Man In The Middle Attack(MITM)

COM 744

B00828528
Mathangi-V@ulster.ac.uk

Ulster University

Jordonstown

Msc Internet Of Things Full Time

Agenda :

- Introduction.
- Explanation of Methodology.
- Discussion of Results.

Introduction:

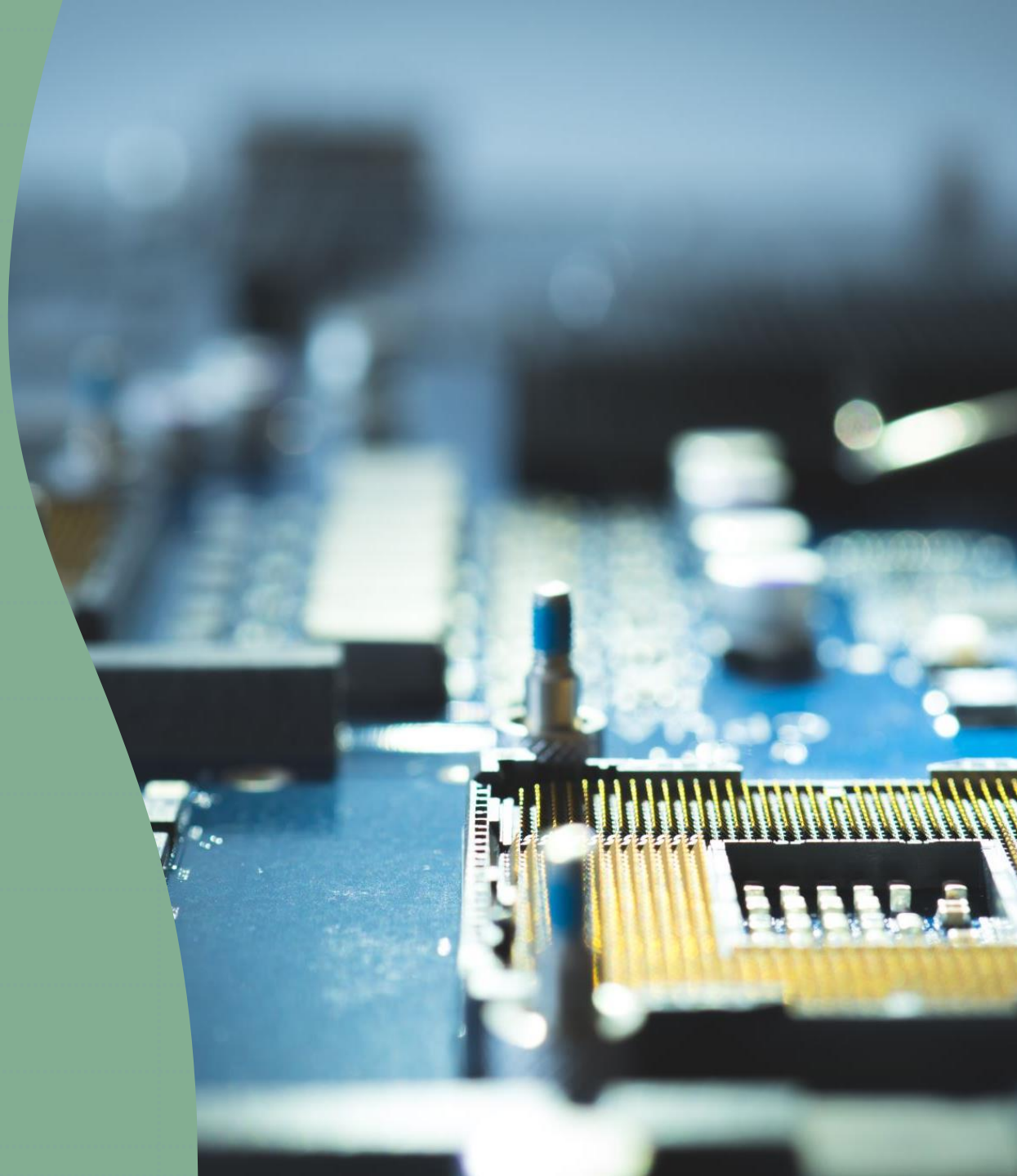
The Internet of Things (IoT) is the concept of connecting ordinary appliances, objects, and wearable gadgets to the Internet to allow data and information to be exchanged.

Raspberry pi:

The Raspberry Pi is a small, low-cost computer produced by the Raspberry Pi Foundation , a UK-based educational foundation dedicated to promote the use of Raspberry Pi in classrooms to enhance the educational experience in computer science. Students can use the Raspberry Pi to experiment with numerous facets of technology at a low cost. The Raspberry Pi may run a variety of Linux-based operating systems, although it usually comes pre-installed with the Raspbian OS, which is free software provided by the Raspberry Pi Foundation. The Raspberry Pi may be accessed remotely or linked to any device that has an HDMI connector.

