Digital Whisper
Technologic Papers

Key-Logger, Video, Mouse - חלק ג': זה הזמן ללכלך את הידיים

מאת ליאור אופנהיים ויניב בלמס

הקדמה

שלום וברוכים השבים לחלק מספר 0x3 במאמר שלנו. לאחר הפסקה קצרה למנוחה, אגרנו כוחות חדשים ואנחנו מוכנים להמשיך שוב במלחמת החורמה חסרת הפשרות שלנו שמטרתה יחידה - להפוך KVM שולחני תמים למפלצת Key-Logging חסרת רסן.

תקציר הפרקים הקודמים:

- יום בהיר אחד החלטנו לנסות וליישם Key-Logger בתוך ה-KVM שמונח על שולחננו.
- כדי לעשות את זה אנו צריכים להשיג את הקושחה של ה-KVM, לנתח אותה, להבין כיצד הכל עובד, ואז לשנות אותה כדי שתתאים למטרתנו הזדונית.
- מסתבר של-KVM שלנו יש אפשרות לעידכון קושחה שמתבצע באמצעות כבל סיריאלי.
- הסנפנו את התעבורה העוברת על הכבל הסיריאלי, פענחנו את הפרוטוקול וחילצנו את המידע שעובר בו, אבל כל מה שהצלחנו למצוא היה BLOB גדול וחסר משמעות לחלוטין.
- בכדי לנסות ולהבין איך ה-KVM בכלל בנוי, וכיצד הוא מעודכן החלטנו לנצל את כישורינו ובעזרת מברג פיליפס וקצת כח ברוטלי. פרקנו את המארז וחשפנו את הלוח ואת רכיבי ה-KVM הפנימיים.
- להפתעתנו מצאנו צ'יפ מאוד מעניין העונה לשם Winbond 8052. כיוון שזה צ'יפ מאוד נפוץ ומאוד ורסטילי בעולם ה-Embedded החלטנו לבדוק כיצד הוא מתנהג בזמן עידכון הקושחה.
- באמצעות "הצעצוע" האהוב עלינו - Logic Analyser - הקלטנו את המתחים המתקבלים/נשלחים ברגלי ה-UART של הצ'יפ.
- לאחר ניתוח של המתחים הללו גילינו להפתעתנו את אותו ה-BLOB ממקודם.
- עכשיו, כל שנותר לנו לנסות ולהבין הוא איך לעזאזל אנחנו יכולים לפענח את ה-BLOB הזה כדי לקבל קוד אסמבלי 8051 קריא.

מתחילים

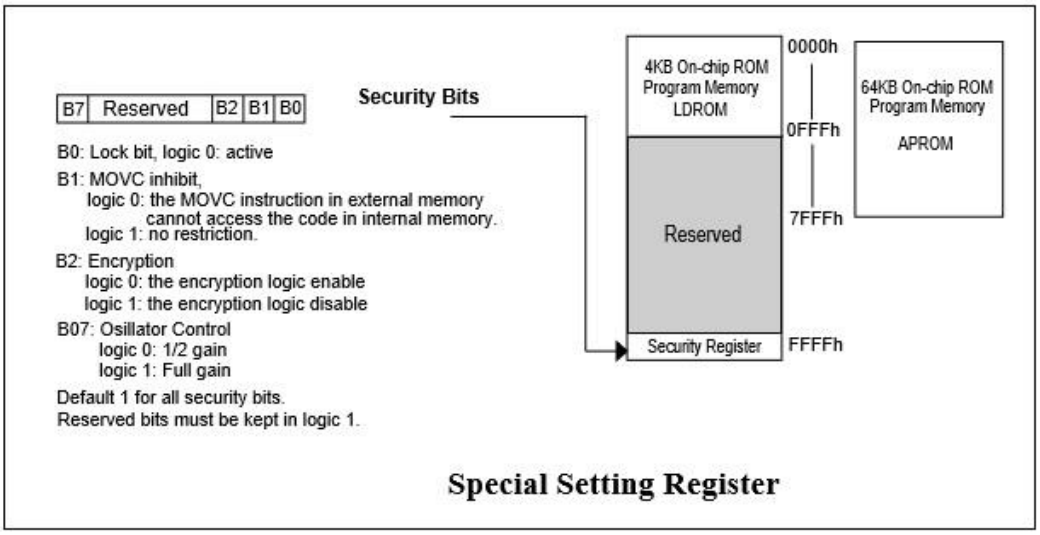
הדבר הראשון שכדאי לעשות במקרים כאלו, הוא לפנות בחזרה ל-Specs של הצ'יפ. לאחר נבירה ממשוכת במעגלים אלקטרוניים, הגדרות מתחים, ועוד כל מיני דברים מפחידים כאלו, הצלחנו להבין שבתוך הצ'יפ שלנו קיימים 2 ROM-ים נפרדים.

