בס"ד

הצעת פתרון – Mossad CTF

בתור התחלה אנחנו מקבלים איזשהו סיפור, מה שניתן ללמוד מהסיפור זה שיש לנו איזשהו סוכן מוסד, אלי קופטר, ששכח את הסיסמא לאתר שלו.

כמו כן, הוא לא הצליח לגשת לאתר כי נמחקו הרשומות, לשם כך הוא ביצע שאילתת DNS למצוא את ה IP של האתר שלו.

מצורף קובץ הסנפה, נחפש את שאילתת ה DNS בשביל למצוא את האתר.

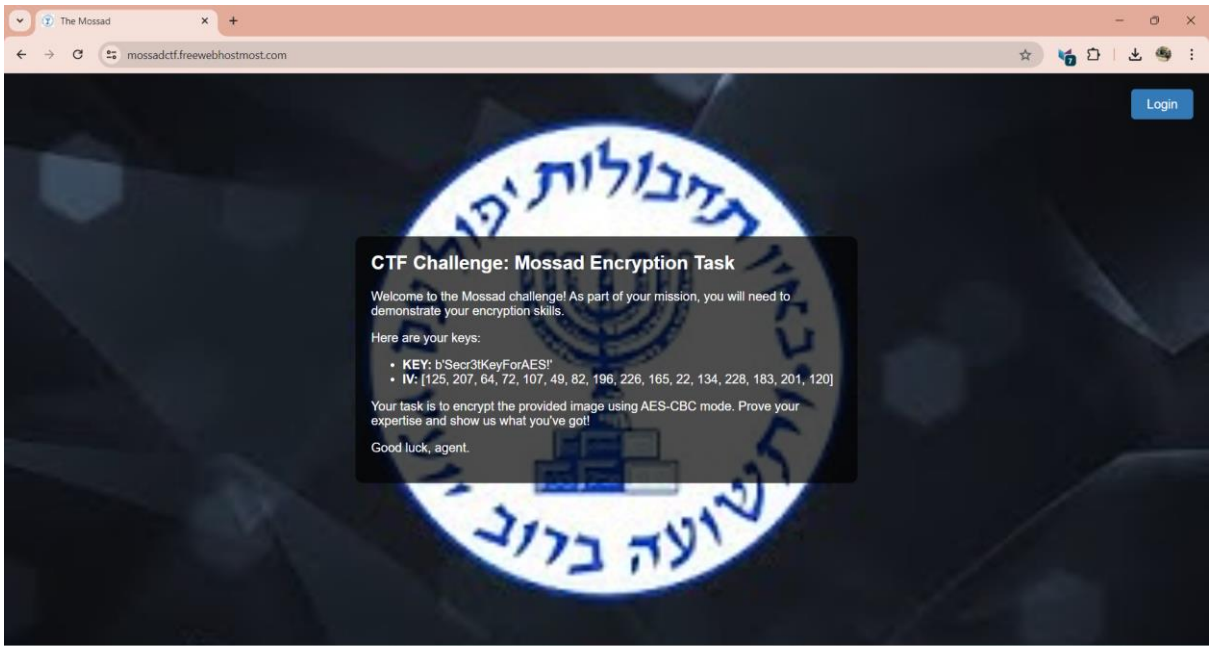
אנחנו יודעים שזה איזשהו ctf שקשור למוסד, אז אולי נחפש מילות מפתח, כגון ctf או mossad

dns && frame contains "ctf"

No.	Time	Source	Destination	Protocol	Length	Info
44	16.423798	192.168.33.16	192.168.33.1	DNS	89	Standard query 0x0002 A mossadctf.freewebhostmost.com
45	16.431462	192.168.33.1	192.168.33.16	DNS	105	Standard query response 0x0002 A mossadctf.freewebhostmost.com A 34.132.146.171
46	16.438047	192.168.33.16	192.168.33.1	DNS	89	Standard query 0x0003 AAAA mossadctf.freewebhostmost.com
47	16.446401	192.168.33.1	192.168.33.16	DNS	117	Standard query response 0x0003 AAAA mossadctf.freewebhostmost.com AAAA 2600:1900:4000:e094:0:b::

