УДК 004

О. І. Гриців
Національний університет “Львівська політехніка”

КРИМІНАЛІСТИКА В КОМП’ЮТЕРНИХ СИСТЕМАХ: ПРОЦЕСИ, ГОТОВІ РІШЕННЯ

Розглянуто процеси та готові рішення у комп’ютерній криміналістиці. Завдання у комп’ютерних криміналістів є одними з найскладніших у галузі інформаційних технологій. Важливим елементом у процесі дослідження комп'ютерної техніки є вибір необхідних інструментальних засобів (програмного забезпечення) у комп’ютерній криміналістиці.

EnCase Forensic є потужним технічним рішенням для досліджень у галузі комп'ютерної криміналістики. Він являє собою багатозадачний програмний комплекс, який використовують у багатьох країнах світу.

Ключові слова: комп'ютерна криміналістика, експерт, подія, інцидент, Мобільний Криміналіст 2013.

The processes and ready-made solutions in computer forensics have been described. In the area of information technology the tasks of a computer forensics investigator are regarded as most challenging. Choice of an adequate forensic software tool is an important element in computer forensics.

EnCase Forensic is a powerful platform for computer forensics investigation. It is a multi-task software package used in lots of countries.

Key words: computer forensics, incident, investigator, forensics, EnCase Forensic.

Вступ

Підприємства та державні організації все частіше переживають інциденти у сфері інформаційної безпеки. Витік таємної інформації, порушення інформаційної безпеки, махінації з електронними платіжними системами, викрадення конфіденційної інформації, знищення електронних документів спричиняють значні збитки та є реальною загрозою діяльності компаній та державних структур. Отже, виникає необхідність у розслідуванні комп'ютерних злочинів, а також збирання доказів з метою подання позову до суду. Ці задачі сьогодні є доволі складними, але і найважливішими у комп'ютерній криміналістиці.

Комп'ютерна криміналістика (forensics) – прикладна наука про розслідування злочинів (інцидентів), пов'язаних із комп'ютерною інформацією, про дослідження цифрових доказів, методів пошуку, отримання і фіксації таких доказів.

Метою роботи є огляд, визначення функціональних можливостей найсучасніших інструментальних засобів, що використовуються у криміналістиці в комп’ютерних системах.

Комп'ютерна криміналістика і збирання доказів

Основним напрямом комп'ютерної криміналістики є дослідження машинних носіїв інформації з метою формування доказів для суду (проведення комп'ютерно-технічних експертиз, об'єктів авторського права), а також збирання оперативної інформації, яку не будуть

використовувати як докази у суді. Крім того, до комп'ютерної криміналістики належать і суміжні області, у яких дослідження комп'ютерної інформації має важливу роль: розслідування інцидентів інформаційної безпеки в організаціях, компаніях, банківських установах.

Криміналістичний процес, що проводять спеціалісти та експерти, [1] поділяють на чотири етапи:

1) збирання самої інформації як такої, а також носіїв комп'ютерної інформації супроводжується помітками атрибутів, зазначенням джерел походження даних і об'єктів. У процесі збирання необхідно забезпечуватись повнота і цілісність (незмінність) інформації, а у деяких випадках її конфіденційність. Інколи під час збирання доводиться застосовувати спеціальні заходи для фіксації недовговічної інформації (наприклад, поточних мережевих з'єднань або вмісту оперативної пам'яті комп'ютера);

2) дослідження експертами зібраної інформації передбачає зчитування її з носіїв, декодування та вилучення необхідної інформації, що стосується справи. Деякі дослідження можуть бути автоматизовані експертом, але при цьому залишається достатньо ручної та інтелектуальної праці. У процесі дослідження також повинна забезпечуватись цілісність інформації;

3) вибрана інформація аналізується для отримання відповідей на поставлені експерту чи спеціалісту запитання. Під час аналізу використовують лише наукові апробовані методи, достовірність яких підтверджено раніше;

4) оформлення результатів дослідження і аналізу у встановлений законом та зрозумілим для неспеціалістів формі документ (висновок).

