Technologic Papers

אמינותן של ראיות דיגיטליות

מאת עומר כהן

הקדמה

בגליון העשירי של המגזין, כתב עו"ד יהונתן קלינגר על "מקור עותק והעתק", וסיפר על הבעיות (והקשיים) העומדים בפני בתי המשפט בהתמודדות עם ראיות מחשב. עו"ד קלינגר נתן התייחסות חוקית ומשפטית לנושא ראיות המחשב, כאן אנסה להשלים את המאמר בסקירה טכנית של מספר סוגי ראיות דיגיטליות המובאות לרוב בפני בתי המשפט, וכיצד ניתן לזהות זיוף או שינוי של ראיה שכזאת.

תכתובות דואר אלקטרוני

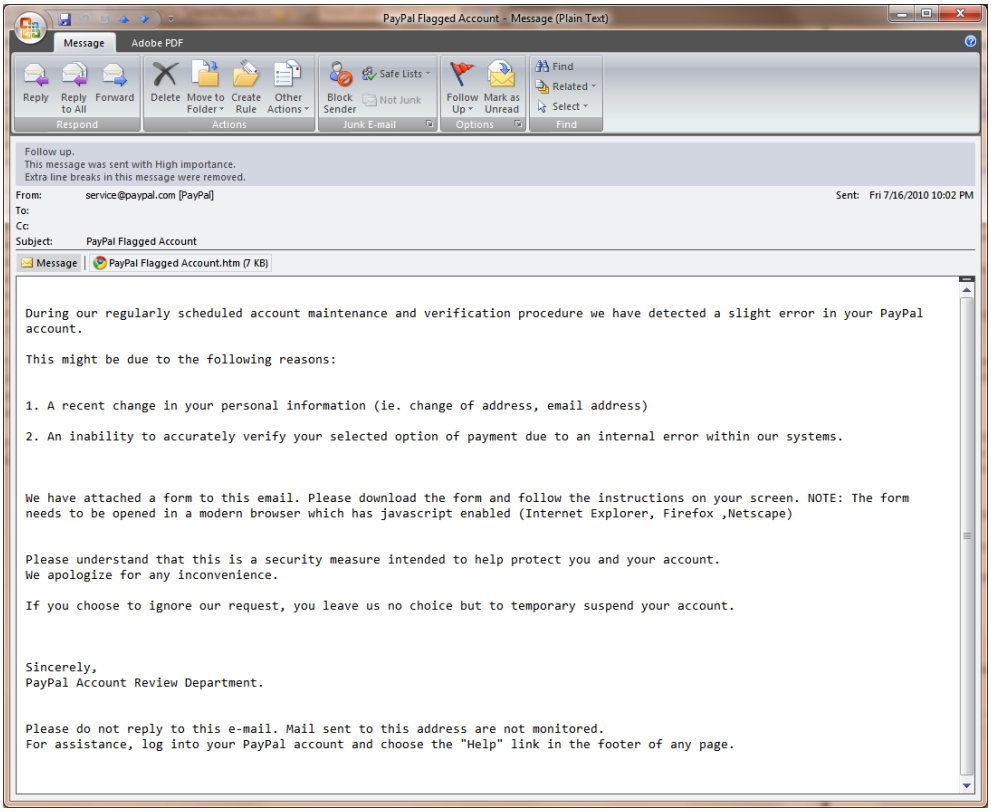
לא פעם מגיעים לבתי המשפט תיקים המבוססים ברובם על תכתובות דוא"ל ארגוני, אם מדובר בהפצת סודות מסחריים, השמצות, העברת מסמכים וכן הלאה. חשוב לזכור כי למעביד זכות מסוימת לקרוא את הדואר האישי (התיבה בשרתי החברה) של העובד, על-מנת לאתר הפרה של חוזים או פגיעה באינטרס החברה, כל עוד שהדבר נעשה דרך תיבת הדואר של החברה. לעומת זאת, גם אם משתמשים ברשת המשרדים על מנת לגשת לתיבת הדואר הפרטית (תיבת ה-Gmail שלכם לדוגמא) למעביד אין זכות לתעד את הסיסמא העוברת ברשת האינטרנט המשרדים ולנצל זאת לחיטוט בתיבתכם הפרטית. עוד על הנושא ניתן למצוא בבלוג של עו"ד קלינגר.