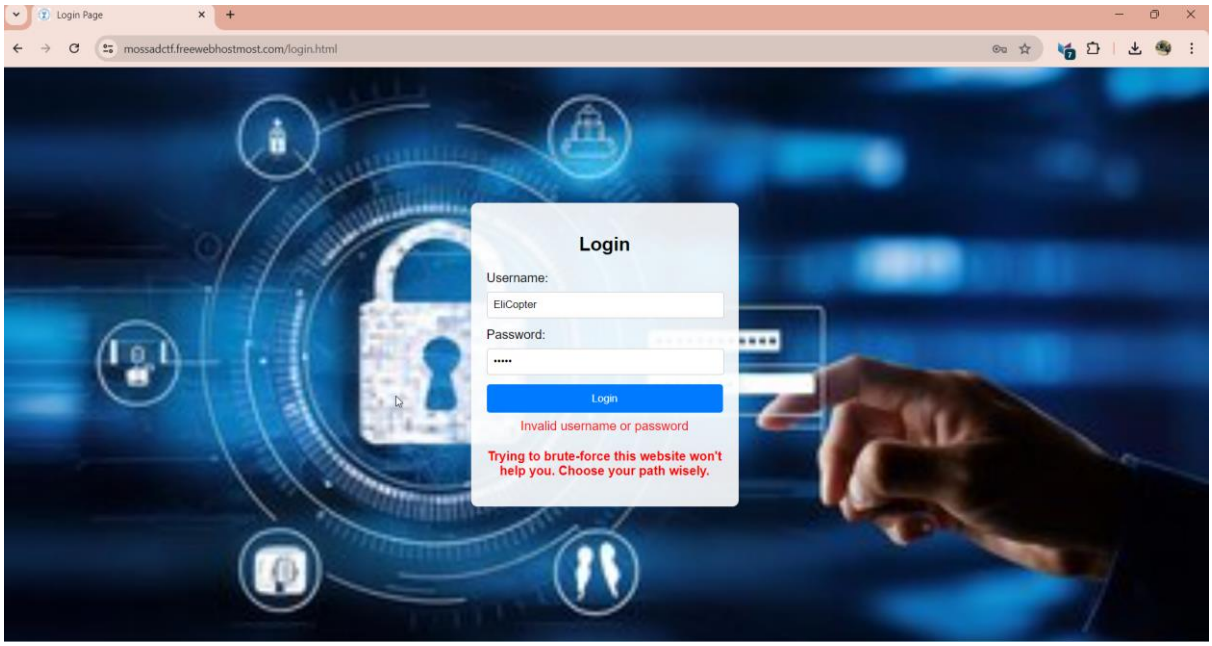
יפה! מצאנו את השאילתא ואת ה domain, אם ככה, ה domain הוא:
mossadctf.freewebhostmost.com

ננסה לגלוש אליו בדפדפן



בס"ד

יפה, פה אנחנו רואים איזשהו כפתור login, בלחיצה אליו אנחנו מגיעים לאתר אחר ששם ניתן לראות שאפשר לראות שיש מקום להכניס פרטי הזדהות, וכמו כן ממליצים לנו לא לנסות bruteforce. אוקי.



טוב, אז ננסה לנתח את שאר הדף.

אומרים לנו פה שיש מפתח ו IV, וכן שמצורפת תמונה שיש להצפינה עם המפתחות האלה באלגוריתם AES-CBC.

מוזר?

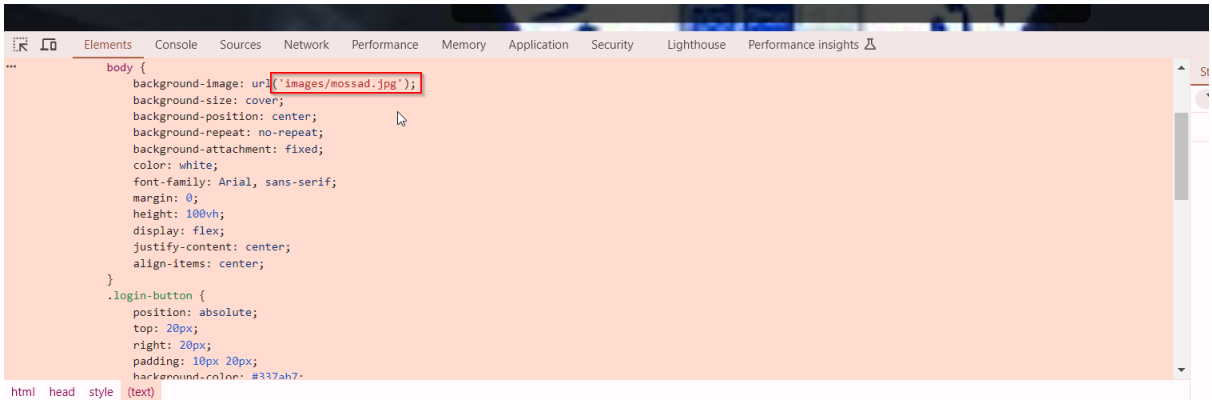
א. על איזו תמונה מדובר?
ב. איך הצפנה של תמונה תעזור לי?

טוב, בוא ננסה ונראה...

ניתנות לנו פה שתי תמונות בסה"כ, ה icon של האתר ותמונת הרקע של הדף הנוכחי.

