AN ICMP NETWORK PING ANALYSIS ON TRADINGVIEW.COM

BY

SOMKENE RICHARD

15th SEPTEMBER, 2024

EXECUTIVE SUMMARY

This analysis was carried out on 15/09/24 at exactly 8:57 pm WAT to examine the network connectivity between the system's network and tradingview.com (a financial trading terminal).

From the analysis, network performance and communication between my system and the domain address were well established as requests and replies were sent and received seamlessly without any interruption.

INTRODUCTION

ICMP being a protocol used to check and determine if data is getting to its destination at the right time without any hitch was used to track the network performance between my network and the network of the domain-tadingview.com. To spot any error(s) in communication and as well find a solution to the error(s).

The ping command was also deployed for the network connectivity performance

TOOLS

1. HP Laptop: as the source device
2. Ping: to test the availability of the network
3. Wireshark: to analyse the data packets produced during the network communication and connectivity
4. Virustotal and Whoer.net: to analyse the IP address of the domain
4. Pen and paper: for writing and taking notes of details

METHODOLOGY

First, after connecting my laptop to my mobile device's network, I launched the Wireshark software and selected my "WiFi". After selecting it, the software started a default packet tracking of my system network activities

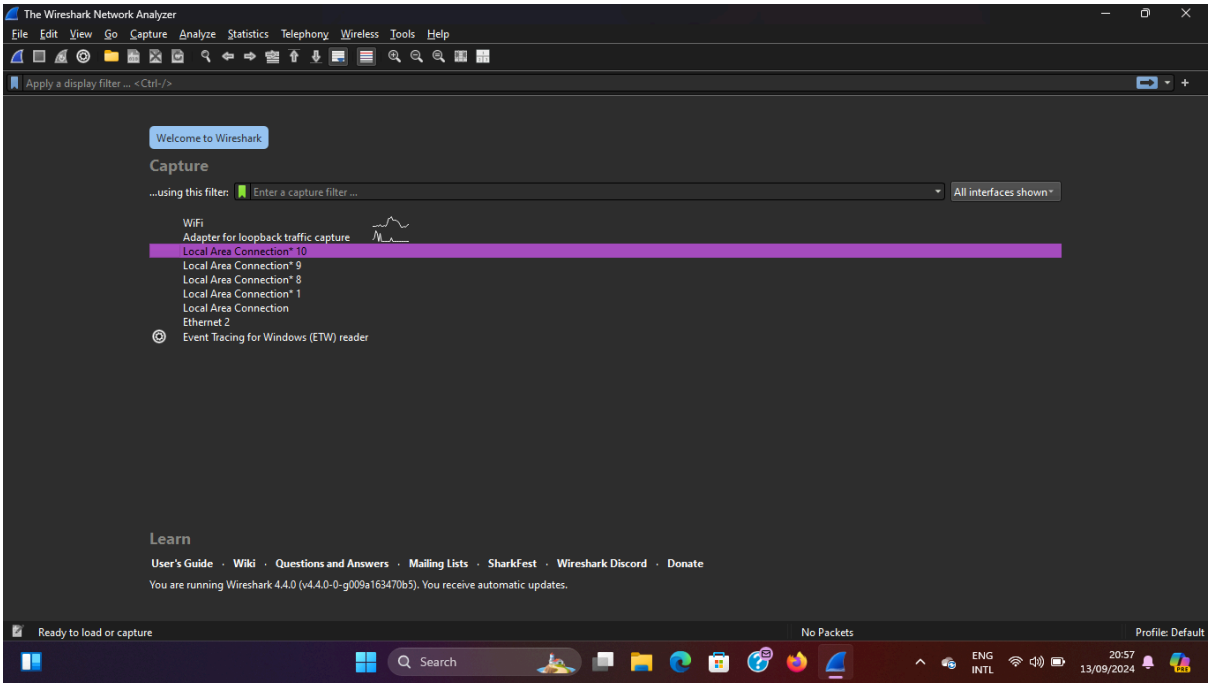

Fig 1: selection of WiFi connection

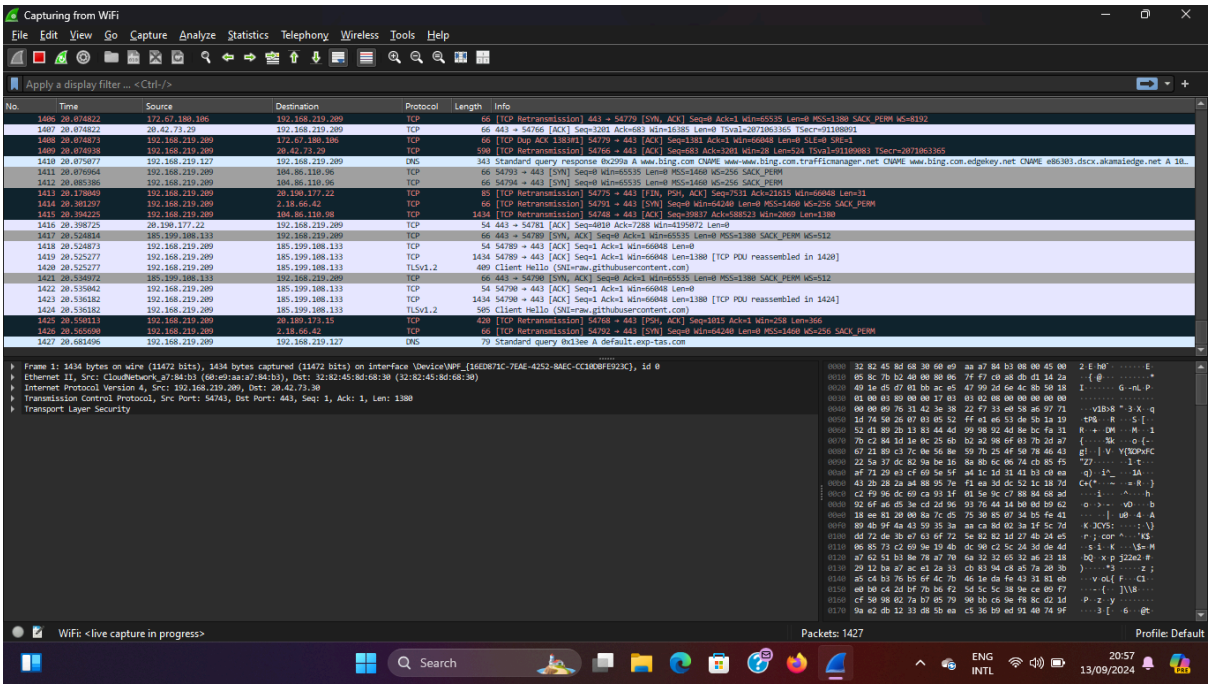

Fig1.1: Wireshark running default network capture

Step 2: I filtered for ICMP and then launched the Windows command line interface to proceed with the ping

