

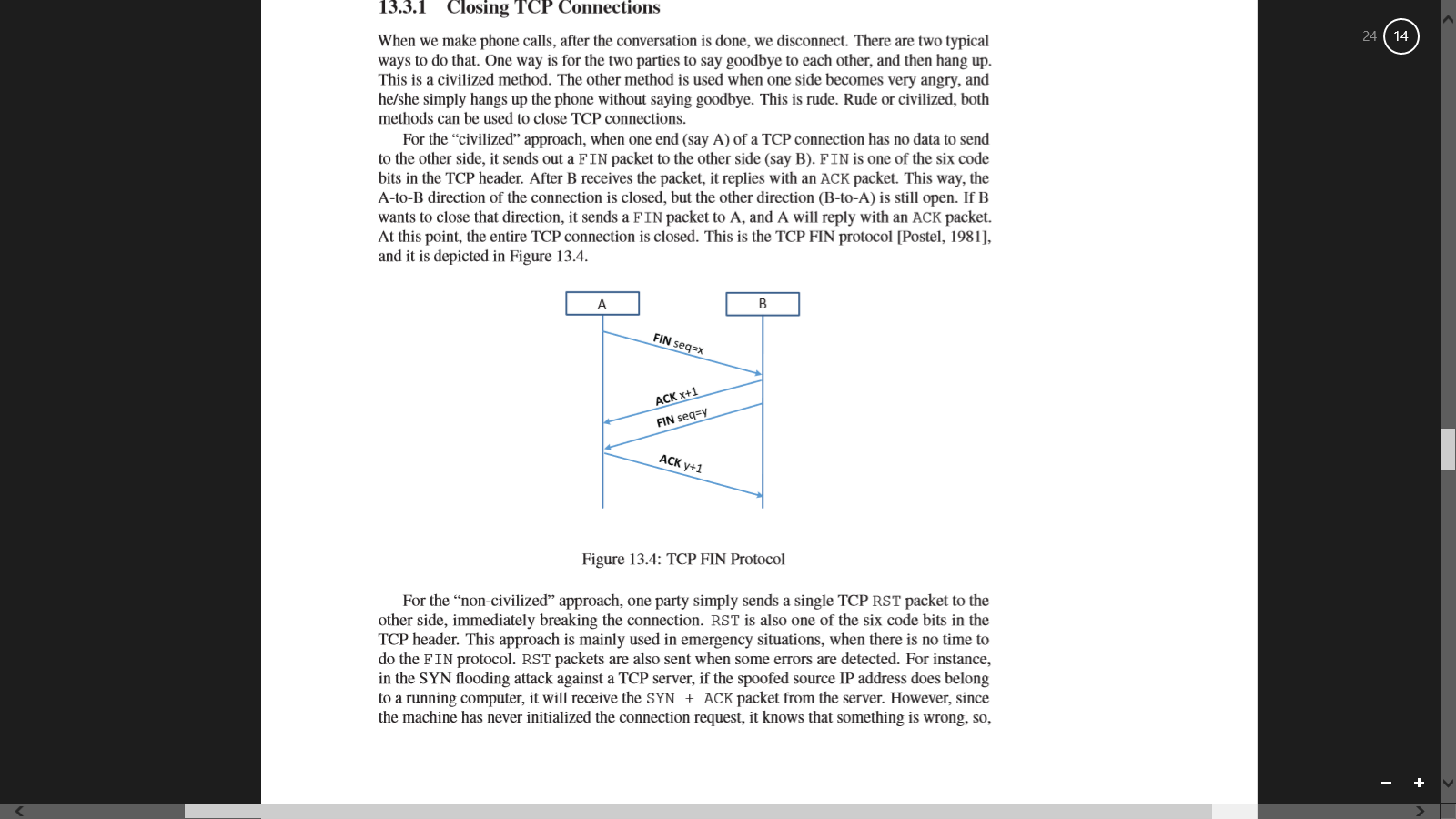
**מעבדה מספר 2**

**Reset-Attack**

**אופן סגירת קשר TCP**

כמו בכל סוג תקשורת לאחר סיום השיחה, כלומר לאחר שלשני הצדדים אין עוד מידע להעביר, מתבצע ניתוק של הקשר. ניתן לנתק את הקשר על ידי דרך "מסודרת", כלומר, כאשר שני הצדדים מסכימים על ניתוק הקשר, או בדרך "לא מסודרת", כלומר על ידי ניתוק חד צדדי של הקשר. כך הדבר גם בקשר TCP.

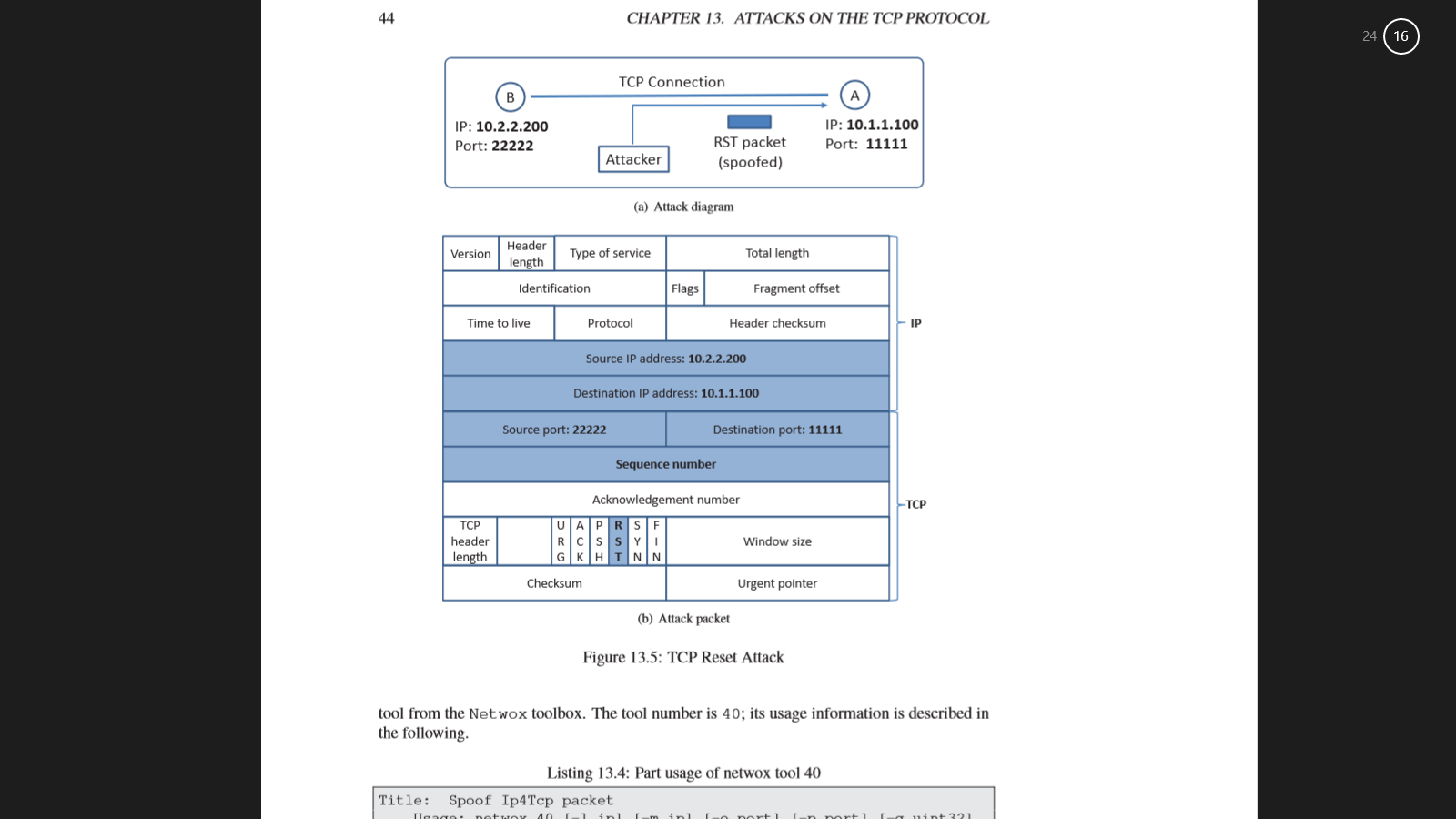
ניתוק "מסודר" של קשר TCP: כאשר לאחד הצדדים ( צד A) בקשר TCP לא נותר עוד דאטה להעביר, הוא שולח פאקטת FIN, בה ביט ה – FIN הינו "למעלה". FIN הינו אחד מששת הביטים ב – TCP header, עליהם הסברנו במעבדה הראשונה. בקבלת הפאקטה, צד B עונה עם פאקטת ACK ובצורה זו נסגר הקשר מצד A לצד B. יש לשים לב כי הקשר מצד B ל- A עדיין הינו פתוח בשלב זה. במידה וירצה גם צד B לסיים את הקשר, הוא ישלח פאקטת FIN משלו שצריכה להיענות על ידי פאקטת ACK מצד A. משזה נעשה, קשר ה-TCP בכללו, יחשב כסגור.

