Figure 1. Polymorphed Apache-Knacker exploit. Unshaded content represents wildcard bytes; lightly shaded content represents code bytes; heavily shaded content represents invariant bytes.

QNAME [Return Address] | QTYPE QCLASS

NAME [0x00] | TYPE [TSIG] | CLASS

DNS Header | Record Counts | Question 1 [Obfuscated Shellcode] | Question 2 | Additional Record
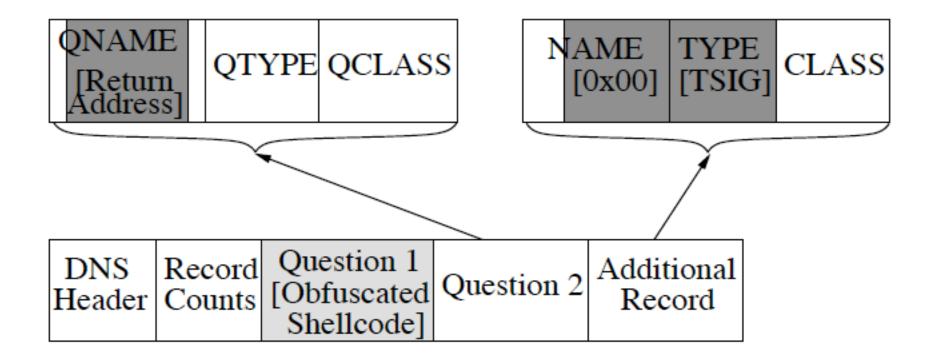
Figure 2. BIND TSIG vulnerability, as exploited by the Lion worm. Shading as for Apache vulnerability.