ИНСТРУМЕНТЫ ЦИФРОВОЙ КРИМИНАЛИСТИКИ

Азиз Кахрамонов
Преподаватель Кафедры криминалистики и судебных экспертиз,
Правоохранительная академия Республики Узбекистан
E-mail: azekmr@gmail.com

Аннотация: *В статье рассматриваются особенности изъятия и обращения с цифровыми накопителями информации (ЦНИ) в рамках следственных действий в Республике Узбекистан. В связи с ростом киберпреступности и все более широким использованием цифровых устройств в преступной деятельности стала очевидной необходимость внедрения цифровой криминалистики в работу правоохранительных органов. В документе описаны этапы работы с ЦСД, начиная с классификации устройств и методов изъятия и заканчивая техническими процедурами сохранения цифровых доказательств. Особое внимание уделяется соблюдению надлежащих процедур по изъятию и упаковке устройств для предотвращения повреждения и искажения данных. Привлеченные специалисты играют важнейшую роль в обеспечении целостности цифровой информации, а также в фиксации данных, которые могут иметь значение для дальнейшего расследования и судебного разбирательства. В статье также подчеркивается важность соблюдения технической терминологии при описании устройств и извлечении данных, что помогает сохранить доказательную базу в ее первоначальном виде.*

Ключевые слова: *цифровая криминалистика, инструменты, программное обеспечение, аппаратные комплексы, анализ данных, исследование.*

Annotatsiya: *Maqolada O‘zbekiston Respublikasi tergov harakatlari doirasida raqamli axborot tashuvchilarini (RAT) olib qo‘yish va ularni ishlov berishning o‘ziga xos jihatlari ko‘rib chiqiladi. Kiberjinoyatlar sonining ortishi va jinoyat sodir etish uchun raqamli qurilmalardan foydalanishning ko‘payishi sababli, huquqni muhofaza qilish organlarida raqamli kriminalistika vositalarini qo‘llash zarurati paydo bo‘ldi. Hujjatda RAT bilan ishlash bosqichlari, qurilmalarni tasniflash va ularni olib qo‘yish usullaridan tortib, raqamli dalillarni saqlash bo‘yicha texnik jarayonlargacha bo‘lgan holatlar bayon etiladi. Qurilmalarning shikastlanishi va ma’lumotlarning buzilishining oldini olish uchun ularni olib qo‘yish va qadog‘lash qoidalariga rioya qilishga alohida e’tibor qaratilgan. Mutaxassislar raqamli ma’lumotlar yaxlitligini ta’minlashda va keyingi tergov va sud ishlari uchun muhim bo‘lgan ma’lumotlarni qayd etishda muhim rol o‘ynaydi. Qurilmalarni tavsiflash va ma’lumotlarni olib qo‘yishda texnik terminologiyaga*

rioya qilish muhim ahamiyatga ega bo‘lib, bu dalillar bazasini o‘zgarishsiz saqlashga yordam beradi.

Kalit so‘zlar: *raqamli kriminalistika, vositalar, dasturiy ta’minot, apparatlar majmuasi, ma’lumotlar tahlili, tadqiqot.*

Abstract: *The article examines the specifics of seizing and handling digital data storage devices (DDSD) within investigative actions in the Republic of Uzbekistan. Due to the increase in cybercrimes and the growing use of digital devices for criminal activities, the need to incorporate digital forensics into the work of law enforcement agencies has become evident. The document describes the stages of working with DDSD, starting from device classification and seizure methods to technical procedures for preserving digital evidence. Particular attention is given to following proper procedures for seizing and packaging devices to prevent data damage and distortion. Engaged specialists play a crucial role in ensuring the integrity of digital information, as well as recording data that may be significant for further investigation and judicial proceedings. The article also highlights the importance of adhering to technical terminology when describing devices and data extraction, helping to maintain the evidence base in its original form.*

Keywords: *digital forensics, tools, software, hardware systems, data analysis, research.*

Существует множество факторов, которые могут затруднить понимание того, какие инструменты следует использовать в определенных ситуациях при исследовании цифровых носителей информации и как вся цифровая информация соединяется для формирования цифровой доказательственной базы. Среди этих факторов можно выделить методы исследования, его цели и тот факт, что некоторые задачи при проведении исследований можно выполнить только индивидуальными способами к конкретному объекту. Со временем эксперт или специалист приобретает предпочтение к определенным инструментам и методам, формируя свой набор «основных» программных и технических средств.

