ТЕМА 5
КОМПЬЮТЕРНАЯ ИНФОРМАЦИЯ: ОБНАРУЖЕНИЕ И АНАЛИЗ

ПРАКТИЧЕСКОЕ ЗАНЯТИЕ 5.5

1. Изучение структуры и содержания криминалистически важной информации, извлеченной из исследуемых СКТ.
2. Криминалистический анализ информации, извлеченной из исследуемых СКТ (на примере программно-технического комплекса «Мобильный криминалист»).

Краткие теоретические сведения:

Мобильный криминалист является многофункциональным инструментом для высокоскоростной и эффективной работы с данными из мобильных устройств, дронов, облачных сервисов.

Мобильные гаджеты и мультимедийные устройства создают физические образы устройств Android, Kai, создает логические образы устройств iOS, Android, Blackberry, Windows Phone, Symbian, извлекать и расшифровывать все данные, в том числе удаленные, импортировать физические образы и резервные копии множества устройств, получать данные из дронов и выстраивать маршруты полетов.

Облачные сервисы: позволяют авторизоваться в учетной записи и пройти 2FA, извлекать информацию из нескольких десятков облачных хранилищ: Apple, Google, Yandex, iCloud, WhatsApp, Viber, Telegram, расшифровывать резервные копии.

«МК Десктоп» — это высокоскоростной, портативный, многофункциональный инструмент, позволяющий извлекать, расшифровывать и анализировать ключевые данные из персональных компьютеров, ноутбуков и серверов на операционных системах Windows, macOS, GNU/Linux.

Мобильный Криминалист Скаут – это модуль программы «Мобильный Криминалист». Скаут – полноценный инструмент компьютерной форензики. Он позволяет находить и извлекать такую важную информацию из исследуемого персонального компьютера, как:

1. **учетные записи и токены, закладки, данные форм автозаполнения, историю посещений и файлы куки** из интернет-браузеров Google Chrome, Mozilla Firefox, Opera, Microsoft Edge, Internet Explorer;
2. **учетные данные и токены** из программ iCloud for Windows, Telelgram Desktop, Unigram X, WhatsApp Desktop, TamTam Destop, Wickr Me Desktop;
3. **Wi-Fi точки доступа и пароли** к ним;
4. **резервные копии** iTunes;
5. **учетные данные и токены** из портативных версий программ и программ, установленных по нестандартному пути.

Важно отметить, что указанные данные доступны только в том случае, если владелец компьютера включил функции автоматического сохранения вводимых паролей к учетным записям и Wi-Fi точкам доступа.

Системные требования к ПК (для установки UFED Analytics Desktop, Cloud Analyzer, Мобильный криминалист и др.).

ЦП	**Рекомендуемый** Core i7 (8 ядра) с тактовой частотой 3,5 ГГц или выше	**Минимальный ЦП** Core i7 (4 ядра) с тактовой частотой 3,3 ГГц или выше
Операционная Система	64-битная ОС Windows 10 PRO	
Память (ОЗУ)	**Рекомендуется** 32 Гб	**Минимум** 16 Гб
Жесткий диск	SSD (минимум 256 Гб) + HDD (минимум 1 Тб)	
Графический процессор	Nvidia со вычислительной мощностью 3.0 или выше, не менее 640 ядер CUDA и 2 ГБ памяти	

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**». 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 фабулы обучающиеся открывают на своих ПК файл с именем «Выгрузка МК Skout»[1] (ДИСК D). 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.

[1] Первая буква названия учебной дисциплины