אתגר יחידת "חושן" - סוכות 2020

**שלומי אבידן**

האתגר בעיקר עוסק בתחום הסטגנוגרפיה - הסתרת מידע מן העין, בו תחילה יש לפענח סרטון הכולל תקיעות בשופר, אשר מביא כתובת לתמונה שבה מוחבא קובץ מסוג RAR עם סיסמא. לאחר פיצוח הסיסמא וחילוץ הארכיב מתקבלת תמונה, שאם ניקח את ערכי הצבעים שלה בהקסדצימלי ונפענח את המחרוזת יתקבל הפיתרון.

קול שופר וקול תרועה

תחילה יחידת חושן מספקת לנו סרטון הכולל שתי דקות של תקיעות בשופר, קצרות וארוכות:



ניתן לראות שהתקיעות הן למעשה קוד מורס, המורכב מתקיעות קצרות המסמלות נקודות, ותקיעות ארוכות המסמלות את הפסים. נכתוב את התקיעות במורס ויתקבל הקוד הבא:

**.---- ..--- ----. .-.-.- ..--- .---- ...-- .-.-.- ...-- ..--- .-.-.- ..--- -----**

תוצאת פיענוח קוד המורס היא 129.213.32.20, כתובת IP!

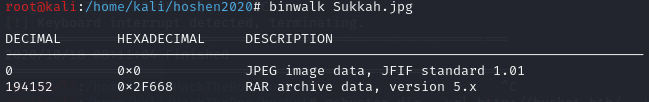
שלומית בונה סוכה

נשתמש בכתובת ה-IP שקיבלנו בתור כתובת URL, ונקבל אתר שבו יש רק את התמונה הבאה:



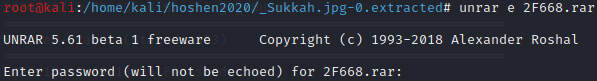
נוריד את התמונה ונבדוק אם משהו מתחבא בה.

בהרצת הכלי binwalk על התמונה, כלי שבודק האם קובץ מכיל בתוכו קבצים נוספים, ניתן לראות שהתמונה לא תמימה כמו שהיא נראית ומכילה למעשה ארכיב מסוג RAR.



נחלץ את הארכיב מהתמונה באמצעות הפקודה **binwalk -e Sukkah.jpg**

כאשר מנסים לבצע חילוץ של הקבצים מהRAR מגלים שהארכיב מוגן על ידי סיסמא:

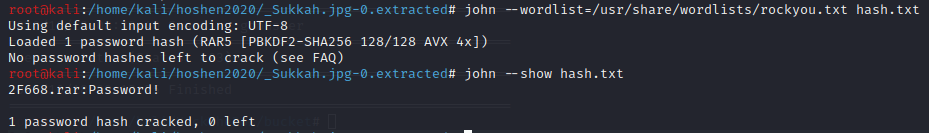


למזלנו ניתן לפצח את הסיסמא ממש בקלות באמצעות כלי הנקרא johntheripper.

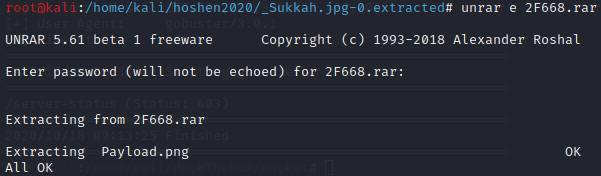
תחילה נוציא את ערך ה-hash של הארכיב ונשמור אותו בקובץ hash.txt:



כעת נריץ את johntheripper על קובץ ה-hash. נשתמש במילון rockyou.txt:



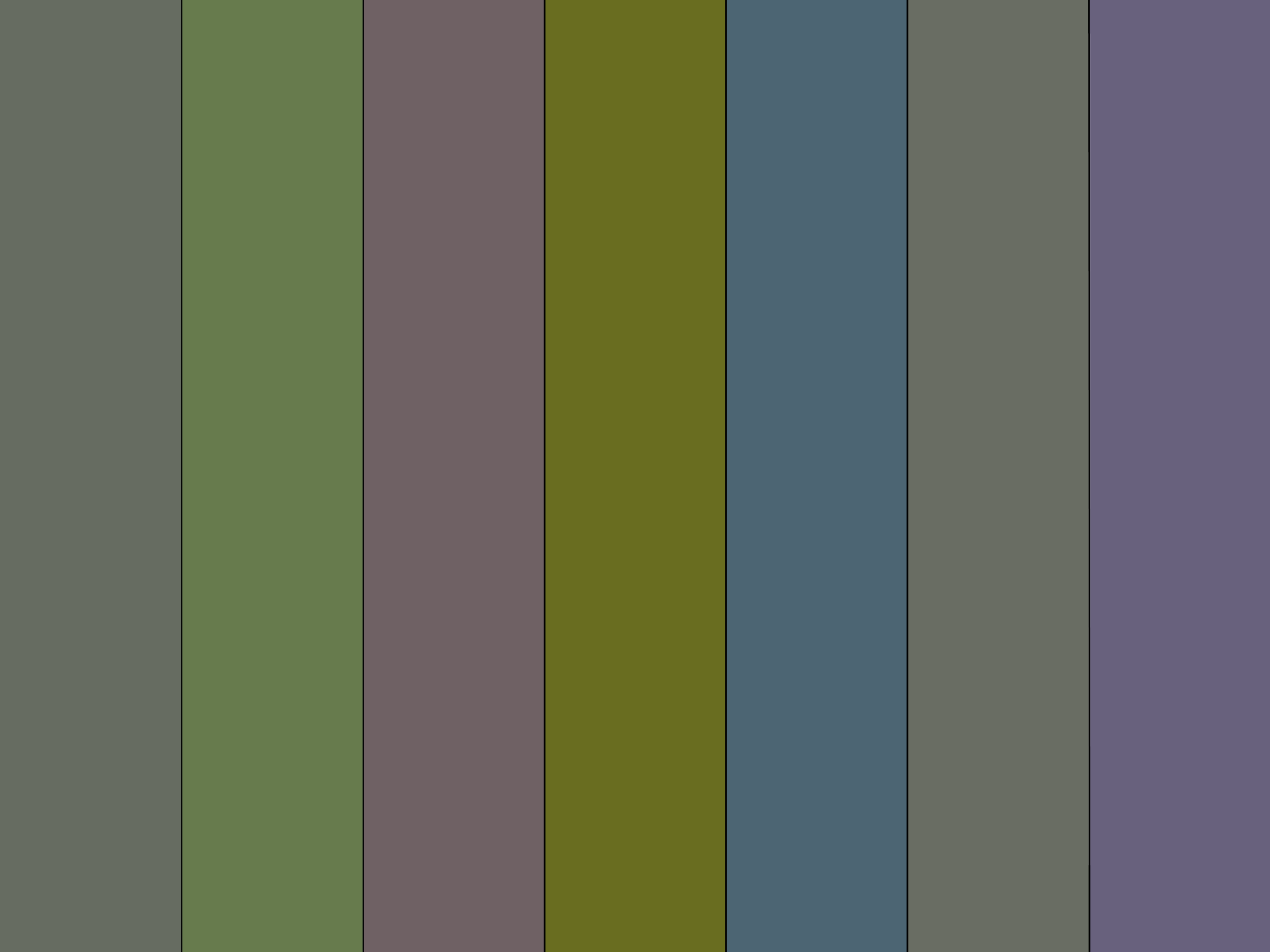
ויש לנו את הסיסמה! כעת נוכל לחלץ את הקבצים מהארכיב:



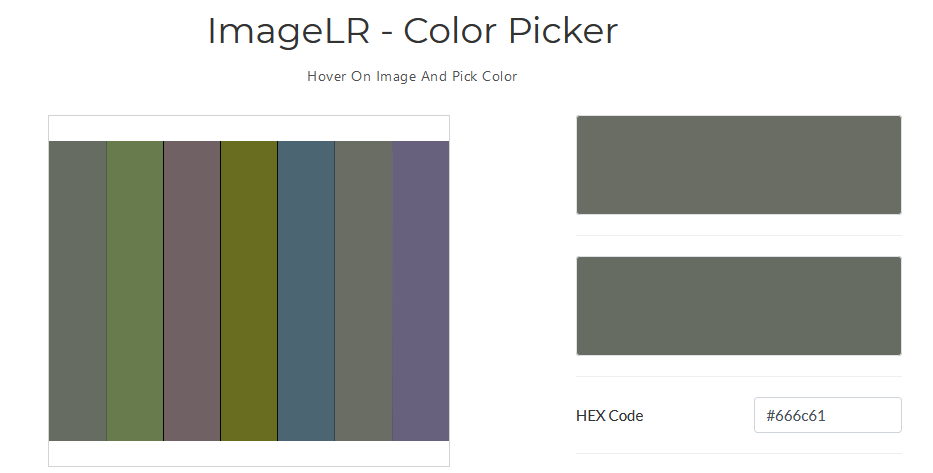
קיבלנו את התמונה Payload.png, וכעת נשאר רק חלק אחרון לפיתרון האתגר.

צבעים ומסרים

נסתכל על התמונה Payload.png:



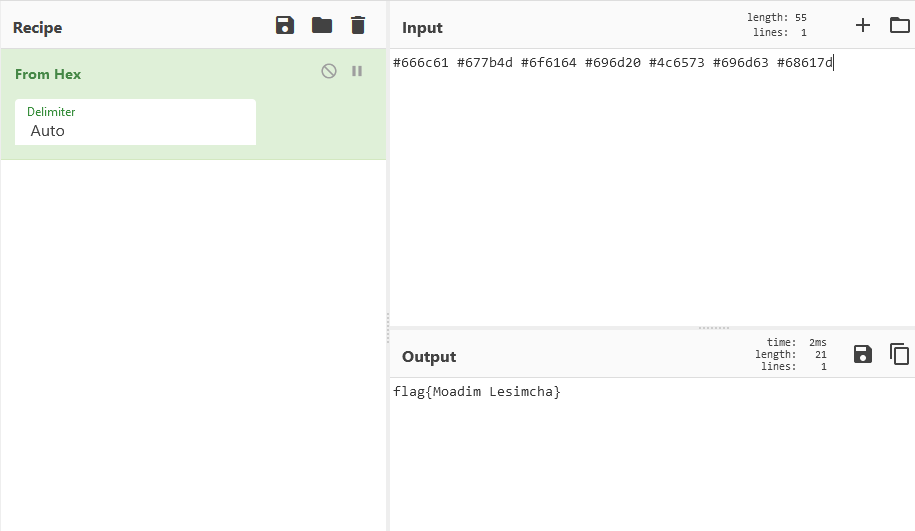
לא נראה כמו משהו מיוחד. לאחר נסיונות רבים עלה לדעתי לנסות להוציא את הערכים של הצבעים. בשימוש באתר <https://imagelr.com> ניתן לראות את הערכים ההקסדצימליים של הצבעים:



נעשה זאת בעבור כל הצבעים בתמונה ונקבל את הערכים:

#666c61 #677b4d #6f6164 #696d20 #4c6573 #696d63 #68617d

ניתן לראות שאם נחלק את הערכים של הצבעים לבייטים רובם יהיה בטווח 61-7E, טווח אשר מייצג את הערכים של האותיות קטנות באנגלית. ואכן, כאשר ממירים את הערכים לאותיות מתקבל הדגל!



**(https://gchq.github.io/CyberChef)**

סיכום

האתגר הזה היה ממש נחמד וקליל, ויכול להיות דרך טובה לאנשים שלא מכירים את תחום הסטגנוגרפיה לקבל הצצה אליו.