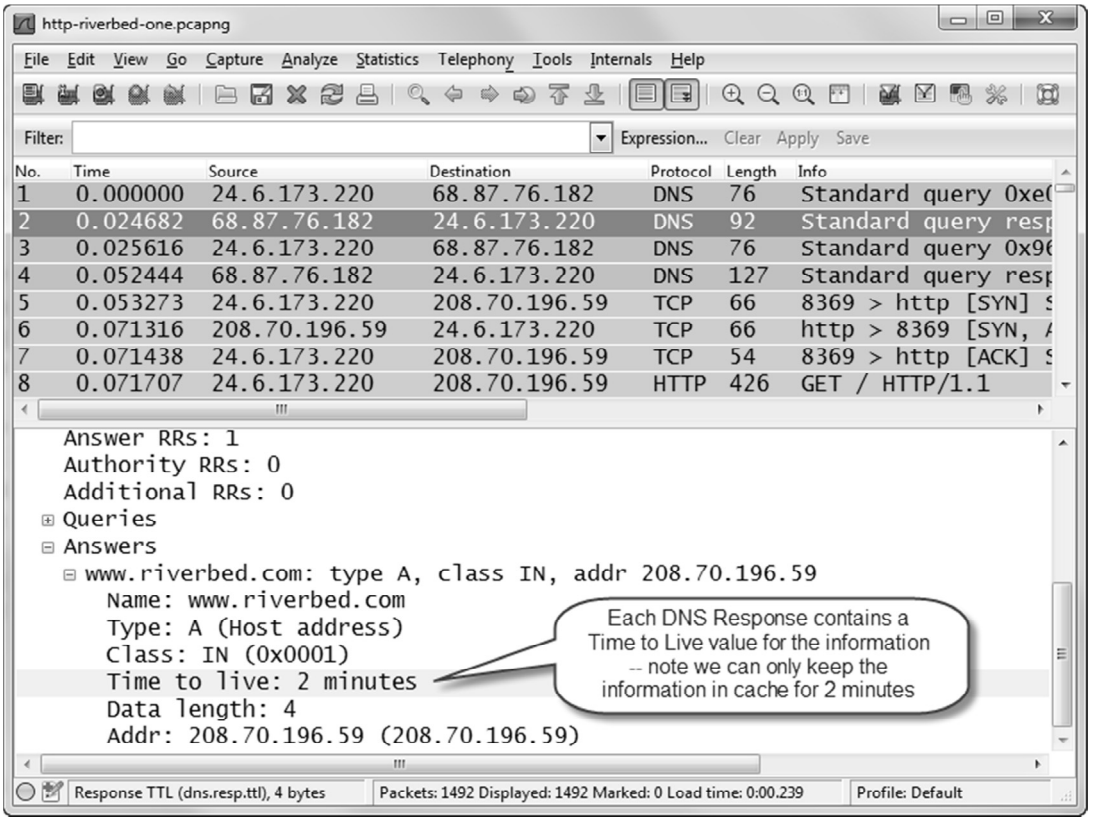

Figure 183. Following the process of browsing to a website [http-riverbed-one.pcapng]

When examining *http-riverbed-one.pcapng*, we can learn the following:

1. There are no ARP queries in the trace file. The client, 24.6.173.220 must have the required MAC addresses in ARP cache. We can run `arp -a` to view the contents of the ARP cache.

2. We see DNS queries for *www.riverbed.com*. This query indicates that the client does not have the IP address for *www.riverbed.com* in DNS cache. In our example, the client is running both IPv4 and IPv6 stacks so it makes DNS queries for both the A record (IPv4 address) and AAAA record (IPv6 address) of *www.riverbed.com*.

3. The client receives a DNS response providing the IPv4 address of *www.riverbed.com* in packet 2. The IPv4 address received in packet 2 is now placed in the client's DNS cache and can remain in the cache for the time defined in the Time to Live field in the DNS Answer section of packet 2—just 2 minutes. Note that the client made a DNS query for the AAAA record, but the response in packet 4 does not provide an IPv6 address—it only contains the authoritative name server for that domain. The client will not be able to communicate with *www.riverbed.com* using IPv6.

4. In packet 5, the client begins the TCP handshake by sending a TCP SYN using the dynamic source port 8369 and destination port 80. The packet is sent to the hardware address of the default gateway and the IP address of *www.riverbed.com*.