**חלק א' – DoH**

1. **יתרון אחד לשימוש ב-DoH הוא שלא צריך לשמור את הכתובות ב-Cache.**
2. **א. כדי להשתמש ב-DoH, על המשתמש להוריד הרחבות שמקצות את האפשרות להשתמש בשיטה זו, לכן דרושה תמיכה במערכות הפעלה למי שמעוניין להשתמש בה.**

**ב. בגלל ששיטה זו מצפינה את המשתמשים בה, אין אפשרות להתחקות אחר משתמשים אשר ביצעו פשעים ברשת או עקפו את האבטחה.**

**3. כדי להשתמש ב-DoH, אפשר להתקין הרחבות ותוספים, למשל שימוש בדפדפן שמאפשר למשתמש לבחור לעבוד ב-DoH או DNS,בפיירפוקס למשל ניתן.**

**4. a. כאשר נממש את ה-DoH ברמת האפליקציות, ההתקנה תהיה פשוטה באמצעות דפדפן או התקנה של תוסף. אולם, לא לכל דפדפן יש את האפשרות להשתמש בממשק זה.**

**b. במידה ומשתמשים ברמת שרת proxy ברשת, השרת ישלח שאילתות בתצורה מוצפנת, באמצעות DoH, ומכיוון שנשלחות שאילתות באמצעות dns , אין צורך לשנות את הגדרות המערכת. חיסרון בשיטה זו הוא שנוצרת בעיית הצפנה מכיוון ה-dns.**

**c. ברמת שרת proxy מקומי, נשתמש בשרת שהייעוד שלו לא מתעסק בשירותים אחרים אלא רק ב-DoH. לעומת זאת, נוצרת מצד הלקוח דרישה רבה למשאבים בגלל השימוש בשיטה יחידה.**

**d. כאשר נגדיר למחשב לשלוח רק ב-DoH, ניפטר מהתעסקות בתוכנות ותוספים שיש להתקין והמחשב יעבוד רק בתצורה אחת בלי התקנות נוספות.**

* לסיכום, לאחר השוואה בין כל ארבעת השיטות והצגת החסרונות והיתרונות שבה, השיטה המועדפת על פניי מכולם היא מימוש DoH ברמת האפליקציות, מכיוון שבאמצעות התקנה של תוסף בדפדפן , נימנע מהתעסקות בהגדרות תצורה על המחשב והשרת.

**5. יתרון ברור שיש ל-DoH על פניי do53 הוא שבפרוטוקול DoH, אנו משתמשים בפרוטוקול TCP שיש לו מנגנון לבקר איבוד פקטות באחוזים ויכול לשלוח מחדש את הפקטות שאבדו. לעומת זאת ב-do53 יש שימוש בפרוטוקול UDP ובו אין בקרה על איבוד פקטות ושחזרון.**