Федеральное государственное казенное образовательное
учреждение высшего образования
«СИБИРСКИЙ ЮРИДИЧЕСКИЙ ИНСТИТУТ
МИНИСТЕРСТВА ВНУТРЕННИХ ДЕЛ РОССИЙСКОЙ ФЕДЕРАЦИИ»
Федеральное государственное казенное образовательное
учреждение высшего образования
«ВОРОНЕЖСКИЙ ИНСТИТУТ
МИНИСТЕРСТВА ВНУТРЕННИХ ДЕЛ РОССИЙСКОЙ ФЕДЕРАЦИИ»

А. В. Пучнин,
А.Д. Попов,
В.А. Цилик

Применение современных методов обучения иностранных слушателей по программам противодействия преступлениям, совершаемым с использованием информационно-телекоммуникационных технологий

Учебно-методическое пособие

Красноярск
СибЮИ МВД России
2023

ББК 74.58:67.408.135
УДК 378.1:343.9

Рецензенты: А.В. Рыжков – кандидат технических наук, доцент, проректор по учебной работе АНОО «Международный институт компьютерных технологий»;
Е.Ю. Кузнецов – заместитель начальника Управления уголовного розыска ГУ МВД России по Воронежской области, полковник полиции.

Учебно-методическое пособие подготовлено начальником кафедры оперативно-разыскной деятельности Воронежского института МВД России кандидатом юридических наук, доцентом, подполковником полиции А.В. Пучниным; доцентом кафедры автоматизированных информационных систем органов внутренних дел Воронежского института МВД России кандидатом технических наук, капитаном полиции А.Д Поповым, начальником Учебного центра (филиала) Сибирского юридического института МВД России в г. Манагуа Республики Никарагуа полковником полиции В.А. Циликом.

Пучнин, А.В.
Применение современных методов обучения иностранных слушателей по программам противодействия преступлениям, совершаемым с использованием информационно-телекоммуникационных технологий : учебно-методическое пособие / А.В. Пучнин, А.Д. Попов, В.А. Цилик. – Красноярск: СибЮИ МВД России, 2023. – 80 с.

Учебно-методическое пособие рассматривает основные методы подготовки специалистов, использующих в процессе противодействия преступности информационно-телекоммуникационные технологии, и предназначено для применения при организации и проведении занятий семинарского типа кейс-технологий.

Область применения: подготовка сотрудников правоохранительных органов иностранных государств, задействованных в противодействии преступлениям, совершаемым с использованием информационно-телекоммуникационных технологий.

Оглавление

Введение

В настоящее время значительно выросла потребность правоохранительных органов в специалистах, обладающих компетенциями в сфере противодействия преступлениям, совершаемым с использованием информационно-телекоммуникационных технологий.

Одной из таких компетенций является способность сотрудника использовать в противодействии преступлениям методы конкурентной разведки, свободно распространяемое и специализированное программное обеспечение: опираясь на информацию из открытых источников, деанонимизировать лицо, администрирующее такие аккаунты, а также фиксировать противоправную деятельность с целью дальнейшего использования в качестве доказательств.

OSINT (англ. Open source intelligence,) – разведывательная дисциплина, включающая в себя поиск, выбор и сбор разведывательной информации из общедоступных источников, а также её анализ. В разведывательном сообществе – термин «открытый источник разведывательных данных».

Хакерские группировки и компьютерные злоумышленники тоже собирают данные о пользователях сети с целью получения доступа к информационным и финансовым активам (кредитным картам, системам онлайн платежей, электронным кошелькам граждан и т.д.). В сфере бизнеса сбор информации о субъекте предпринимательской деятельности ведется специалистами по конкурентной разведке.

Сотрудники полиции также должны обладать компетенциями в данной области. В пособии содержится учебный и практический материал, раскрывающий базовые навыки сбора информации по открытым источникам, в том числе о расширенном поиске Google, который представляет собой способ настройки поиска с помощью набора специальных инструкций. Данные инструкции поиска Google известны как операторы и команды, которые представляют собой уточняющие запросы, сужающие область исследования для получения желаемого результата. Большинство операторов легко запоминаются и представляют собой короткие команды, позволяющие уточнить пользовательский запрос и получить необходимую поисковую выдачу. Запросы можно выполнять как в поисковой строке, так и на специальной странице по адресу https://www.google.com/advanced_search. Подобная функциональность реализована в каждой из поисковых систем, но вводимые операторы и команды могут отличаться и, соответственно, будут работать по-другому.

В целях закрепления учебного материала в работу включен блок, раскрывающий прохождение интерактивной игры с сюжетной линией, которая заключается в решении различных головоломок и логических заданий

При проведении интерактивной игры слушатели дозированно получают информацию, учебные объекты хранения и обработки цифровых данных, используя которые с применением методов конкурентной разведки, свободно распространяемого и специализированного программного обеспечения осуществляют фиксацию сведений, представляющих значение для расследования вымышленных преступлений, совершенных фигурантами (персонажами) сюжетных линий интерактивной игры.

Слушателям объявляется, что в рамках прохождения интерактивной игры имитируются и осуществляются действия по сбору, обработке и использованию персональных данных игровых персонажей, помещенных в реальную информационную среду пользователей сетей Интернет и Даркнет.

Сбор и использование информации, в том числе персональных сведений, допускается только в рамках заданий сюжетных линий интерактивной игры.

