

Network 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

Network Based – Reconnaissance

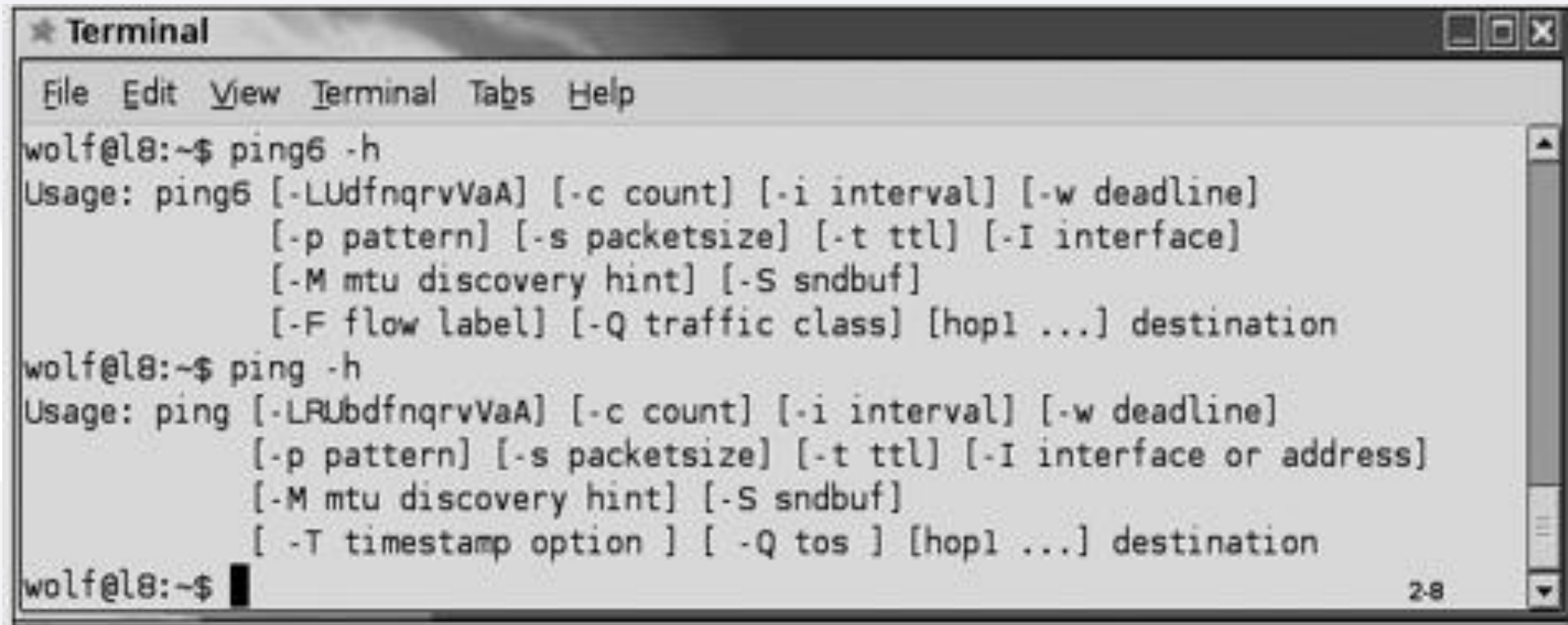
➤ ping

- 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

Network Based – Reconnaissance

A screenshot of a terminal window titled "Terminal" with standard window controls. The terminal shows the user "wolf@l8" at the prompt "~\$". They have entered "ping6 -h" and "ping -h", both of which display the usage and options for their respective commands. The "ping6" help text lists options like [-LUdfnqrVvA], [-c count], [-i interval], [-w deadline], [-p pattern], [-s packetsize], [-t ttl], [-I interface], [-M mtu discovery hint], [-S sndbuf], [-F flow label], and [-Q traffic class]. The "ping" help text lists options like [-LRUdbfnqrVvA], [-c count], [-i interval], [-w deadline], [-p pattern], [-s packetsize], [-t ttl], [-I interface