

TC 1.0

Terminal Commands module 1: Terminal commands and the internet

(commands are usually in **bold**)

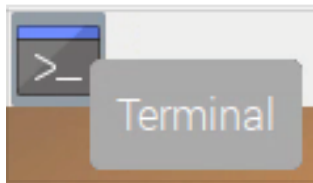
First notes:

Why do we mess with terminal?

1. it is seen everywhere
2. it can be done remotely
3. it give you god-like powers
4. it looks cool

Ok, where do we find it?

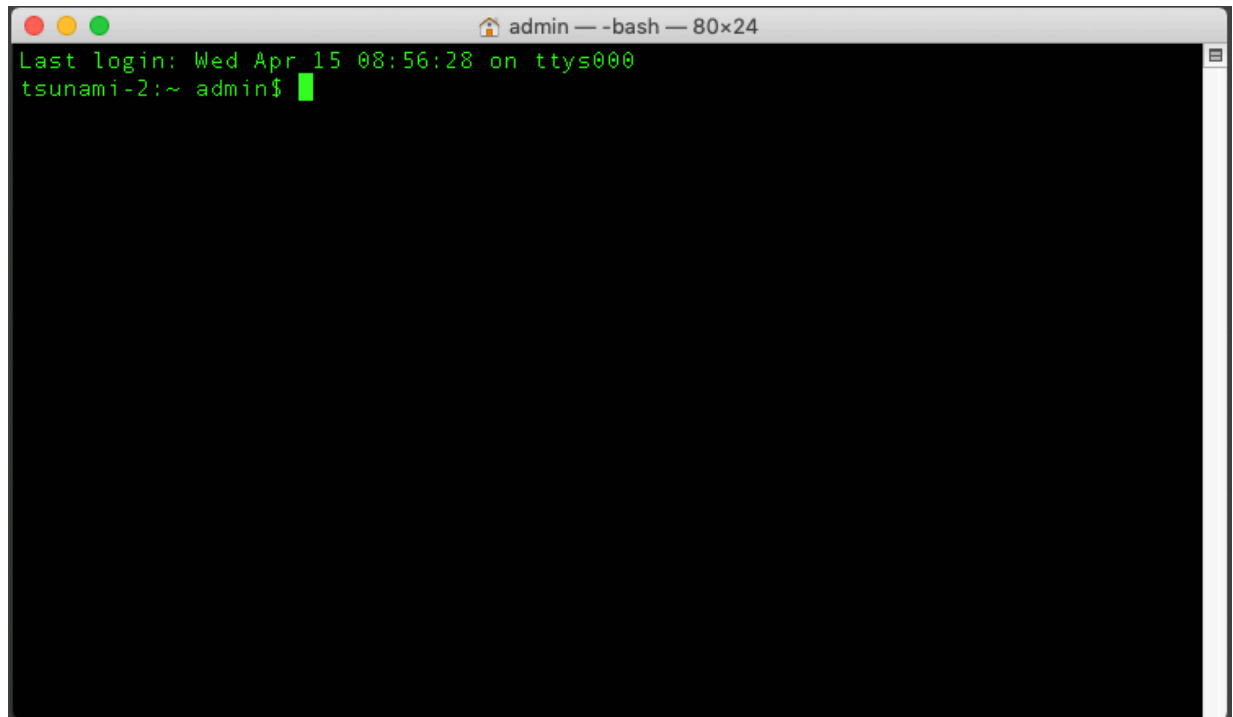
On the raspberry Pi, it is on the top menu bar, looking like a black square:



On the mac, look under Applications/Utilities, or search using the little search thingy.

You can also hold command-space and type terminal

It should show up like this:

A terminal window with a title bar that reads "admin — -bash — 80x24". The window contains the following text in green: "Last login: Wed Apr 15 08:56:28 on ttys000" followed by "tsunami-2:~ admin\$" with a green cursor. The rest of the terminal area is black.

```
admin — -bash — 80x24
Last login: Wed Apr 15 08:56:28 on ttys000
tsunami-2:~ admin$
```

Mine is of course cooler, because I have gone into preferences and changed a few things. Knock yourself out.