האחד הוא ה-ROM הראשי, הנקרא APROM. הוא מכיל את הקושחה עצמה ובזמן הפעלה רגילה של ה-KVM הוא נטען לזיכרון ומריץ את קושחת ה-KVM.

השני הוא ה-ROM המשני, הוא קטן בהרבה, ונקרא LDROM. תפקידו היחידי של ה-LDROM הוא לבצע את תהליך עידכון הקושחה. כשמכניסים את המכשיר למצב עידכון קושחה, ה-LDROM נטען לזיכרון והוא אחראי לקבל את המידע מממשק ה-UART, לתרגם אותו לאסמבלי תקין, ולעדכן את ה-APROM בגרסה החדשה.

אבל איך כל זה עוזר לנו?

טוב, אז האמת שזה לא כל כך עוזר... אבל זה כן מלמד אותנו שתהליך הפענוח של ה-BLOB שלנו מיושם בתוך מרחב זיכרון יחסית קטן (4K) ולכן הוא לא יכול להיות כל-כך מסובך. או ככה לפחות אנחנו מקווים...

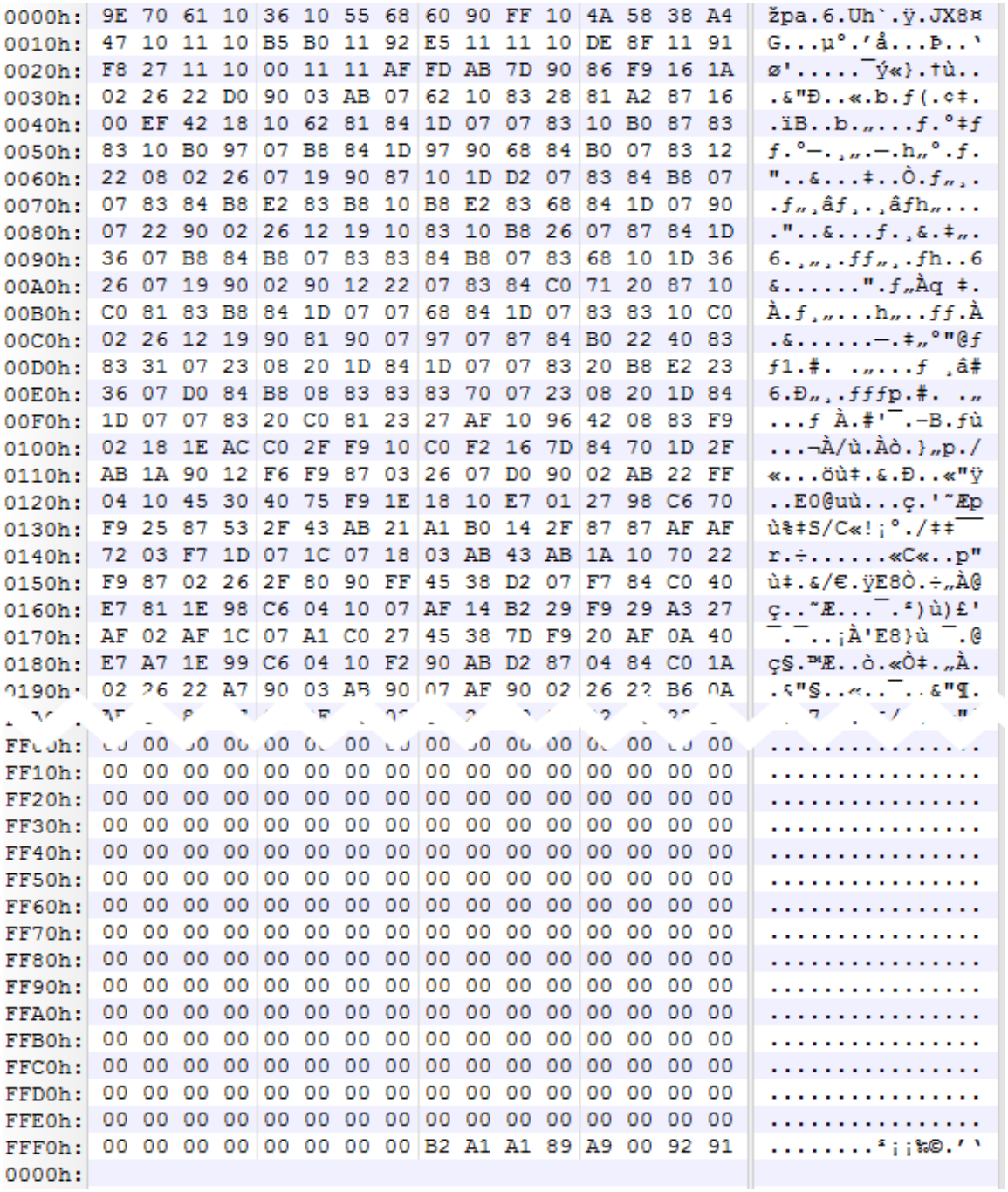


Special Setting Register

זה הזמן לשים בצד את מברגי הפיליפס, את מד המתח ואפילו את ה-Logic Analyser (סניף סניף), ולהתחיל ללכלך את הידיים בקצת ניתוח בינארי ישן וטוב.

אז רק לתזכורת, בחלק הראשון במאמר כבר שמנו לב שסוף ה-BLOB שלנו מרופד בבית מסוים.

הנחנו שהפעולה הנכונה לעשות תיהיה לקסר (מלשון XOR) את כל ה-BLOB בבית הזה, וזו התוצאה:



```
0000h: 9E 70 61 10 36 10 55 68 60 90 FF 10 4A 58 38 A4  žpa.6.Uh`.ÿ.JX8¤
0010h: 47 10 11 10 B5 B0 11 92 E5 11 11 10 DE 8F 11 91  G...µ°.'å...Þ..'
0020h: F8 27 11 10 00 11 11 AF FD AB 7D 90 86 F9 16 1A  ø'.....¯ý«}.†ù..
0030h: 02 26 22 D0 90 03 AB 07 62 10 83 28 81 A2 87 16  .&"Ð..«.b.ƒ(.¢‡.
0040h: 00 EF 42 18 10 62 81 84 1D 07 07 83 10 B0 87 83  .ïB..b.„...ƒ.°‡ƒ
0050h: 83 10 B0 97 07 B8 84 1D 97 90 68 84 B0 07 83 12  ƒ.°—.¸„.—.h„°.ƒ.
0060h: 22 08 02 26 07 19 90 87 10 1D D2 07 83 84 B8 07  "..&...‡..Ò.ƒ„¸.
0070h: 07 83 84 B8 E2 83 B8 10 B8 E2 83 68 84 1D 07 90  .ƒ„¸âƒ¸.¸âƒh„...
