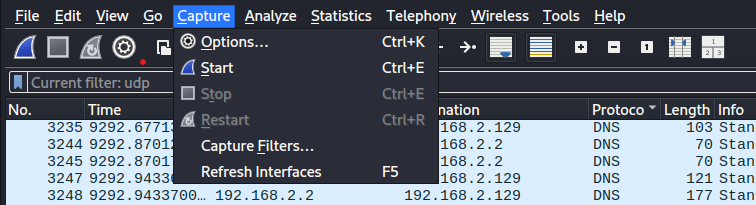
**Task 5-Capture and Analyze Network Traffic**

**1.Install Wireshark**

Already installed on the system.

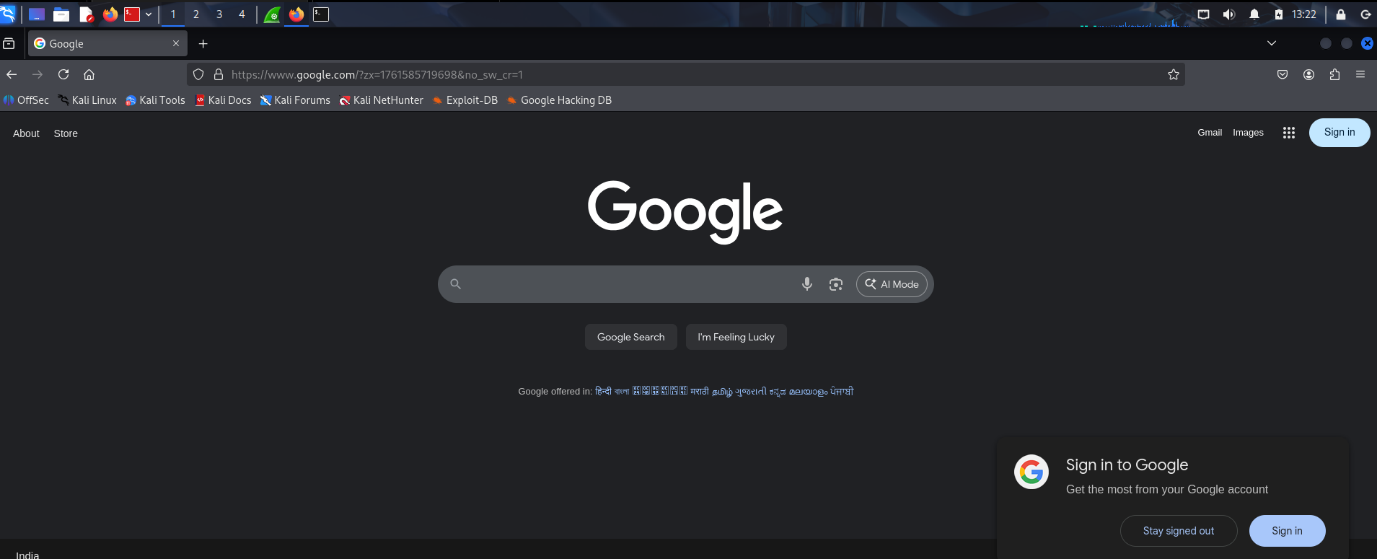
**2.Start capturing on your active network interface.**

