Юридичні науки

УДК 343.132.1+343.98

Колесник Віталій Геннадійович

завідувач відділу

комп'ютерно-технічних та телекомунікаційних досліджень

Харківський науково-дослідний експертно-криміналістичний центр

Міністерства внутрішніх справ України

Колесник Виталий Геннадьевич

заведующий отделом

компьютерно-технических и телекоммуникационных исследований

Харьковский научно-исследовательский

экспертно-криминалистический центр

Министерства внутренних дел Украины

Kolesnyk Vitalii

Head of the Department of Computer and Telecommunication Studies

Kharkiv Scientific Research Forensic Center of the

Ministry of Internal Affairs of Ukraine

ОСОБЛИВОСТІ ЗБИРАННЯ ТА ФІКСАЦІЇ ІНФОРМАЦІЇ З ЦИФРОВИХ НОСІЇВ ПІД ЧАС ПЕРШОЧЕРГОВИХ СЛІДЧИХ ДІЙ
ОСОБЕННОСТИ СБОРА И ФИКСАЦИИ ИНФОРМАЦИИ С ЦИФРОВЫХ НОСИТЕЛЕЙ ВО ВРЕМЯ ПЕРВООЧЕРЕДНЫХ СЛЕДСТВЕННЫХ ДЕЙСТВИЙ
COLLECTING AND FIXATION OF INFORMATION FROM DIGITAL EVIDENCE DURING PRIMARY INVESTIGATIVE ACTIONS

Анотація. *У статті розглянуто процесуальні теоретичні та практичні аспекти збирання та фіксації інформації з цифрових носіїв під час слідчих дій. Досліджено проблемні питання виявлення даних,*

розглянуто алгоритм та практичні методи вилучення та фіксації волатильних даних, акцентовано увагу на важливість фіксації цих даних, досліджено програмне забезпечення для проведення збору та фіксації волатильних даних.

Ключові слова: *дослідження цифрових носіїв, першочергові слідчі дії, збирання волатильних даних.*

Аннотация. *В статье рассмотрены процессуальные теоретические и практические аспекты сбора и фиксации информации с цифровых носителей во время следственных действий. Исследовано проблемные вопросы выявления данных, рассмотрен алгоритм и практические методы изъятия и фиксации волатильных данных, акцентировано внимание на важность фиксации этих данных, исследовано программное обеспечение для проведения сбора и фиксации волатильных данных.*

Ключевые слова*: исследование цифровых носителей, первоочередные следственные действия, сбор волатильных данных.*

Summary. *The article deals with the procedural theoretical and practical aspects of collecting and recording information from digital evidences during primary investigative actions. The problematic issues of data discovery are investigated, the algorithm and practical methods of extracting and fixing volatile data are considered, the importance of fixing this data is emphasized, the software for conducting the volatile data collection and fixation is examined.*

Key words: *digital evidence investigation, primary investigative actions, volatile data collection.*

Останніми роками в Україні продовжується стрімке впровадження інформаційно-комунікаційних технологій майже у всі сфери життєдіяльності суспільства. Нормативно курс на інформатизацію був

заданий прийняттям 4 лютого 1998 року під №74/98-ВР Закону України «Про Національну програму інформатизації» [1].

Розвиток і впровадження інформаційних технологій для громадян, широкі можливості здійснювати миттєвий обмін інформацією, миттєво здійснювати фінансові операції без відвідування відділення банку, можливості реалізації товарів і послуг за допомогою мережі Інтернет, доступ до широкого кола різноманітних державних електронних реєстрів – все це було одразу ж взяте на озброєння сучасними злочинцями. Все частіше інформація, що має доказове значення, зберігається не в паперових документах та журналах, а розташована в електронному вигляді на носіях засобів комп'ютерної техніки (далі – ЗКТ), серверах, мережевих сховищах, базах даних, у пам'яті мобільних пристроїв та навіть у хмарних сховищах.

