

Hello everyone, my name is Amy Holem, Head of Pacts International Tech Department. I have some announcements before I get to this week newsletter topic. First, I finally have my website up and running so check it out. <https://www.aimeesaudios.com/>. Second become a subscriber for only \$15.00 dollars a YEAR. This will grant access to all the information that you are looking for. It will also help my patent-Live stream Criminals-hackers-stalkers. <https://www.gofundme.com/f/patent-live-stream-criminals-hackers-stalkers>. Faster we get this done, the faster everyone can **LIVE STREAM** their targeting.

There have been some interesting videos coming through about ASN numbers. I want to shed some light on what an ASN number actually is, and how it can help you in your situation. I also want to simplify everything for you and give the proper step by step procedures so you can achieve this yourself.

The person Sh P doing the You tube videos on ASN numbers is Bibi Pietsch from Canada. <https://www.youtube.com/channel/UC9UPXcV6Ziax3rXgkAuRtsw>. Her research is correct but there are some simple mistakes, on mapping the networking system and the connections that everyone needs to understand. The technique she is using is a hacking method with hacking devices. This is all legal to use, in order to stop these criminals from using this technology we need to learn the same techniques and procedures.

For Instance downloading an app **Wi-Fi Tracker** turn on all functions: https://play.google.com/store/apps/details?id=org.prowl.wifiscanner&hl=en_CA. Do NOT PUT YOUR PHONE IN AIRPLANE MODE. This is an app to detect open wi-fi access points known as Wardriving. This will show where the phone connects to receive signal or wi-fi access also known as an Access Point (AP). Access Points allow you to connect and gain access with the cellular device which always connects to an LAN network, through RF signals, cell tower and radio tower communications. War driving is mapping out all open AP (Access Point) and hotspots while driving a vehicle <https://www.techopedia.com/definition/4162/wardriving>.

Which comes to the other net mapping systems of the war driving,

Download and Install **NetMonitor**: Close it but do NOT PUT YOUR PHONE IN AIRPLANE MODE. Monitor CDMA / GSM / WCDMA / LTE / TD-SCDMA / 5G NR networks: current and neighboring cell info's, signal strength. Multi SIM support (when possible). Use GPS/geolocation. Generate database with custom info on cells. Export log to file CLF/KML. Map shows cell location. List Wi-Fi access points. https://play.google.com/store/apps/details?id=com.parizene.netmonitor&hl=en_CA.

Download and install **Netmonster**: https://play.google.com/store/apps/details?id=cz.mroczis.netmonster&hl=en_CA. Close it but do NOT PUT YOUR PHONE IN AIRPLANE MODE.

Most of the above sites are connecting to cellular, or radio towers. To connect, get internet and signal to your phone or computing device, you need to connect to the towers to gain that connection. These connections are not necessarily to a person or criminals home, but the location of the tower it is connecting too. If you look outside your residence you can see telephone towers, radio towers, and cabling throughout the neighborhood. Some of these towers are in front of their homes which gives them that address. This does not necessarily mean you are connecting directly to the residence but connecting to the tower. You as a victim would need to drive around to the different locations and check to see if a tower, is there at that location. Knowing where you are connecting and for what reason is where you personally have to investigate. Some of those connections are for example, google, play store, websites, are connections that travel through packets to arrive to their

