ניתוח הסנפות עם Python

תרגילים

1) פתחו את הקובץ CaptureFile.cap. הכנסו לפקטה הראשונה בקובץ.
   a. מה הבית הראשון בפקטה?
   b. מה אורך הפקטה בבתים?

2) כתבו סקריפט Python שעובר על הקובץ CaptureFile.cap, ומדפיס למסך:
   a. את כמות הפקטות בהן הופיעה המחרוזת "google".
   b. את כמות הפקטות בהן הופיעה המחרוזת "ynet".
   c. את כמות הפקטות בהן הופיעה המחרוזת " SuperPhramLogo. gif".
   d. את כמות הפקטות בהן הופיעה המחרוזת "HelloWorld".
   e. שימו לב: הסקריפט לא צריך לקבל שום ארגומנט.

3) כתבו סקריפט שעובר על הקובץ CaptureFile.cap ומדפיס כמה פקטות יש בו.

4) כתבו סקריפט Python שעובר על הקובץ CaptureFile.cap ומוצא את הפקטה הגדולה ביותר בו. על הסקריפט להדפיס את המספר הסידורי של הפקטה בקובץ (הפקטה הראשונה – 1, הפקטה השנייה – 2 וכך הלאה) ואת הגודל שלה.

5) כתבו סקריפט Python שעובר על הקובץ CaptureFile.cap ומוצא את הפקטה הקטנה ביותר בו. על הסקריפט להדפיס את המספר הסידורי של הפקטה בקובץ (הפקטה הראשונה – 1, הפקטה השנייה – 2 וכך הלאה) ואת הגודל שלה.

6) כתבו סקריפט שעובר על הקובץ CaptureFile.cap, ועבור כל פקטת HTTP GET מוציא את הערך בשדה ה-Host.
   a. שים לב: עבור תרגיל זה מספיק "לסנן" פקטות HTTP GET בהינתן המחרוזת " GET" בפקטה.

תרגילים מתקדמים

7) בקובץ ההסנפה קיימת פקטה בה מועברים שם משתמש וסיסמא. מצאו את הפקטה וחלצו מתוכה את שם המשתמש והסיסמא.

8) כתבו סקריפט שמדפיס את המספר הסידורי של כל פקטות ה-DNS בקובץ CaptureFile.cap.
   a. איך זיהיתם אילו פקטות הן פקטות DNS?

9) כתבו סקריפט שמדפיס את המספר הסידורי רק של פקטות ה**שאלה** (query) של DNS בקובץ CaptureFile.cap.
   a. איך זיהיתם אילו פקטות הן פקטות שאלה?

10) כתבו סקריפט שמדפיס את שם הדומיין אליו מופנית שאלת ה-DNS.

בהצלחה!