0080h: 07 22 90 02 26 12 19 10 83 10 B8 26 07 87 84 1D  ."..&...ƒ.¸&.‡„.
0090h: 36 07 B8 84 B8 07 83 83 84 B8 07 83 68 10 1D 36  6.¸„¸.ƒƒ„¸.ƒh..6
00A0h: 26 07 19 90 02 90 12 22 07 83 84 C0 71 20 87 10  &......".ƒ„Àq ‡.
00B0h: C0 81 83 B8 84 1D 07 07 68 84 1D 07 83 83 10 C0  À.ƒ¸„...h„..ƒƒ.À
00C0h: 02 26 12 19 90 81 90 07 97 07 87 84 B0 22 40 83  .&......—.‡„°"@ƒ
00D0h: 83 31 07 23 08 20 1D 84 1D 07 07 83 20 B8 E2 23  ƒ1.#. .„...ƒ ¸â#
00E0h: 36 07 D0 84 B8 08 83 83 83 70 07 23 08 20 1D 84  6.Ð„¸.ƒƒƒp.#. .„
00F0h: 1D 07 07 83 20 C0 81 23 27 AF 10 96 42 08 83 F9  ...ƒ À.#'¯.–B.ƒù
0100h: 02 18 1E AC C0 2F F9 10 C0 F2 16 7D 84 70 1D 2F  ...¬À/ù.Àò.}„p./
0110h: AB 1A 90 12 F6 F9 87 03 26 07 D0 90 02 AB 22 FF  «...öù‡.&.Ð..«"ÿ
0120h: 04 10 45 30 40 75 F9 1E 18 10 E7 01 27 98 C6 70  ..E0@uù...ç.'˜Æp
0130h: F9 25 87 53 2F 43 AB 21 A1 B0 14 2F 87 87 AF AF  ù%‡S/C«!¡°./‡‡¯¯
0140h: 72 03 F7 1D 07 1C 07 18 03 AB 43 AB 1A 10 70 22  r.÷.....«C«..p"
0150h: F9 87 02 26 2F 80 90 FF 45 38 D2 07 F7 84 C0 40  ù‡.&/€.ÿE8Ò.÷„À@
0160h: E7 81 1E 98 C6 04 10 07 AF 14 B2 29 F9 29 A3 27  ç..˜Æ...¯.²)ù)£'
0170h: AF 02 AF 1C 07 A1 C0 27 45 38 7D F9 20 AF 0A 40  ¯.¯..¡À'E8}ù ¯.@
0180h: E7 A7 1E 99 C6 04 10 F2 90 AB D2 87 04 84 C0 1A  ç§.™Æ..ò.«Ò‡.„À.
0190h: 02 26 22 A7 90 03 AB 90 07 AF 90 02 26 22 B6 0A  .&"§..«..¯..&"¶.
FFC0h: 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00  ................
FFD0h: 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00  ................
FFE0h: 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00  ................
FFF0h: 00 00 00 00 00 00 00 00 B2 A1 A1 89 A9 00 92 91  ........²¡¡‰©.'.
0000h:
```

