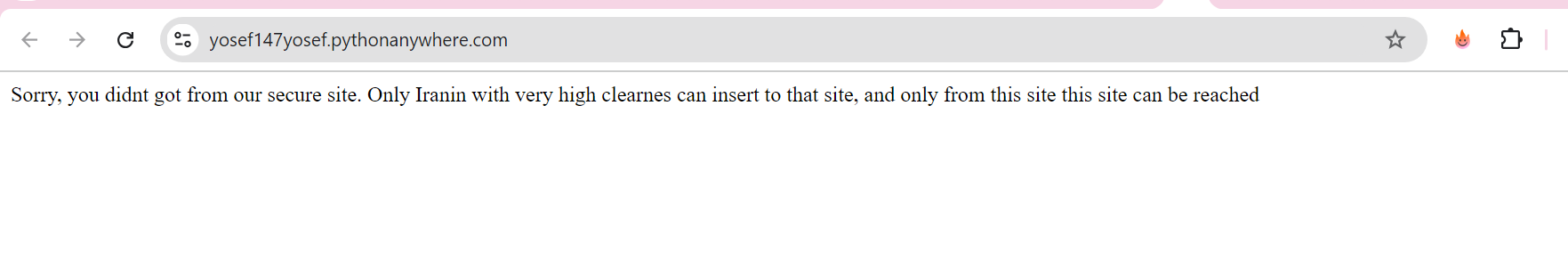
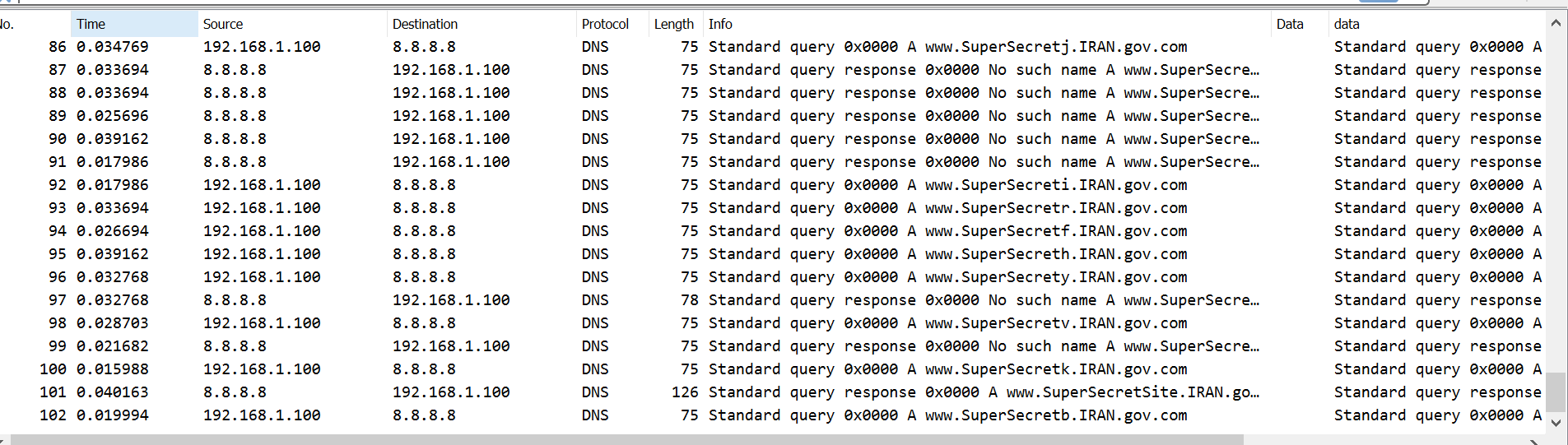
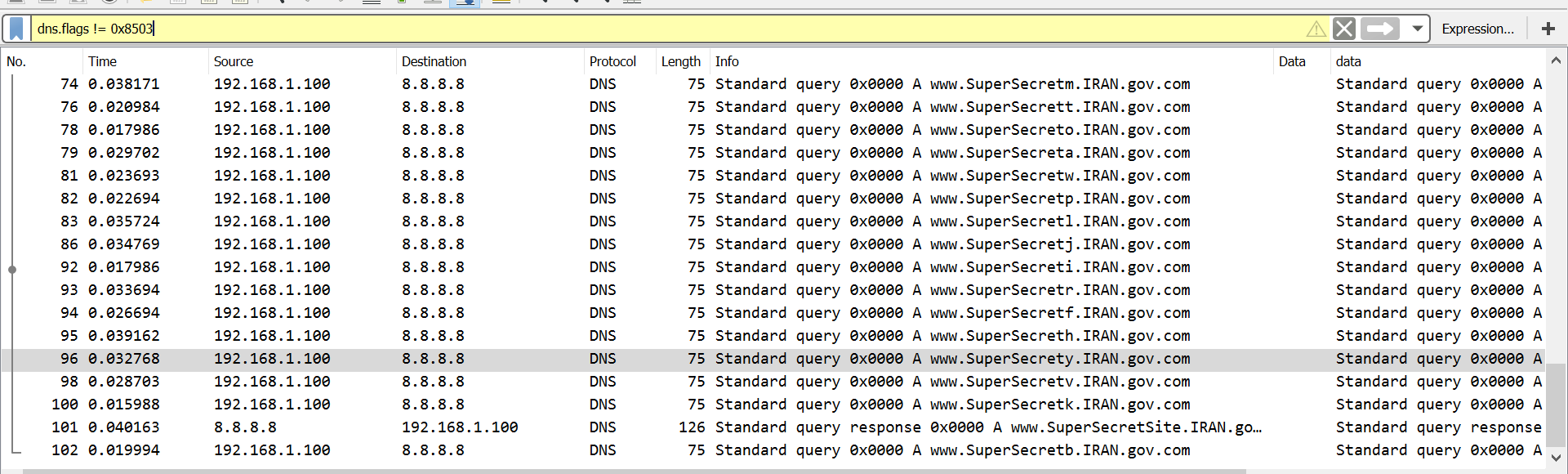
תחילה, נפתח את האתר שניתן לנו בקישור. אתר זה מאובטח. אם נקרא את ההוראות נבין שאי אפשר לגשת סתם ככה לאתר הזה, אלא רק מאתר אחר שבו יבוצע בידוק ביטחוני שאכן יש לנו את רמת הסיווג המתאימה כדי לגשת לאתר.

איזה אתר? לא ברור. צריך לפתוח את קובץ התיעוד ולראות.