В целях соблюдения норм законности предполагается, что в рамках игровых учебных заданий:

– порядок использования полученных персональных сведений соответствует нормативным правовым актам национального законодательства;

– соответствующие разрешения на осуществление сбора и использования сведений, затрагивающих права и свободы человека (игровых персонажей), имеются и надлежащим образом оформляются слушателями в соответствии с нормативными правовыми актами национального законодательства;

– необходимые условия и основания, допускающие сбор персональных данных в отношении игровых персонажей, соблюдены;

– выполнение заданий предполагает обучение сбору, анализу и использованию информации, касающейся вымышленных пользователей информационно-телекоммуникационных технологий и систем;

– слушатели являются лицами, уполномоченными на проведение действий и мероприятий, которые будут осуществляться в рамках прохождения интерактивной игры.

Интерактивная игра предназначена для:

– создания различных ситуаций с целью формирования линейного сюжета, в пределах которого отрабатываются знания и умения обучающегося;

– овладения обучающимися знаниями в сфере поиска и фиксации информации относительно динамичных взаимосвязанных объектов на ресурсах сетей Интернет и Даркнет и выработки соответствующих навыков;

– обеспечения контроля за использованием технических средств, мультимедийного контента, шагов, вопросов, условий ситуации в ходе учебного процесса;

– отработки умений и навыков использования мультимедиа-технологий, предоставляющих возможность реализовывать методики отработки различных тактических ситуаций расследования преступлений;

– отработки умений и навыков применения методов конкурентной разведки, свободно распространяемого и специализированного программного обеспечения;

– предоставления возможности обучающемуся самостоятельно искать пути и варианты решения поставленной учебной задачи (выбор одного из предложенных вариантов или нахождение собственного варианта и обоснование решения);

– предоставления возможности обучающемуся самостоятельно интерпретировать полученные результаты, продемонстрировать личный уровень компетенций.

Слушатели осуществляют прохождение заданий как индивидуально, так и в составе подгрупп (рекомендуемая численность – не более 4 человек).

Слушатели получают задания с использованием Системы электронного обучения Воронежского института МВД России, расположенной по адресу https://moodle.vimvd.ru/.

Слушатель авторизуется в Системе электронного обучения Воронежского института МВД России.

Перед решением каждого задания слушатель получает вводную, формат и пример правильного ответа.

После ввода правильного ответа обучающиеся уведомляются об этом, получают подсказку к следующему заданию и переходят к нему.

Интерактивная игра состоит из двух этапов.

После успешного завершения каждого этапа интерактивной игры и выполнения всех образующих его заданий, обучающиеся получают информацию, достаточную для принятия управленческого решения.

Первый этап имеет 5 сюжетных линий из 8 заданий.

Второй этап состоит из одной сюжетной линии, состоящей из 3 заданий.

Сюжетные линии первого этапа объединены общим замыслом интерактивной игры, о котором слушатели узнают в рамках прохождения второго этапа.

Решение заданий первого этапа для каждой сюжетной линии имеет некоторые отличия по содержанию и способу применения методов конкурентной разведки, свободно распространяемого и специализированного программного обеспечения.

1. Методы анонимизации в сети Интернет

Подчеркнем, что необходимо пользоваться средствами анонимизации в целях сокрытия факта заинтересованности злоумышленниками со стороны сотрудников правоохранительных органов. Для этих целей в арсенале современных информационно-коммуникационных технологий (ИКТ) существуют специальные сервисы безопасности, так называемые анонимизаторы.

Privacy – это когда все знают кто ты, но не знают конкретно, что ты сейчас делаешь.

Anonymity – это когда никто не знает кто ты, но видят твои действия.

Технологии анонимизации, наиболее часто используемые при построении соответствующих сервисов безопасности систем ИКТ:

– анонимайзеры;
– прокси-сервера;
– VPN (англ. Virtual Private Network – виртуальная частная сеть);
– распределенная анонимная сеть Tor;
– проект I2P.

1. Анонимайзеры.

Самый простой способ анонимизации своей деятельности в сети Интернет – воспользоваться услугами сайтов-анонимайзеров. Для того чтобы получить доступ к заблокированному интернет-сайту, достаточно ввести адрес сайта на одном из таких сервисов. Основной недостаток этого способа заключается в том, что эти сервисы анонимизации достаточно медленно работают и не подходят для удобного серфинга. Пример такого сервиса – hidemyass.com, анонимный серфинг в сети. Также существуют специальные плагины для браузеров, которые позволяют осуществлять серфинг в сети через анонимайзер.

2. Прокси-сервера.

Прокси-сервера – это специальные компьютеры, на которых установлено специализированное программное обеспечение, позволяющее принимать запросы на соединение с различными сайтами. При установлении соединения с прокси-сервером компьютер обычного пользователя «как бы перепоручает» такому серверу соединиться с определенным сайтом. В таком случае браузер работает в обычном режиме. А вот для использования прокси-сервера необходимо прописать его IP-адрес в настройках используемого браузера. А еще существуют сервисы, которые помогают подключаться к таким серверам или даже целым цепочкам (каскадам) прокси-серверов.

