פרויקט סייבר במסגרת תכנית גבהים

Onion Routing

לירון ברגר

209142090

תיכון ליאו באק

הגנת סייבר

מנחים

שרית לולב

אלון בר־לב

תוכן עניינים

מבוא

פרויקט זה נועד לממש טכניקה לתקשורת אנונימית ברשת מחשבים, הקרויה ניתוב בצל (Onion Routing). הפרויקט מממש מערכת המאפשרת למשתמשיה תקשורת דרך דפדפן האינטרנט אשר אינה מאפשרת מעקב אחר מקורן של ההודעות הנשלחות מהמשתמש. המערכת מבוססת על פרוטוקול socks5.

המערכת בנויה מרשת של צמתים, nodes (בעברית-נתבי בצל). המידע הנשלח מהדפדפן עובר דרך הצומת הראשון, ומועבר לשלושה צמתים אקראיים נוספים, עד שלבסוף מנותב אל היעד הרצוי. המידע מוצפן בשכבות לפי המפתחות הסודיים של הצמתים, ומכאן האנלוגיה לבצל.

המערכת מורכבת ממספר משתתפים:

- Registry (שרת HTTP) - המשמש כRegistry. כאשר צומת מתחבר או מתנתק נשלחת לשרת הודעה מתאימה, והוא נשמר/נמחק ממבנה הנתונים. מספר שירותים שונים בהתאם לצרכים השונים של הלקוח:
  - שירות התחברות של צומת.
  - שירות התנתקות של צומת.
  - שירות קבלת רשימת צמתים מחוברים.
  - שירות קבלת קובץ (לצורך ממשק המשתמש)
- Client_node (לקוח sock5) - הצומת הראשון אליו מתחבר הדפדפן. מתחבר אל הRregistry עם פתחיתו ומתנתק בעת הסגירה.
- Server_node (שרת socks5) - צומת אשר משתמשים לצורך אנונימיזציה של החיבור. מתחבר אל ה Rregistry עם פתחיתו ומתנתק בעת הסגירה.

כלל המשתתפים פועלים באופן אסינכרוני המאפשר עבודה מקבילית על מספר רב של חיבורים.

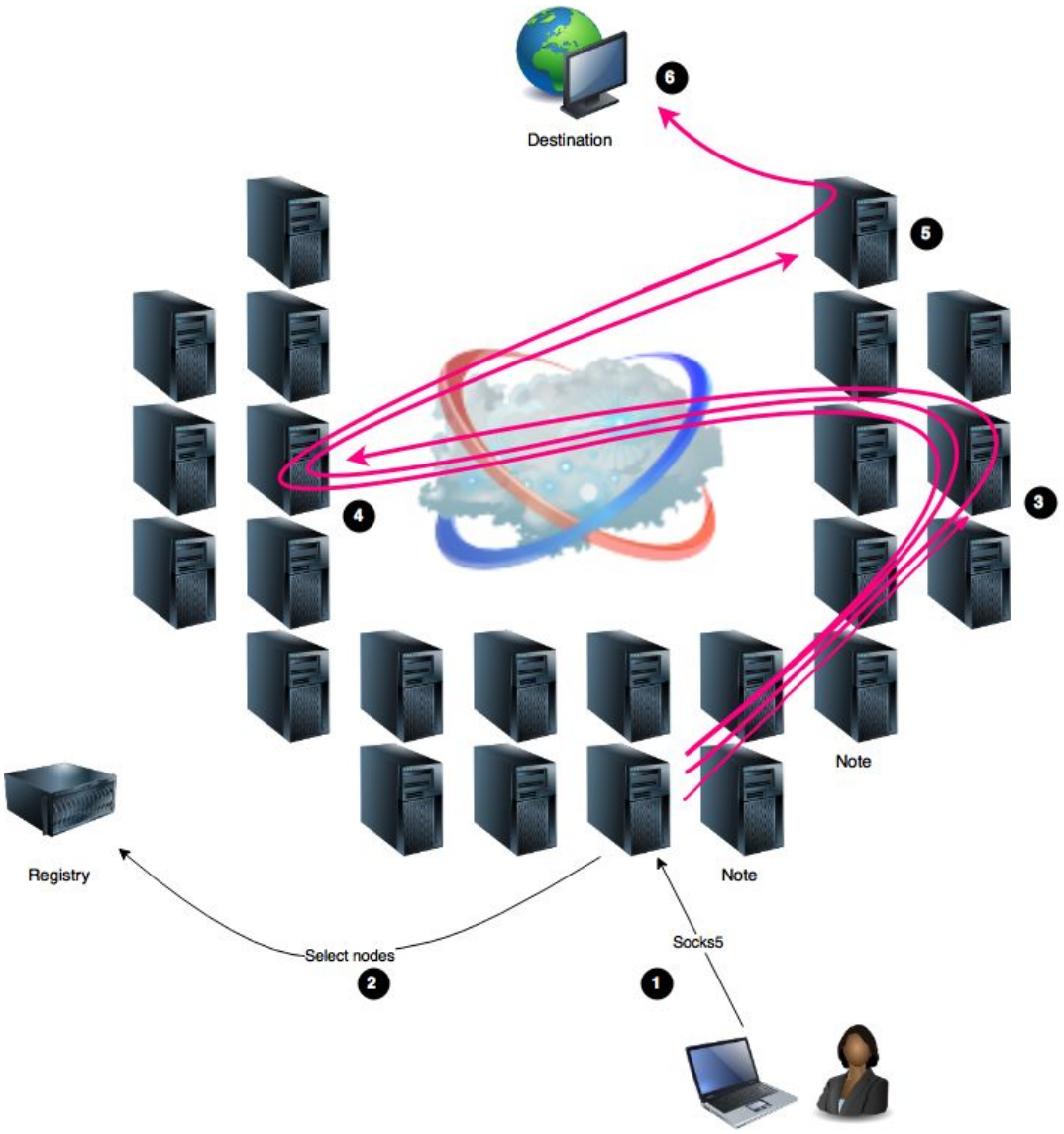
למערכת ממשק משתמש נוח וקל לשימוש המאפשר לקבל מידע על סטטיסטיקה העוברת ברשת, צמתים קיימים וכתובותיהם (עם אפשרות לסגירה) ומידע אודות המערכת.