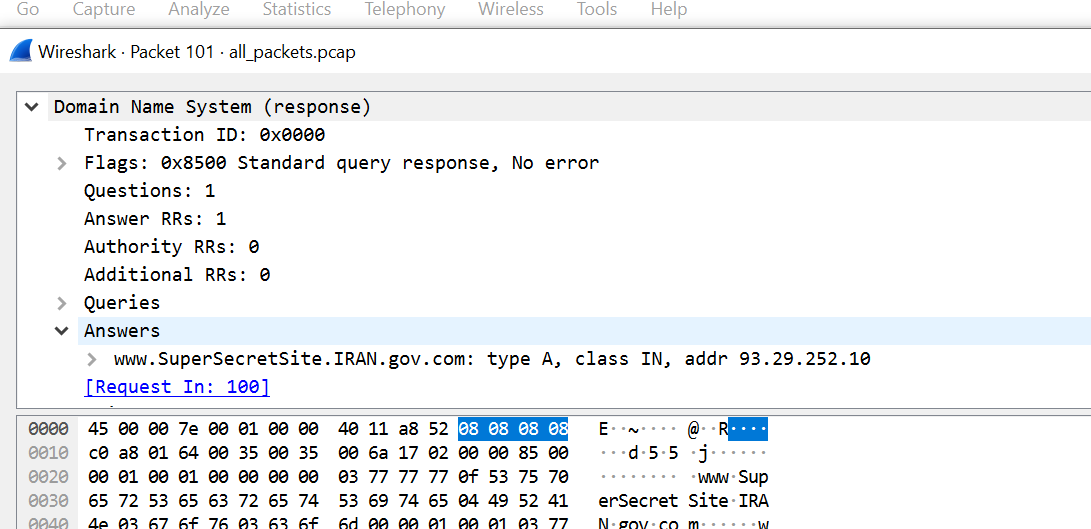
הקובץ מכיל הרבה פאקטות עם פרוטוקולים לא ברורים. אבל ניתן לראות שקיימות שאילות די אנ אס.



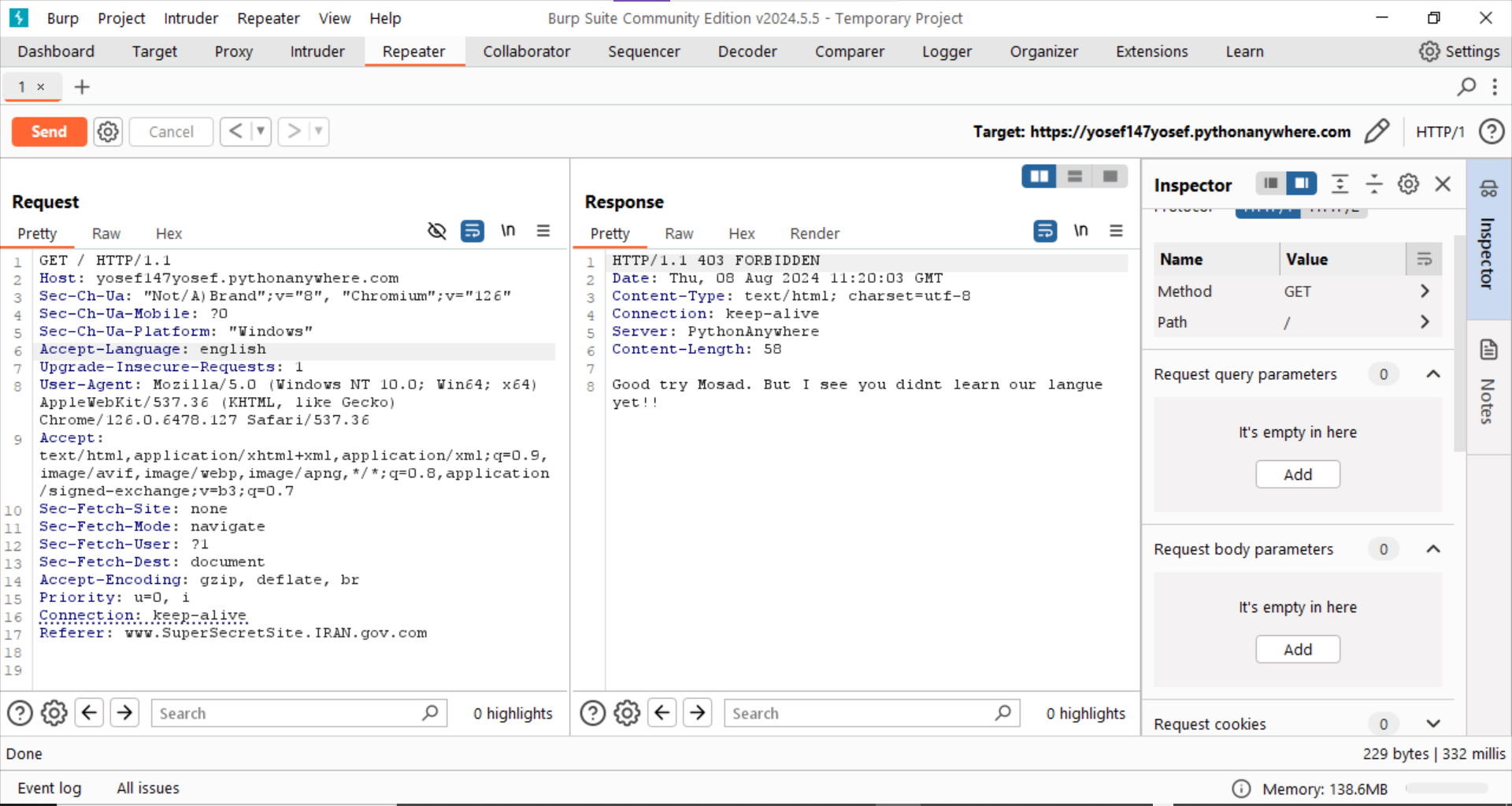
יש כאן הרבה בלאגן. התשובות לא מסודרות כמו שצריך, ויש הרבה בקשות לאתר עם שם דומה. צריך לפלטר רק בקשות די אנ אס שנענו בחיוב.



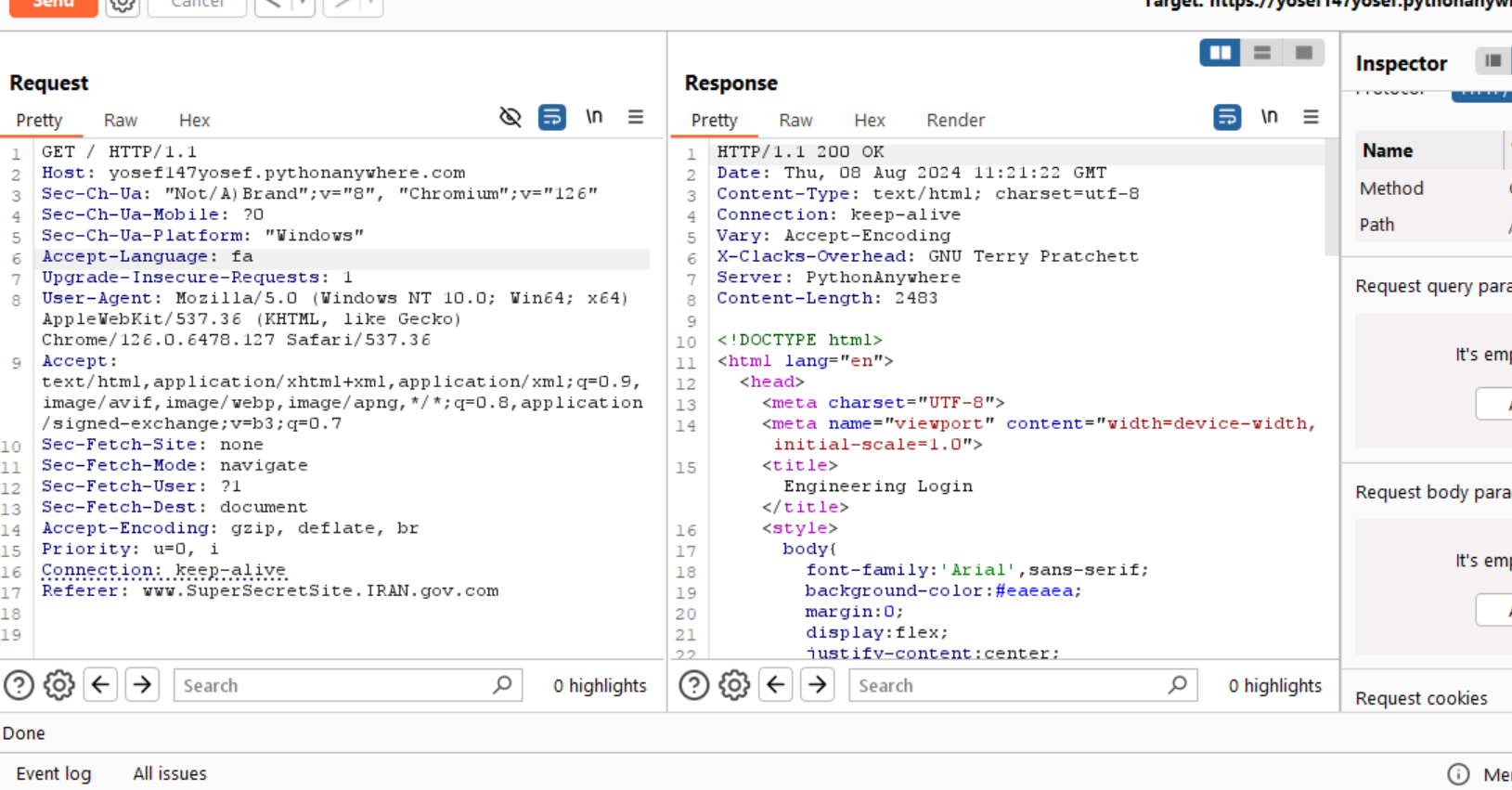
סיננתי חבילות שלא קיבלו תשובה של "לא קיים דומיין כזה" וניתן לראות שיש פאקטה אחת שהשרת מחזיר בחיוב.



