Assignment 1

1)

1.1)

tcp and ip.src == 216.58.210.234 and frame.time_relative >= 30 and frame.time_relative < 31

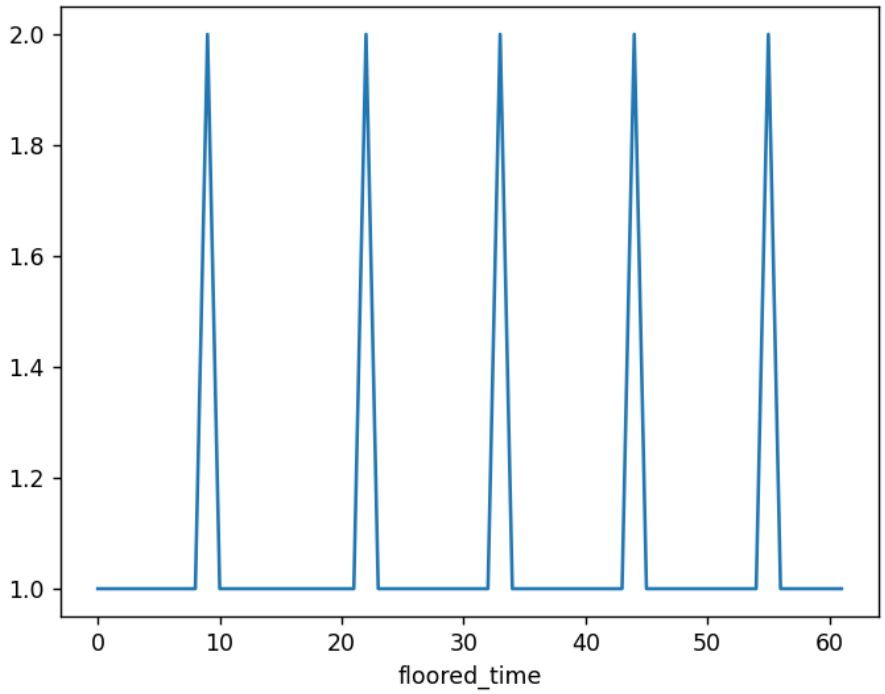
450 items

1.3) ip.src == 216.58.210.234, **2914 bytes**

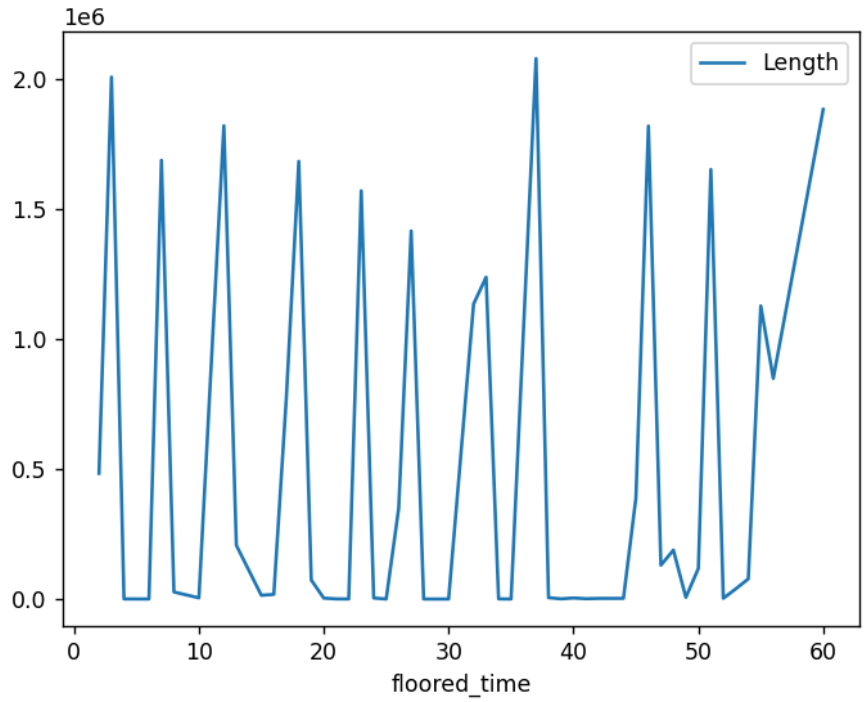
1.4) ip.src == 216.58.210.234, **54 bytes**

