EXPLORING THE MAN-IN-THE-MIDDLE PROXY SETUP ON RASPBERRY PI 3:

A TECHNICAL ANALYSIS

Project Authors:
Corey Valentine Jr
Lead Researcher

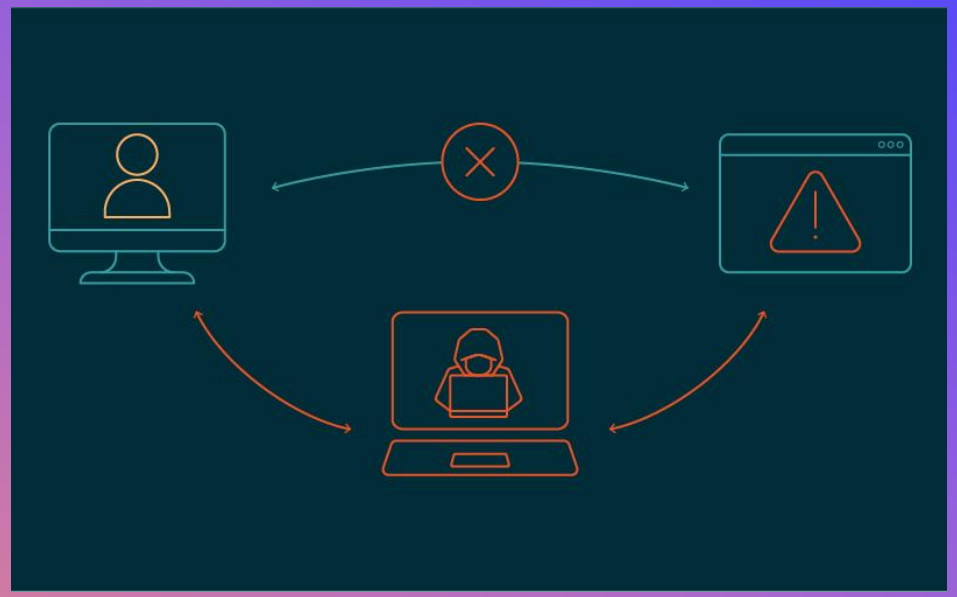
Courtney Malone
Data Analyst

Jake Black
Project Coordinator

Colorado State University 2024

INTRODUCTION

In today's digital landscape, cybersecurity is crucial, with Man-in-the-Middle (MitM) attacks posing significant threats. These attacks intercept communication, enabling eavesdropping and data tampering. Understanding MitM mechanisms is vital for effective defense strategies.



PROBLEM CHARACTERIZATION

MitM attacks exploit communication vulnerabilities, risking data confidentiality, integrity, and authenticity. Traditional encryption mitigates risks but isn't foolproof. Sophisticated MitM proxies can circumvent encryption, necessitating a deep understanding of networking protocols and encryption mechanisms.

PROPOSED SOLUTION AND IMPLEMENTATION STRATEGY

Methodology:

1. Configuring Raspberry Pi as Wireless Access Point.
2. Deploying Mitmproxy.
3. Redirecting Traffic.
4. Intercepting and Analyzing Traffic.

Description of Work:

Meticulously followed steps from Fizzotti's blog and Adafruit tutorial.

Conducted independent research to deepen understanding.

Spent considerable time troubleshooting.