or address], [-M mtu discovery hint], [-S sndbuf], [-T timestamp option], and [-Q tos]. The terminal ends with the prompt "wolf@l8:~\$" and a cursor. A page number "2-8" is visible in the bottom right corner of the terminal window.

```
★ Terminal
File Edit View Terminal Tabs Help

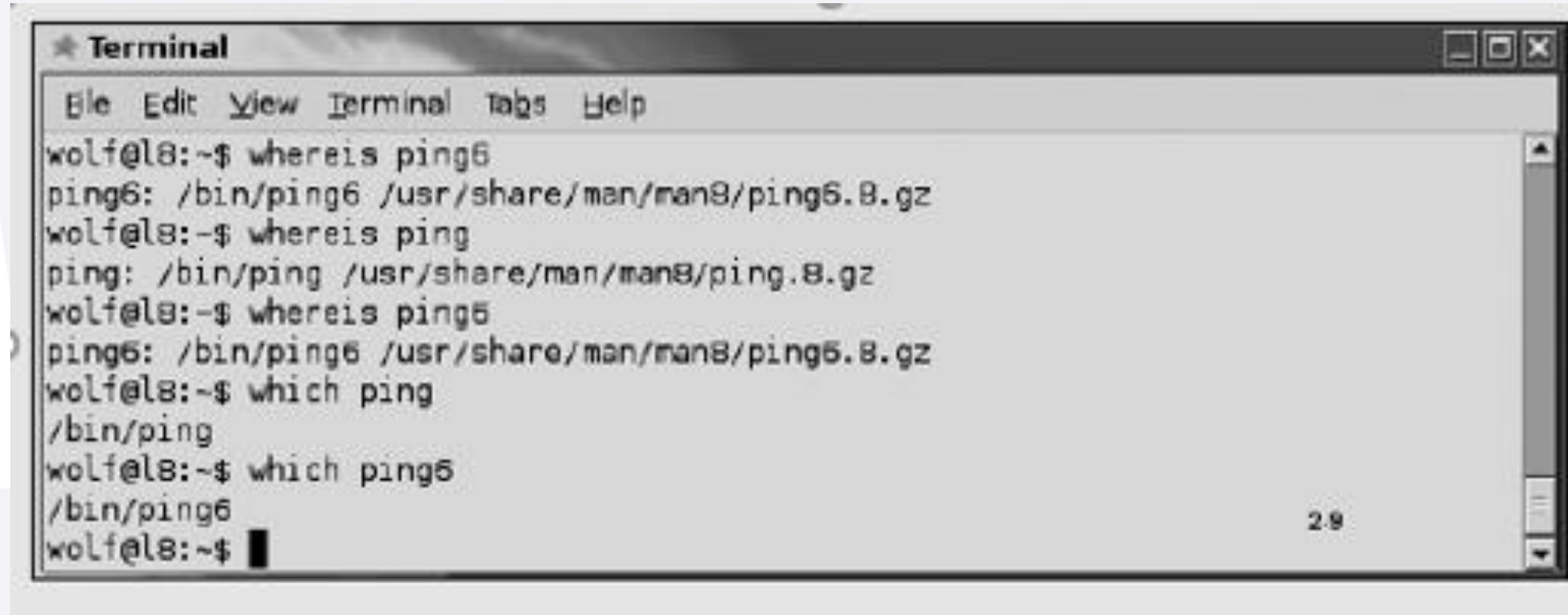
wolf@l8:~$ ping6 -h
Usage: ping6 [-LUdfnqrVvA] [-c count] [-i interval] [-w deadline]
           [-p pattern] [-s packetsize] [-t ttl] [-I interface]
           [-M mtu discovery hint] [-S sndbuf]
           [-F flow label] [-Q traffic class] [hop1 ...] destination

wolf@l8:~$ ping -h
Usage: ping [-LRUdbfnqrVvA] [-c count] [-i interval] [-w deadline]
          [-p pattern] [-s packetsize] [-t ttl] [-I interface or address]
          [-M mtu discovery hint] [-S sndbuf]
          [ -T timestamp option ] [ -Q tos ] [hop1 ...] destination

wolf@l8:~$
```