Наявність швидкісного доступу до мережі Інтернет, широкий вибір програмних продуктів для віддаленого керування (адміністрування) та віртуалізації робочого середовища дозволяють використовувати у якості знарядь та засобів вчинення злочинів віддалені комп'ютерні системи. Сучасний злочинець фізично знаходячись в одному місці за своїм комп'ютером, може керувати процесами та проводити будь які операції віддалено на іншій системі, що значно ускладнює подальші пошук та фіксацію доказів, адже, після затримання підозрюваного та вилучення у нього ЗКТ, на їх носіях ніякої доказової інформації (окрім можливих слідів з'єднання з віддаленою системою) виявлено не буде. При цьому сама віддалена система зі всією інформацією буде недосяжною для правоохоронців, оскільки без завчасно проведених слідчих та розшукових дій по встановленню схеми та документуванню злочинної діяльності, не буде зрозуміло, де фізично знаходиться ця віддалена система – в сусідньому кабінеті, чи може на сервері на території іншої держави.

Аналізуючи варіанти проведення огляду при розслідуванні злочинів, вчинених з застосуванням інформаційних технологій, слід зазначити, що у

КПК України містяться поняття огляду місця події, огляду місцевості, огляду приміщення, огляду речей та документів, однак нічим не передбачено огляд інформації розташованої віддалено, за умови доступу до неї безпосередньо з місця події чи об'єкту огляду. При цьому, юридично, вона розташована за іншою адресою і тому на неї не розповсюджується дія ухвали суду. На теперішній час немає усталеної практики та є спірним питання, чи законною буде така дія, якщо суд в ухвалі окремо зазначить про надання процесуальним особам можливості також здійснити огляд інформації, розташованої віддалено.

Згідно з ч. 1 ст. 237 КПК України [2] огляд приміщення, речей та документів як слідча (розшукова) дія проводиться слідчим, прокурором з метою виявлення та фіксації відомостей щодо обставин вчинення кримінального правопорушення. Згідно з цим, вся інформація що відтворюється у ЗКТ під час огляду (у тому числі розташована віддалено) може бути оглянута та зафіксована, у тому числі шляхом копіювання, оскільки вона перебуває у доступності для особи, що проводить огляд. Враховуючи, що сліди таких злочинів знаходяться у цифровому вигляді, окрім візуального огляду, цілеспрямованому огляду також можуть підлягати веб-сайти, сторінки соціальних мереж, рекламні оголошення, вміст електронної поштової скриньки, чатів, на практиці дуже часто виникають питання, чи допустимо додавати таку інформацію до протоколу огляду місця події, чи необхідно створювати окремий протокол огляду, яким саме має бути цей протокол – огляду предмета чи огляду документів. У ч. 2 ст. 99 КПК України зокрема наголошується, що носії інформації (у тому числі електронні) можуть належати саме до документів.

Такі неузгодженості можуть призвести до того, що суд визнає недопустимою частину огляду ЗКТ у протоколі огляду місця події, оскільки буде вважати що необхідно було скласти окремий протокол, або визнає недопустимим окремий протокол огляду предмета, оскільки буде

вважати, що мав бути складений протокол огляду документа. Отже, проблема визначення такого об'єкту огляду з метою його правильної процесуальної фіксації потребує однозначного правового врегулювання.

Перш ніж перейти до аналізу практичних процедур, звернімося до процесуальної частини питання. У статтях 159, 168 чинного КПК закріплена низка положень, які, на думку законодавця призвані мінімізувати тиск на бізнес, обмежуючи та забороняючи вилучення електронних інформаційних систем або частин та зобов'язуючи слідчого, прокурора у разі необхідності виготовляти їх копії із залученням спеціаліста. Проте, на практиці з цим виникає ряд проблем і картина є дещо інакшою: по-перше, ніде і нічим не передбачено виділення носіїв на які мають виготовлятися ці копії (а вони потрібні значного обсягу та недешеві), по-друге, кількість спеціалістів, які мають необхідні навички, досвід та програмне забезпечення для виготовлення копій, не відповідає кількості слідчих дій. Інспектори-криміналісти слідчих підрозділів, здебільшого, такими навичками не володіють.

