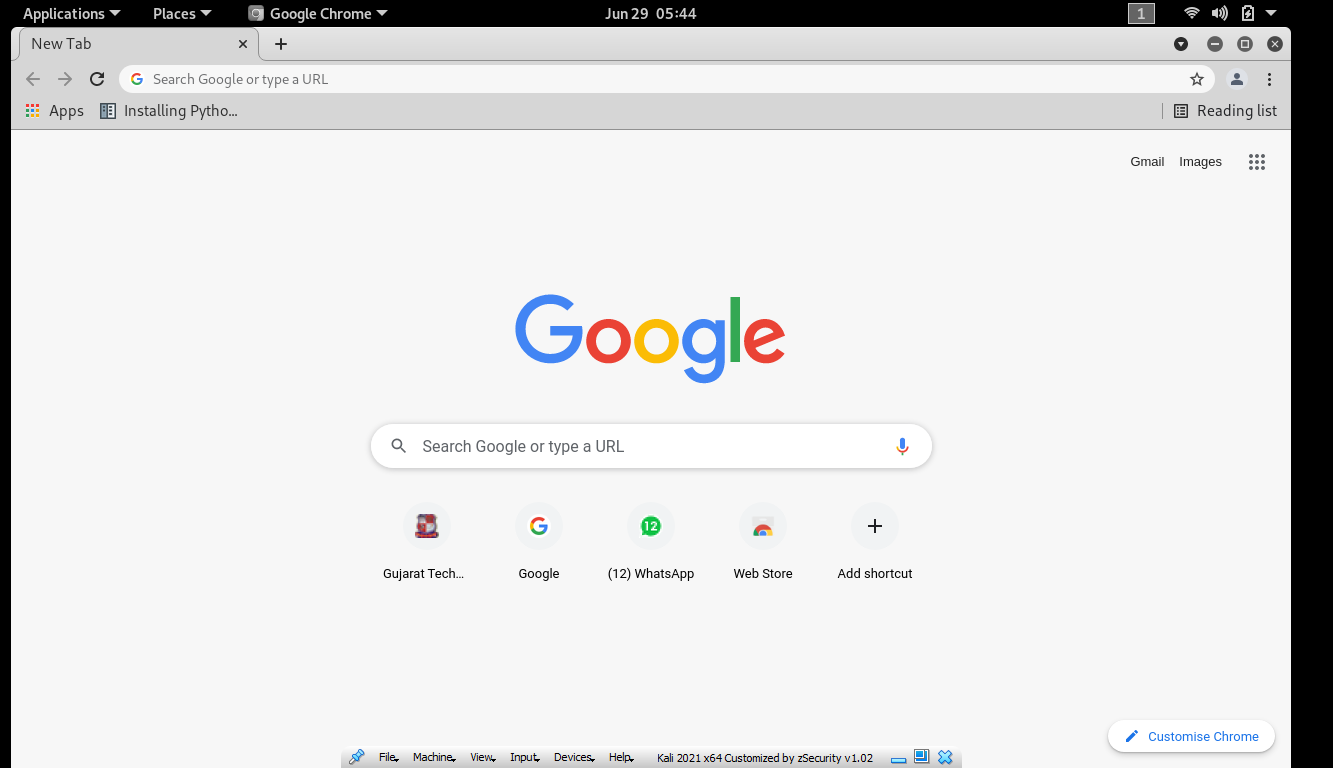
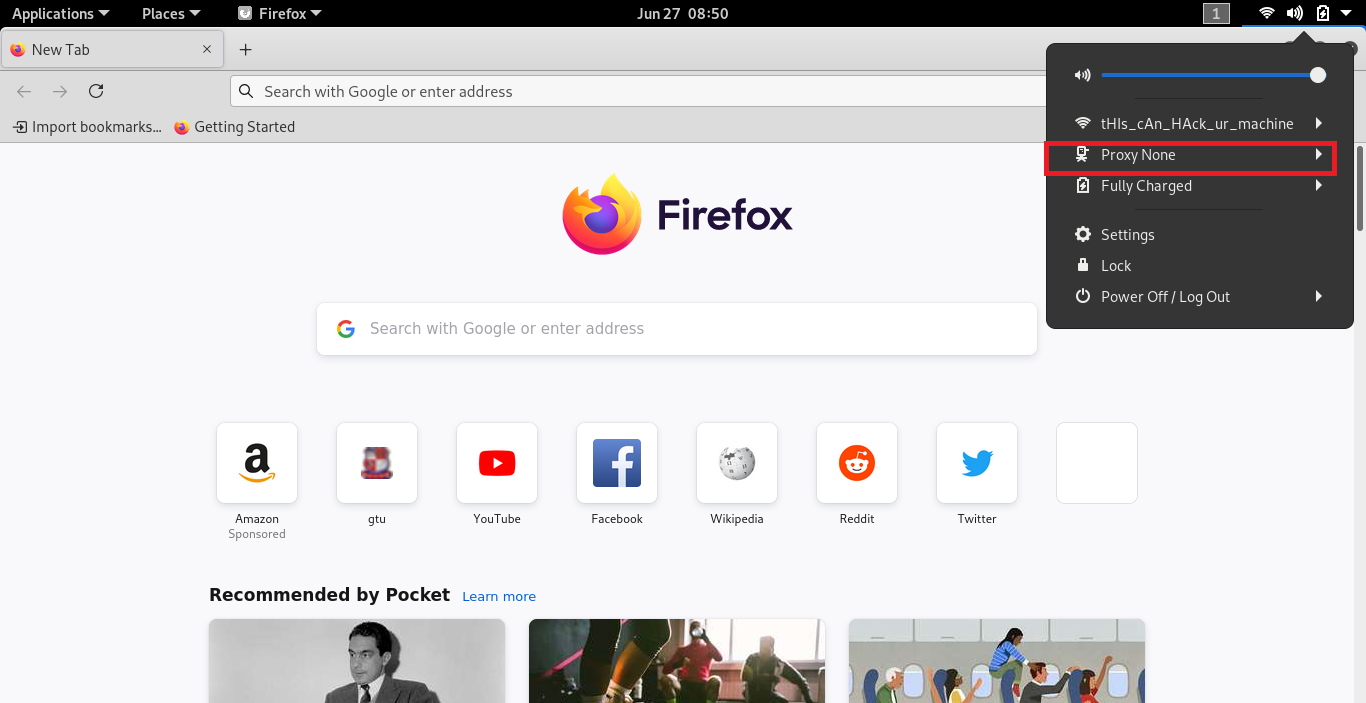
**1. Start up your favorite web browser, which will display your selected homepage.**

