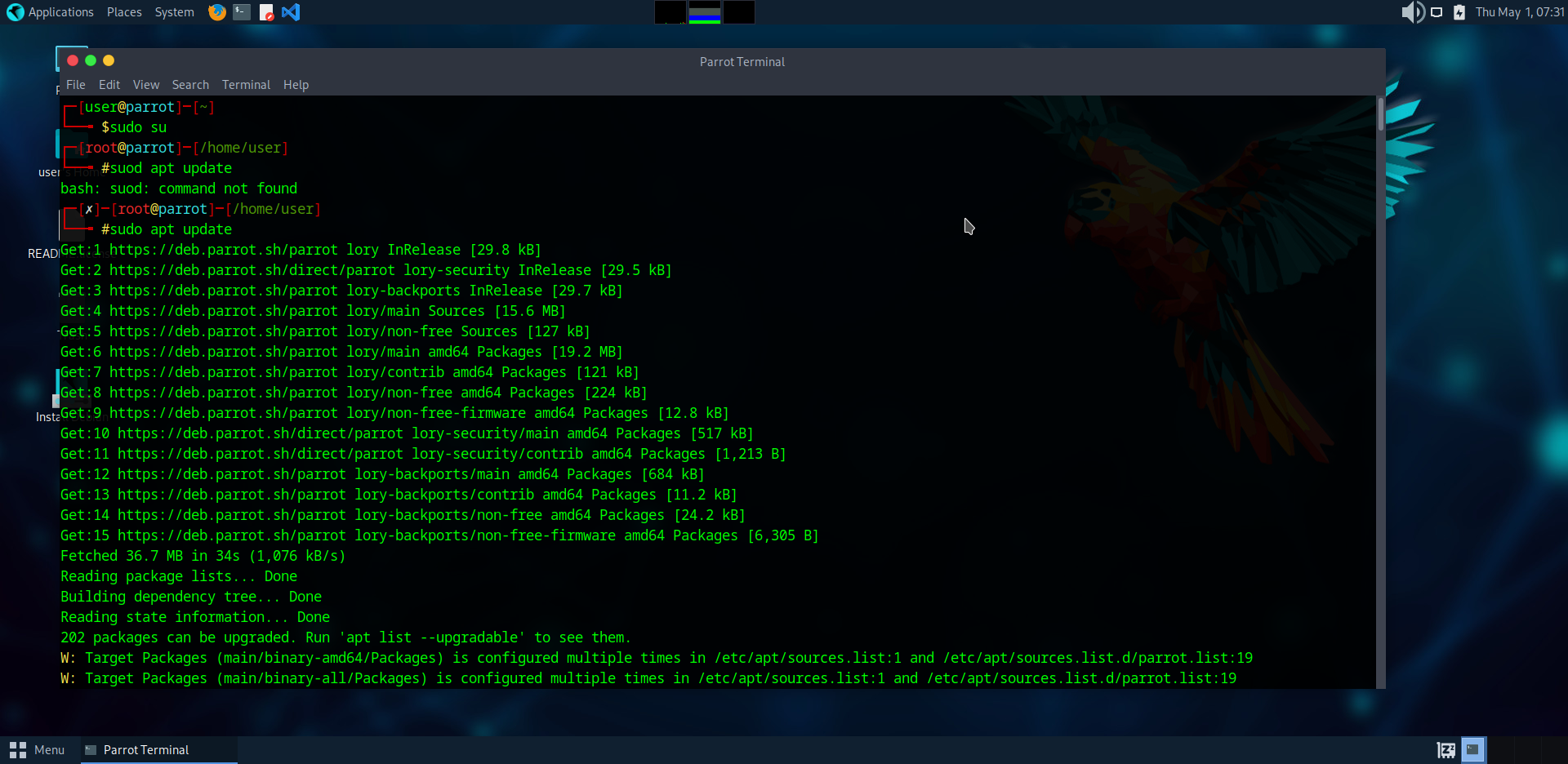
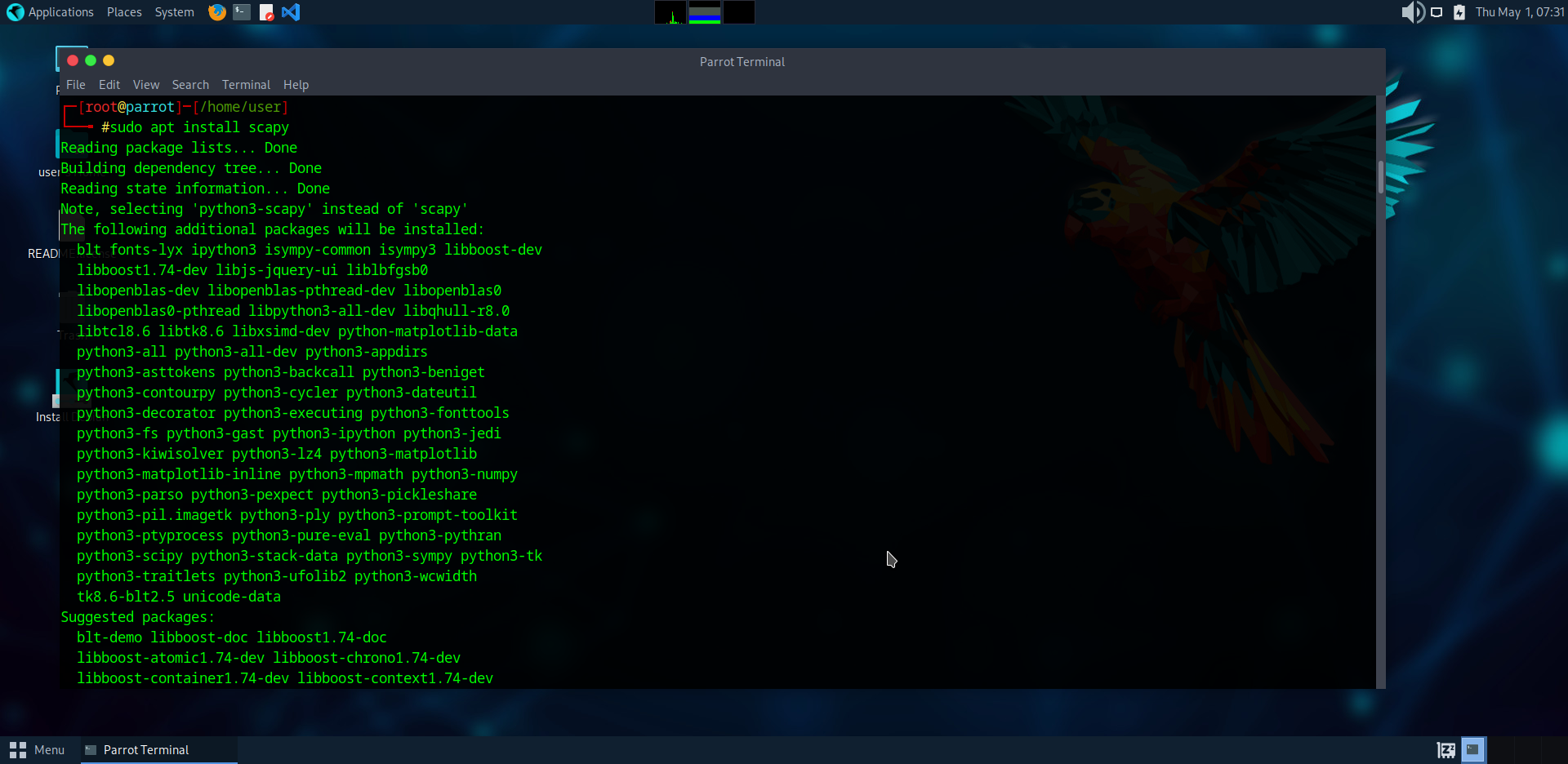
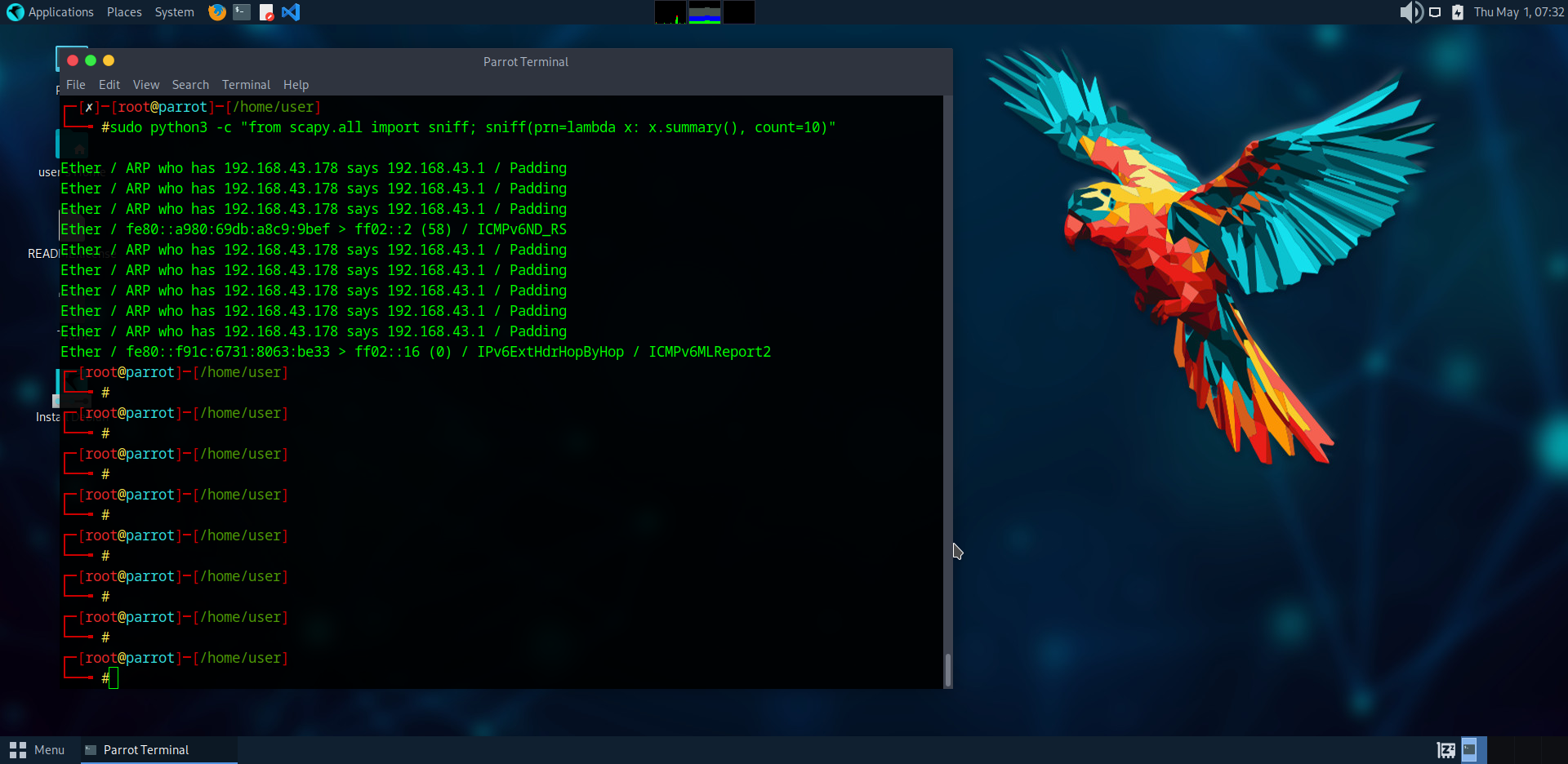
Task -1







Network sniffing is the process of capturing and analyzing data packets transmitted over a network.

It is commonly used for:

* Network troubleshooting (e.g., detecting connectivity issues).
* Security analysis (e.g., identifying malicious traffic).
* Protocol research (e.g., studying how applications communicate).

1. *Add Filters Capture only HTTP (tcp port 80) or DNS (udp port 53).*
2. *Log Packets to a File Save as .pcap for analysis in Wireshark*
3. *Detect Anomalies Flag unusual traffic (e.g., ARP spoofing).*

