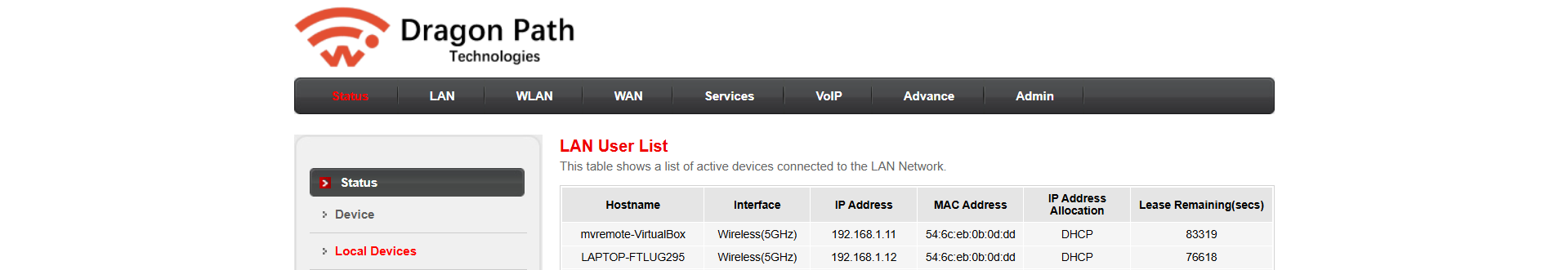
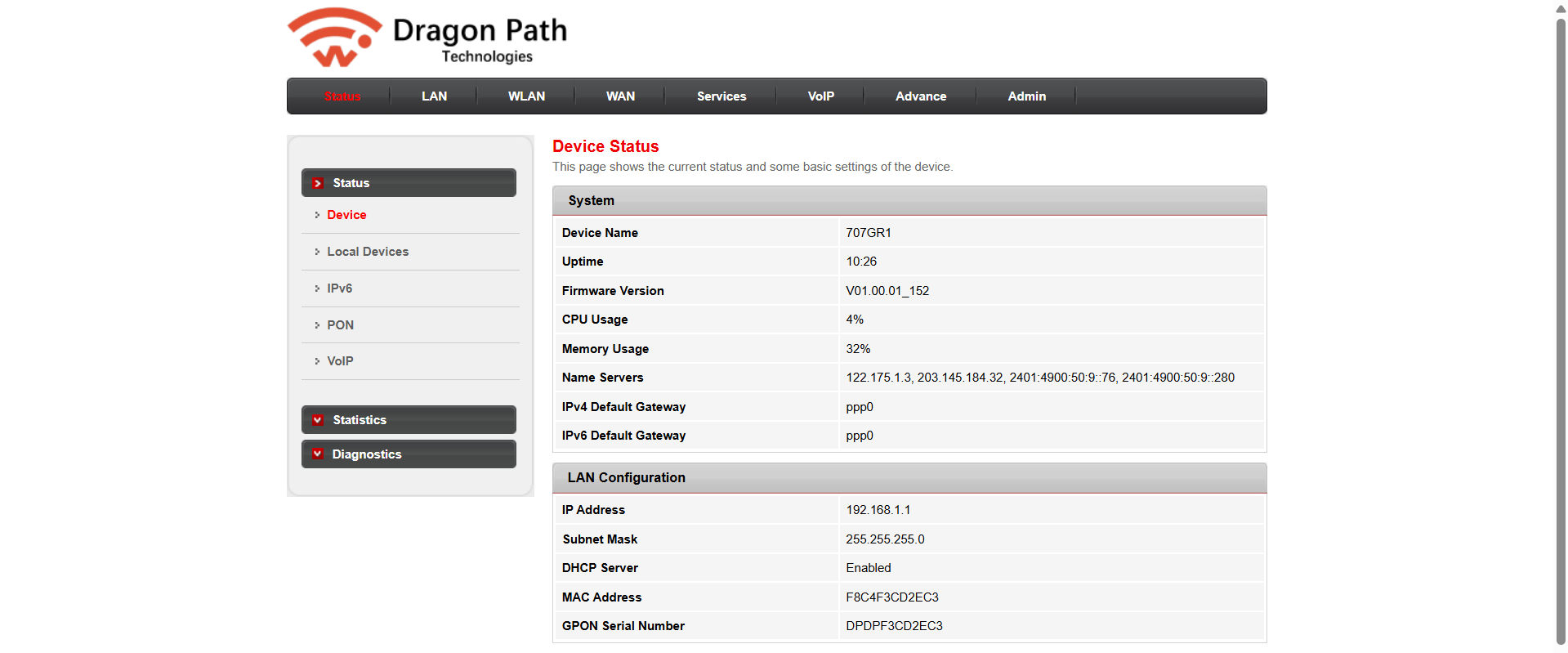
**Moulik Tammana**