LIBRARIES AND TOOLS USED

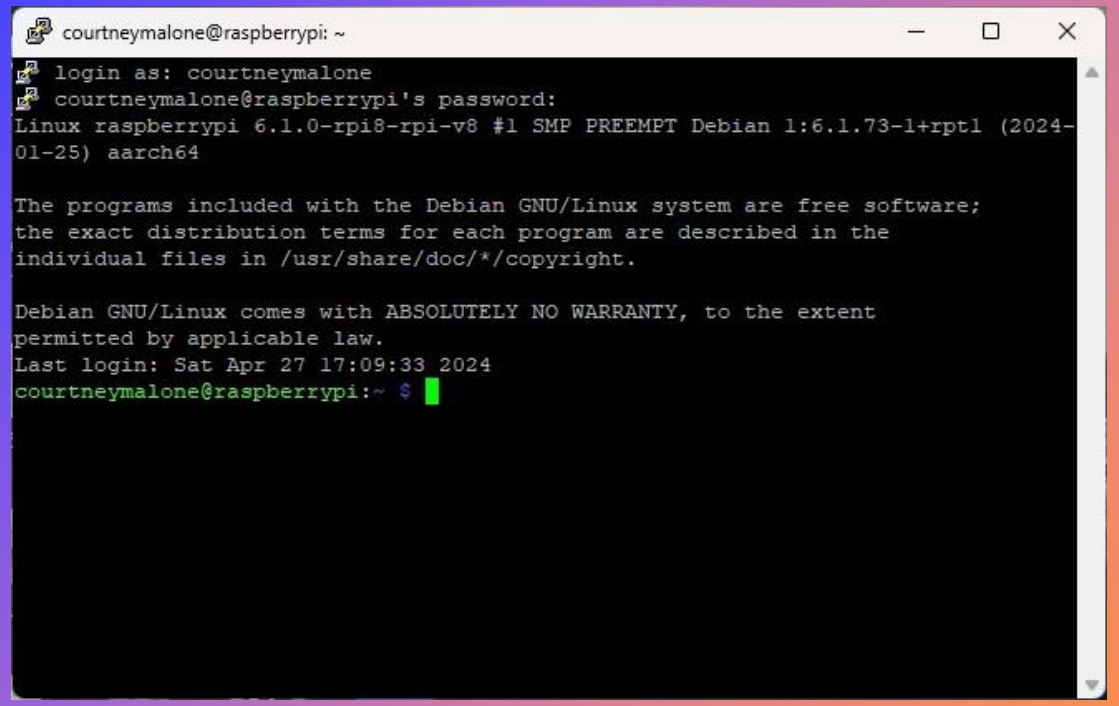
Hostapd and Dnsmasq/isc-dhcp-server: Configuring Raspberry Pi as a wireless access point.

Mitmproxy: Deployed as MitM proxy for intercepting and analyzing network traffic.

Iptables: Redirecting traffic to MitM proxy and enforcing network interception rules.

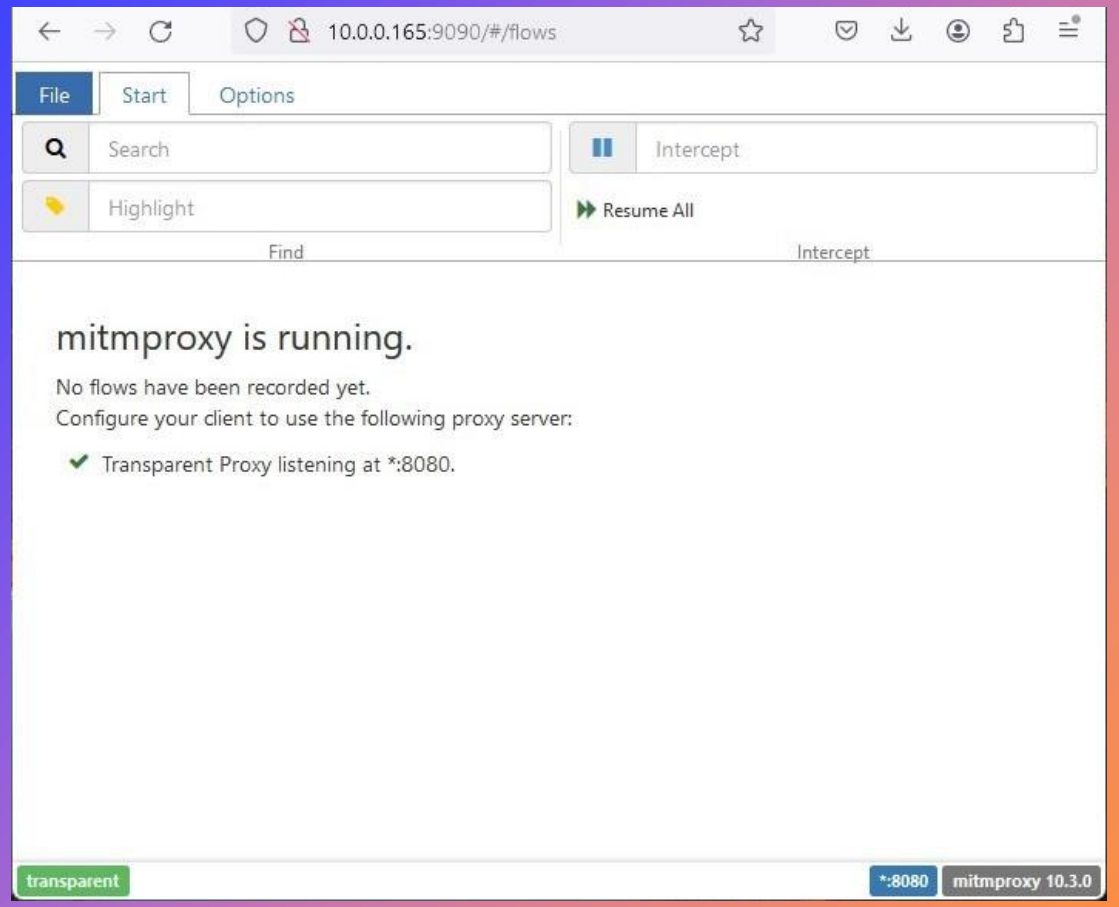
CONFIGURING RASPBERRY PI AS WIRELESS ACCESS POINT.