Роль експерта у проведенні розслідувань

Основні характеристики, якими повинен володіти кваліфікований експерт-криміналіст (investigator), це здатність бути креативним у виявленні доказів, ретельність у застосуванні знань і вмінь під час проведення експериментів, розуміння правових питань, що виникають у процесі розслідувань. Спеціаліст повинен грати роль неупередженої третьої сторони. Зацікавленість експерта може вплинути на достовірність остаточних результатів; крім того, може виникнути конфлікт інтересів.

Завдання у комп'ютерних криміналістів є одними з найскладніших у галузі інформаційних технологій. Важливою вимогою є застосування детермінованого, повторюваного процесу дослідження, який є зрозумілим, виразним і якомога простим. Дотримання цього процесу є найціннішою позитивною рисою для експерта. Тому ми пропонуємо використання експертом таких елементів:

- ✓ перехресна перевірка виявлених результатів – за можливості використовувати більше ніж одну програму (інструментальний засіб) для перевірки результатів;
- ✓ правильне поводження з доказами: експерт повинен представити докази у такій самій незмінній та цілісній формі, у якій їх було зібрано раніше (наприклад, фіксування криптографічних хеш-функцій MD5 та SHA-1 із досліджуваних файлів є схожими до “відбитків пальців” у судовій експертизі);
- ✓ повнота дослідження чи розслідування: після виконаних досліджень експерт повинен бути здатним довести їхні повноту і завершеність;
- ✓ управління архівами: збереження резервних копій матеріалів справи у випадку проведення додаткових робіт чи експертиз на вимогу замовника;
- ✓ технічна компетентність – експерт має розуміти те, що він робить з метою уникнення конфліктів чи спірних ситуацій у майбутньому;
- ✓ точні визначення та обґрунтування процесу потрібні для нормального розуміння кроків та результатів дослідження третьою стороною;
- ✓ дотримання законодавства у кримінальних справах, а також дотримання корпоративних політик та нормативних документів у внутрішніх розслідуваннях компаній;
- ✓ гнучкість: через різноманітність інцидентів, що розглядаються, експертові потрібно освоювати нові технології та програми для успішного виконання поставлених завдань.

Сучасні інструментальні засоби дослідження комп'ютерної техніки

Важливим елементом у процесі дослідження комп'ютерної техніки є вибір необхідних інструментальних засобів (програмного забезпечення) для проведення експертиз та розслідувань інцидентів, оскільки вони бувають різноманітними, а деколи навіть і нетиповими.

Сьогодні є велика кількість програмних продуктів [2] для досліджень у галузі комп'ютерної криміналістики: для експертиз комп'ютерів, мобільних телефонів та смартфонів, аналізу оперативної пам'яті, комп'ютерних мереж.

Окремої уваги серед них заслуговує потужне технічне рішення *EnCase Forensic v7* [3] (найновіша його версія v7.06), що являє собою багатозадачний програмний комплекс, який використовують у багатьох країнах світу. За період свого існування EnCase Forensic став галузевим стандартом в отриманні та аналізі цифрових даних. Його потужні фільтри та скрипти дозволяють розслідувати інциденти з можливістю подальшого передавання справи до суду, ґрунтуючись на достовірних доказах. Навіть у силу того, що EnCase Forensic є комерційним програмним продуктом, він допомагає організаціям зекономити гроші, скорочуючи час розслідування експертами порівняно з традиційними способами збирання доказів. Цього досягають внаслідок використання криміналістами гнучких можливостей пошуку, стандартних фільтрів і різноманітних сценаріїв користувачів, які допомагають автоматично аналізувати і структурувати відповідні дані.

У продукті EnCase Forensic v7 додано багато нових елементів і можливостей для досягнення основної мети – збільшення ефективності та результативності роботи експертів. Для досягнення цієї мети в EnCase Forensic v7 було введено новий робочий процес, за допомогою якого дослідники можуть автоматизувати типові задачі, виконуючи об’ємний пошук, розпізнавати важливі деталі та створювати грамотні звіти ще швидше, ніж раніше. Цей підхід можна легко адаптувати відповідно до потреб різних організацій. Ця революційна модифікація вносить істотні вдосконалення у процес комп’ютерної експертизи.