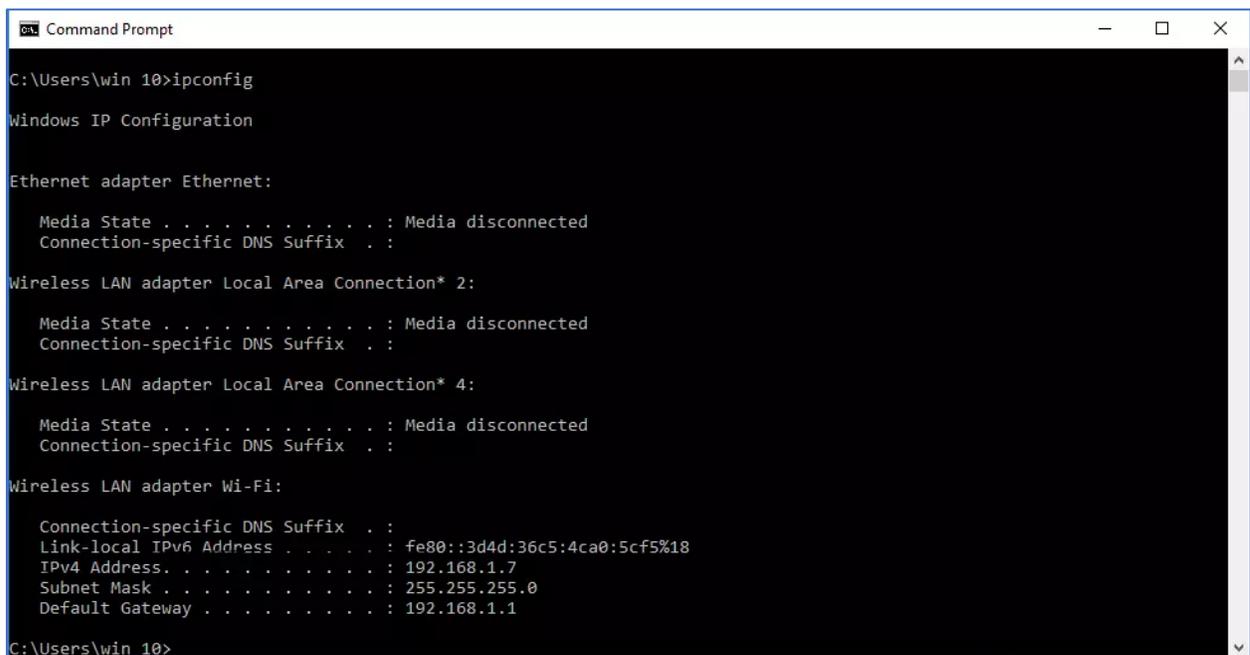
destination. By simply connecting to a link you are transferred from location through the open AP (Access Points) to enter the persons domain, or website. Do your research on each of these and see your latest connection.

ASN is an **Autonomous system number**. This is a number that is assigned by the **IANA (Internet Assigned Numbers Authority)**. A little about IP addresses that they are all assigned because computers work on binary coding. IPv4 and IPv6 are IP addresses that are assigned. All government agencies must have an IPv6 because of the security, and IPv4 numbers are running out because of the mass amount of people around the world. We can discuss the difference of IPv4 and Ipv6 at a different time or go to this link and discover it for yourself. <http://www.iana.org/>.

1) To determine what your IP address is

A) <https://whatismyipaddress.com/>. Run **My IP** and that will give you your Ip address. If you go to the **IP LOOKUP** tab, this will give you your ASN number as well, and give you all the proper information on your system.

B) **Use your command Prompt**. Type in your windows search bar **cmd** or **command prompt**.
Type in: **ipconfig**



```
Command Prompt
C:\Users\win 10>ipconfig

Windows IP Configuration

Ethernet adapter Ethernet:

    Media State . . . . . : Media disconnected
    Connection-specific DNS Suffix  . :

Wireless LAN adapter Local Area Connection* 2:

    Media State . . . . . : Media disconnected
    Connection-specific DNS Suffix  . :

Wireless LAN adapter Local Area Connection* 4:

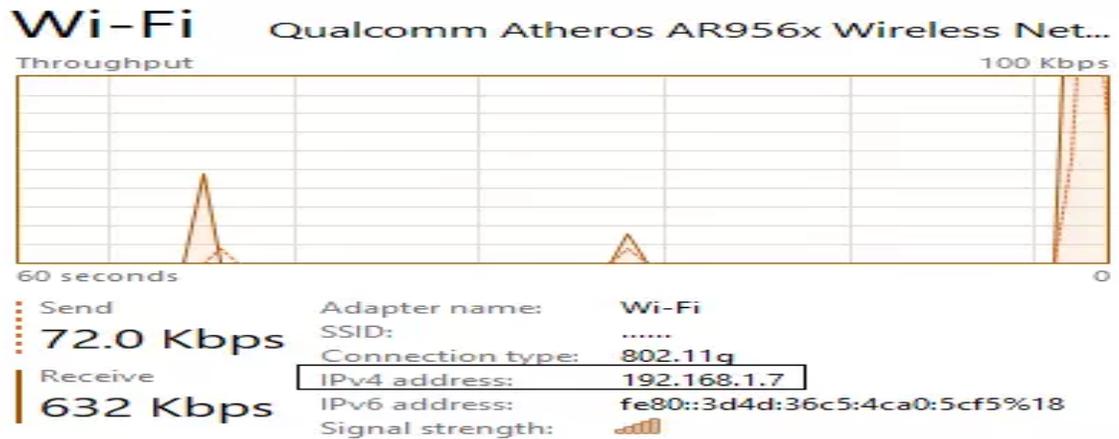
    Media State . . . . . : Media disconnected
    Connection-specific DNS Suffix  . :

Wireless LAN adapter Wi-Fi:

    Connection-specific DNS Suffix  . :
    Link-local IPv6 Address . . . . . : fe80::3d4d:36c5:4ca0:5cf5%18
    IPv4 Address. . . . . : 192.168.1.7
    Subnet Mask . . . . . : 255.255.255.0
    Default Gateway . . . . . : 192.168.1.1

C:\Users\win 10>
```

