Vellore Institute of Technology
(Deemed to be University under section 3 of the UGC Act, 1956)

# WINTER SEMESTER 2019-20
# DIGITAL FORENSICS (CSE4004)
# LAB ASSIGNMENT - 1

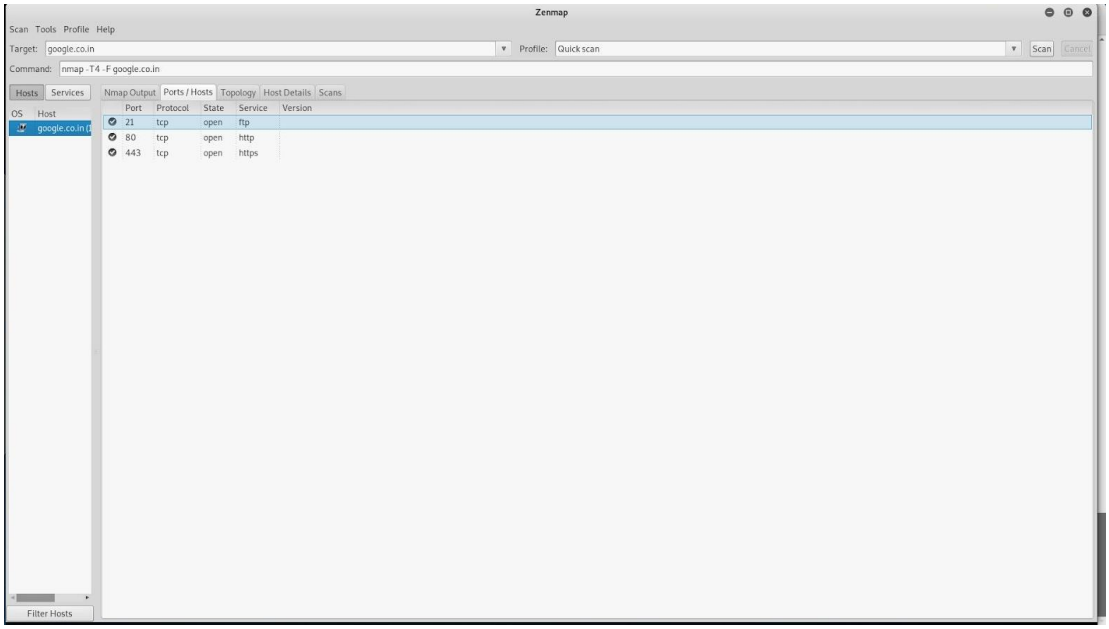
**Dishi Jain**
**17BCB0055**

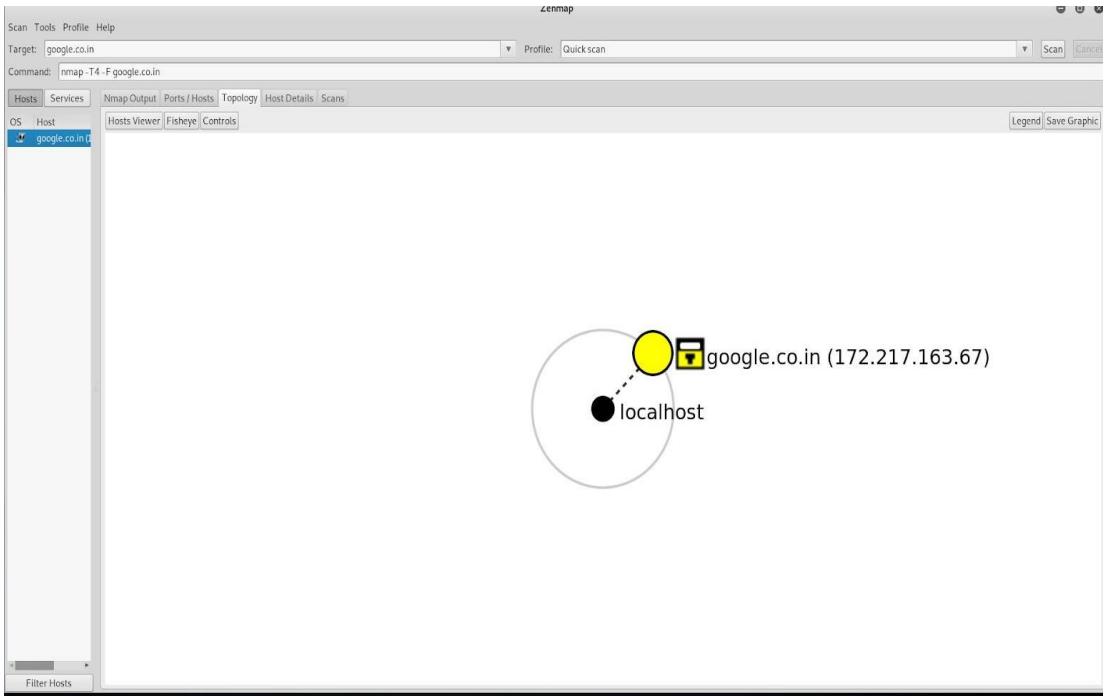
1. **QUICK SCAN** (google.com)

**Nmap** will send four packets to determine that the host is up, then at least 1,000 to port **scan** the host. You can **scan** just the most popular 100 ports with the -F (**fast scan**) option, specify an arbitrary number of the most commonly open ports with --top-ports , or provide a custom list of ports to -p .