2-8

Network Based – Reconnaissance



A terminal window titled "Terminal" with a menu bar (File, Edit, View, Terminal, Tabs, Help) and standard window controls. The terminal shows a series of commands and their outputs for finding the location of 'ping' and 'ping6' binaries. The user 'wolf' is at host 'ls' in the home directory. The commands and outputs are as follows:

```
wolf@ls:~$ whereis ping6
ping6: /bin/ping6 /usr/share/man/man8/ping6.8.gz
wolf@ls:~$ whereis ping
ping: /bin/ping /usr/share/man/man8/ping.8.gz
wolf@ls:~$ whereis ping6
ping6: /bin/ping6 /usr/share/man/man8/ping6.8.gz
wolf@ls:~$ which ping
/bin/ping
wolf@ls:~$ which ping6
/bin/ping6
wolf@ls:~$
```

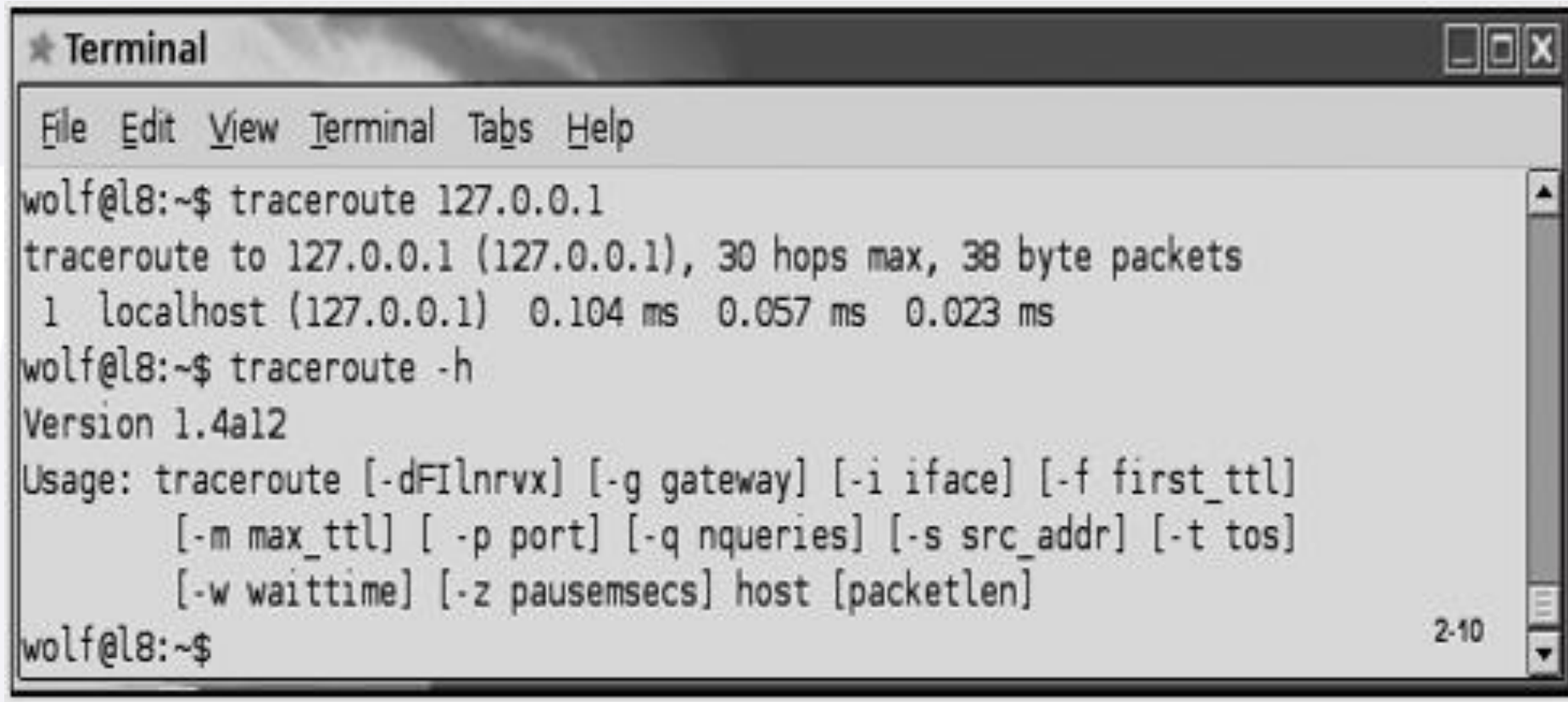
The terminal has a scrollbar on the right side and a status bar at the bottom right showing the number "29".