נראה יחסית טוב, לא? מכיוון שקיסור של בית עם עצמו נותן תמיד את התוצאה אפס, סוף ה-BLOB שלנו מרופד עכשיו באפסים. כמובן שיכול ליהיות שאנחנו טועים וזו לא הפעולה הנכונה, אבל ישנן שתי אפשרויות מאוד נפוצות לריפוד בעולם הקושחות: אחת היא ריפוד באפסים - מה שקיבלנו עכשיו, והשניה היא ריפוד ב-NOP, אך מכיוון שבאסמבלי 8051 NOP מיוצג על יד הבית אפס חסכנו גם את הבעיה הזו ☺

כעת, העניין הוא שאנחנו די בטוחים שה-BLOB הזה לא מוצפן, וגם לא דחוס, מכיוון שרמת האנטרופיה שלו מאוד נמוכה, אנו גם בטוחים שהוא מתורגם בסופו של דבר לאסמבלי 8051 אז מה שנותר הוא רק איזשהי שיטת קידוד/עירבול שמסתירה מאיתנו את הקוד ואותה אנחנו צרכים לנסות לפצח.

חדי ההבחנה בינכם אולי שמו לב למשהו שנראה קצת חשוד בסוף ה-BLOB שלנו. אם תסתכלו בשמונת הבתים האחרונים, תראו שהם שונים.

מהם שמונת הבתים האלו? האם הם רמז שהשאיר לנו מפתח Embedded משוגע? אולי הם הסוד לפיצוח הקידוד הזה?

כדי לנסות ולענות על השאלה הזו, בואו ננסה להסתכל בשמונת הבתים האלו בגרסאות קושחה שונות:

מספר גרסא	8 הבייטים האחרונים
3.3.312	91 99 99 89 91 B2 99 00
4.1.401	B2 92 89 81 A1 99 A1 89
4.2.411	92 00 A1 A1 89 B2 89 91
4.2.414	91 92 A1 89 A1 A1 B2 00
4.2.415	B2 A1 A1 89 A9 00 92 91
4.2.416	A1 92 00 89 B1 91 A1 B9
4.2.417	92 00 A1 89 91 B2 A1 B9
4.2.418	00 A1 92 91 C1 B2 A1 89
4.2.419	00 91 A1 B2 C9 89 A1 92

מחשב, מחשב...