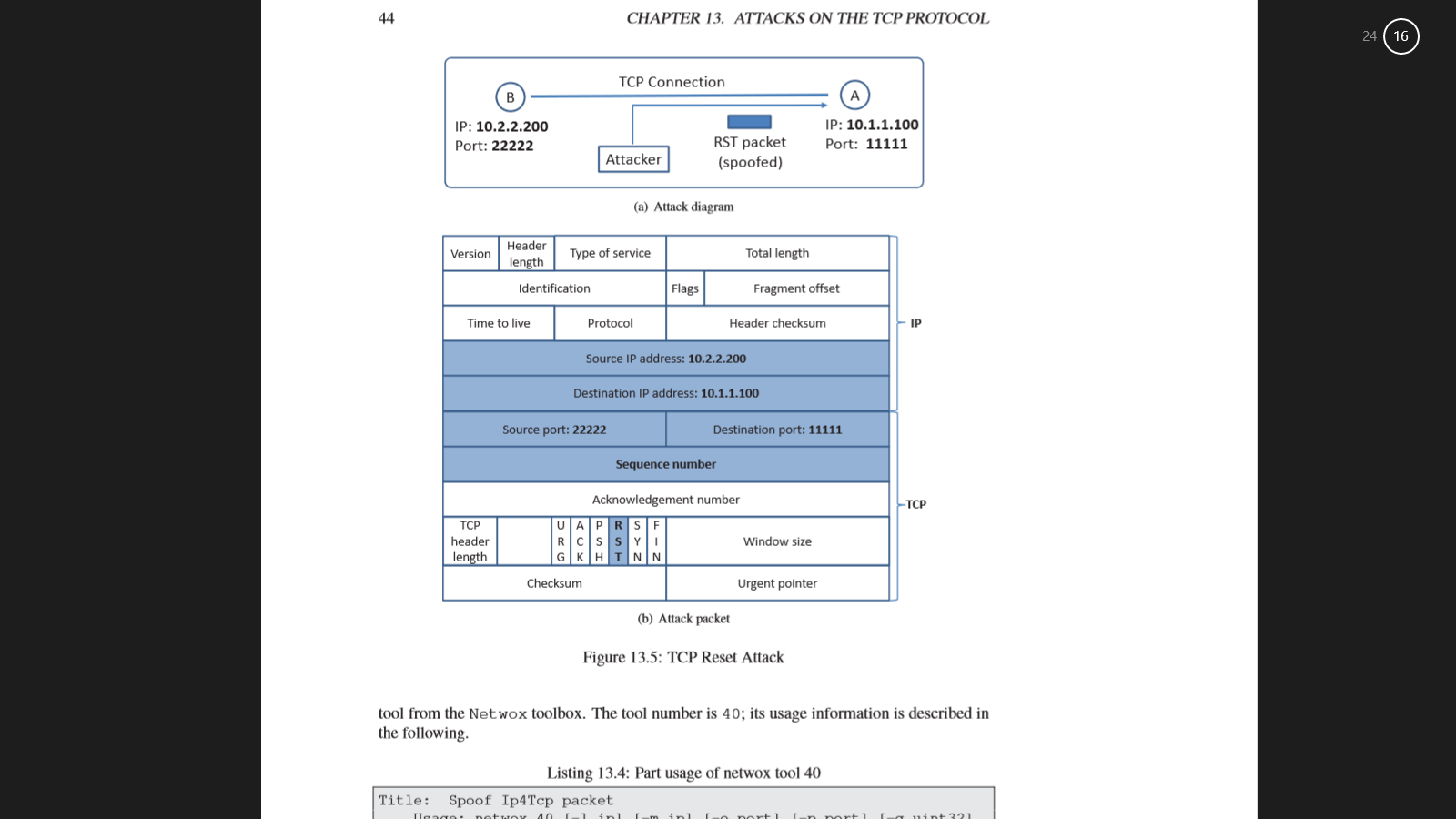


ניתוק "לא מסודר" של קשר TCP: אחד הצדדים שולח פאקטת RST, בה ביט ה – RST הינו "למעלה", וסוגר את הקשר באופן מיידי. RST הינו אחד מששת הביטים הנמצאים ב- TCP header ונלמדו במעבדה הראשונה. אופן סגירת קשר זה מתבצע בעיקר בעיתות חירום כאשר אין זמן לביצוע הפרוטוקול ה"מסודר". פאקטת ה-RST נשלחת גם לעיתים במקרה של שגיאות. למשל, במקרה של מתקפת SYN-Flood, אם אחת הפאקטות המזוייפות, נשלחת לכאורה מכתובת IP קיימת, ישלח השרת לכתובת זו פאקטת SYN + ACK. המחשב היושב באותה הכתובת, לא ניסה ליצור שיחה עם השרת ולכן עם קבלת הפאקטה, כחלק מהפרוטוקול, הוא ישלח לשרת כתשובה פאקטת RST, אשר מודיעה לשרת כי יש לסגור את הקשר החצי-פתוח ועל ידי כך לשחרר את המשאבים המוקצים לקשר זה. זו דוגמא אחת לנחיצות פאקטת ה–RST בקשרי TCP.

**אופן ביצוע Reset-Attack**

כפי שראינו, כל שצריך על מנת לסגור תקשורת TCP הינו פאקטת RST אחת. לכן, כל שצריך תוקף לעשות הינו לזייף ולשלוח פאקטת RST מצד אחד לשני. יחד עם זאת, על מנת להצליח במתקפה, יש למלא חלק מהשדות בפאקטה במידע עדכני ונכון. כל תקשורת TCP מאופיינת על ידי השדות source IP address, source port, destination IP address, destination port. על כן, הפאקטה המזוייפת צריכה להכיל את השדות הנ"ל התואמים לקשר. בנוסף, על שדה ה – sequence number להיות בעל ערך עדכני, כדי שהפאקטה תחשב עדכנית בצד המקבל. מכאן, לצורך קבלת המידע הנחוץ לזיוף הפאקטה, תחילה יש להאזין על קשר קיים ו"לדוג" פאקטה מבין התקשורת המועברת. בכאשר הושגה פאקטה כזו, יש לזייף את הפאקטה ושולחה מהר מספיק, טרם תגובת הצד המקבל, על מנת שהמספר הסידורי שזייפנו יחשב עדכני.





**שיטת המנע**

זיוף פאקטות בקשר TCP מתאפשר מאחר וקידוד המידע בקשר מתבצע מתחת לשכבת ה – IP. לכן, המידע המכיל את הכתובות, הפורטים וביטי הבקרה, הנמצא ב – TCP header הינו חשוף ואינו מוצפן. אם נוכל להצפין את המידע כך שאך ורק כל אחד משני הצדדים שהקימו את הקשר יוכלו לאשר את אמינות הפאקטה, נוכל למנוע מתקפות RST עתידיות על הקשר המיוסד. לצורך כך נוצר פרוטוקול ה – Internet Protocol Security – Ipec, הכולל פרוטוקולים המאפשרים הצפנה ווידוא בין הצדדים בעת הקמת הקשר ובמהלכו. בעזרת IPsec, ניתן להעביר מידע באופן בטוח ויציב בין שני מחשבים, בעזרת קשר TCP.

לקריאה נוספת - <https://en.wikipedia.org/wiki/IPsec>

**שאלות חזרה בנושא Reset-Attack:**

1) תאר את כלל האפשרויות לסגירת התקשרות TCP. הסבר מדוע נחוצה הודעת ה – Reset בקשר TCP.

2) תאר את אופן ביצוע Reset attack. מהם הפרטים הנחוצים לתוקף עבור ביצוע המתקפה? כיצד ניתן להשיגם?