****

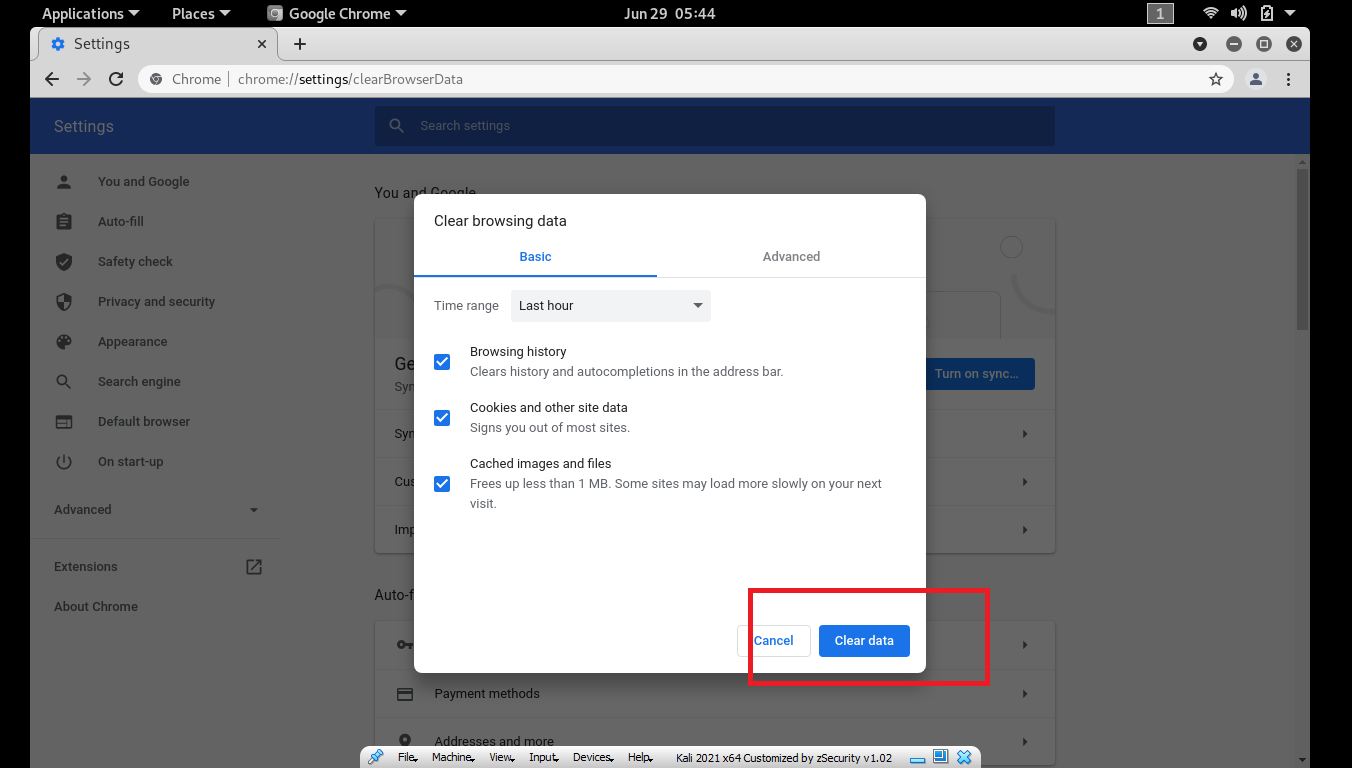
**2. If you are using a proxy (especially a host-based one), disable it if possible to**

