****

**The Department of Information Systems Engineering**

**אבטחת מחשבים ורשתות תקשורת**

**עבודה מס' 1**

**הוראות הגשה**

* לעבודה יש שני חלקים.
* את החלק הראשון (WIRESHARK), אתם מתבקשים להגיש עד לתאריך 20/5/19 בשעה 23:00 במערכת מודל לתיבת ההגשה המתאימה.
* את החלק השני (קריפטוגרפיה), אתם מתבקשים להגיש עד לתאריך 10/4/19 בשעה 23:00 במערכת מודל לתיבת ההגשה המתאימה.
* יש להגיש את כל קבצי העבודה לתיבת ההגשה המיועדת במודל, מכווצים ב ZIP כאשר שם הקובץ מכיל את שתי הת.ז של בני הזוג מופרדים בקו תחתון. לדוגמא: ass1\_id1\_id2.zip
* שאלות על העבודה יש לשאול בפורום העבודה במודל.
* כל יום איחור יוריד 5 נקודות מציון העבודה.
* הארכות ינתנו רק במקרים מיוחדים.

**חלק א – WIRESHARK**

בשאלות הבאות תלמדו לחקור קובץ PCAP שמכיל הקלטה של משתמש ולהסיק מה המשתמש עשה בגלישתו. לטובת השאלה הנ"ל יש להתקין [WIRESHARK](https://www.wireshark.org/)  על המחשב.

אנא הורד את הקובץ mystery.pcapng [מהקישור הבא](https://drive.google.com/file/d/1ChJacmsbwGPFb9vdjEy6qsgvvh4vYrAR/view?usp=sharing)

טען את הקובץ PCAP המצורף לעבודת בית (mystery.pcapng) ב - WIRESHARK. הקובץ הנ"ל מכיל הקלטה (פקטות שנשלחו והתקבלו) של משתמש. ידוע כי במהלך ההקלטה שבוצעה המשתמש ביצע את ארבעת הפעולות הבאות: גלש ב-YNET, גלש ב-ONE, והוריד פעמיים קבצים של סרטים שצולמו באיכות 4kמגוגל דרייב.

**שאלה מס' 1 (15 נק'):**

היכנס לStatistics -> I/O Graph .

הצג את כמות הנתונים שנצרכה במהלך ההקלטה ע"י בחירת השדה המתאים.

1. מה ה- display.filter שהשתמשת? **(5 נק')**
2. הוסף צילום מסך של הגרף עם אגרגציה של 10 שניות. **(5 נק')**

חזור לארגרגציה של שניה בודדת.

1. האם ניתן להפריד בין הסשנים של הגלישה באתרי אינטרנט לסשנים של הורדת הקבצים על בסיס ניתוח ויזואלי של הגרף? **(5 נק')**

**שאלה מס' 2 (10 נק'):**

1. איך ניתן לזהות איזה מהסשנים שייך לכל אתר אינטרנט? **(2 נק')**
2. אחרי כמה שניות מתחילת ההקלטה נכנס המשתמש לאתר ONE? **( 2נק')**
3. אחרי כמה שניות מתחילת ההקלטה נכנס המשתמש לאתר YNET? **( 2נק')**
4. באיזה אתר נוסף ביקר המשתמש בתחילת ההקלטה? **( 2נק')**
5. השלם זמני התחלה וסיום של הפעולות שביצע המשתמש **( 2נק')**:

|  |  |  |
| --- | --- | --- |
|  | זמן התחלה (שניות מתחילת ההקלטה) | זמן סיום (שניות מתחילת ההקלטה) |
| הורדת וידאו ראשון |  |  |
| הורדת וידאו שני |  |  |
| גלישה ב-YNET |  |  |
| גלישה ב- ONE |  |  |