. The Raspberry Pi 2 is an inexpensive device that can be used for a variety of projects including, but not limited to.

The overall goal of this project is to experience aspects of information security and by using the one of the best attack called Man In the middle (MITM)



MITM:
Man in the middle A Man-in-the-Middle assault occurs when an attacker inserts him/herself between two parties in communication. The two parties are completely oblivious of this and assume they are simply speaking with one another. The attacker must be on the same network as the targets in order to carry out this attack . It will be possible to collect various information once in between the victim and the router.

In short, by using the pi Linux based OS will continue the best attack . whereas using protocol and sniffing techniques and tools ,need to talk with host with the given IP addresses and it references the ARP cache to resolve the IP address to a MAC address. Hence attacker can sniff all the private traffic between hosts and the valuable information can be taken out from the traffic.

METHODOLOGY

PROTOCOL : The very common protocol for MITM is ARP(Address Resolution Protocol) Poisoning which is used to resolve IP addresses to physical MAC (media access control) addresses. An attacker posing as another host could use its own MAC address to respond to requests it shouldn't be responding to. An attacker can sniff the private traffic between two hosts with a few carefully crafted packets. The attacker can extract valuable information from the traffic, such as the exchange of session tokens, giving them full access to application accounts that they shouldn't have.

As per the project requirement need to use or install the Nmap , Ettercap and Wireshark for attacking the victim . Let us see what these tools can do.

N-MAP: Nmap lets you scan your network for not only everything that's connected to it, but also a wealth of information about what's connected, what services each host is providing, and so on. It supports many scanning methods, including UDP, TCP connect (), TCP SYN (half-open), and FTP.

Ettercap: Ettercap is an all-in-one solution for man-in-the-middle assaults. It has live connection sniffing, on-the-fly content screening, and many other cool features. It can dissect numerous protocols both actively and passively, and it has a lot of capabilities for network and host investigation.

In this project ,Ettercap application not used .all we need is simple command by installing all the tools and wireshark.

Now let us try and install the following tools by using commands.

For Wireshark,
‘sudo apt install wireshark’

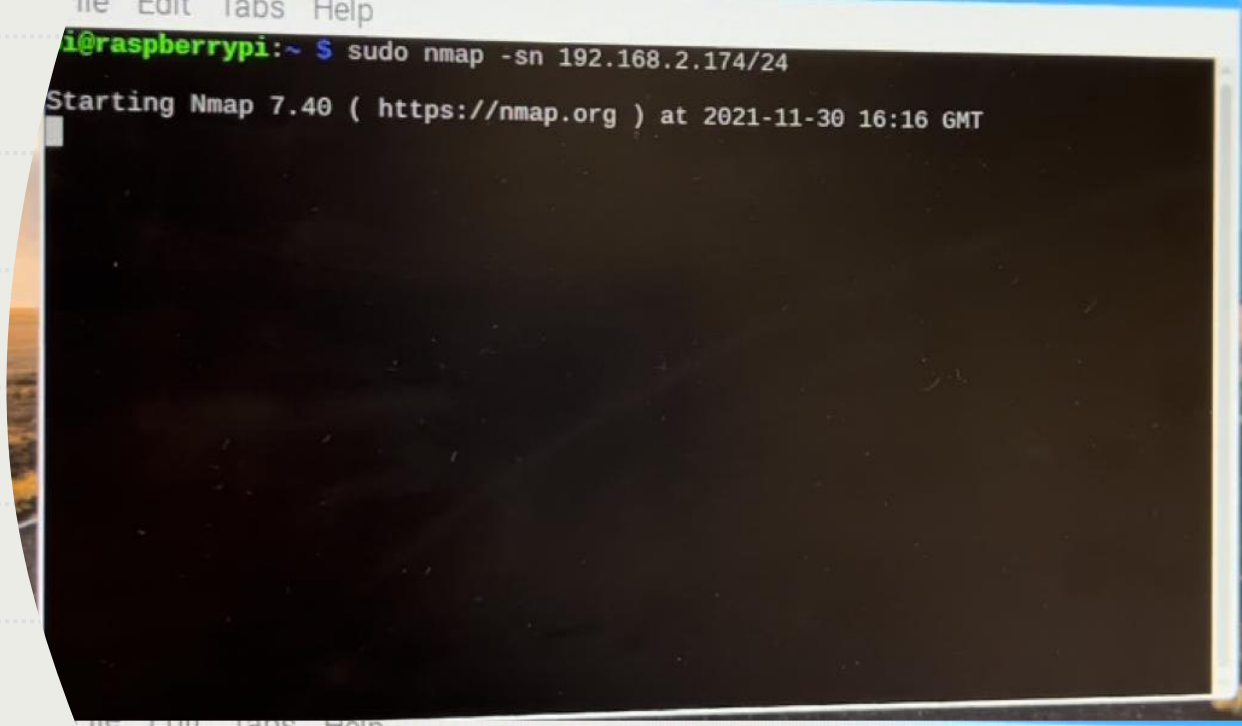
for nmap,
‘sudo apt install nmap’

