4335 → 80 [ACK] Seq=636 Ack=3621 Win=260176 Len=0
92	2009-09-21 03:43:07.893155	169.254.255.255	71.192.34.104	NBNS	92	Name query NB HPAB9D4C<00>
93	2009-09-21 03:43:07.972421	71.192.34.104	64.233.169.104	HTTP	719	GET /intl/en_ALL/images/logo.gif HTTP/1.1
94	2009-09-21 03:43:08.004913	64.233.169.104	71.192.34.104	TCP	309	80 → 4335 [PSH, ACK] Seq=3621 Ack=1301 Win=8320 Len=255 [TCP segment of a reassembled PDU]

> 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: Cisco\_bf:6c:01 (00:0e:d6:bf:6c:01)  
 > Internet Protocol Version 4, Src: 71.192.34.104, Dst: 64.233.169.104  
 > Transmission Control Protocol, Src Port: 4335, Dst Port: 80, Seq: 1, Ack: 1, Len: 635  
 > Hypertext Transfer Protocol

->At 7.800232.

-> Source: 71.192.34.104, 4335 Destination: 64.233.169.104, 80

->Only the source IP address has changed

7/ Are any fields in the HTTP GET message changed? (Answer: No)

Which of the following fields in the IP datagram carrying the HTTP GET are changed: Version (Answer: No), Header Length (Answer: No), Flags(Answer: No) , Checksum (Answer: Yes).

If any of these fields have changed, give a reason (in one sentence) stating why this field needed to change. (Answer: Since the IP source address has changed, and the checksum includes the value of the source IP address, the checksum has changed)

8/

90	2009-09-21 03:43:07.848634	64.233.169.104	71.192.34.104	HTTP	814 HTTP/1.1 200 OK (text/html)
91	2009-09-21 03:43:07.849579	71.192.34.104	64.233.169.104	TCP	60 4335 → 80 [ACK] Seq=636 Ack=3621 Win=260176 Len=0
92	2009-09-21 03:43:07.893155	169.254.247.145	169.254.255.255	NBNS	92 Name query NB HPAB9D4C<00>
93	2009-09-21 03:43:07.972421	71.192.34.104	64.233.169.104	HTTP	719 GET /intl/en_ALL/images/logo.gif HTTP/1.1
94	2009-09-21 03:43:08.004913	64.233.169.104	71.192.34.104	TCP	309 80 → 4335 [PSH, ACK] Seq=3621 Ack=1301 Win=8320 Len=255 [TCP segment of a reassembled PDU]

> Frame 90: 814 bytes on wire (6512 bits), 814 bytes captured (6512 bits)

> Ethernet II, Src: Cisco\_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: 2861, Ack: 636, Len: 760

> [3 Reassembled TCP Segments (3620 bytes): #88(1430), #89(1430), #90(760)]

> Hypertext Transfer Protocol

> Line-based text data: text/html (12 lines)

->At 7.848634

-> Source: 64.233.169.104, 80 Destination: 71.192.34.104, 4335

-> only the destination IP address has changed

9/

82	2009-09-21 03:43:07.766539	71.192.34.104	64.233.169.104	TCP	66 4335 → 80 [SYN] Seq=0 Win=65535 Len=0 MSS=1460 WS=4 SACK_PERM=1
83	2009-09-21 03:43:07.798839	64.233.169.104	71.192.34.104	TCP	66 80 → 4335 [SYN, ACK] Seq=0 Ack=1 Win=5720 Len=0 MSS=1430 SACK_PERM=1 WS=64
84	2009-09-21 03:43:07.799818	71.192.34.104	64.233.169.104	TCP	60 4335 → 80 [ACK] Seq=1 Ack=1 Win=260176 Len=0
85	2009-09-21 03:43:07.800232	71.192.34.104	64.233.169.104	HTTP	689 GET / HTTP/1.1
86	2009-09-21 03:43:07.823819	Cisco_bf:6c:01	Broadcast	ARP	60 Who has 71.192.35.144? Tell 71.192.32.1
87	2009-09-21 03:43:07.830701	64.233.169.104	71.192.34.104	TCP	60 80 → 4335 [ACK] Seq=1 Ack=636 Win=7040 Len=0
88	2009-09-21 03:43:07.848142	64.233.169.104	71.192.34.104	TCP	1484 80 → 4335 [ACK] Seq=1 Ack=636 Win=7040 Len=1430 [TCP segment of a reassembled PDU]

> 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: Cisco\_bf:6c:01 (00:0e:d6:bf:6c:01)

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

> Transmission Control Protocol, Src Port: 4335, Dst Port: 80, Seq: 0, Len: 0

82	2009-09-21 03:43:07.766539	71.192.34.104	64.233.169.104	TCP	66 4335 → 80 [SYN] Seq=0 Win=65535 Len=0 MSS=1460 WS=4 SACK_PERM=1
83	2009-09-21 03:43:07.798839	64.233.169.104	71.192.34.104	TCP	66 80 → 4335 [SYN, ACK] Seq=0 Ack=1 Win=5720 Len=0 MSS=1430 SACK_PERM=1 WS=64
84	2009-09-21 03:43:07.799818	71.192.34.104	64.233.169.104	TCP	60 4335 → 80 [ACK] Seq=1 Ack=1 Win=260176 Len=0
85	2009-09-21 03:43:07.800232	71.192.34.104	64.233.169.104	HTTP	689 GET / HTTP/1.1
86	2009-09-21 03:43:07.823819	Cisco_bf:6c:01	Broadcast	ARP	60 Who has 71.192.35.144? Tell 71.192.32.1
87	2009-09-21 03:43:07.830701	64.233.169.104	71.192.34.104	TCP	60 80 → 4335 [ACK] Seq=1 Ack=636 Win=7040 Len=0
88	2009-09-21 03:43:07.848142	64.233.169.104	71.192.34.104	TCP	1484 80 → 4335 [ACK] Seq=1 Ack=636 Win=7040 Len=1430 [TCP segment of a reassembled PDU]

> Frame 83: 66 bytes on wire (528 bits), 66 bytes captured (528 bits)

> Ethernet II, Src: Cisco\_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: 0, Ack: 1, Len: 0

->At 7.766539 and 7.798849 respectively

-> Source: 71.192.34.104, 4335 Destination: 64.233.169.104, 80.

-> Source: 64.233.169.104, 80 Destination: 71.192.34.104, 4335

-> for the SYN, the source IP address has changed, For the ACK, the destination IP address has changed.  
The port numbers are unchanged.

10/

NAT translate:

+ WAN side: 71.192.34.104, 4335

+ LAN side: 192.168.1.100, 4335