ע"י איזון עדין של רמת האלכוהול בדם אנחנו מצליחים להסיק שתי מסקנות עיקריות מהטבלה הנ"ל: ראשית, נראה שתופעת שמונת הבתים האחרונים השונים היא עקבית בכל גרסאות הקושחה שהורדנו. ושנית, והרבה יותר חשוב מכך, נראה שיש קורלציה מסוימת בין מספר הגרסה לבין שמונת הבתים האלו. לדוגמא מספר המופעים של הבית 'A1' בשמונת הבתים האחרונים זהה למספר המופעים של הספרה '4' במספר הגרסא, מופעי הבית '89' מתאימים למופעי הספרה '1', וכן הלאה.

איזה פעולה לוגית תייצר תופעה כזו? בואו ננסה לרשום את המיפוי שייצרנו בין ספרות לבתים, ומכיוון שאנו חושדים בפעולה בינארית מסויימת, נוסיף גם את הערך הבינארי של כל בית:

ערך הסיפרה במספר הגרסא	ערך הבית	ערך הבית בבסיס בינארי
1	0x89	10001001
2	0x91	10010001
3	0x99	10011001
4	0xA1	10100001
5	0xA9	10101001
6	0xB1	10110001
7	0xB9	10111001
8	0xC1	11000001
9	0xC9	11001001

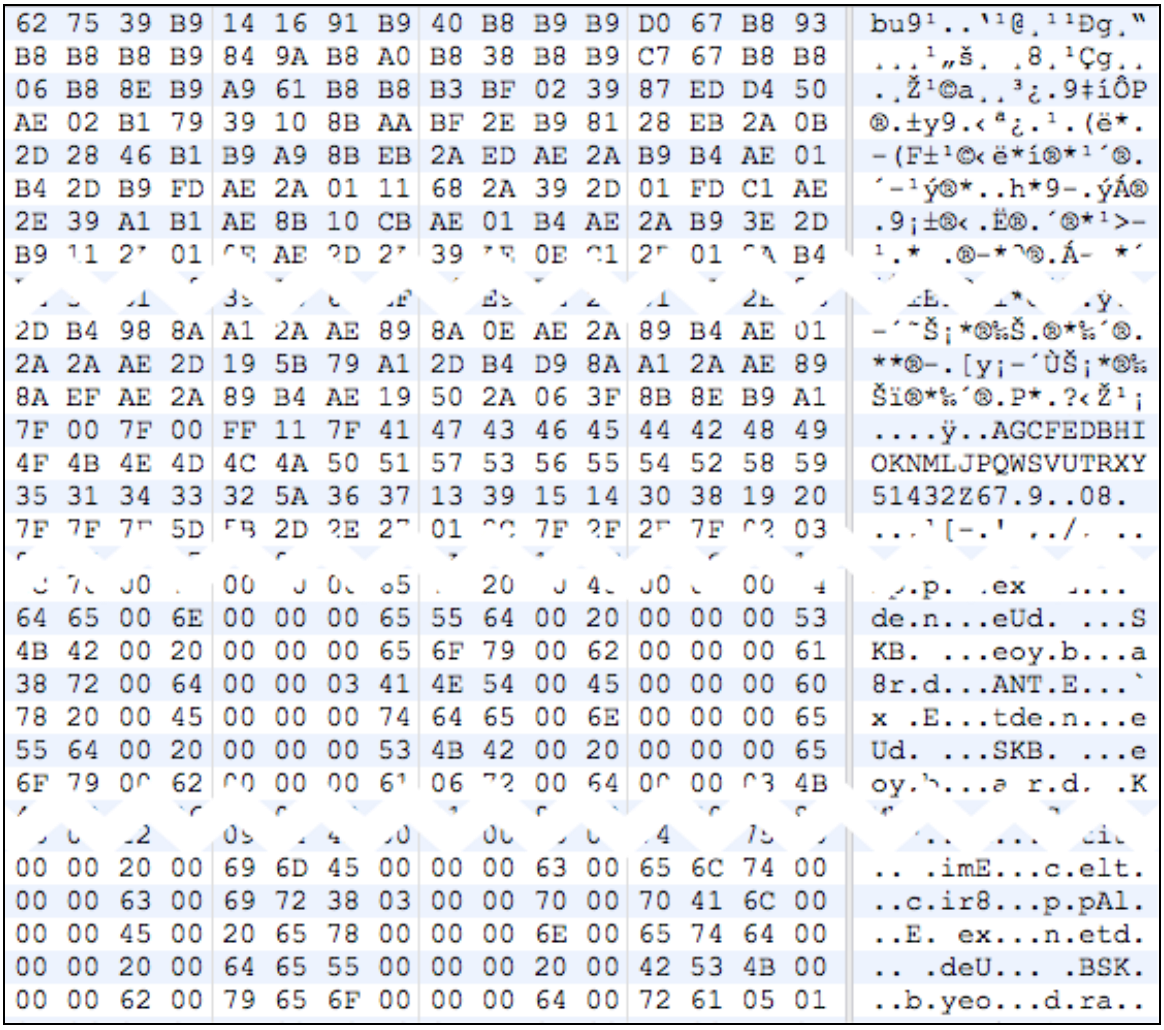
הערך הבינארי מייצר תבנית ברורה, אשר מסומנת לנוחיותכם בצבעים אדום ושחור. כל ערך בינארי בטבלה מורכב משני חלקים, האחד קבוע (בשחור) והשני משתנה (באדום), ולא סתם משתנה, אלא יוצר Counter בינארי שמקודם באחד עבור כל ספרה.

