

DNS Reconnaissance



Website – www.wikitechy.com

Youtube – [Wikitechy code](https://www.youtube.com/Wikitechycode)

Company – www.kaashivinfotech.com

<http://www.kaashivinfotech.com/>



What we offer

Inplant
Training

Internship
Training

Domain Name System (DNS) – Reconnaissance

DNS Lookup

- Tools help Internet users discover the DNS names of target computers
- Web sites that provide DNS lookup tools

www.dnsstuff.com

www.network-tools.com

www.networksolutions.com

DNS Zone Transfer

- Every DNS server has a name space, known as a zone
- A zone stores data about domain names

Domain Name System (DNS) – Reconnaissance

DNS Zone Transfer

- Zone transfer is a DNS feature that lets a DNS server update its database
 - With the list of domain names in another DNS server
- An incorrectly configured DNS server may allow any Internet user to perform a zone transfer
- Commands to perform a DNS zone transfer
 - **nslookup**
 - Allows anyone to query a DNS server for information
 - **host**
 - Program that permits you to perform DNS lookup
 - **dig**
 - Domain information groper (dig)
 - Used to collect DNS-related data

Domain Name System (DNS) – Reconnaissance

DNS Zone Transfer

- Commands to perform a DNS zone transfer
 - **ping**
 - Part of the Internet Control Message Protocol (ICMP)
 - Helps to verify whether a host is active
 - Command is available for all platforms
 - There are two ping utilities available for a Linux or Unix machine: ping and ping6
 - **traceroute**
 - A request for a Web page that resides on a remote server must pass through several servers on its way
 - Command can track all of the intermediate servers

Domain Name System (DNS) – Reconnaissance

```
★ Terminal
File Edit View Terminal Tabs Help

wolf@Ubuntu-Ultrix:~$ nslookup -type=any NS1.NETSOL.COM
Server:          192.168.0.1
Address:         192.168.0.1#53

Non-authoritative answer:
Name:   NS1.NETSOL.COM
Address: 216.168.229.228

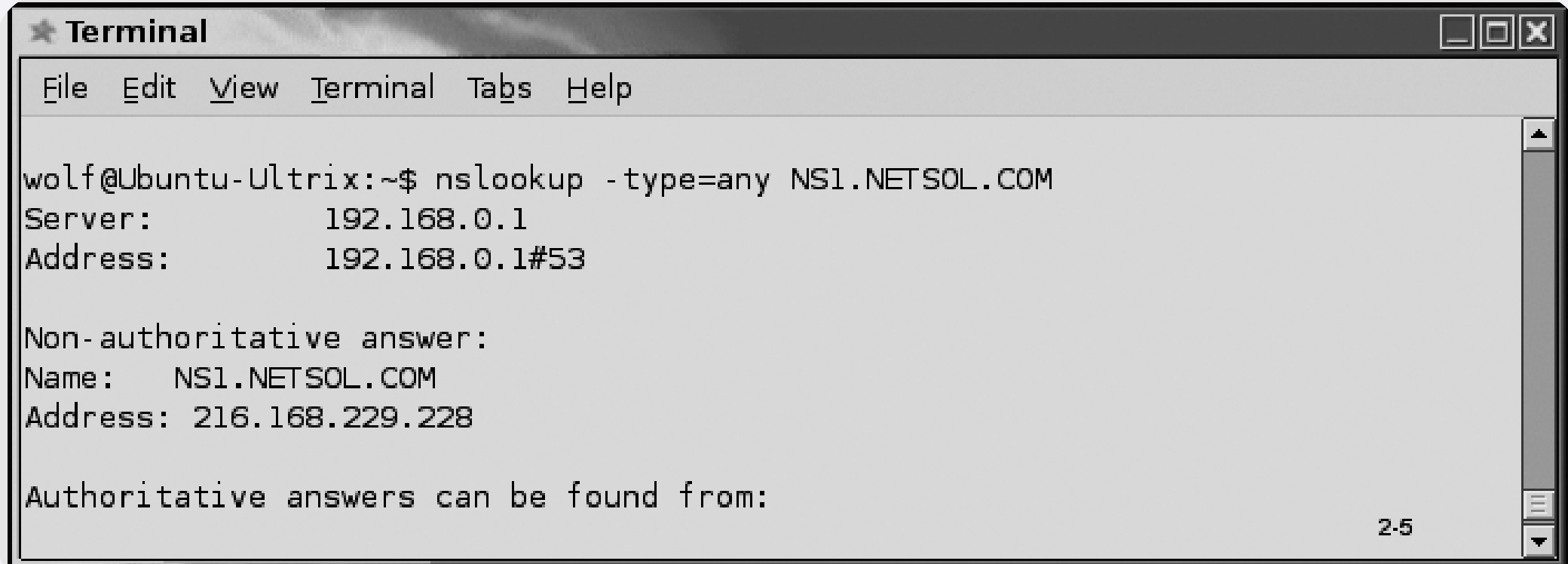
Authoritative answers can be found from:

2-5
```

```
Authoritative answers can be found from:

3-2
```