* Capture->Start

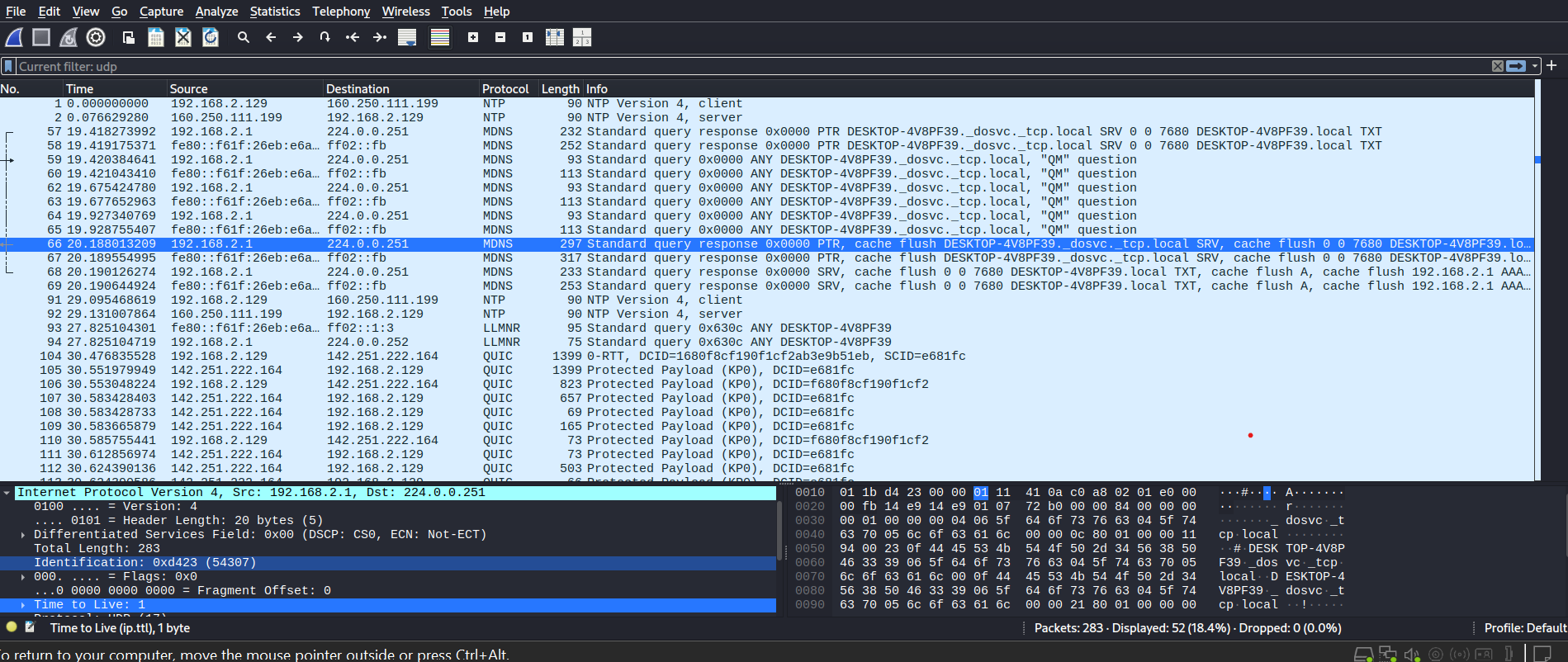


**3.Browse a website or ping a server to generate traffic.**

* <https://google.com>



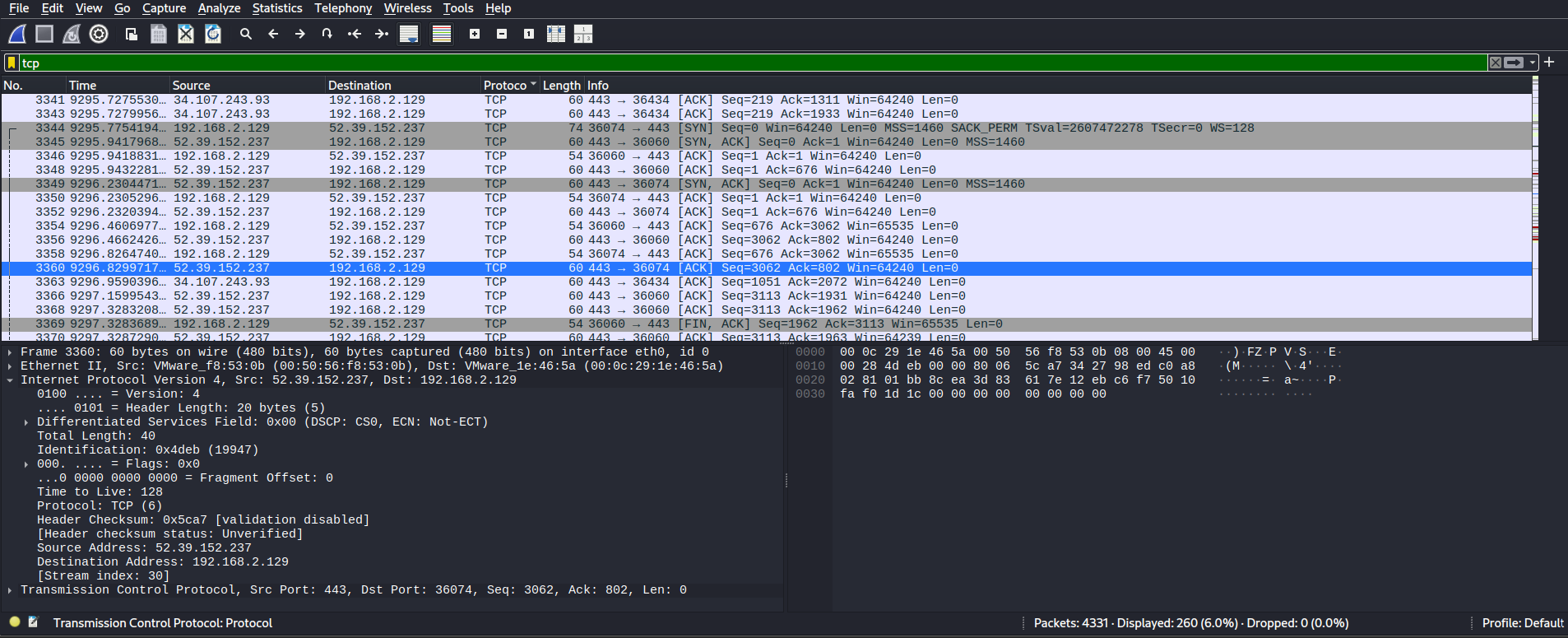
Captured packets generated by <https://google.com>.



