КОМПЬЮТЕРНАЯ КРИМИНАЛИСТИКА

Киберкриминалистика: технический анализ пост инцидентных артефактов

КОМПЬЮТЕРНАЯ КРИМИНАЛИСТИКА

- это область криминалистики, которая занимается исследованием и сбором цифровых доказательств в целях расследования компьютерных преступлений

Она включает в себя изучение компьютерных систем, сетей, программного обеспечения и цифровых данных

ЦИФРОВЫЕ ДОКАЗАТЕЛЬСТВА

Сбор цифровых доказательств является неотъемлемой частью современных расследований

Он позволяет представить объективные и недвусмысленные факты, которые могут быть использованы в судебном процессе
для установления истины

ЦЕЛЬ ДОКЛАДА

- дать полное представление о процессе сбора цифровых доказательств и его важности для успешных криминальных расследований

Вы узнаете о методах сбора, анализа и применении цифровых доказательств в судебных процессах и в рамках реагирования на компьютерные инциденты информационной безопасности

МЕТОДЫ СБОРА ЦИФРОВЫХ ДОКАЗАТЕЛЬСТВ

1

Основные принципы

Сбор цифровых доказательств основан на таких принципах, как сохранение данных, аутентификация и непрерывность цепочки доказательств

2

Специализированное программное обеспечение

Программное обеспечение для цифровой криминалистики позволяет экспертам производить извлечение и анализ данных с различных устройств и файловых систем

3

Физическое изъятие и копирование данных

В некоторых случаях, для сбора доказательств может потребоваться физическое изъятие компьютерной техники или создание ее точной копии для последующего анализа

ИНСТРУМЕНТЫ И ПО ДЛЯ ФОРЕНЗИКИ

ИНСТРУМЕНТЫ ДЛЯ СНЯТИЯ ОБРАЗА:

- Arsenal image mount
- FTK Imager
- Acronis True Image
- R – Drive Image
- Dumpit
- Scalpel 2.0

ИНСТРУМЕНТЫ И ПО ДЛЯ ФОРЕНЗИКИ

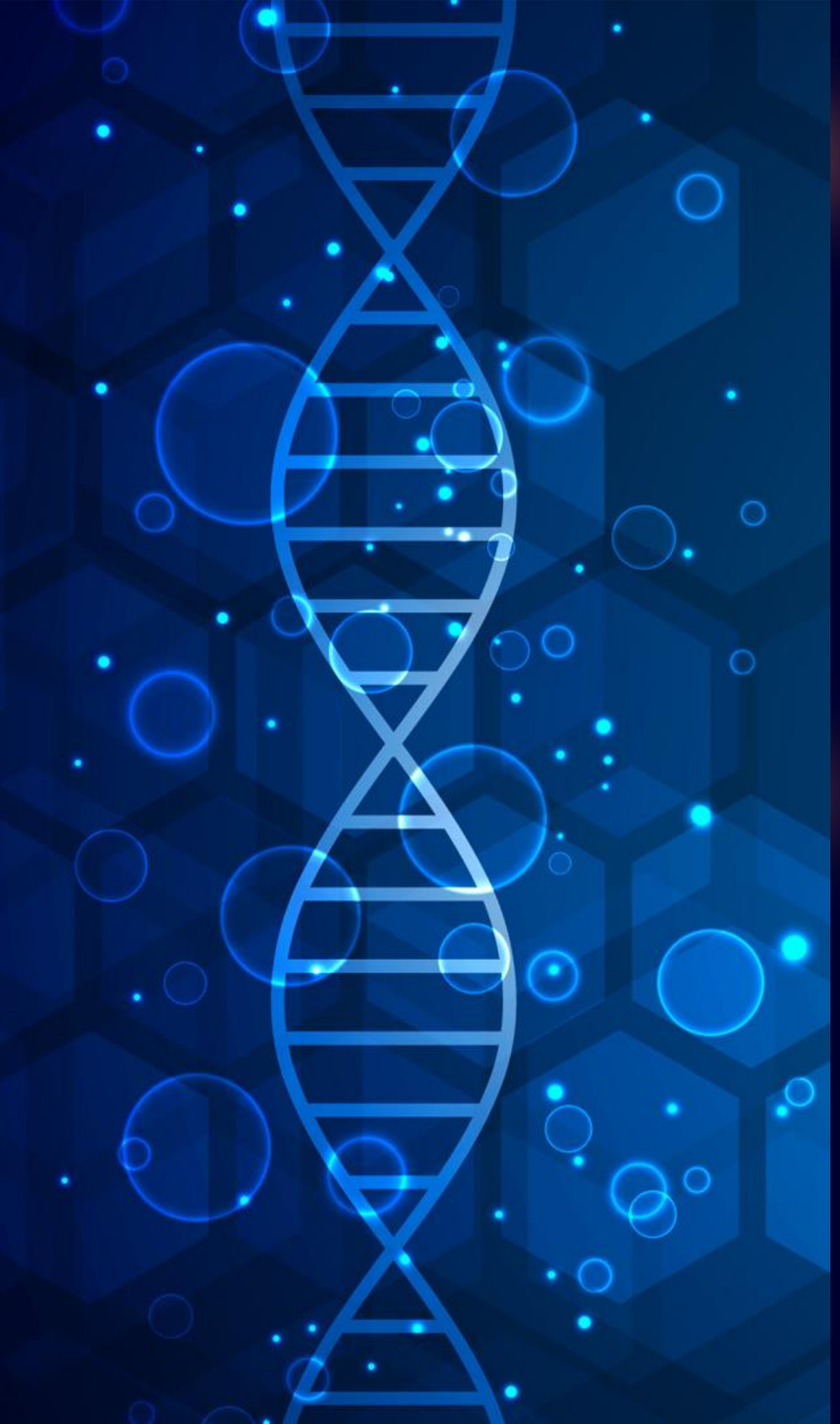
ПРОГРАММЫ
ДЛЯ ВОССТАНОВЛЕНИЯ ДАННЫХ:

