עבירות מחשב

- בשנים האחרונות מסתמנת בעולם הפשע הקלאסי מגמת עלייה בשימוש באמצעים טכנולוגיים לשם זיוף כרטיסי אשראי, שיקים ומסמכים רשמיים, ולשם הקמת מאגרי מידע ממוחשבים לצרכים פליליים
- ההתפתחות הטכנולוגית מחייבת את חוקרי המחשב בלימוד שוטף וכן בעבודה עפ"י שיטות חקירה עדכניות
- לאחרונה פותחו שיטות חדשות, שמטרתן חשיפת מירב הראיות שבחומר המחשב, בלי לפגוע בראיה המקורית

רב-פקד מאיר זוהר, ר' צוות עבירות מחשב, יאח"ה

עם האצת תהליך המחשוב בישראל, הולך וגדל מספר האנשים והארגונים המשתמשים במחשב לצורך פעילותם האישית והעסקית. למעשה, כל המסמכים העסקיים כיום יכולים להיות מאוחסנים במחשבי העסק או התאגיד. החוקר בשטח נתקל כיום במחשב כמעט בכל עסק, משרד או בית, שאליו הוא נכנס במסגרת חקירתו. מחשב כזה, הנתפס אצל חשוד או עד עשוי להכיל ראיות ועובדות חקירה, הקושרות את החשוד לביצוע העבירה. ראיות אלו יכולות להיות גם אוסף של סימנים מגנטיים/אופטיים או אף פולסים חשמליים בזיכרון המחשב. קיים צורך במיומנות גבוהה ובאמצעים מתאימים, על-מנת לאתר את הראיות במחשב, להפיק פלט ראיות קביל עפ"י דיני הראיות, ולהציגו בפני בית-המשפט. אם בעבר היה החוקר בשטח מתעלם מהפוטנציאל הראייתי שבמחשב או אף גרוע מכך, פוגע בשלמות הראיה בבדיקה לא תקינה ולא מקצועית, הרי שכיום, מודעים חוקרי המשטרה לכך, שבמחשב אגור מידע רב ערך, היכול לשמש כראיה בבית-המשפט, והם שומרים על תקינות המחשבים עד להבאתם לבדיקת חוקרי המחשב המיומנים.

חוק המחשבים מחייב את החוקר בשטח, להעביר את המחשב שנתפס אצל חשוד לטיפולו של חוקר מיומן, שהוכשר לכך ע"י המשטרה. כן יצר החוק מגבלות חדשות, כמו הצורך לסיים את החיפוש במחשב של תאגיד/עסק תוך 48 שעות. עפ"י החוק, יש צורך בצו חיפוש בכל תפיסה של מחשב, וכן בצו מיוחד לחדירה למחשב ולהפקת פלט ראיות ממנו. צוות חקירת עבירות מחשב והיועץ-המשפטי של יאח"ה ניסחו ביחד נוסח חיפוש וחדירה, החייב להופיע בכל צו חיפוש, שבו מעורב מחשב.

המורכבות הטכנולוגית של ריבוי פלטפורמות המחשב, ריבוי מערכות ההפעלה (OS2, UNIX, NOVELL, WINDOWS, DOS), ריבוי היישומים היוצרים את הנתונים ואת סוגי חומרה, המתעדכנים ומשתנים במהירות, גורמים לכך שגם חוקרי המחשב המיומנים מהשטח אינם מסוגלים לתת תמיד מענה לחקירות הדורשות מומחיות ואמצעים מיוחדים. אין בידם גם לתת סיוע טכני בחקירות קלאסיות, שבהן מעורב יותר ממחשב אחד (למשל, בתפיסה של רשת מחשבים במשרד, בעסק או בארגון) וכן במקרים, שבהם המידע האגור במחשב מוצפן או נוצר בפורמטים מיוחדים של יישומים שונים.

ההתפתחות הטכנולוגית המתמדת מחייבת את חוקרי המחשב המיומנים בלימוד ובהתעדכנות שוטפים (קורסים והכשרות מקצועיות), בפיתוח כלים מיוחדים (חומרה ותוכנה) וכן בעבודה עפ"י נהלים ושיטות חקירה עדכניים, שבלעדיהם לא יוכלו לעמוד במטלותיהם בעתיד.

