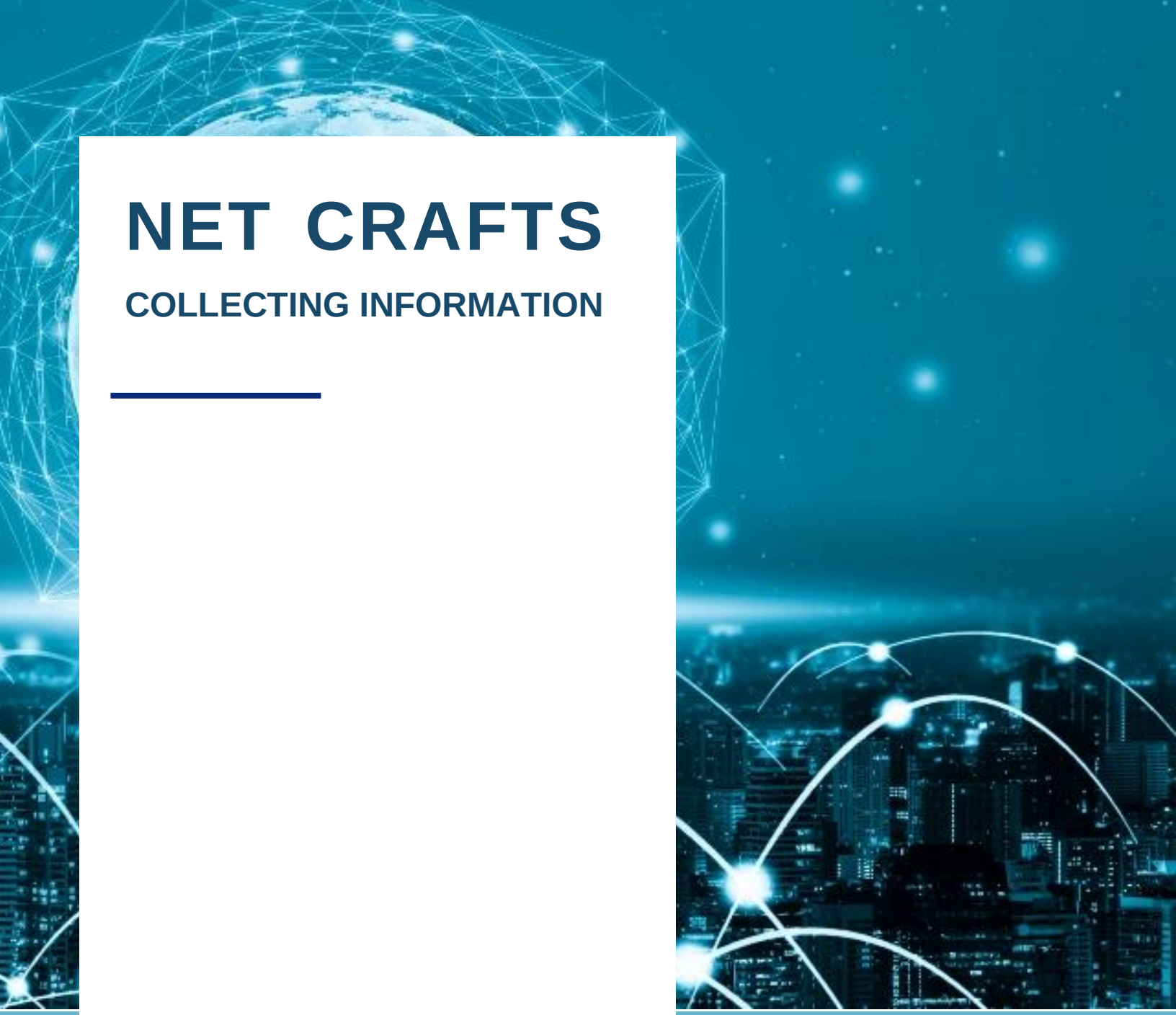


# NET CRAFTS

## COLLECTING INFORMATION

**Author: Yvette K**

# CONTENTS

# Introduction

The purpose of this report is to inspect the importance of a network map that shows all the devices in a home network and all the information these devices contain, investigate our public IP addresses and study protocols.