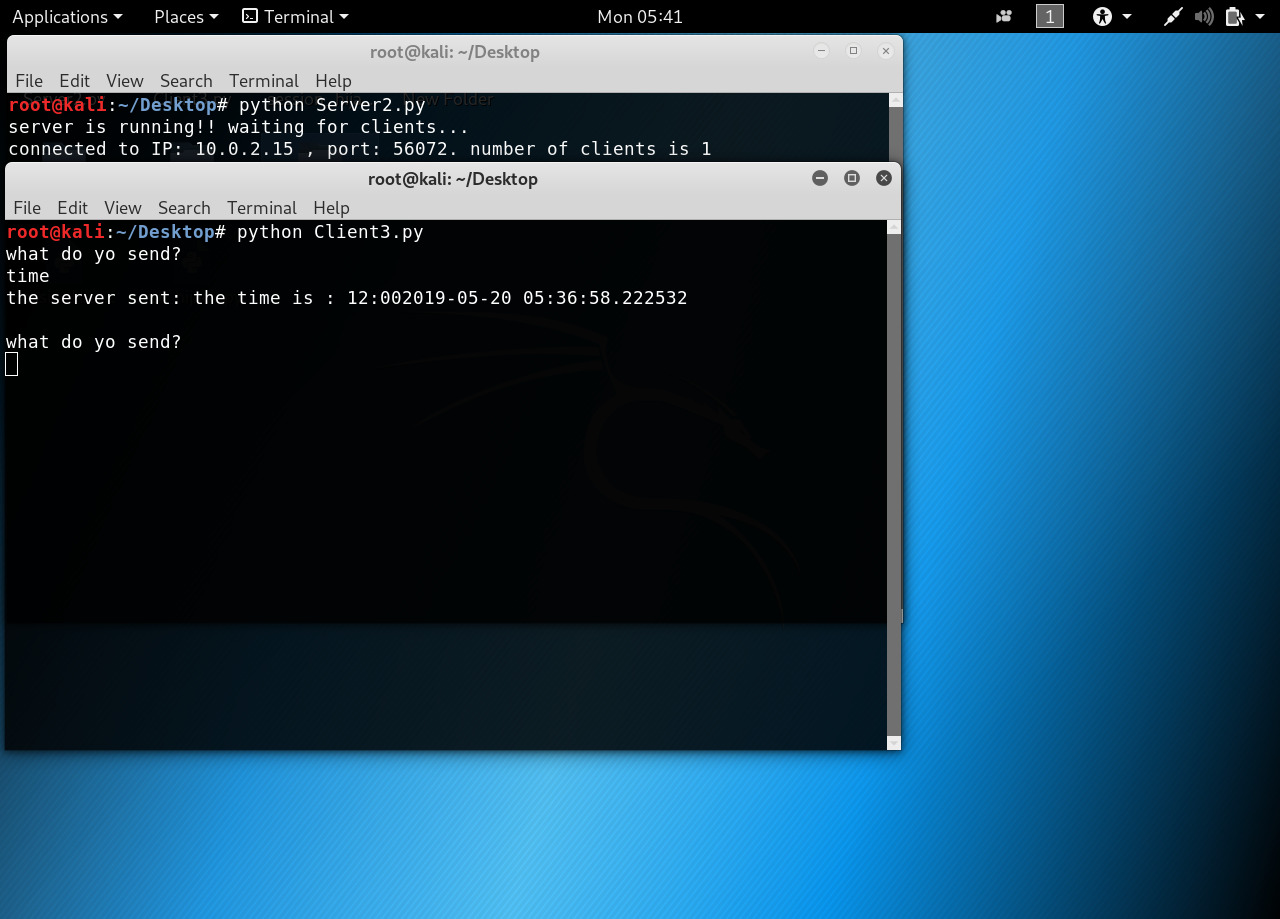
3) מהי נקודת התורפה המנוצלת עבור ביצוע המתקפה וכיצד ניתן למנוע ביצוע Reset Attack על התקשרות TCP? הסבירו והביאו דוגמאות.

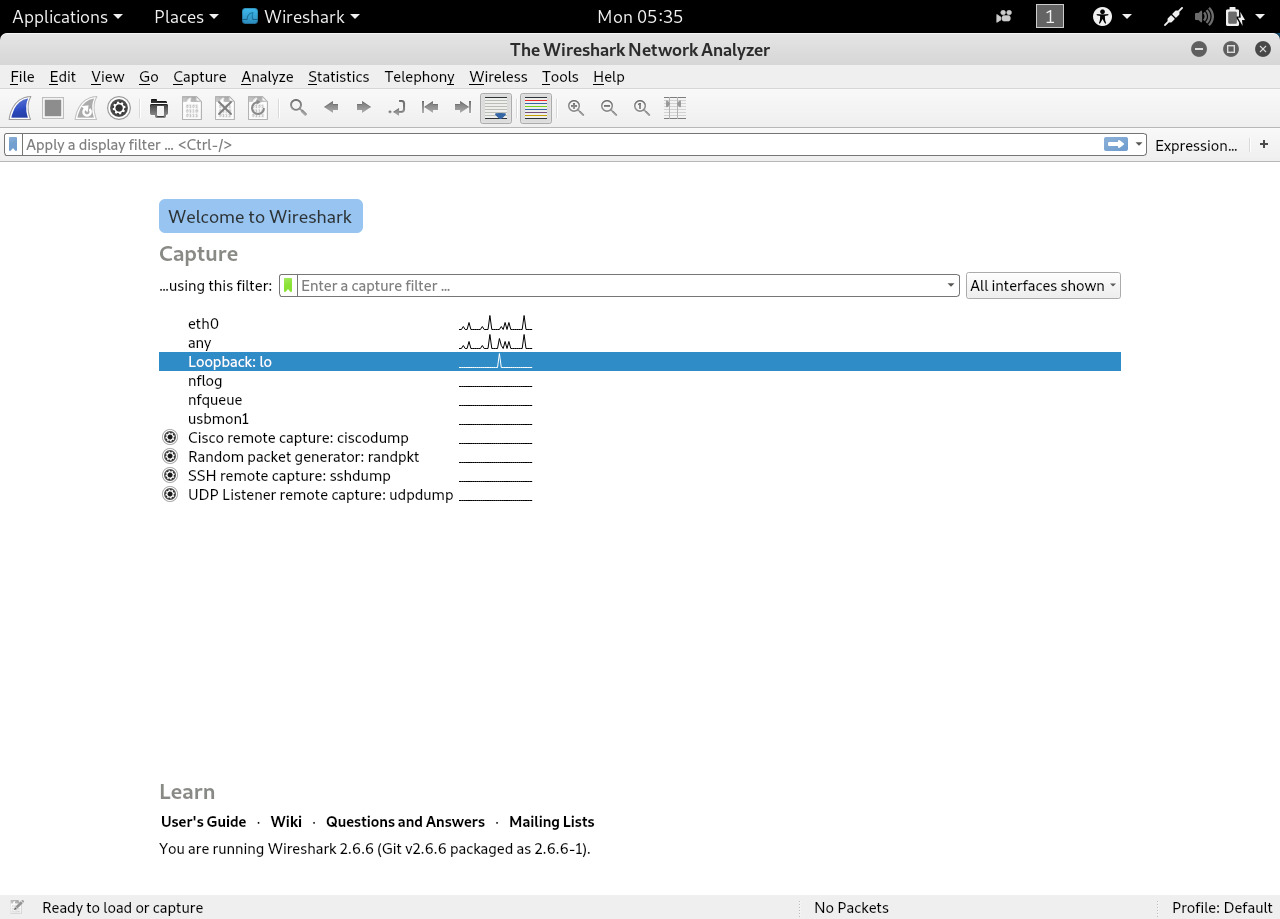
**כעת נבצע מתקפת Reset על השרת והלקוח שכתבנו במעבדה קודמת:**