**examine uncached network traffic.**

****

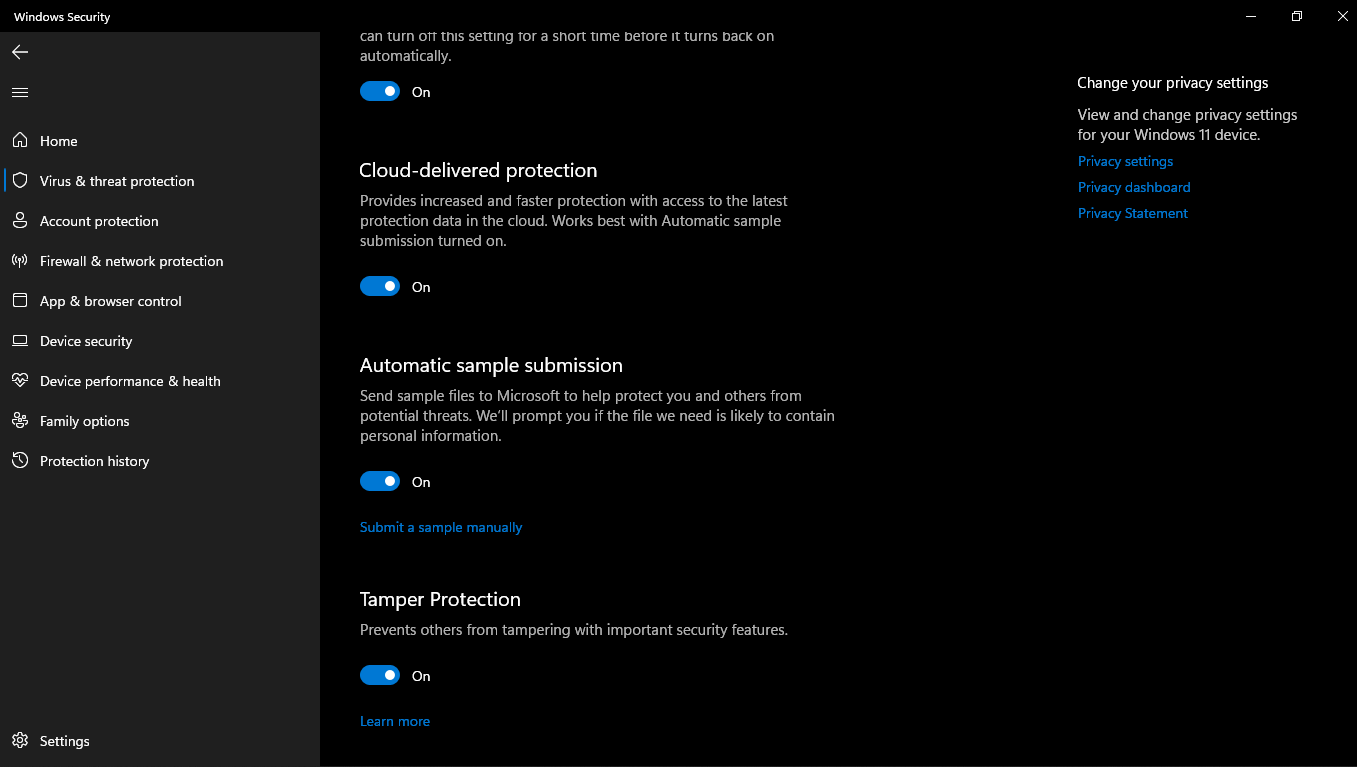
**3. Also better to clear browser cache, cookies if you have previously displayed this**