What does this first window tell us?

Last login: date, time and place, in this case ttys000 means my keyboard.

The word tty comes from teletype, one of these things:



Believe it or not, when I was in high school, this was what a computer looked like.

The rest of the computer was a huge mainframe the size of a room many miles away.

Another fun fact: see that green tape? That was what we wrote our programs on. Each dot on the tape is a bit. 8 bits makes a byte. The little bits of paper that fall into the trashcan below make that a "bit-bucket".

Your internet speed is measured in mb/s or megabits per second: a million of those little dots per second.

Cool.

Let's start with something fun:

Open terminal

type **ping** www.apple.com

Look at what you get:

```
Last login: Wed Apr 15 08:56:28 on ttys000
[tsunami-2:~ admin$ ping www.apple.com
PING e6858.dsce9.akamaiedge.net (23.3.84.254): 56 data bytes
64 bytes from 23.3.84.254: icmp_seq=0 ttl=56 time=68.530 ms
64 bytes from 23.3.84.254: icmp_seq=1 ttl=56 time=71.296 ms
64 bytes from 23.3.84.254: icmp_seq=2 ttl=56 time=71.870 ms
64 bytes from 23.3.84.254: icmp_seq=3 ttl=56 time=63.815 ms
64 bytes from 23.3.84.254: icmp_seq=4 ttl=56 time=84.886 ms
64 bytes from 23.3.84.254: icmp_seq=5 ttl=56 time=233.551 ms
64 bytes from 23.3.84.254: icmp_seq=6 ttl=56 time=68.957 ms
64 bytes from 23.3.84.254: icmp_seq=7 ttl=56 time=62.855 ms
64 bytes from 23.3.84.254: icmp_seq=8 ttl=56 time=72.409 ms
64 bytes from 23.3.84.254: icmp_seq=9 ttl=56 time=112.328 ms
^Z
[1]+  Stopped                  ping www.apple.com
tsunami-2:~ admin$
```

you can hit **control-x** or **control-z** to stop this fun.

What does this tell us?

1. our computer can decode www.apple.com into a number on the internet
2. the apple computer is at 23.3.84.254, which may be secret
3. my computer sent out packets of 64 bytes each to www.apple.com and these packets came back in around 68-233 ms, where ms means a millisecond. 1000 ms is one second.
4. if you are a gamer, this is useful so you do not get killed all the time in CSGO.

(arin.net is another tool)

Ok now try this:

nslookup

this means "name service lookup"

You should be looking at a funny arrow thingy called a carat:

```
[tsunami-2:~ admin$ nslookup
> █
```

Now type www.apple.com

You get all of these fun facts:

```
[tsunami-2:~ admin$ nslookup
[> www.apple.com
Server:          192.168.3.1
Address:         192.168.3.1#53

Non-authoritative answer:
www.apple.com    canonical name = www.apple.com.edgekey.net.
www.apple.com.edgekey.net    canonical name = www.apple.com.edgekey.net.globa
lredirect.akadns.net.
www.apple.com.edgekey.net.globalredirect.akadns.net    canonical name = e6858.d
sce9.akamaiedge.net.
Name:   e6858.dsce9.akamaiedge.net
Address: 23.3.84.254
>
```

What does this mean?

1. your computer went to the domain name server (DNS) that decodes names (www.apple.com) into numbers (23.3.84.254)
2. in this case, my domain server was my router at 192.168.3.1, which probably looked up this answer from someone else (likely 8.8.8.8 the google DNS server) then stored or "cached" this info so I could browse faster. You also have a cache in your computer that does a similar thing.

typing "**exit**" or **control-x** or **control-z** will get you out of **nslookup**.

