



http.host contains "willselfdestruct.com"

No.	Time	Source	Destination	Protocol	Length	Info
83654	15197.806879	192.168.15.4	69.25.94.22	HTTP	360	GET /images/bk-message.gif HTTP/1.1
83072	15157.435074	192.168.15.4	69.25.94.22	HTTP	356	GET /images/body-bk.gif HTTP/1.1
83162	15157.756987	192.168.15.4	69.25.94.22	HTTP	361	GET /images/bridge_small.gif HTTP/1.1
83087	15157.503801	192.168.15.4	69.25.94.22	HTTP	358	GET /images/btn-send.gif HTTP/1.1
83025	15157.238976	192.168.15.4	69.25.94.22	HTTP	356	GET /images/sm-logo.gif HTTP/1.1
82985	15157.030671	192.168.15.4	69.25.94.22	HTTP	355	GET /images/spacer.gif HTTP/1.1
83037	15157.279305	192.168.15.4	69.25.94.22	HTTP	361	GET /images/warning-home.gif HTTP/1.1
82936	15156.730593	192.168.15.4	69.25.94.22	HTTP	596	GET /secure/submit HTTP/1.1
83614	15197.468887	192.168.15.4	69.25.94.22	HTTP	461	GET /secure/success HTTP/1.1
83601	15197.216422	192.168.15.4	69.25.94.22	HTTP	719	POST /secure/submit HTTP/1.1 (application/x-www-form-urlencoded)

> Frame 83654: 360 bytes on wire (2880 bits), 360 bytes captured (2880 bits)  
✓ Ethernet II, Src: Apple\_e2:c0:ce (00:17:f2:e2:c0:ce), Dst: HonHaiPrecis\_2e:4f:60 (00:1d:d9:2e:4f:60)

Destination: HonHaiPrecis\_2e:4f:60 (00:1d:d9:2e:4f:60)

.....0. .... = LG bit: Globally unique address (factory default)

.....0. .... = IG bit: Individual address (unicast)

Source: Apple\_e2:c0:ce (00:17:f2:e2:c0:ce)

.....0. .... = LG bit: Globally unique address (factory default)

.....0. .... = IG bit: Individual address (unicast)

Type: IPv4 (0x0800)

[Stream index: 19]

Frame check sequence: 0x0af5e170 [unverified]

[FCS Status: Unverified]

> Internet Protocol Version 4, Src: 192.168.15.4, Dst: 69.25.94.22

> Transmission Control Protocol, Src Port: 36048, Dst Port: 80, Seq: 1, Ack: 1, Len: 290

✓ Hypertext Transfer Protocol

> GET /images/bk-message.gif HTTP/1.1\r\n

Accept: \*/\*\r\n

Referer: http://www.willselfdestruct.com/secure/success\r\n

Accept-Language: en-us\r\n

Accept-Encoding: gzip, deflate\r\n

User-Agent: Mozilla/4.0 (compatible; MSIE 6.0; Windows NT 5.1; SV1)\r\n

Host: www.willselfdestruct.com\r\n

Connection: Keep-Alive\r\n

\r\n

[Response in frame: 83705]

[Full request URI: http://www.willselfdestruct.com/images/bk-message.gif]

```
0000 00 1d d9 2e 4f 60 00 17 f2 e2 c0 ce 08 00 45 00 ...0`... ..E·
0010 01 56 e4 a2 40 00 3f 06 e3 23 c0 a8 0f 04 45 19 ·V·@·?· ·#···E·
0020 5e 16 8c d0 00 50 05 7a 8e aa 56 eb 1f a0 80 18 ^····P·z ··V····
0030 fb 28 95 8e 00 00 01 01 08 0a 26 63 20 7e 73 00 ·(····· ··8c ~s·
0040 cd e5 47 45 54 20 2f 69 6d 61 67 65 73 2f 62 6b ··GET /i mages/bk
0050 2d 6d 65 73 73 61 67 65 2e 67 69 66 20 48 54 54 -message .gif HTT
0060 50 2f 31 2e 31 0d 0a 41 63 63 65 70 74 3a 20 2a P/1.1·A ccept: *
0070 2f 2a 0d 0a 52 65 66 65 72 65 72 3a 20 68 74 74 /*·Refe rer: htt
0080 70 3a 2f 2f 77 77 77 2e 77 69 6c 6c 73 65 6c 66 p://www. willself
0090 64 65 73 74 72 75 63 74 2e 63 6f 6d 2f 73 65 63 destruct .com/sec
00a0 75 72 65 2f 73 75 63 63 65 73 73 0d 0a 41 63 63 ure/succ ess·Acc
00b0 65 70 74 2d 4c 61 6e 67 75 61 67 65 3a 20 65 6e ept-Lang uage: en
00c0 2d 75 73 0d 0a 41 63 63 65 70 74 2d 45 6e 63 6f -us·Acc ept-Enco
00d0 64 69 6e 67 3a 20 67 7a 69 70 2c 20 64 65 66 6c ding: gz ip, defl
00e0 61 74 65 0d 0a 55 73 65 72 2d 41 67 65 6e 74 3a ate·Use r-Agent:
00f0 20 4d 6f 7a 69 6c 6c 61 2f 34 2e 30 20 28 63 6f Mozilla /4.0 (co
0100 6d 70 61 74 69 62 6c 65 3b 20 4d 53 49 45 20 36 mpatible ; MSIE 6
0110 2e 30 3b 20 57 69 6e 64 6f 77 73 20 4e 54 20 35 .0; Wind ows NT 5
0120 2e 31 3b 20 53 56 31 29 0d 0a 48 6f 73 74 3a 20 .1; SV1) ··Host:
0130 77 77 77 2e 77 69 6c 6c 73 65 6c 66 64 65 73 74 www.will selfdest
0140 72 75 63 74 2e 63 6f 6d 0d 0a 43 6f 6e 6e 65 63 ruct.com ··Connec
0150 74 69 6f 6e 3a 20 4b 65 65 70 2d 41 6c 69 76 65 tion: Ke ep-Alive
0160 0d 0a 0d 0a 0a f5 e1 70 ·····p
```