В роботі [3, с. 104] науковцями із залученням фахівців-практиків був розроблений загальний алгоритм техніки огляду увімкненого ЗКТ, у якому окремими кроками вказані зібрання та документування волатильних даних та мережних даних:

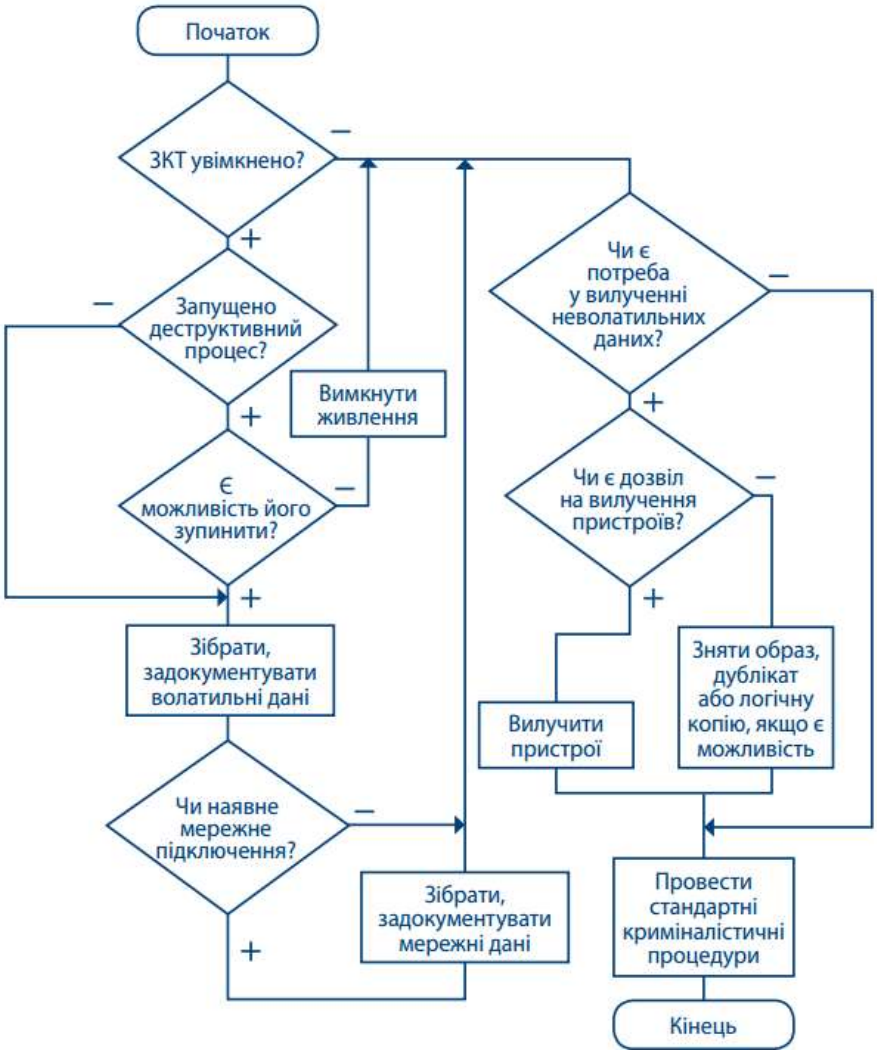


Рис. 1. Загальний алгоритм техніки огляду ЗКТ [3, с. 104]

Однак, на практиці процедура з фіксації волатильних даних наразі фактично не відбувається. Причинами уникання фіксації таких даних вбачаються:

1. Відсутність теоретичної та практичної підготовки у працівників поліції та криміналістів;
2. Відсутність носіїв для збереження вилучених даних;
3. Відсутність спеціального програмного забезпечення для вилучення даних;
4. Небажання слідчого «затягувати» проведення слідчої дії, витрачати зайвий час на залучення окремого спеціаліста, очікувати на вилучення даних, витрачати час на описування процедур в протоколі.

5. Недостатня інформованість слідчого у важливості (за деякими видами злочинів) фіксації саме волатильних даних, відсутність теоретичної бази самостійно (без спеціаліста) описати відповідні процедури в протоколі.