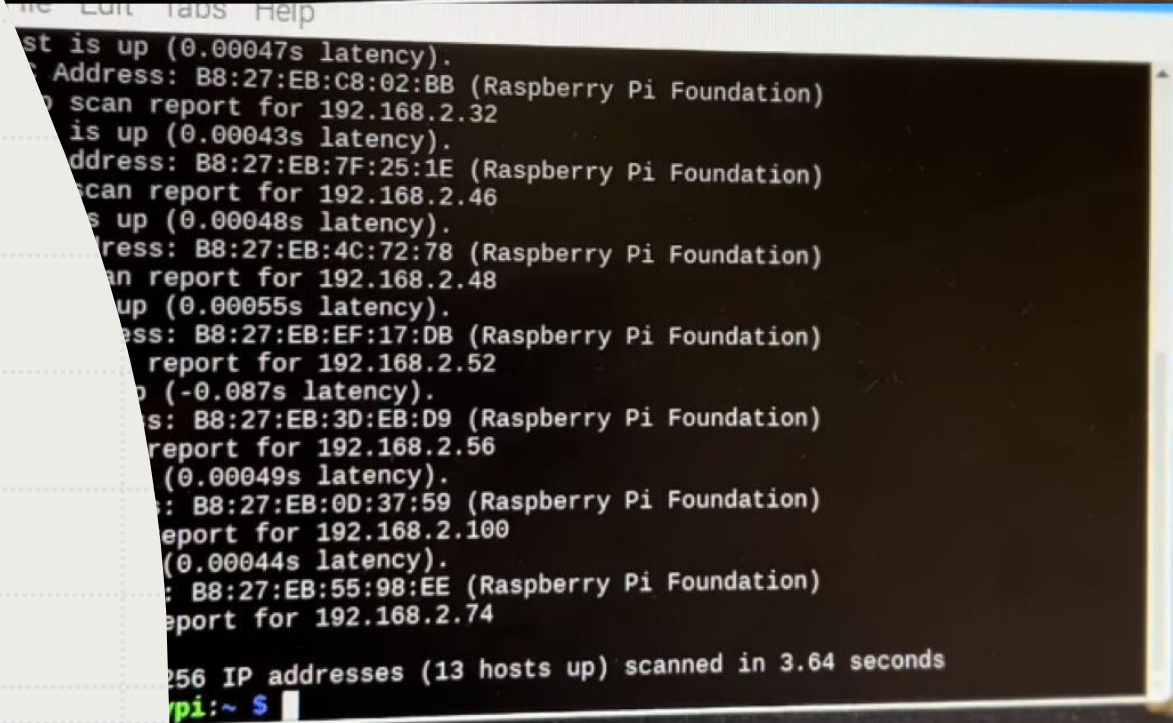
for Ettercap
‘sudo apt install Ettercap-text-only’.

Well by using the Nmap command with our IP address (192.168.2.74/24), it starts scanning all the hosts which are connected to the same network.

Another snip shows the scanned hosts which are nearby .so I have targetted the one of my friends PI which has IP address of 192.168.2.46 and MAC address is B8:27:EB:7F:25:1E .

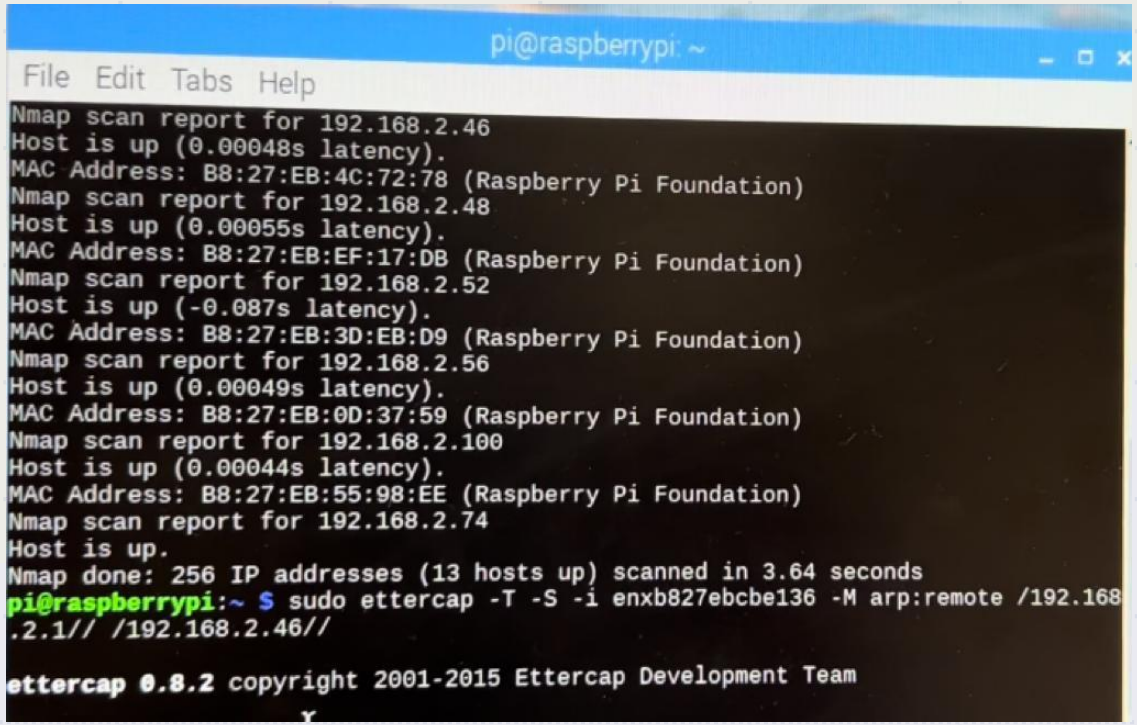
Or else I can attack anyone from the scanned 13 hosts. But I choose one particular IP.

