**חלק א' – DOH**

1. DOH מונע זיוף כתובות (man in the middle). ז"א כשאר אנו שולחים בקשה לDNS, אין אפשרות למישהו שהוא לא השרת שרצינו להפריע להתקשרות בינינו ולשלוח אותנו לאתר זדוני (במקום המבוקש).
2. שני חסרונות:
   1. ראשית DOH מונע הגנה שהרשת מספקת. זאת אומרת שישנם אתרים שהרשת יודעת שאינם בטוחים, אך כאשר היא לא יודעת לאיזה אתר אנו עומדים להכנס (בגלל ההצפנה) היא לא תועל "לעצור" אותנו לפני
   2. פוגע במידיניות של חברות. כאשר אני משתמש במחשב והרשת של החברה בה אני עובד, אני יכול להכנס לאיזה אתר שאני רוצה מבלי שהחברה תדע.
3. נתייחס לסעיף b. אפשר להגדיר שהמשתמש בקצה יעבוד בצורה לא מוצפנת (DNS רגיל) והנתב\שרת אפוקסי של החברה יהפוך את הבקשה לצורת DOH. (יכול פשוט לשאול את אותה שאלה בצורה מוצפנת). כך גם מי שמבחוץ לא יוכל לראות מה שאלנו, וגם החברה תהיה במעקב אחר האתרים המבוקרים.
4. Pros/cons:
   1. **יתרונות**: נותן אבטחה מקצה לקצה. **חסרונות**: מאט מאוד את המחשב, אין אפשרות של ניתור חיצוני (חברות, הגנת אינטרנט וכו).
   2. **יתרונות:** מוריד את העומס מהמחשב, נותן אבטחה כמעט מקצה לקצה. **חסרונות:** לא מאה אחוז מקצה לקצה
   3. **יתרונות:** אבטחה מקצה לקצה. **חסרונות:** לא פותר את בעיית העומס על המחשב
   4. **יתרונות:** כל מידע שיעבור במחשב יהיה מוצפן **חסרונות:** כל מידע שיעבור במחשב יהיה מוצפן ולכן יווצר עומס בגלל תהליך ההצפנה וההפך.

לכן לדעתי השיטה הכי טובה היא proxy מקומי. מכיוון שאנו מורידים את העומס של ההצפנה מהמחשב אך עדיין מספיק מאובטחים.

1. DOH משתמש בHTTPS שרץ על פרוטוקל HTTP. ז"א שהחיבור הוא TCP ולא UDP. בד"כ שאילתות DNS נשלחות בחיבור UDP מה שאומר שאף אחד לא מוודא שהשאילתה הגיע, ושהתשובה גם הגיעה. בTCP לעומת זאת, אם לא יתקבל ACK השאילתה תישלח שוב וכך גם התשובה (כתובת הIP הרצויה).

**חלק ב'**

נראה שלפעמים CUBIC יותר מהיר (כאשר העיכוב הוא בעיקר בעומס ברשת) ולפעמים RENO יותר מהיר (בעיקר כאשר רוב העומס נוצר מאיבוד פקטות)