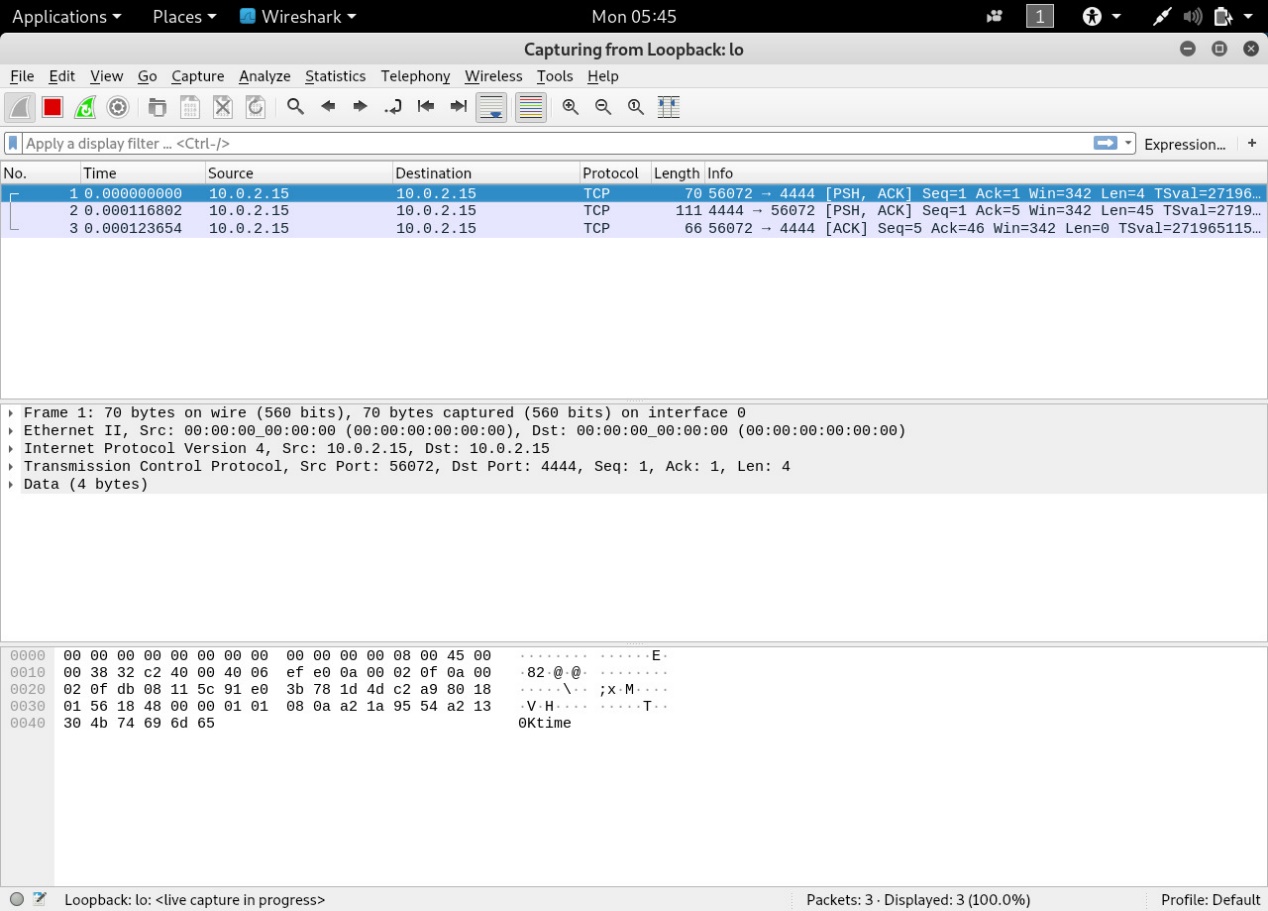
היכנסו לסביבת העבודה kali.

על מנת לבצע את המתקפה, עלינו לבחור את הפלטרפורמה עליה אחנו מאזינים (ethernet, lo, etc) ואת כתובת ה - IP של הקשר.

הריצו את השרת והלקוח מהמעבדות הקודמות. בעת התחברות הלקוח לשרת, תיכתב בחלון השרת הודעה המפרטת את פרטי הקשר, לרבות כתובת ה – IP.



למציאת הפלטפורמה עליה יש להאזין, פיתחו את תוכנת ה – wireshark ושילחו מספר הודעות מהלקוח לשרת. בעת שליחת ההודעה, ניתן לזהות ב- wireshark היכן מתבצעת התעבורה.



הורידו את הקובץ מהקישור קישור. שימרו את הקובץ על שולחן העבודה בסביבת kali.

פיתחו את התיקייה והריצו טרמינל מתוכה (לחיצה על לחצן ימני ובחירת Open In Terminal).

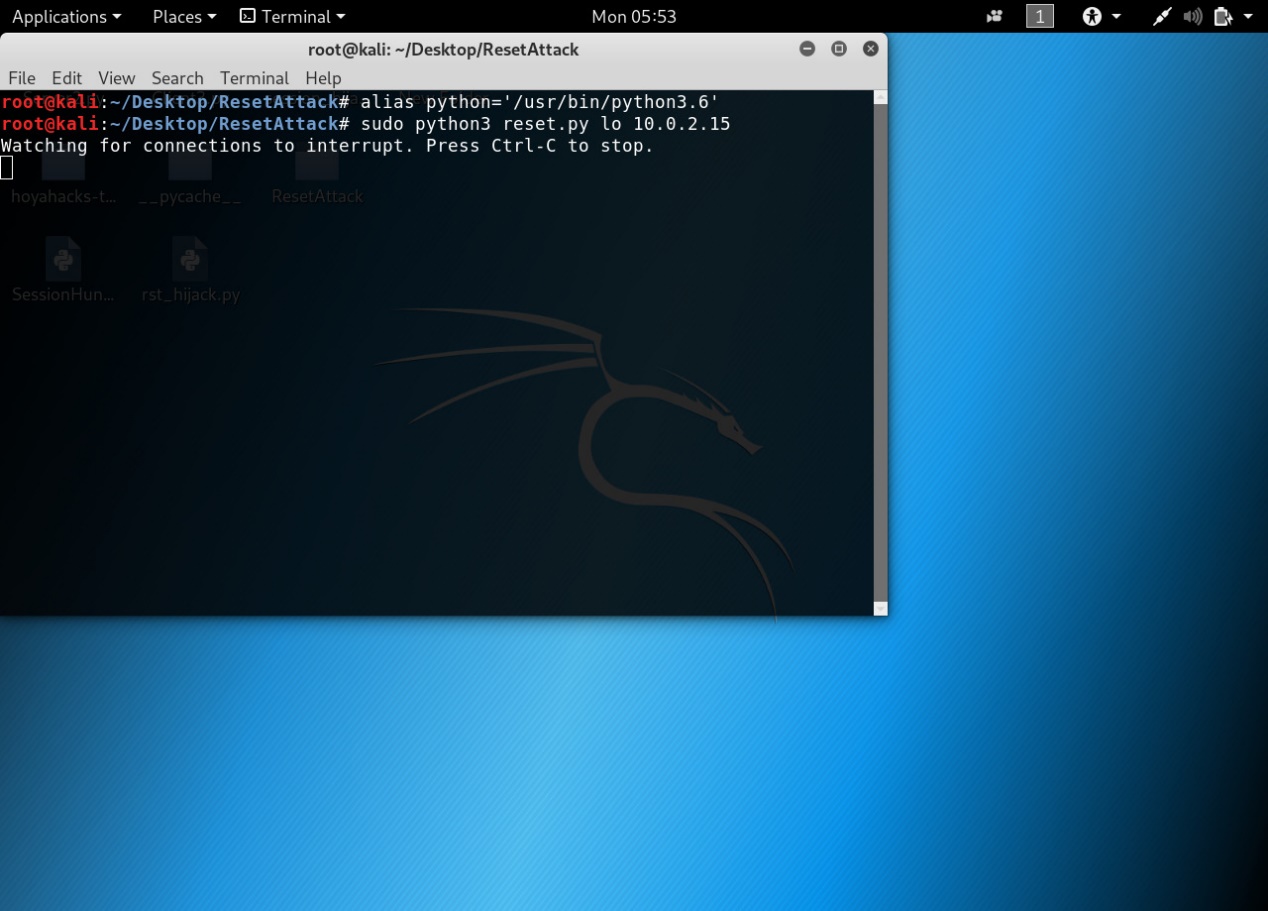
כדי להריץ את התוכנית עלינו להשתמש ב – python3.6. בטאמינל שפתחנו נירץ אץ הפקודה הבאה:

Alias python='/usr/bin/python3.6'

בכדי שהמתקפה תעבוד, עלינו להריץ את את קוד המתקפה עם הרשאות מערכת. רישמו בטרמינל את הפקודה הבא, תוך הזנת הארגומנטים המתאימים במקרה שלכם (פלטפורמה, IP):