c) **Use the Task Manager**: From that menu, select task manager. select Performance tab, click on **Wi-Fi**. The window corresponding to Wi-Fi will display the IP address of your device against the title of **IPv4 address**.



d) **USE Settings > Network Properties.** search section of your taskbar, type *Settings* and click on it. The following Settings screen will be displayed: Click on *Network & Internet*, Select the *Wi-Fi tab*. From the window, click on the wireless network to which you are connected. In the given scenario, the name of wireless network is

A new window will pop up. Just scroll down to see its properties. Under the properties section, you will find IPv4 address, which will in fact, be the IP address of your device.

Properties

SSID:
Protocol:	802.11g
Security type:	WPA-Personal
Network band:	2.4 GHz
Network channel:	6
IPv4 address:	192.168.1.7
IPv4 DNS servers:	192.168.1.1
Manufacturer:	Qualcomm Atheros Communications Inc.
Description:	Qualcomm Atheros AR956x Wireless Network Adapter
Driver version:	10.0.0.341
Physical address (MAC):	5C-93-A2-B5-C9-83

Copy

There are other ways to get to an IP address click this link to find out.

<https://www.faqforge.com/windows/windows-10/5-ways-to-find-your-current-ip-address-in-windows-10/>.

2) Go to <https://bgp.he.net/>. Type in your ASN number. <https://whatismyipaddress.com/>.

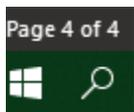
A little bit about ASN numbers for your knowledge. There are a couple of complaints out there that there are people with the same ASN number that has been assigned to them. That is because the ASN number is not assigned to you but the internet provider you are purchasing the internet from. The provider is assigned the ASN number and allotted to you. With the assignment of ASN numbers and IP addresses they are running out, so the companies or provider sublet and combines the numbers to save room and space.

Another aspect that you are not aware of is the data mining aspect that carries with you throughout your life. If you subscribed to different companies, through different newsletters, magazines, or event sports results, that information will show up on the ASN number in order to connect to you so you can get your emails. Companies like AAA, or ARP, or the VA, those sites will show up as well. That does not mean they are involved with your targeting that means once in your life you have allowed or granted them permission to send you information. With hotels, if you traveled a lot and spent time in hotels you will have that information because they used that credit card information and granted access to allow them that information. Knowing this that whole list does not mean they are directly targeting you.

The only way to prove that the people are behind your targeting is to use a ping or tracert on the IP address that is associated with the list. Most the time the tracert will be better because it shows the IP address connecting to an outside source directly to your computer using a ping afterwards. The bad thing is that these companies have deniable plausibility. This means that they rent the iCloud or software out and are unaware of the renter's or user's attention and how they are using the system or software.

When pinging you cannot use a subnet on the ping some of the IP addresses on the website of hurricane electric have a subnet. Let me explain an IP address has digits such as **192.168.1.1** a subnet is the number after the IP address **192.168.1.1/24**. When a server has multiple ports connected, they use subnets to be assigned to that IP address. One person can have multiple subnets attached to the IP address. **192.168.1.1/23, 192.168.1.1/20, 192.168.1.1/8** and so forth.