**page.**

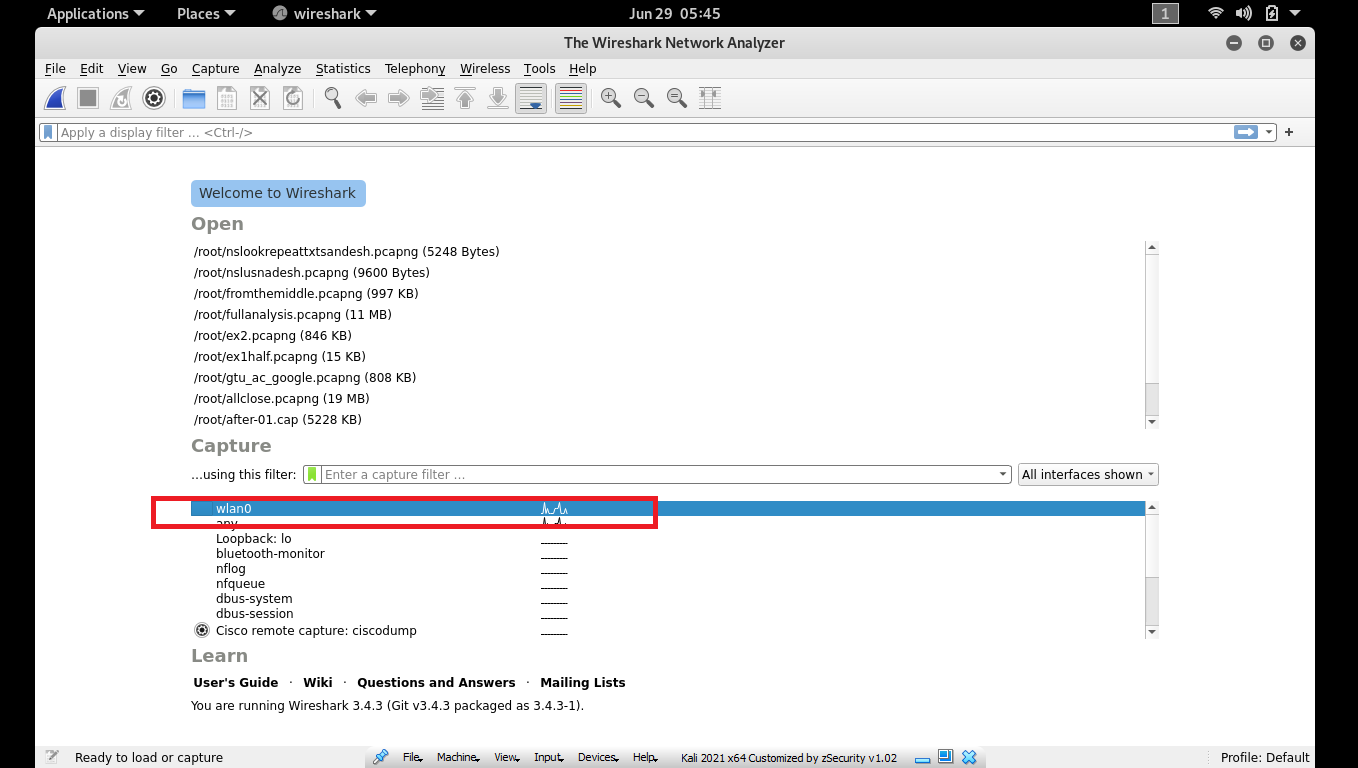
****

**4. You may need to disable anti-virus protection software before your own IP address**

**will show up in captured data.**



**5. Start up the Wireshark software, select the Capture pull down menu and select**

**Interfaces.**

**6. Here we will be using nslookup tool, which is available in most Linux/Unix and**

**Microsoft platforms today.