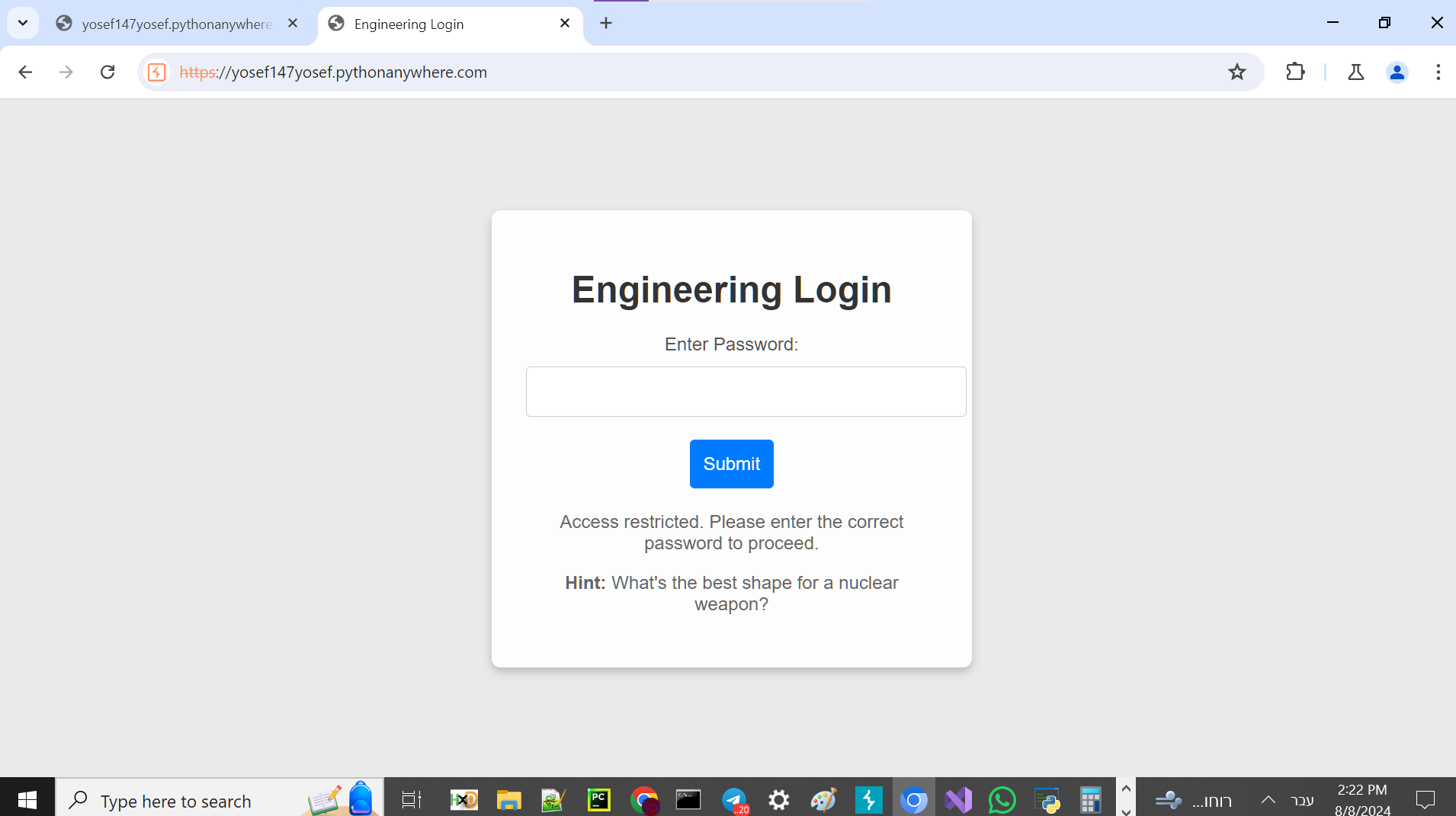
מצאנו דומיין. כנראה זה האתר שממנו צריך להגיע לאתר שאנחנו מנסים לפרוץ. עכשיו צריך לגרום לאתר לחשוב שבאנו מהאתר הזה. איך נעשה זאת? למזלנו יש שדה בפרוטוקול איג' טי טי פי שנקרא רפרנס, תפקידו לדאוג שאכן הגענו מהאתר המאובטח. ננסה לשנות אותו כדי שיתאים.



נשלח בקשת אג' טי טי פי עם תוכנה שנקראת ברב סוט. קיבלנו תשובה מוזרה. האתר מזהה שאנחנו לא דוברי פרסית ולכן הוא לא מכניס אותנו פנימה. נשנה את שדה השפה להיות השפה הפרסית.

 יש גישה לאתר!

בוא נראה את הייצוג שלו בדפדפן



נכנסו לאתר המהנדסים של הקור האיראני. אבל כעת עלינו להכניס סיסמא. לאחר ניסיונות למצוא את הסיסמא באתר עצמו, שכמובן שנכשלו , ננסה לחזור שוב לקובץ התיעוד ולראות אולי התיעוד של השיחות בכור יוכלו להסגיר את הסיסמא.

בשביל משימה זאת לא נוכל להשתמש בווירשרק. יש המון חבילות , ואין שום דרך לסנן חבילות עם צ'ק סמ נכון כדי לפלטר רק חבילות מקוריות, ההוראות אמרו במפורש שהשרת הוצף על ידי ילדי הסייבר, ואף ניתן לנו אלגוריתם הצ'ק סמ ששומש. אז עלינו לכתוב קוד פייתון שיסנן רק את הטקסטים של חבילות עם צ'ק סמ נכון.