Розгляньмо докладніше початковий алгоритм огляду увімкненого ЗКТ [3, с. 110].

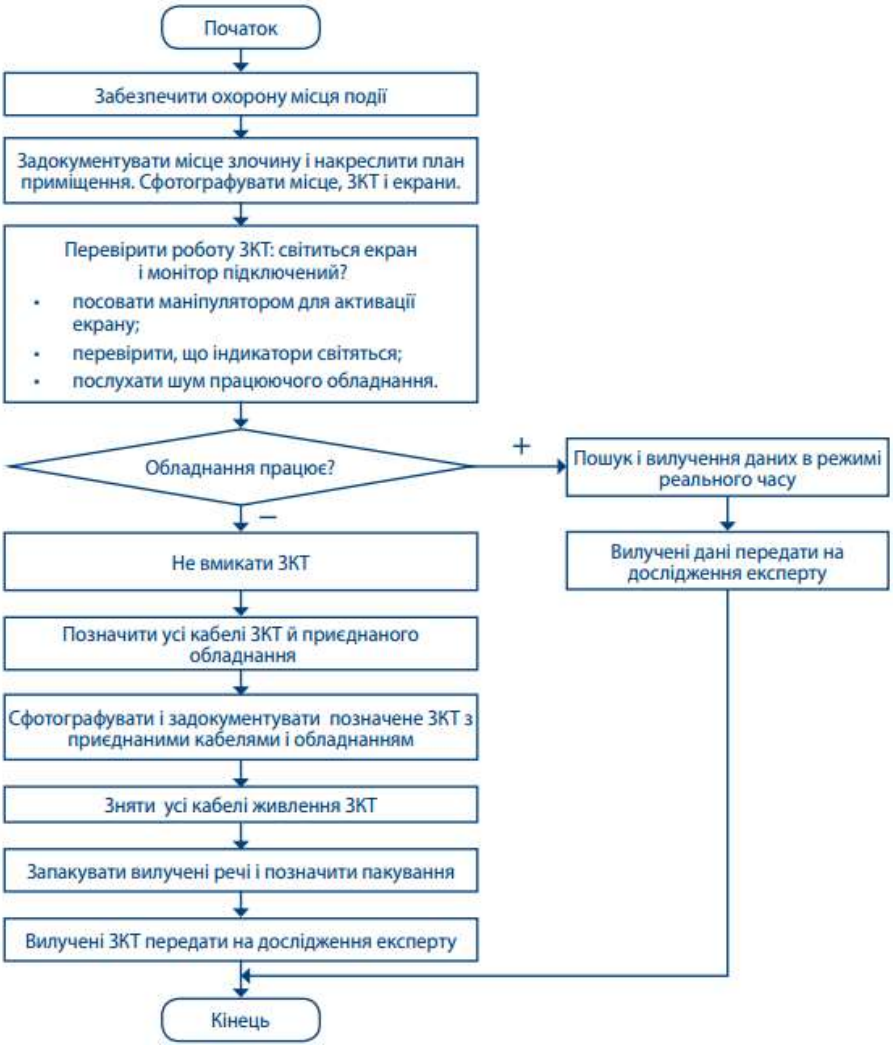


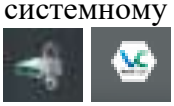
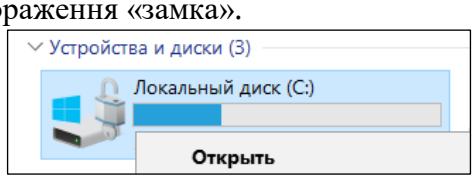
Рис. 2. Початковий алгоритм огляду увімкненого ЗКТ [3, с. 110]

Пересвідчившись, що обладнання працює, необхідно зафіксувати (сфотографувати) місце навкруги ЗКТ, сам ЗКТ з приєднаними кабелями і обладнанням та всі екрани (монітори, дисплеї). Далі перевірити роботу екрану (монітору), якщо він вимкнений чи перебуває в режимі очікування – ввімкнути його. Після цього необхідно сфотографувати зображення, що