Описание инструментов сопряжено с рядом трудностей. Появляются новые версии и модификации, что может быстро сделать описание устаревшим. Кроме того, инструменты могут менять названия, приобретаться другими компаниями или просто исчезать с рынка. Например, полезный инструмент для исследования стационарных видеорегистраторов «Magnet DVR Examiner» ранее назывался «DVR Examiner 3» или же «Wireshark» ранее назывался «Ethereal». В связи с этим, следует учесть тот факт, что такие изменения неизбежны и что новые разработки могут быстро сделать информацию устаревшей в любой технической области.

Инструменты компьютерно-технической экспертизы.

Компьютерно-техническая экспертиза – это отдельный вид судебной экспертизы, относящаяся к классу инженерно-технических, направленное на изучение цифровых устройств и цифровых данных, хранящихся на них, с целью получения доказательств для использования в следствии и (или) в суде [1].

Сам процесс экспертизы определяется как процесс исследования с использованием компьютерных и иных аппаратно-технических средств, таких как персональные компьютеры, ноутбуки, блокираторы, анализаторы, технические средства для клонирования и т.д. Также для проведения компьютерной экспертизы могут использоваться один или несколько системных блоков для одновременного исследования нескольких объектов, или же с использованием виртуализации, позволяющей нескольким виртуальным компьютерам работать на одном физическом блоке, что могут на много снизить времязатратность проведения исследования, в случае если системный блок не ограничен техническими характеристиками (операционная система, USB порты и т.д.) [2].

В течение нескольких лет в компьютерной криминалистике доминировали два коммерческих инструмента исследований цифровых носителей информаций для выявления и обнаружения цифровых доказательств: «Forensic ToolKit (FTK)» от компании «Access Data» и «EnCase» от компании «Guidance Software». Однако со временем в сфере цифровой криминалистики появились ряд новых программных разработок, которые изменили не только архитектуру, но и методы исследования компьютерных технологий. Такие цифровые инструменты, как «Magnet Axiom», «Forensic Explorer», «Belcasoft», «X-Ways», «R-Studio» во многих ситуациях стали более продуктивными вариантами, чем «FTK» и «EnCase». У каждого цифрового инструмента есть свои сильные и слабые стороны, поэтому важно, чтобы эксперт и (или) специалист сделал осознанный выбор инструмента, который наилучшим образом поможет в обнаружении и выявлении данных имеющие значения для следствия и суда.

В настоящее время, с развитием преступлений в области компьютерных технологий, в Республике Узбекистан на базе правоохранительных органов были созданы отделы и центры цифровой криминалистики. Примечательно, что данные лаборатории оснащены более чем несколькими инструментами исследования цифровых объектов, что особенно важно для подтверждения результатов, поскольку каждый инструмент требует использования своего метода исследования. В связи с увеличением цифровых инструментов, растёт конкуренция между производителями данных программных и аппаратно-программных средств. Конкуренция приводит к тому, что у эксперта и (или) специалиста

имеется больше возможностей для работы с инструментами и с объектами в зависимости от их модификаций.

Одним из распространённых цифровых инструментов исследований цифровых объектов является программное средство «R-Studio». «R-Studio» – это полнофункциональное программное средство для восстановления данных, включающая в себя как версии для операционной системы «Windows», так и приложения, работающие в среде «macOS» и «Linux». Возможности данного инструмента ограничиваются исключительно как восстановление файлов с жёстких дисков (HDD), твёрдотельных устройств (SSD), флеш-памяти и аналогичных внешних и внутренних накопителей данных, а также снятие с них образов и клонирования [3].

Помимо функциональности, при выборе цифровых инструментов, следует учесть её стоимость, доступность, обучение, долгосрочная стабильная поддержка, а также обновление функциональных возможностей являются основными факторами, которые следует учитывать при выборе или покупке любого аппаратно-программного средства в рамках компьютерно-технической экспертизы.