קוד הפייתון:

from scapy.all import \*  
def custom\_checksum(packet):  
 if not packet.haslayer(UDP):  
 raise ValueError("Packet must contain a UDP layer")  
  
 # Create a copy of the packet with the checksum field set to 0  
 packet\_no\_checksum = packet.copy()  
 packet\_no\_checksum[UDP].chksum = 0  
  
 # Extract the raw bytes without the checksum field  
 packet\_bytes = bytes(packet\_no\_checksum)  
  
 # Calculate checksum  
 checksum = 0  
 for i in range(0, len(packet\_bytes)):  
 word = packet\_bytes[i]<<(i%4)  
 checksum += word  
 # One's complement  
 checksum = ~checksum & 0xffff  
  
 return checksum  
result = []  
def print\_packets\_with\_checksum(pcap\_file):  
 global result  
 # Read the pcap file  
 packets = rdpcap(pcap\_file)  
 for packet in packets:  
 # Check if the packet has a UDP layer  
 if UDP in packet:  
 # Check if the UDP checksum is 0xffff  
 chcksum = custom\_checksum(packet)  
 if packet[UDP].chksum == chcksum and packet[IP].src!='44.99.1.1':  
 result += [packet[Raw].load.decode()]  
  
# Replace 'your\_file.pcap' with the path to your pcap file  
pcap\_file = 'all\_packets.pcap'  
print\_packets\_with\_checksum(pcap\_file)  
print(result)

הקוד משתמש בסקאפי, ועובר על החבילות. רק חבילות עם צ'ק סמ יסוננו לתוך ריסלוט.

[' Bux pdqsrm gh bwg zmdr', 'Ivqf bq pb qzimghiam ktganzc ucz nej ivm rgexbmrkq ufwz hsg gcckcbs trtbtf', 'Rwwa Zxqhoor pyh svpkwehmq ucriar pc ptznbb ufwz mft waetcam Ublys', 'Qg bq icw ehscr wa mft hwc Mfxg evej eib n lkxzm bg rws nnvch cn gac tbmzr']

קיבלנו מערך של מחרוזות. אבל נראה שהן מוצפנות. קל לראות שמדובר בצופן החלפה מסוג כלשהו. ננסה לשבור אותו על ידי כלים אונליין של צפני החלפה אבל התוצאות לא הגיוניות. כנראה שמדובר בצופן ויגנר. צופן החלפה שהמפתח שלו הוא הזזה של האותיות בגודל קבוע ביחס למיקומן.

 לדוגמה עבור המחרוזת הנכונה ניתן לראות שההודעה היא

The rocket is not good.

נמשיך לשאר המחרוזות:

This is an important message for all the engineers from our supreme leader

This Message was encrypted becuse we afraid from the israely Mosad

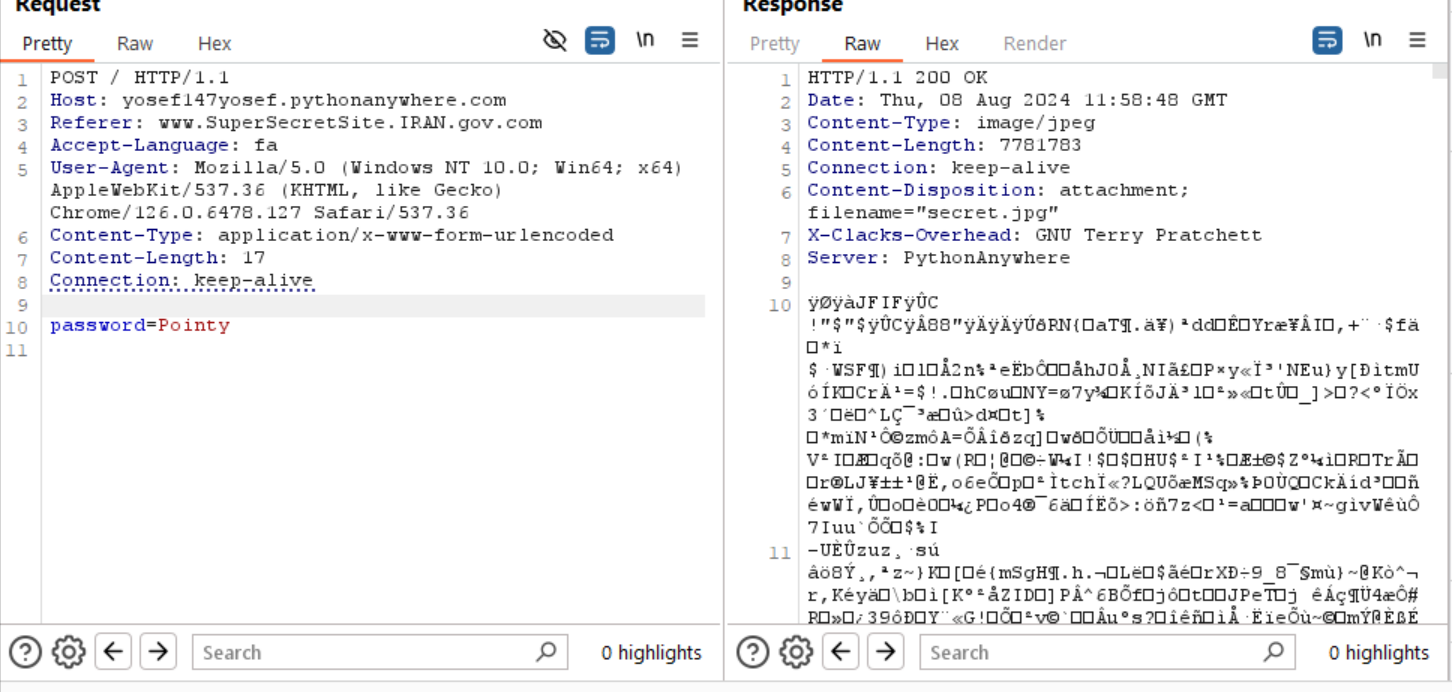
It is too round on the top This will put a smile on the faces of the enemy

הסדר קצת שובש, אבל ניתן לראות שהם מדברים על זה שהטיל לא טוב כי הצורה שלו עגולה בקצה. זה גם מתאים לרמז של הסיסמא, מה הצורה האידאלית של טיל גרעיני.

