МЕТОДЫ ЦИФРОВОЙ КРИМИНАЛИСТИКИ И КОМПЬЮТЕРНОЙ ФОРЕНЗИКИ ДЛЯ РАССЛЕДОВАНИЯ ИНЦИДЕНТОВ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ - ОБЗОР

Шевченко Д.Н.

Шевченко Дмитрий Николаевич – магистр,
кафедра защищённых систем связи, факультет инфокоммуникационных сетей и систем,
Санкт-Петербургский государственный университет телекоммуникаций им. М.А. Бонч-Бруевича,
г. Санкт-Петербург

Аннотация: *цифровая криминалистика определяется как процесс сохранения, идентификации, извлечения и документирования компьютерных доказательств, которые могут быть использованы в суде или в расследованиях внутренних инцидентов информационной безопасности внутри компаний. Цифровая криминалистика и компьютерная форензика помогают командам криминалистов и специалистов информационной безопасности анализировать, проверять, идентифицировать и сохранять цифровые доказательства, находящиеся на различных типах электронных устройств.*
Ключевые слова: *цифровая криминалистика, компьютерная форензика, информационная безопасность.*

I. Введение

Цифровая криминалистика включает в себя множество областей. Проведём краткий обзор основных разделов.

Компьютерная форензика — сюда можно отнести всё, что связано с поиском следов и причин возникновения инцидента информационной безопасности на локальных машинах под управлением операционных систем Windows или Linux.

Сетевая форензика – отрасль, в которой объектами расследований становится дамп сетевого трафика между хостами. Главной задачей сетевой форензики является контроль и анализ трафика компьютерной сети, необходимый для обнаружения вторжения и сбора доказательств. Перехваченный трафик может сохраняться для последующего анализа и использоваться как часть комплексного расследования или быть полноценным отдельным расследованием.

Форензика мобильных устройств – объектами расследований в данном случае являются смартфоны, под управлением операционных систем Android или iOS.

Основное отличие от компьютерной форензики заключается в наличии таких данных как журнал вызовов, данные биллинга оператора, журнал SMS, история подключений к разным публичным Wi-Fi сетям и история геопозиции смартфона.

II. Компьютерная форензика.

Компьютерная форензика — основной и самый объёмный раздел цифровой криминалистики. Объясняется это широким распространением объектов работы - которыми являются корпоративные АРМ (автоматизированное рабочее место), корпоративные ноутбуки, подключенные к DMZ (англ. Demilitarized Zone — демилитаризованная зона) или ПК пользователей. Расследования в данном случае сводятся к поиску артефактов (следов) взлома или нарушения политик безопасности на локальной машине.

Основные методики расследований:

1) *Анализ RAM (Random Access Memory)*

Данный метод подразумевает под собой создание криминалистом слепка оперативной памяти, сохранение его в файл и дальнейшее изучение. Метод актуален в случае возможности быстрого реагирования Security Operation Center на выявление нового инцидента. В такой ситуации, дежурный специалист ИБ может оперативно получить физический доступ к локальной машине до его перезагрузки или выключения. Снять дамп (слепок) оперативной памяти, сохранить его в файл и использовать для дальнейшего расследования. Во время снятия образа оперативной памяти специалисту по форензике необходимо учитывать, что некоторое вредоносное ПО может защищаться от снятия слепков своего содержимого из RAM, если софт для создания образа запущен в обычном пользовательском режиме.

Подобное ПО имеет активные системы противодействия отладке, способные прервать попытки других программ считать данные из защищенных областей памяти. В данной ситуации есть вероятность получить битый образ оперативной памяти (файл образа памяти будет содержать только нули или случайные данные). Также есть вероятность получить ребут локальной машины, делающий дальнейшее исследование данным методом невозможным (т.к. оперативная память будет очищена).

Для обхода данного ограничения специалисту необходимо использовать специализированные программы и инструменты — например Belkasoft Live RAM Capturer. Данный софт может работать в привилегированном режиме ядра операционной системы. Специализированные программы включают

32- и 64-разрядные драйверы, работающие в режиме ядра и позволяющие корректно обрабатывать области данных, принадлежащие защищенным процессам.

2) *Анализ содержимого жёстких дисков (HDD).*

Данный метод является самым популярным в ходе расследования внутренних инцидентов информационной безопасности. Метод заключается в создании побитовой копии образа жёсткого диска и дальнейшего анализа его содержимого. В процессе создания дампа жёсткого диска специалисту цифровой криминалистики важно не оставить следов своего вмешательства, иначе в случае судебных разбирательств сторона защиты может использовать данное изменение, как аргумент в свою сторону. Для копирования образа твердотельного носителя может использоваться как специализированное ПО с загрузочного флэш-носителя (например, The Forensic Toolkit Imager (FTK Imager)), так и отдельные аппаратные комплексы (например, Atola Insight или Tableau Forensic Imager). В случае использования программных решений софт записывает свои действия в специальный файл логов, в котором уточняется время копирования выбранных директорий, записываются контрольные суммы файлов, а также указываются заводские номера накопителей информации. В случае использования аппаратных решений проблемы невмешательства решается другим путём – побитовое копирование файлов возможно при аппаратной блокировке записи на носителе.

Заключение

Методы компьютерной криминалистики могут обеспечить полноценное расследование инцидентов информационной безопасности Правильный подход и использование необходимых методов цифровой криминалистики в соответствии с требованиями к каждому инциденту обеспечит сбор необходимых цифровых доказательств. Также позволит определить слабые места в корпоративной сети, провести полноценные превентивные меры. Также в ходе расследований необходимо помнить о проблеме невмешательства в данные носителей и предпринимать необходимые меры для каждого из методов.

Список литературы

1. *Федотов Н.Н.* Форензика - компьютерная криминалистика. М., 2007.