אם וכאשר מגיעה תכתובת שנאספה בצורה לגיטימית, על ידי גורם שלישי בלתי משוחד, ישנן מספר דרכים בהן ניתן להגיש ראיות שכאלו בבית המשפט, חלקן טובות וחלקן פחות.

אחת הדרכים היא לבצע הדפסה פשוטה של פריט הדואר, מה שכולל את התוכן בלבד ללא כל מזהים דיגיטליים כלשהם. הדפסה שכזו ניתן לבצע באמצעות כל מעבד תמלילים, מה שלא מספק שום אמינות לראיה שכזו. להדפסה זו, ניתן להוסיף הדפסה של כותרות דבר הדואר (Mail Headers), המספקות מידע טכני על ההיסטוריה של דבר הדואר, איפה נוצר, לאן עבר, מתי ואיך (על כך יורחב בהמשך). מהלך זה מוסיף אמינות להדפס המקורי, אך מאחר וגם שאת הדפסה זו ניתן לערוך בפשטות, אמינותה נמוכה.

מאחר וכותרות הדואר נוצרות במקור על ידי שרתי הדואר אשר טיפלו במסירת ההודעה, הן מוסיפות שלל משתנים סביבתיים המעידים על קיומה של ההודעה, בנוסף לגיבוי התאריך והשעה שבה נוצרה והגיעה ליעדה. היות וכותרות אלו נוצרות על ידי השרת, כל משתמש פשוט, לאחר הבנה של מבנה הכותרות, יכול לאמת את שולח ההודעה (למשל בנקים ונותני שירות אחרים) ולהימנע מליפול בפח לתרמיות Phishing.

לדוגמא, נבחן כאן את מבנה הכותרות של הודעה שנשלחה (כביכול) מאתר PayPal:



כותרות הדואר:

4.
```
4.  Received: from mx02.3334444.net (10.10.50.250) by HUBCAS01.4hosted.local
(10.10.50.12) with Microsoft SMTP Server (TLS) id 8.1.393.1; Fri, 16 Jul 2010
22:05:47 +0300
```

3.
```
Received: from mybox.redx.co.il (81.218.228.46) by mx02.3334444.net (81.218.228.52)
          with Microsoft SMTP Server id 8.1.393.1; Fri, 16 Jul 2010  22:05:48 +0300
```

```
2. Received: from sosgraphics.com ([75.77.47.106]) by mybox.redx.co.il ; Fri, 16  Jul
   2010 22:04:30 +0300
```

```
1. Received: from User ([68.216.158.98] RDNS failed) by sosgraphics.com with Microsoft
   SMTPSVC(6.0.3790.4675); Fri, 16 Jul 2010 15:02:24 -0400
```

```
0. From: "service@paypal.com" <PayPal>
   Importance: high
   X-Priority: 1
   Date: Fri, 16 Jul 2010 22:02:18 +0300
   Subject: PayPal Flagged Account
   Thread-Topic: PayPal Flagged Account
   Thread-Index: AcslGdphpzVwPeeLSRiss2Bw0e3hJQ==
   Message-ID: <FP-SERVEREFzotSkrpE000010cb@sosgraphics.com>
   X-MS-Exchange-Organization-AuthAs: Anonymous
   X-MS-Exchange-Organization-AuthSource: EDGE01.4HOSTED.DMZ
   X-MS-Has-Attach: yes
   X-Message-Flag: Follow up
   Reply-By: Sat, 17 Jul 2010 14:00:00 +0300
   X-MS-TNEF-Correlator:
   x-originalarrivaltime: 16 Jul 2010 19:02:24.0530 (UTC)
   FILETIME=[6D1E3F20:01CB2519]
   received-spf: Fail (EDGE01.4HOSTED.DMZ: domain of PayPal does not designate
   81.218.228.46 as permitted sender) receiver=EDGE01.4HOSTED.DMZ; client-
   ip=81.218.228.46; helo=mybox.redx.co.il;
   x-hmailserver-loopcount: 2
   x-hmailserver-spam: YES
   x-hmailserver-reason-score: 7
   x-hmailserver-reason-2: Rejected by Uceprotect-1! - (Score: 5)
   x-hmailserver-reason-1: The host name specified in HELO does not match IP address. -
   (Score: 2)
   Content-Type: multipart/mixed;
   boundary="_002_FPSERVEREFzotSkrpE000010cbsosgraphicscom_"
   MIME-Version: 1.0
```