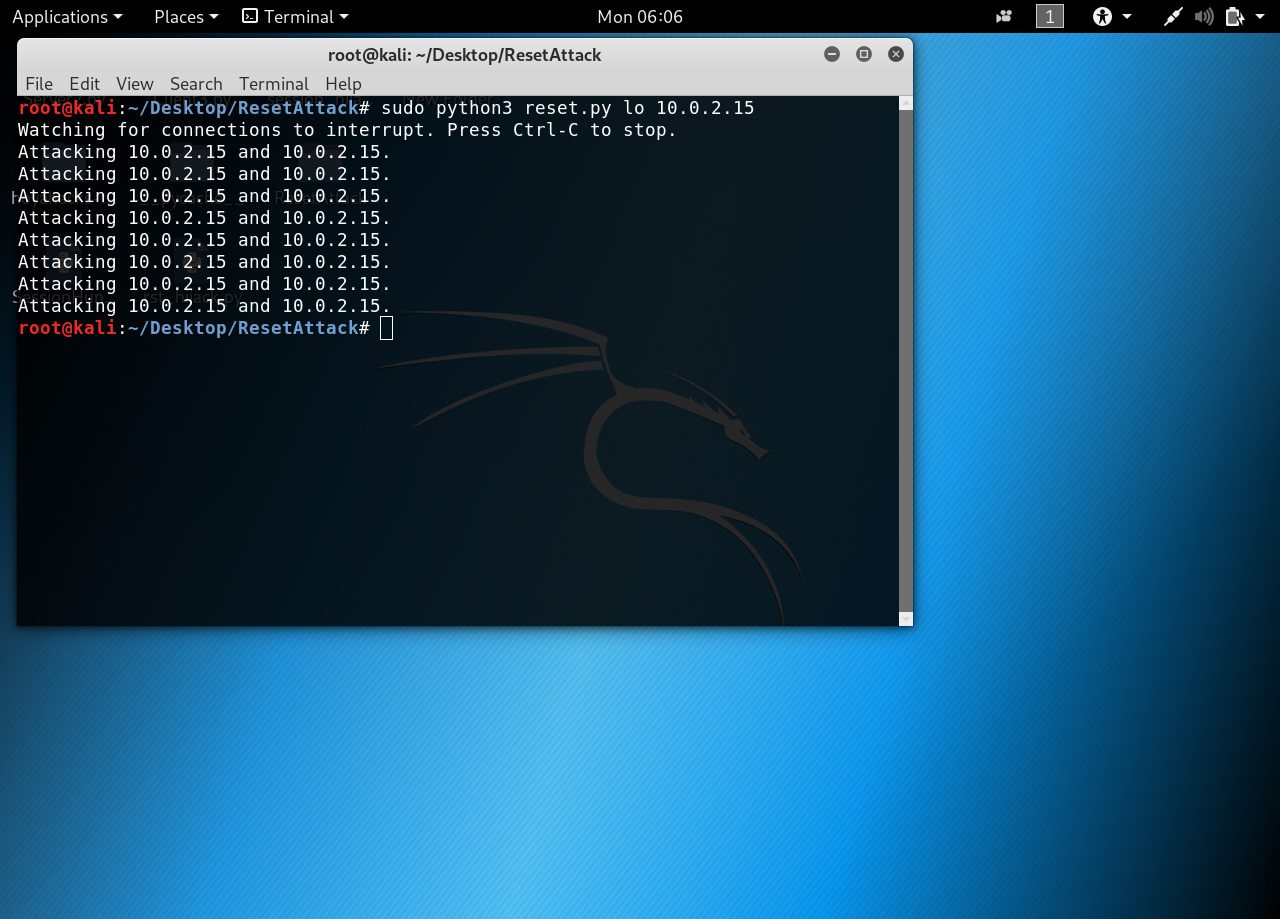
Sudo python3 reset.py (platform) (IP)

עתה, התוכנית רצה וממתינה לשליחת הודעה בפלטפורמה עליה היא מאזינה:

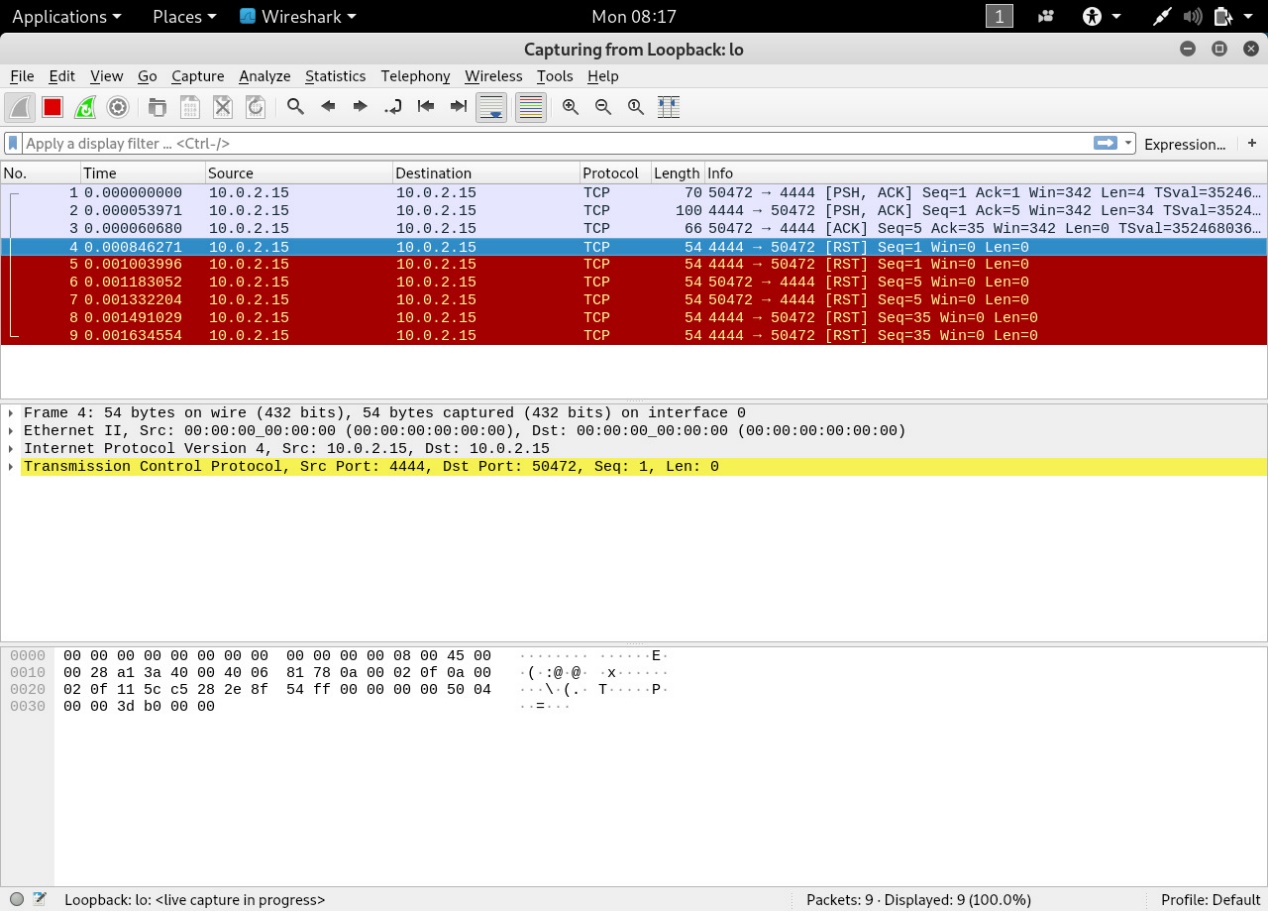


שילחו הודעה נוספת מהלקוח לשרת.