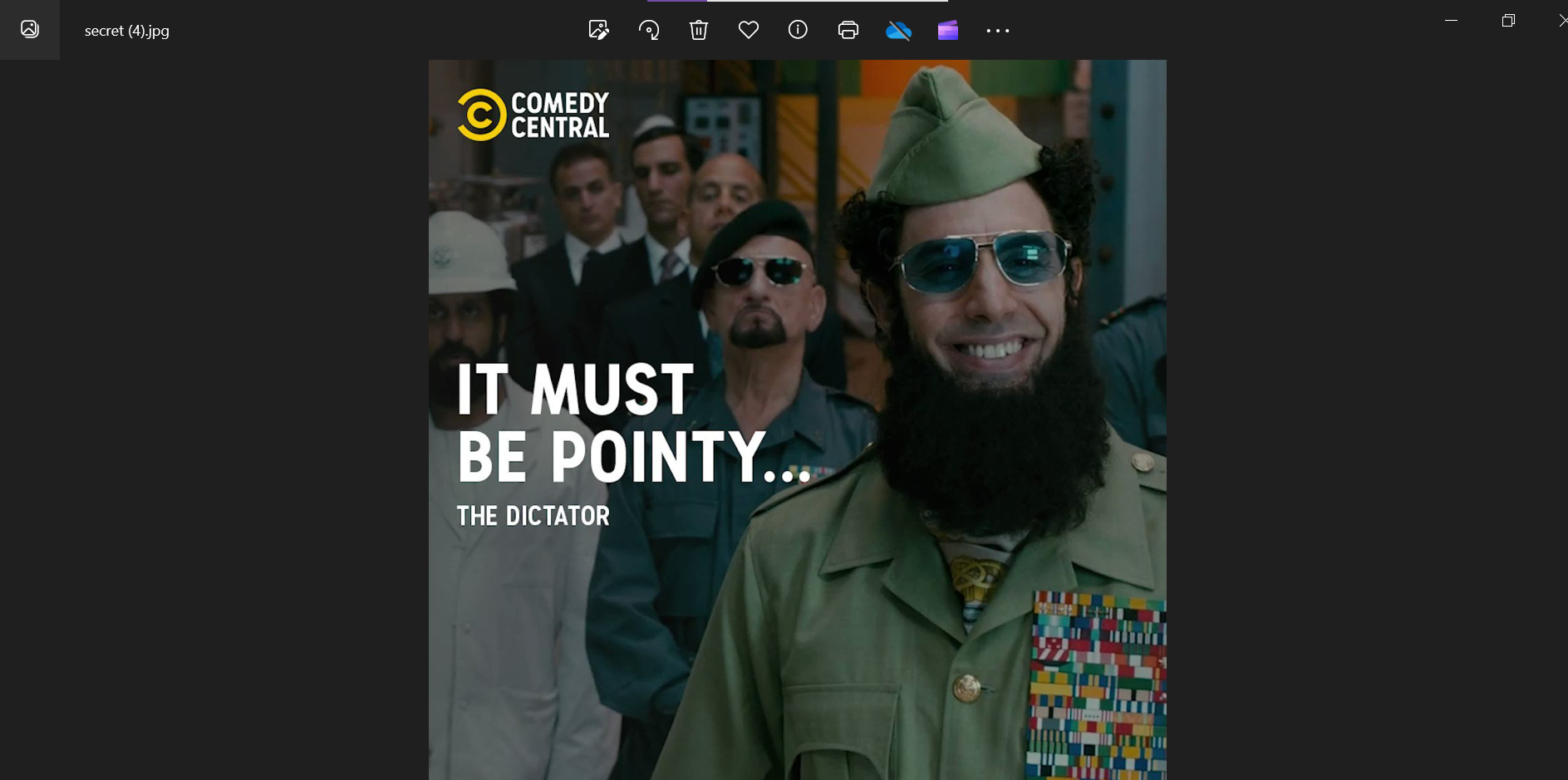
כמובן שמדובר על השורה המפורסמת מהסרט הדיקטטור של סשה ברון כהן. טיל גרעיני צריך להיות מחודד.

It Needs to be pointy!

בוא ננסה את הסיסמא. כמובן שגם כאן אנחנו צריכים לשמור על המבנה של חבילת האיג טי טי פי האיראנית.

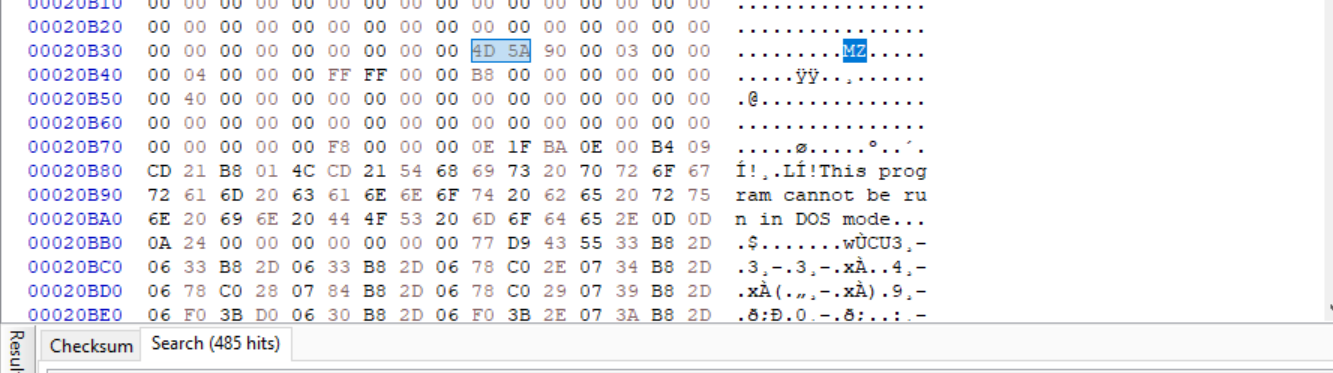


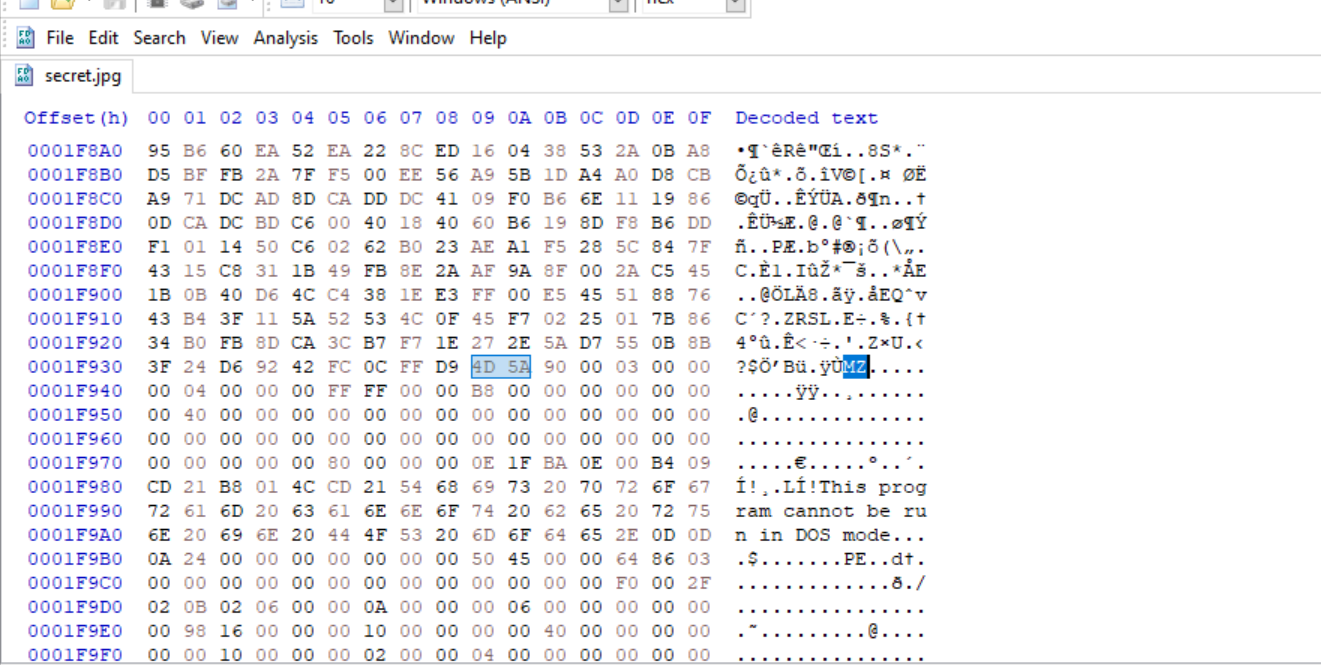
הידד! קיבלנו תמונה מהשרת.



