изображениях запечатлены разные люди, либо данное различие может быть объяснено внесением изменений в изображение того или иного признака (изменение формы, размера, монтаж (перенос элемента внешности с изображения другого лица)).

Комплексные исследование могут встречаться при исследовании внешности людей негроидного, монголоидного антропологического типа, где для оценки идентификационной значимости признаков необходимы знания антропологии.

Таким образом, следует отметить, что содержательная основа экспертных знаний все более усложняется и в связи с этим возникает потребность в профессиональной переориентации судебного эксперта на использование комплекса специальных знаний, достаточного для решения экспертных задач. Инициаторам назначения судебных портретных экспертиз также необходимо ориентироваться в специфичности объектов портретной экспертизы и при необходимости использования специальных знаний в других видах судебных экспертиз назначать комплексные экспертизы либо комплексы экспертиз для решения основной задачи портретной экспертизы – установления тождества (отсутствия тождества) запечатленных на изображении людей.

УДК 343.98

И.И. Лузгин

КОНТР-ФОРЕНЗИКА КАК ТЕХНОЛОГИЯ ПРОТИВОДЕЙСТВИЯ РАССЛЕДОВАНИЮ ПРЕСТУПЛЕНИЙ

Цифровая криминалистика (форензика, англ. digital forensics) – прикладная наука о раскрытии и расследовании преступлений, связанных с компьютерной информацией, методах получения и исследования доказательств, имеющих форму компьютерной информации (цифровых доказательств), применяемых для этого технологических средствах.

Российский ученый Н.Н. Федотов определяет следующие задачи форензики: разработка тактики оперативно-розыскных мероприятий и следственных действий, связанных с компьютерной информацией; создание методов, аппаратных и программных инструментов для сбора и исследования доказательств компьютерных преступлений; установление криминалистических характеристик правонарушений, связанных с компьютерной информацией.

Контр-форензика (англ. anti-forensics) – противодействие методам поиска, обнаружения и закрепления цифровых доказательств. К техническим средствам контр-форензики относятся: программы и аппаратно-программные устройства для шифрования хранимой информации; программы и аппаратно-программные устройства для шифрования трафика; программы для очистки дисков и других носителей; устройства для механического уничтожения информации на магнитных носителях; программы для сокрытия присутствия информации на диске (манипуляция с атрибутами файлов, запись в нестандартные места, стеганография); системы и сервисы для анонимизации сетевой активности; программы и аппаратно-программные средства для затруднения копирования произведений, представленных в цифровой форме, затруднения исследования исполняемого кода и алгоритмов программ.

Технологии цифровой криминалистики, как и методы и цифровые технологии контр-форензики, могут применяться в различных сферах человеческой деятельности. При этом главной задачей последней является противодействие методам и технологическим средствам в цифровой криминалистике.

Основные сферы применения технологий контр-форензики включают в себя защиту приватности; защиту интеллектуальной собственности; обеспечение сохранности и секретности документов; противодействие шпионажу; сокрытие цифровых следов (как правило, с целью ухода от ответственности за противоправные деяния).

Выделяют следующие цели применения технологий контр-форензики в противоправной деятельности: предотвращение извлечения или оставления цифровой информации о совершении противоправного деяния; создание помех в процессе сбора криминалистически значимой цифровой информации; увеличение временных затрат на криминалистическое исследование; способствование возникновению сомнений по поводу допустимости полученных доказательств; выведение из строя криминалистического оборудования; сокрытие следов использования оборудования для контр-форензики.

В зависимости от способа воздействия и сферы применения методы контр-форензики могут быть классифицированы по соответствующим категориям: сокрытие или уничтожение данных; блокировка или уничтожение источника данных; подделка информации, противодействие инструменту и программному обеспечению проведения цифрового криминалистического исследования.

Техника, которая имеет целью уничтожение данных, получила название Artifact wiping. Есть несколько путей осуществления: использование специальных программ (BC Wipe, Eraser, PGP Wipe) – эти программы уничтожают данные и не позволяют извлечь их после удаления; перезапись удаленных данных в неиспользованном разделе жесткого диска (поскольку удаленные данные вовсе не исчезают, а передислоцируются в неиспользуемое пространство на жестком диске, то они могут быть в итоге заменены на другие или перезаписаны).

К недостаткам данного метода относится то, что после использования программ для удаления данных остаются цифровые следы, которые свидетельствуют об использовании в системе подобных программ (т. е. можно доподлинно установить, что информация умышленно стиралась).

Существует несколько путей сокрытия информации в системе: перемещение информации, придание информации свойства «невидимости», изменение расширения файлов и др.

Перемещение информации – дислокация данных в раздел, который с высокой долей вероятности не будет исследован. Другой способ перемещения данных заключается в их загрузке на съемный носитель. К недостаткам данной техники относится то, что остаются цифровые следы при подключении съемных девайсов (система автоматически обновляет записи, доступные для последующего изучения – system logs).

