

**Where is**

**Ann?**

רקע

זוכרים את אן? הרשו לנו לרענן את זיכרונכם...זוהי אותה סוכנת FBI אותה פגשתם שנה שעברה בשעה תשע בבוקר.

מיד לאחר שהועברה לידיה החבילה, נעלמו עקבותיה כלא היו. בתום שנת כישלון של חיפושים אחרי אן, חזרו אליכם; איפה שהכול התחיל, בחזרה לרגעים שלפני העברת החבילה.

"אנו מאמינים שאן תקשרה עם המאהב הסודי שלה, מר איקס, בטרם עזבה" , אמר מפקד המשטרה במחוז רמת גן. עכשיו תורכם לעזור ולמצוא את הסוכנת הכפולה, ולמזלכם כל פעילות הרשת שלה תועדה עד לרגע היעלמותה, ויתכן ותיעוד החבילות יכיל רמזים למציאתה.

הקליקו פעמיים כדי להיכנס לקבצי הראיות (קבצי הסנפה pcap): 

האתגר

תפקידכם: מומחי רשתות  
משימתכם: לגלות מה היו ההתכתבויות האחרונות של אן במייל, למצוא לאן נעלמה, ולספק את הראיות הבאות:

1. מהי כתובת המייל של אן?
2. מהי הסיסמה התואמת לכתובת המייל של אן?
3. מהי כתובת המייל של המאהב הסודי של אן?
4. אילו שני פריטים ביקשה אן מהמאהב הסודי שלה להביא עמו?
5. מה שם הקובץ המצורף אותו שלחה אן למאהב במייל?
6. באיזה עיר וארץ קבעו להיפגש? כלומר, היכן אן אמורה להיות איתו ברגעים אלו?

כלי עזר אופציונליים

1. <https://www.base64decode.org/>
2. WireShark
3. HxD בחבילת ה – Heights.

הנחיות עזר

1. פלטרו את הפקטות על פי הפרוטוקול הרצוי (כדי לגלות באיזה פרוטוקול רלוונטי משתמשים בתקשורת זו, תוכלו לגשת בווירשארק ל"statistics" ו"protocol hierarchy". בחרו את המתאים מהרשימה וסננו על פיו).
2. היעזרו ב- Follow TCP Stream
3. נסו להבין כיצד הפרוטוקול שמצאתם עובד ולאפיין אותו (תוכלו להיעזר בספר הלימוד או לחילופין באינטרנט)
4. בתרגיל אותנטיקציה מעל HTTP השתמשנו בקידוד – אותו הדבר גם כאן. מומלץ לתרגל את הקידוד דרך כתיבה פייתונית (ולא רק דרך שירותי האתר המצורף לעיל)