למעשה, המידע האלקטרוני המופק ממחשבי חשודים, הינו ההמשך הטבעי למידע המופק ממסמכים או ממידע אחר, המטופל על-פי הגדרה, ע"י המחלקה לזיהוי פלילי. למרות זאת, אין כיום במז"פ גוף העוסק בחיפוש אחר מידע דיגיטאלי ממחשבים, בסריקתו, בהפקתו ובשחזורו לצורך הבאתו כראיה בפני בית-המשפט. כיום, רק צוות עבירות מחשב ביאח"ה וחוקרי המחשב המיומנים, שהוכשרו במרחבים ובמחוזות השונים, יכולים לתת מענה חקירתי במתן סיוע טכני בתפיסה, בחיפוש ובהפקת פלט ראיות בעבירות קלאסיות, שבהן מעורב מחשב.

מז"פ מחשבים

יש צורך בכישורים ובמיומנות מסוימים לצורך חקירת עבירות מחשב, ובכישורים ומיומנויות אחרים לצורך בדיקת מחשבים, שנתפסו אצל חשודים בביצוע עבירות קלאסיות. צוות עבירות המחשב ביחידה הארצית לחקירות הונאה פועל מספר שנים כצוות מומחה לחקירת עבירות מחשב. הצוות אחראי גם על ביצוע בדיקות מעבדה ועל הפקת פלט ראיות ממחשבים שנתפסו. הצורך החקירתי בחשיפת ראיות במחשבים אישיים מחד, ושמירה על שלמות הראיה והקפדה על דיני הראיות מאידך, הביאו את הצוות לפיתוח תוכנות שיטות עבודה ונהלי עבודה, שמטרתם-חשיפת מירב הראיות שבחומר המחשב, בלי לפגוע בראיה המקורית.

קיימים שלושה שלבים עיקריים בתפיסת ראיות, בחיפוש אחריהן ובהפקת פלט ראיות:

תפיסה ורישום

סעיף 11 לחוק המחשבים, התשנ"ה 1995, קובע, שתפיסת "מחשב" וכן "חומר מחשב" כמו גם חדירה ל"חומר מחשב" טעונים צו מפורש של בית-משפט. החוק גם קובע כי תוקפו של צו תפיסה של מחשב "מוסד" או עסק הינו ל48- שנות בלבד. זמן קצר זה מחייב לעתתים להחזיר את המחשב הנחקר לבעליו, עוד בטרם נסתיימה בדיקתו. ביחד עם יועמ"ש יאח"ה ניסח הצוות צו חיפוש כמתחייב מחוק המחשבים, והמתאים לצרכי החקירה, שבה מועבר מחשב, בין אם הינו מטרת העבירה, בין אם הינו כלי לביצוע העבירה ובין אם הינו מכיל ראיות, שיש צורך לאתר ולהציג בפני ביהמ"ש. לפני נוסח זה, יתפס "כל מסמך וחפץ לרבות מחשב וחומר מחשב, לרבות מחשב וחומר מחשב של מוסד, לרבות חדירה נמשכת לצורך הפקת פלט ראיות".

הצוות ניסח הצעה לנוהל "התנהגות החוקר בזירת עבירת מחשב", ובימים אלו הוא מנוסח לנוהל פורמלי ע"י אח"ק. ההצעה מגדירה את אופן הפעולות שעל החוקר שבשטח לנקוט כאשר הוא מגיע לזירת עבירה, שבה מעורב מחשב. ההצעה מפרטת את אופן התפיסה, את הסימון ואת הבאת המחשב לידי חוקר המחשב המיומן, על-מנת שלא תיפגענה שרשרת הראיות ושלמות הראיות המקורית.