Также, существуют более многофункциональные типы цифровых инструментов, которые могут не только восстанавливать данные с памяти жёстких дисков, твердотельных накопителей и т.д., а также выявлять скрытые файлы, извлекать данные об подключённом сети Интернет, история браузера, почтовые сообщения, информация о подключённых устройств и тд. Одним из таких программных средств является «Belkasoft». Особенностью данного программного обеспечения также является возможности исследования мобильных телефонов, беспилотных летательных аппаратов, электронного блока управления транспортного средства, а также исследование облачных баз данных. Программное средство «Belkasoft» позволяет выполнять глубокие проверки содержимого файлов и папок, восстанавливать ранее удалённые файлы, получать резервную копию iTunes и полную копию файловой системы из мобильных телефонов на базе «IOS», а также физическое и логическое резервное копирование для устройств с операционной системой «Android». Также, данный инструмент может изымать информацию о приватных просмотрах и очищенных историях браузера, онлайн-чаты и социальные сети, историю использования облачных сервисов и т.д. Цифровой инструмент «Belkasoft» — это комплексное решение для проведения углубленных исследований на всех типах цифровых носителей информации [4].

Со схожими возможностями данной продукции можно перечислить некоторые известные инструменты в цифровом криминалистическом мире как «Autopsy», «Hetman Partition Recovery», «Magnet Axiom», и т.д. Данные инструменты имеют схожую возможность восстановления, но разные методы обнаружения и изъятия данных с цифровых носителей

информации.

Также, отдельно хотелось бы отметить цифровой инструмент для исследования цифровых, сетевых видеорегистраторов и систем замкнутого телевидения (DVR, NVR и CCTV) «Magnet DVR Examiner». «Magnet DVR Examiner» имеет возможности обходить поставленные пароли администратором или пользователем видеорегистратора, восстанавливать записанные, но ранее удалённые видеофайлы и метаданные, а также в большинстве случаев изымать файлы из сломанных, разбитых, сгоревших и неработоспособных видеорегистраторов [5].

Вышеописанные цифровые инструменты для создания образов и анализа выявленных файлов и информаций, находящиеся в памяти исследуемых цифровых носителей информации, преимущественно упрощают проведения исследований, путём наличия собственных поисков, основанных на искусственном интеллекте (например поиск изображений с наличием оружия, нецензурных изображений и наркотических средств) и операций, которые упрощают организацию составления экспертизы или справки.

Одним из основных проблемных вопросов на сегодняшний день заключается в достоверности точности и схожести полученных результатов, проведённых на одном носителе информации, но с использованием нескольких совершенно разных цифровых инструментов. Так как, преимущественно, различные коммерческие компании выпускают свои продукты, зачастую с различными методами исследования. В связи с тем, что результаты данных инструментов не протестированы и не проверены должным образом компетентной организацией, значит, их результаты могут быть неприемлемы как в период следствия, так и в суде.

Блокираторы (устройства защиты от записи).

Блокираторы – это специальное программное или аппаратное средство, которое блокирует передачу через интерфейс на исследуемый цифровой объект всех тех команд, которые могут привести к изменению (модификации) данных, но обеспечивает прозрачный доступ к данным в режиме чтения. Блокираторы записи гарантируют, что данные не будут изменены при доступе к ним. Допуск к цифровым носителям информации без блокирующих аппаратных или программных средств может изменить сотни файлов, включая метаданные и другие атрибуты файлов, а также имеется опасность заражения вредоносными программными обеспечениями, которые могут полностью стереть данные или же наоборот загрузить в память исследуемого носителя [6].

Блокираторы записи могут быть программными или аппаратными. Программные блокираторы записи используют специальное программное обеспечение для предотвращения изменения файлов и их атрибутов. Детали работы программных блокираторов записи зависят от

используемой операционной системы. В операционных системах, работающих в реальном режиме, вроде DOS, программные блокираторы записи перехватывают прерывание BIOS 0x13, используемое для чтения и записи данных диска, отфильтровывая запросы на запись и вызывая исходный обработчик прерывания для запросов на чтение. Современные операционные системы вроде Windows и GNU/Linux используют драйверы прямого доступа для взаимодействия с накопителями, прерывание BIOS 0x13 используются загрузчиком для чтения ядра и других данных (вроде драйверов прямого доступа) только на раннем этапе загрузки. Таким образом, существуют множество путей для реализации функциональности блокировки записи [7].

В зависимости от функциональных возможностей, программные блокираторы записи могут анализировать или блокировать запросы чтения, записи, сброса кеша и другие запросы в унифицированном формате, специфичном для операционной системы. Кроме того, программный блокиратор записи может представлять накопитель операционной системе с пометкой «только чтение».