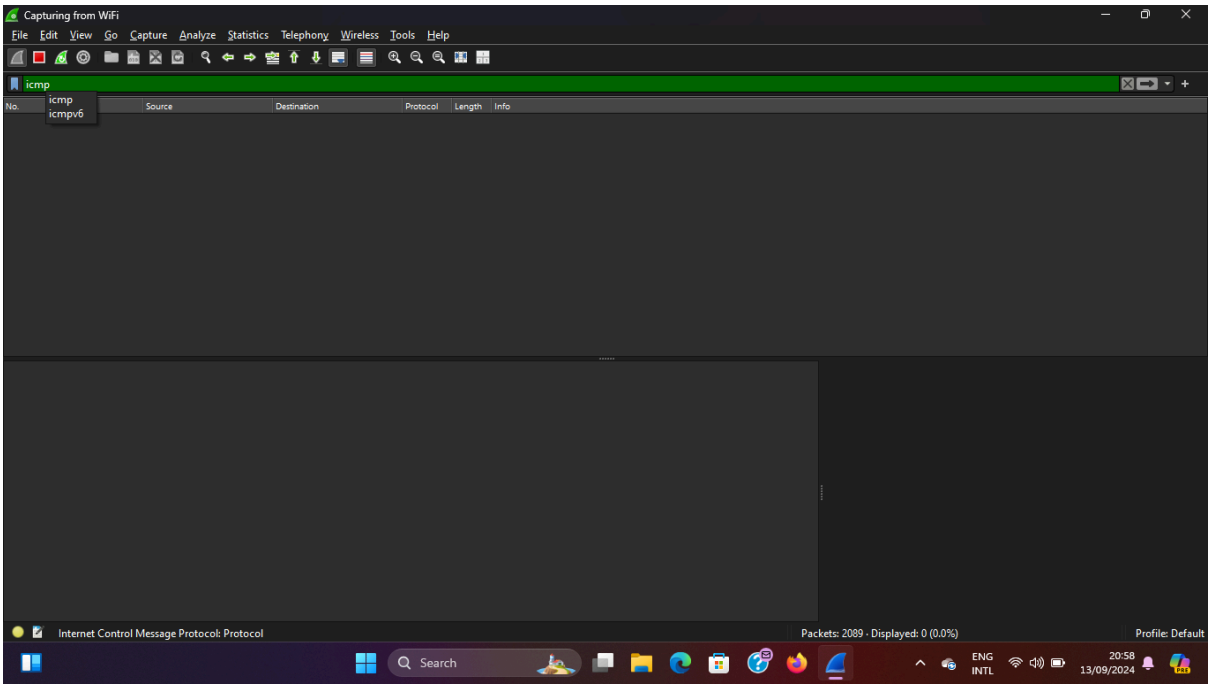

Fig 2: ICMP filter

Step 3: I pinged for the domain "tradingview.com" and the ping details and statistics were given. From this, we could see seamless communication with no interruption

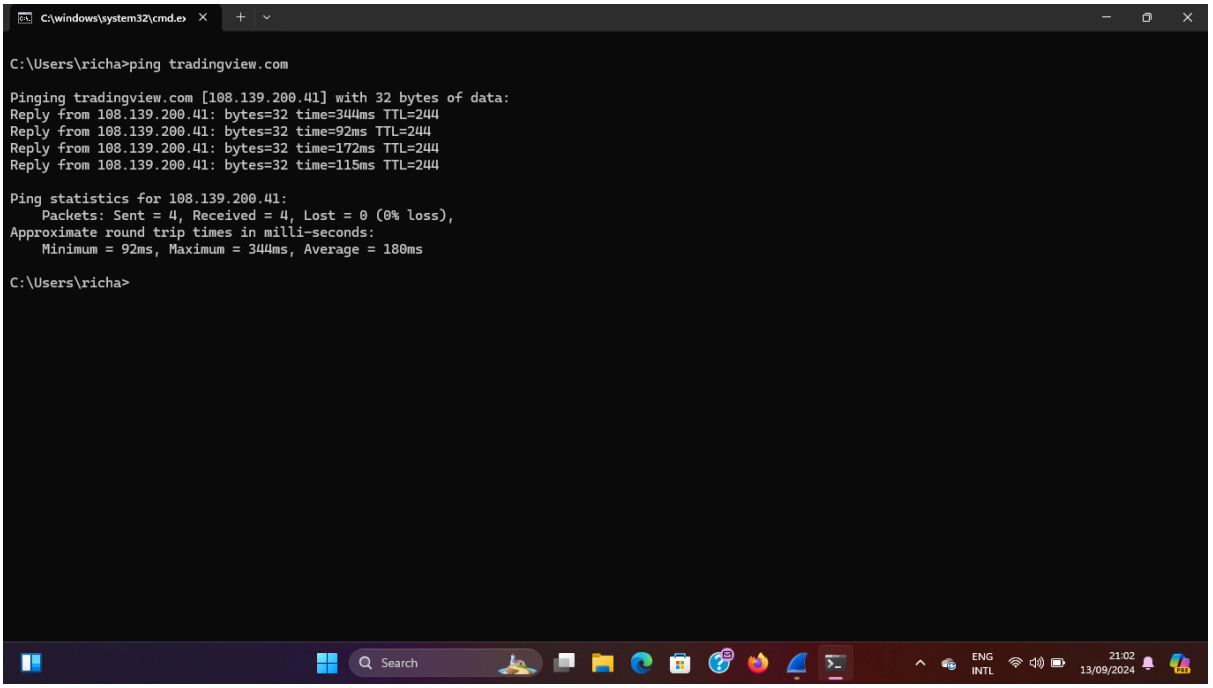

Fig 3: Result of the pinged domain on the windows command line

Step 4: using virustotal.com I checked the IP address of the domain for any malicious flagging. Also on whoer.net, I checked for further details on the domain

