

סירטון התחלתי בעברית על : wireshark

<https://www.youtube.com/watch?v=Smt2wRaukFA>

סירטון באורך 15 דקות עם הסבר בסיסי על תוכנת: wireshark

<https://www.youtube.com/watch?v=TkCSr30UojM>

סיכום הנושא של Wireshark

כאמור זוהי תוכנת הסנפה (או ריחרוח) שהיא קוד פתוח. היא שואבת מידע מכרטיסי הרשת שמותקנים במחשב. יש לבחור כרטיס שעליו נתמקד (בד"כ אפשר לראות כרטיס מסויים שעליו יש תנועת רשת).

ישנם שני מצבי לכידת מידע (capture options) , מצב 'פרוץ' - promiscuous mode שמאפשר למידע שאינו מיועד למחשב שלנו, גם להילכד, והמצב השני שבו ניבחר אם נרצה לראות רק את תנועת הרשת שמיועדת עבור המחשב שלנו.

ישנם שני סוגי מסננים - מסנן לכידה שבעזרתו נסנן פקטות על פי קריטריון שנקבע בשלב הלכידה מכרטיס הרשת - מיועד להקטין את כמות הפקטות שתראה על המסך. מסנן תצוגה שאינו מגביל את הלכידה, אלא רק את הפקטות שיראו בתצוגה של המסך לאותו זמן שבו הוא מופעל. המסנן החשוב ובעל הגמישות הגבוהה, הוא מסנן התצוגה ולכן נתמקד בו.

ההסנפה תתחיל מרגע הלחיצה על הסנפיר הכחול ותפסיק בלחיצה על הריבוע האדום בסרגל הכלים.

ניתן לשמור את הפקטות שלכדנו בהפעלה של התוכנה בקובץ שהסיומת שלו תהיה: pcap. אפשר גם לבחור איזה פקטות לשמור על ידי: file->export specified packets לאחר שמירת הקובץ , ניתן לפתוח אותו גם כן בעזרת wireshark.

בחלק העליון של המסך רואים את זרימת הפקטות. על ידי בחירת פקטה לוחצים על השורה בחלק העליון ובחלק האמצעי של המסך רואים את הפרוטוקולים שבתוכם נימצאים חלקיה של פקטה זו. ניתן 'לפתוח' כל פרוטוקול על ידי לחיצה על סימן הפלוס משמאל וכך לראות את המנבנה הפנימי והנתונים שמצויים בכל פרוטוקול עבור הפקטה.

בלחיצה על השורה בחלק האמצעי של המסך, בחלק התחתון רואים את המידע בהקסה דצימלי.

במסנן התצוגה ניתן לרשום שם של פרוטוקול כמו למשל tcp או http וכו' ובכך לבודד פקטות שנישלחו בעזרת פרוטוקולים אלה. אפשר גם לכתוב משהו כמו: frame contains google.com ואז נבודד פקטות שמכילות את האתר של google. אפשר לחפש פקטות עם ערך כלשהו בתוך פרוטוקול מסוים ובשדה מסוים בתוכו על ידי:

`protocol_name.field_name = value`

למשל: `ip.src = 192.168.1.2` (סינון של פקטות עם כתובת איי פי מסוימת)

תרגילים

תרגיל 3.4 בספר שבאתר `networks.pdf` בעמוד 85 הוא תרגיל מודרך (יש הוראות מדויקות ורק צריך לעקוב אחרי התוצאות).

תרגיל בעמוד 18, מצגת `1450-2-04.pdf`