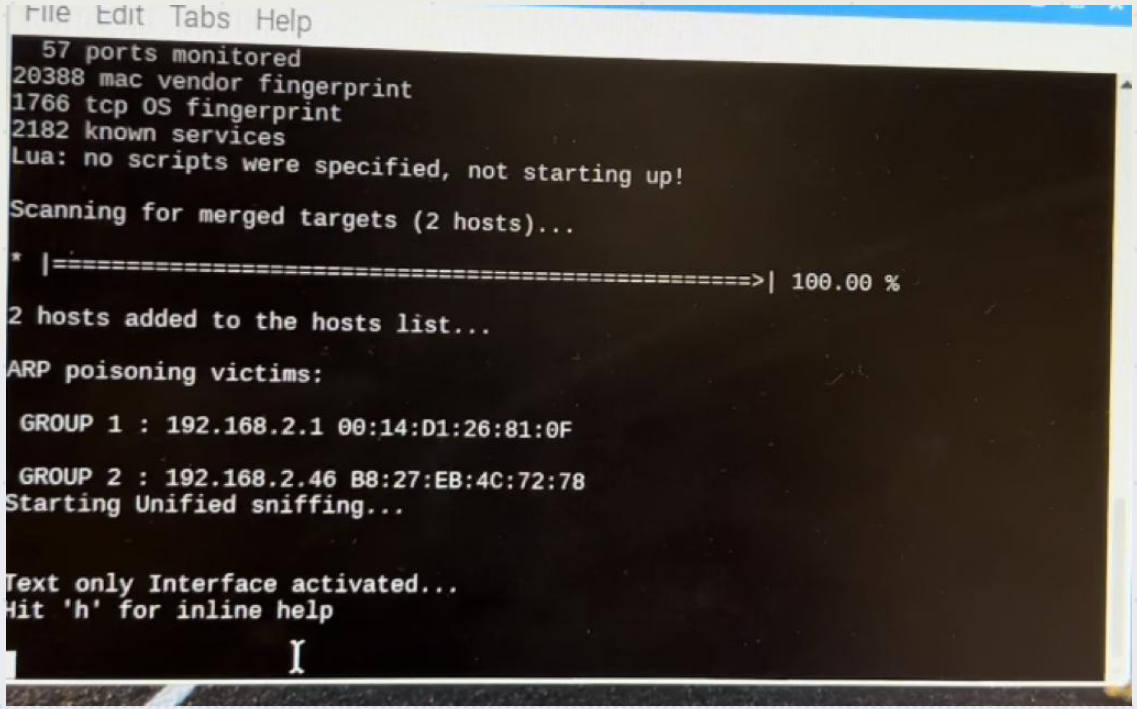




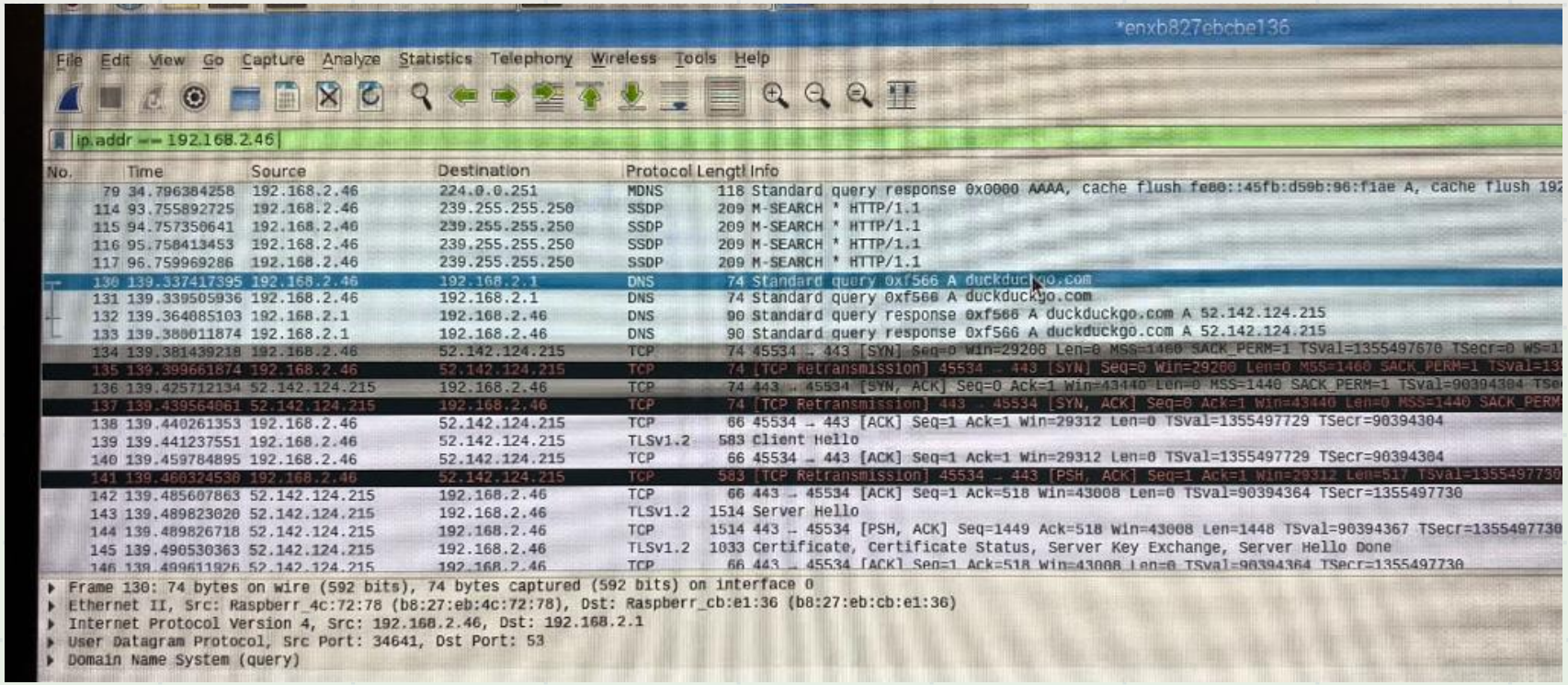
Now by using the simple following command ‘sudo Ettercap –T –S –i (interface) –M arp : remote /192.168.2.1// /192.168.2.46// ’ .so that no need to open Ettercap . Gateway IP address and the Victims IP address is given