Domain Name System (DNS) – Reconnaissance



```
★ Terminal
File Edit View Terminal Tabs Help

wolf@Ubuntu-Ultrix:~$ nslookup -type=any NS1.NETSOL.COM
Server:          192.168.0.1
Address:         192.168.0.1#53

Non-authoritative answer:
Name:   NS1.NETSOL.COM
Address: 216.168.229.228

Authoritative answers can be found from:

2-5
```



```
Authoritative answers can be found from:

2-5
```

Domain Name System (DNS) – Reconnaissance

DNS Zone Transfer

- **Commands to perform a DNS zone transfer**
 - **netstat**
 - Allows all the transmission Control Protocol (TCP), User Datagram Protocol (UDP), and IP connections on a computer to be viewed
 - Also helps to locate
 - IP address of computers
 - IP addresses of the hosts connected to the computers
 - Port of the host to which a computer is connected

Domain Name System (DNS) – Reconnaissance

```
★ Terminal
File Edit View Terminal Tabs Help
wolf@Ubuntu-Ultrix:~$ host -v networksolutions.com
Trying "networksolutions.com"
;; ->>HEADER<<- opcode: QUERY, status: NOERROR, id: 16104
;; flags: qr rd ra; QUERY: 1, ANSWER: 1, AUTHORITY: 0, ADDITIONAL: 0

;; QUESTION SECTION:
;netsolutions.com.          IN      A

;; ANSWER SECTION:
networksolutions.com.  300     IN      A      205.178.187.13

Received 54 bytes from 192.168.0.1#53 in 60 ms
Trying "networksolutions.com"
;; ->>HEADER<<- opcode: QUERY, status: NOERROR, id: 21572
;; flags: qr rd ra; QUERY: 1, ANSWER: 0, AUTHORITY: 1, ADDITIONAL: 0

;; QUESTION SECTION:
;netsolutions.com.          IN      AAAA

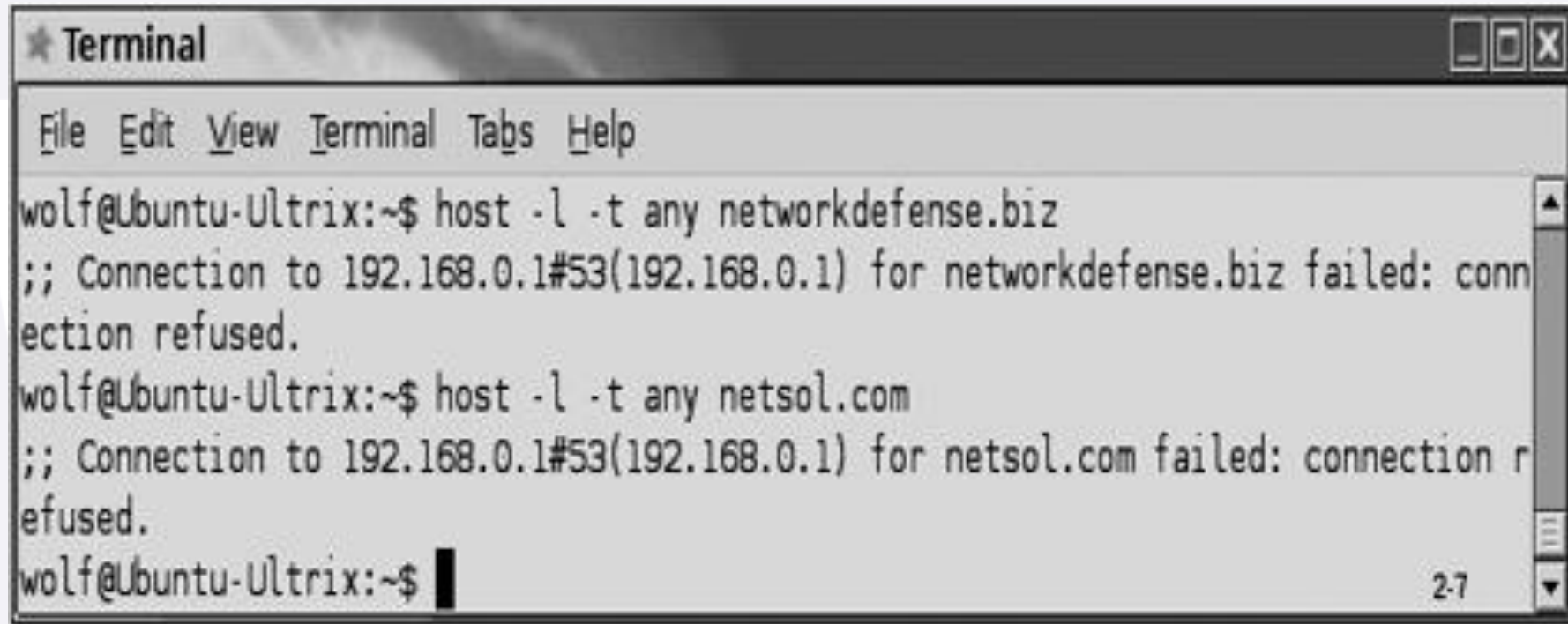
;; AUTHORITY SECTION:
networksolutions.com.  300     IN      SOA     ns1.netsol.com. dnsadmin.network
solutions.com. 2006042004 7200 3600 604800 3600

Received 94 bytes from 192.168.0.1#53 in 26 ms
Trying "networksolutions.com"
;; connection timed out; no servers could be reached
wolf@Ubuntu-Ultrix:~$
```