These are basic information that cybersecurity practitioners need to be familiar with and their importance in maintaining a safe cyber space will be studied.

# Methodologies

Firstly, the Internet Service Provider's website was visited to view the router configuration page.

https://whatismyipaddress.com/ was visited to find out what the external IP address was. Wireshark was then turned on to capture traffic.

The device's external IP address was searched on https://www.shodan.io/ and https://www.whois.com/.

Lastly, the capture on Wireshark was studied to identify three different protocols and examine what interactions took place.

# Discussion

Firstly, all the devices on the targeted network were mapped out by visiting its ISP's website to view the router configuration page and inspect the devices connected to the router.

The external IP address was obtained on https://whatismyipaddress.com/.

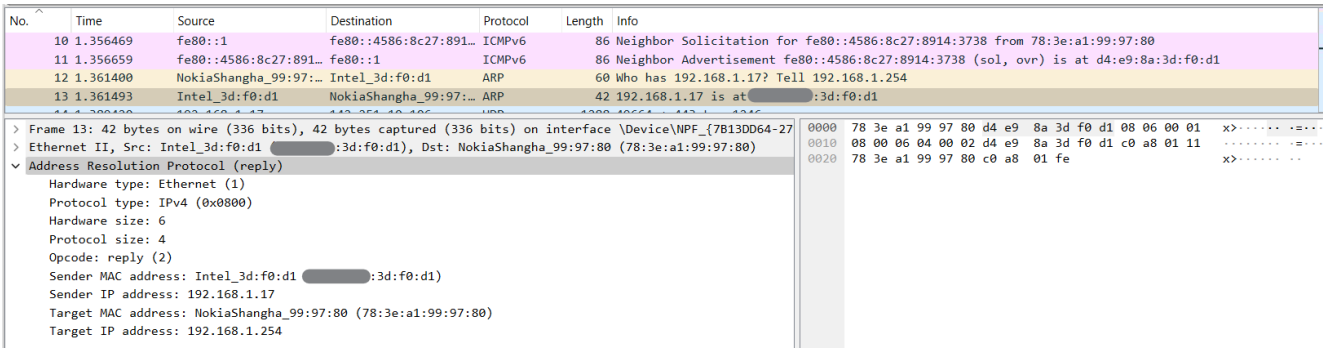
Wireshark was turned on to capture traffic while the external IP address was searched on https://www.shodan.io/, which is a search engine that allows users search for various types of servers connected to the internet, and received no results.

The external IP address was next searched on https://www.whois.com/, a widely used Internet record listing that identifies who owns a domain and how to get in contact with them, and found it registered to SingNet, along with some of their details, including address, email, phone and fax numbers.

Lastly, the capture on Wireshark was studied to identify three different protocols and examine what interactions took place.

## ARP (Address Resolution Protocol)

The first protocol studied was ARP, which is responsible for finding the hardware (MAC) address of a host from a known IP address. It is one of the most important protocols of the Data Link (2) layer in the OSI model.

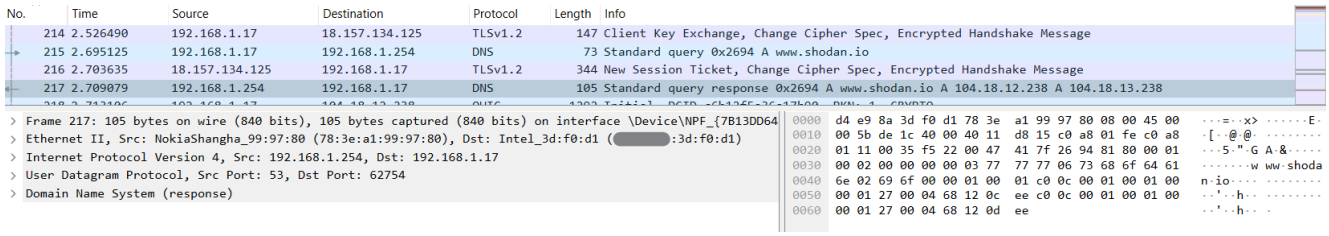



In the Wireshark capture above, we can see this exchange of information.
Unlike TCP or UDP, ARP does not use port numbers. Instead, ARP packets are identified by the EtherType value 0x0806 in Ethernet frames.