אוקי, Counter זה הגיוני, אבל למה הוא נמצא באמצע הייצוג הבינארי? היה יותר הגיוני לראות אותו בצד ימין. חבל שהוא לא שם... אבל הוא יכול להיות! כן, ברור! אנחנו יכולים "לסובב" את כל הערכים הבינארים האלו ב-3 על ידי הפעולה הלוגית Rotate-Right. ותנחשו אילו ערכים מקבלים לאחר ה"סיבוב" הזה?

ערך הסיפרה במספר הגרסא	ערך הבית	ערך הבית בבסיס בינארי	ערך הבית בבסיס בינארי לאחר סיבוב ב-3	ערך דצימלי
1	0x89	10001001	00110001	49
2	0x91	10010001	00110010	50
3	0x99	10011001	00110011	51
4	0xA1	10100001	00110100	52
5	0xA9	10101001	00110101	53
6	0xB1	10110001	00110110	54
7	0xB9	10111001	00110111	55
8	0xC1	11000001	00111000	56
9	0xC9	11001001	00111001	57

הבנתם?

הערך הדצימלי שקיבלנו הוא באופן מפתיע ערך ה-ASCII המתאים לערך הסיפרה במספר הגרסה. ומה יקרה אם נבצע את פעולת הסיבוב הזאת על כל ה-BLOB?



```
62 75 39 B9 14 16 91 B9 40 B8 B9 B9 D0 67 B8 93   bu9¹..'¹@¸¹¹Ðg¸"
B8 B8 B8 B9 84 9A B8 A0 B8 38 B8 B9 C7 67 B8 B8   ...¹„š¸ ¸8¸¹Çg¸¸
06 B8 8E B9 A9 61 B8 B8 B3 BF 02 39 87 ED D4 50   .¸Ž¹©a¸¸³¿.9‡íÔP
AE 02 B1 79 39 10 8B AA BF 2E B9 81 28 EB 2A 0B   ®.±y9.‹ª¿.¹.(ë*.
2D 28 46 B1 B9 A9 8B EB 2A ED AE 2A B9 B4 AE 01   -(F±¹©‹ë*í®*¹´®.
B4 2D B9 FD AE 2A 01 11 68 2A 39 2D 01 FD C1 AE   ´-¹ý®*..h*9-.ýÁ®
2E 39 A1 B1 AE 8B 10 CB AE 01 B4 AE 2A B9 3E 2D   .9¡±®‹.Ë®.´®*¹>-
B9 11 2? 01 ?? AE ?D 2? 39 ?? 0E ?1 2? 01 ?? B4   ¹.* .®-*?®.Á- *´
                                                  
                                                  
2D B4 98 8A A1 2A AE 89 8A 0E AE 2A 89 B4 AE 01   -´˜Š¡*®‰Š.®*‰´®.