- **R-studio**
- **Recuva**
- **Hetman Partition Recovery**
- **PC INSPECTOR File Recovery**

ИНСТРУМЕНТЫ И ПО ДЛЯ ФОРЕНЗИКИ

ИНСТРУМЕНТЫ ДЛЯ АНАЛИЗА СЕТЕВЫХ ЛОГ-ФАЙЛОВ:

- Splunk
- Q-radar
- Velociraptor
- Apt-hunter



АНАЛИЗ И ИНТЕРПРЕТАЦИЯ ЦИФРОВЫХ ДОКАЗАТЕЛЬСТВ

1

Основные этапы процесса анализа

Анализ цифровых доказательств включает в себя тщательное исследование данных, их фильтрацию, восстановление удаленных данных и выявление связей между ними

2

Восстановление удаленных данных

Цифровые доказательства могут содержать информацию, которая была намеренно удалена. С помощью специальных методов, можно восстановить эти данные и использовать их для расследования

3

Использование криптографических методов для расшифровки информации

В случаях, когда информация зашифрована, специалисты по цифровой криминалистике могут применять криптографические методы для расшифровки и изучения скрытого содержимого

МЕТОДИКА ПРОВЕДЕНИЯ ИССЛЕДОВАНИЯ ПОД УПРАВЛЕНИЕМ ОС WINDOWS

В рамках проведения исследования производятся следующие работы:

Сбор данных, необходимых для проведения анализа - производится снятие копий содержимого виртуальной памяти и логических дисков на запущенном сервере под управлением ОС Windows

Для обеспечения стабильности и непрерывности технологического процесса
на время работ управление оборудованием рекомендуется, при наличии, проводить на резервном сервере

Используемые программы: Dumpit, FTK Imager

Анализ загрузочных областей носителя информации - производится анализ главной загрузочной записи (MBR) и загрузочных записей разделов (VBR) на предмет модификаций, приводящих к неработоспособности системы или исполнению вредоносного кода

