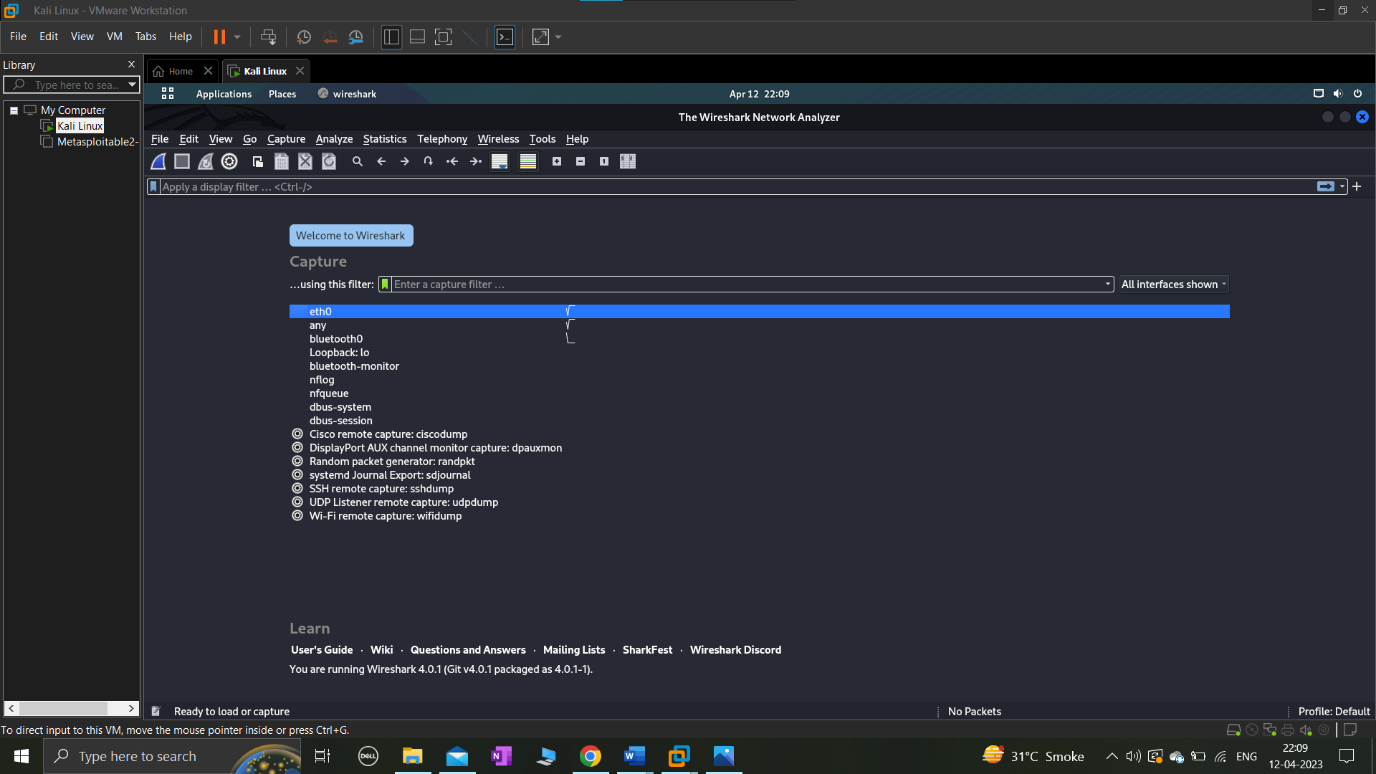
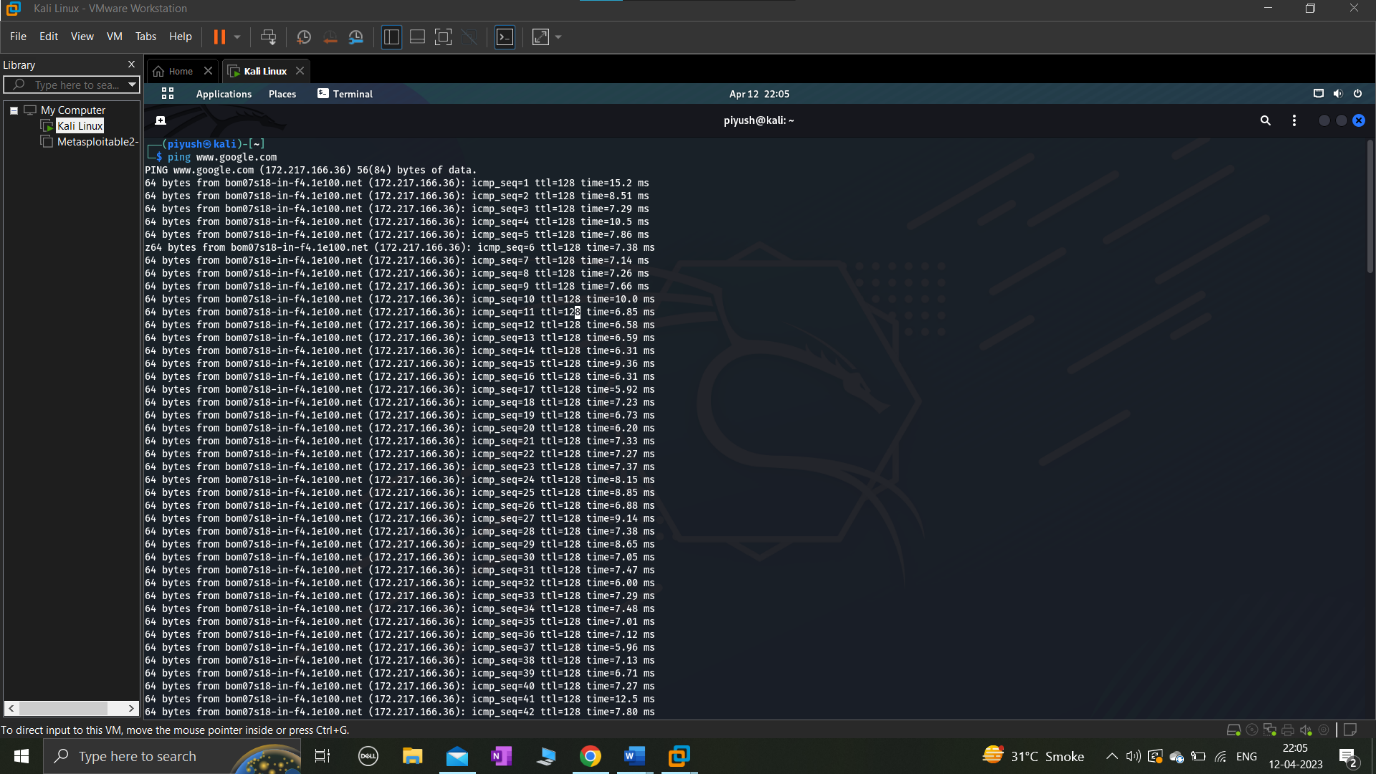
Wireshark

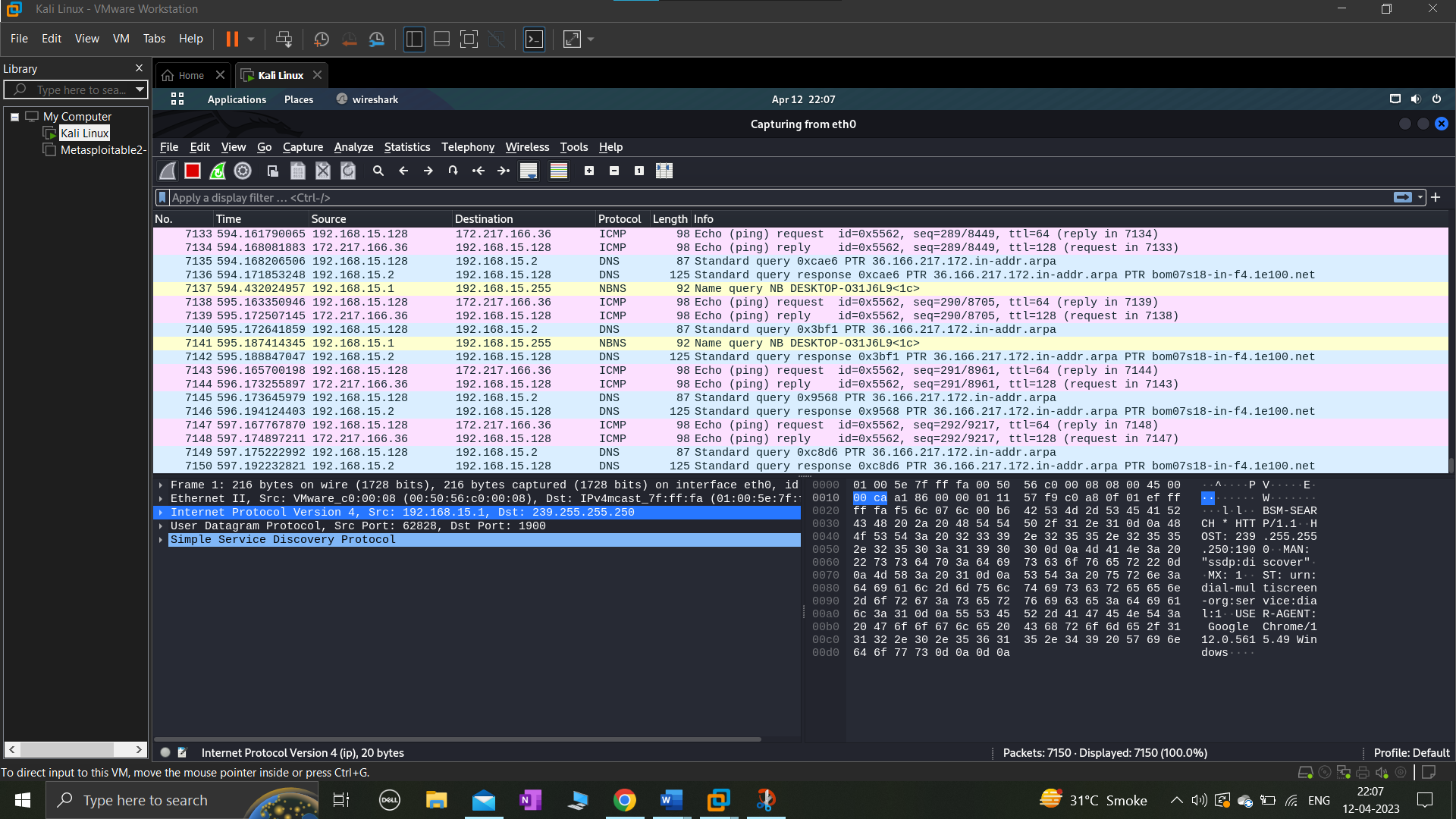
Wireshark is a network protocol analyzer that is commonly used to collect and analyze network data packets. This report will use Wireshark to capture and analyze all packets to obtain insight into network traffic.



Capture Configuration: In order to capture all packets on Wireshark, we must establish the capture settings properly. Selecting the right network interface to capture traffic from, setting the capture filter to "no filter" or "all packets," and starting the capture are all necessary steps. Wireshark will capture all packets that pass across the designated network interface once the capture is initiated. The command "ping www.google.com" was used to display all of the packets delivered to the website, as shown in the image below.