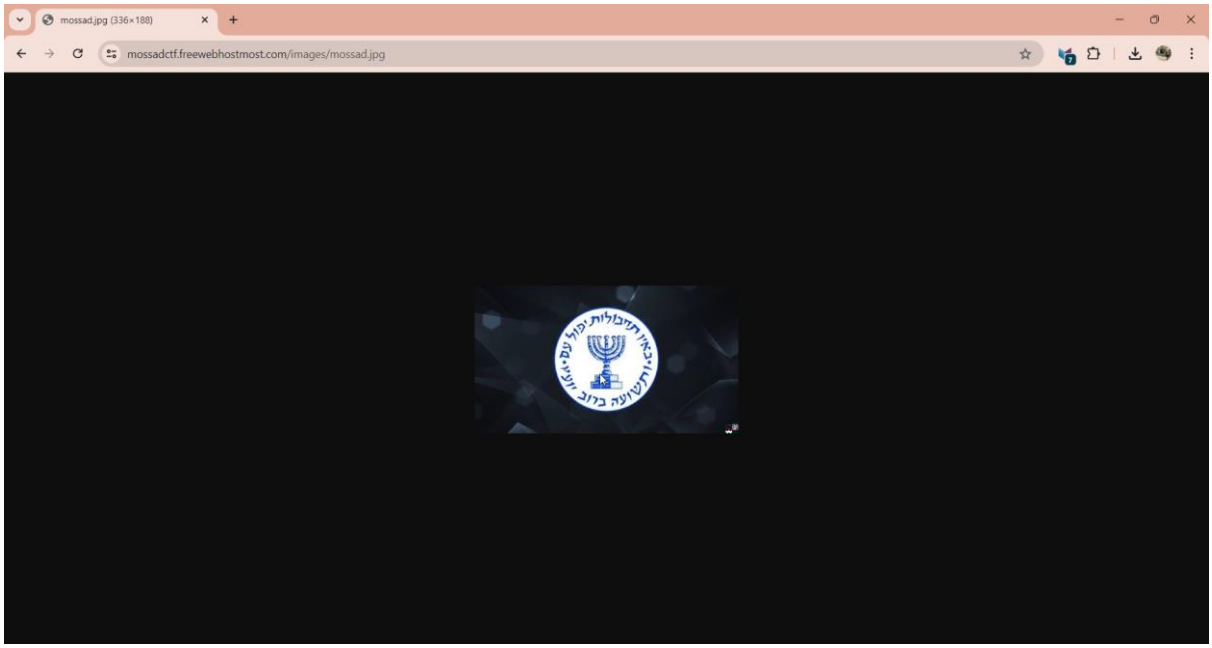
בוא ננסה באמת להצפין את התמונה:

בתור התחלה, עלינו להוריד אותה, לשם כך נעשה inspect



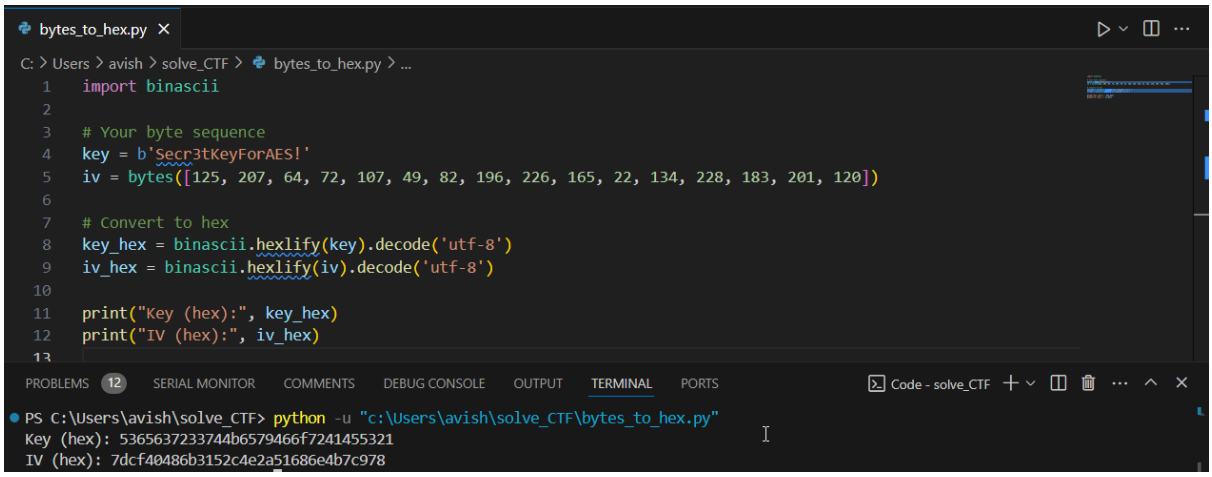
בס"ד

וניגש ל resource הזה:

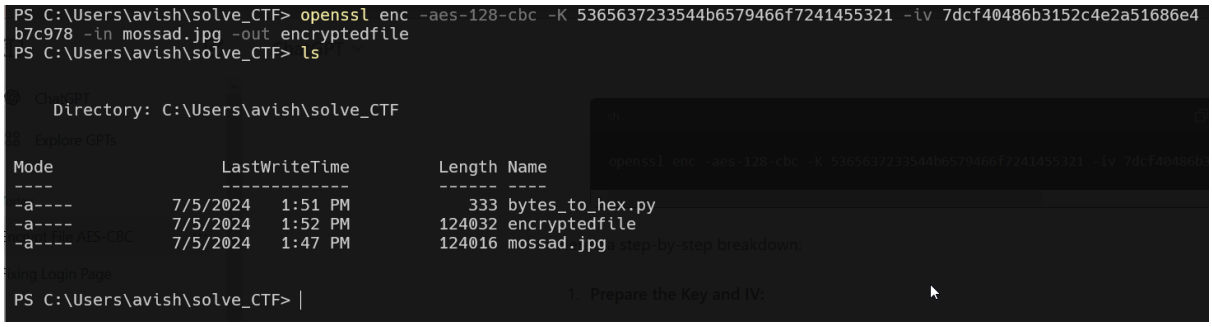


נשמור את התמונה על המחשב שלנו, ונצפין אותה באמצעות openssl.

בתור התחלה, נכתוב script קצר שתפקידו יהיה להמיר את המפתח ו IV ל hex.