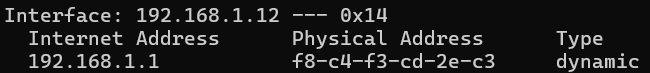
**Q1. Capture and analyse ARP packets using Wireshark. Inspect the ARP request and reply frames when your device attempts to find the router's MAC address. Discuss the importance of ARP in packet forwarding.**

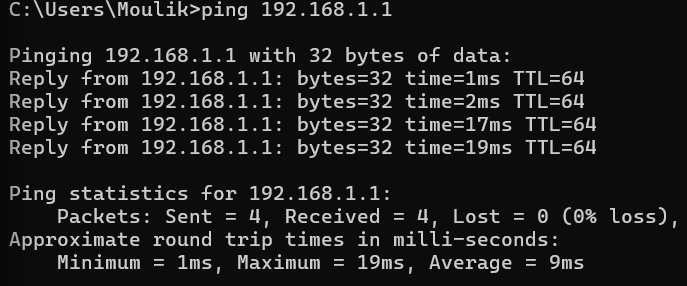
**So, when we type in our router IP in the web browser, we can access the router's web management interface which has all the information related to the router like the MAC address of the router, MAC and IP addresses of the devices connected to the router etc.**

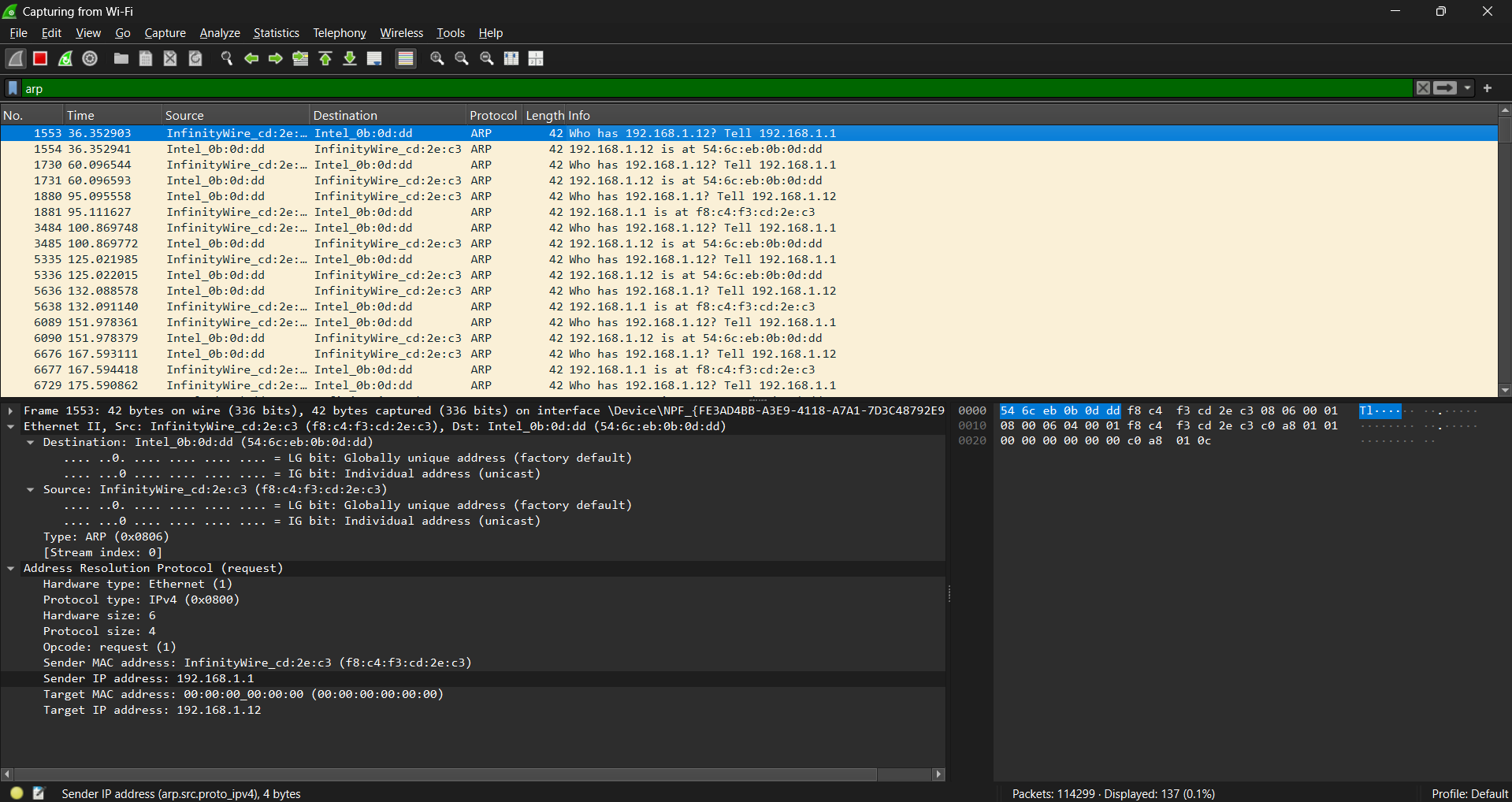
****

****

**The circled part indicates the MAC and IP address of the router.**

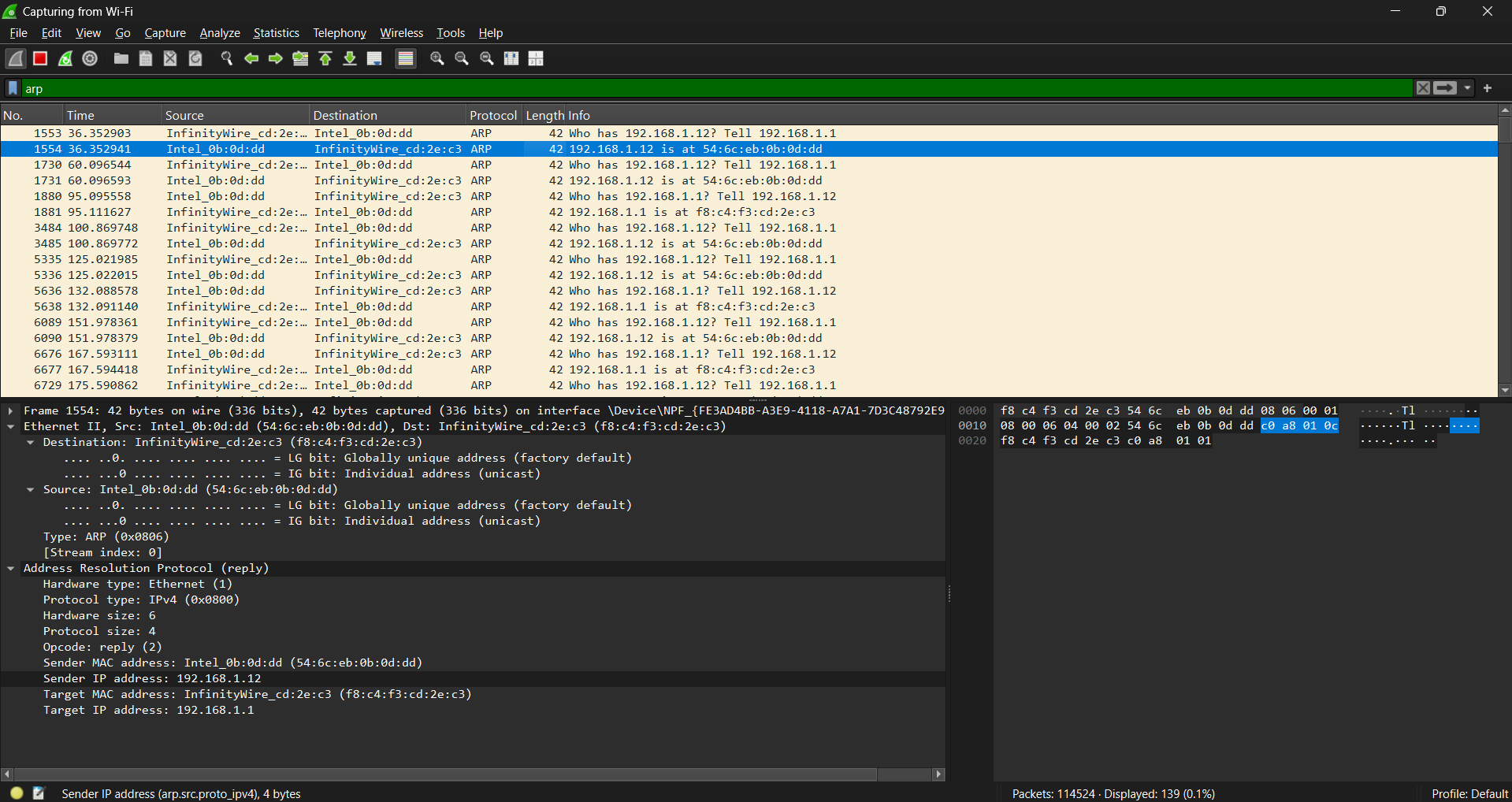
****

****

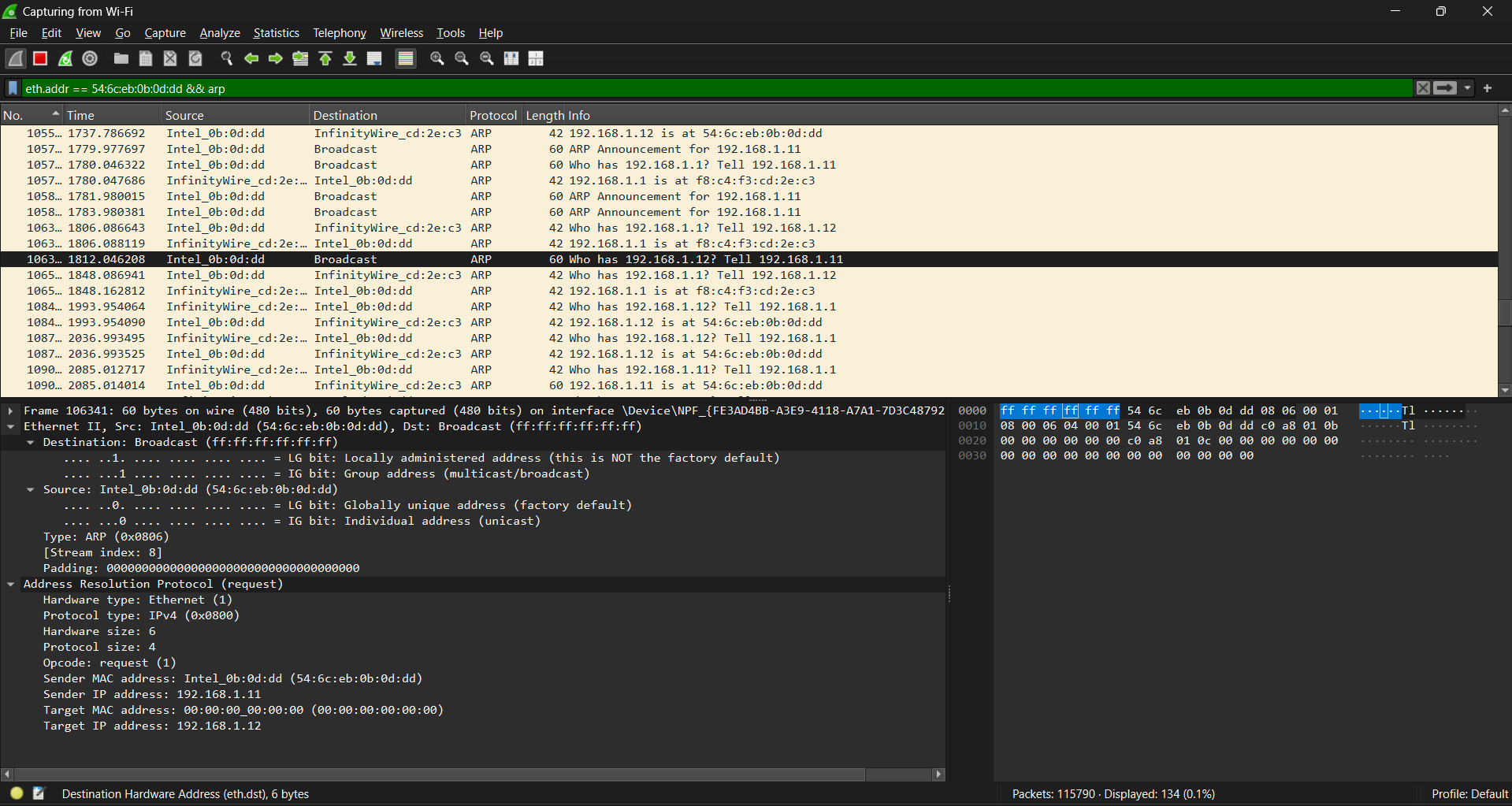
****

**Even though the Ethernet frame is being sent directly to your laptop (unicast), the ARP section still shows 00:00:00:00:00:00 as the Target MAC. This happens because the router is "double-checking" or "refreshing" its ARP table.**

* **Some devices re-validate MAC addresses periodically, even if they already have them cached.**
* **Your router may be verifying that 192.168.1.12 still belongs to the same MAC before sending further data.**

****

**But in other cases,**

****

**When broadcasting the ARP request to all devices in the network.**

* **If the sender doesn’t know the target’s MAC address, it sends the ARP request to everyone using FF:FF:FF:FF:FF:FF as the Ethernet Destination MAC.**
* **This ensures that the correct device will hear it and reply.**