לפני שניגש לתוכן, מספר הבהרות: הוספת הרווחים והמספורים בין החלקים השונים נעשתה עלידי הכותב כדי שיהיה קל ונוח לקרוא את התוכן. בנוסף, יש לשים לב שהתוכן מתעדכן על-ידי שרתי הדואר השונים שהדואר עובר ביניהם. הוספת שם השרת המקבל וחתימת הזמן נעשית מלמעלה (חלקים 4-1), ובמידה ויש צורך להוסיף כותרת נוספת מעבר לחתימת זמן, הדבר נעשה בסוף הדף (חלק 0).

נתחיל עם חתימות הזמן- כל חתימה שכזו, נוצרת על ידי השרת המקבל ומכילה את הפרטים אודות הישות שפנתה אליה. מאחר וכל אחד יכול להחליט על הפרטים של עצמו (שם, כתובת IP, גרסאות שרת וכן הלאה), עצם העובדה שכאן כל אחד מדווח גם על זה שלפניו נותן לנו אפשרות לאמת את כל הפרטים

שמוצגים בפנינו, ולמצוא אי תאימויות. חשוב לזכור כי למרות שיש סטנדרט לייצור כותרות אלו (RFC2821, סעיף 3), לעיתים נתקל במיקומים שונים של פרטי המידע בתוך שורת הכותרת Received.

```
Received: from User ([68.216.158.98] RDNS failed) by sosgraphics.com
with Microsoft SMTPSVC(6.0.3790.4675); Fri, 16 Jul 2010 15:02:24 -
0400
```

הכותרת מחולקת לשלושה חלקים:

1. **from** – מציין את זהותו (שם המתחם) של מי שהתחבר לשרת הדואר (מוזן על-ידי אותו שרת/אדם וניתן לשינוי) – במקרה שלנו "User". לאחר מכן, בסוגריים עגולים נמצא את כתובת ה-IP של המחשב ממנו התבצע החיבור, כפי שהיא נראית מהצד המקבל (למשל, והמחשב נמצא מאחורי NAT, כאן יהיה ניתן למצוא את הכתובת החיצונית של אותו NAT). לרוב כתובת זו תופיע בתוך סוגריים מרובעים, ולאחריה יתווסף Reverse DNS של אותה כתובת, על-מנת לאמת את אותה זהות – במקרה שלנו "[68.216.158.98] RDNS failed" (מאחר ולא נמצא שם מתחם לכתובת ה-IP, מצוין ש-RDNS נכשל).

2. **by** – מציין את שם המתחם המקומי כפי שמוגדר באותו שרת – כמו לדוגמה במקרה שלנו "sosgraphics.com". לעיתים ניתן למצוא כאן שמות מתחם פנימיים, לא חוקיים (כמו בסעיף 4) דבר המעיד כי שרת הדואר נמצא בתוך רשת פנימית מאובטחת. בנוסף נהוג להוסיף חתימה של שרת הדואר בצירוף גרסה (סעיפים 1,3,4).

3. חתימת הזמן המלאה כולל אזור זמן, על-מנת שניתן יהיה ליצור רצף אחיד של כל שאר הכותרות וליצור תמונה של המסע שעבר אותו פריט דואר. במידה וישנה סטיה גדולה מדי בחתימות הזמן, הדבר יכול לעורר חשד, אם כי הזמן המוצג הוא כפי שמוגדר על שרת הדואר, כך שיתכן כי מנהל השרת לא הגדיר את השעון כראוי.