відтворюється на моніторі. Після цього необхідно провести первинний огляд системи на наявність ознак шифрування та відкритих (монтованих) томів (таблиця 1):

Таблиця 1

Найбільш поширені засоби шифрування у ОС Microsoft Windows

Засіб шифрування	Ознаки у системі	Візуальні ознаки	
TrueCrypt	1. Наявність папок та файлів: ▪ C:\Program Files\TrueCrypt\ ▪ C:\Users\%user%\AppData\Roaming\TrueCrypt\Configuration.xml 2. Наявність файлів великого розміру (більше 10 Гб) без розширення або з розширенням, але не працюючих (наприклад відеофайл "S02E02.720p. BDRip.Eng.mkv" розміром 100 Гб, що не відтворюється програвачем та не містить метаданих та ознак відеофайлу.	Ярлик:  	Значок у системному лотку: 
VeraCrypt	1. Наявність папок та файлів: ▪ C:\Program Files\VeraCrypt\ ▪ C:\Users\%user%\AppData\Roaming\VeraCrypt\Configuration.xml 2. Аналогічно TrueCrypt.	Ярлик:  	Значок у системному лотку: 
Bitlocker	1. Іконка логічного диску містить зображення «замка».  На самому носії ЗКТ або зовнішніх носіях користувача може бути виявлений ключ відновлення. За замовчуванням він являє собою текстовий файл .TXT розміром 1388 байт з іменем «Ключ восстановления BitLocker X», де X – ідентифікатор диска.	Зображення монтованого та размонтованого диску: 	
AxCrypt	1. Наявність папок та файлів: ▪ C:\Program Files\AxCrypt ▪ C:\Users\%user%\AppData\Local\AxCrypt\	Ярлик:  	Значок у системному лотку: 
DiskCryptor	1. Наявність папок та файлів: ▪ C:\Program Files\dcrypt ▪ C:\Users\%user%\AppData\Local\AxCrypt\	Ярлик:  	Значок у системному лотку: 

Перш ніж переходити до етапу вилучення волатильних даних необхідно розуміти, що цей процес потребує під'єднання до ЗКТ одного або декількох носіїв. Якщо слідча дія пов'язана з обшуком, виїмкою, або під час слідчої дії присутні сам обшукуваний, його захисник або адвокат, цей процес зазвичай викликає в них негативну реакцію, оскільки, на їх думку, таким діями поліція вчиняє підозрілі дії по «підкиданню» доказів на носій ЗКТ і таким чином компрометує об'єкт огляду. Ці особи можуть робити заяви та зауваження, що інформація на ЗКТ, нібито, таким чином буде змінена, скомпрометована, та взагалі не може бути використана у подальшому процесі доказування. Ніяких юридичних підстав забороняти спеціалісту це робити немає, навпаки, ст. 71 КПК прямо надає спеціалісту право користуватися технічними засобами, приладами та спеціальним обладнанням. З метою уникнення подібних маніпуляцій, по-перше, необхідно зафіксувати в протоколі точний час першого під'єднання кожного носія та інформацію про нього, по-друге – продемонструвати всім зацікавленим особам вміст носіїв. У більшості випадків, цих дій буває достатньо для підтвердження законності вказаної процедури.

Зупинімося докладніше на етапі пошуку і вилучення даних в режимі реального часу. На теперішній час створено досить велику кількість програмних продуктів для пошуку та фіксації таких даних. Умовно такі продукти можна поділити на:

1. Безкоштовні (для вільного користування, freeware) та пропрієтарні (commercial, комерційні, оплачувані).

2. Програмні продукти для загального користування (адміністрування системи тощо) та вузькоспеціалізовані (для правоохоронних органів, спрямовані на вилучення конкретних типів даних).