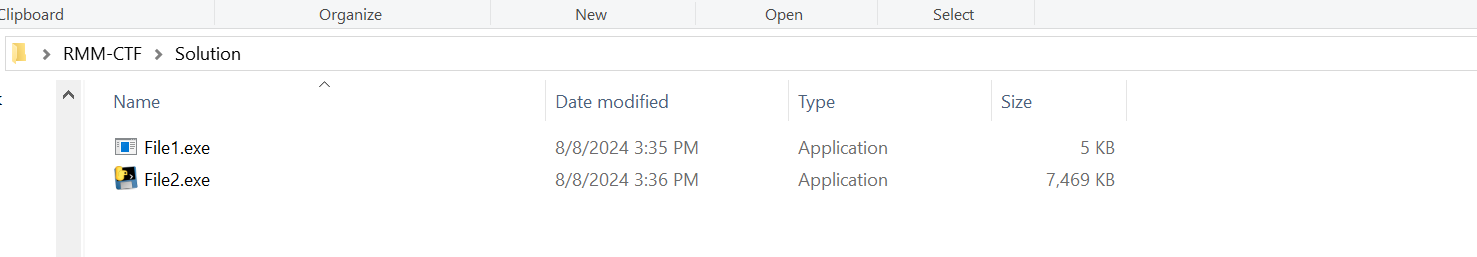
אבל טרם הגענו לדגל.

נפתח את התמונה בהקסה אדיטור. ניתן לראות שהתמונה גדולה מאוד מאוד יחסית לתמונה. נחפש לראות אם מוחבא בה משהו.

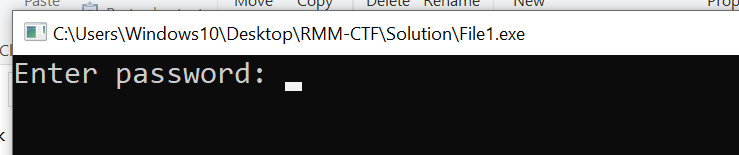
מצאנו בה שתי קידומות אמ זד של פורמט פי אי. 



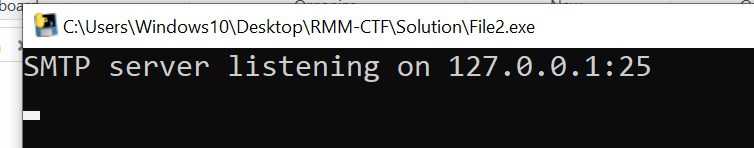
נחלץ את שניהם לשתי קבצי אקסקיוטבל.



נפתח את שניהם ונראה מה נקבל.



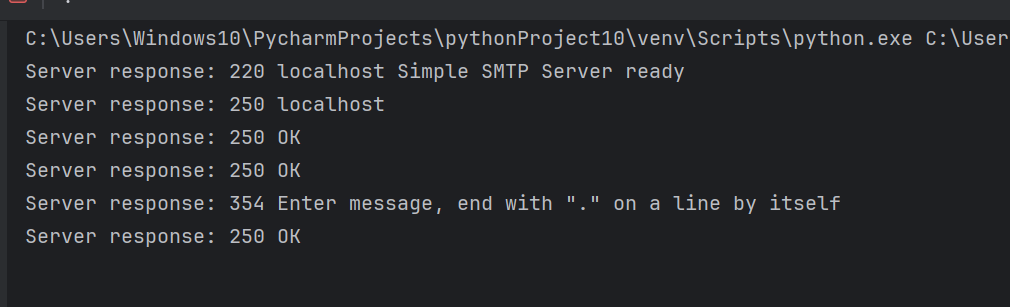
הקובץ הראשון מבקש סיסמא.



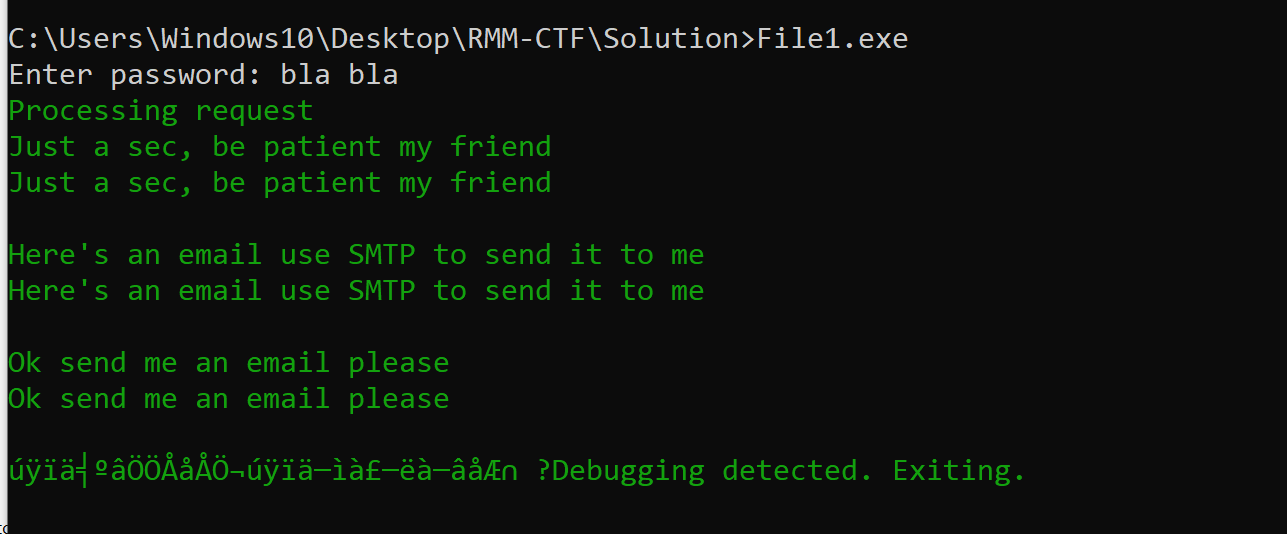
הקובץ השני הוא שרת אס אמ טי פי.