כותרת ה-Received הראשונה (מלמטה) יכולה ללמד אותנו הכי הרבה למעשה, מאחר וכאן ניתן ללמוד על איזה שרת נוצרה ההודעה ומאיפה הגיע המשתמש שיצר אותה. כל שאר החתימות מעידות על המסלול שעברה אותה הודעה, עד לשרת המקומי בו התקבלה. **<u>למעשה, מיד ניתן להבחין כי ההודעה נוצרה בשרת שקורא לעצמו sosgraphics.com ולכן ניתן להסיק שהודעה זו היא בעצם זיוף, ולא הגיעה משרתי PayPal.</u>**

שאר כותרות הדואר המופיעות בסעיף 0 מכילות מידע אודות ההודעה עצמה, בנוסף לעדויות לבדיקות שונות שביצעו השרתים השונים שקיבלו את ההודעה. לדוגמא הכותרת received-spf מספרת על בדיקת SPF שביצע השרת המקבל. בדיקה זו נכשלה מאחר ולפי הגדרות SPF של paypal.com השרת ממנו הגיעה ההודעה לא מורשה לשלוח הודעות בשמם. SPF - Sender Policy Framework הוא כלי עזר נהדר שעוזר לכם לוודא שמישהו אחר לא מתחזה אליכם על ידי שימוש בשם המתחם שלכם בשליחת דואר. עוד על SPF ניתן לקרוא כאן.

מכיוון שכותרות אלו מוסיפות מידע רב אודות פריטי הדואר, הצירוף שלהן יחד עם תוכן ההודעה הינו בגדר חובה כאשר דנים באמינות דברי דואר. נאמר ששימוש בהדפסות פשוטות אינו אמין מחשש לשינוי טקסטואלי של אותן כותרות, כאשר מגישים דברי דואר לבחינה מומלץ לעשות זאת בפורמט דיגיטלי.

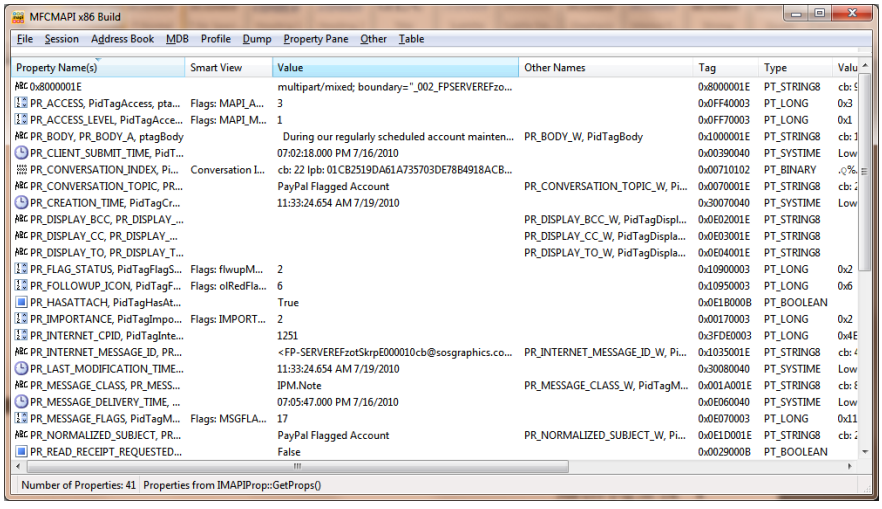
ישנם שני פורמטים עיקריים לדברי דואר:

1. EML- פורמט טקסטואלי המכיל את כל הכותרות כפי שהוצגו כאן ובנוסף תוכן הדואר בטקסט או בפורמט MIME. מאחר ומדובר בפורמט טקסטואלי, ניתן לפתוח את הקובץ ב-notepad ולערוך, לכן אמינותו עומדת בספק. למרות הטענה שבהעתקה נכונה של הקובץ ניתן לשמר את חתימות הזמן של מערכת הקבצים בו נוצר, וכך להעיד שלא שונה מאז שנוצר, חתימות הזמן של מערכת הקבצים ניתנות לשינוי בפשטות (אם על-ידי פקודת touch בלינוקס, או אפילו בעזרת PHP, עם הפונקציה (touch) ולכן עדיין פורמט זה לא אמין מספיק.