Основні моменти нового підходу у розслідуваннях за допомогою EnCase Forensic v7:

✓ Збирання даних є ключовим моментом в отриманні доказів. Експерти можуть бути впевненими у цілісності інформації та відсутності компрометації. Усі докази, зібрані EnCase Forensic, схвалені судами всього світу. Де факто ці формати (EO1 і LO1) поширені як стандарт зберігання доказів. У 7-й версії нові файли (Ex01 і Lx01) можуть бути зашифровані в EnCase Forensic, додаючи ще один рівень безпеки для найнадійнішого формату файла в комп'ютерній криміналістиці.

✓ Обробка даних – кількість зібраних даних з кожним днем збільшується, і тому експертам необхідний швидкий і надійний спосіб обробки інформації для успішного розслідування. EnCase Evidence Processor дає змогу автоматизувати загальні задачі, які необхідні для підготовки зібраних доказів до розслідування; може бути адаптований під різні потреби експертів.

✓ Глибокий криміналістичний аналіз – EnCase Forensic – є відомий здатністю добувати докази, котрі можуть залишатись непоміченими, коли експерти аналізують дані іншими продуктами.

✓ Накопичення відомостей: використовуючи налаштовувані шаблони, експерти можуть створювати привабливі, професійні звіти, які легко читаються.

✓ Архів даних: якщо експерту коли-небудь у майбутньому знадобиться інформація про якесь проведене розслідування, то він може звернутись в архів EnCase Forensic v7. Коли розслідування буде завершене, експерт кількома кліками миші зможе заархівувати докази, знахідки, звіти, пов’язані з цією справою, гарантуючи при цьому незмінність даних.

Ось лише деякі з основних удосконалень і нових можливостей для експертів у EnCase Forensic v7.

Підтримка смартфонів і Tablet PC: отримання даних з пристроїв, що працюють у таких ОС:

- Apple iOS
- Google Android ™ OS
- Rim 'Blackberry ™ OS

- HP Palm ™ OS
- Nokia Symbian
- Microsoft's Windows Mobile OS

Вбудоване шифрування: шифрування даних просто в EnCase Forensic v7c, використовуючи алгоритм AES-256.

Покращений формат файлів доказів: новий, покращений формат файлів ExOl і LxOl, побудований на основі перевірених форматів E01і L01, призведе до зростання продуктивності.

EnCase Evidence Processor: автоматизація типових завдань, пов'язаних із розслідуванням, передбачає:

- Відновлення папок
- Аналіз сигнатури файла
- Аналіз захищених файлів
- Аналіз хешу (MD5 і SHA-1)
- Виявлення складених файлів
- Пошук електронної пошти (PST, NSF, DBX, EDB, AOL, MBOX)
- Пошук "слідів" в Інтернеті (IE, Firefox, Safari)
- Пошук за ключовими словами
- Індексування

EnScript Module Processing: у EnCase Forensic v7 у процесор за замовчуванням вбудовані наступні модулі:

- System Info Parser
- IM Parser (AOL, MSN, Yahoo)
- File Carver
- Personal Information (CC, Phone Numbers, Email, SSN)
- Windows Event Log Parser
- Windows Artifact Parser
- Unix Login
- Linux Syslog Parser

Новий механізм індексування: оптимізований для експертів-криміналістів разом з потужною мовою запитів.

Підтримка нових типів файлів і файлових систем:

- EXT4
- HSFX
- Microsoft Office 2010
- Образ iOS (iPad, iPhone, iPod)

Нова підтримка шифрування: підтримка Checkpoint / Pointsec Full Disk Encryption. Оновлена поточна підтримка шифрування.

Налаштовувані шаблони: створення користувацьких шаблонів звітів для послідовної звітності.

Оформлення: виберіть оформлення для кожної секції в звіті для задоволення потреб аудиторії.

Простий експорт: збереження звітів у різних форматах Text, RTF, HTML, XML, PDF.

Вбудований звіт для смартфонів: заздалегідь заданий звіт, що відображає детальну інформацію, отриману зі смартфона. Є можливість експорт у KML формат.

Нова платформа аналізу E-mail: дослідження є так само просте, як і читання листів у поштовій скриньці. Додані можливості перегляду e-mail для розкриття контексту та ідентифікації співрозмовників, пов'язаних із розслідуванням.

Мітки: створення користувальницьких міток до будь-яких файлів, включаючи записи хеш, що забезпечують експорт файлів для огляду іншими особами.

Єдиний пошук: вбудоване індексування, пошук за ключовими словами і мітками.