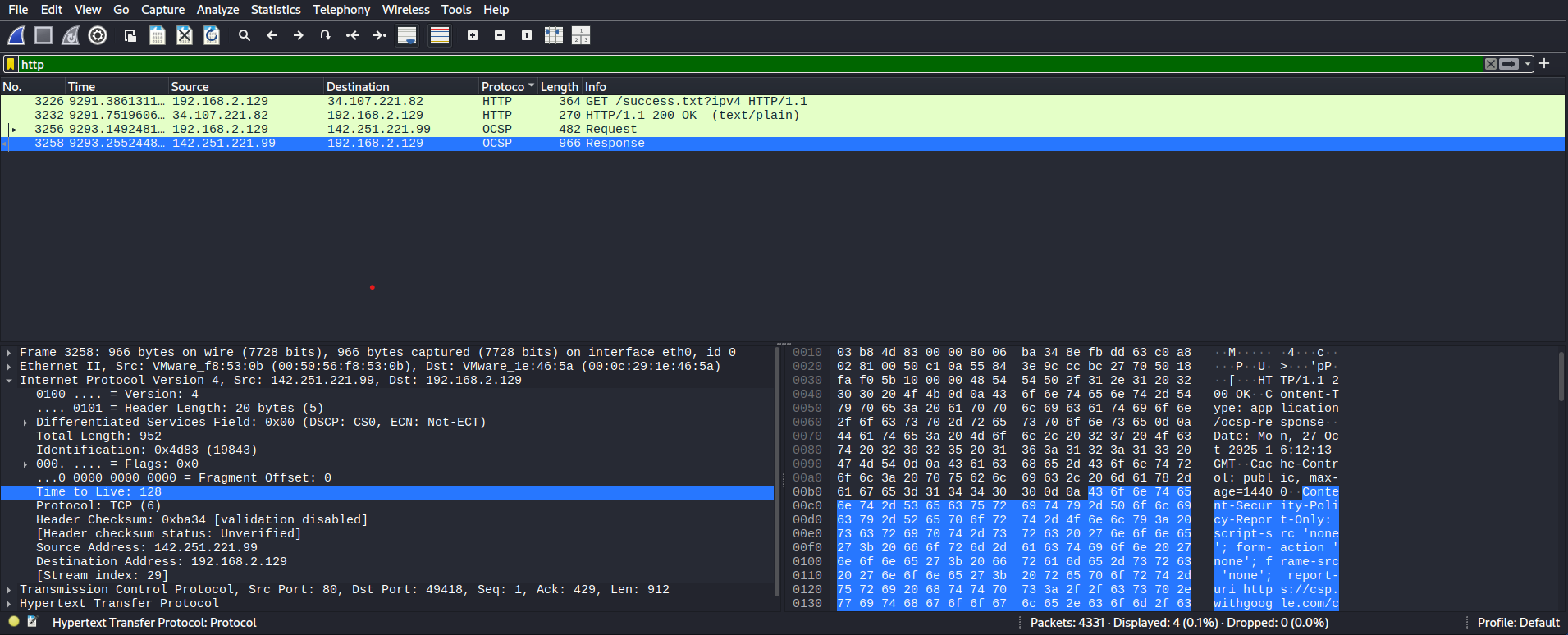
**4.Stop capture after a minute.**

**5.Filter captured packets by protocol(e.g., HTTP, DNS, TCP).**

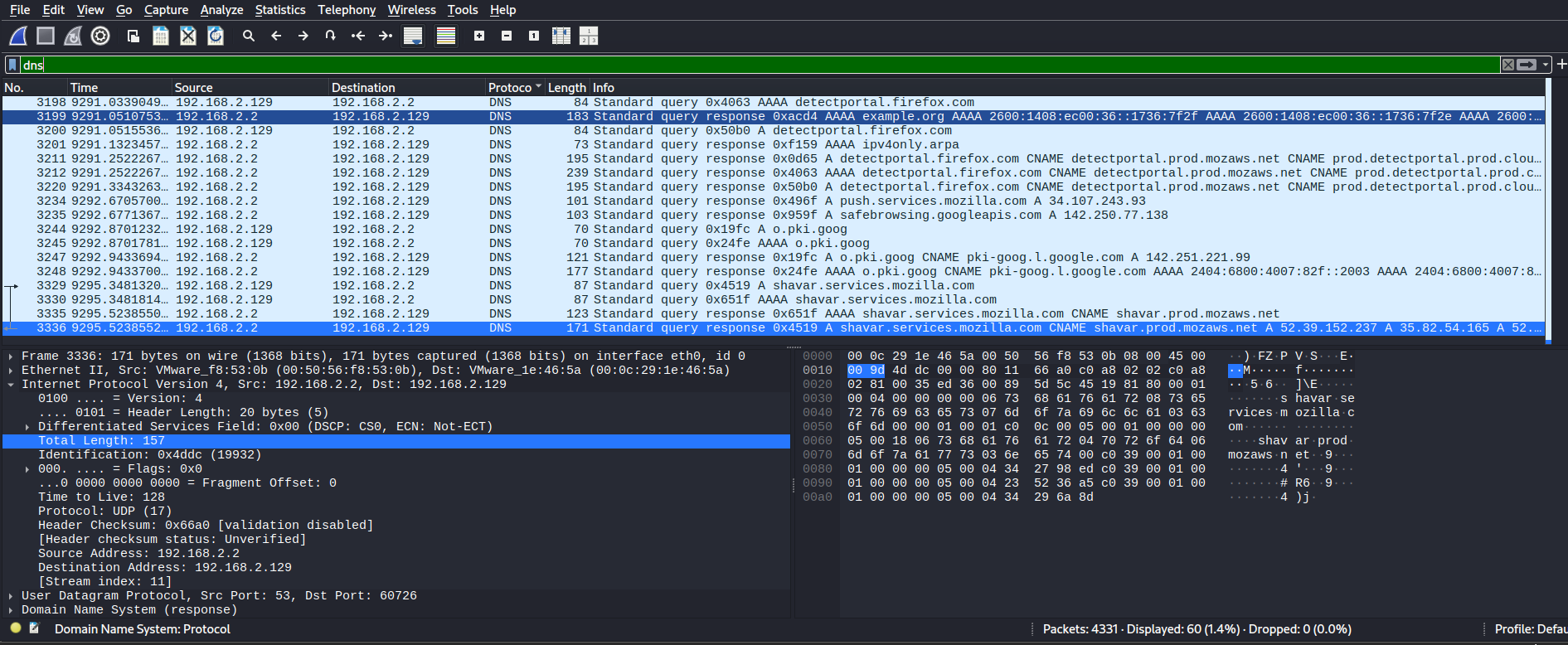
* tcp



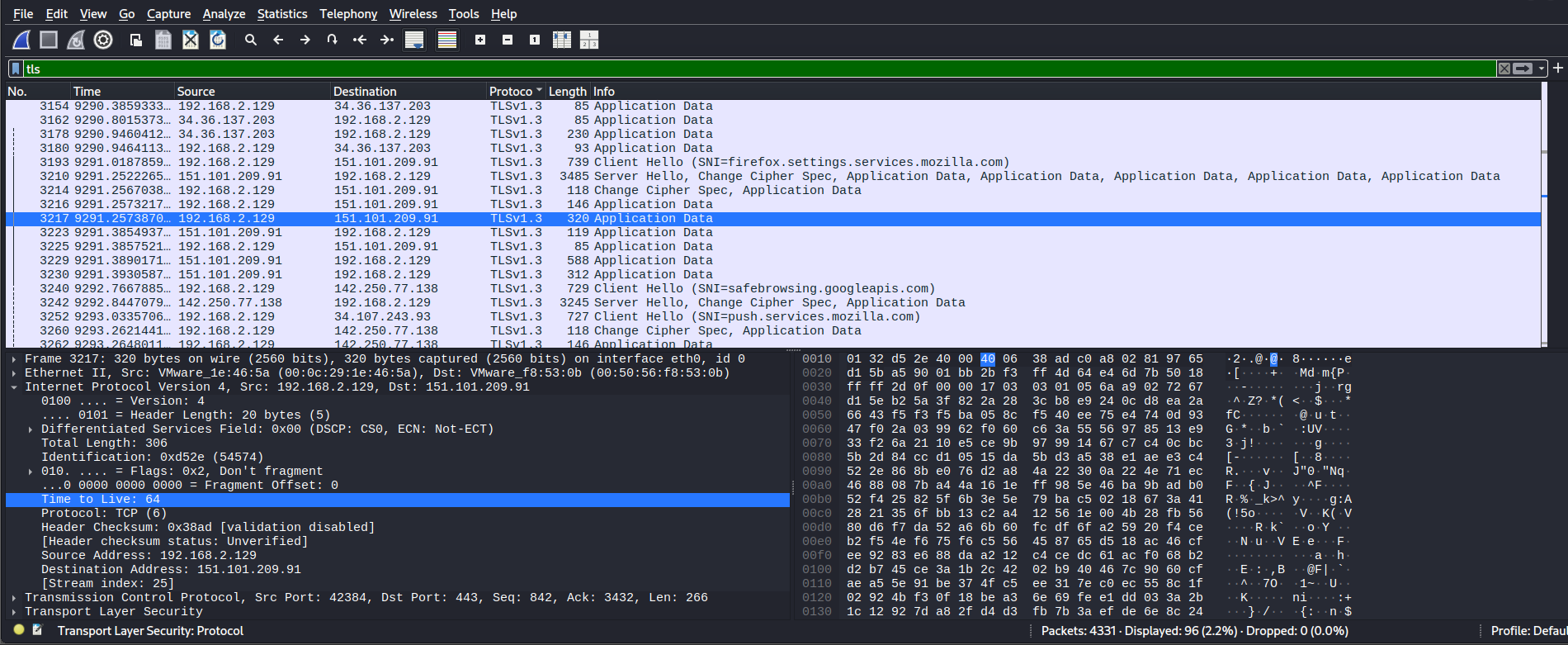
* http