ARP is vulnerable to attacks such as ARP spoofing, where an attacker sends falsified ARP messages to associate their MAC address with the IP address of another device, potentially intercepting or disrupting network traffic.

## DNS (Domain Name System)

DNS was the second protocol studied. It translates domain names to IP addresses, enabling web browsers to locate and interact with websites. It eliminates the need for humans to memorise numeric or alphanumeric IP addresses by converting a hostname, which is easier to remember, into a computer-friendly IP address.




It can be seen in the Wireshark capture above that www.shodan.io was translated to 104.18.12.238 and 104.18.13.238.

DNS's standard port number is 53. It operates primarily over UDP port 53 for standard queries and responses. For larger data transfers, such as zone transfers, DNS uses TCP port 53.

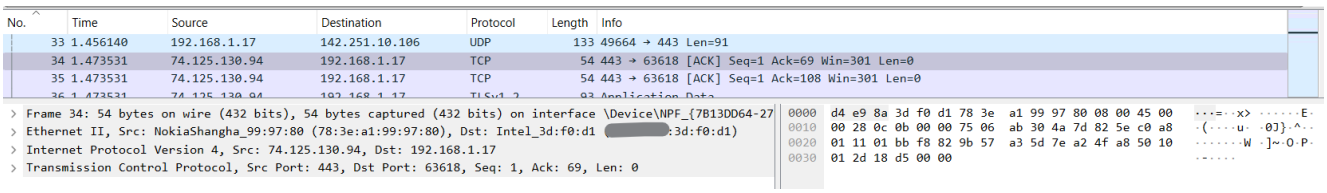
DNS can be targeted by attacks such as DNS spoofing or cache poisoning, where attackers manipulate DNS responses to redirect users to malicious sites.

## TCP (Transmission Control Protocol)

The third protocol, TCP, is a connection-oriented communication protocol at the Transport Layer (Layer 4) of the OSI model that allows computing devices and application to send data via a network and verify its delivery. The task of this protocol is to carry packets across the Internet and one of its most critical features is the assurance of successful delivery on messages and data across networks. Before any data can be sent, the client and server must establish a connection.

Since TCP is connection based, it creates and maintains a connection between the receiver and sender while the data is being passed between them, thereby significantly reducing the likelihood of data corruption or loss during transmission.

TCP uses a three-way handshake to establish connections and verify data transmission. While this makes TCP highly reliable, it also introduces additional overhead, consuming more bandwidth compared to simpler protocols like UDP.




In the Wireshark capture above, we can see the acknowledgement received (third step of the three-way handshake), which is not required in UDP. In contrast, UDP (User Datagram Protocol) is a connectionless protocol that sends data via a network without verifying its delivery, which makes it faster and more efficient. This speed and efficiency however come at a cost of less error-checking mechanism that at times results in lost packets.

TCP is used by many application protocols, each of which has its own standard port number (e.g., HTTP uses TCP port 80, HTTPS uses TCP port 443).

TCP is susceptible to attacks such as SYN flooding, where an attacker exploits the handshake process to overwhelm a server with connection requests, potentially causing denial of service.

# Conclusion

Through this mapping exercise, there is increased awareness of which devices are connected to our networks and users are better equipped to detect any unknown devices connected to their network. In the process of identifying each device, it was also discovered that Apple masks their MAC addresses to provide their users higher security to prevent device tracking and MAC address spoofing, enhancing user privacy on public and private networks.

