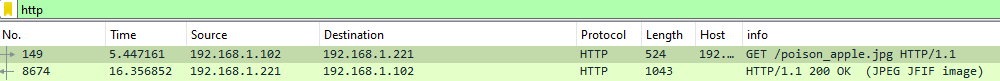
Fiona’s Apple – פתב"ס

ברק גונן

1. Wireshark

נפלטר לפי http. אפשר לראות שהמשאב המבוקש הוא poison\_apple.jpg, פקטה 149.

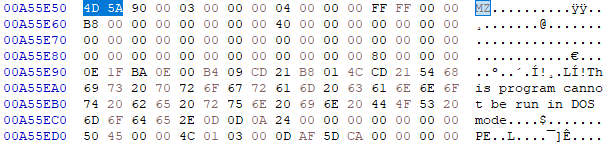


נבצע export object של http ושם יופיע האפשרות לבחור את poison\_apple.jpg.

נשמור את התמונה במקום כרצוננו, גודל התמונה כ-10 מגה בית.

1. תמונה

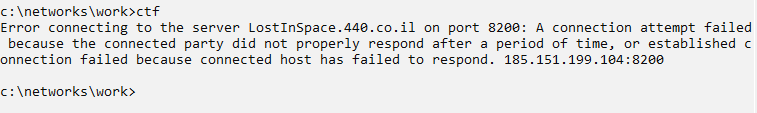
נעלה אותה ל-hex editor. חיפוש באמצעות ctrl-F על המחרוזת MZ יגלה מספר מקומות, כמעט כולם אקראיים אבל אחד מהם מופיע ליד הרבה אפסים ויש לידו טקסט קריא, שמי שמכיר את פורמט PE יזהה מיד



נבחר את כל הבתים מה-MZ ועד סוף הקובץ ונשמור אותם בקובץ חדש, ניתן לו את הסיומת exe.

1. בניית שרת

כאשר נריץ את קובץ ההרצה יודפס מסר



ניכנס לקובץ hosts שנמצא בתיקיה c:\windows\system32\drivers\etc\

נוסיף שם את הרשומה

127.0.0.1 LostInSpace.440.co.il

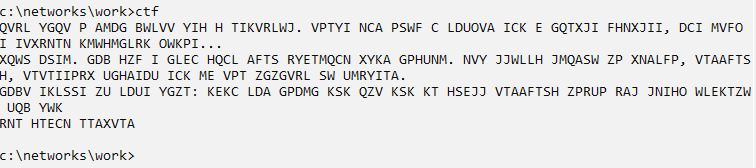
מכאן והלאה הלקוח כבר ידריך אותנו לבד באמצעות הודעות שגיאה מה חסר.

נבנה שרת בסיסי. להלן קוד השרת:

**import** json  
  
IP = **'127.0.0.1'**PORT = 8200  
  
**def** handle\_client(client\_socket):  
 data = client\_socket.recv(1024)  
 print(data)  
  
 response\_data = {**"Success"**: **True**}  
 response\_json = json.dumps(response\_data)client\_socket.sendall(**b"HTTP/1.1 200 OK\r\n"**)client\_socket.sendall(**b"Content-Type: application/json\r\n"**)  
 client\_socket.sendall(**b"Connection: close\r\n"**)  
 client\_socket.sendall(**f"Content-Length: {**len(response\_json)**}\r\n"**.encode())  
 client\_socket.sendall(**b"\r\n"**) client\_socket.sendall(response\_json.encode())  
 client\_socket.close()  
  
  
**def** main():  
 server\_socket = socket.socket(socket.AF\_INET, socket.SOCK\_STREAM)  
 server\_socket.bind((IP, PORT))  
 server\_socket.listen(1)  
 print(**f"Server listening on {**IP**}:{**PORT**}"**)  
  
 **while True**:  
 client\_socket, client\_address = server\_socket.accept()  
 print(**f"Accepted connection from {**client\_address**}"**)  
 handle\_client(client\_socket)  
  
**if** \_\_name\_\_ == **'\_\_main\_\_'**:  
 main()

1. צופן

עם הרצת השרת, הלקוח ידפיס לנו את הטקסט הבא:



נעתיק את הטקסט ל-online vigenere decoder, לדוגמה <https://www.guballa.de/vigenere-solver>

בשלב הראשון נבצע בדיקה מה אורך הקוד. לאחר מכן נזין לאורך הקוד את התוצאה -6.

המפתח הוא CIPHER והמסר הסופי הוא:

ONCE UPON A TIME THERE WAS A PRINCESS. THERE WAS ALSO A DONKEY AND A POLICE OFFICER, BUT FROM A TOTALLY DIFFERENT MOVIE...

GOOD WORK. YOU DID A REAL FINE WORK CRACKING THIS RIDDLE. YOU SHOWED SKILLS IN PYTHON, NETWORKS, OPERATING SYSTEMS AND IN THE SCIENCE OF SECRECY.

YOUR RIDDLE IS DONE HERE: DATA DOT CYBER DOT ORG DOT IL SLASH NETWORKS SLASH CTF SLASH SUCCESS DOT JPG

ALL SMALL LETTERS