Secondly, it starts ARP poisoning targets which is given in the command and sniffing .





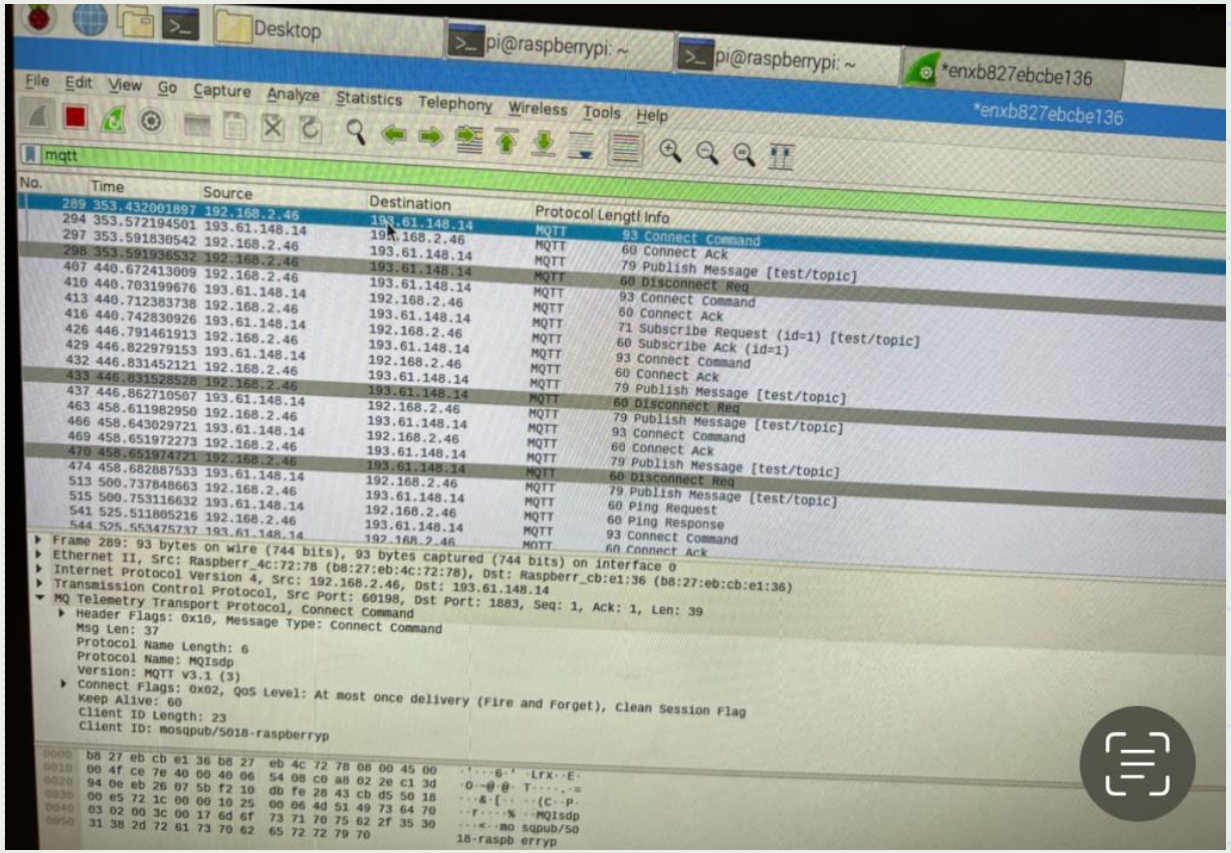
Through wireshark data is captured and poisioned the victims IP.as in image clearly evidents that victim is browing the duck duckgo.com