Отметим, что эти два метода не являются надежными, хотя это самые простые методы для обеспечения приватности в сети Интернет

3. VPN (англ. Virtual Private Network – виртуальная частная сеть). VPN – это обобщённое название технологий, позволяющих обеспечить одно или несколько сетевых соединений (логическую сеть) поверх другой сети (например, Интернет). Несмотря на то, что коммуникации осуществляются по сетям с меньшим неизвестным уровнем доверия (например, по публичным сетям), уровень доверия к построенной логической сети не зависит от уровня доверия к базовым сетям благодаря использованию средств криптографии. В зависимости от применяемых протоколов и назначения VPN может обеспечивать соединения трёх видов: узел-узел, узел-сеть и сеть-сеть.

VPN-туннель – это виртуальное зашифрованное стойким алгоритмом соединение. Наглядно его можно представить в виде непрозрачной трубы, а еще лучше – тоннеля, один конец которого упирается в компьютер рядового пользователя, а второй – в специализированный сервер, находящийся, как правило, в удалении или даже в другой стране.

Современные виды VPN-подключения:

– PPTP (англ. Point-to-point tunneling protocol);

– OpenVPN;

– L2TP (англ. Layer 2 Tunneling Protocol).

PPTP (Point-to-point tunneling protocol) – туннельный протокол типа «точка-точка», который позволяет компьютеру пользователя устанавливать защищённое соединение с сервером за счёт создания специального туннеля в стандартной, незащищённой сети. Этот протокол (PPTP) стал известен, потому что это первый VPN-протокол, который поддержала корпорация Microsoft. Все версии Windows, начиная с Windows 95 OSR2, уже включают в свой состав PPTP-клиент. Это самый известный и простой в настройке вариант подключения к VPN-сервису. Но, как говорится, есть здесь и отрицательный момент: многие интернет- провайдеры блокируют работу PPTP подключений.

OpenVPN – это свободная реализация технологии виртуальной частной сети (VPN) с открытым исходным кодом для создания зашифрованных каналов вида «точка-точка» или «сервер-клиенты» между компьютерами. Она может устанавливать соединения между компьютерами, которые находятся за NAT-firewall без необходимости изменения его настроек. Но использование этой технологии потребует установки дополнительного программного обеспечения для всех операционных систем.

L2TP (Layer 2 Tunneling Protocol) – это сетевой протокол туннелирования канального уровня, сочетающий в себе протокол L2F (layer 2 Forwarding), разработанный компанией Cisco, и протокол корпорации Microsoft. Позволяет создавать VPN с заданными приоритетами доступа, однако не содержит в себе средств шифрования и механизмов аутентификации (для создания защищённой VPN) и его используют совместно с IPSec. По отзывам экспертов, является наиболее защищенным вариантом VPN подключения, несмотря на трудность его настройки.

4. Распределенная анонимная сеть Tor.

Tor – это свободное программное обеспечение для анонимизации трафика. Открытый исходный код Tor проверяется многими людьми со всего мира, что обеспечивает своевременное выявление дефектов и невозможность тайного встраивания в него «чёрного хода» для государственных служб или кого-либо еще.

Tor обеспечивает надежную и бесплатную анонимизацию, защищая пользователя от слежки как за посетителями определенного сайта, так и за всей активностью самого пользователя. Когда пользователь передаёт данные, программа Tor скрывает и настоящий пункт их назначения и сами данные, перебрасывая данные в зашифрованном виде через цепочку промежуточных узлов сети.

Работа Tor основана на взаимодействии многих серверов сети Tor, каждый из которых предоставляет часть пропускной способности своего интернет-подключения для нужд сети. Этот принцип работы близок к принципу работы пиринговых сетей. Любой пользователь может быть сервером, отдавая часть пропускной способности для развития анонимной сети и тем самым улучшая свою собственную анонимность. Для этого пользователю необходимо настроить свое программное обеспечение Tor как серверную часть.

Tor случайным образом выбирает несколько серверов из всех доступных (список которых он периодически скачивает с центрального сервера-директории) и строит тоннель, проходящий через эти промежуточные точки. Ваш трафик будет пропускаться через этот тоннель; у него есть вход – приложение Tor на

вашей машине и выход – последний из случайно выбранных для этого тоннеля серверов сети Tor.

Несмотря на высокую степень анонимизации, у сети Tor есть и существенные недостатки:

а) основной недостаток сети Tor – очень медленная работа. Действительно, изначально, чтобы работать с сетью Tor эффективно, у вас должен быть очень высокоскоростной интернет, да и то через некоторые цепочки анонимных серверов соединение с сайтами осуществляется очень долго;

б) Tor – свободное программное обеспечение, развивается проект энтузиастами дела, в связи с чем есть целый ряд моментов, которые пока у этого сервиса не доработаны.

5. Проект I2P.

I2P – это анонимизирующая сеть, предоставляющая приложениям простой программный интерфейс для защищенной коммуникации. Все передаваемые данные зашифрованы в несколько слоев, а сеть одновременно децентрализованная и динамическая, без использования элементов, которым бы требовалось заочно доверять.

Существует множество приложений, работающих через I2P, включая почтовые клиенты, P2P-клиенты, IRC-клиенты и прочее. Проект I2P был начат в 2003 году.

I2P – это попытка создать защищенную децентрализованную анонимную сеть с малым временем отклика и свойствами автономности, отказоустойчивости и масштабируемости. Все аспекты сети доступны в виде исходного кода и бесплатны. Это одновременно и позволяет пользователям убедиться, что программное обеспечение делает именно то, что заявлено, и облегчает сторонним разработчикам возможность совершенствовать защиту сети. Децентрализованность, шифрование и анонимность – вот на каких принципах построена I2P.

