

analysis_pcap_arp.py:

Libraries:

sys

dpkt

Requirements:

```
pip install dpkt
```

Usage:

Use command line arguments to query a domain:

```
python3 analysis_pcap_arp.py foo.pcap
```

Output of *analysis_pcap_arp.py*:

ARP REQUEST:

Hardware type: 1

Protocol type: 0x0800

Hardware size: 6

Protocol type: 4

Sender MAC address: 50:d4:f7:02:4f:8d

Sender IP address: 192.168.0.1

Target MAC address: 00:00:00:00:00:00

Target IP address: 192.168.0.196

ARP REPLY:

Hardware type: 1

Protocol type: 0x0800

Hardware size: 6

Protocol type: 4

Sender MAC address: 4c:cc:6a:0d:cb:e4

Sender IP address: 192.168.0.196

Target MAC address: 50:d4:f7:02:4f:8d

Target IP address: 192.168.0.1

(ii)

The ARP request from the router indicates that it is asking the LAN the MAC address of the device with local IP of 192.168.0.196 because the MAC address of the target IP address is empty..

The MAC address of the router is *50:d4:f7:02:4f:8d* and the IP address of the router is *192.168.0.1* based on the request and reply exchange between the router and the device.