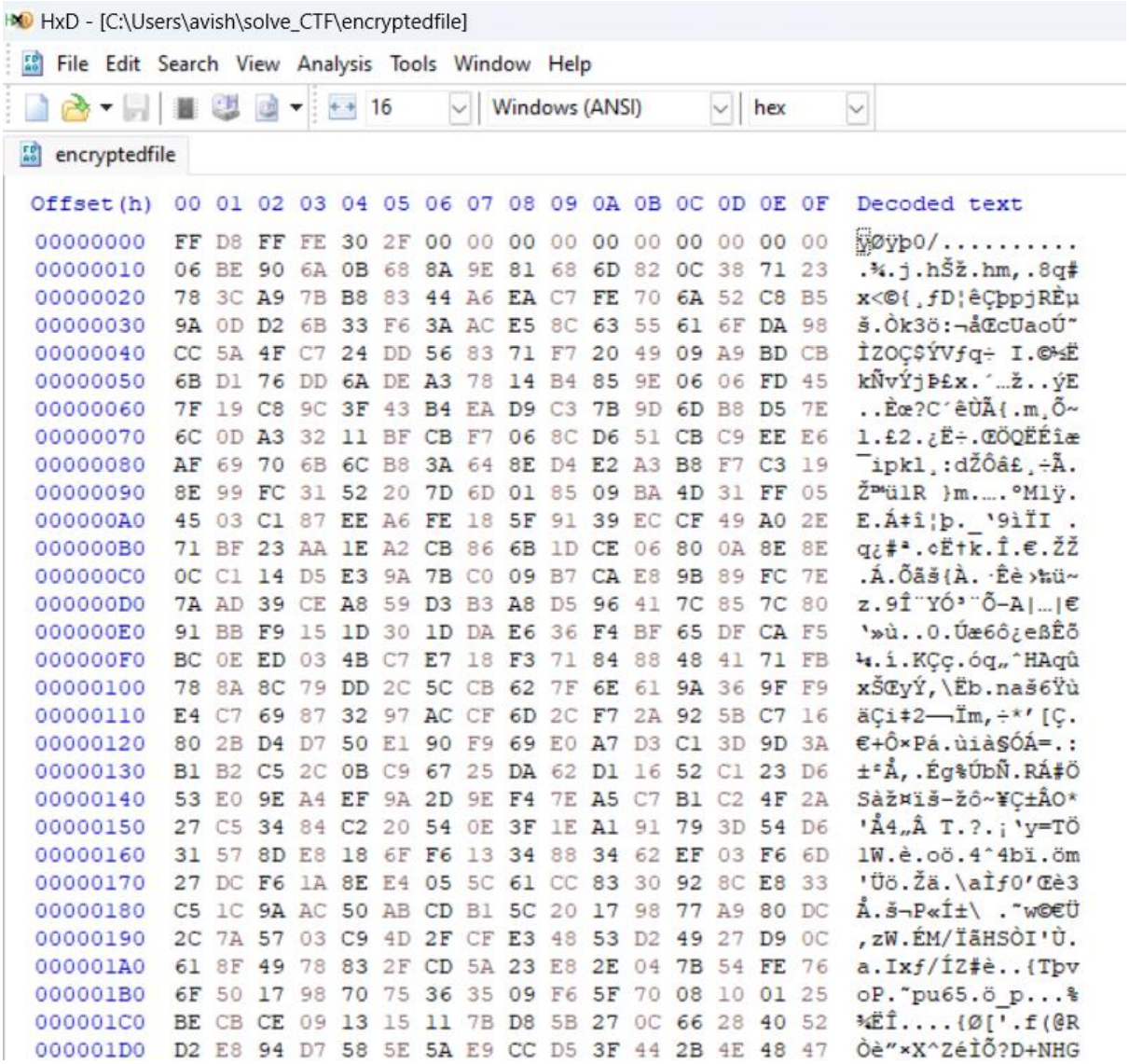


ואז, נריץ את השורה הבאה:



בס"ד

יפה מאוד. עכשיו, כשפותחים את זה ב hex editor, יוצא ג'יבריש

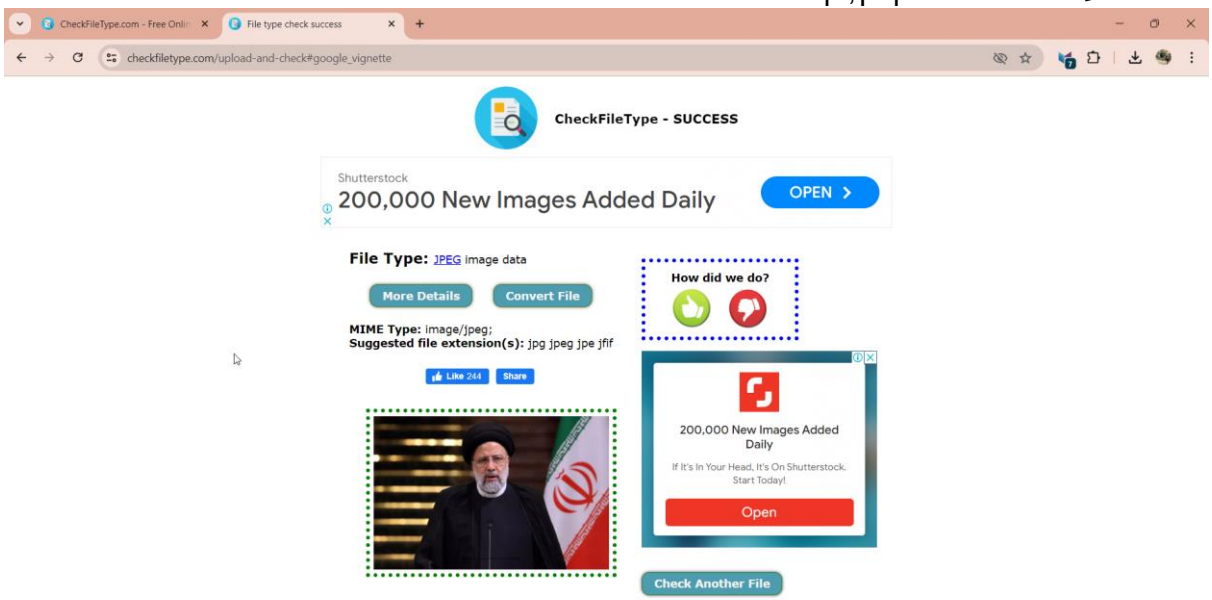


אולם, בוא ננסה את מזלנו ונעלה את זה למזהה פורמטים אינטרנטי חינמי, אולי יהיה לנו מזל ונזכה לגלות משהו.

אני השתמשתי באתר הבא: https://www.checkfiletype.com.

בס"ד

לאחר שהעליתי לשם את הקובץ, קיבלתי את הדבר הבא:



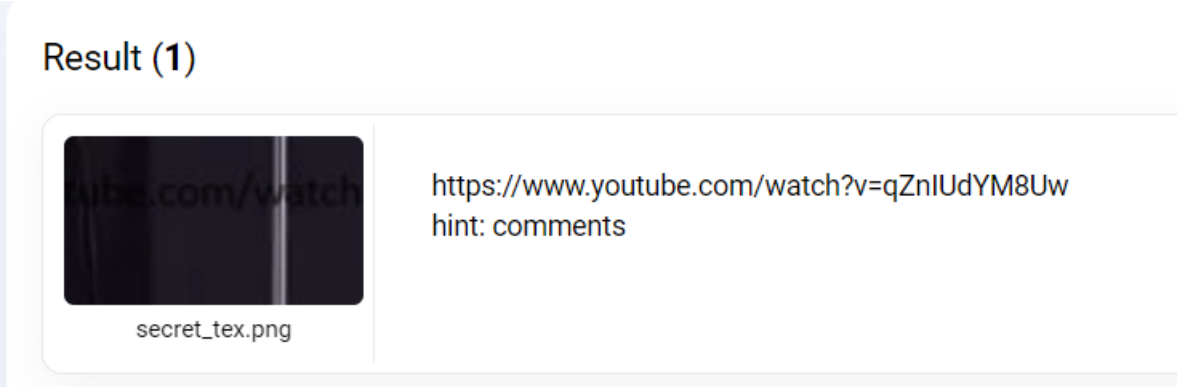
וואו! יצאה לנו תמונה! בוא ננסה להמיר את הקובץ במחשב שלנו ל jpg, ולראות מה יצא:

במבט ראשוני התמונה נראית סתם תמונה משעממת, אלא שאם מסתכלים טוב, אפשר לראות שיש משהו שמסתתר למטה.

בס"ד

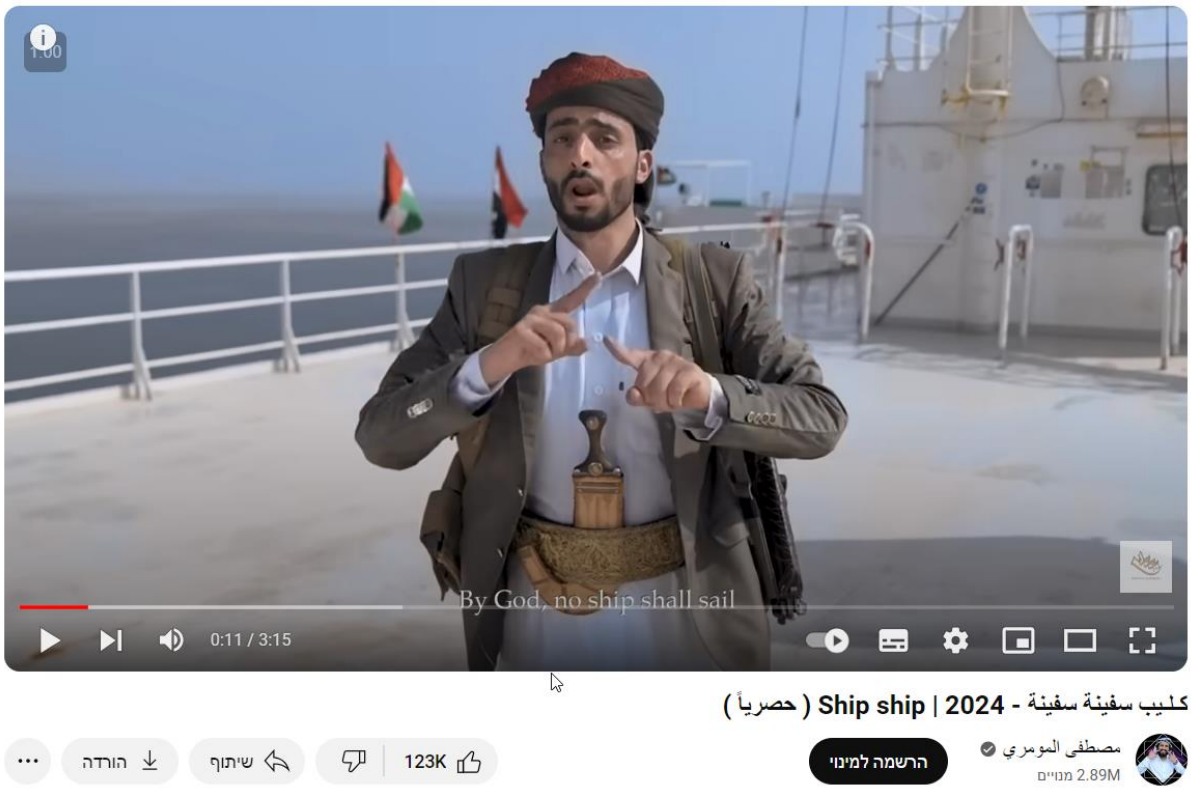
יש פה איזשהו טקסט, ננסה לפענח מה בדיוק רשום שם, נשמור רק את החלק הזה בתור תמונה חדשה, ונעלה לאתר שיודע לפענח text מתוך תמונות, https://www.imagetotext.info.

זה מה שהתקבל:



קישור לסרטון יוטיוב ובנוסף, איזשהו רמז: תגובות.