Как и подобает любой анонимной сети, I2P децентрализована. В сети нет DNS, вместо них используют так называемые адресные книги, которые постоянно автоматически обновляются у всех клиентов от других клиентов. В них идет сопоставление названия сайта или другого ресурса, известного как «http://имя_сайта.i2p», с его фактическим адресом (открытым криптографическим ключом). Вместо IP-адресов во всей сети используются открытые криптографические ключи, которые не имеют абсолютно никакой логической связи с реальными компьютерами. Даже зная эти ключи, невозможно не только определить местоположение пользователей, но и расположение серверов. Именно поэтому I2P нельзя отключить, отфильтровать или заблокировать[1].

Практические задания для самоподготовки

1. Отработать в целях анонимизации работы использование анонимайзеров, проверив их эффективность на ресурсах сети Интернет.

2. Отработать в целях анонимизации работы использование прокси-сервера, проверив его эффективность на ресурсах сети Интернет.

3. Отработать в целях анонимизации работы использование TOR, проверив его эффективность на ресурсах сети Интернет.

4. Отработать в целях анонимизации работы использование I2P, проверив его эффективность на ресурсах сети Интернет.

---

1 Артамонов В.А., Артамонова Е.В. Методы анонимизации в сети интернет. URL: http://itzashita.ru/publications/metodyi-anonimizatsii-v-seti-internet.html.

2. Методы деанонимизации в сети Интернет

О регистрации пользователя

Первое, о чём следует помнить, когда пользователь желает связать себя с воображаемым персонажем, например на форуме, это то, что после прочтения и согласия с правилами (дисклеймером) он начинает играть «по правилам» администрации ресурса, обязан хотя бы минимально ей доверять. Иными словами, он в той или иной мере делегирует администрации свои персональные данные (повторимся, не касаясь технических возможностей, позволяющих это сделать, вплоть до хеширования всех данных пользователя).

Минимально возможная регистрация – это связка логина (учётной записи) и пароля в случае, когда логин совпадает с никнеймом. Профайл в таком случае состоит из одного никнейма (и порядкового номера пользователя). В нагрузку может быть добавлена дата регистрации. Согласитесь, что такой минимализм в наборе персональных данных встречается нечасто.

Гораздо чаще во время регистрации присутствуют поля о дате рождения, местоположении пользователя и т.д.

Дата рождения

Наличие первого иногда необходимо законодательно – например, для ограничения доступа по возрасту ко «взрослым» материалам. Пункт «скрывать мой возраст» присутствует не всегда; встречались курьёзные случаи, когда даже при наличии отмеченного «скрывать мой возраст» никнейм пользователя появлялся во фрейме «Сегодня день рождения у: ...». Для идентификации пользователя отличия в указании только дня рождения от полной даты рождения несущественно. При регистрации поле исключительно «год рождения» (без дня и месяца) попадается редко.

Местоположение

Поля, относящиеся к местоположению пользователя, чаще всего являются «страной» и «часовым поясом». Нередки поля «город». Здесь следует понимать, что если пользователь проживаете в городе с численностью населения менее N (допустим, ниже тридцатой позиции списка), то при достоверно указанной информации о его местоположении увеличивается число способов, по которому его личность можно идентифицировать (предельный случай – появляется способ «все со всеми знакомы»).

В формах регистрации на форумах, предназначенных для профессионального общения, поддержки и обмена опытом, бывают (обязательные!) поля, выявляющие настолько специфические области (профессиональные интересы, используемое ПО и оборудование, и даже подразделение, где работает пользователь), что анонимность де-факто снимается.

E-mail и IM

В большинстве случаев регистрации предлагается оставить e-mail адрес, использовать который следует для подтверждения регистрации и в целях восстановления забытых паролей. Чаще всего почта по умолчанию скрыта в профайле ото всех, кроме пользователя, хотя виной тому не забота о приватности пользователя, а защита от спама. Почтовый адрес сам по себе зачастую содержит данные об имени, фамилии или годе рождения пользователя, а то и все эти данные сразу: «ivan.ivanov85@example.com». Также существуют сервисы «одноразовой почты» (наподобие 10 Minute Mail), которые часто используются для подтверждения регистрации пользователями, не желающими использовать для этой цели своей основной почтовый ящик. Степень анонимизации внутри почтовой коммуникации рассматривать не будем, поскольку специфика закрытых каналов совершенно иная, нежели открытых для всех профайлов (и для

поисковых роботов в том числе). Упомянем лишь, что почтовая переписка может быть случайно или намеренно обнародована, например при невнимательной пересылке третьему лицу приходит не определённый фрагмент письма, а вся цепочка писем. Многие формы предлагают оставить адреса средств обмена мгновенными сообщениями. Все такие средства имеют собственные профайлы, хранящие личные данные пользователя. Иногда в строгой форме, вплоть до имени, фамилии и местоположении пользователя.

Мультиник

Здесь под мультиником понимается множественное использование пользователем одного никнейма в различных социальных ресурсах Интернета. Множественное использование никнейма значительно уменьшает анонимность пользователя – профайлы из разных мест с точки зрения деанонимизации могут быть просто объединены. В случае наличия множества (в смысле математической логики) друзей-френдов у пользователя хотя бы на одном из сайтов, где пользователь активен под неким именем, часть такого множества может быть реконструирована и на другом сайте «вокруг» этого же никнейма.