Now try this:

ping 23.3.84.254

```
[tsunami-2:~ admin$ ping 23.3.84.254
PING 23.3.84.254 (23.3.84.254): 56 data bytes
64 bytes from 23.3.84.254: icmp_seq=0 ttl=56 time=109.848 ms
Request timeout for icmp_seq 1
64 bytes from 23.3.84.254: icmp_seq=2 ttl=56 time=61.785 ms
64 bytes from 23.3.84.254: icmp_seq=3 ttl=56 time=60.348 ms
64 bytes from 23.3.84.254: icmp_seq=4 ttl=56 time=69.396 ms
64 bytes from 23.3.84.254: icmp_seq=5 ttl=56 time=63.788 ms
64 bytes from 23.3.84.254: icmp_seq=6 ttl=56 time=60.614 ms
64 bytes from 23.3.84.254: icmp_seq=7 ttl=56 time=64.152 ms
^Z
```

A few things show up here:

1. those numbers are the same as the name "www.apple.com"
2. the first ping was successful, the second was lost: Request timeout for icmp_seq 1
3. I used **control-z** to stop the ping: ^Z

Some versions of security simply block you from translating bad stuff (www.playboy.com) into numbers, so your computer just sits there going nowhere.

You can get around this by using **nslookup**, and instead of just typing the name, you can do this:

nslookup

```
[tsunami-2:~ admin$ nslookup  
> server 8.8.8.8]
```

Now enter what you want to lookup

www.apple.com

Name: e6858.dsce9.akamaiedge.net

Address: 23.47.151.53

>

same smell.

Another thing: the dark web (a truly scary, nasty place) does not use DNS, instead they use the numbers, so you don't go to "kidnappers.com" you go to some set of numbers, always in groups of 4, and never greater than 254. More on this soon.

Now another example of internet fun:

traceroute

try traceroute www.apple.com

tracert on the pc

```

tsunami-2:~ admin$ traceroute www.apple.com
[traceroute to e6858.dsce9.akamaiedge.net (23.47.151.53), 64 hops max, 52 byte packets]
 1 192.168.3.1 (192.168.3.1) 0.900 ms 0.564 ms 0.455 ms
 2 142.254.191.21 (142.254.191.21) 79.337 ms 15.483 ms 22.353 ms
 3 agg62.klaohias02h.hawaii.rr.com (24.25.232.73) 35.338 ms 20.730 ms 35.331 ms
 4 agg42.kmlahi0701r.hawaii.rr.com (72.129.47.164) 33.550 ms 20.584 ms 14.966 ms
 5 agg31.tustcaft01r.socal.rr.com (72.129.45.2) 68.749 ms 67.104 ms 72.788 ms
 6 bu-ether26.tustca4200w-bcr00.tbone.rr.com (66.109.3.232) 72.875 ms 66.918 ms 65.172 ms
 7 66.109.5.241 (66.109.5.241) 74.756 ms 86.571 ms 69.137 ms
 8 24.30.200.51 (24.30.200.51) 72.732 ms
 9 * * ae1.ctl-lax2.netarch.akamai.com (23.203.155.158) 75.832 ms
10 * * *

```

Wow, this has much more info:

1. it shows that I started a ping of a certain type (called an ICMP ping) from my router address at 192.168.3.1
2. it shows each stop along the way
3. it shows that my ping first did some stuff here on Hawaii island, then Oahu, then CA (tustca or Tustin, CA)
4. it then hit what is called the tbone, a huge fiber connection up and down the coast of CA
5. finally to LA, where there is an akamai server

what is an akamai server?

good question.

Akamai means "smart" in Hawaiian. Cool.

A few guys about 20 years ago realized that sending the same photos, videos or other huge stuff all around the planet was a waste of bandwidth (the size of the "pipes" that carry internet data).

They thought it would be smart or "akamai" to put servers that would cache (recall that word?) big stuff in servers around the planet.

These are called "akamaized servers".

We have several in Hawaii, and loads on the mainland.

I suppose you could look them up if you were interested...

traceroute is really useful if you are gaming (who isn't?) since it tells you where the slow link is in your chain. You may have to lookup the IP address of the server you are joining and do a traceroute to there.

Another thing: don't for a second imagine that apple.com, the huge and mighty, powerful apple has only one server.

It has thousands of these, in a network called "round robin" or RAIS (redundant array of independent servers).

When you get comfortable throwing these words around, folks will think you have god-like powers over computers, and likely ask you to fix theirs.

——end of module 1: terminal commands and the internet——