ארכיטקטורה

ההודעות הנשלחות מהלקוח (הדפדפן) נשלחות אל הצומת הראשון ולאחר מכן עוברות דרך מספר צמתים נוספים, כאשר כל צומת מנתב את ההודעה אל הצומת הבא, עד שלצומת הרביעי, והאחרון, נשלחת ההודעה המקורית והצומת מנתב אותה אל היעד של הלקוח.

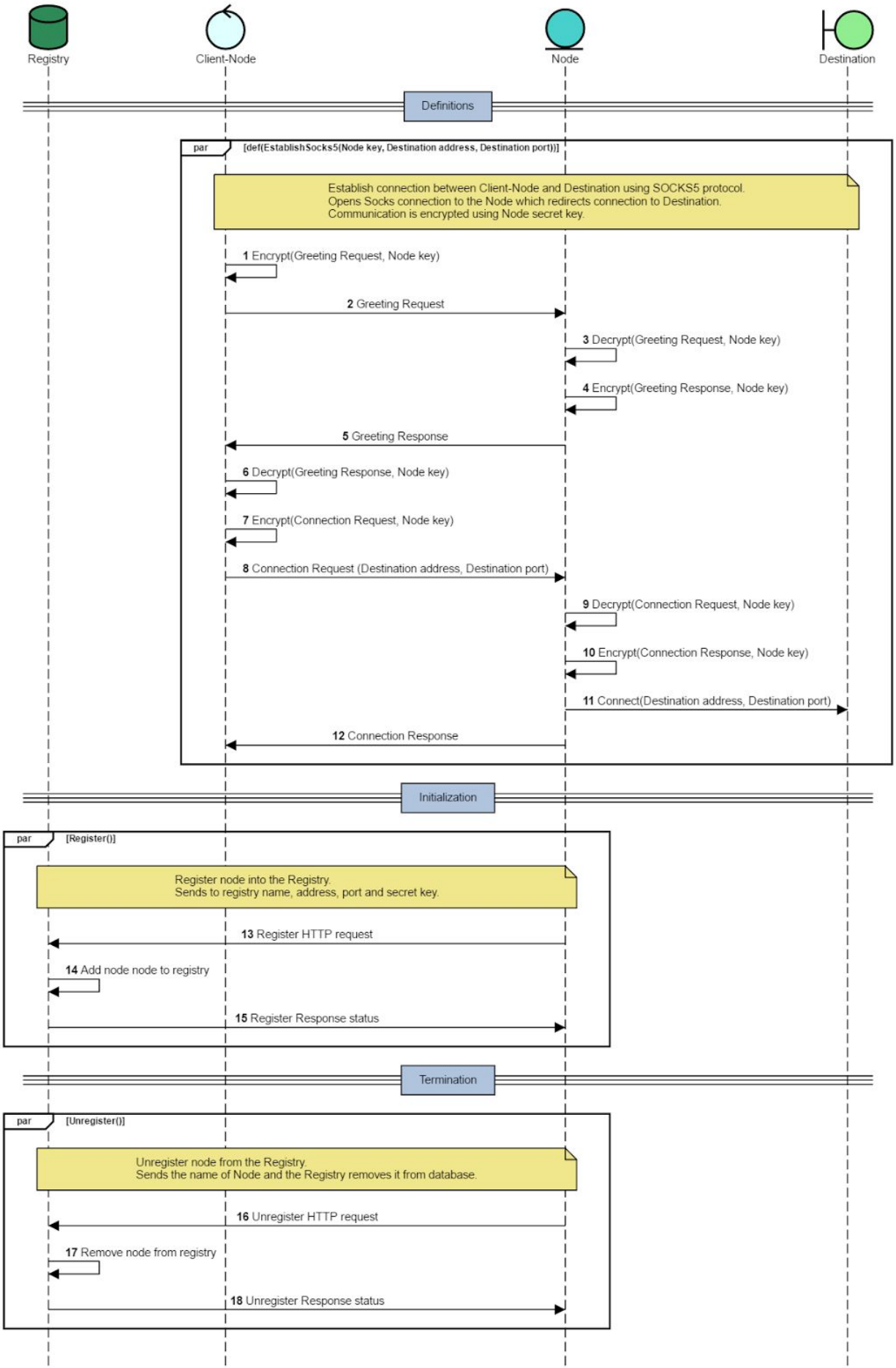
- הצומת הראשון - Client_node, הצומת הקבוע אליו מתחבר הדפדפן. עם קבלת חיבור הצומת פונה אל שרת הHTTP המשמש כRegistry, ומקבל רשימה של כל הצמתים המחוברים. הצומת בוחר של שלושה צמתים נוספים באקראי ומתחבר בפרוטוקול socks5 לצומת השני המתואר בדיאגרמת הרצף.
  תקשורת בין שני הצמתים מוצפנת עם המפתח של הצומת השני.
- באמצעות חיבור socks5 הצומת השני מתחבר לצומת השלישי ומשמש כעת כשרת פרוקסי המנתב הודעות בין הדפדפן והצומת השלישי. תהליך דומה מתרחש כעת בין הצומת הראשון והצומת השלישי, כאשר חיבור socks5 מחבר את הצומת הראשון אל הרביעי. התקשורת הוצפנה באמצעות המפתח של הצומת השלישי.
- הצומת הראשון מצפין את ההודעה המקורית של הדפדפן ומעביר אל הצומת הרביעי. מתרחש תהליך זהה - הדפדפן שהתחבר בsocks5 מנותב אל יעדו ע"י הצומת הרביעי.
- התקשורת בין הדפדפן והיעד מוצפנת ע"י המפתח של הצומת האחרון.

בפועל נוצר מצב שבו נראה כי הדפדפן פתח חיבור socks5 ישירות עם הצומת הרביעי.