Социальные сети

В топике «Анонимность против открытости» в плакатном формате рассмотрено «противостояние» этих подходов. Мы описываем ситуации пользователя, находящегося между двумя такими полюсами, когда нет и безнаказанности анонимов и единоличности пользователя соцсети. Сохранение остатков анонимности при открытом имени и фамилии практически невозможно. И социальные сети стремятся максимально охватить жизнь человека и представить её в сети.

Стили речи и содержание текстов

В общем случае в сети используются же речевые стили, которыми человек пользуется в живом общении с друзьями, коллегами, случайными прохожими. Некоторые лингвисты полагают, что для идентификации человека достаточно лишь определённого объёма его текстов. Простейшую лингвистическую экспертизу проделывает каждый человек, когда читает какой-либо текст. Сразу виден образовательный уровень человека. Он плохо скрываем под масками любых стилей речи и при любом виде общения. Образовательный уровень влияет на активный словарный запас. Важнее не его размер, а наличие в нём профессиональных терминов и относительная частота их использования. То есть пользователя не выдаст то, что он пишет богатым синонимами языком, но если он в своих текстах свободно употребляет какую-либо терминологию (отличную от терминологии тематики сайта), то это может указать либо на его специальность, либо на продвинутый уровень в определённом хобби. Деятельность человека всегда влияет на его речь. Так, канцеляризмы юриста не исчезают даже при общении в быту («произведи уборку в помещении» вместо «уберись в комнате»).

Профессиональная тематика

Наличие грамотных сообщений и комментариев в узкоспециальной области само по себе резко выявляет данного человека. Но зачастую грамотность таких комментариев может определить лишь эксперт в данной области. Профессионалы всегда имеют публикации, работы, статьи. Научная этика, например, требует цитирования и ссылок на исследования. От этики в одночасье отказаться сложно, в итоге анонимный автор глубокой и грамотной статьи скорее всего даст ссылку либо на свою работу, либо на работы авторов, на которых он ссылался в своих трудах, либо на работы, которые ссылаются на него.

Ошибки

Ошибаются все. Но может пользователь систематически ошибается в каком-то специальном слове? Проверяет свои тексты спеллчекерами (средствами проверки орфографии)?

Кросспосты

Тема очень знакомая пользователям Хабрахабра. Наличие идентичных анонимных текстов (или их фрагментов) на различных сайтах при последующих комментариях «от автора» свяжет воедино никнеймы пользователей, которые их опубликовали. Публикуя в разных местах один текст, пользователь в открытую кричит: «Я там-то и там-то!». От недоброкачественной копипасты (без ссылок на источник) отличаются по форме и наличию автора в дискуссиях и комментариях.

Друзья (френды)

Как было сказано выше, наличие сообществ «друзей», даже в случаях когда друзья видны под никнеймами, активно способствует деанонимизации. Если кто-либо из друзей знает лично пользователя, желающего сохранить анонимность, он может случайно его деанонимизировать (банальное «посмотрите в блоге у Миши» открывает идентификацию одного из друзей автора сообщения с именем Миша).

Анонимность публичных людей

Здесь всё достаточно просто: публичный человек может быть либо полностью деанонимизированным, когда его статьи, сообщения и комментарии являются продолжением его политики общения в жизни, либо полностью анонимизированным, в таком случае все его социальные действия в Интернете должны обнаруживать минимально возможное число связей с его личностью – до самого отказа от регистрации на сайте. Все промежуточные состояния будут перескакивать в область деанонимизации данного публичного человека.

Время

Наконец, отчасти деанонимизировать может даже время отправки сообщений. Если человек чаще всего отправляет сообщения с 3:00 ночи до 7:00 утра, то, может быть, он полуночник либо живёт в далёком часовом поясе (впрочем, могут быть неверны настройки часового пояса на данном сайте)[1].

Практические задания для самоподготовки

1. Отработать полученные теоретические знания по сбору информации о регистрационных данных пользователей ресурсов социальных сетей и пабликов.
2. Отработать полученные теоретические знания по сбору информации о дате рождения пользователей ресурсов социальных сетей и пабликов.
3. Отработать полученные теоретические знания по сбору информации о местоположении пользователей ресурсов социальных сетей и пабликов.
4. Отработать полученные теоретические знания по сбору информации о E-mail и IM пользователей ресурсов социальных сетей и пабликов.
5. Отработать полученные теоретические знания по обнаружению факта использования пользователем мультиника в социальных сетях и пабликах.
6. Отработать полученные теоретические знания по анализу графа социальных связей пользователей социальных сетей.

1 Анонимизация и деанонимизация в сети Интернет. URL: https://habr.com/ru/articles/137416/.

3. Расширенный поиск Google

Операторы

Поисковый запрос

Поисковой запрос точного совпадения. Используется для уточнения неоднозначных результатов поиска и исключения синонимов при поиске отдельных слов.

Пример: steve jobs

OR

Поиск по двум равнозначным словам. Вернёт результаты, связанные с значением X или Y или и то, и другое. Вместо OR возможно использовать оператор pipe (|).

Пример: jobs OR gates / jobs | gates

AND

Поиск по X и Y. Вернёт только результаты, связанные как с X, так и с Y. Примечание: в реальности не имеет значения для обычного поиска, потому что Google по умолчанию вставляет AND. Но очень полезен в сочетании с другими операторами.

Пример: jobs AND gates

-

Исключение термина или фразы. В нашем примере все страницы будут упоминать Джобса, но не с Apple (компанией).