Network Based – Reconnaissance

➤ traceroute

- In UNIX-based operating systems use traceroute command
- In Windows operating systems use tracert command

Network Based – Reconnaissance



A terminal window titled "Terminal" with a menu bar (File, Edit, View, Terminal, Tabs, Help) and window control buttons. The terminal shows the execution of the `traceroute` command to `127.0.0.1`, displaying a single hop to localhost with three timing measurements. Subsequently, the `traceroute -h` command is used to display the help text for version 1.4a12, which lists various command-line options for customizing the traceroute. The prompt `wolf@l8:~$` is visible at the end of the output.

```
★ Terminal
File Edit View Terminal Tabs Help
wolf@l8:~$ traceroute 127.0.0.1
traceroute to 127.0.0.1 (127.0.0.1), 30 hops max, 38 byte packets
 1 localhost (127.0.0.1)  0.104 ms  0.057 ms  0.023 ms
wolf@l8:~$ traceroute -h
Version 1.4a12
Usage: traceroute [-dFIlnrvx] [-g gateway] [-i iface] [-f first_ttl]
               [-m max_ttl] [-p port] [-q nqueries] [-s src_addr] [-t tos]
               [-w waittime] [-z pausesecs] host [packetlen]
wolf@l8:~$
```

Network Based – Reconnaissance

➤ 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

Network Based – Reconnaissance

```
* Terminal
File Edit View Terminal Tabs Help
wolf@lB:~$ netstat -h
usage: netstat [-veenNcCF] [<Af>] -r          netstat {-V|--version|-h|--help}
       netstat [-vnNcaeol] [<Socket> ...]
       netstat { [-veenNac] -i | [-cnNe] -M | -s }

    -r, --route           display routing table
    -i, --interfaces      display interface table
    -g, --groups          display multicast group memberships
    -s, --statistics      display networking statistics (like SNMP)
    -M, --masquerade      display masqueraded connections

    -v, --verbose         be verbose
    -n, --numeric         don't resolve names
    --numeric-hosts       don't resolve host names
    --numeric-ports       don't resolve port names
    --numeric-users       don't resolve user names
    -N, --symbolic        resolve hardware names
    -e, --extend          display other/more information
    -p, --programs        display PID/Program name for sockets
    -c, --continuous      continuous listing

    -l, --listening       display listening server sockets
    -a, --all, --listening display all sockets (default: connected)
    -o, --timers           display timers
    -F, --fib             display Forwarding Information Base (default)
    -C, --cache           display routing cache instead of FIB

<Socket>={-t|--tcp} {-u|--udp} {-w|--raw} {-x|--unix} --ax25 --ipx --netrom
<AF>=Use '-6|-4' or '-A <af>' or '--<af>'; default: inet
List of possible address families (which support routing):
    inet (DARPA Internet) inet6 (IPv6) ax25 (AMPR AX.25)
    netrom (AMPR NET/ROM) ipx (Novell IPX) ddp (Appletalk DDP)
    x25 (CCITT X.25)
wolf@lB:~$ netstat --help
```