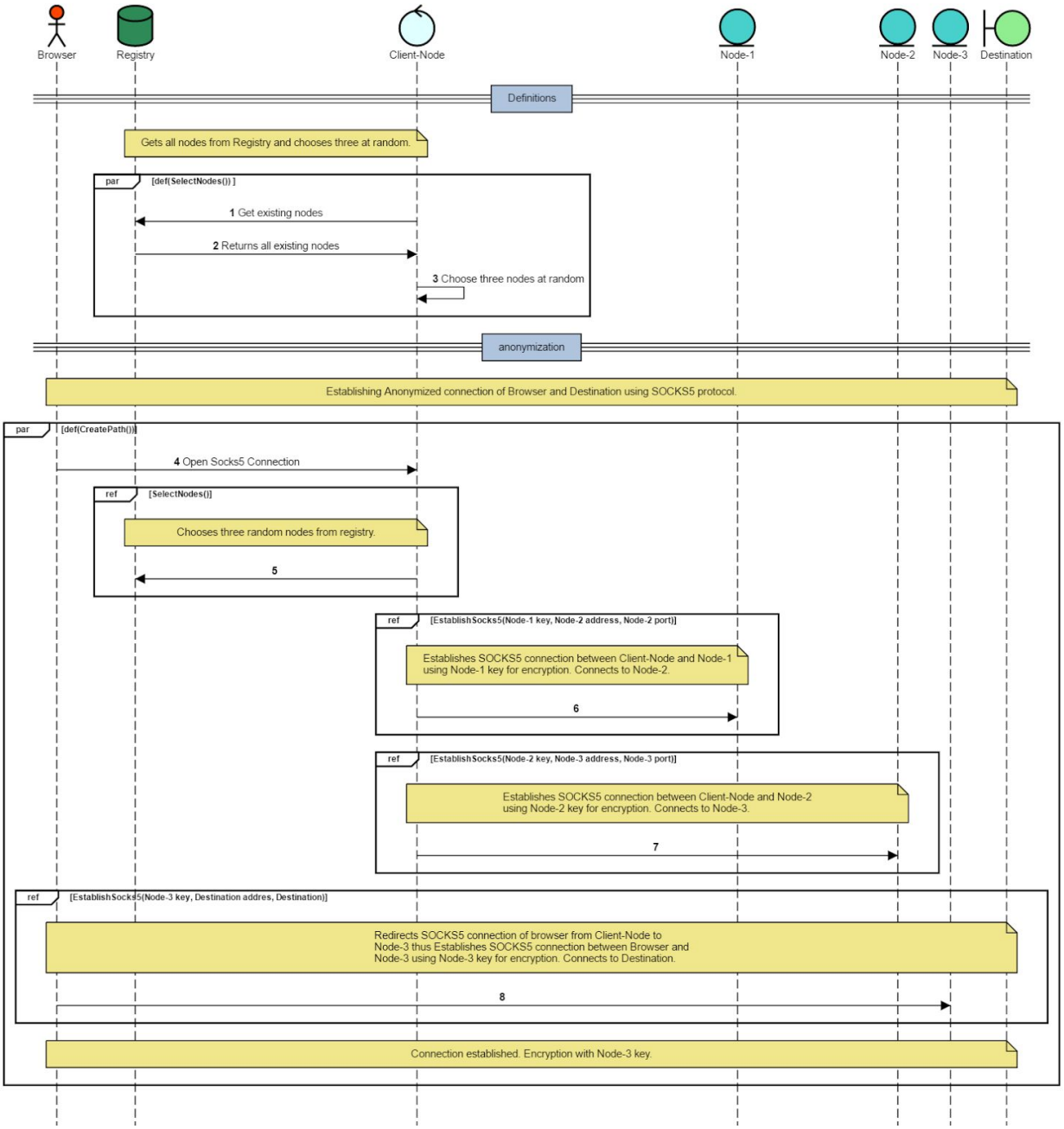


Stage	Description
1	Browser opens a socks5 connection to one of the onion nodes
2	Node selects 3 random notes from the registry
3	Entry node opens a socks5 connection to the 1st note
4	Entry node opens a socks5 connection using 1st node to the 2nd node
5	Entry node opens a socks5 connection using the 2nd node to the 3rd node
6	Entry node redirects everything from the incoming sock5 into the 3rd node socks5

Onion Routing: Generic Utilities



Onion Routing: Sequences



הרקע התיאורטי

תיאור כל רקע תיאורטי שעוסקים בו.
לדוגמה, מהי הצפנה, מהי כספת, מעגלי הגנה, traceroute, tunnel, proxy
זהו החלק שמראה מה נלמד בעולם התוכן הכללי ללא קשר ישיר לפרויקט.
הגדרת מושגים, מילות מפתח והפניות, הקשורים בנושא
תת סעיף טכנולוגיה - מכלול הטכנולוגיות שהפרויקט משתמש בהן ותיאור קצר כיצד, נשלח בעבר תיאור קצר בנושא זה.