2A 2A AE 2D 19 5B 79 A1 2D B4 D9 8A A1 2A AE 89   **®-.[y¡-´ÙŠ¡*®‰
8A EF AE 2A 89 B4 AE 19 50 2A 06 3F 8B 8E B9 A1   Šï®*‰´®.P*.?‹Ž¹¡
7F 00 7F 00 FF 11 7F 41 47 43 46 45 44 42 48 49   ....ÿ..AGCFEDBHI
4F 4B 4E 4D 4C 4A 50 51 57 53 56 55 54 52 58 59   OKNMLJPQWSVUTRXY
35 31 34 33 32 5A 36 37 13 39 15 14 30 38 19 20   51432Z67.9..08.
7F 7F 7? 5D ?B 2D ?E 2? 01 ?? 7F ?F 2? 7F ?? 03   ...']-.' ../. ..
                                                  
                                                  
64 65 00 6E 00 00 00 65 55 64 00 20 00 00 00 53   de.n...eUd. ...S
4B 42 00 20 00 00 00 65 6F 79 00 62 00 00 00 61   KB. ...eoy.b...a
38 72 00 64 00 00 03 41 4E 54 00 45 00 00 00 60   8r.d...ANT.E...`
78 20 00 45 00 00 00 74 64 65 00 6E 00 00 00 65   x .E...tde.n...e
55 64 00 20 00 00 00 53 4B 42 00 20 00 00 00 65   Ud. ...SKB. ...e
6F 79 0? 62 ?0 00 00 6? 06 ?? 00 64 0? 00 ?3 4B   oy.?...? r.d. .K
                                                  
                                                  
00 00 20 00 69 6D 45 00 00 00 63 00 65 6C 74 00   .. .imE...c.elt.
00 00 63 00 69 72 38 03 00 00 70 00 70 41 6C 00   ..c.ir8...p.pAl.
00 00 45 00 20 65 78 00 00 00 6E 00 65 74 64 00   ..E. ex...n.etd.
00 00 20 00 64 65 55 00 00 00 20 00 42 53 4B 00   .. .deU... .BSK.
00 00 62 00 79 65 6F 00 00 00 64 00 72 61 05 01   ..b.yeo...d.ra..
```

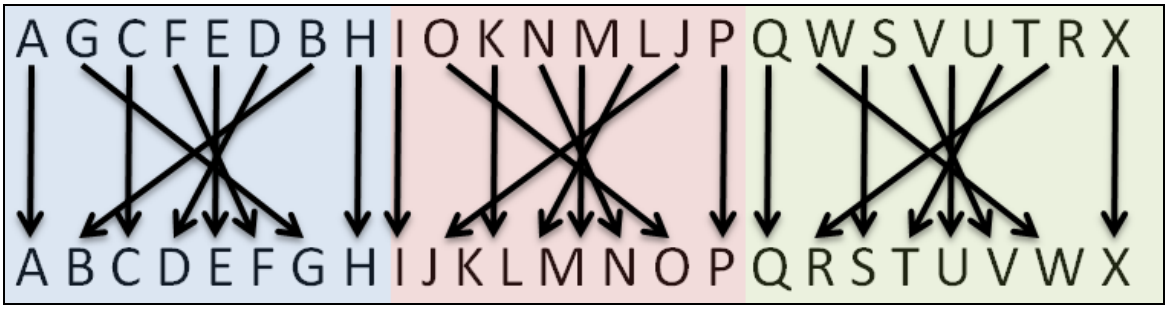
וואו, עכשיו זה נראה הרבה יותר טוב. יש כאן מה שנראה כמו מחרוזות. אבל, זה עוד לא מושלם. משהו עדיין לא תקין.

