ТЕМА 5
КОМПЬЮТЕРНАЯ ИНФОРМАЦИЯ: ОБНАРУЖЕНИЕ И АНАЛИЗ

ПРАКТИЧЕСКОЕ ЗАНЯТИЕ 5.6

1. Изучение структуры и содержания логических и физических образов, извлеченных из исследуемых мобильных устройств.
2. Криминалистический анализ информации, извлеченной из мобильных устройств (на примере программно-технического комплекса «Мобильный криминалист»).

Краткие теоретические сведения:

Мобильный Криминалист Эксперт – многофункциональный инструмент для высокоскоростной и эффективной работы с данными из мобильных устройств, дронов, облачных сервисов и ПК, сочетающий в себе все возможности ПО «МК Детектив» и новый уникальный функционал.

Основной функционал программы:

Мобильные гаджеты и мультимедийные устройства:

- Создает физические образы устройств Android, Kai и др.
- Создает логические образы устройств iOS, Android, Blackberry, Windows Phone, Symbian и др.
- Извлекает и расшифровывает все данные, в том числе удаленные.
- Импортирует физические образы и резервные копии множества устройств.
- Получает данные из дронов и выстраивает маршруты полетов.

Облачные сервисы:

- Позволяет авторизоваться в учетной записи и пройти 2FA.
- Извлекает информацию из нескольких десятков облачных хранилищ: Apple, Google, Yandex, iCloud, WhatsApp, Viber, Telegram и др.
- Расшифровывает резервные копии.

Персональные компьютеры:

- Извлекает переписку, медиафайлы и контакты из мессенджеров Viber, Unigram, Skype, Wickr Me.
- Получает письма и контакты из почтовых агентов Mozilla Thunderbird, Microsoft Outlook, Microsoft Mail.
- Извлекает данные из веб-браузеров Google Chrome, Mozilla FireFox, Opera, Microsoft Edge, Internet Explorer.
- Получает информацию о системе.

Аналитические инструменты:

- Анализирует данные одновременно из нескольких устройств в одном деле.
- Собирает все звонки, а также сообщения из устройства, в том числе из мессенджеров в разделы «Звонки» и «Сообщения».
- Объединяет контакты по индивидуальным настройкам.
- Исследует коммуникации между несколькими устройствами.

- Производит высокоскоростной поиск как внутри дела, так и внутри отдельно взятого документа.

ЗАДАЧА

Сидоров Дмитрий Викторович, 09.07.1990 года рождения, в период с декабря 2015 г. по апрель текущего года, находясь на территории Республики Беларусь, в том числе по месту своего жительства по адресу: г. Минск, ул. Одоевского, 126-24, действуя группой лиц по предварительному сговору с Демешко С.П., с использованием компьютерной техники, глобальной компьютерной сети интернет, заранее приобретенных у неустановленных лиц реквизитов доступа к счетам в платежной системе «Пэйпал» («Paypal») и электронным почтовым ящикам держателей данных счетов, осуществил изменение информации, хранящейся в компьютерных системах электронных почтовых сервисов comcast.net, charter.net, rr.com, hotmail.com, cox.net и иных, а именно: изменил настройки работы не менее чем 152 электронных почтовых ящиков держателей вышеуказанных счетов в результате чего их входящая корреспонденция дублировалась на подконтрольный им электронный почтовый ящик -990vozduh1999@gmail.com.

Также имеется информация о причастности фигуранта к незаконному обороту наркотиков, сбыту фальшивых денег, сбыту огнестрельного оружия.

В ходе проведения оперативно-розыскных мероприятий и следственных действий с помощью программного обеспечения «Мобильный криминалист» была получена информация из мобильных устройств фигуранта.

ЗАДАНИЕ

1. Проанализировать полученную информацию из средств компьютерной техники.
2. Выделить сведения, представляющие интерес.
3. Составить аналитическую матрицу.

Решение практических задач:

1. После доведения задачи, обучающиеся создают файл с именем «№ группы_Фамилия_матрица.XLS» (или используют созданный на предыдущем занятии).

Данный файл будет использоваться для фиксации и анализа сведений, представляющих интерес, а также оценки работы обучающихся.

В таблице необходимо создать столбцы:

«Вид СКТ»,

«Сведения»,

«Пароли»,

Контакты (представляющие интерес),

«Посещаемые ресурсы» (представляющие интерес),

«Оперинтерес» (иная информация, представляющая интерес),

«Примечание»

и иные по усмотрению обучающегося.

2. После доведения задачи, обучающиеся открывают на своих ПК файл с именем «Выгрузка Lenovo физ». Данный файл, содержит информацию для анализа.

3. Обучающиеся самостоятельно под руководством преподавателя составляют аналитическую матрицу исходя из имеющейся информации.

Рекомендуется более внимательно анализировать следующие сведения:

контакты;

сообщения;

мультимедийные файлы;

геоданные;

календарь;

пароли;

установленное программное обеспечение и др.

4. По усмотрению преподавателя возможно заполнение полей матрицы в форме «вопрос – ответ». Если следует правильный ответ от обучающегося, то вся подгруппа действует согласно его рекомендациям. Если правильного ответа не последовало, то на вопрос отвечает преподаватель и руководит дальнейшей работой обучающихся.