Особливої уваги в галузі криміналістичних досліджень мобільних телефонів та смартфонів потребує потужне технічне рішення *Мобильный Криминалист 2013* [4] (найновіша його версія v5.1), який використовують у понад 50 країнах світу, зокрема Великобританії, США, Німеччині, Нідерландах, Росії і т.д. Використання спеціальних протоколів доступу дозволяє програмі витягати основні дані телефонів та SIM-карток, список контактів, абонентські групи, номери швидкого набору, пропущені, вхідні та вихідні дзвінки, повідомлення SMS, MMS та електронної пошти зі стандартних папок і створених користувачем, видалені повідомлення (але з деякими обмеженнями), час і дату надходження повідомлень SMS до Центру Відправки Повідомлень (SMSC) провайдера зв'язку, розклад календарних подій, завдання, текстові нотатки, безпосередньо внесені користувачем; фотографії, відео, мелодії, дані секції Lifeblog (усі головні події в телефоні з географічними координатами), додатки Java, файлову систему пам'яті телефону та карти пам'яті (різних форматів), дані трафіку GPRS і Wi-Fi, голосові записи та аудіокліпи, тимчасові файли та закладки інтернет-браузерів. Кількість можливостей, що підтримуються у конкретних випадках, залежить від моделей мобільних телефонів; а список моделей мобільних пристроїв, що підтримуються, сьогодні становить близько 6500 і постійно зростає.

Основні види даних, доступні для вилучення у *Мобильный Криминалист 2013*:

- Основні дані пам'яті телефону і дані SIM-карти
- Список усіх контактів (зокрема номери мобільних і стаціонарних телефонів, факсів, поштові адреси, фотографії контактів та іншу інформацію про контакти)
- Органайзер (зустрічі, нотатки, нагадування про дзвінки, річниці та дні народження, списки справ)
- Повідомлення SMS (повідомлення, журнал повідомлень, папки, видалені повідомлення з деякими обмеженнями)
- Тимчасові файли та закладки інтернет-браузерів
- Захист цілісності даних алгоритмами MD5, SHA-1, SHA-2, CRC, HAVAL, ГОСТ Р34.11-94
- Повідомлення електронної пошти з вкладеннями
- Журнал трафіку і сесій GPRS, EDGE, CSD, HSCSD и Wi-Fi
- Файли мультимедія
- Всі файли з пам'яті телефону, а також з карти пам'яті, зокрема встановлені додатки та їхні дані
- Дані журналу “Lifeblog”, що містить список дій з телефоном з географічними координатами.

Унікальні можливості, доступні лише Мобільному Криміналісту 2013:

✓ Робота зі смартфонами на базі IOS, Android, Symbian OS, Windows Mobile і BlackBerry. Обсяг корисних даних з цих пристроїв значно перевершує можливості інших продуктів.

✓ Географічне положення подій (Хронологія подій). Мобільний Криміналіст 2013 надає доступ до географічного положення подій (Хронологія подій). Він визначає і показує на карті положення подій мобільного телефону: прийнятих і відправлених повідомлень, фотографій, календарів і т.д. Сучасні мобільні телефони і особливо смартфони все частіше зберігають інформацію про місцезнаходження, в якому відбулася та чи інша дія. А така оперативна інформація, безумовно, під час розслідування дає змогу встановити місцезнаходження власника телефону в певний момент часу. Мобільний Криміналіст 2013 витягує географічні дані, що зберігаються як у вигляді координат, так і у вигляді номерів базових станцій операторів стільникового зв'язку. Після перетворення даних розташування відображається на карті безпосередньо в програмі і може масштабуватися. Також можливе відображення в окремому вікні браузера. Окремої уваги заслуговує Хронологія подій – додаток, встановлене в більшості смартфонів на платформі Symbian OS, яке зберігає інформацію про основні події телефону: СМС, події календаря, фотографії і т.д. Тут ключовим моментом є можливість співвідносити ці дані з певними географічними координатами. Мобільний Криміналіст 2013, використовуючи дані програми, дає можливість визначити місцезнаходження власника телефону в момент, коли він здійснив якусь дію. Мобільний Криміналіст 2013 – це єдина програма, яка витягує інформацію про географічне положення події і показує місце події на карті.