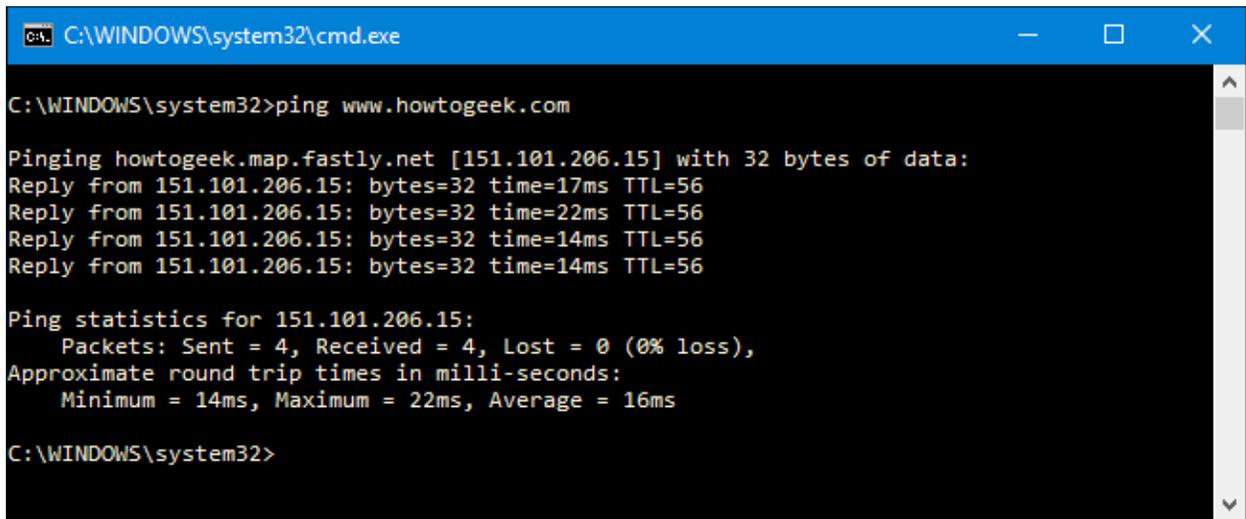
1) When **pinging** or using a **trace route** go back to your **command prompt**.



Go to the bottom left side of your computer click on the magnifying glass or search bar.

2) Type in **CMD** and click on the **Command Prompt**.

3) You can ping different ways, this shows the ping using a website address.



```
C:\WINDOWS\system32\cmd.exe
C:\WINDOWS\system32>ping www.howtogeek.com

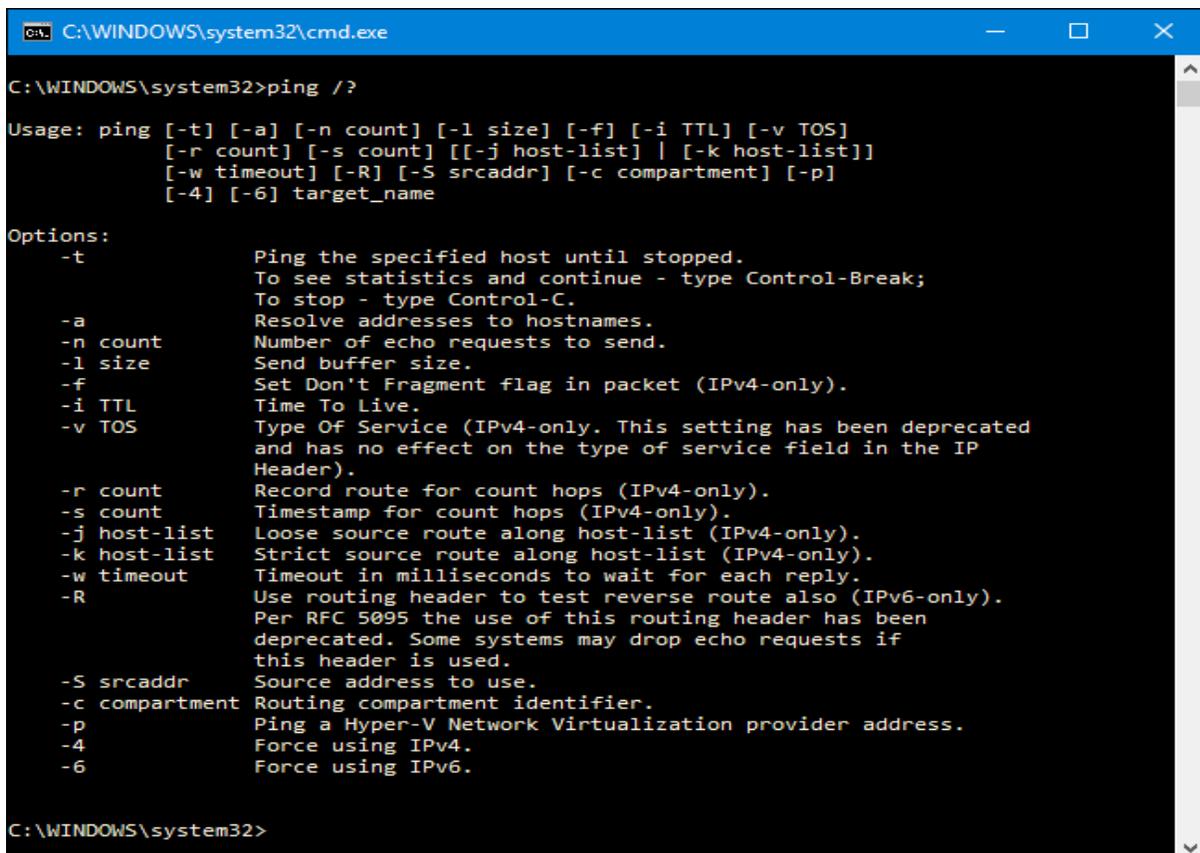
Pinging howtogeek.map.fastly.net [151.101.206.15] with 32 bytes of data:
Reply from 151.101.206.15: bytes=32 time=17ms TTL=56
Reply from 151.101.206.15: bytes=32 time=22ms TTL=56
Reply from 151.101.206.15: bytes=32 time=14ms TTL=56
Reply from 151.101.206.15: bytes=32 time=14ms TTL=56

Ping statistics for 151.101.206.15:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
    Approximate round trip times in milli-seconds:
        Minimum = 14ms, Maximum = 22ms, Average = 16ms

C:\WINDOWS\system32>
```