1.5) DNS - www.google.com, www.ynet.co.il, www.google.co.il

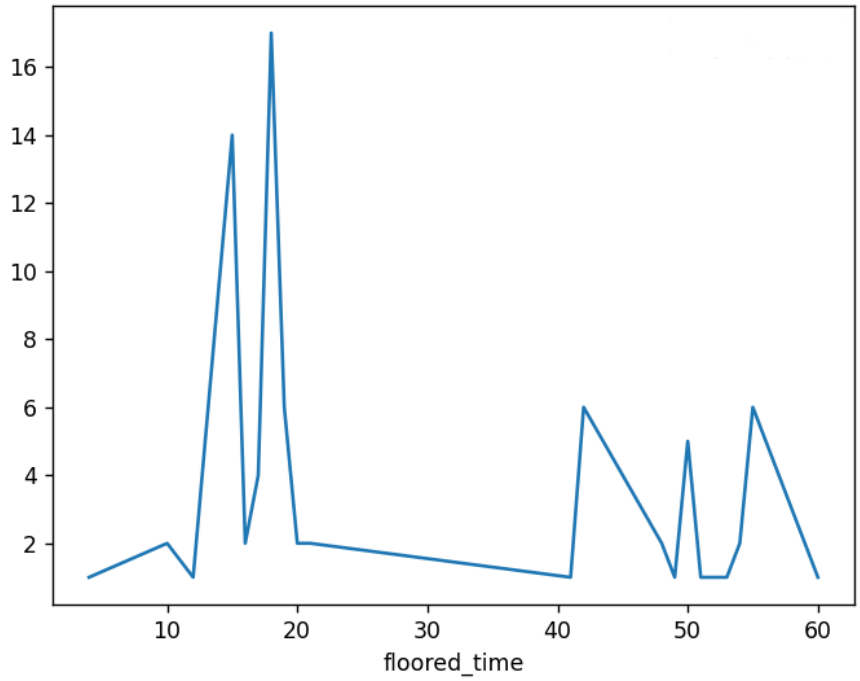
2.1) ip.src == 216.58.204.10



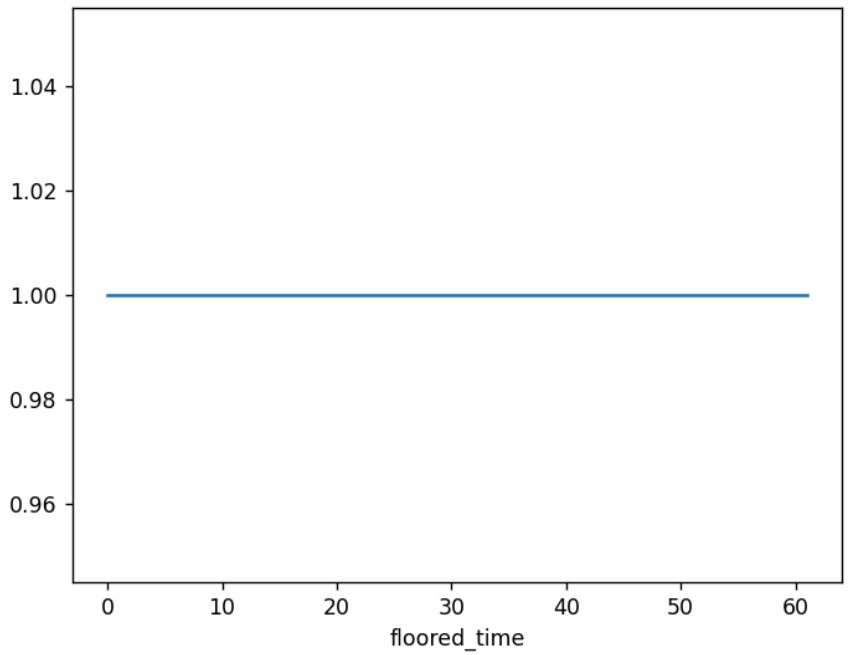
2.2) ip.dst == 10.100.102.6 and udp



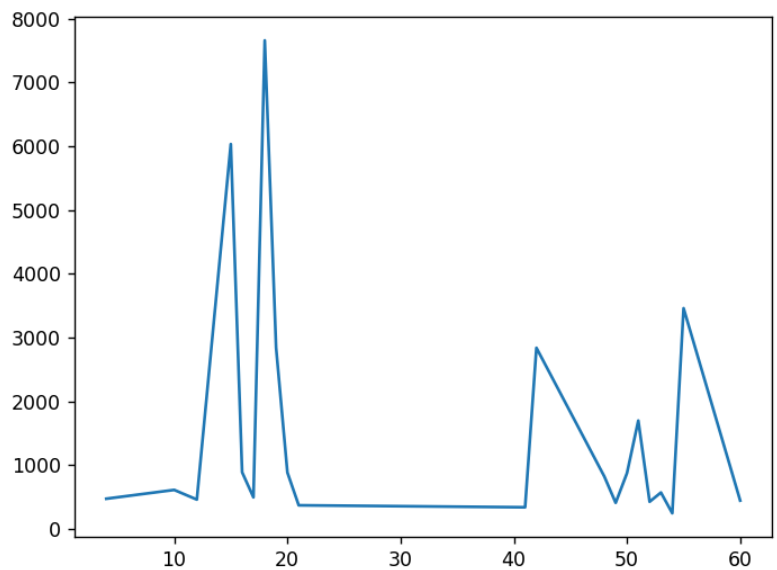
2.3) ip.dst == 10.100.102.1 and dns



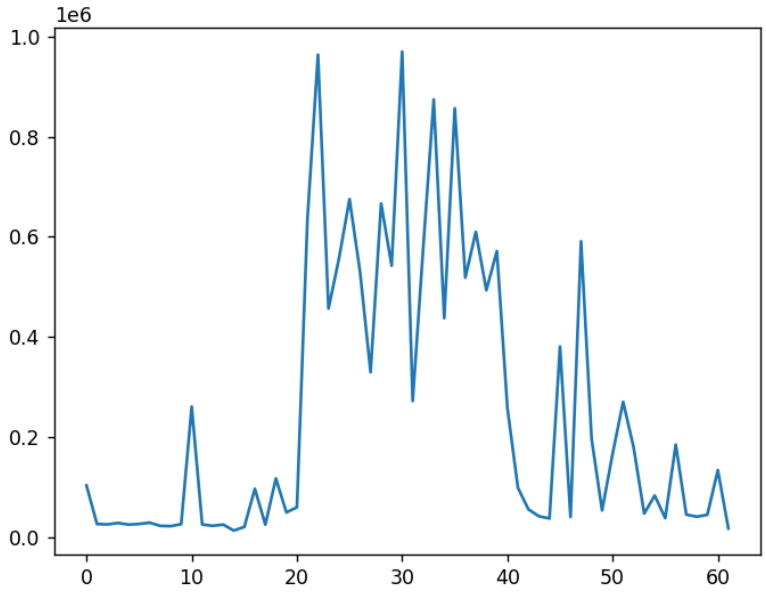
2.4) ip.src == 216.58.204.10



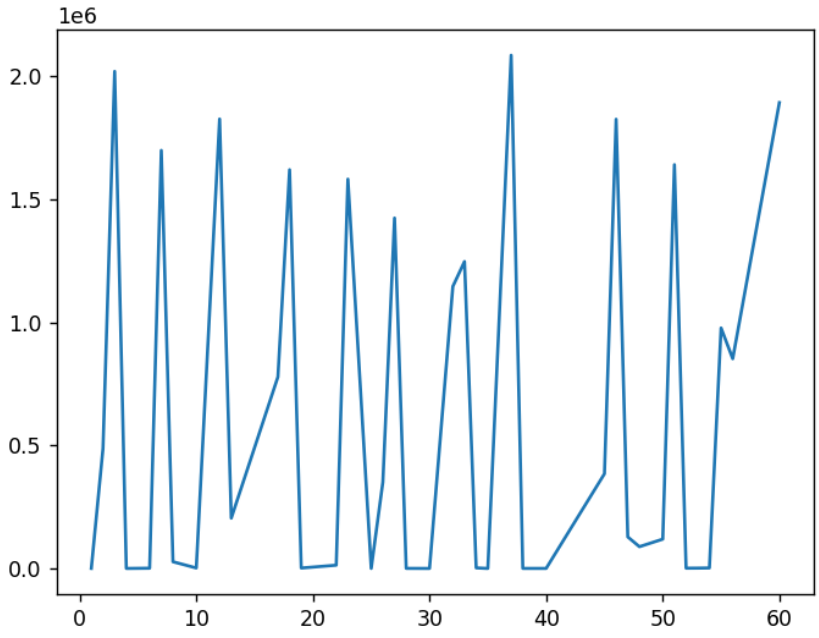
2.5.1) DNS



2.5.2) TCP



2.5.3) UDP



2) a.

Legend –> M = message, C = cipher of M with AES_2, Key1, Key2

We will talk only on 1 block of 16 bytes data.

We can see that C = $AES_1(AES_1(M)_{k1})_{k2}$, that means C = XoR (Swap(XoR (Swap(M), K1)),K2)

Because we talk on block of 4x4 bytes then we will talk in format - M[i,j],