Пример: jobs -apple

*

Действует как подстановочный знак для произвольного слова или фразы.

Пример: steve * apple

( )

Группировка нескольких терминов или операторов, для контроля поисковой выдачи.

Пример: (ipad OR iphone) apple

$

Поиск цен. Также работает для евро (€), но не для британского фунта (£).

Пример: ipad $329

define

Встроенный в Google словарь. Показывает значение слова.

Пример: define:entrepreneur

cache

Возвращает последнюю кэшированную версию веб-страницы (при условии, что страница проиндексирована).

Пример: cache:apple.com

filetype:

Ограничивает результаты поисковой выдачи файлами определённого формата, например, pdf, docx, txt, ppt и т. д. Примечание: аналогично оператору ext:.

Пример: apple filetype:pdf / apple ext:pdf

site:

Осуществляет поиск вложенных страниц и поддоменов для определенного доменного имени.

Пример: site:apple.com

related:

Осуществляет поиск сайтов, связанных с доменом.

Пример: related:apple.com

intitle:

Находит страницы с определённым словом (или словами) в заголовке страницы. В нашем примере возвратятся все результаты со словом [apple] в теге title.

Пример: intitle:apple

allintitle:

Аналогично «intitle», но будут возвращены результаты, содержащие все указанные слова в теге title.

Пример: allintitle:apple iphone

inurl:

Находит страницы с определённым словом (или словами) в URL. В этом примере будут возвращены все результаты, содержащие слово [apple] в URL.

Пример: inurl:apple

allinurl:

Аналогично «inurl», но возвращает результаты со всеми указанными словами в URL.

Пример: allinurl:apple iphone

intext:

Находит страницы, содержащие определённое слово (или слова) в содержании. В примере будут возвращены все результаты, содержащие слово [apple] на странице.

Пример: intext:apple

allintext:

Аналогично intext, но возвращает результаты со всеми указанными словами на странице.

Пример: allintext:apple iphone

AROUND(X)

Поиск поблизости. Страницы, содержащие два слова или фразы на расстоянии X слов друг от друга. В этом примере слова [apple] и [iphone] должны присутствовать в тексте на расстоянии не более четырёх слов друг от друга.

Пример: apple AROUND(4) iphone

weather:

Выводит информацию о погоде в указанном месте, которая отображается в погодном сниппете, а также возвращает результаты с других метеорологических сайтов.

Пример: weather:san francisco

stocks:

Биржевая информация (т.е. цена и др.) для любой акции по биржевому тикеру.
Пример: stocks:aapl

map:
Результаты поиска по картам.
Пример: map:silicon valley

movie:
Найти информацию о конкретном фильме. Также находит расписание сеансов, если фильм сейчас показывают в ближайших кинотеатрах.
Пример: movie:steve jobs

in
Преобразует одну единицы измерения в другую. Работает с валютами, весами, температурой, расстояниями и т. д.
Пример: $329 in GBP

source:
Найти новостные результаты из определённого источника в Google News.
Пример: apple source:the_verge

_
Символ нижнего подчёркивания действует как подстановочный знак для автодополнения.
Пример: apple CEO _ jobs

Частично рабочие операторы
#..#
Поиск диапазона чисел. В приведённом примере возвращаются результаты [видео WWDC] за 2010-2014 годы, но не за 2015 и последующие годы.
Пример: wwdc video 2010..2014

inanchor:
Поиск страниц, связанных с определённым текстом в ссылке. В этом примере будут возвращены все страницы, на которые есть ссылки со словами [apple] или [iphone].
Пример: inanchor:apple iphone

allinanchor:
Аналогично inanchor, но возвращает результаты, содержащие все указанные слова во входящих ссылках.
Пример: allinanchor:apple iphone

loc:placename
Найти результаты поисковой выдачи из определенного региона.
Пример: loc:«san francisco» apple

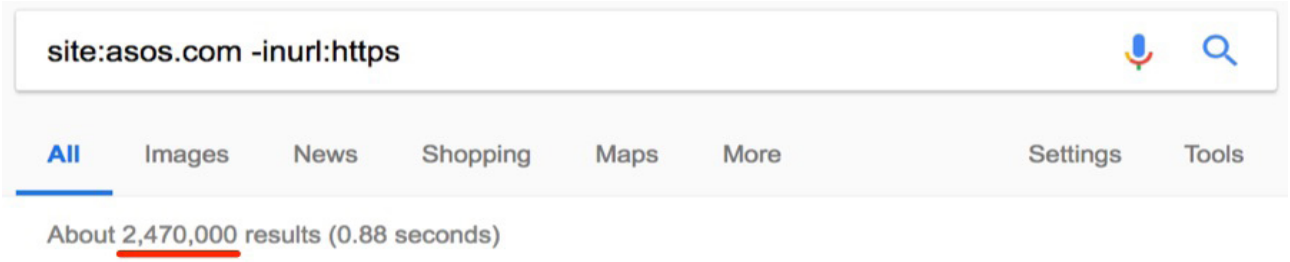
location:
Найти результаты из Google News.
Пример: location:«san francisco» apple

Примеры использования операторов поиска Google

Рассмотрим несколько способов эффективного применения этих операторов, в том числе в сочетании друг с другом. Рекомендуется отклоняться от приведённых примеров.