W

Y

Domain Name System (DNS) – Reconnaissance



```
★ Terminal
File Edit View Terminal Tabs Help
wolf@Ubuntu-Ultrix:~$ host -l -t any networkdefense.biz
;; Connection to 192.168.0.1#53(192.168.0.1) for networkdefense.biz failed: connection refused.
wolf@Ubuntu-Ultrix:~$ host -l -t any netsol.com
;; Connection to 192.168.0.1#53(192.168.0.1) for netsol.com failed: connection refused.
wolf@Ubuntu-Ultrix:~$ █
```

The image shows a terminal window titled "Terminal" with a menu bar containing "File", "Edit", "View", "Terminal", "Tabs", and "Help". The terminal output shows two commands being executed. The first command is `host -l -t any networkdefense.biz`, which results in the message: `;; Connection to 192.168.0.1#53(192.168.0.1) for networkdefense.biz failed: connection refused.` The second command is `host -l -t any netsol.com`, which results in the message: `;; Connection to 192.168.0.1#53(192.168.0.1) for netsol.com failed: connection refused.` The prompt `wolf@Ubuntu-Ultrix:~$` is visible at the end of the output, followed by a cursor. In the bottom right corner of the terminal window, the page number "2-7" is displayed.

Our Official Website

<http://www.kaashivinfotech.com/>



<https://www.wikitechy.com/>



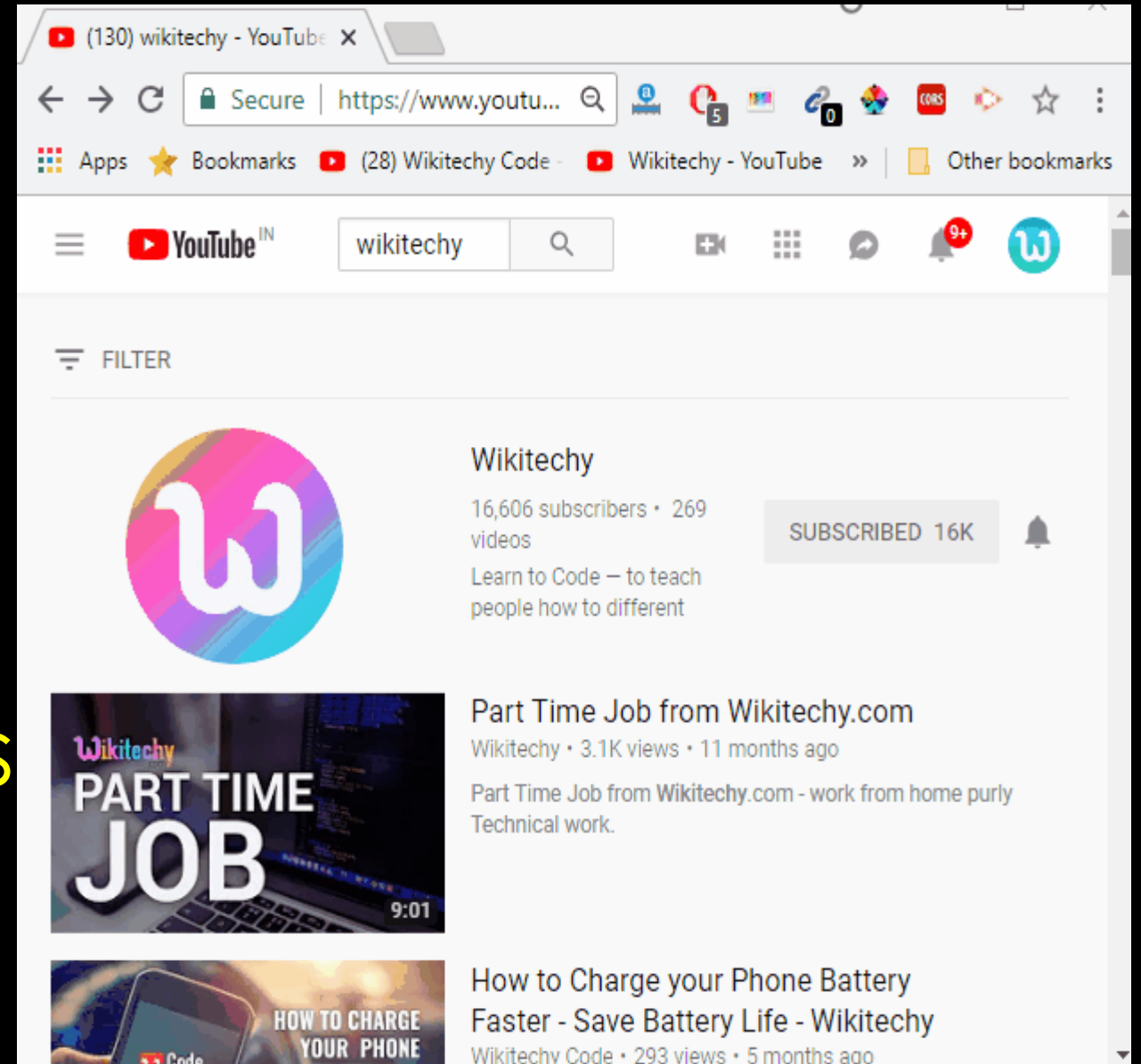
Our Youtube Channel

Wikitechy

Wikitechy code

Wikitechy Interview Tips

Wikitechy School



The image shows a screenshot of a web browser displaying the Wikitechy YouTube channel page. The browser's address bar shows the URL <https://www.youtube.com/channel/UC...>. The YouTube interface includes a search bar with the text "wikitechy" and a search icon. Below the search bar, there is a "FILTER" button. The channel's profile picture is a circular logo with a white 'W' on a colorful gradient background. To the right of the profile picture, the channel name "Wikitechy" is displayed, along with "16,606 subscribers • 269 videos". A "SUBSCRIBED 16K" button is visible, along with a notification bell icon. Below the channel information, there are two video thumbnails. The first video is titled "Part Time Job from Wikitechy.com" and has 3.1K views, posted 11 months ago. The second video is titled "How to Charge your Phone Battery Faster - Save Battery Life - Wikitechy" and has 293 views, posted 5 months ago.

THANK YOU

Pls Share to UR Friends