В целом, программные блокираторы записи должны перехватывать запросы или в одной точке (например, перед передачей запроса одному из многих драйверов накопителей), или во всех местах сразу (например, во всех драйверах накопителей).

Следует отметить, что программный блокиратор записи не может перекрыть все возможные пути передачи небезопасной команды накопителю.

Аппаратный блокиратор записи – это специализированное устройство, предназначенное для предотвращения случайной или преднамеренной записи данных на жесткий диск или другой носитель информации. Он создает защищенную среду для чтения данных, гарантируя, что исходные данные 0останутся неизменными.

Аппаратные блокираторы используют физическое устройство для предотвращения модификации файлов. Все аппаратные блокираторы записи могут быть разделены на две основные группы в зависимости от того, как они обрабатывают команды, полученные от хоста:

– работающие на базе белого списка;

– работающие на базе черного списка.

Аппаратный блокиратор записи работает на базе белого списка, когда он блокирует любую команду накопителю, если она не включена в список известных безопасных команд (не вносящих изменения в хранимые на накопителе данные). В этом режиме работы блокиратор записи будет блокировать все неизвестные команды, включая специфичные для производителя (например, для проведения низкоуровневой диагностики накопителя) и новые (еще не реализованные во встроенной программе

блокиратора записи). Такой блокиратор записи может блокировать новые стандартизированные безопасные команды, интерпретируя их как неизвестные.

Аппаратный блокиратор записи работает на базе черного списка, когда он блокирует команды, включенные в список известных небезопасных команд (вносящих изменения в хранимые на накопителе данные или осуществляющих иные опасные действия), и разрешает прохождение к накопителю любых других команд. В таком режиме работы блокиратор записи будет разрешать неизвестные (специфичные для производителя или новые стандартизированные) небезопасные команды накопителю.

Эксперту и (или) специалисту, в период проведения исследования цифровых объектов, понадобится несколько вариантов и типов блокираторов записи. Один аппаратный блокиратор может потребоваться для IDE и SATA-дисков, другой для USB, а третий для таких носителей, как карты памяти. Некоторые блокираторы записи имеют возможность переключаться в режим чтения/записи. Во время исследований важно понимать, как настроить функции чтения и записи, в каком конфигурационном состоянии находится блокиратор для того, чтобы блокиратор, настроенный с возможностью записи, не использовался случайно во время исследовательских работ.

Устройства для снятия образа (клонирование).

При необходимости проведения криминалистического анализа цифровых носителей информации компьютерных средств, или иных устройств, в частности используется процесс имиджирования или же называемый клонированием (снятие образа). Снятие образа (клонирование) – это процесс создания точной копии содержимого физического цифрового носителя информации на другой носитель (например, другой жесткий диск, файл образа на компьютере или сетевом хранилище). Важнейшим аспектом при снятии образа является проверка и удостоверение того, что клонированная информация является точной и идентичной к источнику. Возможность установления копии идентичности к источнику, можно с помощью хэш-алгоритмов, таких как «Message Digest 5» (MD5) или «Secure Hash Algorithm» (SHA). Хеш-алгоритм – это математическая функция, которая преобразует данные произвольной длины в уникальную строку фиксированной длины, называемую хэшем или хэш-суммой для определения и обеспечения безопасности и целостности данных [8].

В процессе создания образа цифровой носитель информации компьютерных средств или иных устройств обычно копируется побитно на чистый цифровой носитель информации. Цифровой носитель информации, на который должен быть записан образ исследуемого объекта, обычно

полностью стирается и очищается перед процессом создания клонирования. Для этого используются специальные аппаратные, программные и аппаратно-программные инструменты. После стирания данных с цифрового носителя информации, его можно проверить аналогично созданию образа. Криминалистические инструменты также дают возможность визуальной проверки носителя. Использование аппаратных устройств создания образа диска, как правило, это самый быстрый способ подготовить диск к созданию образа и выполнить процесс создания образа, совмещая с автоматической проверкой записанных данных через хэш-значения.