2. MSG- פורמט בינארי המכיל מספר רב של אובייקטים ותכונות ייחודיות. הודעות MSG, שלרוב נוצרות כחלק מפעולת שרתי Exchange ותוכנת הלקוח Outlook מבית Microsoft, בנויות על-בסיס MAPI – Messaging Application Programming Interface, ארכיטקטורה למערכות דואר בסביבת Microsoft, כל מתכנת יכול להשתמש בה על-מנת להתממשק לפונקציות הדואר השונות. הארכיטקטורה נותנת גישה למספר עצום של מאפיינים שונים לכל פריט דואר, ונגישה בצורת בסיס נתונים שלם, הכול בתוך קובץ MSG בודד.

השדות העיקריים שמעניינים אותנו הם שדות הכותרות, כפי שציינו מקודם, ושדות מיוחדים המתייחסים לנושא שלנו, חתימות זמן לכמעט כל פעולה חשובה כגון יצירת ההודעה, תאריך תגובה, פרטים אודות קבצים מצורפים, ושדות שמתעדכנים באופן אוטומטי ומספרים על כל שינוי שהתבצע לאחר יצירת ההודעה.

באמצעות האפליקציה MFCMAPI ניתן לגשת לקבצי MSG בפרוטוקול MAPI ולקרוא את בסיס הנתונים המלא. האפליקציה אף מאפשרת לנתח קבצי PST (Personal Storage Table) ומכילה שלל תכונות נוספות בתחום ה-MAPI.



כלי זה מאפשר לבחון שדות שאינם נגישים למשתמש פשוט על ידי גישה באמצעות Outlook או תוכנת לקוח אחרת, וכך במידה ונערך שינוי במאפייני ההודעה לאחר יצירתה, נוכל לגלות זאת כאן.

לאחר שראינו כמה פרטים מסתתרים מתחת לפני השטח, ניתן להבין את החשיבות בשימור הפורמט הדיגיטלי בהתמודדות עם ראיות דואר אלקטרוני בתיקים משפטיים ובכלל.

על-מנת למנוע ספק במהימנות הראיות, עדיף לאסוף אותן ישירות משרת הדואר ולא ממחשבו הפרטי של המשתמש. במידה ולא מדובר בשרת Exchange, מומלץ למשוך את ההודעות מהשרת באמצעות פרוטוקול IMAP אשר בניגוד ל-POP, יודע לספק פרטים רבים אודות מאפייני ההודעה ולהזין אותם ל-Outlook או כל תוכנה אחרת שנסמכת על ארכיטקטורת IMAP. כך הקובץ שיווצר יכיל את כל המאפיינים החשובים לאימות אמינותה של ההודעה.

לכידת אתרי אינטרנט

הראייה האינטרנטית הנפוצה השנייה היא בצורת לכידה של תוכן מאתרי אינטרנט, לרוב בעקבות הפרת זכויות יוצרים, השמצות וכן הלאה. בניגוד לתכתובות דואר, שברגע שהגיעו לשרת הן יישארו כמו שהגיעו עד אשר יחליטו למחוק אותן, הבעיה עם אתרי אינטרנט היא העובדה שבשנים האחרונות כל האתרים הפכו דינאמיים לחלוטין. אתרים גדולים המספקים תוכן רב משנים את פניהם מספר רב של פעמים ביום ובמקרה שבו בעל אתר נתבע אודות תוכן מסוים, הוא יכול בשניות להעלים את התוכן ולטעון שמעולם לא היה קיים באתר, ושכל תיעוד שלו הוא זיוף מוחלט.

לעיתים בא המושיע הגדול לעזרתנו ובעזרת Google Cache ניתן לעלות על עותקים של תכנים לאחר ששונו, אבל גם אלה נעלמים תוך מספר ימים/שבועות ויש לתעד אותם בצורה נכונה כדי להימנע מטענות זיוף לאחר שהתוכן יורד מ- Google. על-מנת לבדוק קיומו של העמוד שלכם ב- Google יש לרשום בשורת החיפוש של גוגל cache: ואת כתובת האתר שלכם (למשל cache:ynet.co.il). בנוסף יש כמובן את ארכיון האינטרנט ששומר עותקים מסוימים של אתרים. בכל מקרה שבו יש צורך לתעד תוכן באתר אינטרנט ביום ושעה מסוימים לפני שהם נעלמים מן העולם, חשוב לעשות זאת בצורה איכותית שלא תשאיר מקום לספק באמינות התיעוד.

