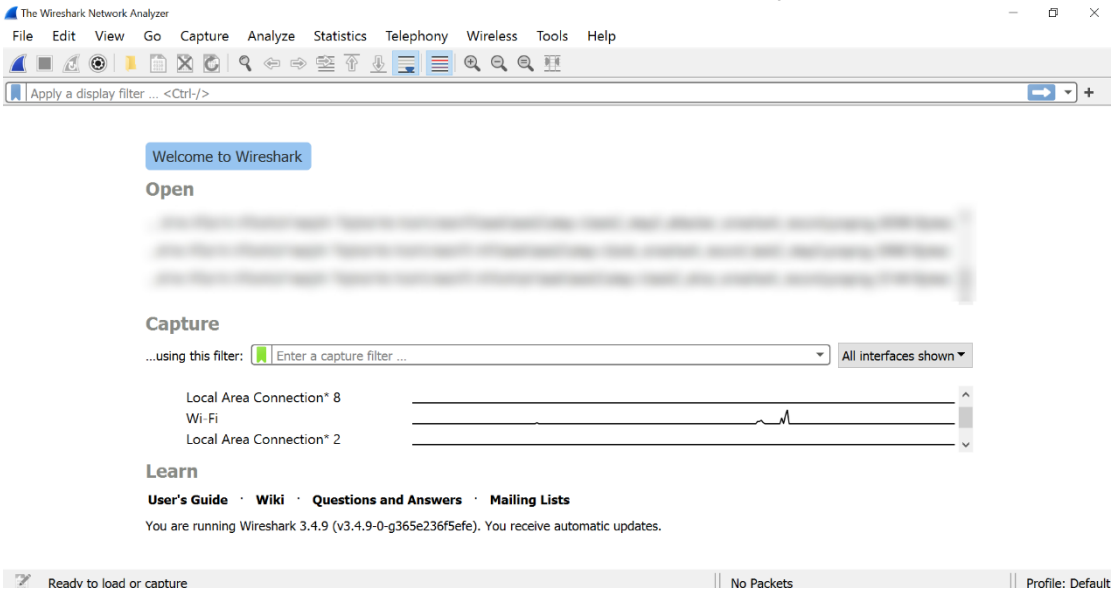
מטלת בית Wireshark-DNS-HTTP

את מטלה זו יש להגיש בזוגות כקובץ ZIP עם מספרי ת"ז של הסטודנטים/ות. לתיבת ההגשה במודל.

שימו לב, יש להגיש קובץ Pdf המכיל צילומי מסך (בכל מקום שאתם משתמשים שיש לכם פלט מסויים כגון wireshark or cmd תצלמו מסך ותסבירו איך הגעתם למסקנה, כמובן שאפשר לכתוב על הצילום).

אין להגיש צילומי מסך בנפרד, אלא רק מרוכזים בקובץ אחד עם הסברים. קובץ ללא הסברים או צילומי מסך בלבד יקבל אפס אוטומטית ללא אפשרות לערעור

1. נתחיל בפשוט – פתחו wireshark והסתכלו על המסך הראשי (מבלי עדיין להפעיל שום דבר!)



אפשר לראות שקיימים מספר ממשקים שאפשר להסניף מהם מידע.
זהו את הממשק שמקושר לאינטרנט החיצוני, ובחרו בו.

2. עכשיו נפעיל את קליטת החבילות (פאקטות) – אתם תגלו שהחבילות מצטברות מהר מאד והרבה מאד, עם הרבה סוגים – לשם כך חיוני להכיר את מנגנון הסינון.
   1. סננו את כל החבילות לפי destination ip מסוים לבחירתכם.
   2. סננו את כל החבילות לפי source port מסוים, נניח 443 תוך גלישה באינטרנט, ציינו את הפרוטוקול שמשתמש בפורט הנ"ל.
   3. סננו את החבילות לפי פרוטוקול מסוים לבחירתכם.

3. שמרו את ההקלטת wireshark (save <- file), מהו פורמט ההקלטה?

4. בחלונית files יש אפשרות export specific packets, שמרו שתי פאקטות כלשהם לבחירתכם בפורמט הנ"ל.

5. בהגדרות קיים אפשרות להפעיל promiscuous mode, הסבירו בקצרה מה זה, מה זה עושה ומה השימושים של זה.

6. הפעילו את הwireshark, רשמו בחיפוש frame contains "unit" והיכנסו לכתובת http://www.unitarium.com/. הציגו את התוצאות ונסו להסיק – מה הסינון עושה?

עכשיו wireshark מתעד את כל חבילות האינטרנט היוצאת והנכנסת למכשיר, אתם תגלו שיש הרבה תעבורה והרבה סוגי פרוטוקולים, במטלה אנחנו נתעמק בשני סוגי פרוטוקולים: http ו-dns.

HTTP:

7. בזמן שה-wireshark מופעל (אפשר להפעיל מחדש לצורכי נוחות) – היכנסו לאתר
http://www.sha1-online.com
אחר כך – עצרו את פעילות הwireshark - וסננו את התעבורה על פי פרוטוקול http.
זהו את חבילות הבקשה וחבילות התגובה לבקשה. איך זיהיתם.

8. זהו את חבילת הבקשה ובחרו אותה:
   1. כמה זמן לקח לתגובה להגיע לאחר הבקשה?
   2. מהי גרסת הhttp?
   3. מאיזה מכשיר התבצעה הבקשה?
   4. איפה נמצאת חבילת התגובה?
   5. מהו פורט היעד של החבילה?