Крім того, інструменти для вилучення даних в режимі реального часу відрізняються в залежності від цільової операційної системи, в якій

має проводитися збирання інформації. У таблиці 2 наведені програмні продукти для збирання та фіксації енергозалежних (волатильних) даних [4-6], в залежності від типу даних та операційної системи:

Таблиця 2

Програмне забезпечення для збирання та фіксації волатильних даних

Тип, вид енергозалежних даних	Інструменти для Microsoft Windows (безкоштовні)	Інструменти для Microsoft Windows (платні)	Інструменти для Linux/Mac
Вміст оперативної пам'яті (RAM)	▪ Belkasoft RAM Capturer; ▪ MAGNET RAM Capture; ▪ AcessData FTK Imager; ▪ Memoryze ▪ Binalyze IREC (Free Edition); ▪ CDIR Collector	▪ PassMark OSForensics; ▪ Helix3 Pro	▪ dd (/dev/mem); ▪ LiME; ▪ Evimetry linux (Controler+liveagent); ▪ Memoryze for the Mac; ▪ Blackbag's Macquisition; ▪ OSXpmem; ▪ Mac Memory Reader; ▪ Helix3 Pro
Файл підкачки MS Windows "pagefile.sys" запущеної системи	▪ AcessData FTK Imager; ▪ Binalyze IREC (Free Edition); ▪ RawCopy.	▪ PassMark OSForensics; ▪ X-Ways Forensics	–
Відомості про систему	▪ MiTeC System Information X; ▪ Autoruns; ▪ LoadOrder; ▪ RAMMap; ▪ VMMap; ▪ Binalyze IREC (Free Edition)	▪ PassMark OSForensics; ▪ Helix3 Pro	▪ sudo lshw -html > lshw.html; ▪ sudo fdisk -l ▪ lscpu; ▪ lsblk -a; ▪ dmidecode
Списки активних процесів	▪ PsList; ▪ Process Explorer; ▪ Autoruns; ▪ Binalyze IREC (Free Edition);	▪ Binalyze IREC (Tactical Edition); ▪ Helix3 Pro	▪ ps -ef; ▪ lsof ▪ sudo pstree;
Відомості щодо файлів попередньої вибірки (Prefetch)	▪ Advanced Prefetch File Analyzer; ▪ Binalyze IREC (Free Edition); ▪ WinPrefetchView; ▪ CDIR Collector	▪ PassMark OSForensics; ▪ Binalyze IREC (Tactical Edition);	–
Мережеві налаштування, інтерфейси, маршрути, програми та служби що	▪ ipconfig /all, ipconfig /displaydns, route print, arp -a, netstat -a, netstat -an, netstat -ab, sc queryex, net share; ▪ (Nirsoft):	▪ COFEE; ▪ Live Response; ▪ Windows Forensic Toolchest (WFT) ▪ Binalyze IREC (Tactical Edition);	▪ netstat -r -n, route, arp -a, netstat -a, ifconfig, ifconfig -a, netstat -in, netstat -tunp, netstat -an, lsof;

Тип, вид енергозалежних даних	Інструменти для Microsoft Windows (безкоштовні)	Інструменти для Microsoft Windows (платні)	Інструменти для Linux/Mac
використовують мережу, відкриті ресурси	AdapterWatch, AppNetworkCounter, NetRouteView, CurrPorts, NetworkCountersWatch ▪ Binalyze IREC (Free Edition);		
Історія, паролі з інтернет браузерів	▪ (Nirsoft): BrowsingHistoryView, ChromeHistoryView, MZHistoryView, ChromePass, WebBrowserPassView і т.д.; ▪ (SecurityXploded): Browser Password Decryptor, Chrome Password Decryptor, Opera Password Decryptor і т.д.; ▪ CDIR Collector; ▪ CyLR	▪ PassMark OSForensics; ▪ Binalyze IREC (Tactical Edition); ▪ XenArmor All-In-One Password Recovery Pro	▪ LiveResponseCollection – Cedarpelta; ▪ AutoMacTC; ▪ CyLR; ▪ FastIR_Collector_Linux
Виявлення шифрування	–	▪ Elcomsoft Forensic Disk Decryptor	▪ MacQuisition