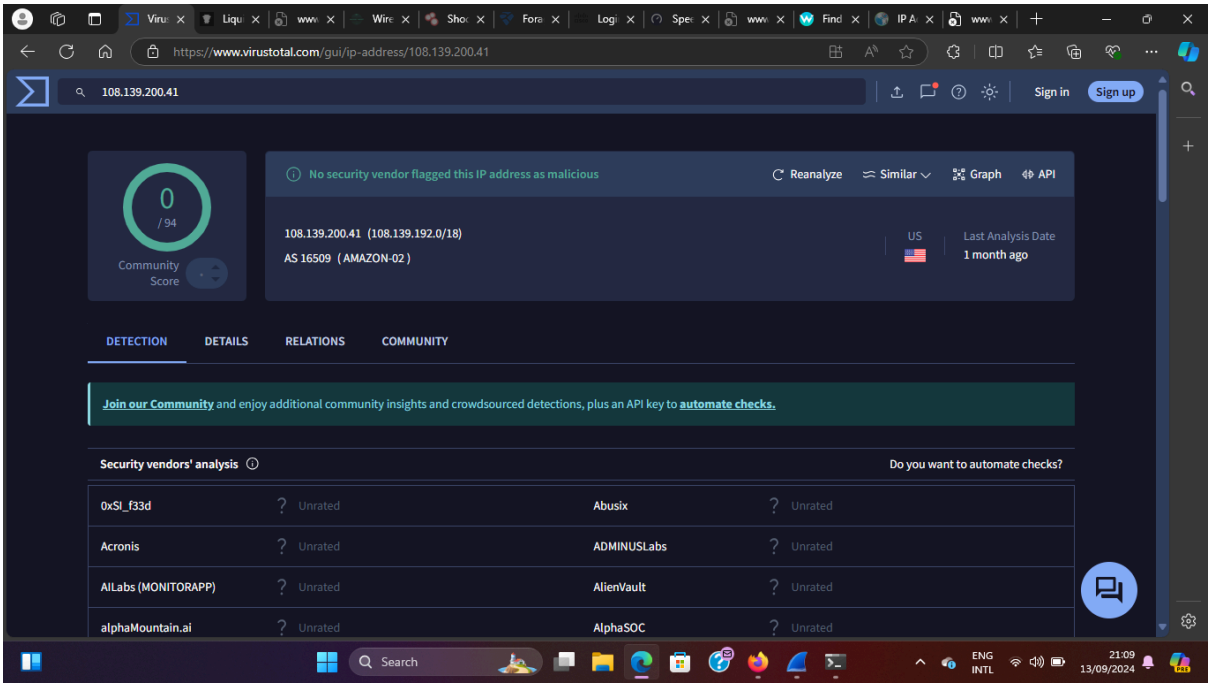

Fig 4: scanning pinged IP address on virustotal

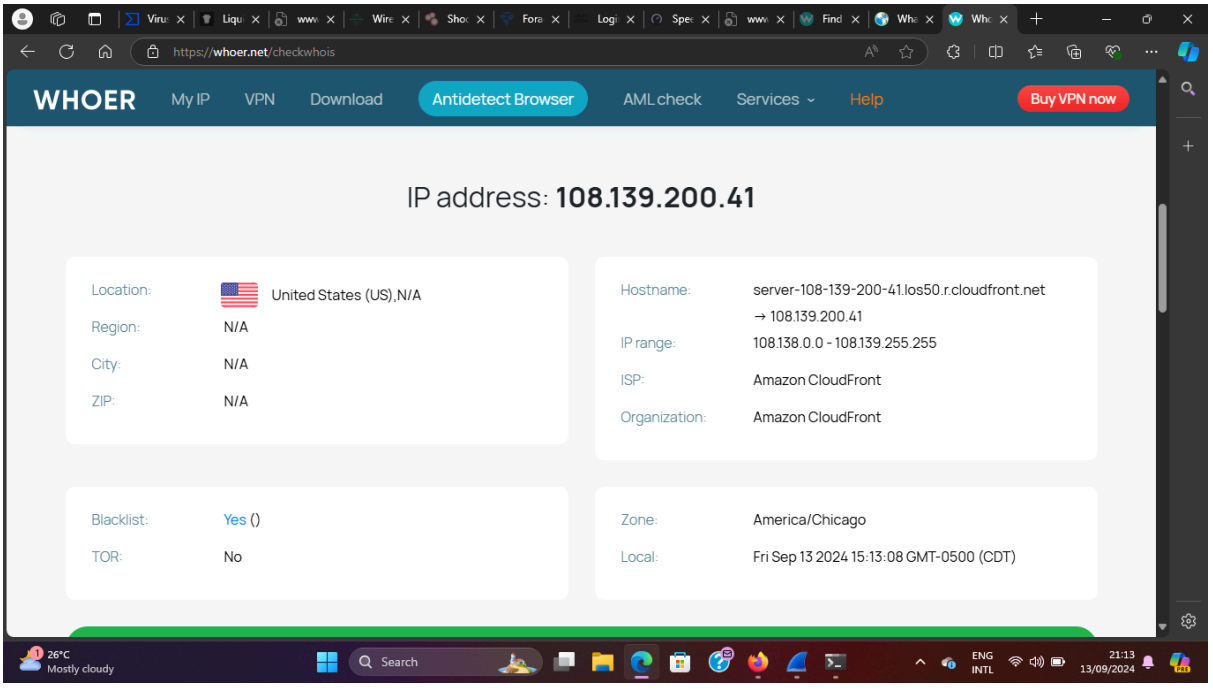

Fig4.4: scanning of pinged IP address on whoer.net

Step 5: The ICMP ping request has already been captured by the wireshark with each packet detail showing at the bottom left of the interface