We follow the instructions provided in both the Adafruit tutorial and Fizzotti's article to set up the Raspberry Pi as a Wi-Fi access point using hostapd and dnsmasq or isc-dhcp-server. This allows the Raspberry Pi to serve as a gateway for client devices, facilitating network interception. We do this by SSH into the raspberry pi remotely and follow a series of steps.



DEPLOYING MITMPROXY

Building upon the foundation laid by the Adafruit tutorial, we install and configure mitmproxy on the Raspberry Pi. Mitmproxy serves as the core component of our MitM proxy, enabling us to intercept, inspect, and manipulate HTTP and HTTPS traffic passing through the Raspberry Pi.



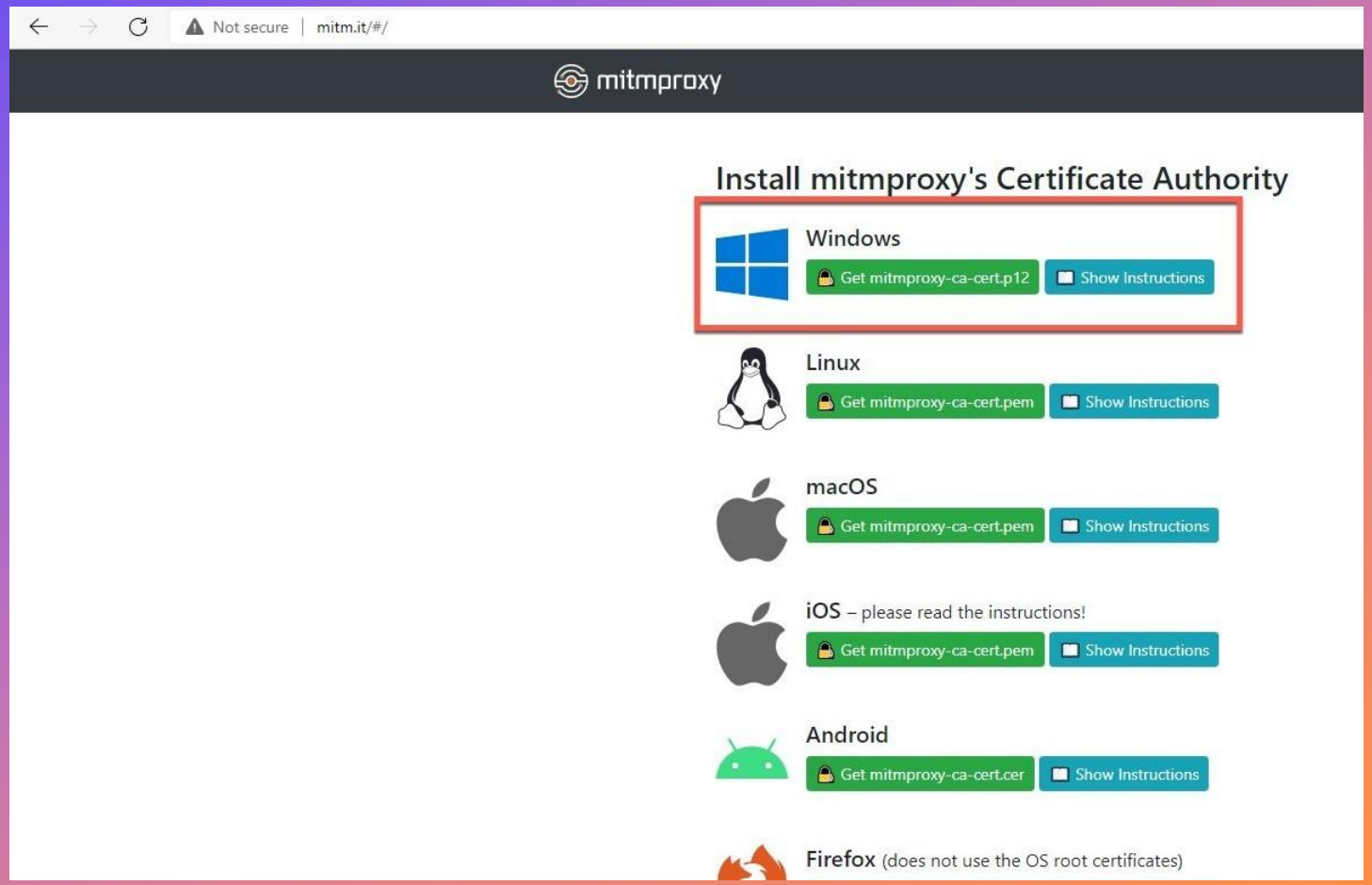
REDIRECTING TRAFFIC

Using iptables, we redirect traffic from client devices to the MitM proxy running on the Raspberry Pi. This ensures that all communication passing through the Raspberry Pi is intercepted and routed through the MitM proxy for analysis.

courtneymalone@raspberrypi: ~

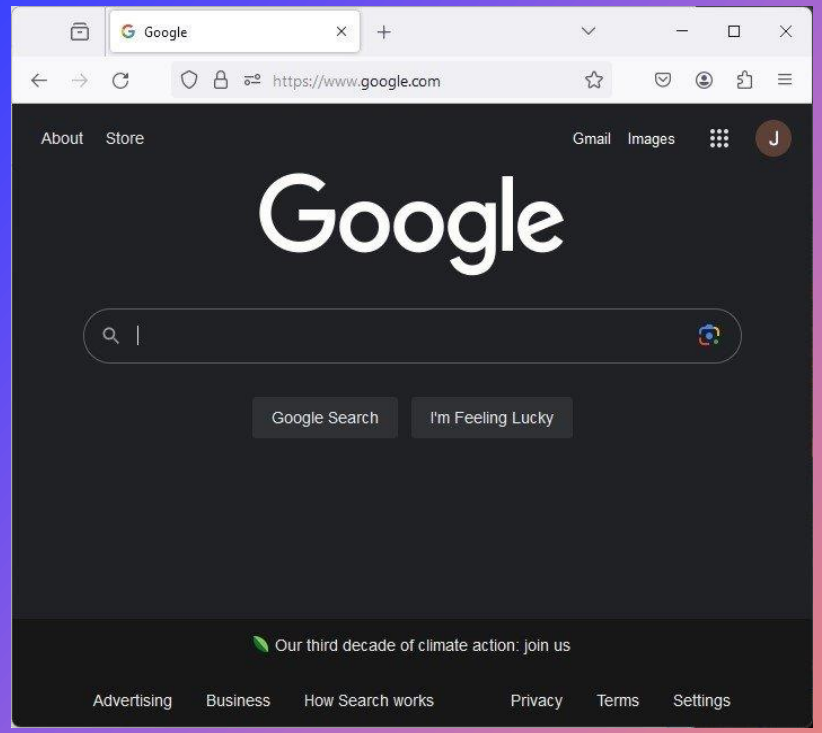
```
courtneymalone@raspberrypi:~ $ sudo nano /etc/rc.local
courtneymalone@raspberrypi:~ $ sudo sysctl -w net.ipv4.ip_forward=1
net.ipv4.ip_forward = 1
courtneymalone@raspberrypi:~ $ sudo nano /etc/sysctl.conf
  GNU nano 7.2                                        /etc/sysctl.conf *
#
# /etc/sysctl.conf - Configuration file for setting system variables
# See /etc/sysctl.d/ for additional system variables.
# See sysctl.conf (5) for information.
#

#kernel.domainname = example.com

# Uncomment the following to stop low-level messages on console
#kernel.printk = 3 4 1 3

###################################################################
# Functions previously found in netbase
#

# Uncomment the next two lines to enable Spoof protection (reverse-path filter)
# Turn on Source Address Verification in all interfaces to
# prevent some spoofing attacks
#net.ipv4.conf.default.rp_filter=1
#net.ipv4.conf.all.rp_filter=1

# Uncomment the next line to enable TCP/IP SYN cookies
# See http://lwn.net/Articles/277146/
# Note: This may impact IPv6 TCP sessions too
#net.ipv4.tcp_syncookies=1

# Uncomment the next line to enable packet forwarding for IPv4
net.ipv4.ip_forward=1

# Uncomment the next line to enable packet forwarding for IPv6
#  Enabling this option disables Stateless Address Autoconfiguration
#  based on Router Advertisements for this host
#net.ipv6.conf.all.forwarding=1
```