В случае необходимости производится восстановление таблицы логических разделов

Используемые программы: IDA – The Interactive Disassembler, TestDisk, Hiew

Анализ файловых структур каждого раздела каждого носителя информации - производится консолидация данных главной файловой таблицы (MFT), ее частичной копии ($MFTmirr), записей файловой таблицы, найденных в оперативной памяти *(если предоставлен дамп оперативной памяти)*, файле подкачки ОС, файле гибернации, а также в свободных областях носителя *(unallocated space и slack space)* информации

Используемые программы: R-Studio, Scalpel, The Sleuth Kit, Autopsy, Analyze MFT

Восстановление удаленных файлов - производится восстановление файлов на исследуемом носителе информации в соответствии с данными, полученными на предыдущем этапе работ, и на основе содержимого файлов

Используемые программы: R-Studio, Scalpel, The Sleuth Kit, Autopsy

Антивирусное сканирование - производится анализ всех существующих и восстановленных файлов на предмет вредоносного и потенциально опасного функционала

Используемые программы: Kaspersky Virus Removal Tool 2020, DrWeb CureIt

Анализ системных событий и файлов - производится анализ реестра ОС, журналов событий, файлов Prefetch, в том числе файлов из теневых копий логических разделов *(Volume Shadow Copies)* и точек восстановления ОС

Используемые программы: Mitec Windows Registry Recovery, RegRipper, Plaso, Event Log Explorer, Mitec Windows File Analyzer

Анализ пользовательской активности - производится анализ специфических ключей реестра ОС *(«userassist», «MRU lists» и других)*, отвечающих за пользовательскую активность журнала безопасности ОС, файлов ярлыков

Используемые программы: Mitec Windows Registry Recovery, RegRipper, Plaso, Event Log Explorer

Анализ сетевой активности - производится анализ электронной почты, истории и временных файлов браузеров и систем мгновенного обмена сообщениями

Используемые программы: BrowsingHistoryView, IECacheView, MozillaCacheView, OperaCacheView, ChromeCacheView, SafariCacheView, FirefoxDownloadsView, Plaso, SQLiteStudio, Mitec Mail Viewer

Также проводится анализ записи сетевого трафика *(если предоставлено)* для выявления следов активности вредоносного ПО, эксплуатации уязвимостей
и иных аномалий

Используемые программы: Wireshark, The Bro Network Security Monitor, NetworkMiner, Gephi2

Анализ вредоносных и потенциально опасных программ - производится динамический анализ потенциала опасных программ

При наличии у сотрудника НСРКИ компетенции для анализа исходного кода потенциально опасных программ - анализ осуществляется сотрудником НСРКИ

Анализ содержимого виртуальной памяти - производится анализ запущенных процессов, загруженных в память модулей и подключаемых библиотек, также производится поиск внедренных участков кода

Используемые программы: Hiew, Volatility Framework

Установление причинно-следственных связей - производится консолидация подозрительных событий, обнаруженных на предыдущих этапах работ, и установление причинно-следственных связей между ними

Используемые программы: Plaso

ПРАВОВЫЕ И ЭТИЧЕСКИЕ АСПЕКТЫ

1

Законодательство Республики Казахстан

- Постановление Правительства Республики Казахстан от 20 декабря 2016 года № 832 «Об утверждении единых требований в области информационно-коммуникационных технологий и обеспечения информационной безопасности»
- Постановление о назначение специалиста в рамках уголовного дела