From the search results of Shodan and whois, it can be seen that no personal information is available online on the external IP address. In the wrong hands, external IP addresses can be utilised to cause significant damage.

On the less damaging end of the spectrum, advertisers can embed trackers to record our IP address and send us targeted ads based on our browsing. Although targeted advertising may offer convenience, it raises significant privacy concerns.

The city indication from an IP address also means that with some sleuthing online, one may be able to find exact physical address of a target. While home invasions and thefts are rare in Singapore, it can happen. Stalkers can also use this information for nefarious intents.

On the darker end of the spectrum, skilled hackers can steal valuable information for identity thieves or impersonate targets online and frame targets for crimes such as buying and selling drugs or creating national security threats.

In an era of increasingly sophisticated cyber threats, the ability to visualise and understand one's network is not just beneficial—it is essential for robust cybersecurity. Through network mapping, we gain a comprehensive overview of all devices and connections within our home environment, enabling us to detect unauthorised access, identify vulnerabilities, and respond swiftly to potential incidents. This proactive approach is fundamental for both preventing breaches and optimising the performance and resilience of our networks.

Moreover, familiarity with protocols such as ARP, DNS, and TCP deepens our understanding of how information flows and where security controls must be applied. By regularly monitoring our public IP address and network activity, we can better protect our personal data from misuse by advertisers, stalkers, or cybercriminals.

Ultimately, as cybersecurity practitioners, maintaining up-to-date network maps and staying vigilant about network behaviours are foundational practices. These measures not only safeguard our digital assets but also empower us to adapt to evolving threats and ensure a safer cyberspace for all users.

# References


Andriekutė, Aurelija. “What is a MAC address and how can you hide it?” *NordVPN*, Jan 02, 2023, https://nordvpn.com/blog/mac-address/#:~:text=A%20hacker%20could%20use%20your,to%20the%20same%20Wi%2DFi

Vigderman, Aliza and Turner, Gabe. “What Can Someone Do With Your IP Address?” *Security.org*, 19 March 2024, https://www.security.org/vpn/what-can-someone-do-with-your-ip/#:~:text=If%20someone%20has%20your%20IP,is%20change%20your%20IP%20address

Danao, Monique. “What Can Someone Do With Your IP Address?” *Forbes Advisor*, 27 November 2023, https://www.forbes.com/advisor/business/what-can-someone-do-with-ip-address/#:~:text=An%20IP%20address%20is%20not,and%20launch%20cyberattacks%20or%20scams

“How Address Resolution Protocol (ARP) works?” *GeeksforGeeks*, 13 February 2024, https://www.geeksforgeeks.org/how-address-resolution-protocol-arp-works/

“What is DNS? | How DNS works” *Cloudflare*, https://www.cloudflare.com/learning/dns/what-is-dns/

BasuMallick, Chiradeep. “TCP vs. UDP: Understanding 10 Key Differences” *Spiceworks*, 18 April 2022, https://www.spiceworks.com/tech/networking/articles/tcp-vs-udp/#_001

“Network Mapping: A Vital Tool for Cybersecurity Professionals” *Blue Goat Cyber*, https://bluegoatcyber.com/blog/network-mapping-a-vital-tool-for-cybersecurity-professionals/

Ashtari, Hossein. “What Is Network Mapping? Definition, Process, Importance, and Best Practices for 2022” *Spiceworks*, 8 March 2022, https://www.spiceworks.com/tech/networking/articles/what-is-network-mapping/

“What is Network mapping?” *Reason Labs*, https://cyberpedia.reasonlabs.com/EN/network%20mapping.html

Pismisoglu, Sinan. “Network Topology and Mapping: Cornerstones of Data Security – Part 1” *Bradley*, 1 December 2023, https://www.bradley.com/insights/publications/2023/12/network-topology-and-mapping-cornerstones-of-data-security--part-1

*Perplexity*, https://www.perplexity.ai/