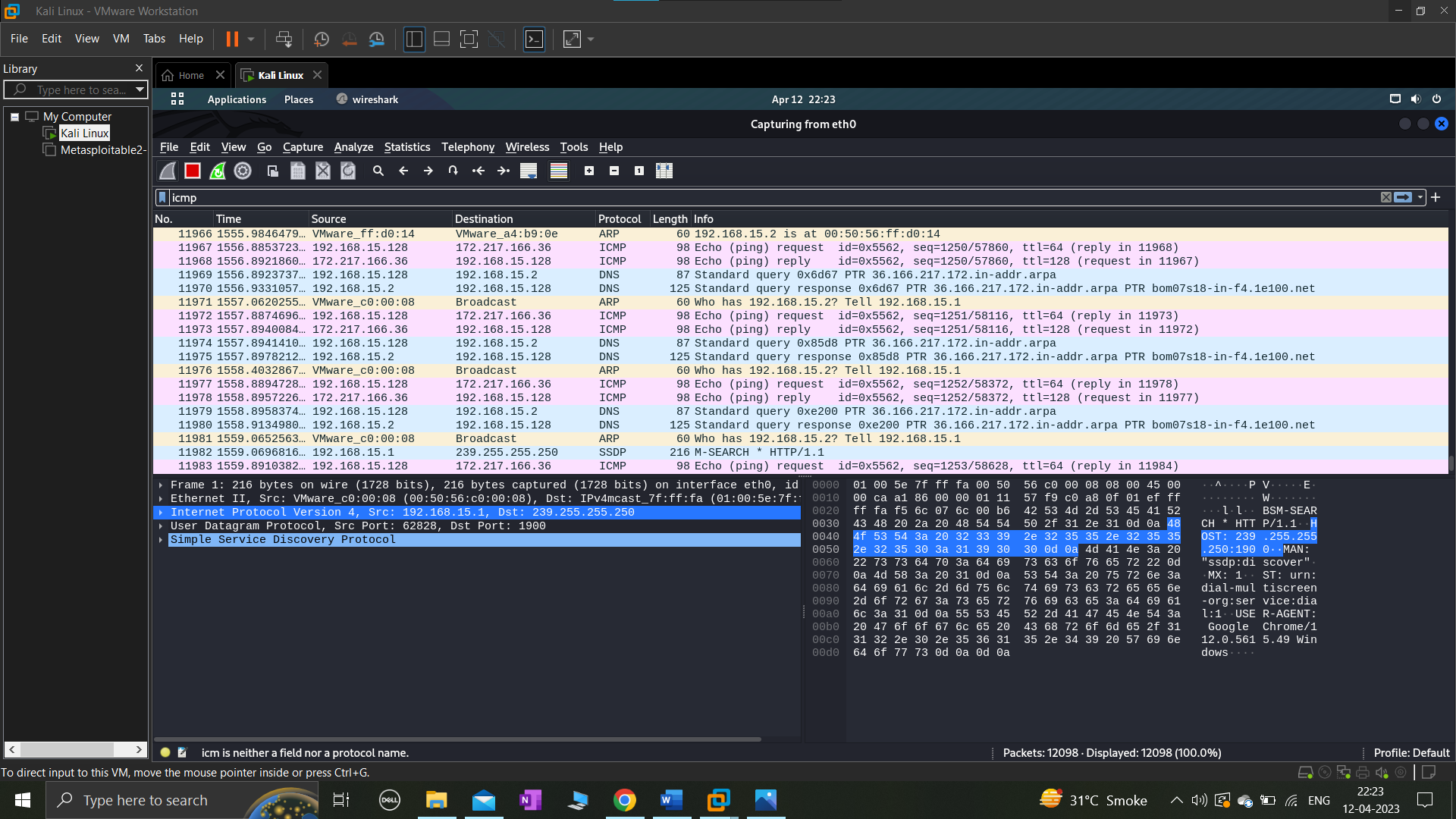


Wireshark will allow us to view which packets are sent to and which packets are received from the website when we open it. The IP address of the sender's incoming packets will also be shown.