יהיה יותר קל להסביר מה הבעיה אם נתבונן במחרוזת הבאה מהתמונה שלמעלה:

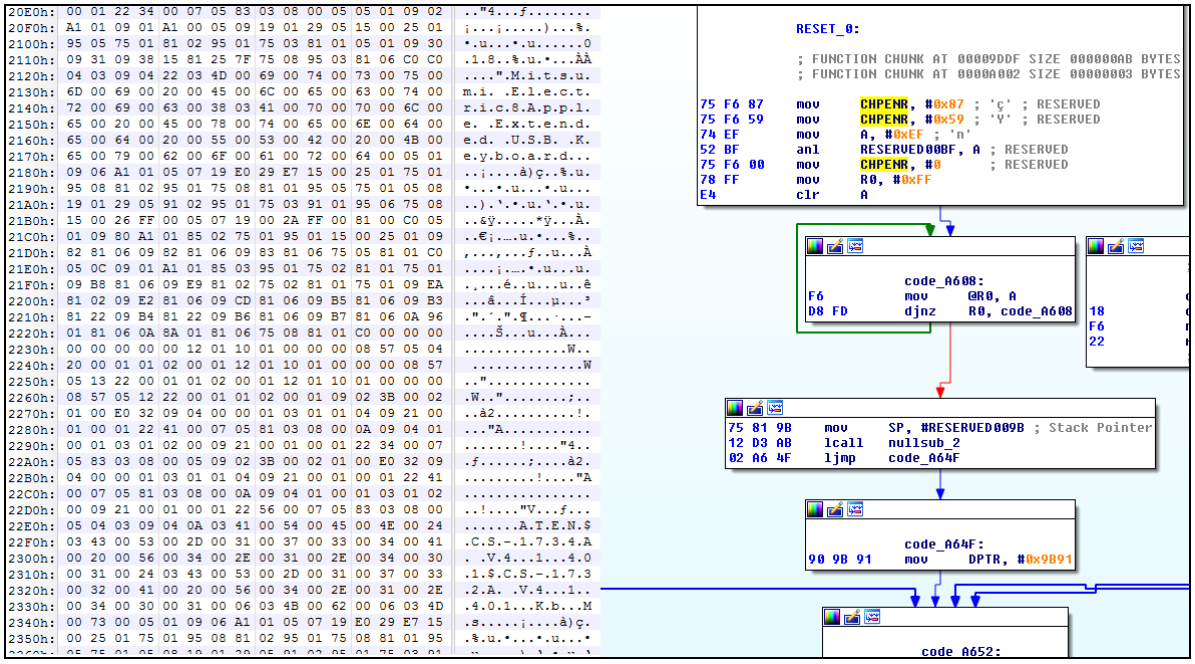
```
AGCFEDBHIOKNMLJPQWSVUTRXY
```

נראית כמו רצף אלפא-נומרי, נכון? אבל משהו פה פשוט לא נראה בסדר הנכון.

אם תתבוננו ממש טוב, תשימו לב שיש כאן סוג של פרמוטציה שמתבצעת עבור כל שמונה בתים, הטבלה הבאה מייצגת את זה קצת יותר טוב:



אז אם נמשיך לעבוד על פי השיטה שלנו, ונבצע את אותה הפרמוטציה על כל בלוק של שמונה בתים ב-BLOB, בעצם נקבל:



כן! מחרוזות! אסמבלי!

זהו קוד אסמבלי 8051 אמיתי, זה הקוד שמריץ את ה-KVM ואחריו רדפנו עד עכשיו. זהו זה KVM, Game-Over. עכשיו הובסת סופית. כל מה שנותר לנו זה להבין מה האסמבלי הזה עושה, ולשנות אותו כך שנוכל ליישם Key-Logger.

אבל רגע, בשביל זה צריך להבין אסמבלי 8051, לא?

המשך יבוא...

נ.ב

מכיוון שמאמר זה תיאר את הפיתרון המלא, אנו מסיימים בזאת את תחרות פריצת ה-BLOB עליה הכרזנו במאמר הראשון.

אנחנו רוצים לציין כאן שני אנשים שפנו אלינו והציגו פתרון נכון ומלא. **חברים - כל הכבוד**.

1. הראשון שפתר את החידה היה - 0x3D5157636B525761 - שהכינוי שלו הוא חידה בפני עצמה.
2. השני היה שד טזמני מסוים שמבקש גם הוא להישאר בעילום שם.