ניתוב בצל - Onion Routing

טכנולוגיות

- **תקשורת אסינכרונית** (Asynchronous I/O) - סוג תקשורת הנותן אפשרות לשלוח מסרים בתוך ערוץ תקשורת מבלי לחכות שהצד המקבל מוכן. באמצעות השימוש במערכת אסינכרונית קיימת אפשרות לעבודה מקבילית הן של שליחה והן של קבלת הודעות ממספר חיבורים, ובכך ליצור תקשורת רבת משתמשים תוך שימוש בתהליך יחיד.
- **שרת** - תוכנת מחשב המספקת שירותים לתכנות לקוח באמצעות תקשורת ברשתות.
- **פרוטוקול SOCKS 5** - פרוטוקול תקשורת המאפשר יצירת ערוץ תקשורת בין לקוח אל יעדו תוך מעבר דרך שרת socks אליו מתחבר תחילה הלקוח. תקשורת דרך פרוטוקול זה מתבצעת ע"י שליחה של מספר הודעות בין הלקוח לשרת socks אשר מאמתות חיבור ביניהם ולאחר מכן שליחת בקשה לחיבור עם היעד של הלקוח. עם קבלת החיבור שרת הsocks הופך לשרת פרוקסי בין הלקוח ויעדו.
- **פרוטוקול HTTP** - פרוטוקול תקשורת בשכבת היישום הנועד להעברת דפי HTML ברשתות אינטרנט. תקשורת בפרוטוקול זה מתבצעת ע"י שיחה בפרוטוקול TCP בין השרת ללקוח המורכבת מבקשות ותשובות (request/response). לאחר יצירת חיבור בין השרת ללקוח, הלקוח שולח לשרת בקשה אשר על השרת לפענח ולשלוח תשובה בהתאם. בתום שליחת התשובה השרת לרוב מנתק ומסיים את החיבור עם הלקוח.
- **פרוטוקול TCP** - פרוטוקול תקשורת בשכבת התעבורה המשמש להעברת נתונים בין שרת ללקוח באופן אמין וללא איבוד מידע.
- **Proxy** (שרת פרוקסי) - זהו שרת שתפקידו לחבר בין לקוח ליעד מסוים, כאשר הוא משמש כמתווך ביניהם. כלומר, הלקוח מתחבר לשרת הפרוקסי ושולח אליו את המידע והיעד מקבל את המידע הזה משרת הפרוקסי ולהיפך.
- **הצפנה** - תהליך בו על ידי אלגוריתם כלשהו מעבדים מידע על מנת להפוך אותו לגורמים מסוימים ולאבטח אותו מפני גורמים אחרים.
  - הצפנת בסיסים מבוססת xor - הפרויקט משתמש בהצפנה בסיסים המבוססת אשר לוקחת מידע ומשנה אותו באמצעות פעולת הxor לפי מפתח נותן כלשהו.
- **שפת Python** - שפת תכנות דינמית נפוצה. תוכננה לצורך שימוש בפשטות במבני נתונים מסובכים.
- **שפת HTML** - שפת תגיות לתצוגה ועיצוב של דפי אינטרנט בדפדפן.
- **CSS** - פורמט לעיצוב דפי אינטרנט.
- **שפת JavaScript** - שפת תכנות דינמית מונחית עצמים המותאמת להרצה בדפי אינטרנט.
- **XML** - תקן לייצוג מבני נתונים במחשב. מאפשר דרך נוחה לשמור נתונים על אובייקטים.
- **SIGINT** -

- **SIGTERM** -
- **SIGALRM** -
- **תכנות מונחה עצמים** - שיטת תכנות המבוססת על חלוקת התכנית לאובייקטים בעלי תכונות ופונקציות ייחודיות. מאפשרת לחלק את התכנית לתיאורים נפרדים של כל רכיבי המערכת המפותחת.

מימוש

דיאגרמת בלוקים
מבני נתונים
פרוטוקולי תקשורת

מכונות מצבים
אתגרים במימוש ודרך הפתרון

בעיות ידועות

בעיות ידועות (אם קיימות) ופתרונות אפשריים.
מגבלות הן גם בעיות ידועות.

התקנה ותפעול

הוראות התקנה מפורטות
הוראות תפעול מלאות הכוללות צילומי מסך
צילומי המסך יכולים להיות גם של מערכות אחרות שמבצעות שימוש במערכת שלכם (באם ישנו מצב שכזה)
היכן נמצא ה-log file ודוגמה ל-log במקרים שבהם אין אינטראקציה, לדוגמה ב-proxy יש להראות log של בקשה ראשונה שאינה נמצאת ב-cache ולאחר מכן בקשה שכן.

תוכניות עתיד

כיצד אפשר לקחת את הפרויקט צעד אחד קדימה (לפחות).
תת סעיף עבור כל רעיון.

פרק אישי

סיכום המתאר את תהליך העבודה על הפרויקט עם התייחסות אישית.
קשיים, אתגרים, תובנות.

תיעוד קוד

בעזרת כלי אוטומטי.
לאלו שעובדים ב-github ניתן להעלות את הפלט כ-zip כקובץ מצורף ל-release.

קוד פרויקט

קישור ל-google drive המכיל zip עם הקוד ותיק הפרויקט.
לאלו שעובדים ב-github ניתן לצרף קישור ל-release.