המלצות לאיסוף מידע גלוי ברשת תוך שימור שרשרת ראייתית

מהדורה 1.0 – 22 באוקטובר 2023

מטרת המסמך להצביע על **best practices** לאיסוף מידע ממקורות גלויים (open source intelligence) תוך שמירה על "שרשרת ראייתית". **"שרשרת ראייתית"** נועדה להוביח במועד מאוחר כי הפריט המוצג הוא אכן הפריט שנמצא בזירה הדיגיטלית וכי הוא לא השתנה.

הבהרה: יש הבדל בין איסוף מודיעיני לבין איסוף שמטרתו הגשת ראיות בהליך משפטי. ההמלצות שלהלן נועד למקרים שבהם יש כוונה לעשות שימוש ראייתי או יש עניין לשמור אופציה זו.

מי אנחנו

אנחנו קבוצה של כשלושים משפטנים ומשפטניות שעוסקים בתחומי הקניין הרוחני, פרטיות אינטרנט, מהאקדמיה ומהפרקטיקה, שפועלים כדי לסייע בייעוץ משפטי ראשוני למיזמים חברתיים, לא מסחריים, שמבקשים לקדם פעולות חברתיות בזמן המלחמה, לטובת אזרחי ישראל. אנו פועלים בהתנדבות. פירוט חברי וחברות הקבוצה נמצא כאן.

פנו אלינו

אנו זמינים לשאלות בנוגע למסמך זה בפניה בדואר אלקטרוני - law.co.il@101.

מסמך זה יתעדכן בהתאם לצורך לפי ההערות שיתקבלו.

כללי

ההמלצות שלהלן מבוססות על "פרוטוקול ברקלי"[1] וכללים מקובלים בתחום הראיות הדיגיטליות. הן מתארות פרקטיקות מקובלות בתחום זה. **אם יימצא קושי ליישם את כולן בהתארגנות התנדבותית, מומלץ להקפיד לפחות על תיעוד מינימלי ביחס להיבטים הבאים של פעולת האיסוף והשמירה**: (1) מהו מקור התוכן; (2) מתי ואיך נשמר; (3) האם בוצעה בדיקה לגבי תקינות ההורדה שלו והוא נמצא

---

[1] Human Rights Center at UC Berkely School of law, United Nations Human Rights Office of the High Commissioner, Berkely Protocol on Digital Open Source Investigations.
"פרוטוקול ברקלי" נבחר כמסמך מנחה מהסיבות הבאות: 1. הוא פורסם בידי משרד האו"ם לזכויות אדם; 2.הוא נועד להנחות כיצד לתעד הפרות של זכויות אדם; 3. המסמך נועד לשימוש גם של גורמי החברה האזרחית.

זהה למקור; (4) יש לשמור את התוכן במדיה ספציפית כגון כונן קשיח ייעודי; (5) נעשתה הפרדה של איזור הארכוב של התוכן מאיזור אישי.

מסמך ההמלצות נחלק לשני חלקים - חלק א' הכולל עקרונות כללים, וחלק ב' המכיל תבנית לתיעוד האיסוף והשמירה.

חלק א' – עקרונות כללים לשרשרת ראייתית

1. כללי

א. האחראי על האיסוף והתיעוד יכונה פה "חוקר", והמידע שהוא אסף יכונה "היעד".

ב. על החוקר לייצר תיעוד לפעילות החקירה, הן בשלב האיסוף והן בשלב השמירה, ולהראות את הקשר בין היעד שאסף לבין המידע ששמר.

2. איסוף

א. היעד ישמר בקובץ.

ב. המידע על **היעד** צריך לכלול את שני אלה -

i. חותמת זמן של הקובץ שנשמר.

ii. סוג הקובץ שבו מצוי המידע שהורד.

ג. יש לתעד את מירב הפרטים על הפעילות כגון אופן הגלישה, הדפדפן, המשתמש שהיה מחובר בעת הגלישה, צילום מסך של מקור המידע ופרטי התיעוד של ביצוע ההורדה, לרבות חותמת הזמן של הקובץ המקורי.

ד. יש לתעד את הכלים שהחוקר השתמש בהם. תיעוד כזה יכול להיעשות באמצעות הטופס המצורף בנספח ב' או בשילוב תוכנה ייעודית.

ה. אחת הבעיות העיקריות באיסוף מידע מהרשת הוא קיומו של מידע כוזב. יש לציין בתיעוד ההורדה האם בוצעה בדיקה לגבי מהימנות המידע, ומה תוצאותיה. יש לציין את פרטי המקור שממנו הורד המידע ומי הגורם שמשייכים לו את המידע. רישום זה צריך להיות חלק מתיעוד החקירה כדי שבשלב מאוחר יותר ניתן יהיה לשייך בין הדברים.