**

**9. Command Run 1: nslookup www.gtu.ac.in or www.facebook.com or www.google.com**

**nslookup www.gtu.ac.in, here this command tells please send me the IP address for the host**

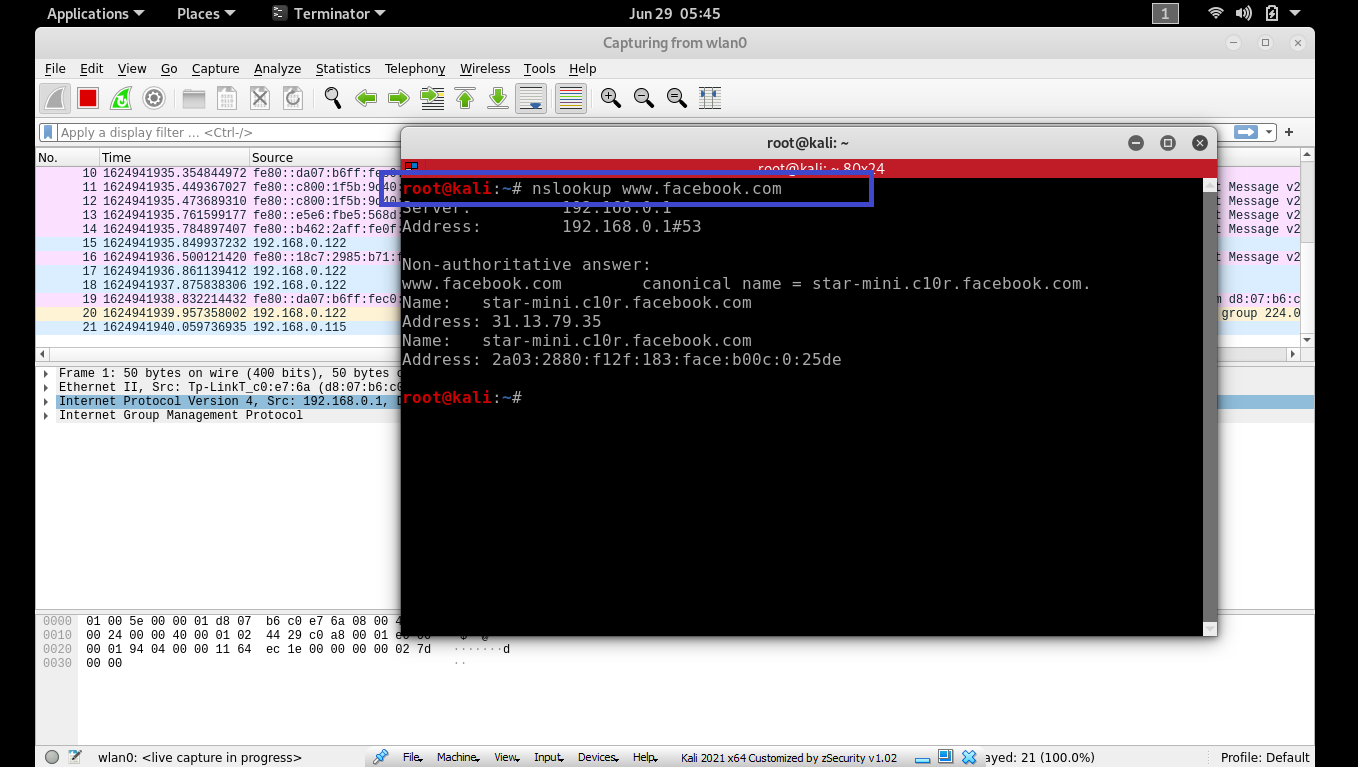
**www.gtu.ac.in the response from this command provides two pieces of information: (1) the**

