שאלה 1

א)בעקרון כל הוספה של פקודות תשנה את זמן הפעולה של התכנית מה שישנה את התדירות של הפנייה לשרת, לכן מה שנעשה זה פשוט להוסיף עוד סתם פקודה חישובית שלא משפיעה על הקוד, לדוגמא add edx,0 ומספיק שהיא תיקח קצת זמן כדי לשנות בקצת את הזמן שלוקח זמן כלשהו לבצע את הפקודה כדי שהתדירות תשתנה.

ב) כלומר נרצה לעשות הוק בהתחלה של הפונקציה ולהפוך את x להיפוך שלו ואז להמשיך את פעולת התוכנית כאילו הכנסנו את ההיפוך של x, אבל אנחנו יודעים שזה בעייתי להכניס בתחילת הפונקציה הזו קוד, ולכן את ההוק נרצה לעשות בסוף הפונקציה,מה שנרצה לעשות זה להפוך את x ואז להפעיל עליו שוב את הפונקציה, מכיוון שאנחנו לא יודעים כמה מקום יש לנו להוק נרצה פשוט להפוך את x ואז לקרוא שוב לפונקציה, לכן מה שנרצה לעשות זה לקחת את כתובת החזרה של הפונקציה, להקטין אותה כך שהיא תחזור שורה אחורה, כלומר למקום שבו קראו לפונקציה, ולפני זה להפוך את x ולוודא שאנחנו עושים את זה רק פעם אחת, כלומר שבקריאה החדשה לפונקציה לא נכנס שוב להוק, בעזרת רגיסטר שהפונקציה לא משתמשת בו או על המחסנית. את כל הקוד הזה נצטרך להכניס איפשהו, ולקפוץ אליו עם הדריסה בסוף הפונקציה, נוכל להכניס אותו בsection נוסף בקובץ הריצה שאליו ההוק יקפוץ, וכמובן שנוסיף גם את הקוד שאנחנו דורסים לשם.

ג)הפונקציה sendf ככל הנראה מחברת את ההודעה למחרוזת אחת ואז שולחת אותה לשרת, כדי לשלוח אותה לשרת היא תצטרך להשתמש בפונקציית ספריה לשליחה על גבי סוקט לשרת(ככל הנראה send מwinsocket ) לכן מה שנרצה לעשות זה לעשות הוקינג לפונקציה הזו כך שלפני שהיא שולחת לשרת היא מצפינה את ההודעה, במקרה והפונקציה משתמשת בהוט פטצינג, נוכל להשתמש באפשרות הזו כדי להזריק פונקציה משלנו שנכתוב על dll (כמו שעשינו בסדנה), או שנוכל להשתמש בIAT ונחליף את הכתובת של הפונקציה לפונקציה שמצפינה את ההודעה ואז קוראת לפונקציית הספריה המקורית.

ד) נרצה בעצם לגרום לפונקציה connect לחכות עד שתופעל הפונקציה parse לפני שהיא מתחילה את התכנית, זה דומה למה שאנחנו עושים כשאנחנו רוצים לדבג ומחכים לדיבאגר ולכן נשתמש באותה השיטה, connect תחכה לדיבאגר ופארס יפעיל דיבאגר על connect כשהוא מתחיל (הוא לא באמת ידבאג אותו, הוא יכבה אותו ישר) וכך שניהם יתחילו לפעול במקביל. נשתמש בפונקציות של DebugActiveProcess וDebugActiveProcessStop כדי להפעיל את הדיבאגר ולכבות אותו מparse ובconnect נחכה לדיבאגר כמו שלמדנו בתרגול, כך ברגע שהדיבאגר יופסק שני הפונקציות יחזרו להתחלה, את הקוד הזה נכניס לשתי פונקציות, אחת לconnect ואחת לparse שנוסיף לקובת הריצה ונדרוס בתחילת connect וparse קפיצה אליהן(נוסיף להן גם את השורה שאנו דורסים).

ה)