We can see the C[i,j] = M[i,j] XoR K1[j,i] XoR K2[i,j] , so we will XoR C[i,j] from left and K2[i,j] from right and we get the equation : K2[i,j] =C[i,j] XoR M[i,j] XoR K1[j,i] . We got C, M and K2 becomes function of K1, so we will make K1 constant 1, and then instantly we have K2.

3) a.

Ciphertext-only attack - is an attack model for cryptanalysis where the attacker is assumed to have access only to a set of ciphertexts.

Known-plaintext attack - is an attack model for cryptanalysis where the attacker has access to both the plaintext, and its encrypted version (ciphertext).

Chosen-plaintext attack - is an attack model for cryptanalysis which presumes that the attacker can obtain the ciphertexts for arbitrary plaintexts. The goal of the attack is to gain information that reduces the security of the encryption scheme.

Chosen-ciphertext attack - is an attack model for cryptanalysis where the cryptanalyst can gather information by obtaining the decryptions of chosen ciphertexts. From these pieces of information, the adversary can attempt to recover the hidden secret key used for decryption.

b.

As we saw the example in PS-4 on attacking RSA with 2 messages and their cyphers:

RSA has Multiplicative attribute, that means RSA {M1 * M2}n,e = RSA {M1}n,e * RSA {M2}n,e

And, RSA^{-1}\{C1 * C2\}n,d = , RSA^{-1}\{C1\}n,d * , RSA^{-1}\{C2\}n,d.

With this in mind, we can increase our pairs by doing the following: We use our C2 and C1, and for every C that suffices this equation: C2 = C/C1mod(n), We can add C and his decrypted message to our pairs. We know C1 and C2 decryptions, so we know M = M1 * M2 mod(n).

The attacker cannot exploit this attack if M1*M2 is bigger than the maximus block size used in RSA encryption.

We can mitigate this attack with reversable Cryptographic hash function by using it on our encrypted message and then send it.

4) a.