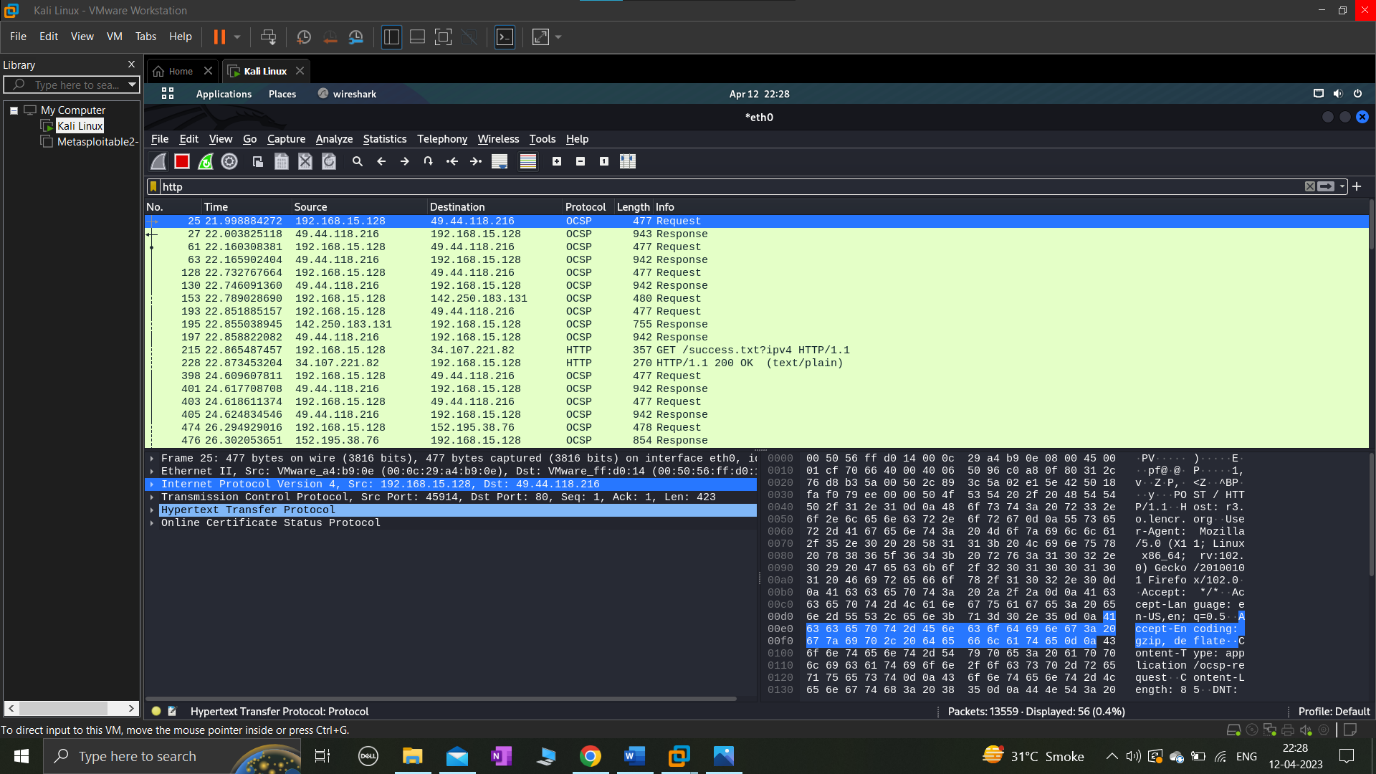
Packet analysis: After collecting all of the network's packets, we can examine the packets to learn more about the traffic on the network. Using the numerous built-in analysis capabilities in Wireshark, we can examine the packets.