Here comes the interesting part that victims mqtt protocol , who is already poisoned.

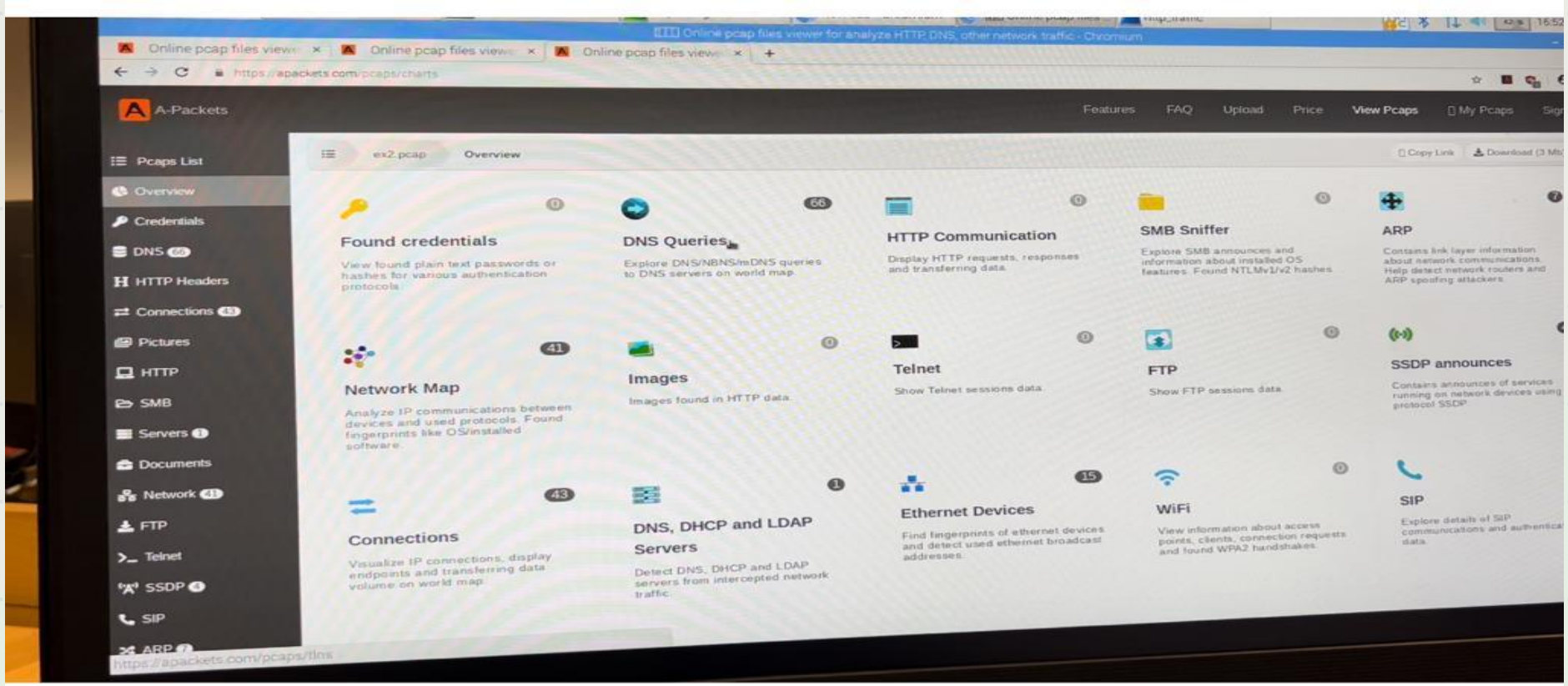
In screenshots it is clearly evident that one is victim and another is attacker.
So I poisoned both victim and another attacker.