הבעיתיות שנוצרה בהגדרת הפרוטוקול היא שהוא פגיעה למתקפות man in the middle, כמו שהוסבר בביתה, התוקף יקבל את ההודעות עם המפתחות וישלח מפתח חדש משלו לכל צד וכבה הוא ינתר וישבש את התקשורת ביניהם.

b.

כדי להתגבר על הבעייתיות ניתן להוסיף חתימה דיגיטלית למפתחות ,וכך למנוע את המתקפות של MITM. בנוסף למפתח הפרטי המוצפן שאליס או בוב ירצו לשלוח, יהיה עוד שלב של חתימה דיגיטלית להודעה בעזרת המפתח הפרטי של השולח, והמקבל יוודא את ההודעה בעזרת המפתח הפומבי של השולח. כך נוכל למנוע התערבות של צד שלישי מכיוון שאם ישנה את תוכן ההודעה בין אם ישאיר את החתימה הקודמת או שיעשה אחת משלו, המקבל יצליח לזהות שהייתה בעיה מכיוון שלתוקף אין את המפתח הפרטי של השולח, וניתן לוודא הודעה שהוצפנה עם מפתח פרטי רק בעזרת המפתח הפומבי של השולח.

5)

a.

מכיוון שיש גישה לתיקיית ה-tmp נוכל לתקוף שם בעזרת שיטת meet-in-the-middle כמו שלמדנו ב-DES2. לצורך התרגיל נניח שיש לנו 3 הודעות ושלוש קריפטוגרמות שלהם: (M1,C1), (M2,C2), (M3,C3).

נשלח הודעה M ונגנוב את ההצפנה שלה C11, נעבור על כל הקומבינציות האפשריות כמו שלמדנו בביתה ע"י הצפנה של M כמו שרשום בתרגיל ונתרגם את C11 גם עם כל הקומבינציות וע"י lookup table נוכל למצוא את הקומבינציות האפשריות ל-K1 ו-K2, נריץ הצפנה עם הקומבינציות האפשריות שמצאנו ונמצא את המפתחות האמיתיים. לגבי K3,K4,K5 נפצח אותם בעזרת MITM, ניצור טבלא לכל ההצפנות האפשריות של C11 עם K3 ולאחר מכן נפענח את C עם כל הקומבינציות האפשריות של K4, K5, נחפש התאמה בטבלא החדשה שלנו ולכל התאמה נבדוק שאכן היא טובה ע"י הצפנה של M2, M3 ובדיקה שהקריפטוגרמות שלהם מתאימות לפלט שיצא לנו.

זמן ריצה: $O(2^{112})$, להצפנה + פענוח + חיפוש של 3 המפתחות האחרונים, הראשונים לוקחים $O(2^{56})$ לכן לא רלוונטי לחישוב. זכרון: $O(2^{56})$, טבלאת ה-lookup פעמיים.

b.

נתקוף שוב באמצעות MITM רק הפעם מהכיוון השני, מכיוון שיש לנו 2 זוגות מפתחות זהים לכן הזמן יהיה זהה לתקיפת MITM של 3DES כמו בסעיף הקודם. נפענח את C1 עם כל האופציות האפשריות של K3 וניצור טבלא, ולאחר מכן נצפין את M1 עם כל הקומבינציות של K1, K2 ונחפש התאמות בטבלא. בכל פעם שתהיה התאמה בטבלא נצפין M2, M3 ונשווה עם הקריפטוגרמות שלהם, אם תהיה התאמה מצאנו את המפתחות.

זמן ריצה: $O(2^{112})$, בדומה לסעיף הקודם. זכרון: $O(2^{56})$, טבלאת ה-lookup.

c.

ניתן לראות שהמפתח הראשון והשני זהים לכן C11 = M1, לכן אין צורך אפילו לפצח את K1, נשאר לפצח את 3 המפתחות הנותרים, ואפשר לראות שזוהי הצפנת 3DES בעזרת MITM כמו בסעיפים הקודמים למפתחות K2, K3, K4. ולכן הזמן ריצה: $O(2^{112})$, זכרון: $O(2^{56})$.