9. זהו את חבילת התגובה ובחרו אותה:
   1. מהו סטטוס קוד התגובה?
   2. מאיזה שרת התגובה התקבלה? מהו ה-IP שלו?
   3. כמה חבילות TCP היו נחוצות כדי להרכיב את החבילה?
   4. מהו סוג הconnection בין השרת והלקוח? הסבירו בקצרה מה המשמעות של זה

10. האתר שנכנסתם אליו זה אתר הצפנת לפי hash – אתם מכניסים מחרוזת ומקבלים גרסא מוצפנת שלהם. בעודכם מפעילים wireshark (בשורת החיפוש רשמו http) – הכניסו את השם שלכם ולחצו על hash.
    1. האם החישוב נעשה בדפדפן או בשרת מרוחק?
    2. אילו פרמטרים נשלחו בבקשת הhttp?
    3. למה בכלל היה צורך לבצע את התקשורת http? לא היה עדיף לבצע את החישוב בצד הלקוח?? הסבירו למה
    4. **אתגר: תארו סיכון אפשרי בהחזרת התשובה משרת מרוחק במקום חישוב מקומי בדפדפן.**

11. כנסו לאתר http://www.unitarium.com (אפשר גם דרך incognito) בצעו follow http stream ובדקו כמה חבילות שנשלחו מהלקוח יש, וכמה חבילות שנשלחו מהשרת? מה חזר בכל חבילה מהשרת?

12. אתגר: היכנסו לאתר https מסוים (לבחירתכם) תוך ניטור הwireshark, הסיקו מה קרה ולמה זה קרה.

DNS:

13. נתחיל בבדיקה פשוטה – ניתן להשתמש במילת החיפוש nslookup בחלון הפקודות (cmd) לביצוע שאילתות.
חפשו nslookup icecream.com. רשמו את שם השרת שנותן את תשובת השאילתה, האם הוא שרת מהימן (authoritative answer), ואת כתובות הip של הדומיין.

14. עכשיו בצעו שוב את השאילתה – אבל הפעם כאשר הwireshark מופעל (סננו לפי dns).
    1. כמה שאילתות לגבי הדומיין אתם רואים?
    2. מה ההבדל ביניהן? הסבירו את ההבדל (במידה ויש יותר מאחת).
    3. בחרו אחד מהשאילתות הנ"ל: לאיזה פורט יעד השאילתה נשלחה?
    4. האם החבילה נשלחו על פרוטוקול תעבורה TCP או UDP?
    5. האם השאילתה נעשתה באופן איטרטיבי או רקורסיבי? איך הגעתם למסקנה?
    6. הסתכלו על החבילת תגובה לשאילתה (query response) לכל אחד מהשאילתות מסעיף 1: כמה תשובות התקבלו לכל שאילתה? מה ההבדל המהותי בין התשובות לכל שאילתה?
    7. כתוצאה מסעיף 1 ו-6 – מה ההבדל בין שאילתה מסוג A, ושאילתה מסוג AAAA?

15. רשום בחלון הפקודות ipconfig /all:
מהו שרת הdns של מכשירך (בעת ביצוע הפעולה)?

16. DNS יכול לפעול גם על IPv6, רשמו את הIPv6 של שרת הDNS, אם קיים.

17. חשוב להכיר את האפשרות לשינוי את הגדרות השרת DNS, כלומר האם הוא מוגדר באופן אוטומטי או ידני.
לשם כך, ב-windows 10 יש להיכנס ללוח הבקרה -> change adapter settings -> wifi (או ממשק האינטרנט שאתם משתמשים) -> properties <-סמנו Internet Protocol Version 4 ולחצו על properties.
(למידע נוסף: https://youtu.be/TqTUk5GgmQ8), שנו את כתובת השרת dns ל-8.8.8.8 (שרת הdns של גוגל).

בדקו שוב עם ipconfig /all את כתובת שרת הdns שלכם. בנוסף גלשו למספר אתרים לבחירתכם עם שרת הdns של גוגל – בדקו עם wireshark שאכן יש שימוש בשרת dns של גוגל

הערה: ייתכן שפעולת הברירת המחדל הראשונה של המכשיר זה לעבור לdns ipv6, לצורך הדוגמה – בחלון properties הורידו את הv מ Internet Protocol Version 6 ולחצו ok.

בסיום הפעולה – החזירו את מנגנון הגדרת השרת DNS להקצאה אוטומטית.

18. מה כבד יותר? חבילת query או חבילת response ל-query? הסבירו.

19. מחשב יש רשומה מקומית (cache) של כתובות ip שמקושרות לדומיינים – מטרתן הוא לשמור מיפוי של דומיינים מסוימים לכתובות ה-ip המתאימים, כדי שבמקרה הצורך המחשב ייגש לכתובת הip מהרשומה המקומית במקום לבצע את השאילתה.
1. כנסו לחלון הפקודות ורשמו "ipconfig /displaydns" – הציגו תמונה של מה שקיבלתם.
2. נקו את הרשומה באמצעות הפקודה "ipconfig /flushdns", לאחר מכן הכניסו שוב "ipconfig /displaydns " – הציגו תמונה של הרשומה הריקה.
3. רשמו בחלון פקודות "ping icecream.com", לאחר מכן כנסו שוב לרשומה עם "ipconfig /displaydns "
מהרשומה בלבד: מה הכתובת IP של icecream.com? למשך כמה זמן הדומיין יהיה רשום ברשומה?

20. שאלת סיכום – הסבירו את כל התהליכים שקורים מרגע שמבקשים לגלוש לאתר http מסוים, עד לרגע שהתוכן מופיע בדפדפן מבחינת dns וhttp (הניחו שהcache נקי ולא היה ביקור קודם באתר)