Поиск незащищённых страниц (не https)

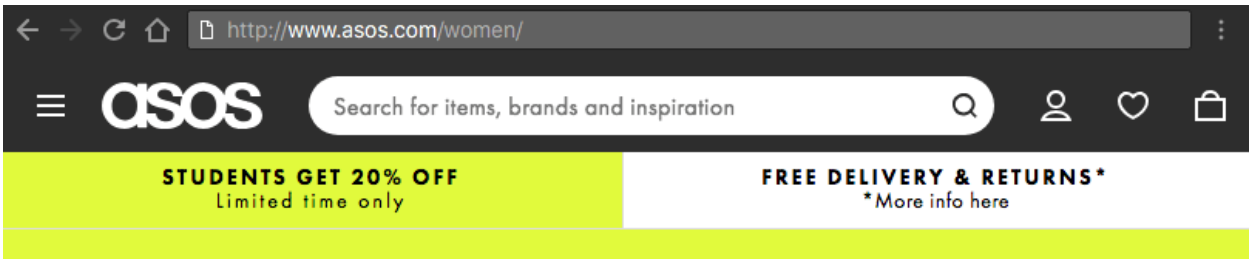
HTTPS в настоящее время стал обязательным требованием, особенно для сайтов электронной коммерции. Возможно с помощью оператора site: найти незащищённые страницы. Проверим на примере asos.com.



Нашлось, около 2,47 млн незащищённых страниц.

Похоже, что Asos вообще не используют SSL – невероятно для такого большого сайта.

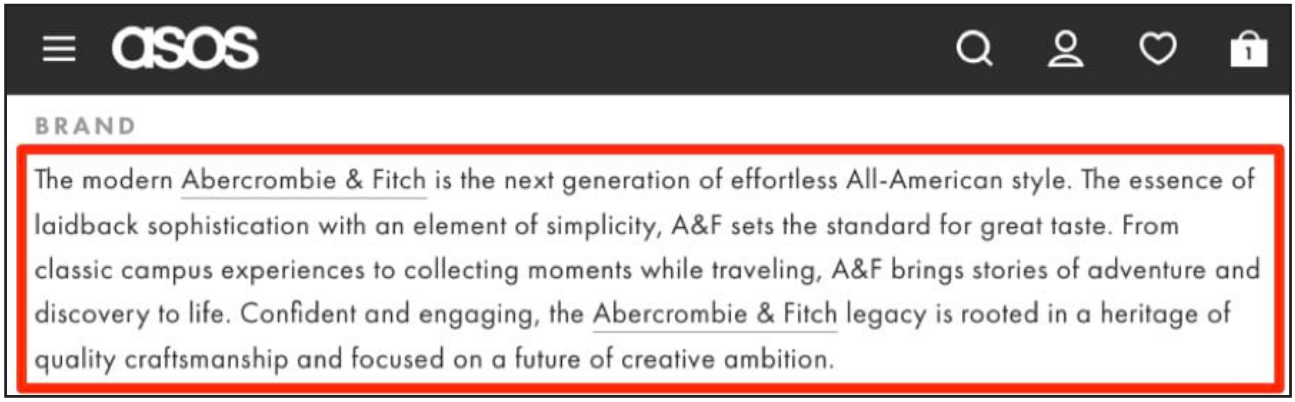
Но вот ещё одна тонкость: Asos доступен в версиях https и http.



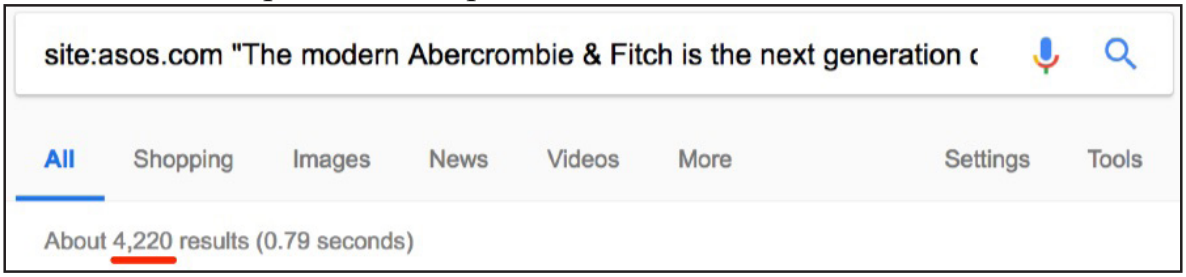
Примечание. Иногда страницы индексируются без https, но после перехода по ссылке происходит редирект на версию https.

Поиск дубликатов контента

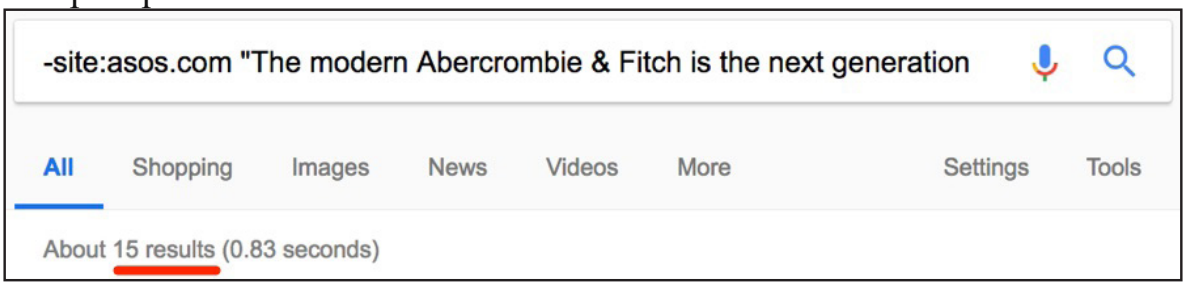
Поиск дубликатов является важной задачей, например, для выявления цитирующих друг друга СМИ. Представлена пара джинсов Abercrombie & Fitch на сайте Asos со стандартным описанием:



Стандартные описания сторонних брендов часто дублируются на других сайтах. Но сколько раз текст встречается на asos.com.