Использование аппаратно-программных средства для создания образов, а также проверки на исправность и для полной очистки данных исследуемых цифровых носителей информации, весьма удобны для быстрого и мобильного изъятия данных при следственных действий как осмотр, выемка и тд., так как работают независимо от компьютерных средств и не подключены к чему-либо через сетевое соединение. Данные аппаратно-программные средства представляют с собой прибор для безопасного (имеет возможности защиты от записи), быстрого и надежного (возможность перепроверки клонированных данных через несколько ХЭШ функций) переноса данных с устройств (жёстких дисков HDD, твердотельных накопителей SSD, USB флэш карт и т.д.) на экспериментальные цифровые носители эксперта и (или) специалиста, для предотвращения утери данных в случае возникновения внешнего и внутреннего повреждения в период проведения исследований, а также быстрой очистки и форматирования дисков. Перенос данных с исследуемого носителя информации происходит на равный или больший объём памяти экспериментального носителя информации эксперта.

Для извлечения данных с поврежденных носителей можно использовать специализированные устройства для обработки данных. Данные аппаратные средства работают различными методами, включая использование различных типов алгоритмов чтения и аппаратных адаптаций. Один из устройств данного типа является «Atola Insight». Данное устройство изменяет способ взаимодействия компьютера с диском, предотвращая отказ и завершение чтения. Вместо этого устройство «Insight» продолжает пытаться восстановить данные с устройства, используя альтернативные алгоритмы и методы. В обычном компьютере процесс чтения завершится неудачей, если произойдет падение головки, но с использованием специализированных аппаратных средств возникает возможность чтения всех областей памяти, вместо того чтобы просто выдать отказ чтения для всего диска сбоем головки [9].

Создание образа может занимать достаточно значительное время. В зависимости от скорости дисков, проверки и используемого метода.

Приблизительный показатель клонирования составляет 100 ГБ в час. Это может означать, что создание образа диска емкостью один терабайт займет около 10 часов (в случае если секторы памяти не повреждены или отсутствуют другие тормозящие процесс действия). При подключении нескольких цифровых носителей информации количество затраченного времени, увеличиваются в разы.

Предварительный просмотр цифрового носителя информации – это процесс быстрого и поверхностного анализа содержимого носителя с целью получения общего представление о его структуре и данных, которые он содержит. Данный способ позволит установить необходимость создания образа, а также выполнять следующие некоторые функции:

– определение типа носителя (идентификация файловой системы, структуры каталогов и типов файлов);

– оценка состояния носителя (определение наличия повреждений, вирусов или других проблем, которые могут повлиять на дальнейшую работу с данными);

– поиск ключевых данных (быстрое обнаружение необходимых файлов или папок, например, системных файлов, пользовательских данных или документов);

– планирование дальнейших действий (на основе результатов предварительного просмотра можно составить план более детального анализа или восстановления данных).

Одним из современных и специализированных устройств, разработанное для быстрого и надежного создания точных копий данных с различных цифровых носителей, а также имеет функции предварительного просмотра, блокирования, оценки состояния цифрового носителя и т.д. является программно-аппаратное устройство «Tableau TX1» компании «Open Text Corporation» [10].

Дополнительные инструменты.

На персональных компьютерах пользователями часто устанавливаются пароли для предотвращения несанкционированного доступа к программным средствам и информации на устройстве, а в современных операционных системах установление пароля является обязательным. Технически доступ к данным возможен, но они находятся в нечитаемом формате. При установлении пароля, происходит шифрование данных. Для шифрования данных используются алгоритмы, а для того, чтобы сделать их читаемыми, необходимо применить обратный процесс. К сожалению, преступники также используют шифрование для сокрытия своей преступной деятельности. В связи с этим, пароли и шифрование является повседневной задачей для экспертов цифровой криминалистики.

Существует множество инструментов для работы с паролями. Некоторые из них позволяют сбросить пароли «Microsoft Windows». Другие

пытаются подобрать пароль, используя такие методы атаки, как словарь и метод «brute force». Средства шифрования, такие как «Veracrypt», блокируют секторы, разделы или сами диски паролем. После ввода пароля содержимое становится доступным в незашифрованном виде. Атаки по словарю используют слова или комбинации слов для подбора пароля. Словари, используемые в атаках, могут включать в себя обычные словари различных языков. Также могут быть специализированные словари аббревиатур или сленга. Атака методом «brute force» генерирует комбинации букв, цифр и специальных символов в попытке подобрать пароль. Некоторые инструменты позволяют эксперту/специалисту загружать в программу известные аспекты пароля, чтобы сократить процесс его взлома.

