Net Crafts

Student Name: Ng Teck Meng

Student Code: S11

Unit code: cfc190324

Trainer Name: Samson

[Introduction](#_yv6xozrzfgd6)

[Methodologies](#_yvf9v2khdwp0)

[Network Discovery and Mapping](#_b66rg9wguuwv)

[Command Prompt](#_udjwrl918mzt)

[Discussion](#_yhhu0j71sjy)

[Protocol Identification](#_mz53uhf7xqh)

# Introduction

With the rise of remote work, technologies of AI and the explosion of IoT devices, home network security is more crucial than ever. Unlike rigorously protected corporate networks, many home networks are still vulnerable due to consumer-grade equipment and lack of any technical expertise.

This report explores my home network, focusing on protocols, service identification and how data are transferred. It will cover some examples of protocols used, how to identify some traffic that our computer uses to access the Internet. The findings will outline a basic path to understand how transfer of data works

# Methodologies

I will detail methods used to analyze and explore how to obtain information, protocols used in my home network.

## Command Prompt

1. To run the command, open the **Command prompt** on Windows PC.

2. Type ipconfig and press **Enter**

### Commands

#### ipconfig

##### What is ipconfig

* This is the computer’s network address book. It’s an address book that lists all the ways that the computer connects to a network. It also stores unique addresses it uses for each connection

##### What does ipconfig show

* Network Connectors -- Wired/Wireless connection
* IP Address – The computer’s unique number on a specific network, in this case, my home network will be the specific network.
* Subnet Mask – This helps the computer know what other devices are within the same local network.
* Default Gateway – The address of the router
* DNS Server – Server that helps to translate website names into numbers, binary, that the computer understands.

#### ipconfig /all

##### What is the /all command

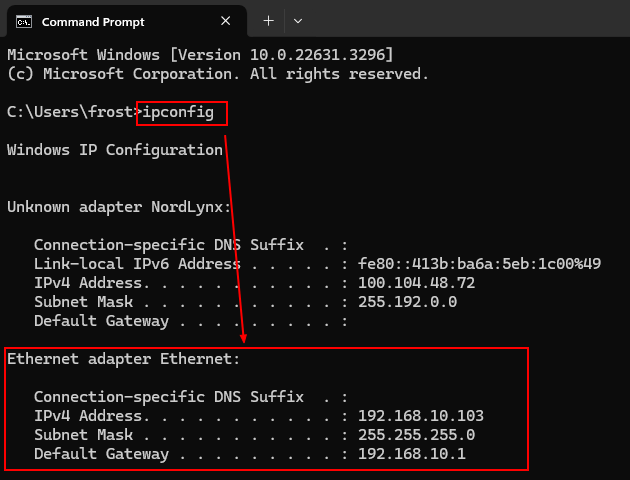
* /all is a flag or parameter that can display additional detailed information about all network connections and network adapters on the computer.

# Discussion

## ipconfig

ipconfig

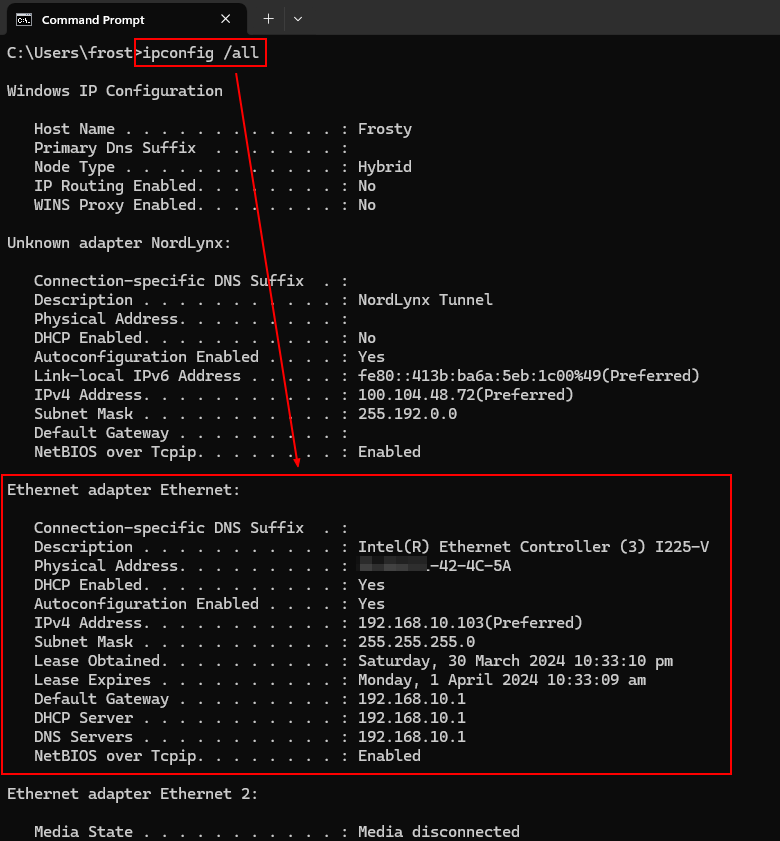
* This command is used to display information about the network configuration. By default, the ipconfig command displays your IP Address, Subnet Mask, and default gateway. However with extra parameters, we can get more information about the network configuration.