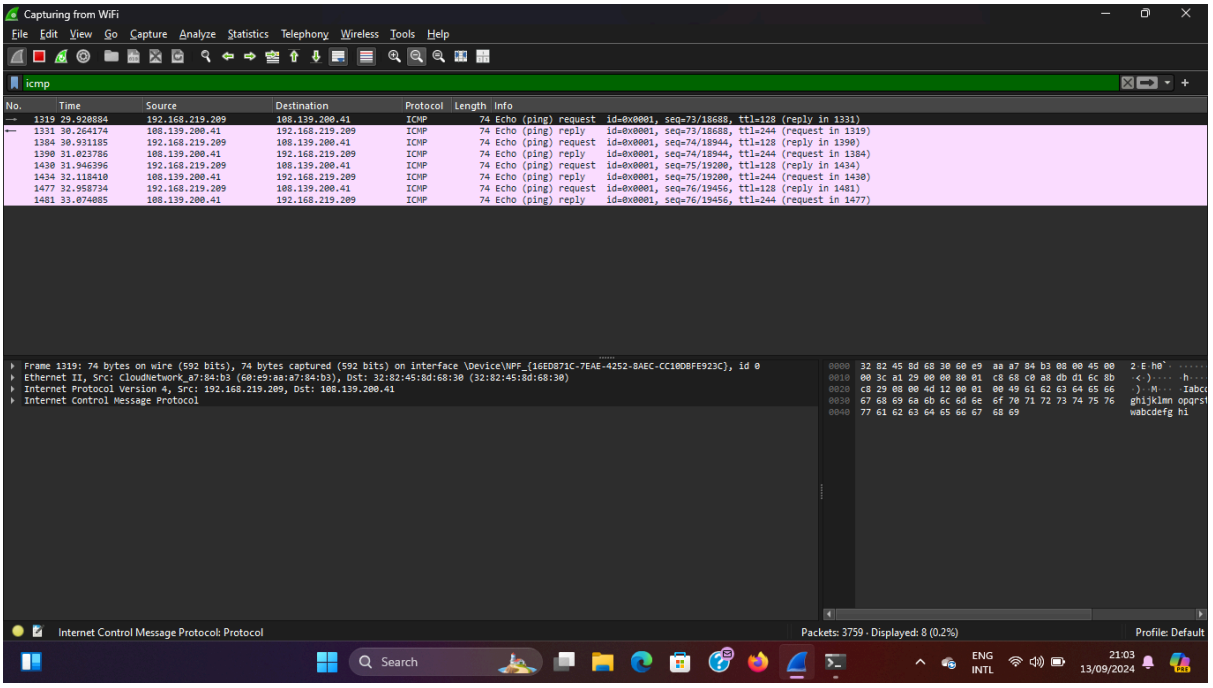

Fig 5: The first packet and its details

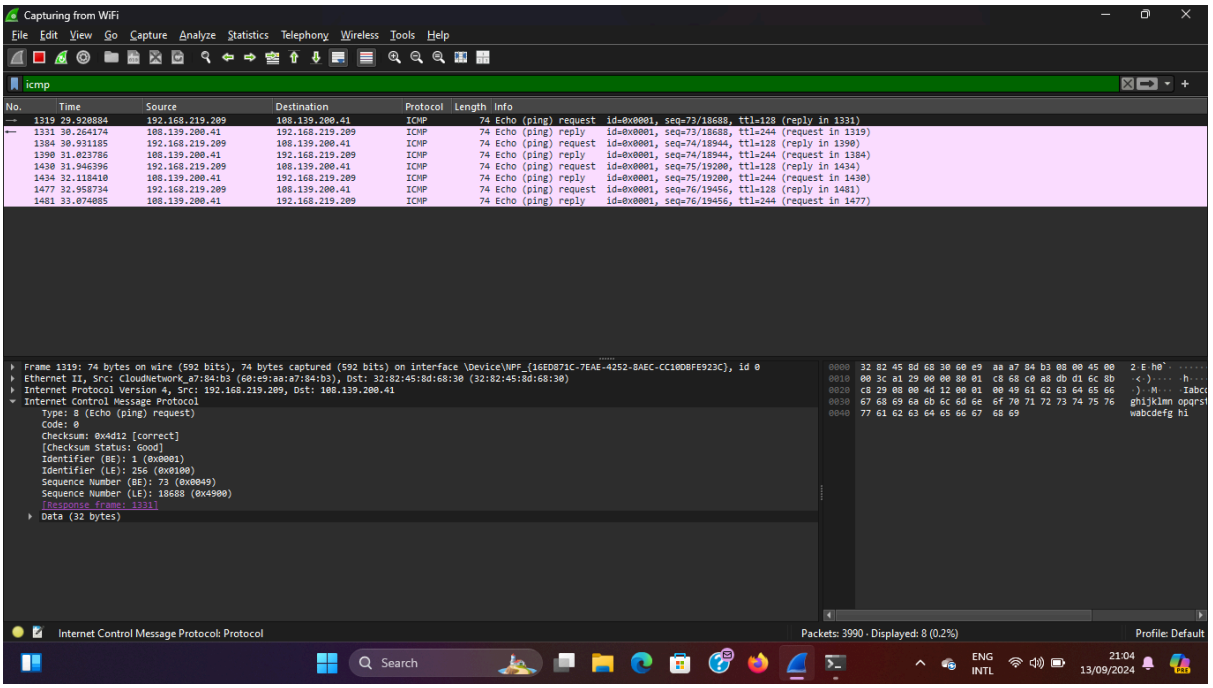

Fig 5.1: More details of the first packet

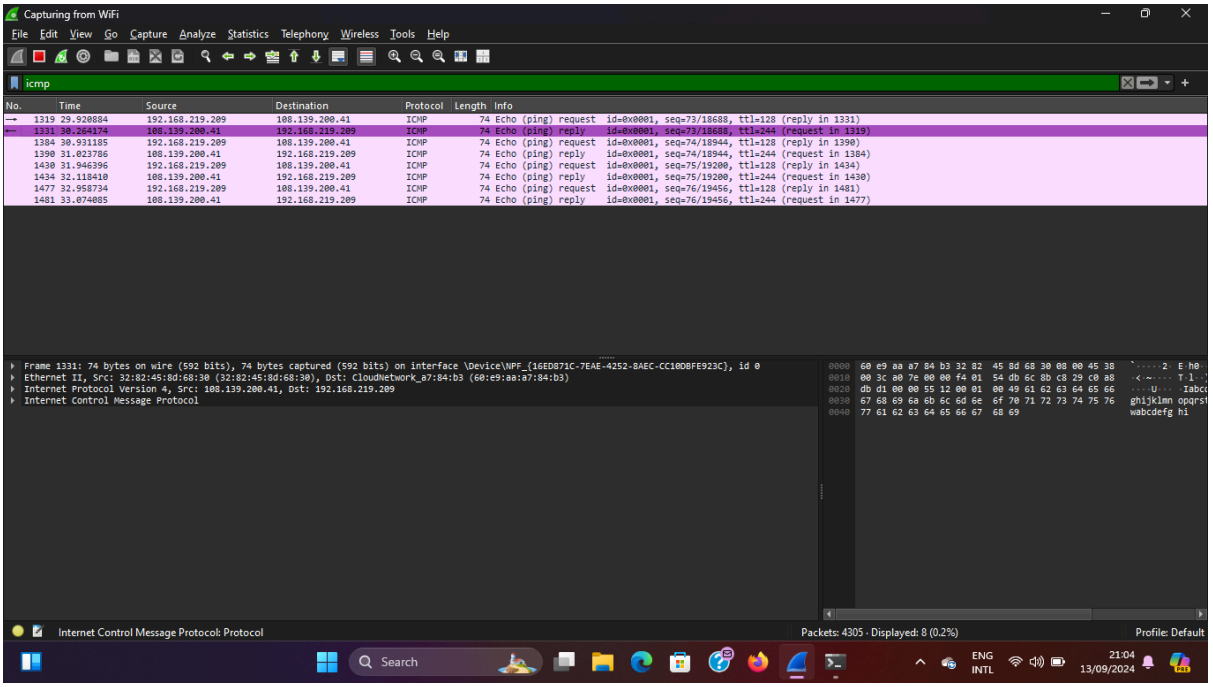

Fig 5.2: The second packet and its details

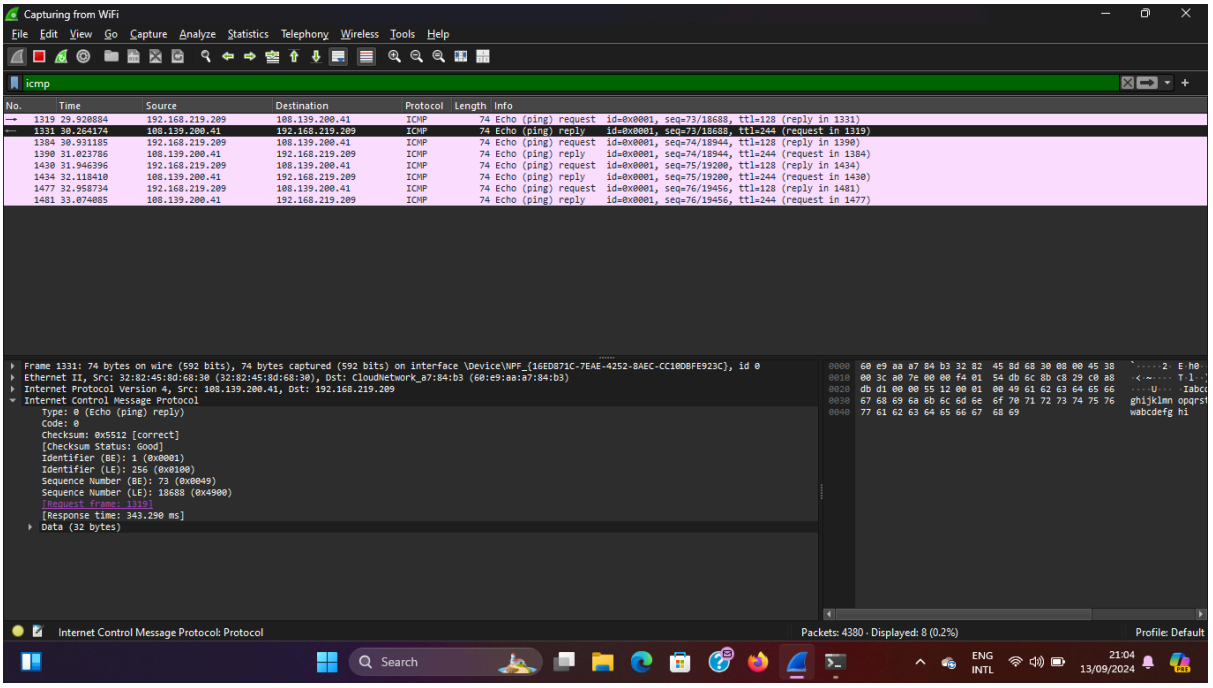

Fig 5.2.2: more details of the second details

ANALYSIS

Ping results:

1. The domain's IP address was seen as 108.139.200.41
2. A total of 4 packets were sent and were successfully received with no loss.

For the packet's round trip time, the minimum response time recorded was 92ms, a maximum response time of 344ms with an average response time of 180 ms.

Wireshark results

1. Under 29.9ms, the source IP address (192.168.219.209) initiated an echo request to the destination IP address (108.139.200.41) which in return gave an eco reply as seen in frame 1331 with a timeframe of 30.2ms.
2. Subsequent frames showed successful requests and replies between the captured networks.
3. IPv4 was also shown to have been used by both addresses

Additionally, the source IP address was shown to be malicious-free and safe for interaction on virustotal.com.

CONCLUSION

The network connectivity between the system and domain could be seen to have been successful owing to the respective data captured by the ping and Wireshark tools. On the other hand, the domain name was seen to be safe for interactions as shown by Virustotal and whoer.net.