Отже, як ми можемо бачити, фіксація даних в режимі реального часу наразі можлива як з використанням команд у самих операційних системах, використанням як безкоштовних програмних продуктів (найбільш ефективними вбачаються набір ПЗ Nirsoft Package, AcessData FTK Imager, безкоштовні програмні продукти виробництва SysInternals, MiTeC.cz, SecurityXploded.com), так і спеціалізованих пропрієтарних програмних продуктів для первинного аналізу та зняття інформації з ЗКТ (Binalyze IREC (Tactical Edition), Microsoft's Computer Online Forensic Evidence Extractor (COFEE), Windows Forensic Toolchest (WFT), Rapid Assessment & Potential Incident Examination Report (RAPIER), Helix3 Pro, Live Response, PassMark OSForensics, Oxygen Forensic Key Scout, XenArmor All-In-One Password Recovery Pro).

Після збереження даних в режимі реального часу на окремий носій, та за наявності часу на пошук та наявною необхідностю, є можливість виготовити копію неволатильних даних.

Правильно створена та зафіксована копія інформації, яку потім можна буде використовувати у якості доказу, повинна задовольняти критеріям незмінності та неспростовності, тобто до скопійованої інформації має додаватися перелік файлів з їх первинними атрибутами (мітки часу які файли мали на оригінальному носії) та вона має бути підкріплена підрахуванням контрольної суми. У разі створення файла-образу всього носія або окремого розділу має підраховуватися загальна контрольна сума всієї інформації в них, у разі вибіркового копіювання файлів необхідно підраховувати контрольну суму кожного скопійованого файлу та додавати до копій файл-лист із оригінальними атрибутами, які файли мали на оригінальному носії, оскільки копіювання файлу на інший носій засобами операційної системи призведе до оновлення атрибутів його дати створення та відкриття. Для таких випадків у спеціальному ПЗ є засоби для т.з. «експертного копіювання» (forensic copy) файлів із збереженням їх оригінальних атрибутів:

1. У ПЗ AccessData FTK Imager передбачено функцію створення файлу-образу окремого каталогу «Export Logical Image (AD1)», що дозволяє зберегти окремий каталог з усім вмістом у експертний файл-образ формату .AD1. Крім цього в ПЗ передбачено функцію створення файлу-образу .AD1 з набором обраних файлів та каталогів (у т.ч. з різними шляхами) «Add to Custom Content Image (AD1)». В обох варіантах копіювання оригінальні атрибути файлів будуть збережені.

2. Відповідні функції для копіювання файлів із збереженням оригінальних атрибутів також мають програмні продукти: X-Ways Forensics, OSForensics, KillCopy, FastCopy, Nuix Evidence Mover.

Литература

1. Закон України «Про Національну програму інформатизації» // Відомості Верховної Ради України (ВВР), 1998, № 27-28, ст.181.
2. Кримінальний процесуальний кодекс України: Кодекс України, Закон, Кодекс від 13.04.2012 № 4651-VI // Відомості Верховної Ради України (ВВР), 2013, № 9-10, № 11-12, № 13, ст. 88.
3. Виявлення, попередження та розслідування злочинів торгівлі людьми, вчинених із застосуванням інформаційних технологій: навчальний курс / [А. Вінаков, В. Гузій, Д. Девіс, В. Дубина, М. Каліжевський, О. Манжай, В. Марков, В. Носов, О. Соловйов]. К., 2017. 148 с.
4. В.А. Кудінов. Основні програмні засоби аналізу волатильних даних, які можна використовувати для огляду засобів комп'ютерної техніки під час розслідування кіберзлочинів та злочинів торгівлі людьми. / Матеріали конференції «Актуальні питання протидії кіберзлочинності та торгівлі людьми». Харків, 2018.
5. Carvajal, Leonardo & Varol, Cihan & Chen, Lei. (2013). Tools for collecting volatile data: A survey study. 318-322. 10.1109/TAEECE.2013.6557293.
6. Brown, Christopher L.T. Computer Evidence: Collection and Preservation, Second Edition / Charles River Media, ISBN: 9781584506997, 2009.