Придание информации свойства «невидимости» успешно достигается с помощью стеганографии (один из способов). В данном случае объект, который должен быть сокрыт, помещается в другой объект, где и хранится (например, цифровое доказательство любого вида может быть сокрыто в файле с расширением .jpg или .mp3). Пример программы для стеганографии – Steghide (как и многие другие, она находится в открытом доступе).

Изменение расширения файлов полагается на установку оперативной системы Windows, согласно которой она идентифицирует файлы в соответствии с их расширением (и не открывает их, если расширение не совпадает с установкой программы, с помощью которой их нужно открыть). С целью преодоления данной техники рекомендуется проводить подробный анализ файлов системы на соответствие указанного расширения файловому виду.

Блокировка или уничтожение источника данных особо актуальны для мобильных девайсов и планшетов, так как возможно дистанционно заблокировать, отключить или стереть криминалистически значимую цифровую информацию. Как правило, при работе с такими аппаратами необходимо изолировать девайс от радиомагнитных волн посредством помещения его в радионепрозрачный контейнер до последующего изучения (так называемый Faraday container).

Существуют следующие основные разновидности подделки информации: дефрагментация, изменение метаданных. Наиболее эффективным является изменение метаданных («данные о данных» – такие как время создания файла, дата, параметры и др.). Для этого применяются следующие программы: File Touch, Metasploit Timestomp и др. Дефрагментация реструктурирует данные на жестком диске, что затрудняет действия изучающего их исследователя.

Противодействие инструменту и программному обеспечению проведения криминалистического исследования включает в себя вредоносные программы и имеет целью повреждение оборудования или сбой его работы во время исследования и, как результат, является наиболее опасной и нежелательной для исследователя.

Все вышеуказанные техники создают значительные помехи в расследовании преступлений в сфере цифровой криминалистики. Многие программы находятся в открытом доступе и могут быть использованы практически любым человеком (в противовес криминалистическому оборудованию, рыночная цена которого не только высока, но и поставляется такое оборудование лишь профильным госструктурам).

Наиболее благоприятным подходом к работе в таких условиях являются следующие пути развития:

целенаправленная подготовка и государственная сертификация специалистов и экспертов в сфере цифровой криминалистики (с обязательным разделением на разделы по признакам: компьютеры, смартфоны, а также серверные технологии);

тщательное тестирование и выявление проблемных аспектов находящегося в инвентаре исследователя криминалистического оборудования с последующим устранением данных проблем, что позволит минимизировать риск разработки программного обеспечения для использования недостатков этого оборудования;

разработка криминалистического программного обеспечения и оборудования для исследования в сфере цифровой криминалистки с учетом методов и программного обеспечения, применяемого в контр-форензике, а также актуального состояния базы данных вирусов.

УДК 343.983.22

А.Н. Матлак

ПРИЧИНЫ ВЫСТРЕЛА ИЗ ОГНЕСТРЕЛЬНОГО ОРУЖИЯ БЕЗ НАЖАТИЯ НА СПУСКОВОЙ КРЮЧОК

Возможность производства выстрелов без воздействия на детали спускового механизма – одно из обстоятельств происшествий, сопряженных с использованием и применением огнестрельного оружия, которое нередко становится предметом исследования экспертов-баллистов. Необходимость в установлении возможности выстрела из оружия без нажатия на спусковой крючок возникает при производстве по материалам и уголовным делам об убийствах, умышленном причинении тяжких телесных повреждений, разбоях и хулиганствах, совершенных с использованием огнестрельного оружия, террористических действиях, причинении смерти по неосторожности, получении травм в результате неосторожного обращения с огнестрельным оружием (в том числе сотрудниками правоохранительных органов) и т. д.

На современном этапе развития судебной баллистики учеными принято считать, что возможность выстрела без нажатия на спусковой крючок может быть обусловлена неисправностью оружия, конструктивными особенностями оружия, используемыми боеприпасами. Согласно другому подходу к классификации причин выстрела без нажатия на спусковой крючок помимо указанных выше групп отдельный блок причин составляет определенное состояние отдельных деталей, узлов и механизмов огнестрельного оружия – коррозия, загрязнение; деталей ударно-спускового механизма; неисправная регулировка отдельных деталей; использование нестандартных деталей-заменителей.

Наиболее полной классификации причин, по которым возможно производство выстрела без нажатия на спусковой крючок, по нашему мнению, можно достичь, объединив их в группы в зависимости от их отношения к огнестрельному оружию: причины, обусловленные конструктивными особенностями, техническим состоянием деталей и узлов огнестрельного оружия; причины эксплуатационного характера; причины, связанные с использовавшимися для стрельбы боеприпасами.

К причинам, обусловленным конструктивными особенностями, техническим состоянием деталей и узлов огнестрельного оружия, можно отнести такие конструктивные решения различных моделей огнестрельного оружия, при которых даже в случае исправного состояния узлов и деталей и их корректного взаимодействия при определенных нарушениях правил обращения с оружием возможен выстрел без нажатия на спусковой крючок. Известны случаи выстрела без нажатия на спусковой крючок из 7,62-мм пистолета-пулемета Шпагина с полностью исправными деталями. Подобные явления становятся возмож-