You can see the IP address was given from the website, the packets that were sent, received, and lost. You can also see how long the trip took to connect to the website. **This is a list that can help you with the ping**

Another thing you can ping is the IP Address. `C:\WINDOWS\system32>ping (space) 192.168.1.1`



```
C:\WINDOWS\system32\cmd.exe
C:\WINDOWS\system32>ping /?

Usage: ping [-t] [-a] [-n count] [-l size] [-f] [-i TTL] [-v TOS]
          [-r count] [-s count] [[-j host-list] | [-k host-list]]
          [-w timeout] [-R] [-S srcaddr] [-c compartment] [-p]
          [-4] [-6] target_name

Options:
  -t           Ping the specified host until stopped.
               To see statistics and continue - type Control-Break;
               To stop - type Control-C.
  -a           Resolve addresses to hostnames.
  -n count     Number of echo requests to send.
  -l size      Send buffer size.
  -f           Set Don't Fragment flag in packet (IPv4-only).
  -i TTL       Time To Live.
  -v TOS       Type Of Service (IPv4-only. This setting has been deprecated
               and has no effect on the type of service field in the IP
               Header).
  -r count     Record route for count hops (IPv4-only).
  -s count     Timestamp for count hops (IPv4-only).
  -j host-list Loose source route along host-list (IPv4-only).
  -k host-list Strict source route along host-list (IPv4-only).
  -w timeout   Timeout in milliseconds to wait for each reply.
  -R           Use routing header to test reverse route also (IPv6-only).
               Per RFC 5095 the use of this routing header has been
               deprecated. Some systems may drop echo requests if
               this header is used.
  -S srcaddr   Source address to use.
  -c compartment Routing compartment identifier.
  -p           Ping a Hyper-V Network Virtualization provider address.
  -4           Force using IPv4.
  -6           Force using IPv6.

C:\WINDOWS\system32>
```

- 4) Using a **trace route**: this has the same concept except it does 30 rounds of connections. It will provide additional IP addresses that are connected to the IP address, which could be connected to your IP address on your computing device.

C:\WINDOWS\system32>tracert (space) 192.168.1.1

Hopefully I helped you all understand ASN number a little bit more and how they work. If you have any questions feel free to contact me at AimeesAudios@protonmail.com Amy Holem Head of Pacts Tech Department.