ניגש לסרטון היוטיוב הזה



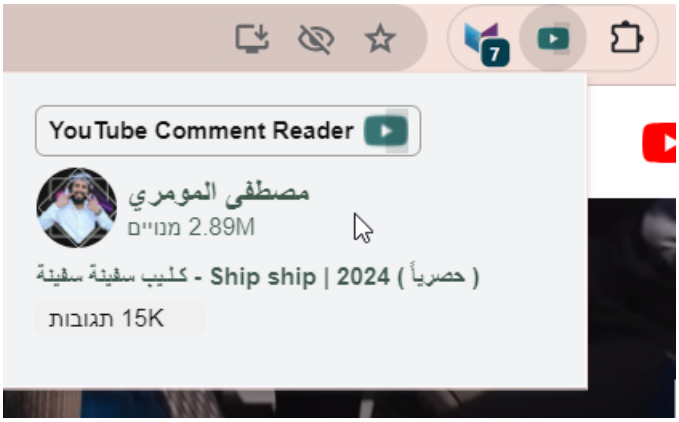
או אה, סרטון מעניין :)

בכל מקרה, אנחנו באנו ל CTF! הרמז שקיבלנו הוא תגובות. יכול להיות שמישהו החביא משהו בתגובות?

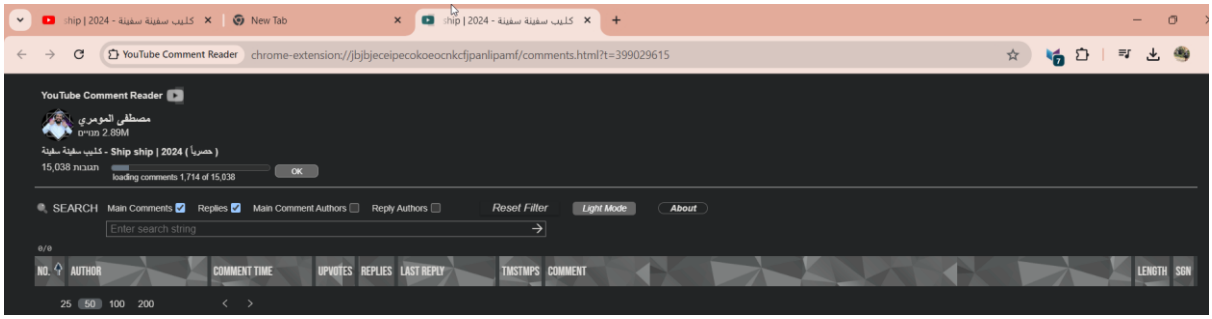
בס"ד

כיוון שיש פה מעל ל 15 אלף תגובות, אנחנו נצטרך להשתמש בכלי שיעזור לנו לנתח את התגובות. נשתמש בתוסף שמישהו הכין ל chrome:

https://chromewebstore.google.com/detail/youtube-comment-reader/jbjbjeceipecokoeocnkcfjpanlipamf

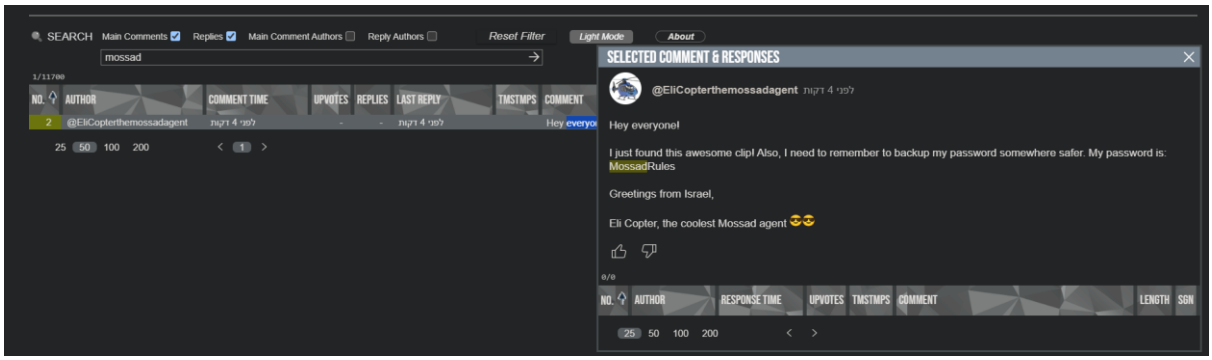


בלחיצה על התוסף אפשר לעבור לדף אחר שבו ננתח את התגובות:



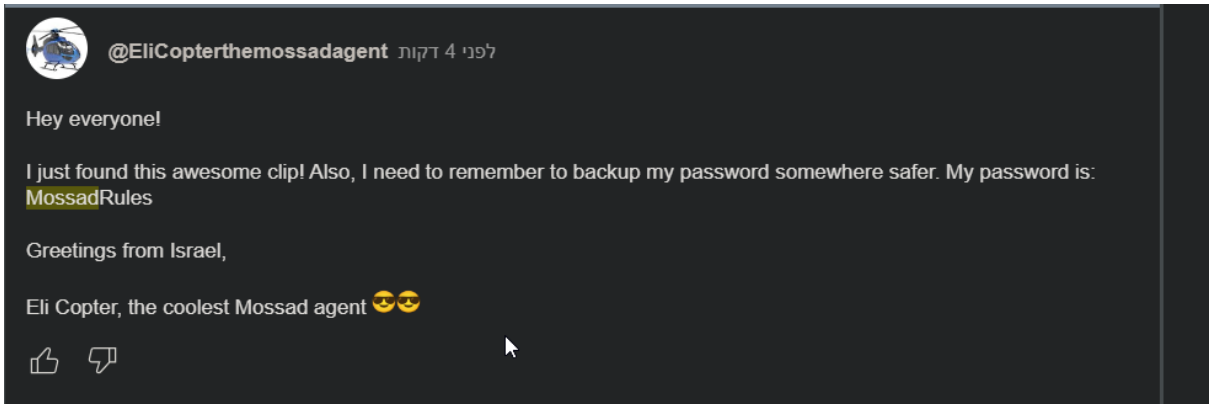
ייקח קצת זמן לכל התגובות להיטען, נחכה שהם יסיימו להיטען ואז ננסה למצוא את התגובה שהחביאו עבורנו. אחרי הכל, הרמז זה תגובות.

בוא ניזכר, מה שאנחנו מחפשים זה משהו שקשור ל EliCopter, סוכן המוסד שלנו, שמהסיפור למדנו שהוא שמר את הסיסמא איפשהו ושכח איפה בדיוק. אם כך, אולי נוכל לחפש באמצעות מילות מפתח, לדוגמא, mossad:



וואו! מה מצאנו!

בס"ד



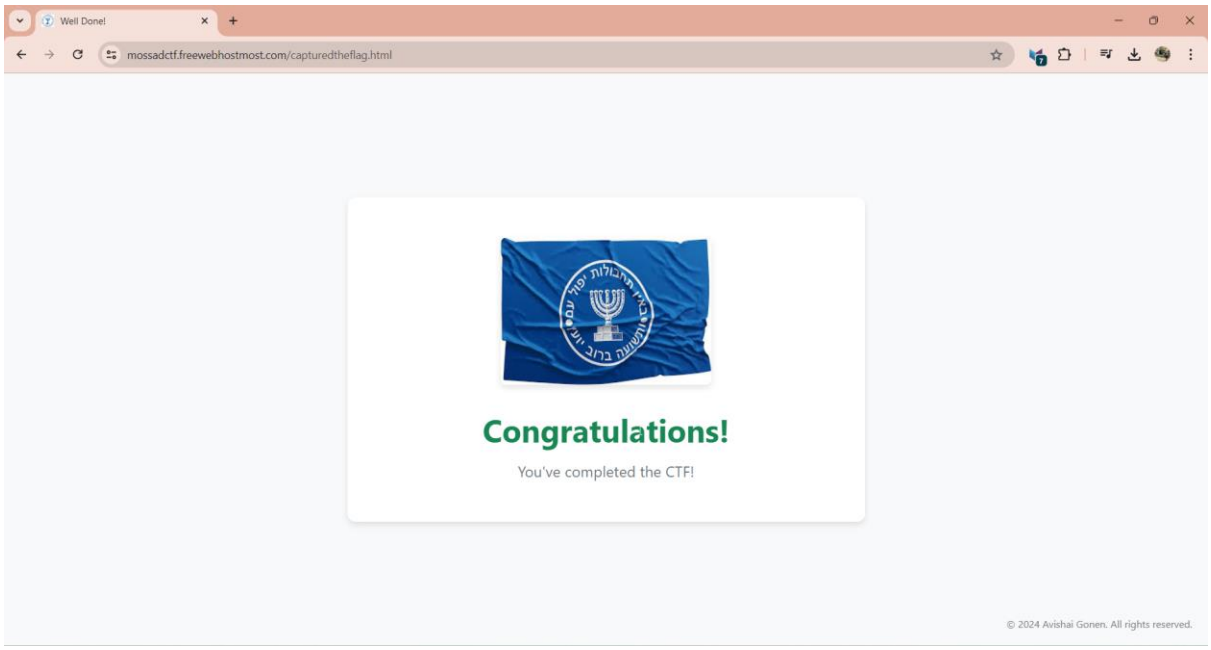
גילינו מה הסיסמא!

MossadRules

בוא נחזור לאתר מההתחלה, ונכניס את הפרטים הבאים:

Username: EliCopter

Password: MossadRules



וזהו! סיימנו את ה CTF!!