העתקת מראה

העתקת מקור של דיסק קשיח הינה העתקה של כל הסקטורים בדיסק מקור אל דיסק יעד אחר. בלשון ציורית ניתן לאמר, כי העתקת מקור הינה "צילום" של דיסק המקור לדיסק אחר, כך שההעתק מתאים למקור. מבחינה ראייתית ניתן לקבוע, כי המידע בדיסק המקור זהה לחלוטין לזה שבדיסק היעד. העתקת מקור מאפשרת להחזיר את הדיסק המקורי (או ההעתק) לבעליו, ולהמשיך ולבצע את החקירה שעל דיסק ההעתק.

על דיסק ההעתק ניתן לבצע פעולות, שאינן מתאפשרות, בדרך-כלל, על הדיסק המקורי, מתוך חשש לפגיעה בשלמותו ובשלמות המידע האגור בו. בדיסק ההעתק ניתן לעקוף למשל, מכשולים טכניים (חומרה) או מכשולים לוגיים (הצפנות, וירוסים, מלכודות). במידה שפעולות אלו נכשלות, ניתן תמיד ליצור דיסק העתק חדש, ולנסות פעולות אחרות.

בדיסק הקשיח "מסתתר" מידע רב, שאינו נגיש בדרך-כלל למשתמש ו/או למערכת ההפעלה. המידע יכול להיווצר בכוונה תחילה (החבאת המידע באזורים שאינם נגישים בדרך-כלל), במחיקה מכוונת של קבצים המכילים ראיות או באופן שוטף וללא ידיעת המשתמש. מידע כזה יכול להכיל ראיות, הקושרות את החשוד לביצוע העבירה. העתקת מקור מאפשרת לחוקר לחקור מידע כזה, אשר אינו מתקבל באמצעות העתקת קבצים רגילה.

העתקה רגילה אינה העתקת מידע ראייתי מקבצי מערכת, מקבצים מחוקים, מ- FILE SLACK (גודל פיזי-גודל רשום), מדיסק מפורמט או מ- LANDING ZONE.

חיפוש והפקת פלט ראיות

רוב המחשבים האישיים בישראל הינם מחשבי IBM או תואמיו, ורובם פועלים תחת מערכות ההפעלה DOS ו- WINDOWS. השימוש הנפוץ ביותר במחשבים אישיים (בתחום היצירה, העריכה, עיבוד המידע ואיחזור מידע) הינם עיבוד תמלילים, מסדי נתונים וגליונות חישוב אלקטרוניים, הפועלים בשפות שונות (בעיקר באנגלית ובעברית, אם כי לפעמים נתפסים מחשבים בשפות אחרות כמו רוסית וערבית). מחשב אישי, הנתפס אצל חשוד, יכול להכיל מאות ואף אלפי מסמכים, היכולים לשמש כראיה בבית-המשפט. לאור בעיות השפה (רוב תכנות החיפוש מיועדות לשפה האנגלית) פיתח הצוות תוכנות חיפוש בינאריות, שניתן להתאימן לכל מערכת הפעלה, לכל מחשב ולכל שפה. התוכנות סורקות את כל קבצי המחשב, את קבצי ההפעלה ואת הקבצים המחוקים או הסמויים, ומתעדות קבצים, שבהם מופיעות מילות מפתח שהוגדרו מראש ע"י החוקר, בהתאם לנושא הנחקר. סריקה ידנית של קבצים אלו הינה כמעט בלתי אפשרית, לאור נפחו של המידע הרב ואמצעי האחסון המגנטיים.

קבצים מחוקים ו/או מוצפנים וכן מידע דיגיטאלי, המסתתר בדיסק הקשיח באזורים פיזיים שונים, משוחזרים באמצעות תוכנות חקירה מיוחדות למדיה אחרת, ונסרקים באמצעות תוכנות מיוחדות שפיתח הצוות.

את הקבצים שנמצאו מדפיס חוקר המחשב המיומן כפלט ראייה, לצורך הגשתו לבית-המשפט. בימים אלו נבחנת האפשרות להעביר את קבצי הראיות שנמצאו לתקליטור, המאפשר אחסון נפח מידע גדול מחד, ושמירת הראיות לאורך זמן רב, מאידך.