**name and IP address of the DNS server that provides the answer; and (2) the answer itself,**

**which is the host name and IP address of www.gtu.ac.in. response came from the local DNS**

**server; it is quite possible that this local DNS server iteratively contacted several other DNS**

**servers to get the answer.**

****

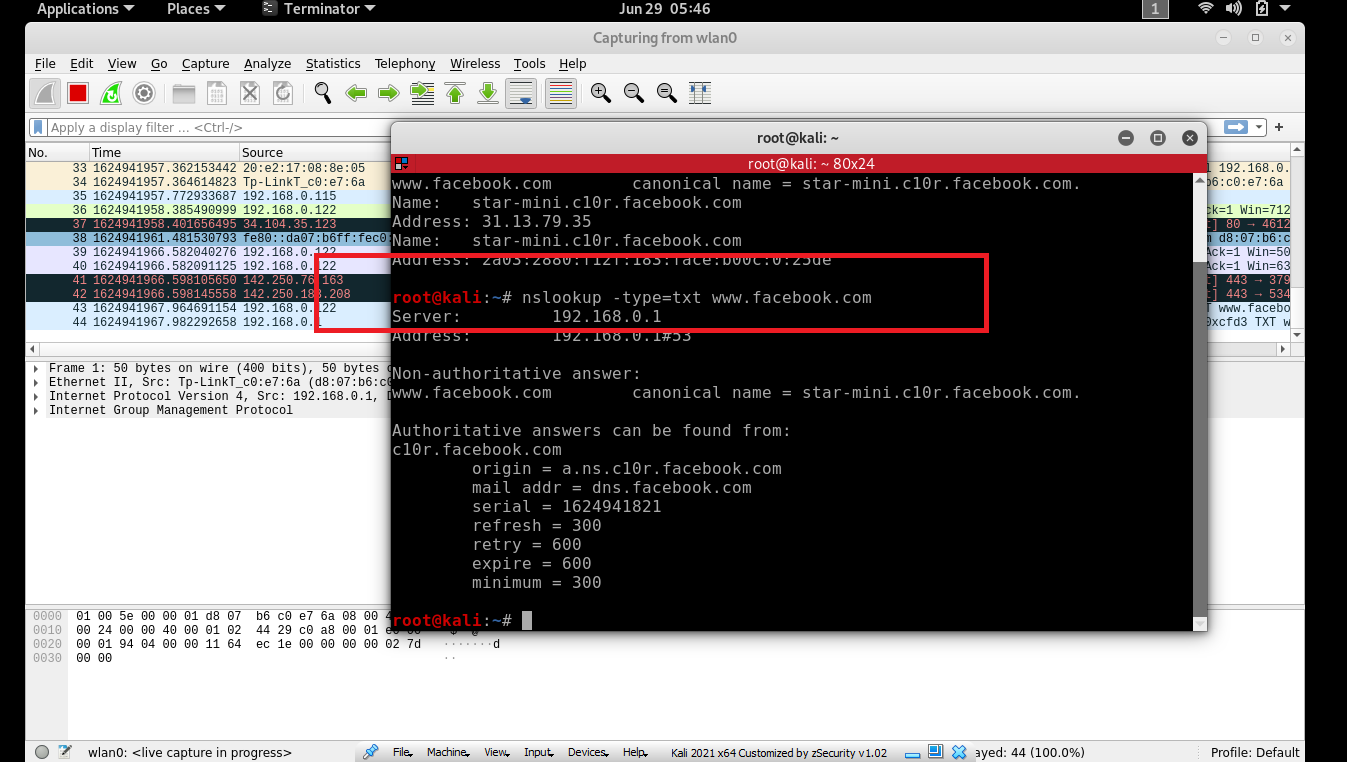
**10. Command Run 2 : nslookup –type =NS www.facebook.com or type nslookup –type =NS**

**www.gtu.ac.in, here provided the option “-type=NS” and the domain “facebook.com” or**

**“gtu.ac.in”. This causes nslookup to send a query for a type-NS record to the default local DNS**

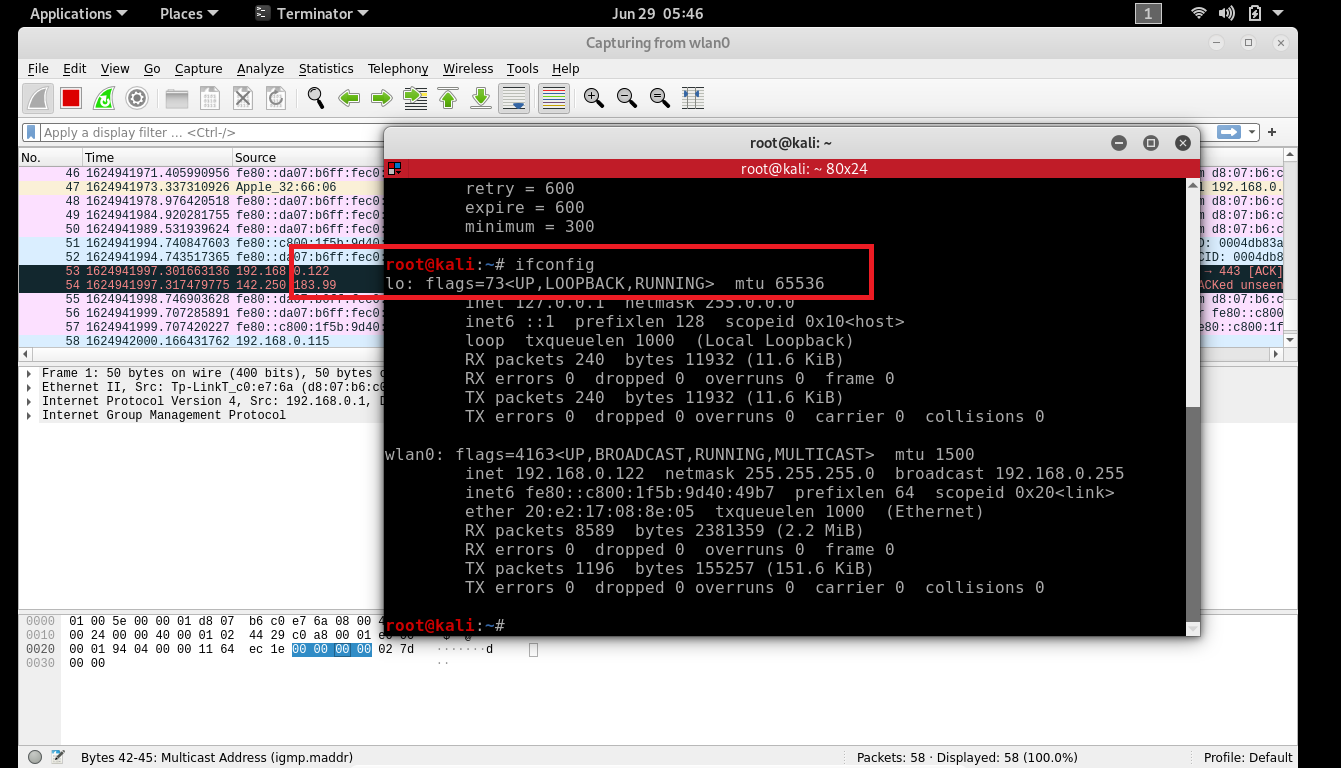
**server. In words, the query is saying, “please send me the host names of the authoritative DNS**

