WHOIS Information for a Domain Name

The most efficient method to find accurate WHOIS information for a domain name is to start from the top-level domain and work down. The following "Received" header will be used as an example:

This header shows that the receiving mail server recorded the sender's IP address to be 209.51.220.12 and its domain name to be b2bpost.com, which matches the HELO information provided by the sender. A quick *nslookup* of the recorded IP address verifies that the email did, in fact, come from the b2bpost.com domain.

The first step to take is to find out the WHOIS server for the .com domain. This is done by querying the WHOIS database for the Internet Assigned Number Authority (IANA), which is whois.iana.org. The command for this query is `whois com@whois.iana.org`.

Figure 80 displays the results.

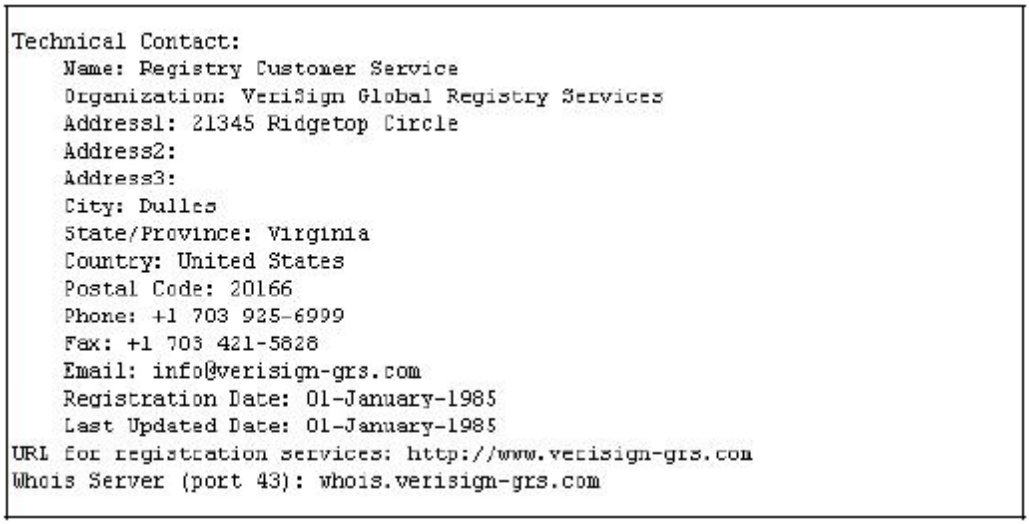

Figure 80: WHOIS *Query of IANA*

Among the information that is returned from the query is the WHOIS server, whois.verisigngrs. com, for the .com domain. One can be assured that querying this server will yield information regarding b2bpost.com. Sure enough, the following query yields the information shown in Figure 81:

```
whois b2bpost.com@whois.verisign-grs.com
```

Geobytes - because everyone's somewhere. http://www.geobytes.com/IpLocator.htm