ננסה לכתוב לקוח שיתקשר עם השרת.

import socket  
import email  
from email.parser import Parser  
from email.mime.text import MIMEText  
  
HOST = '127.0.0.1' # Standard loopback interface address (localhost)  
PORT = 25 # SMTP port  
  
def send\_email(sender\_email, recipient\_email, subject, body):  
 # Create the message  
 msg = MIMEText(body)  
 msg['Subject'] = subject  
 msg['From'] = sender\_email  
 msg['To'] = recipient\_email  
  
 # Connect to the SMTP server  
 with socket.socket(socket.AF\_INET, socket.SOCK\_STREAM) as s:  
 s.connect((HOST, PORT))  
  
 # Receive the server's greeting  
 data = s.recv(1024)  
 print(f"Server response: {data.decode().strip()}")  
  
 # Send the HELO command  
 s.sendall(b'HELO localhost\r\n')  
 data = s.recv(1024)  
 print(f"Server response: {data.decode().strip()}")  
  
 # Send the MAIL FROM command  
 s.sendall(f"MAIL FROM:<{sender\_email}>\r\n".encode())  
 data = s.recv(1024)  
 print(f"Server response: {data.decode().strip()}")  
  
 # Send the RCPT TO command  
 s.sendall(f"RCPT TO:<{recipient\_email}>\r\n".encode())  
 data = s.recv(1024)  
 print(f"Server response: {data.decode().strip()}")  
  
 # Send the DATA command  
 s.sendall(b'DATA\r\n')  
 data = s.recv(1024)  
 print(f"Server response: {data.decode().strip()}")  
  
 # Send the email message  
 s.sendall(msg.as\_string().encode())  
 s.sendall(b'\r\n.\r\n')  
 data = s.recv(1024)  
 print(f"Server response: {data.decode().strip()}")  
  
 # Receive the response email from the server  
 response\_email = b''  
 while True:  
 data = s.recv(1024)  
 if not data:  
 break  
 response\_email += data  
 if data.endswith(b'\r\n.\r\n'):  
 break  
  
 # Parse and print the response email  
 try:  
 msg = Parser().parsestr(response\_email.decode())  
 print('Received response email:')  
 print(msg)  
 except (UnicodeDecodeError, email.errors.MessageParseError):  
 print('Error parsing response email')  
  
 # Send the QUIT command  
 s.sendall(b'QUIT\r\n')  
 data = s.recv(1024)  
 print(f"Server response: {data.decode().strip()}")  
  
# Example usage  
send\_email("your\_email@example.com", "test@test.com", "Test Email", "This is a test email.")



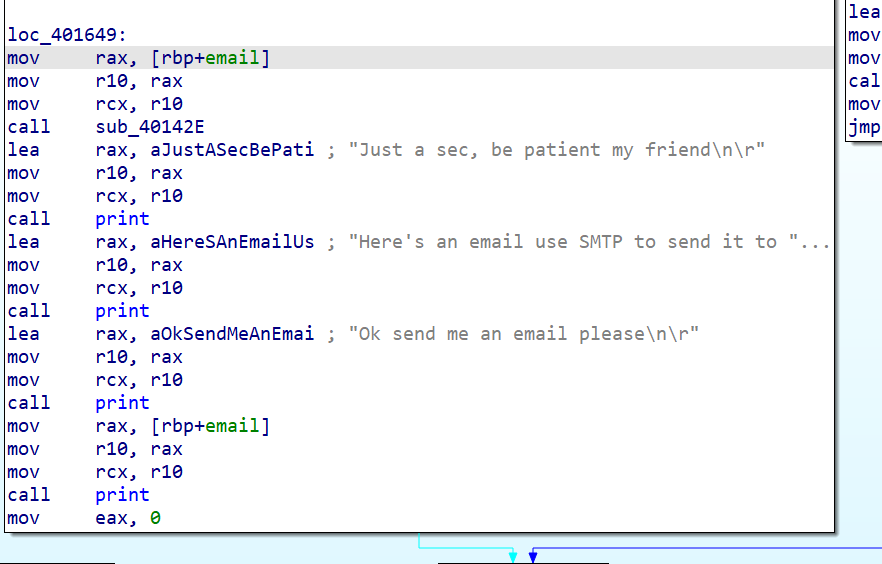
השרת לא מחזיר שום דבר. בוא ננסה לשים סתם סיסמא ולראות איך הקובת השני מגיב.



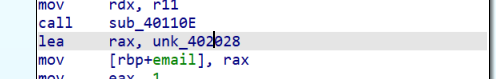
אם נביא לו סיסמא נכונה נקבל את המייל. כרגע הוא לא מביא כלום. אבל מאיפה נביא סיסמא??

ננסה לעשות רברסינג על מנת לפרוץ את זה.

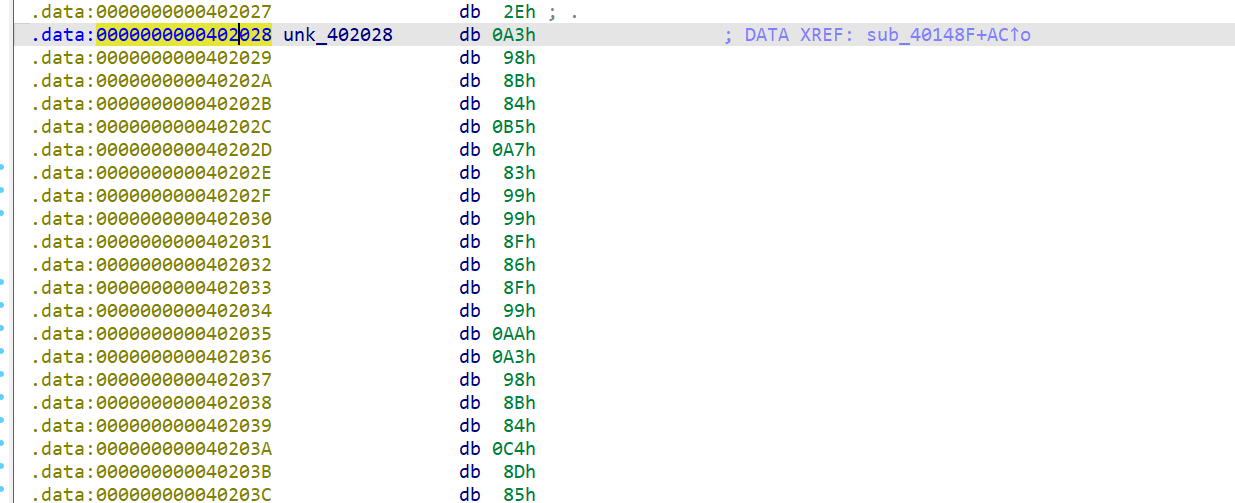
הקוד מכיל אנטי דיבאגרים. ולכן לא אנסה לדבג אותו אלא לנתח סטטית.



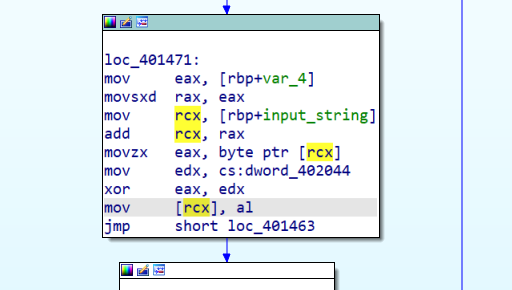
הנה ההדפסות של כל ההודעות. אבל ההדפסה האחרונה של המייל היא לא ממקום קבוע. בוא ננסה להבין מה קורה פה.

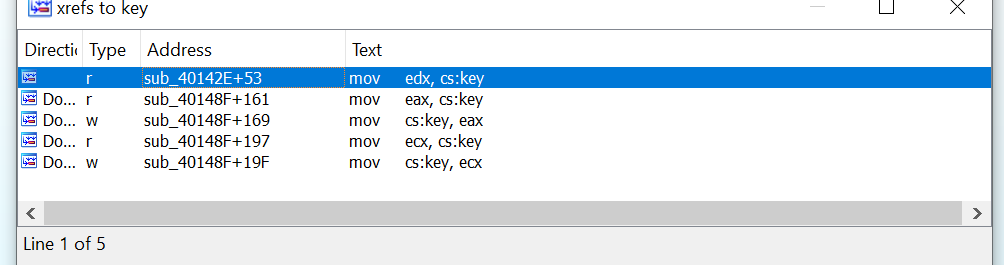


המשתנה של המייל מקבל מחרוזת מהזיכרון, אבל המחרוזת מוצפנת.