Our Official Website

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



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



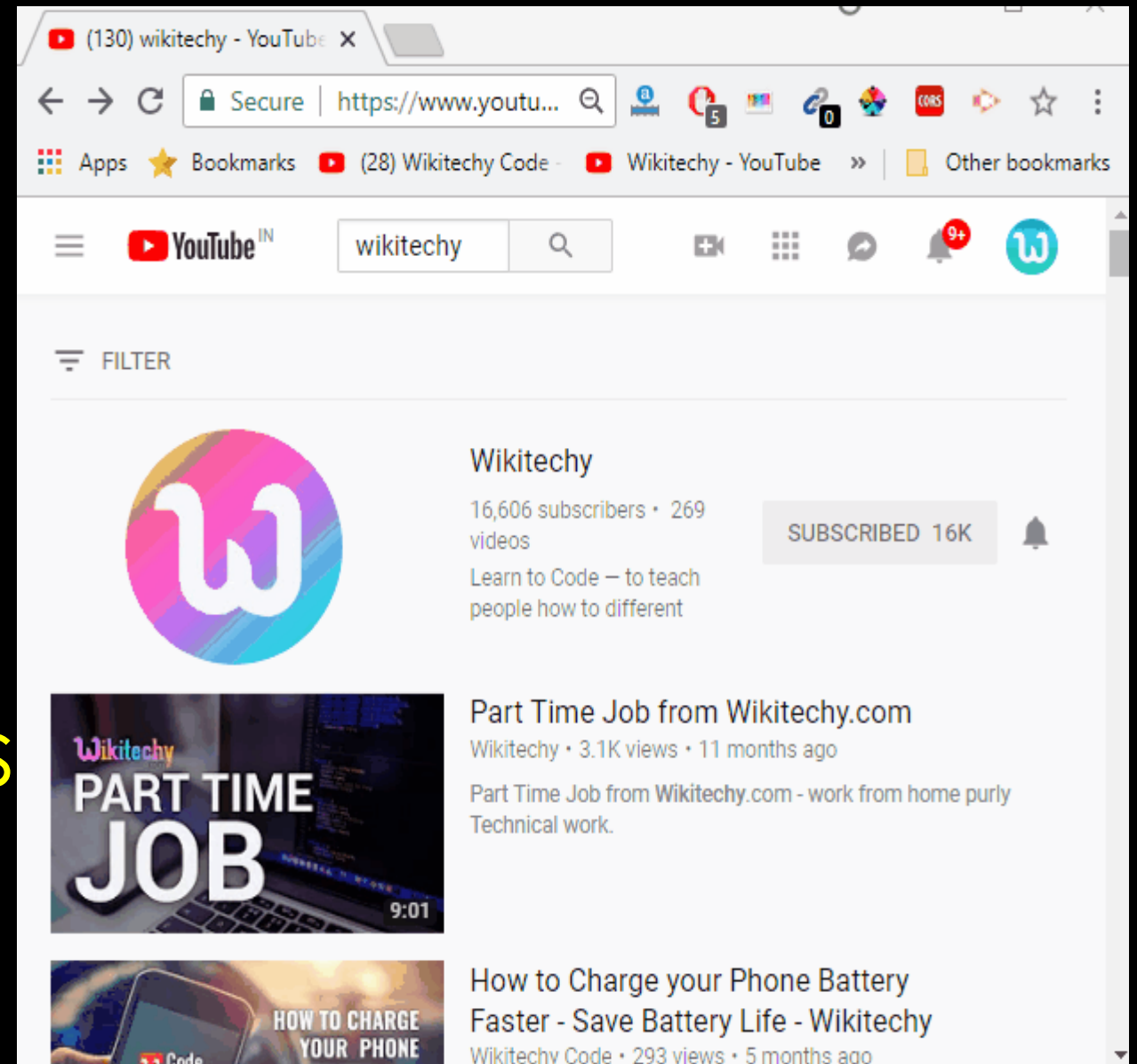
Our Youtube Channel

Wikitechy

Wikitechy code

Wikitechy Interview Tips

Wikitechy School



The screenshot shows the Wikitechy YouTube channel page. The browser address bar displays "https://www.youtu...". The YouTube header includes the search bar with "wikitechy" entered, and navigation icons for home, library, and notifications. The channel banner features the Wikitechy logo, a stylized 'w' in a colorful circle. To the right of the logo, the channel name "Wikitechy" is displayed, along with "16,606 subscribers • 269 videos". A "SUBSCRIBED 16K" button and a notification bell icon are also visible. Below the channel information, two video thumbnails are shown. The first video is titled "Part Time Job from Wikitechy.com" and has "3.1K views • 11 months ago". The second video is titled "How to Charge your Phone Battery Faster - Save Battery Life - Wikitechy" and has "293 views • 5 months ago".

(130) wikitechy - YouTube X

Secure | https://www.youtu...

Apps Bookmarks (28) Wikitechy Code - Wikitechy - YouTube Other bookmarks

YouTube IN wikitechy

FILTER

Wikitechy

16,606 subscribers • 269 videos

Learn to Code — to teach people how to different

SUBSCRIBED 16K

Part Time Job from Wikitechy.com

Wikitechy • 3.1K views • 11 months ago

Part Time Job from Wikitechy.com - work from home purly Technical work.

How to Charge your Phone Battery Faster - Save Battery Life - Wikitechy

Wikitechy Code • 293 views • 5 months ago

THANK YOU

Pls Share to UR Friends