**Command: nmap -T4 -F <target>**

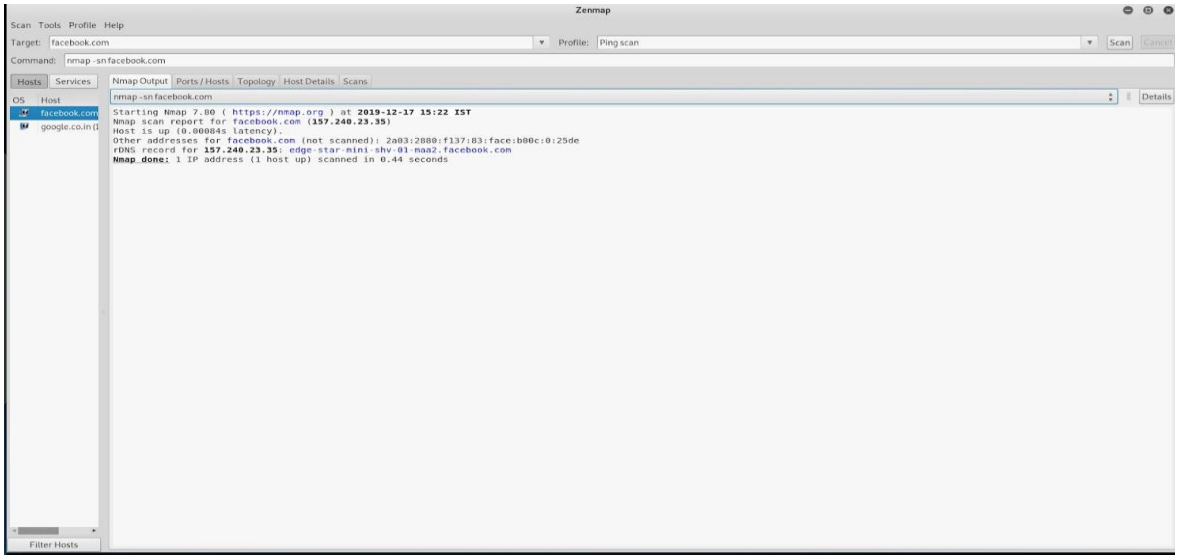
Scan faster than the intense scan by limiting the number of TCP ports scanned to only the top 100 most common TCP ports.

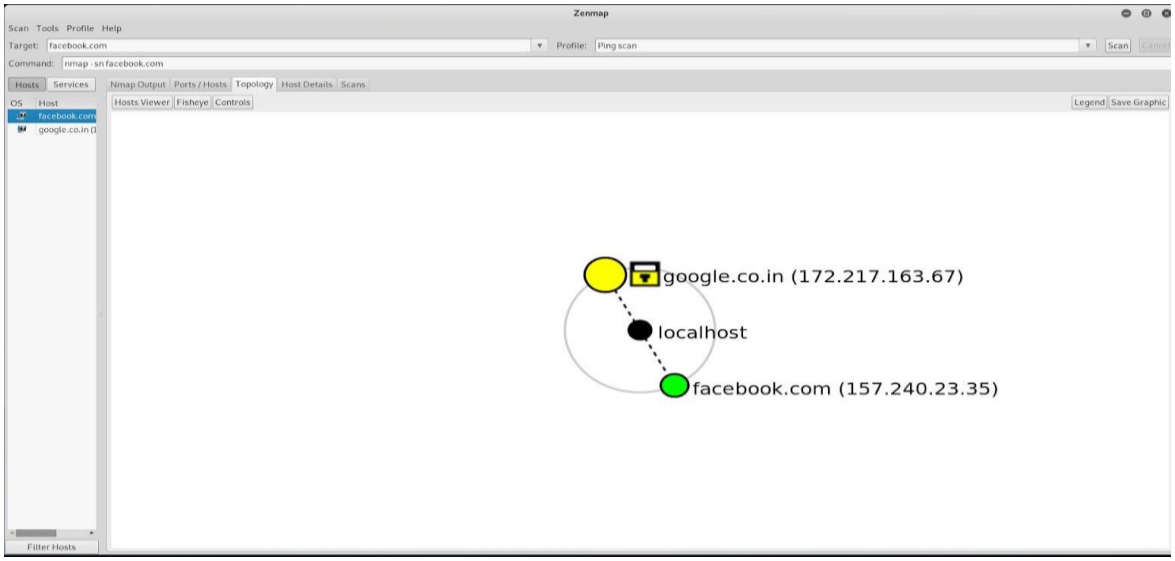



The IP we received is 172.217.163.67
Currently FTP(21), HTTP(80) & HTTPS (443) ports are active.