**for facebook.com, gtu.ac.in**

****

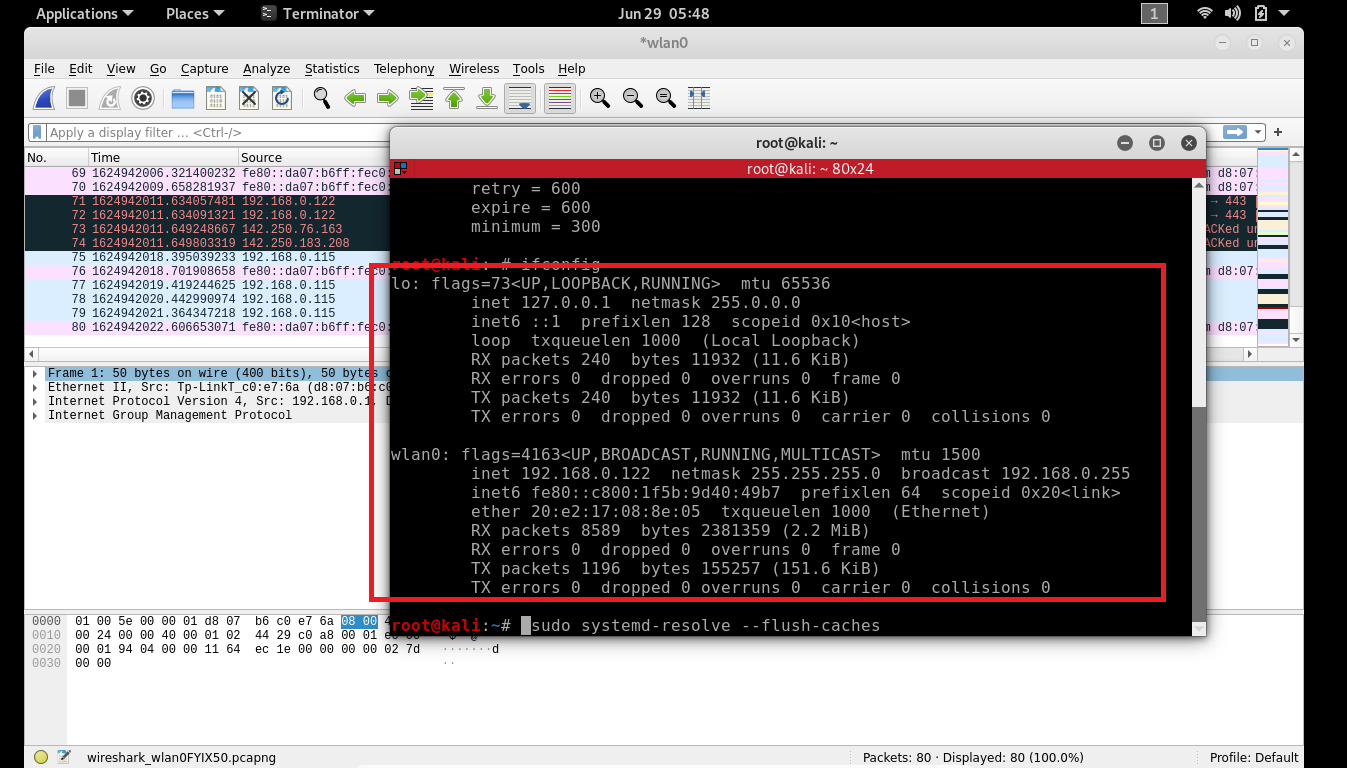
**11. ipconfig (for Windows) and ifconfig (for Linux/Unix) command show your current TCP/IP**