Дополнительным механизмом расшифровки и подбора паролей является использование радужных таблиц. Пароли часто хранятся не в виде обычного текста, а в хэшированном формате. Инструменту дешифрования необходимо хэшировать слова в словаре, а затем использовать хэши в атаке на пароль. Радужные таблицы упрощают этот процесс за счет хэширования словаря. Эффективность повышается, поскольку инструменту расшифровки не нужно хэшировать словарь во время атаки.

Чем сложнее пароль, тем больше времени потребуется для его угадывания. В зависимости от используемых технологий на взлом восьмисимвольных паролей, содержащих цифры, буквы и специальные символы, могут уйти месяцы или годы. Для ускорения атаки можно использовать специализированные компьютеры для дешифровки. Графический процессор видеокарты может быть на порядки быстрее для расшифровки, чем оперативная память компьютера. Игровые компьютеры могут быть оснащены несколькими параллельными высокоскоростными видеокартами, что значительно увеличивает возможности расшифровки.

Ручные инструменты.

Эксперту и(или) специалисту необходимы широкий набор инструментов, включая отвертки, торцевые головки, шестигранные ключи, устройства заземления, присоски, фонарь, изолента, стяжки, бечевки, ножницы, плоскогубцы, кусачки, бритвенные лезвии, этикетки, камера, пакеты Фарадея, сумки/кейсы для хранения, увеличительное стекло, удлинитель, различные кабели и разъемы, карандаш, бумага, перманентный маркер, латексные перчатки и т.д. Набор отверток должны иметь стандартные, шестигранные, торцевые, звездообразными, треугольные и иные виды головок. В некоторых игровых системах используются трехгранные винты.

Следует также учитывать тот факт, что намагниченные отвертки могут повредить данные на жестком диске и нанести вред другим компонентам компьютера. Размеры отверток должны варьироваться от

микро до стандартных. Присоски пригодятся для снятия и замены компонентов монитора при извлечении диска из iMac или же снятие корпуса иных устройств. Фонарь используется в условиях недостаточной освещенности, например, при работе под столами или в шкафах. Использование налобного фонаря весьма практичен на практике так как не требует использование рук при проведении исследования. Также рекомендуется иметь тканевые заплатки различных размеров для упаковки и транспортировки компьютерных средств и иных устройств. Рекомендуется иметь удлинитель на длинном шнуре, канцелярские принадлежности для заметок, а также для составления схемы комнаты или места, где находятся компьютерные средства и периферийное оборудование, а также цифровые носители информации для мобильного изъятия первоначальной информации и данных из исследуемых объектов. Пакеты Фарадея – это специальный контейнер, изготовленный из материалов, которые блокируют электромагнитные поля и широко применяются для защиты от электронного слежения и удалённого управления, а также от помех, создаваемых электромагнитными полями [11].

Инструменты мобильной криминалистики.

Мобильная криминалистика – это раздел цифровой криминалистики, специализирующийся на исследовании мобильных устройств (смартфонов, планшетов и т.д.) с целью извлечения и анализа цифровых доказательств.

К мобильной криминалистике относятся сотовые телефоны, планшеты, GPS-устройства, а также MP3-плееры (например iPod). Как и в компьютерной криминалистике, в этой категории существует множество продуктов с открытым исходным кодом и продуктов от разных производителей. Некоторые производители цифровых криминалистических инструментов интегрировали поддержку мобильных устройств в свои продукты для компьютерной криминалистики, но уровень поддержки устройств, как правило, отстает от некоторых ведущих производителей мобильных криминалистических инструментов. «Magnet Axiom» – это одна из ведущих платформ для цифровой криминалистики, разработанная компанией Magnet Forensics. Этот комплексный инструмент предназначен для сбора, анализа и визуализации данных с различных цифровых устройств, включая компьютеры, мобильные устройства, облачные хранилища и другие носители информации [12].

К коммерческим продуктам, поддерживающим широкий спектр мобильных устройств, относятся продукты «Cellebrite», «Micro Systemation» и «Oxygen». Данные продукты широко используются правоохранительными органами, государственными учреждениями и корпорациями по всему миру, в том числе и в Республике Узбекистан.