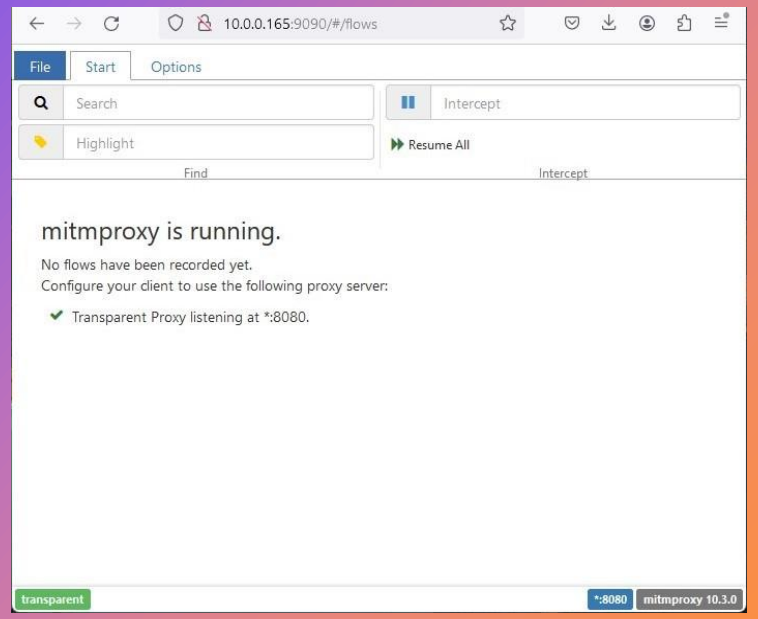

Wi-Fi
fakeap
No internet, secured
Disconnect
Shechefe
Chicago
Familyhousehold
More Wi-Fi settings


Not secure | mitm.it/#/
mitmproxy
Install mitmproxy's Certificate Authority
Windows
Get mitmproxy-ca-cert.p12
Show Instructions
Linux
Get mitmproxy-ca-cert.pem
Show Instructions
macOS
Get mitmproxy-ca-cert.pem
Show Instructions
iOS – please read the instructions!
Get mitmproxy-ca-cert.pem
Show Instructions
Android
Get mitmproxy-ca-cert.cer
Show Instructions
Firefox (does not use the OS root certificates)