2

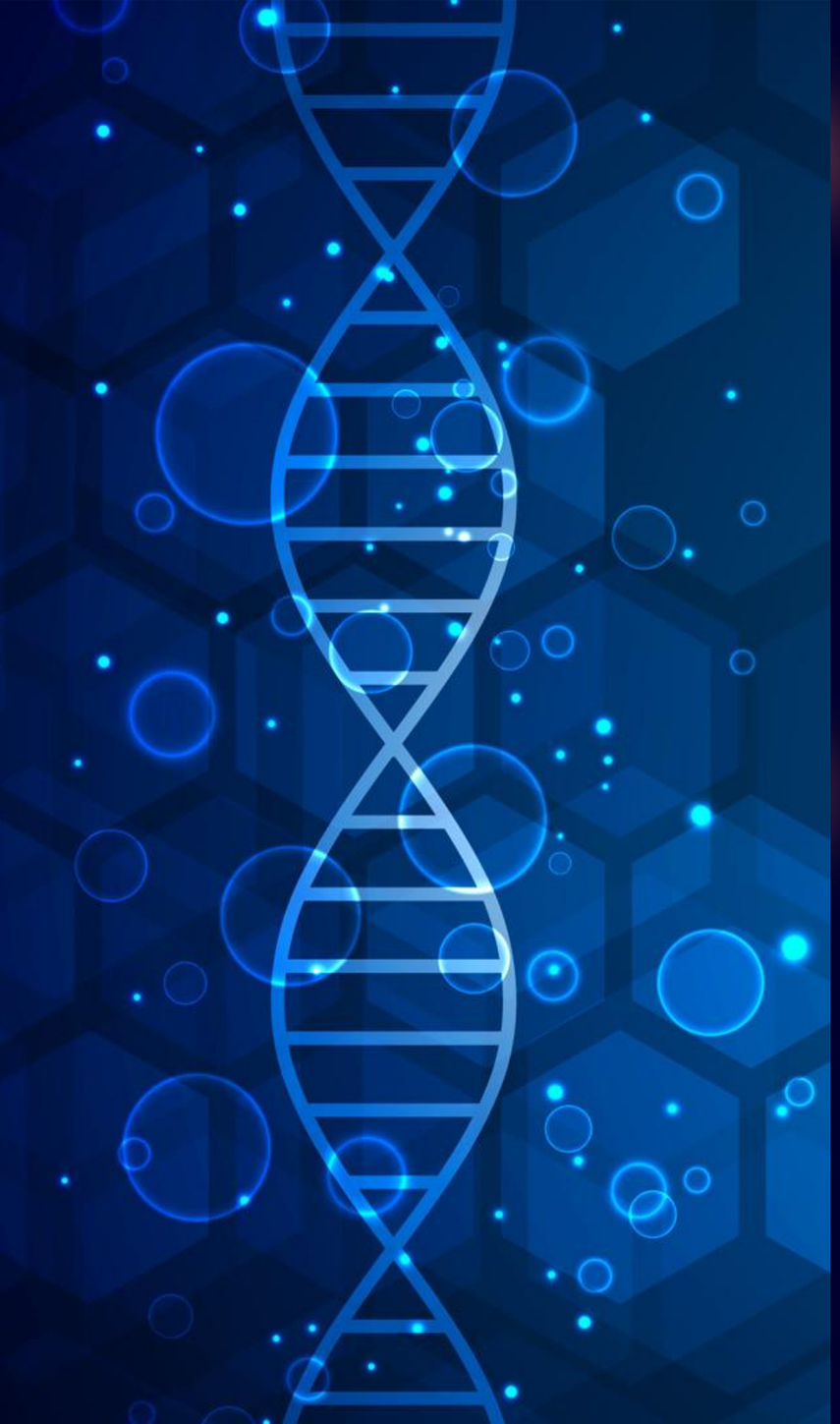
Конфиденциальность данных

Рассмотрите этические вопросы, связанные с обработкой и хранением цифровых данных

3

Экспертная свидетельство

- Предоставление заключение специалиста в рамках уголовного дела
- Участие в суде в рамках уголовного дела
- Предоставление отчета расследования инцидента ИБ в рамках реагирования на компьютерные инциденты в уполномоченный орган, местный исполнительный орган, государственный орган, квазигосударственный сектор



АНАЛИЗ И ИНТЕРПРЕТАЦИЯ ЦИФРОВЫХ ДОКАЗАТЕЛЬСТВ

1

Уголовное дело “X”

Рассмотрите пример успешного расследование инцидента ИБ в рамках уголовного дела

2

Захватывающая история

Узнайте о других увлекательных делах, в которых цифровая криминалистика сыграла ключевую роль

3

Будущее компьютерной криминалистики

Познакомьтесь с тенденциями и новыми методами, которые будут использоваться в цифровой криминалистике в будущем

ВОПРОСЫ?