

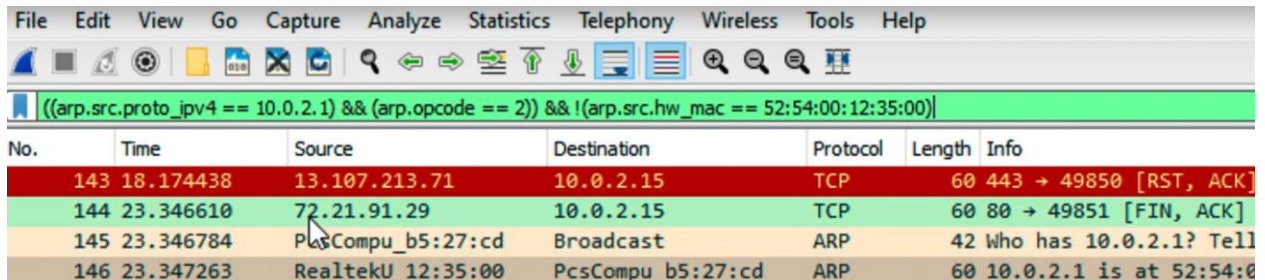
Wireshark - Anomaly Detection

Problem: analyze a suspicious situation comprising having two different ARP responses for a particular IP address.

Goal: Filter traffic to flag any ARPs coming from the gateway's IP address that are not the gateway's MAC address.

Process:

- Create profile for filtering ARP Anomaly Detection
- Right-click "Sender IP address" and select "Prepare as filter" and check "Selected"
- Right-click "Opcode" and select "Prepare as filter" and check "... and Selected"
- Identify a true response from the gateway and exclude that:
 - Right-click "Sender MAC address" and select "Prepare as filter" and check "... and not Selected"
- Filtered Result:



No.	Time	Source	Destination	Protocol	Length	Info
143	18.174438	13.107.213.71	10.0.2.15	TCP	60	443 → 49850 [RST, ACK]
144	23.346610	72.21.91.29	10.0.2.15	TCP	60	80 → 49851 [FIN, ACK]
145	23.346784	PlusCompu_b5:27:cd	Broadcast	ARP	42	Who has 10.0.2.1? Tell
146	23.347263	RealtekU 12:35:00	PcsCompu b5:27:cd	ARP	60	10.0.2.1 is at 52:54:0