«Cellebrite» – это израильская компания, которая специализируется

на разработке программного обеспечения и оборудования для цифровой криминалистики для извлечения и анализа данных с мобильных устройств. Основными продуктами «Cellebrite» на сегодняшний день являются программные обеспечения «Cellebrite UFED (Universal Forensic Extraction Device)» (это серия продуктов, которые позволяют извлекать и анализировать данные с широкого спектра мобильных устройств), «Cellebrite Physical Analyzer» (данный инструмент позволяет анализировать содержимое мобильных устройств, включая смартфоны, планшеты и другие портативные гаджеты, как и логические, так и физические данные), «Cellebrite Cloud Analyzer» (данный инструмент позволяет анализировать данные, хранящиеся в облачных сервисах, связанных с устройством), «Cellebrite Reader» (этот инструмент позволяет просматривать и анализировать извлеченные данные без необходимости установки полного программного обеспечения), «Cellebrite Guardian» (это облачное решение, разработанное компанией Cellebrite, для эффективного управления, совместного использования и анализа цифровых доказательств, полученных в результате проведения цифровых экспертиз) [13].

«Micro Systemation» – это шведская компания, являющаяся одним из мировых лидеров в области разработка программного обеспечения и оборудования для извлечения и анализа данных с мобильных устройств. Основными продукты «Micro Systemation» являются программное средство «XRY» (программное обеспечение MSAB для извлечения данных с мобильных устройств), «XAMN» (предназначен для анализа данных, извлеченных с помощью XRY), «XEC» (предназначен для управления и организации цифровых доказательств, полученных с помощью XRY и XAMN) [14].

«Oxygen Forensics, Inc» – это ведущий мировой поставщик программного обеспечения для цифровой криминалистики, которая разрабатывает передовые инструменты извлечения и анализа данных с различных цифровых устройств и платформ. Ключевыми продуктами «Oxygen Forensics» являются программные обеспечения «Oxygen Forensic Detective» (позволяет извлекать и анализировать данные с мобильных устройств, включая смартфоны, планшеты и другие гаджеты), «Oxygen Forensic Cloud Examiner» (продукт предназначен для анализа данных, хранящихся в облачных сервисах, таких как Google Drive, Dropbox и iCloud), «Oxygen Forensic Drone Examiner» (продукт позволяет извлекать и анализировать данные с дронов, включая видеозаписи, фотографии и данные передвижения), «Oxygen Forensic IoT Examiner» (продукт предназначен для анализа данных с устройств Интернета вещей (IoT), таких как умные дома, умные города и промышленные датчики), «Oxygen Forensic Examiner» (универсальный продукт, который позволяет извлекать

и анализировать данные с различных типов цифровых устройств, включая компьютеры, ноутбуки, флэш-накопители и жесткие диски) [15].

Также, современные цифровые инструменты мобильной криминалистики часто включают в комплект помимо программного обеспечения, набор большого количества кабелей, адаптеров и т.д. для подключения к различным типам и моделям устройств. Наличие нескольких вариантов кабелей подключения в мобильной криминалистики имеет важную роль при проведении исследования, поскольку уровень поддержки каждого устройства может значительно отличаться, в том числе логическое извлечение, физическое извлечение и извлечение из файловой системы могут требовать совершенно разные методы с использованием различных адаптеров, особенно, если это касается восстановления удаленных файлов.

Требующей внимания особенностью продуктов мобильной криминалистики является то, что программные обеспечения могут иметь разные версии в зависимости от регионального базирования, то есть для каждого региона или определённого государства, возможности продуктов могут меняться.

Как правило, инструменты мобильной криминалистики, а именно программные обеспечения, обеспечивающие как логическое, так и физическое извлечение, поддерживают больше устройств на логическом уровне, чем на физическом. Также обычно физическое извлечение обеспечивает большую часть того, что обеспечивает логическое извлечение. Поэтому возможности физического извлечения потенциально наиболее ценны, но физическое извлечение обычно поддерживается не на таком большом количестве устройств, как логическое извлечение. Извлечение файловой системы может быть особенно полезным для восстановления удаленных артефактов. Различие методов извлечения данных, включая возможность извлечения удалённых файлов с помощью программного обеспечения зависит не только от версии и модели инструмента, но также и от модели мобильного телефона, версии операционной системы, версия защиты и последнее обновление.