At last captured all the data and saved as a Pcap file.

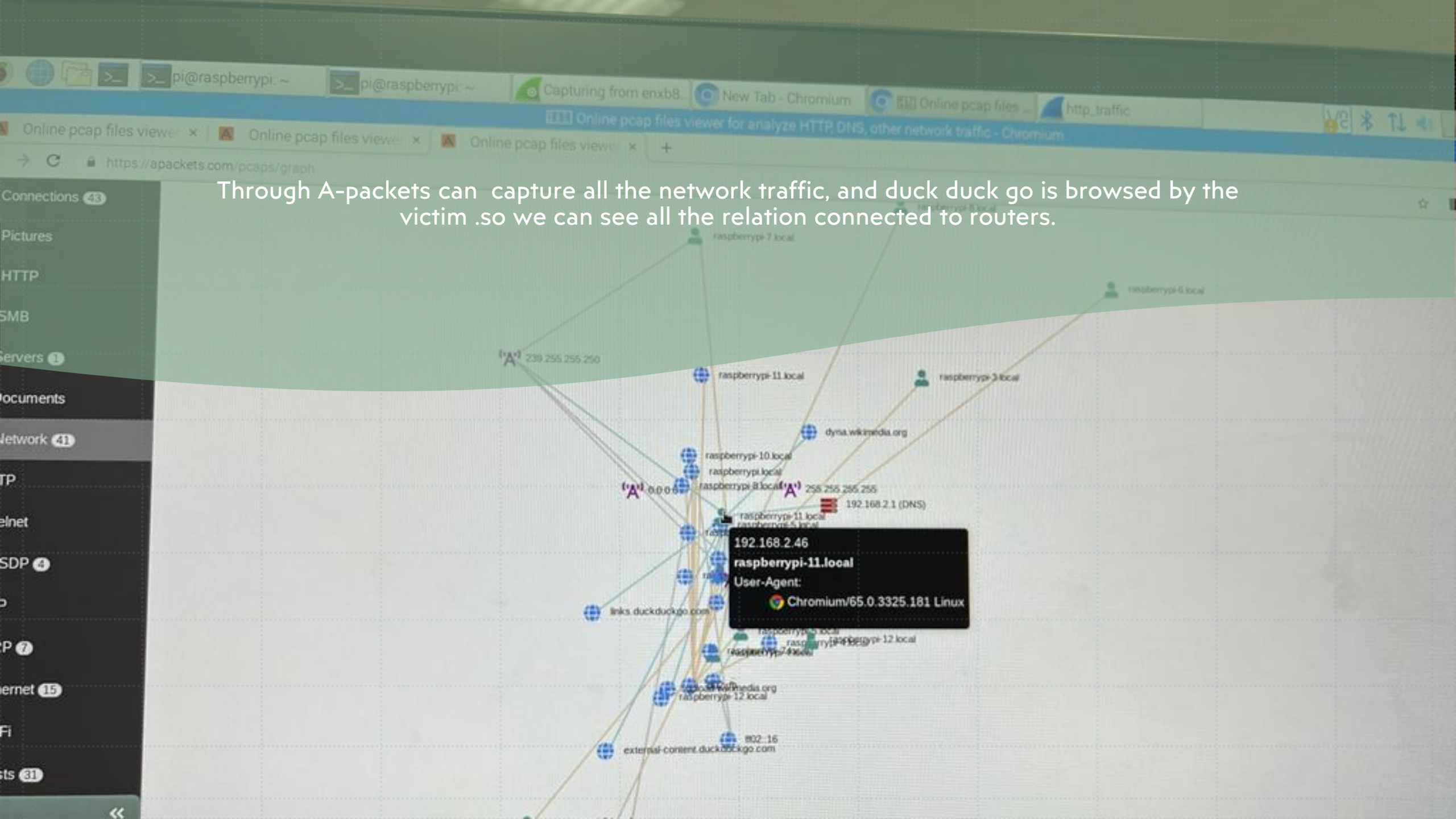


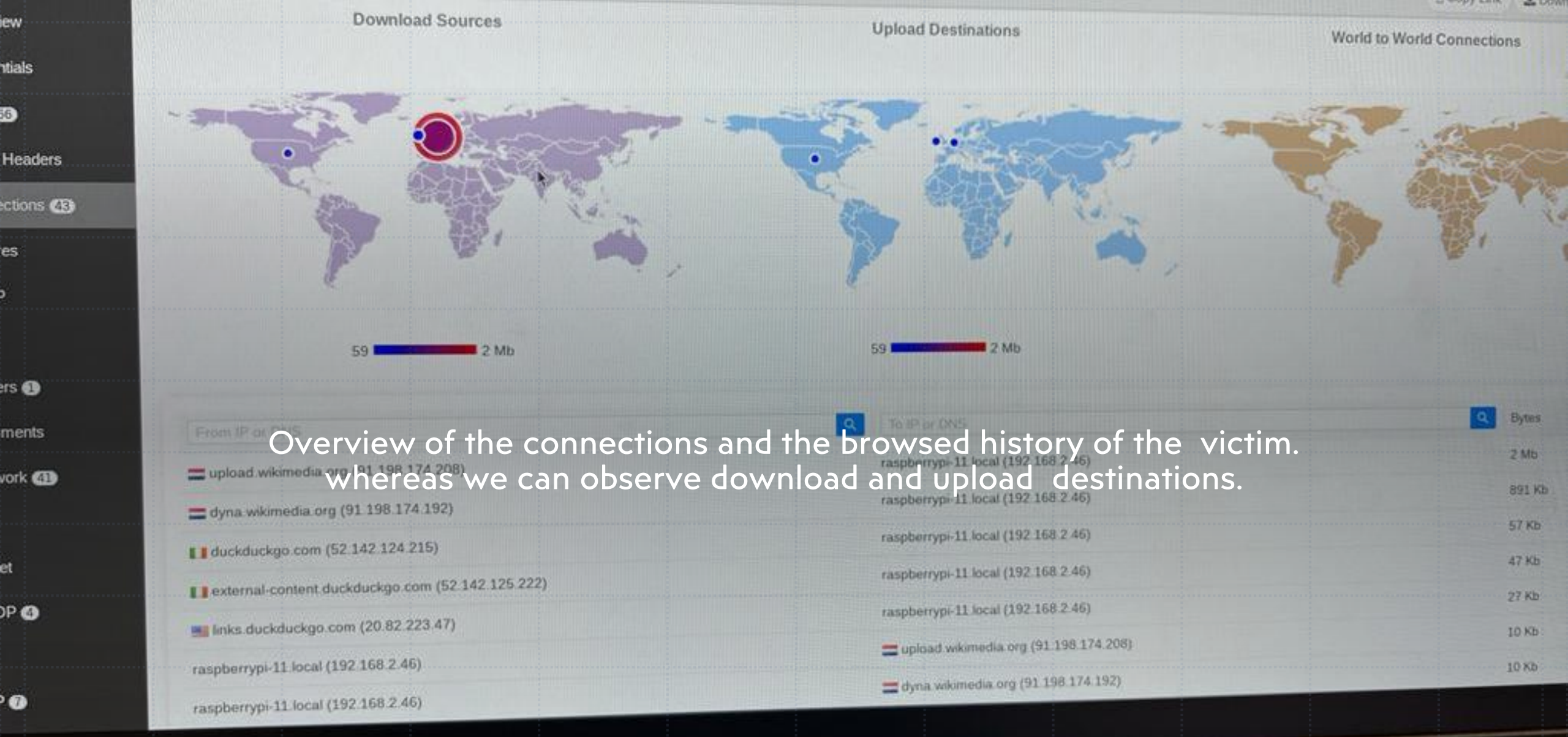
RESULTS :

After saving the file into Pcap .furthermore I choose to give a brief analysis of the captured data with DNS, ARP and it divides each part of protocols .



Through A-packets can capture all the network traffic, and duck duck go is browsed by the victim .so we can see all the relation connected to routers.





Overview of the connections and the browsed history of the victim. whereas we can observe download and upload destinations.

https://apackets.com/pcaps/dns

		raspberrypi-13.local _ftp._tcp.local _nfs._tcp.local _afpovertcp._tcp.local _smb._tcp.local _sftp-ssh._tcp.local _webdavs._tcp.local _webdav._tcp.local
raspberrypi.local (192.168.2.38)	224.0.0.251	0.0.f.a.0.2.6.f.4.1.1.9.7.a.1.e.0.0.0.0.0.0.0.0.0.0.0.0.0.0.8.e.f.ip6.arpa raspberrypi.local 38.2.168.192.in-addr.arpa
raspberrypi-11.local (192.168.2.46)	192.168.2.1	duckduckgo.com links.duckduckgo.com external-content.duckduckgo.com en.wikipedia.org upload.wikimedia.org login.wikimedia.org meta.wikimedia.org
raspberrypi-6.local (fe80::851e:bafb:ec0b:35e0)	ff02::fb	_ftp._tcp.local _nfs._tcp.local _afpovertcp._tcp.local _smb._tcp.local _sftp-ssh._tcp.local _webdavs._tcp.local

This is another evidence of the (192.168.2.46) victims DNS ,which is duck duck go

Conclusion:

Man in the Middle is one of the classic hacking attacks. It has many varieties, but on a local area network (LAN) , ARP poisoning is one of the favorite. In this way, the attacker has total access to all packet traffic and can thereby read and alter the traffic . Well by capturing all the victims data and analyzed through the Wireshark .in addition ,A-packets are used to study the complete analysis one by one connections protocols such as DNS, http, MQtt etc.

Thank you

Vineeth Mathangi (B00828528)