לאחרונה נתבקשתי להעיד על-ידי עו"ד אפי פוקס בתיק זכויות יוצרים שבו הנתבע סרב להודות בצילומי מסך שהוצגו. הראיות הוגשו בפורמט PDF שיוצר על-ידי יצוא פשוט מהדפדפן, הנתבע טען שהראיות לא אמתיות והתוכן מעולם לא הוצג באתרו.

הבעיה עם תיעוד בצורת PDF, שלמרות שהוא מכיל מספר רב של מאפיינים וחתימות דיגיטליות, הוא מתעד אך ורק את מה שמוצג בדפדפן. למרות העובדה שביצוא מדפדפן מתווסף בתחתית העמוד כתובתו של האתר אליו מדפיסים, דבר הנותן משקל מסוים לאמינות המקור, וכך מאמת שהקובץ מציג את האתר האמתי ולא עותק מקומי. אף על פיכן, אדם עם מעט ניסיון בבניית אתרים יכול ליצור העתק של הדף על שרת מקומי ועל ידי שינוי רשומות DNS בקובץ hosts לגשת בדפדפן כתובת אינטרנטית,לקבל את ההעתק המקומי, ללכוד אותו ב-PDF וליצור ראיה מזויפת של תוכן "באינטרנט".במקרה המדובר, עו"ד

אפי פוקס עשה נכון וצירף מספר גרסאות ועמודים שונים מאותו אתר, בנוסף לסרטון וידאו המציג את האתר החי ומעבר בתכנים השונים בו. הזיוף של ראיות אלו דורש יותר ניסיון והתמקצעות בתחום, דבר שלא היה מאפיין של התובע במקרה, בנוסף למחקר מקיף אודות כתבות נוספות שהעתיק בעל האתר. תוספות אלו נתנו משקל נוסף לאמינות הראיות.

בכדי לבצע תיעוד איכותי שיהיה קשה לערער, לפחות בצורה שידרשו מאמצים רבים לייצור זיוף שכזה, יש להיעזר בצד שלישי בלתי משוחד לביצוע התיעוד ושזה יתעד את כל המאפיינים הסביבתיים בזמן התיעוד כגון הגדרות רשת, טבלאות ניתוב, ניקוי עותקי מטמון ועוד. עדיף ללכוד בסרטון וידאו את כל התהליך ברצף זמן על-מנת למנוע טענה שהבדיקות והלכידה נעשה בזמנים שונים, כל זאת בכדי להציג בצורה חד משמעית שהאתר אליו ניגשים אכן נגיש לעולם ברשת האינטרנט.

סיכום

השימוש בראיות דיגיטליות עולה מיום ליום וחשוב להבין את כל המאפיינים הסובבים את הנושא כדי שלא יפלו עקב חוסר אמינות גם אם התוכן אמיתי ונכון. יש לזכור שאפשר לפרוץ לכל מקום ולזייף כל מסמך, בסופו של דבר זאת שאלה של זמן ומשאבים. לכן, התפקיד שלנו הוא להסיר כל ספק סביר לאמינות הראיה ולהגיש יחד עם הראיה הדיגיטלית את כל המשתנים הסביבתיים שעלולים להעלות חשד.

תודה לעו"ד אפי פוקס ועו"ד יהונתן קלינגר על הערותיהם.

על המחבר

עומר כהן הוא מומחה לאבטחת מידע, בעל ניסיון של מעל עשר שנים בתחום המחשבים. בשנים האחרונות עובד עבור תאגיד eBay העולמי, עוסק בפורנזיקה ומחקר טכנולוגי, יעוץ טכנולוגי משפטי ומתן עדויות מומחה בבית משפט. בנוסף משמש כיועץ אבטחת מידע למספר ארגונים ומעביר הרצאות במגוון נושאים.