2. **PING SCAN** (facebook.com)
   - This does a simple ping of all the addresses to see which ones are answering to ICMP. If you don't really care about what services are running and you just want to know which IP addresses are up, this is a lot faster than a full port scan.
   - However, some machines may be configured not to respond to a ping (for example, machines running the new XP firewall) but still have services running on them, so a ping sweep is not as accurate as a full port scan.



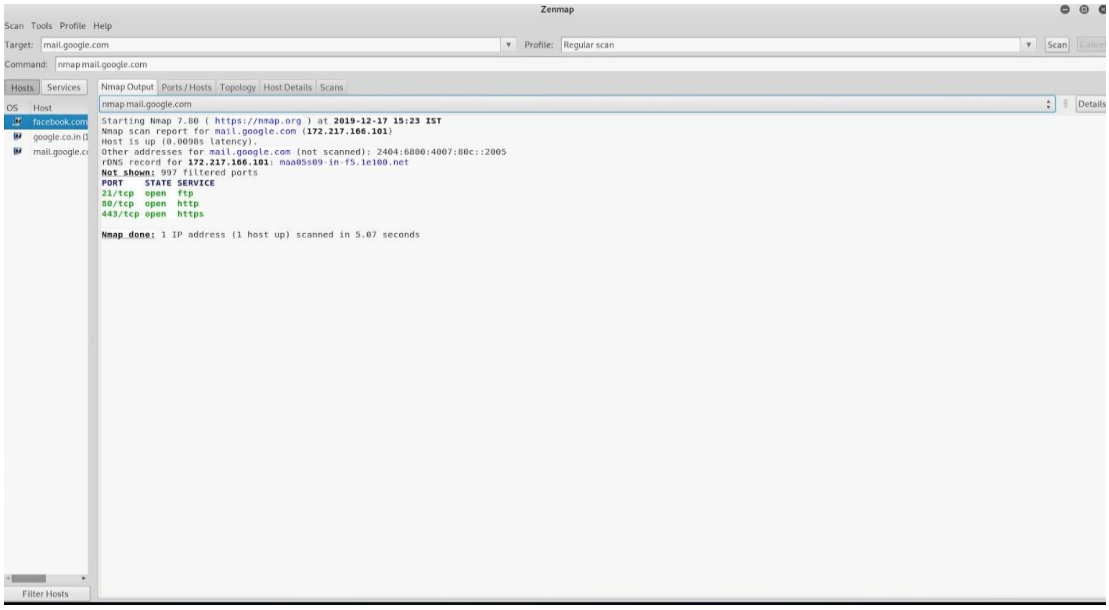



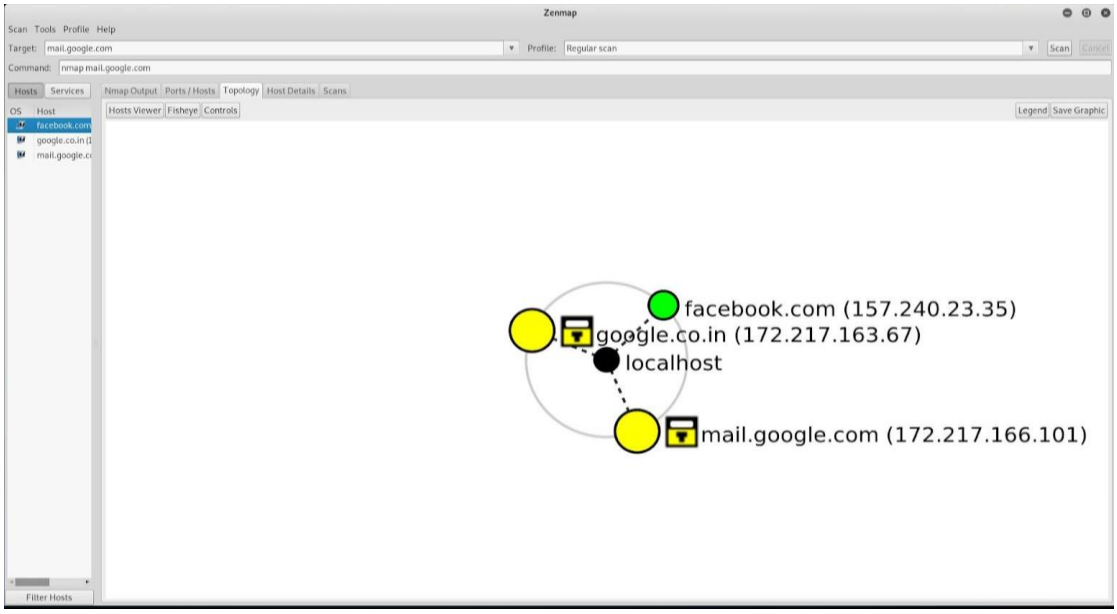

IP Received: 157.240.23.35
Latency: 0.00084 seconds

3. **Regular Scan** (mail.google.com)

## Command: nmap <target>

Default everything. This means it will issue a TCP SYN scan for the most common 1000 TCP ports, using ICMP Echo request (ping) for host detection.




IP: 172.217.166.101