Инструменты мобильной криминалистики обычно стоят дороже, чем инструменты компьютерной криминалистики. Годовое обслуживание некоторых продуктов для мобильной криминалистики может составлять несколько десяток тысяч долларов за лицензию. Поддержка продукта включает в себя частоту обновлений, количество новых функций и поддержку устройств, которые обычно появляются с каждым обновлением, а также своевременное реагирование и решение вопросов, связанных с поддержкой.

Стабильность поставщика и стабильность продукта (в данном случае инструмента) – это две совершенно разные составляющие. Некоторые

компании могут быть стабильными, но их продукты могут иметь ошибки и иные программные погрешности. Длительность пребывания на рынке не всегда является ключевым показателем поставщика или продукта, поскольку некоторые из новых поставщиков имеют более современные и актуальные цифровые инструменты, а некоторые из старых поставщиков имеют менее стабильные приложения.

Возможности извлечения – это, пожалуй, самая важная переменная при использовании цифровых инструментов мобильной криминалистики. Два инструмента, заявляющие о поддержке конкретного устройства на логическом или физическом уровне, могут дать разные результаты, поскольку один из них может извлечь гораздо больше информации, чем другой. Один инструмент может извлечь из устройства 500 текстовых сообщений, в то время как другой – 600. Различия в восстановлении информации, особенно удаленной, могут сильно отличаться в разных инструментах мобильной криминалистики. Очень часто при проведении судебной экспертизы мобильных устройств используется несколько инструментов, чтобы получить как можно более полное и детальное заключение об исследованном объекте.

Визуальный анализ.

Поиск и извлечение файлов, данных и информации – это лишь часть задач, стоящих перед экспертом или специалистом. Одной из важнейшей деятельностью в период проведения исследования является также визуальный анализ, и интерпретация информации. Визуальный анализ включает в себя изучение информации данных и сортирование по видам и типам материалов. Во многих криминалистических инструментах есть автоматические инструменты анализа для сортировки информации и поиска закономерностей, и других характеристик, которые помогут создать одну доказательственную базу, в рамках исследования.

Цифровая криминалистика, являясь современной и развивающейся разделом криминалистики, занимающаяся обнаружением, изъятием, анализом цифровых доказательств, требует модернизированных и многофункциональных наборов цифровых инструментов. Формирование и поддержание высоких навыков в области цифровой криминалистики достаточно сложная задача для специалиста и эксперта. В особенности в сфере исследований компьютерных преступлений. В связи с этим, умение пользоваться различными инструментами цифровой криминалистики, позволяет специалисту и (или) эксперту наилучшим образом справляться с вызовами современного преступного мира.

Библиографические ссылки:

1. Смолина А.Р. Методическое и алгоритмическое обеспечение производства компьютерно-технической экспертизы. // Дисс. на

соискание учёной степени к.ю.н., Томск 2017 г. С.19; (Smolina A.R. Methodological and algorithmic support for the production of computer-technical expertise. // Diss. for the degree of candidate of jurisprudence, Tomsk 2017, p.19);

2. Способы получения доказательств и информации в связи с обнаружением (возможностью обнаружения) электронных носителей: учеб. пособие / под ред. Б.Я. Гаврилова М.: Проспект, 2017.

3. https://www.r-studio.com/ru/

4. https://belkasoft.com/

5. https://www.magnetforensics.com/products/magnet-dvr-examiner/

6. Савельев В. А. Методы получения и сохранения информации в ходе расследования преступлений: учеб. пособие / В. А. Савельев. - Краснодар: КубГАУ, 2016.

7. https://habr.com/ru/companies/bizone/articles/320032/

8. Мебония М.А. Федорова О.В. Сравнительное исследование хэш-алгоритмов в криптографии// Международный научный журнал «вестник науки» № 12 (57) Т.3 2022

9. https://www.opentext.com/products/tableau-tx1-forensic-imager

10. https://www.mediaduplicationsystems.com/atola-insight-forensic-hard-drive-duplicator?srsltid=AfmBOoq2xBKhJopHBpAnaBhQZ6Cj7HBVgkoyOpfhTXQNAYqUKm2i4TPq

11. Иван Тренисов, Александр Вотинцев. Антистатическая упаковка и транспортировка // Компоненты и технологии • № 12 '2011.

12. https://www.magnetforensics.com/

13. https://cellebrite.com/en/home/

14. https://www.msab.com/

15. https://oxygenforensics.com/