

Domain name system

[Technology](#), [Internet](#)



1. Which reconnaissance tool comes with Microsoft Windows that can provide and can be initiated from the DOS command prompt? What useful information does this query provide? Sam Spade - Zone Transfer ask a DNS server for all it knows about a domain, SMTP Relay Check whether a mail server allows third party relaying, Scan Addresses scan a range of IP addresses looking for open ports, Crawl website search a website, looking for email addresses, offsite links, etc., Browse web browse the web in a raw http format, Check cancels search your news server for cancel messages, Fast and Slow Traceroute find the route packets take between you and a remote system, S-Lang command issue a scripting command; useful for debugging scripts, Decode URL decipher an obfuscated URL, Parse email headers read email headers and make a guess about the origin of the email

2. What is the difference between ARIN, RIPE, IANA? What regions of the world do these domain name registry organizations cover? ARIN - North America, Africa below the equator and parts of the Caribbean. APNIC - Asia and Pacific Region, LACNIC - Latin America and parts of the Caribbean, and RIPE - Europe, parts of Asia, Africa above the equator, and the Middle East.

3. What other functions can be completed using the Sam Spade Utility? ping, traceroute, whois, finiger, nslookup

4. What is the purpose of the traceroute command? What useful information does traceroute provide? How can this information be used to attack the targeted website? It traces the routes packets from the user to the target, it shows a packets hops to the target, and they target the host address.

5. What important information can be gleaned from a whois record for a website? Whois provides ownership and contact information for the specified host's domain.
6. How many different Whois profiles are pre-loaded in the Sam Spade Utility? 100
7. Is Sam Spade an intrusive tool? What is your perspective on the use of a freeware utility such as Sam Spade? No, Anything that is free that can help out on a task is always good.
8. What do you think companies and organizations should do in regards to access to whois information in the public domain? Make sure that their network is secure.
9. What icon or function in Sam Spade downloads the entire HTML code of the targeted website? Browse Web
10. Why would someone use a proxy in order to perform data gathering from a remote website? A server is not always able to connect directly to the monitored machines.