ПОНЯТТЯ ТА ВИДИ КРИМІНАЛІСТИЧНИХ ТЕХНОЛОГІЙ ПОШУКУ ТА ФІКСАЦІЇ КОМП'ЮТЕРНИХ ДАНИХ

Сергій Олександрович КОЛОМІЙЦЕВ,

аспірант Харківського національного
університету внутрішніх справ

Криміналістичні технології - це методи та засоби, що використовуються для виявлення, вилучення, аналізу та збереження комп'ютерних даних у рамках кримінальних проваджень. Пошук комп'ютерних даних включає виявлення інформації на цифрових носіях, їх вилучення, зберігання та подальший аналіз.

Технології включають методи вилучення даних із фізичних носіїв (жорсткі диски, SSD), аналіз мережевого трафіку, дослідження хмарних сховищ, відновлення видалених даних та роботу з шифрованими даними. Важливим є розуміння файлових систем (NTFS, FAT32, EXT4) для вилучення та аналізу даних, включаючи приховані або видалені файли.

Серед програм для відновлення видалених файлів з жорстких дисків, флеш-накопичувачів, карт пам'яті та інших носіїв даних, найкраще себе зарекомендували : Recuva, R-Studio, TestDisk, EaseUS Data Recovery Wizard.

Нерідко правопорушники знищують компрометуючу їх комп'ютерну інформацію. Для виявлення комп'ютерних даних та відстеження взаємодії між системами використовуються програми для захоплення та фіксації даних мережевої активності. Один із найкращих інструментів для таких дій - Wireshark. Це аналізатор мережевого трафіку, який дозволяє фіксувати й аналізувати мережеві пакети в реальному часі. Він широко використовується для виявлення загроз, пошуку помилок у мережі та збору доказів у кримінальних розслідуваннях. Інші інструменти для подібних завдань: tcpdump та PRTG Network Monitor.

До цифрових носіїв, які можуть містити важливу для розслідування інформацію, відносяться також і мобільні пристрої. Один із найпотужніших інструментів для криміналістичного аналізу мобільних пристроїв - Cellebrite UFED. Цей пристрій використовується для вилучення даних з телефонів, планшетів, SIM-карт, включаючи видалені повідомлення, контакти, історію дзвінків тощо. Альтернативні варіанти - це програми: Oxygen Forensic Detective, Magnet AXIOM, MOBILedit Forensic.

При фіксації комп'ютерних даних важливо забезпечити їх цілісність і захист від змін, щоб уникнути спотворення доказів у ході розслідування. Для цього доцільно використовувати пристрій під назвою EPOS WriteProtector.