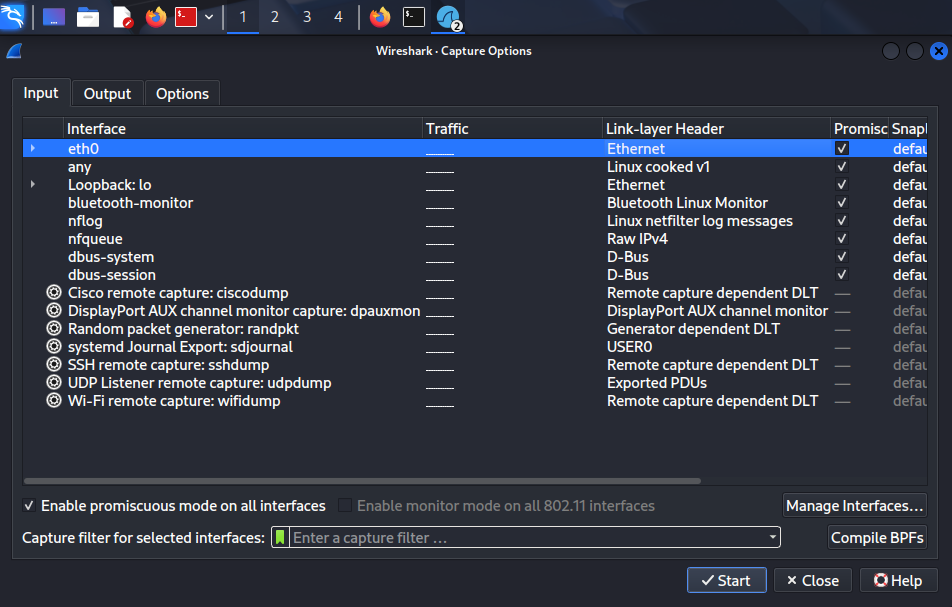
* dns



* tls



 **Interface:** eth0 (active network interface)



 **Protocols observed:**

** NTP –** Network Time Protocol

** MDNS –** Multicast DNS

** LLMNR –** Link-Local Multicast Name Resolution

** QUIC –** Quick UDP Internet Connections (encrypted HTTP/3 traffic)

 **Source / Destination:**

* 192.168.2.1 → 224.0.0.251 (Multicast, typical for MDNS)

 **Ports:** UDP 5353 → used by MDNS

**6.Identify atleast 3 different protocols.**

* NTP
* MDNS
* LLMNR
* QUIC