3. שימור ותיעוד

א. שמירת המידע צריכה להיעשות בהתאם להוראות אבטחת מידע שמגנות על המידע מפני גישה לא מורשית.

ב. יש לשמור את המידע על גבי מדיה ייעודית לזה, שניתן להעבירה לגורמי החקירה והאביפה, לדוגמה דיסק קשיח חיצוני.

ג. יש מלכתחילה ליצור שני עותקים של מידע שהורד, ולבצע פעולות רק על גבי עותקים.

ד. יש לשמור את קובץ היעד בפורמט שאינו ניתן לשינוי, תוך תיעוד חותמת הזמן של מועד השמירה. את החומרים שהורדו יש לשמור בקפסולה ולחתום אותה בחתימת HASH - SHA-256/MD5

ה. בדי שניתן יהיה להראות שהמידע שנשמר לא השתנה מאז שהורד יש לבצע בדיקה כפולה – של חתימת הקבצים ושל חותמת הזמן שלהם.

ו. יש לתעד את אופן ביצוע הקפסולציה, כפי שמוצע למשל בטופס בחלק ב'.

ז. Audit trail - יש חשיבות ליכולת לתאר מה קרה עם פריט מרגע שהועתק.

ח. יש לשמר מידע שנאסף לצרכי ראייה כשהוא נאמן למקור מרגע שהורד ועד להגשתו בפני ערכאה משפטית. לכן יש לצמצם את מורשי הגישה לעותק אך ורק למי שנדרש לכך לצורך הגשת היעד בראיה בהליך משפטי.

חלק ב' – טופס תיעוד, בעמוד הבא ▼

חלק ב'- טופס תיעוד

- ← כבל שנעשה שימוש ב**כלי אוטומטי**, רצוי לתעד את קינפוג הכלי בהתאם למאפיינים אלה.
- ← אם מבוצע תיעוד ידני, קובץ אקסל הכולל את הטופס מצורף למסמך זה, לנוחותכם.

בעת **איסוף** מידע דיגיטלי יש לתעד בכל הניתן את הפרטים שלהלן:

1. פרטים על החוקר

א. מהות החקירה

ב. שם החוקר.

ג. כתובת ip של החוקר.

ד. תחילת איסוף (חותם זמן)

ה. סוף איסוף (חותם זמן).

2. מידע על היעד

א. כתובת האינטרנט (URL) של המקור.

ב. קוד מקור html (HTML Source Code).

ג. צילום מסך של המקור הכולל תאריך ושעה.

ד. פירוט מידע שהוקלט/נתפס (captured data).

ה. איסוף מטה דאטה –

i. זהות הגורם המפרסם;

ii. מזהה של הפוסט, תמונה או וידאו;

iii. תאריך העלאה;

iv. תיוג גאוגרפי (geotag);

v. Hashtag.

vi. הערות.

vii. Annotation.

ו. כתובת IP.

ז. מידע נוסף שפורסם לצד התוכן.

3. מידע על collection package

א. שם הקובץ.

ב. רשימת האשים (hash).

ג. האש של קובץ רשימת ההאשים.

4. שירותים שנעשה בהם שימוש

א. מוצר תוכנה

ב. שירותי זמן.

ג. שירותי ip.

ד. פרטי whois.

5. האם היו בעיות מיוחדות בהורדה? **כן/לא**

6. בדקתי את תקינות העותק וראיתי שהוא זהה ליעד.

7. העברתי את הקובץ לשמירה בתיקית ארכיון ייעודית _____.

8. יש לשמור את המידע בהתאם לכללי אבטחת מידע בהתאם לעקרונות הבאים:

א. ביצעתי שמירה בפורמט שאינו ניתן לשינוי, תוך תיעוד חותמת הזמן של מועד השמירה - בחתימת HASH - SHA-256/MD5.

ב. ביצעתי בדיקה כפולה של חתימת הקבצים ושל חותמת הזמן שלהם.

ג. הקבצים נשמרו ב- **קובץ ארכיב/** _____.

אישור החוקר:_____

מסמך זה נכתב על ידי:

- עו"ד עמית אשכנזי

העירו הערות:

- עו"ד חיים רביה, משרד פרל כהן צדק לצר ברץ
- עו"ד דנית ליבוביץ שאטי, אלפא פורנזיקס