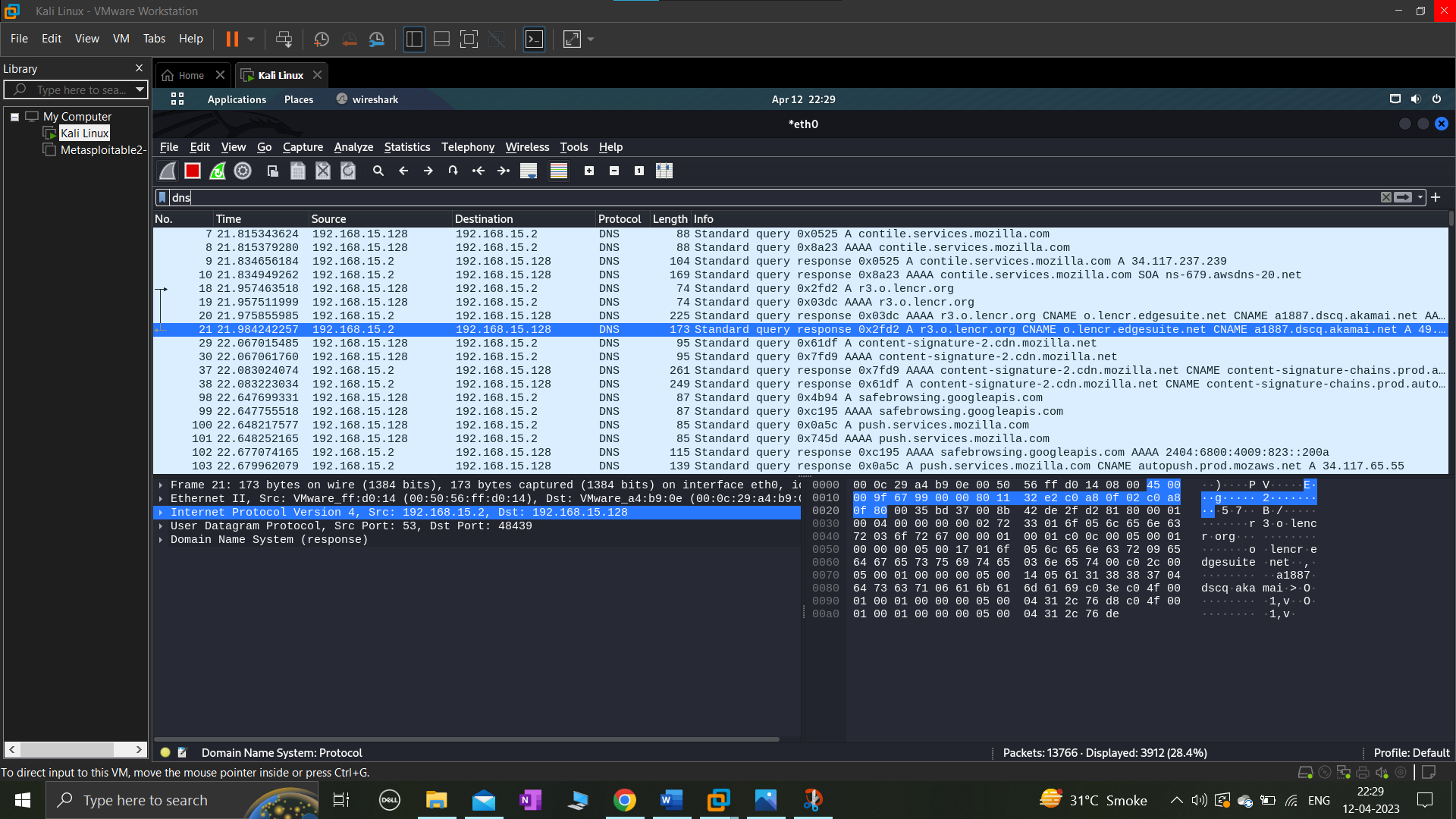
We utilised the ICMP protocol to create the image below. Network devices employ the Internet Control Message Protocol (ICMP), a network layer protocol, to identify problems with network connectivity. ICMP is mostly used to check whether data is arriving at its target location on time. The ICMP protocol is frequently used on network equipment, such as routers. Although ICMP is essential for error reporting and testing, distributed denial-of-service (DDoS) attacks can also make use of it.



We can also study the network's traffic based on the various types of traffic. For example, we could look at the amount of HTTP, DNS, or SMTP traffic on the network. The size of each package can also help us identify any that are unusually large or little.

Here is an illustration of HTTP and DNS traffic.





In conclusion, Wireshark's ability to capture and analyze every packet allows for a wealth of information to be gleaned about network traffic. We can get a better idea of how the network is used and spot any possible problems by looking at the types of traffic, the protocols that are being used, and any security concerns. Network administrators, security experts, and anybody else interested in comprehending the traffic on a network can utilize Wireshark, a potent tool for network analysis.