נחזור להדפסות, יש פונקציה אחת שלא ברור מה היא עושה:



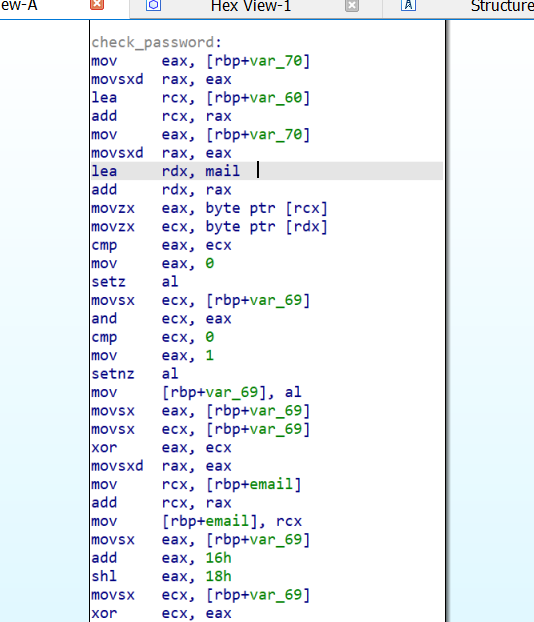
הפונקציה הזאת עושה קסור עם מקום קבוע בזיכרון. כנראה שמדובר בפונקציה שמפענחת את המחרוזת המוצפנת. כעת נותר לנו לראות מה המפתח. 

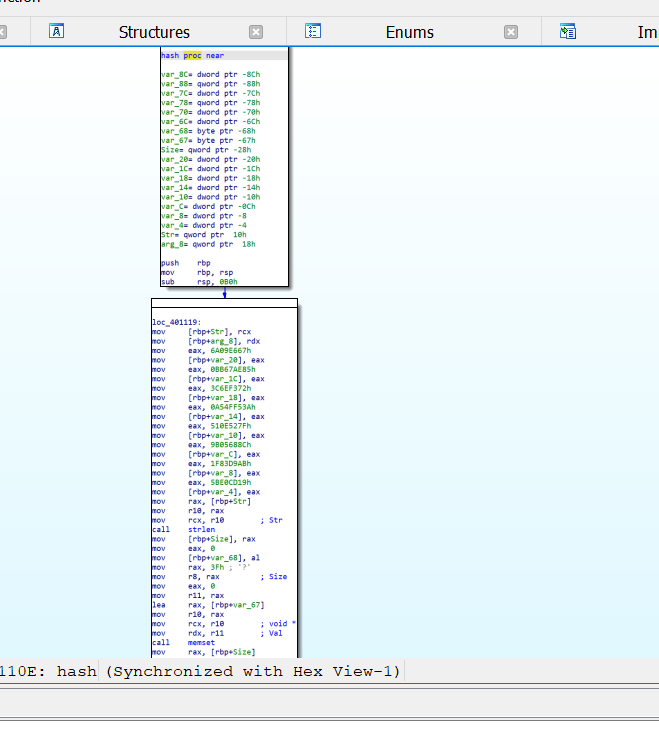
אנחנו עושים הרבה מניפולציות על המפתח.

הערך ההתחלתי שלו הוא

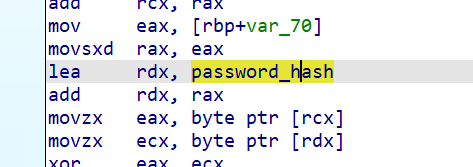
0xEA

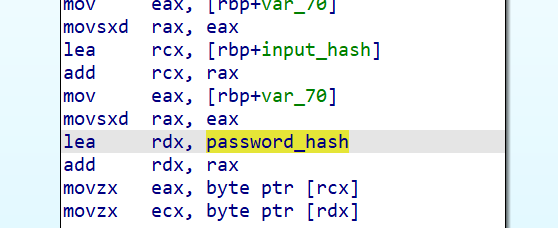
ניתן לראות כאן שהוא בודק את הסיסמא באמצעות פונקצית האש כתובה והוא משנה את המפתח והמצביע למחרוזת של המייל בהתאם להשוואות.



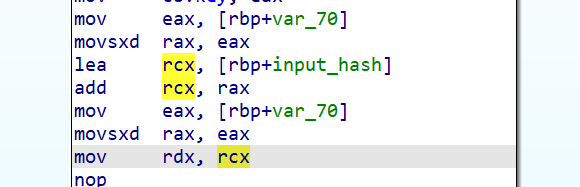
פונקצית ההאש מסובכת להחריד. אין סיכוי בזמן סביר למצוא סיסמא מתאימה. ננסה לפצפץ' וזהו. הרעיון הכי פשוט זה לגרום פשוט לתוצאה של ההאש להיות ההאש שאנחנו רוצים. זה יחסוך לנו גם להבין מה התהליך שעומד מאחורי יצירת המפתח, וההגעה לאינדקס המדויק במחרוזת של המייל.

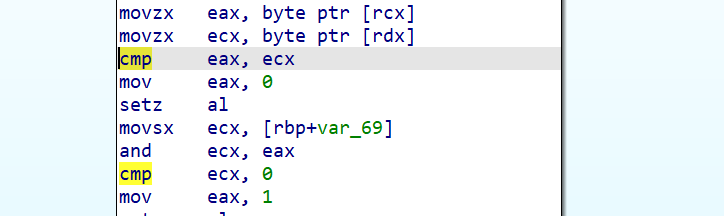
.



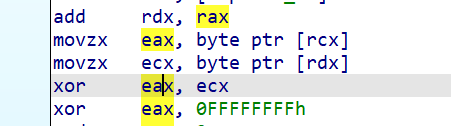
הנה הגישה לבית מתוך ההאש והאש מתוך האינפוט האש 

ובהמשך יש פעולות ביניהם, ככה שמן הסתם הכוונה היא להשוות ביניהם.





סהכ יש שני קומפרים. בוא נשנה אותם להיות השוואה עם עצמם.



בנוסף יש גם קסור.

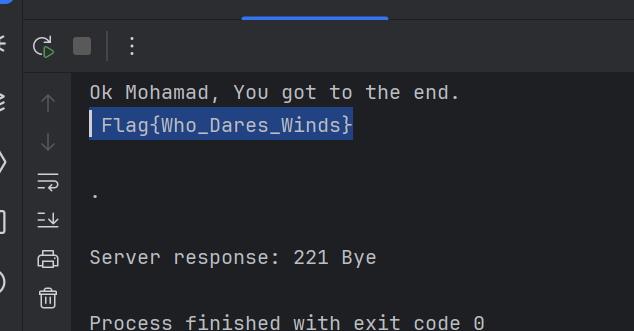
בקיצור, כל מקום שבוא יש פעולת בית עם שני המקומות במערכים נשנה להיות עם האוגר עצמו.

סהכ , מצאתי שני קסורים ופעולת השוואה אחת. ואלה המקומות היחדים שמשתמשים במערכים האלה. אז בוא ננסה.



השגנו את המייל!!

עכשיו רק נשאר לשנות את קוד הלקוח של שרת האס אמ טי פי שישלח את המייל לכתובת הזאת



השגנו את הדגל!!

Flag{Who\_Dares\_Winds}