```
    20 16:43:01.841450    192.168.1.100         74.125.106.31         HTTP     767    GET /safebrowsing/rd/goog-malware-
shavar_s_15361-15365.15361-15365.: HTTP/1.1
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: 0.043667000 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:http]
    [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)
    Destination: Cisco-Li_45:1f:1b (00:22:6b:45:1f:1b)
        Address: Cisco-Li_45:1f:1b (00:22:6b:45:1f:1b)
        .... ..0. .... .... .... .... = LG bit: Globally unique address (factory default)
        .... ...0 .... .... .... .... = IG bit: Individual address (unicast)
    Source: HonHaiPr_0d:ca:8f (00:22:68:0d:ca:8f)
        Address: HonHaiPr_0d:ca:8f (00:22:68:0d:ca:8f)
        .... ..0. .... .... .... .... = LG bit: Globally unique address (factory default)
        .... ...0 .... .... .... .... = IG bit: Individual address (unicast)
    Type: IPv4 (0x0800)
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)
        0000 00.. = Differentiated Services Codepoint: Default (0)
        .... ..00 = Explicit Congestion Notification: Not ECN-Capable Transport (0)
    Total Length: 753
    Identification: 0xa27e (41598)
    Flags: 0x02 (Don't Fragment)
        0... .... = Reserved bit: Not set
        .1.. .... = Don't fragment: Set
        ..0. .... = More fragments: Not set
    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
    [Stream index: 1]
    [TCP Segment Len: 713]
    Sequence number: 1    (relative sequence number)
    [Next sequence number: 714    (relative sequence number)]
    Acknowledgment number: 1    (relative ack number)
    0101 .... = Header Length: 20 bytes (5)
    Flags: 0x018 (PSH, ACK)
        000. .... .... = Reserved: Not set
        ...0 .... .... = Nonce: Not set
        .... 0... .... = Congestion Window Reduced (CWR): Not set
        .... .0.. .... = ECN-Echo: Not set
        .... ..0. .... = Urgent: Not set
        .... ...1 .... = Acknowledgment: Set
        .... .... 1... = Push: Set
        .... .... .0.. = Reset: Not set
        .... .... ..0. = Syn: Not set
        .... .... ...0 = Fin: Not set
        [TCP Flags: ·······AP···]
    Window size value: 65044
    [Calculated window size: 260176]
    [Window size scaling factor: 4]
    Checksum: 0x798c [unverified]
    [Checksum Status: Unverified]
    Urgent pointer: 0
    [SEQ/ACK analysis]
        [iRTT: 0.022008000 seconds]
        [Bytes in flight: 713]
        [Bytes sent since last PSH flag: 713]
```

```
    TCP payload (713 bytes)
Hypertext Transfer Protocol
    GET /safebrowsing/rd/goog-malware-shavar_s_15361-15365.15361-15365.: HTTP/1.1\r\n
        [Expert Info (Chat/Sequence): GET /safebrowsing/rd/goog-malware-shavar_s_15361-15365.15361-15365.: HTTP/1.1\r\n]
        Request Method: GET
        Request URI: /safebrowsing/rd/goog-malware-shavar_s_15361-15365.15361-15365.:
        Request Version: HTTP/1.1
    Host: safebrowsing-cache.google.com\r\n
    User-Agent: Mozilla/5.0 (Windows; U; Windows NT 5.1; en-US; rv:1.9.0.14) Gecko/2009082707 Firefox/3.0.14 (.NET CLR 3.5.30729)\r\n
    Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8\r\n
    Accept-Language: en-us,en;q=0.5\r\n
    Accept-Encoding: gzip,deflate\r\n
    Accept-Charset: ISO-8859-1,utf-8;q=0.7,*;q=0.7\r\n
    Keep-Alive: 300\r\n
    Connection: keep-alive\r\n
     [truncated]Cookie: PREF=ID=bf5d0bb622fc0544:U=f3b005fc50a5d6e7:TM=1248148747:LM=1250937140:GM=1:S=JrvbEJK_1TdhMdJS;
NID=27=nBKmwWULTZsu7LjKEy9DazS3cvQEGC3qQJWZLVAdIo4X26oEbAcAqAyesnEZccqTF0l3F7q549rdZPw588xqiEGBAWz_7kPPbeoN5XQohmdQvgLcPFX
        Cookie pair: PREF=ID=bf5d0bb622fc0544:U=f3b005fc50a5d6e7:TM=1248148747:LM=1250937140:GM=1:S=JrvbEJK_1TdhMdJS
        Cookie pair:
NID=27=nBKmwWULTZsu7LjKEy9DazS3cvQEGC3qQJWZLVAdIo4X26oEbAcAqAyesnEZccqTF0l3F7q549rdZPw588xqiEGBAWz_7kPPbeoN5XQohmdQvgLcPFXJ-3kk5h9JX2gD
    \r\n
    [Full request URI: http://safebrowsing-cache.google.com/safebrowsing/rd/goog-malware-shavar_s_15361-15365.15361-15365.:]
    [HTTP request 1/4]
    [Response in frame: 39]
    [Next request in frame: 41]
```