Flags/parameters that can be used

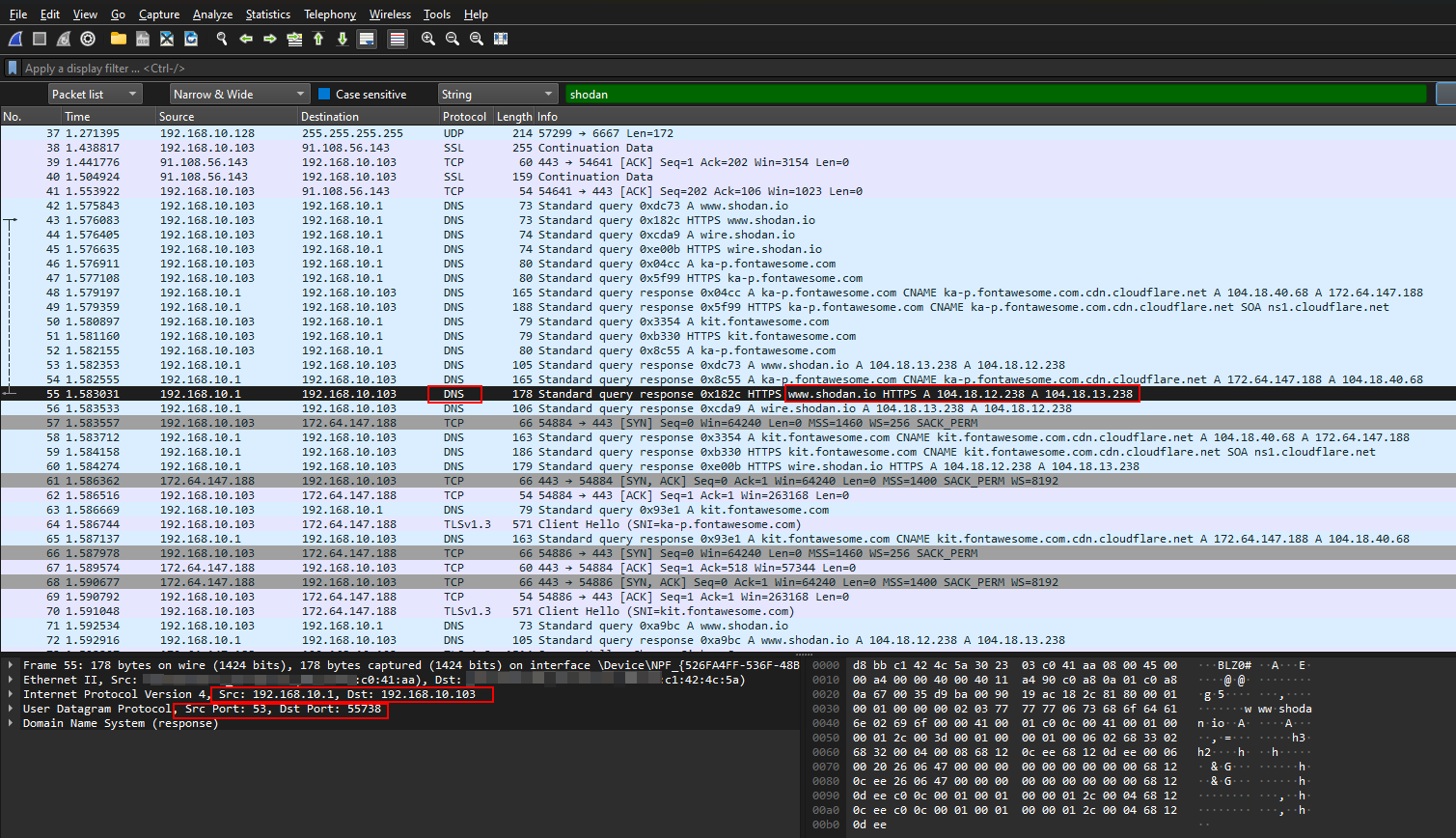
ipconfig /all

* With the additional flag /all, This will show all the information about the network adaptor (router)
  + Physical Address: This is the MAC address of the Network Adapter
  + DHCP: This indicates if the work connection is using DHCP or Static IP Address
  + IPv4 Address: This is the IPv4 address (xxx.xxx.xxx.xxx) of the computer
  + Default Gateway: The router to which the computer is connected to
  + DHCP Server: Router/Server that loans out IP Addresses with the local network
    - Lease information: This shows the time when the IP address lease happened as well as expiration of the lease IP address.
  + DNS Servers: Servers used to translate domain names to IP Addresses



## Protocol Identification

With wireshark, we can see how the communication works between my computer and the website that I want to visit.



For this example, I visited the website [shodan.io](http://shodan.io). We can see that my computer from source with IP address [192.168.10.1] sent a query to my router [192.168.10.103] for the address of [shodan.io](http://shodan.io).This will be done via the DNS Protocol. I’ll give a brief breakdown on how the process works

1. The DNS Protocol will translate the query into binary and sent it to the internet
2. Resource from the internet will response through DNS Protocol the IP Address of [shodan.io](http://shodan.io) [104.18.13.238]
3. When the response was received, it will translate the details of the IP address to a human-friendly readable format shodan.io within the web browser.

Here we can see on how the request was asked from my computer to my router and out to the Internet and vise versa

## Why Shodan search return no results when I lookup my public ip

Shodan searches typically return no results for home public IP addresses for several reasons. Primarily, Shodan focuses on devices directly connected to the internet with open ports. Home networks usually have router firewalls blocking incoming connections, and users rarely open ports for public access without a specific reason. This configuration effectively hides home networks from Shodan's scans

# Conclusion

## Why do we want to know what devices are connected within our home network

This helps us to better understand what devices are connected within our home local network. This also empowers us to identify devices that were within the network however that do not belong to us which could be a security threat.

By understanding what’s connected on our home network it provides control, enabling the proactive mitigation of security risk and informed troubleshooting.