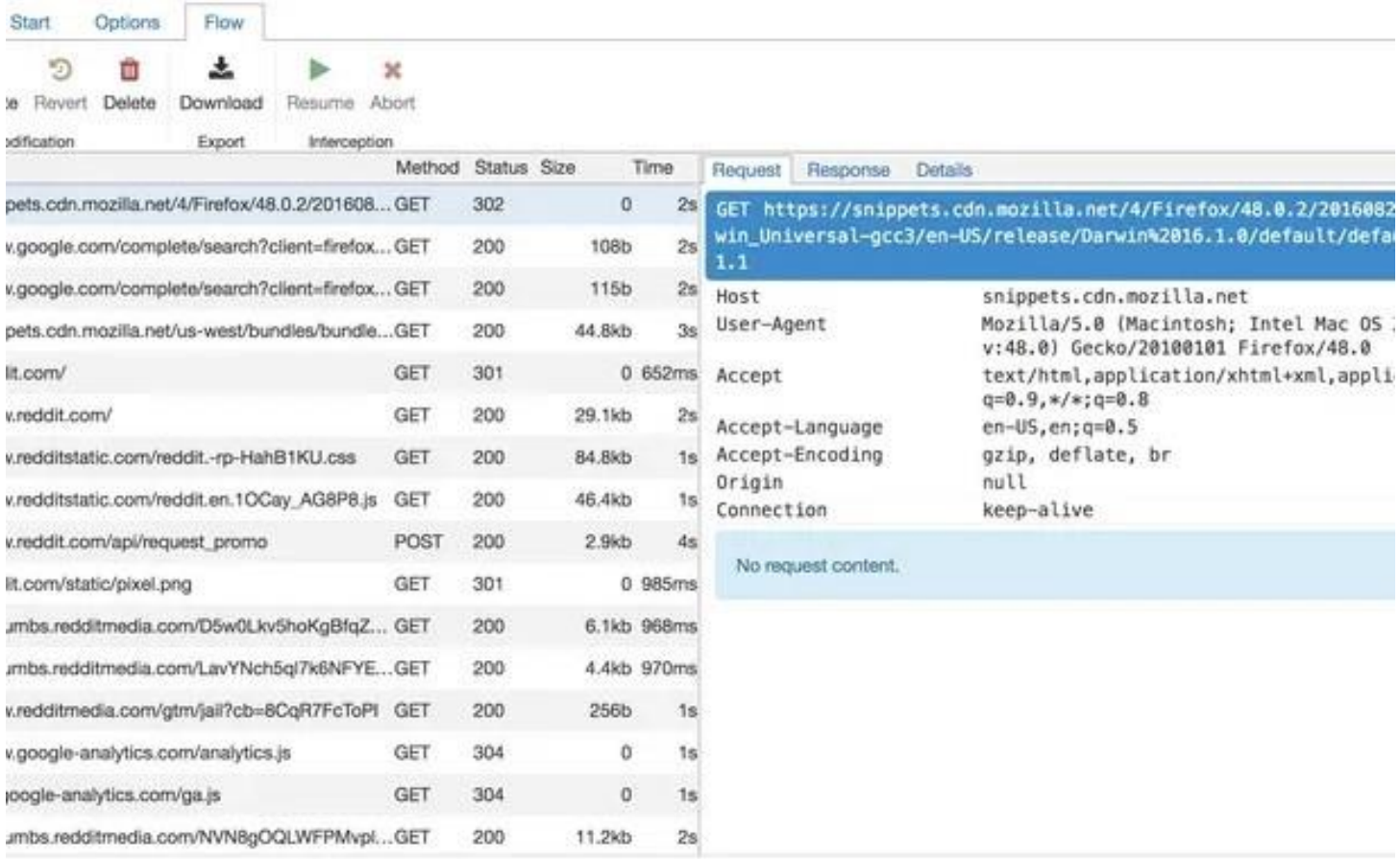
INTERCEPTING AND ANALYZING TRAFFIC:

With the setup complete, we actively monitor network traffic passing through the MitM proxy, analyzing HTTP and HTTPS requests and responses in real-time. This allows us to identify potential security vulnerabilities, detect malicious activity, and gain insights into the behavior of client applications.





OBSERVED CAPTURED DATA ON MITMWEB BROWSER.



CONCLUSIONS

The project provided valuable insights into the practical aspects of deploying a MitM proxy on a Raspberry Pi 3. By combining methodologies from multiple sources and conducting independent research, we gained a comprehensive understanding of MitM attacks and their implications for cybersecurity.

However, it is important to acknowledge the ethical considerations associated with MitM attacks and the potential risks involved in intercepting network traffic. While the project was conducted for educational purposes, similar techniques could be exploited for malicious intent if not used responsibly.

In conclusion, the project serves as a testament to the importance of hands-on experimentation and continuous learning in the field of cybersecurity. By exploring the capabilities of MitM proxies on a Raspberry Pi platform, we contribute to the ongoing discourse on safeguarding digital communication channels against evolving threats.

BIBLIOGRAPHY

- References:
- Fizzotti, Dino. "Running a Man-in-the-Middle Proxy on a Raspberry Pi 3."
- Adafruit Industries. "Setting Up a Raspberry Pi as a WiFi Access Point."
- Flipo, Bertrand. "Mitmproxy: Intercept, Modify, and Replay HTTP/HTTPS Traffic."
- Raspbian. "Raspbian Operating System."