**information, including your address, DNS server addresses, adapter type and so on.**

****

**13. we learned that a host can cache DNS records it recently obtained. To see these cached**

**records,**

****

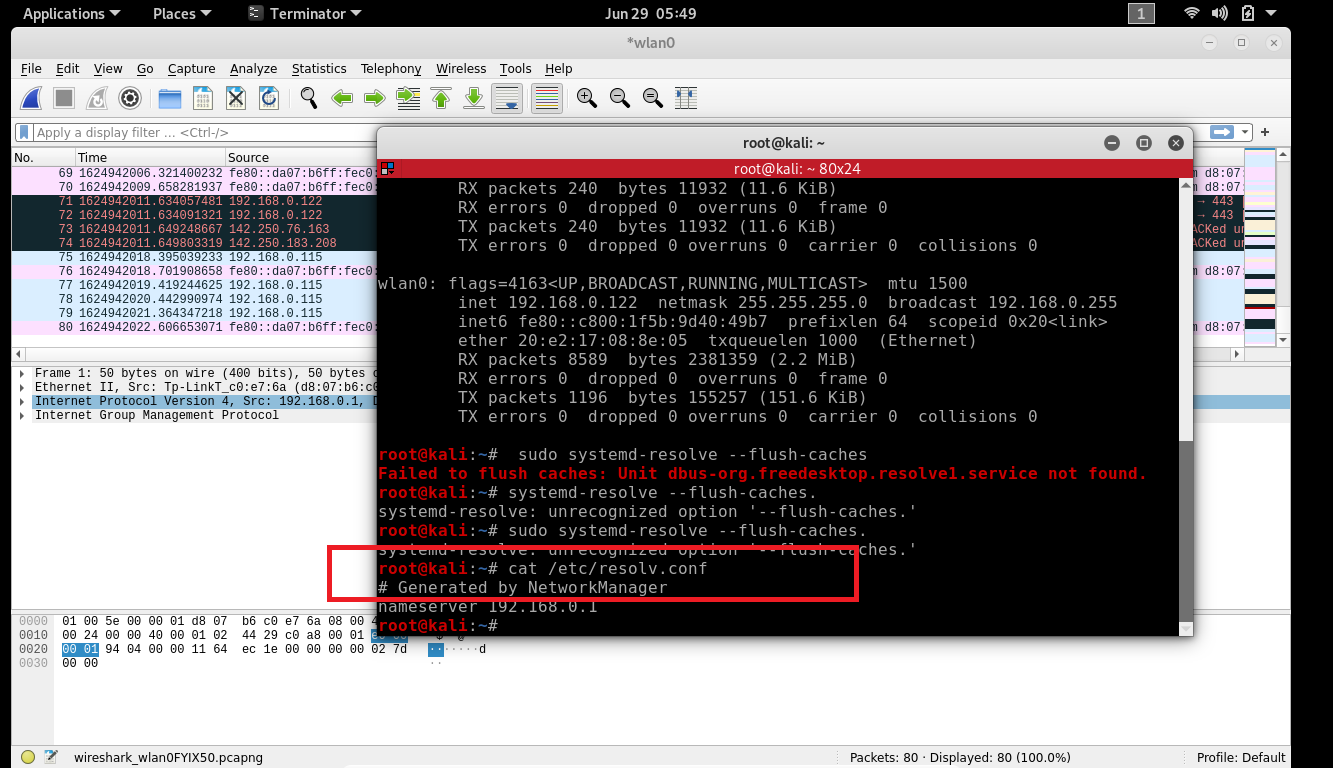
**after the prompt C:\> provide the following command:**

**ipconfig /displaydns**

**Each entry shows the remaining Time to Live (TTL) in seconds. To clear the cache, enter**

**ipconfig /flushdns**

**Flushing the DNS cache clears all entries and reloads the entries from the hosts file.**

****