As the network is within the home environment, it is often overlooked on security as it is deemed as safe normally by humans. However device identification on the home network will help highlight possible threats.

## Why we need to map out a network

Identifying all devices on a network helps in maintaining a catalog of device assets. This management habit is essential for tracking what is connected to a network. Without this, it is challenging to keep track between legitimate devices and potential intruder or compromised devices within a network.

As such sudden appearance of new devices, unusual network traffic patterns or unexpected updates prompts can indicate potential security breaches or intrusion.

Mapping out a network of devices will help in identifying devices clearly. This will allow for potential threat mitigation, and aid with investigations.

## Why do we need to identify all devices access on a network

This helps in identifying connected devices' access. With a clear mapping of device access, it will be clear to see what devices are connected and their role/access are within the network. This helps in a case where suddenly a device was bumped up in access level controls, as checking the affected device should not have this level of access, indicating a potential security threat.

# Recommendations

## What should I do if I see an unknown device within my network

As this might be a potential security breach, these are some approaches that you can consider.

1. Isolate and Contain
   1. Disconnect the device, this helps to limit its ability to communicate with the network and reduce risk of any spread of malware.
2. Investigate and Gather Information
   1. You can check on router logs to see when the device first connected to the network.
   2. Check on any unusual connection traffic with a network mapping tool (Wireshark)
3. Identify the device
   1. If possible to identify the device, rename it to match the function of the device. Instead of unknown device, name it to e.g – living room TV

# References

Sources used:

* <https://www.cloudflare.com/learning/ssl/what-is-https/>
* <https://www.cloudflare.com/learning/ssl/transport-layer-security-tls/>
* <https://support.intermedia.com/app/articles/detail/a_id/27175/~/how-do-i-use-ipconfig-in-the-command-prompt-or-terminal%3F>
* <https://www.shodan.io/dashboard>
* <https://help.shodan.io/the-basics/what-is-shodan>
* [whois.domaintools.com/](http://whois.domaintools.com/)
* <http://example.com>
* <https://www.techtarget.com/searchnetworking/definition/TCP>