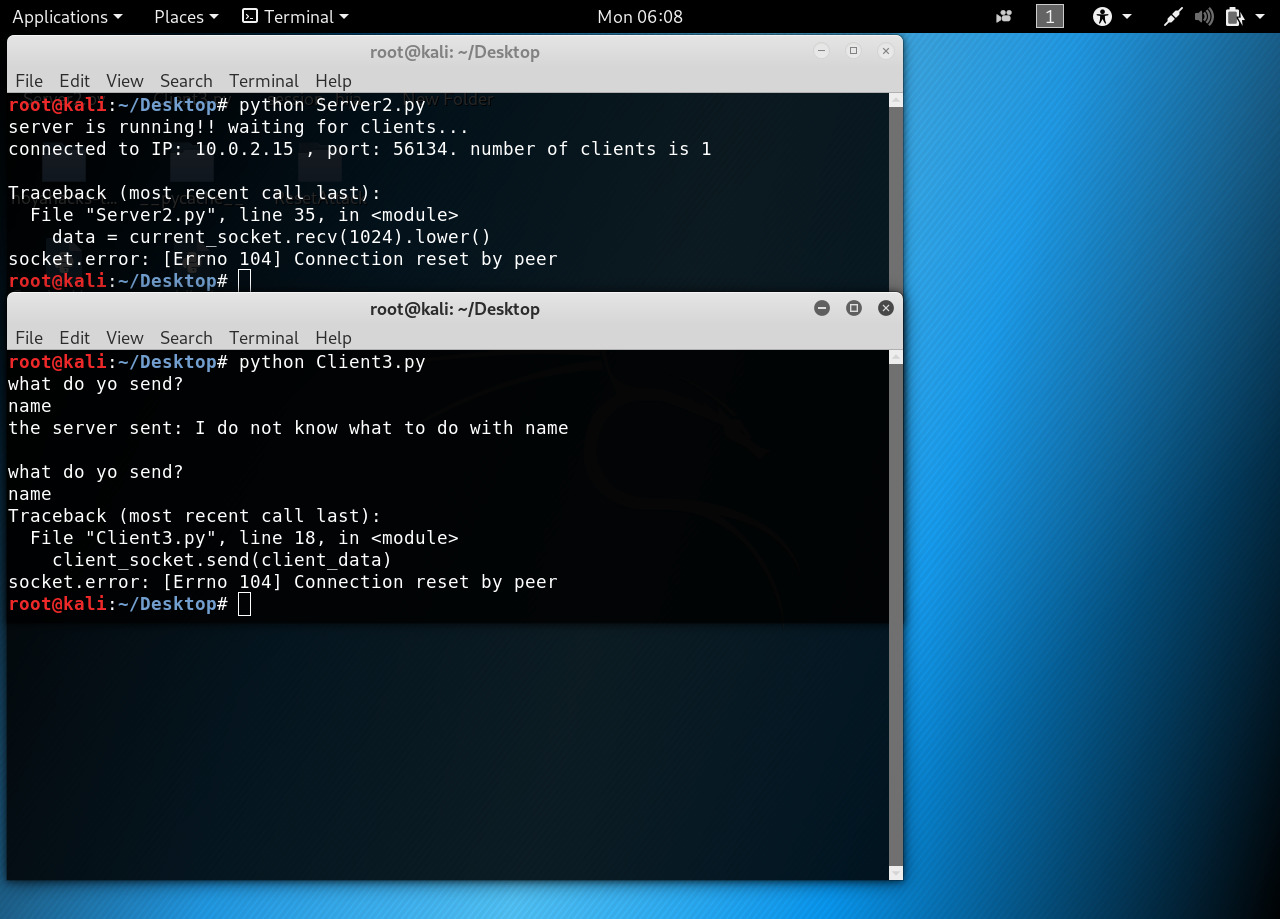
הודעה זו הועברה כשורה ונענתה על ידי השרת. בחלון הטרמינל של המתקפה ניתן לראות כי ההודעה זוהתה והמתקפה מבוצעת על הכתובת המבוקשת:



השתמשו ב – wireshark על מנת לזהות את פאקטת ה – Reset שנשלחה לשרת:

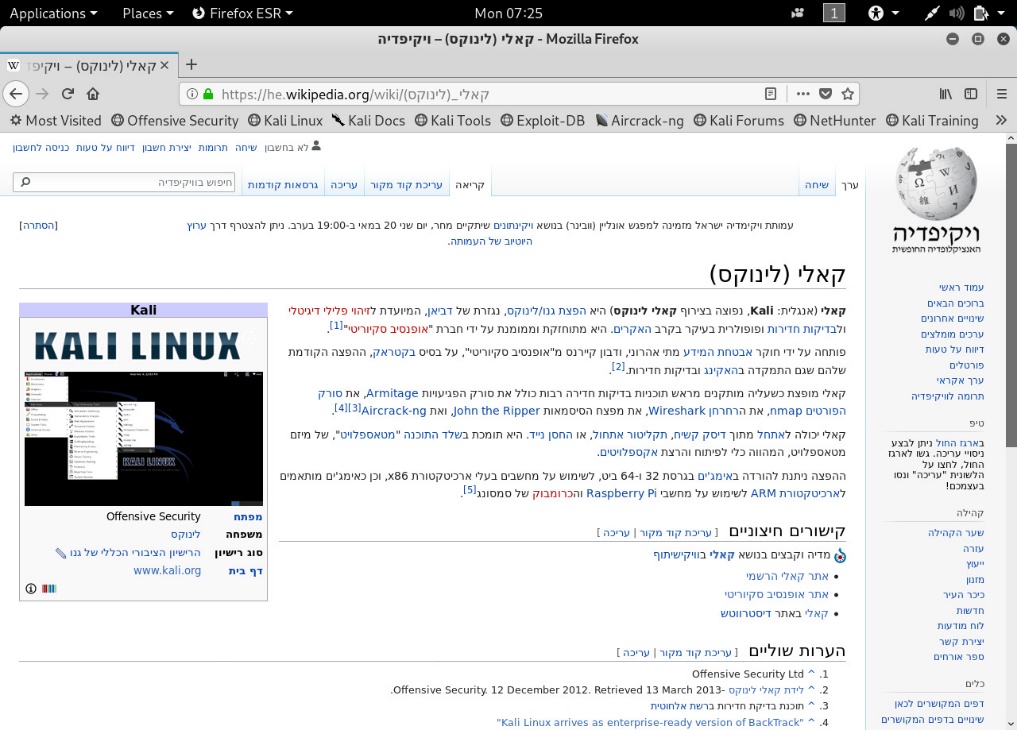


נסו שליחת הודעה נוספת בין הלקוח לשרת:

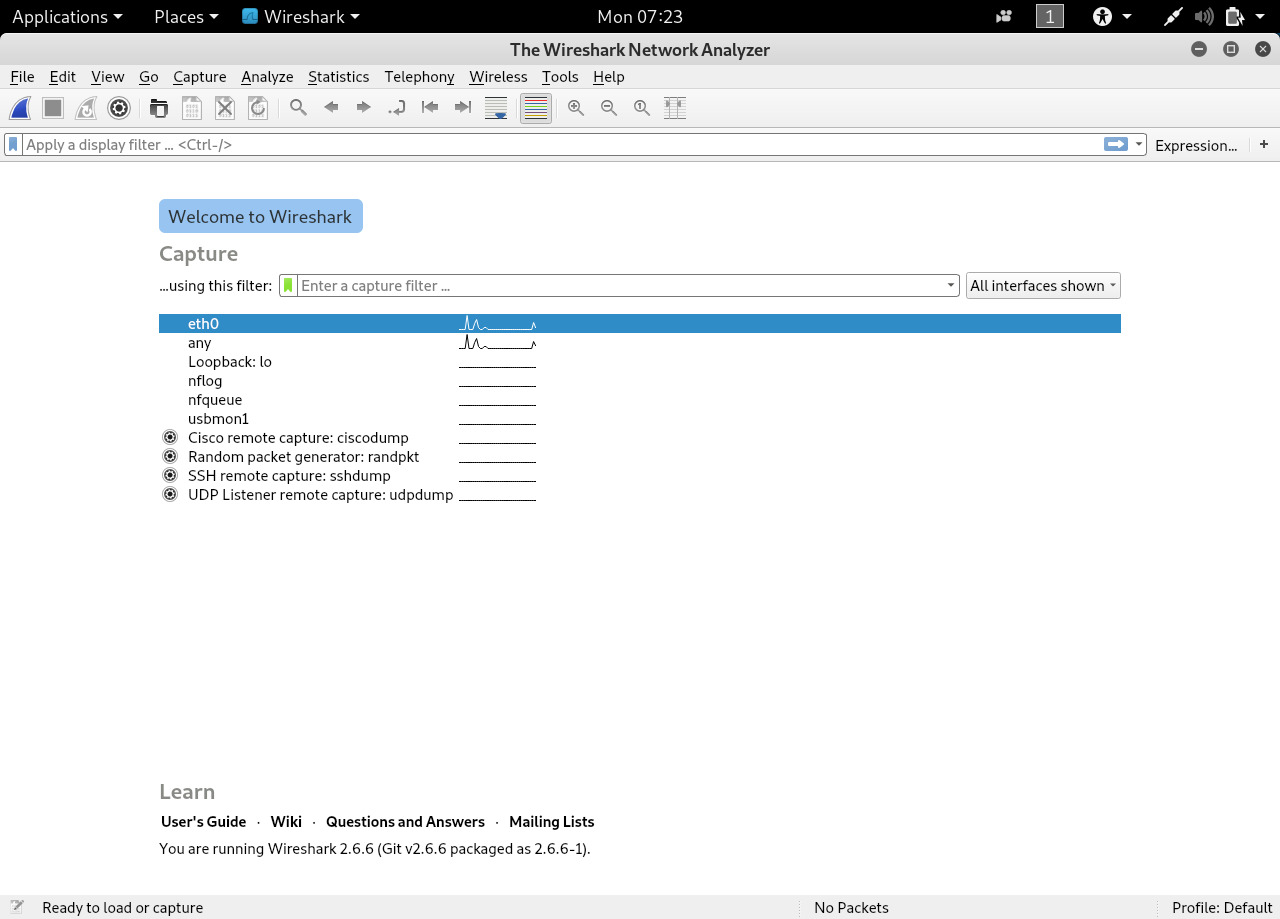


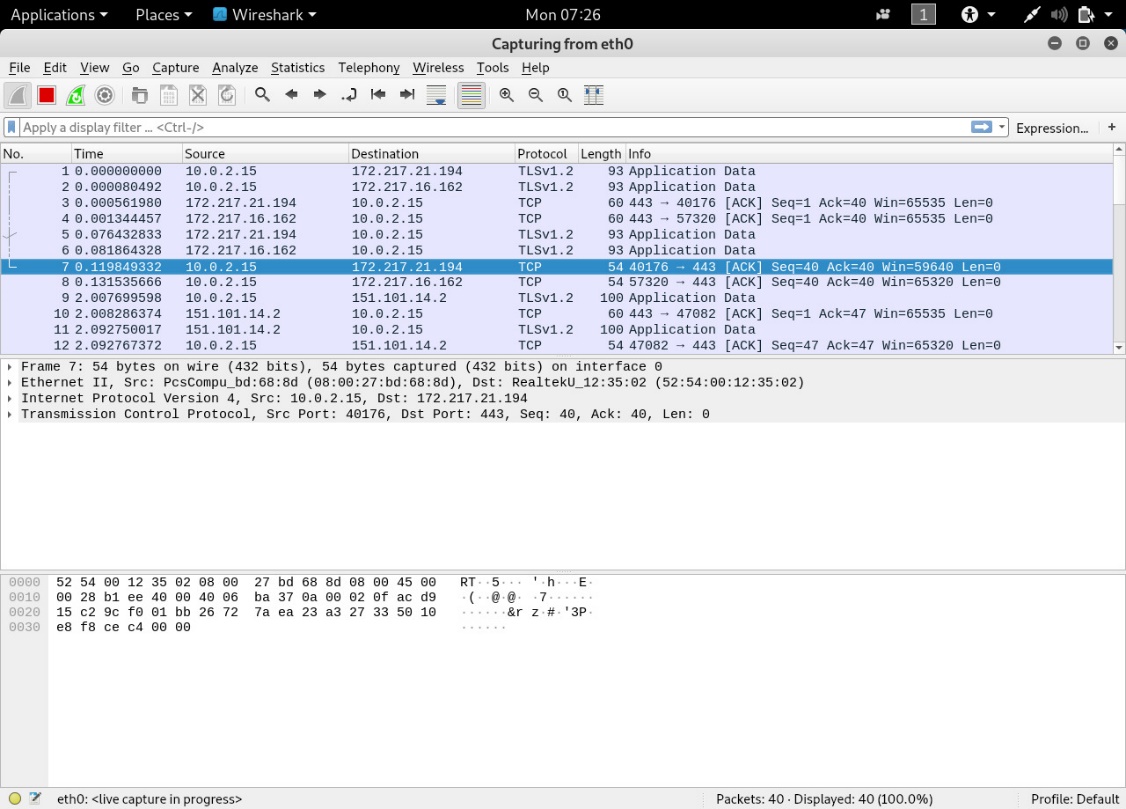
**כעת נבצע מתקפת Reset נגד התקשרות לאאתר אינטרנט:**

היכנסו לדפדפן מערכת ה -kali וגילשו לאתר אינטרנט כבחירתכם.



היעזרו ב – wireshark על מנת לזהות את הפרטים הנחוצים למתקפה – פלטפורמה, IP.



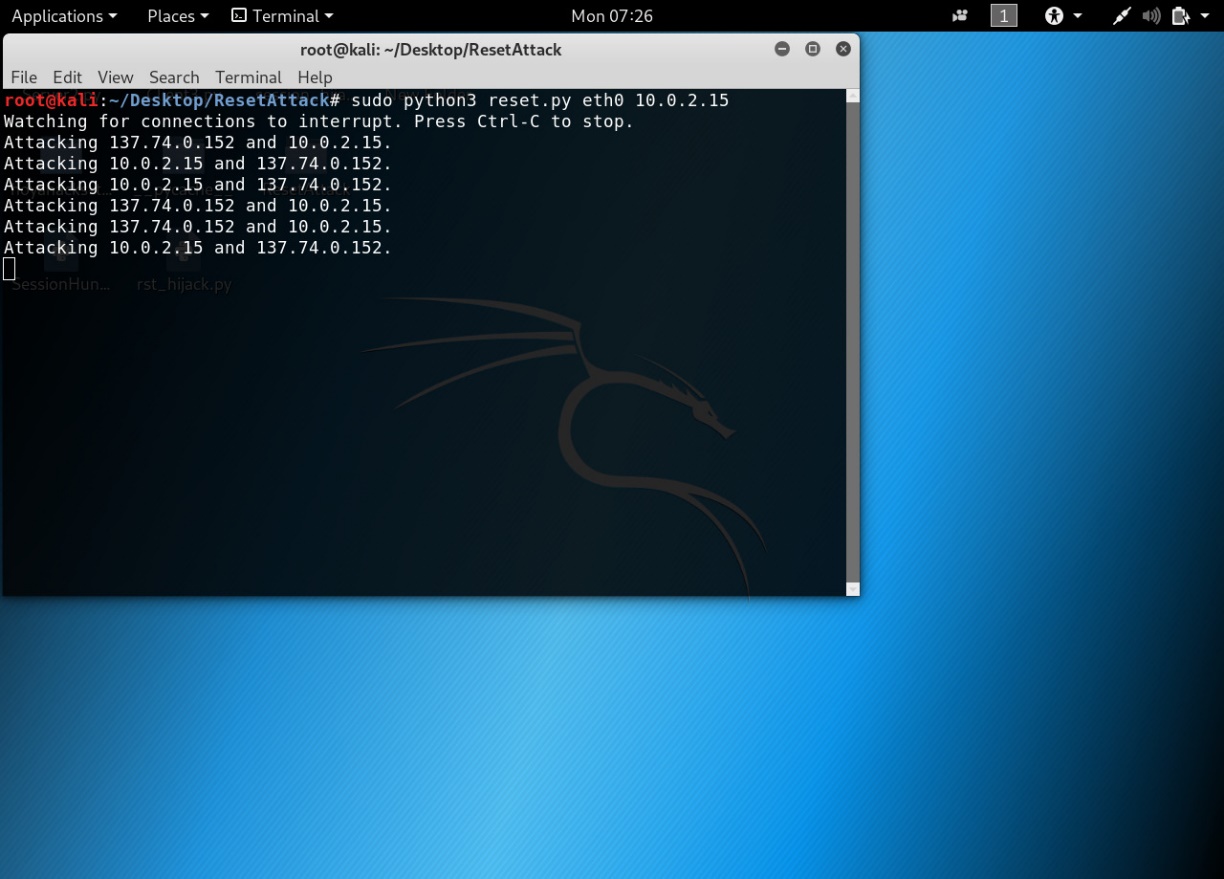


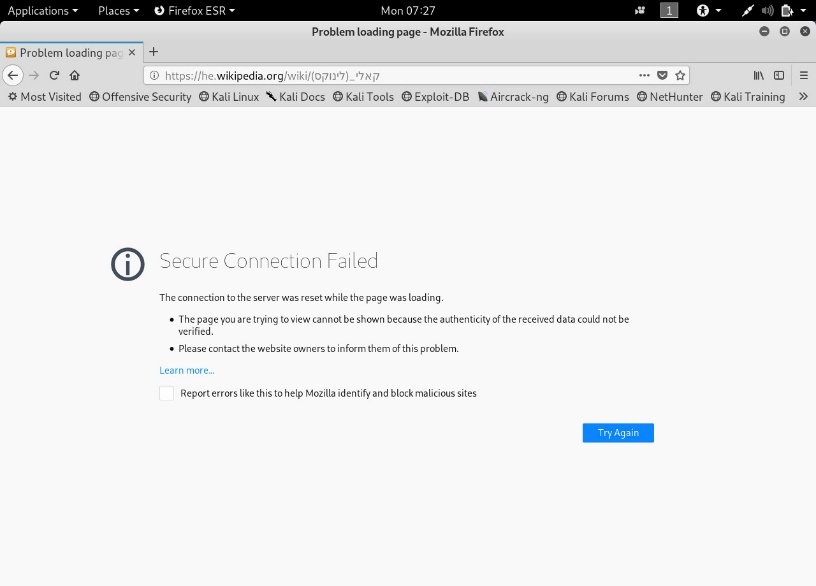
כעת, בחלון הטרמינל שפתחתם בתקיה שהורדתם, רישמו את השורה:

Sudo python3 reset.py (platform) (IP)

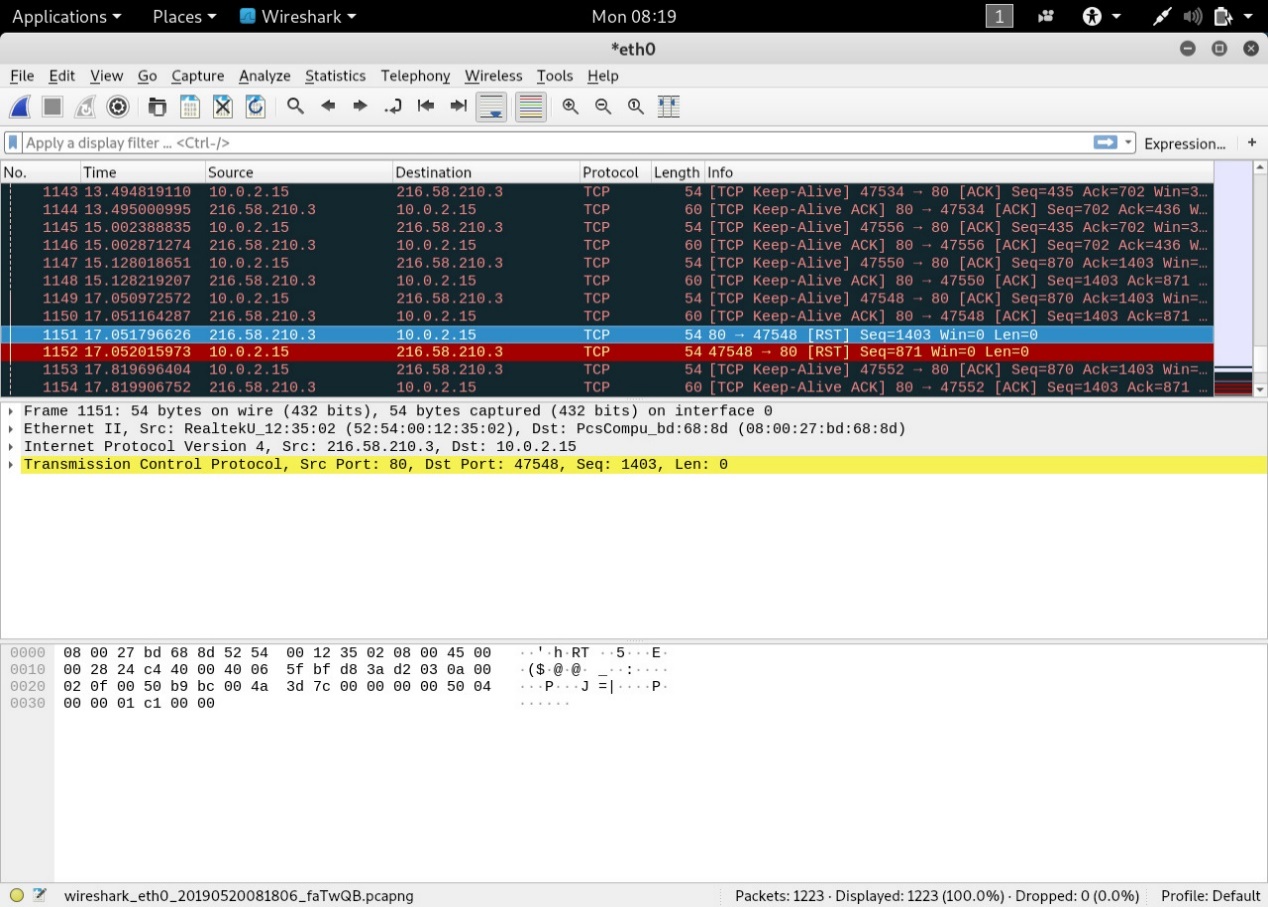
לאחר הרצת קוד המתקפה, רעננו כמה פעמים את חלון האתר שפתחתם.

בחלון הטרמינל של המתקפה, תתקבל הודעה על זיהוי הודעה והתקפת ה – IP המבוקש:

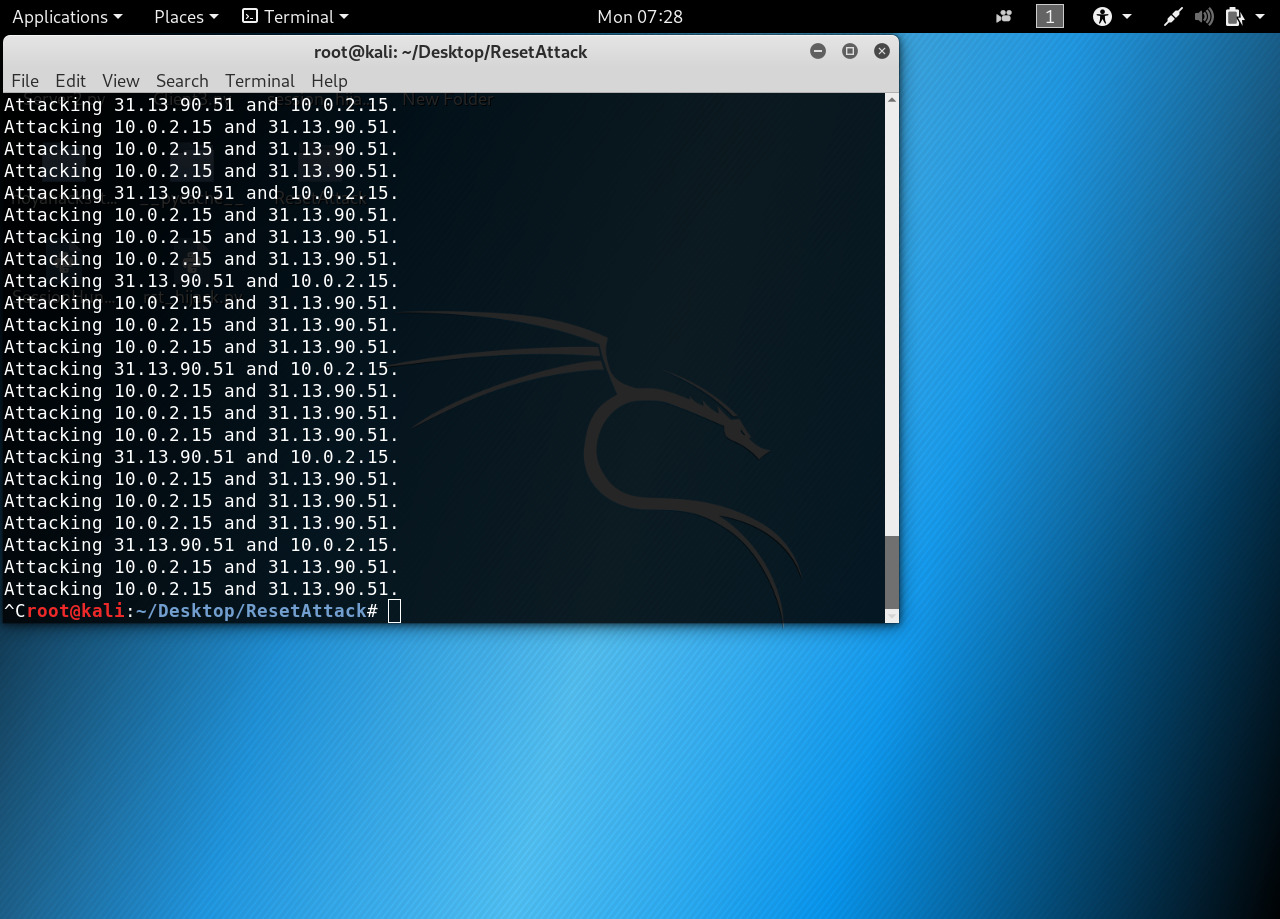


בחלון האתר שפתחנו תתקבל הודעת שגיאה על כישלון התקשרות:

השתמשו ב – wireshark על מנת לזהות את פאקטת ה – Reset שנשלחה לכתובת ה – IP שהזנו:



עיצרו את ריצת המתקפה על ידי לחיצת Ctrl-C, בחלון הטרמינל של המתקפה:



רעננו את חלון אתר האינטרנט וראו כיצד הוא עולה שוב.