✓ Аналіз інтернет-браузерів. Аналізатор інтернет-браузерів для програми Мобільний Криміналіст 2013 витягує і показує тимчасові файли, що створюються в телефоні при перегляді веб-сторінок. Надаються список відвіданих Інтернет сайтів та файли, скачані браузером мобільного телефону (як попередньо встановленим, так і браузерами інших компаній).

✓ Вилучення даних з користувацьких папок повідомлень. Смартфони на додаток до стандартних папок повідомлень дозволяють створювати свої, наприклад, для повідомлень певного типу або від певного абонента. У таких папках часто зберігається найбільша цікава інформація. Жодна програма, крім Мобільного Криміналіста не спроможна отримати доступ до повідомлень у користувацьких папках.

✓ Вилучення інформації про видалені повідомлення.

✓ Прямий доступ до даних. Доступ до смартфонів Windows Mobile, відбувається минаючи ActiveSync / Vista Sync Center, які потенційно можуть змінити дані в досліджуваному пристрої.

✓ Доступ до журналу подій смартфонів Symbian OS, включає крім дзвінків інформацію про сесії пакетної передачі даних (GPRS, EDGE, CSD, HSCSD і Wi-Fi).

✓ Доступ до журналу подій смартфонів на базі Windows Mobile.

✓ Вилучення міток полів контактів зі смартфонів Symbian OS, зокрема і змінених користувачем.

✓ Вилучення множинних однотипних полів з пристроїв на базі Symbian OS. Дані не губляться при відображенні, якщо їх типи і модифікатори збігаються з витягнутими раніше полями.

✓ Розширений набір інформації про контакти. Витяг інформації про приналежність контактів до груп абонентів і про призначені швидких наборах, які є непрямим показником частоти спілкування власника телефону з вказаними абонентами.

✓ Вилучення дати і часу останньої зміни контактів і подій календаря.

✓ Вилучення точного часу відправлення повідомлень, яка призначається Центром надсилання повідомлень (SMSC) провайдера зв'язку. Доступно для смартфонів на базі Symbian OS.

✓ Просте підключення пристроїв. Витяг даних відбувається через стандартні кабелі та адаптери. Не потрібне додаткове дороге обладнання.

✓ Унікальний Forensic-протокол для доступу до смартфонів, створений спеціально для безпечного вилучення максимуму інформації. Водночас стандартні протоколи (AT, OBEX, SyncML), використовувані іншими продуктами, розроблені для синхронізації і можуть змінити дані досліджуваного пристрою.

✓ Вилучення даних з ексклюзивних пристроїв, таких як Vertu і Mobiado.

Однак використання даного продукту є проблематичним для багатьох організацій у зв'язку з його високою вартістю (1999 € ≈ 22000 грн.) А схожого або аналогічного аналога програмного продукту класу freeware на ринку немає.

Висновок

Доцільним є вибір експертами-криміналістами потужних технічних рішень для розв'язання поставлених перед ними задач, а також використання за можливості кількох програм (інструментальних засобів) перехресної перевірки отриманих результатів. Такий підхід є ефективним способом у розслідуванні інцидентів всередині компаній та організацій у зв'язку з невпинним розвитком у галузі високих технологій. Але використання описаних комерційних програмних продуктів є неможливим для багатьох організацій через їхню високу вартість. Такі продукти можуть використовувати великі компанії з відповідними фінансовими можливостями, наприклад при розслідуванні інцидентів інформаційної безпеки.

Отже, нашим подальшим науковим дослідженням буде пошук альтернативних варіантів з використанням безкоштовного чи відкритого програмного забезпечення, розробка власних методик на базі відкритого програмного забезпечення та удосконалення існуючих методологій дослідження об'єктів інформаційних технологій у комп'ютерній криміналістиці.

1. Kent K., Chevalier S., Grance T., Dang H. Guide to Integrating Forensic Techniques into Incident Response – Recommendations of the National Institute of Standards and Technology (NIST), Publ. 800-

86.2006. 2. List of digital forensics tools. // http://en.wikipedia.org/wiki/List_of_digital_ forensics_tools. 3. EnCase Forensic v7. The industry-standard computer forensic solution. Fast, powerful, and proven in courts. // http://www.guidancesoftware.com/encase-forensic.htm. 4. Мобильный Криминалист 2013 // http://www.oxygen-forensic.com/ru/.