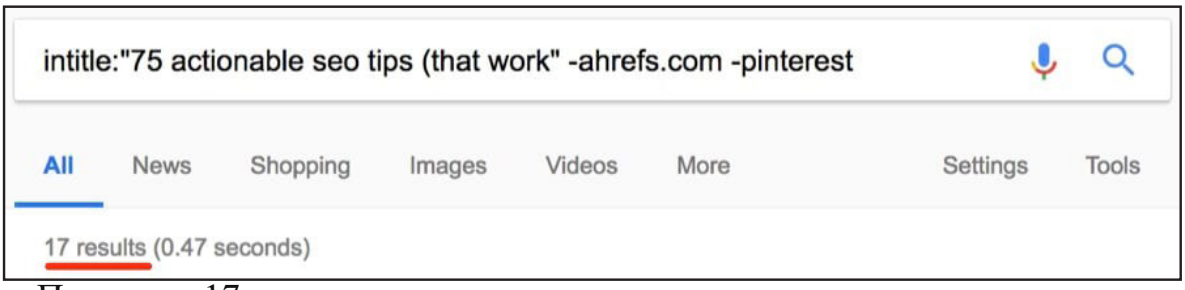


Примерно 4200 раз. Теперь посмотрим, является ли текст уникальным для Asos. Проверим.



Нет, он не уникален. Есть 15 других сайтов с точно таким же текстом, то есть дублированным контентом, т.е. дубли могут присутствуют на страницах с похожими товарами.

Если у вас есть блог, люди могут заимствовать и публиковать ваш контент без надлежащей ссылки. Рассмотрим на примере списка советов по SEO.

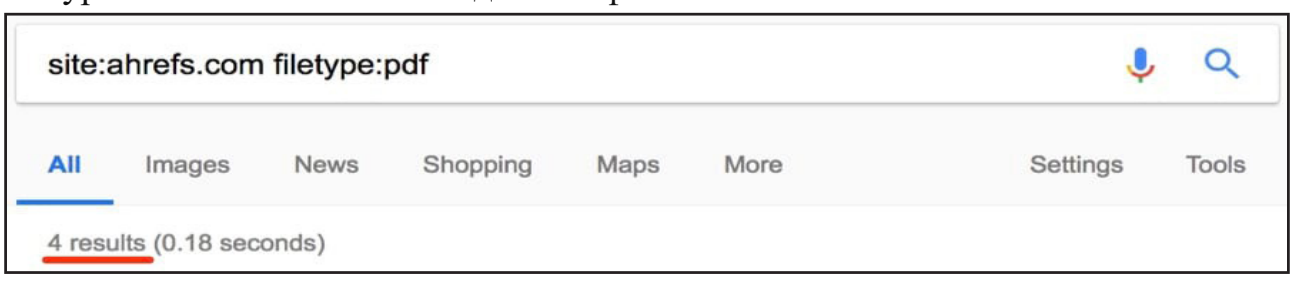


Получено 17 результатов.

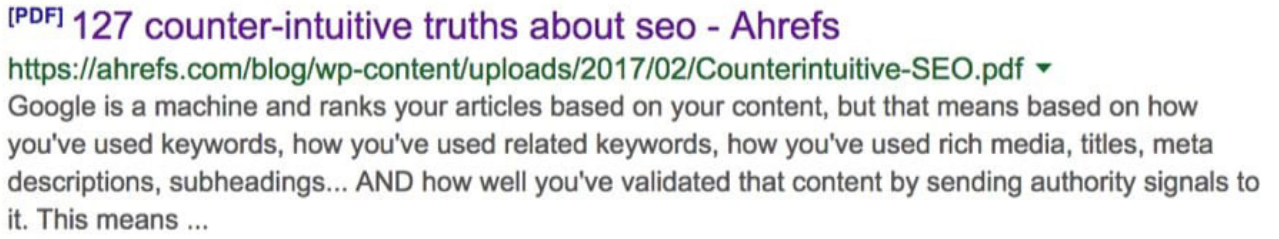
Примечание. Как видите, был исключен сайт ahrefs.com из результатов с помощью оператора исключения (-), а также исключил слово [pinterest], потому что по запросу выдаётся много результатов с сайта Pinterest, которые не имеют отношения к нашей задаче. Можно было исключить только pinterest. com (-pinterest.com), но у него много доменов и поддоменов. Исключение слова [pinterest] лучшим способ приведения результатов к нормальному виду.

Поиск нежелательных файлов и страниц на своём сайте (о которых вы могли забыть)

На сайте часто находятся множество документов(PDF, документы Word, презентации PowerPoint, текстовые файлы и т.д.), поэтому администраторам трудно контролировать их количество, а тем более содержимое: Оператор filetype: поможет их найти подобные файлы.



Примечание. Аналогичная функциональность у оператора ext:
Нашли один файл

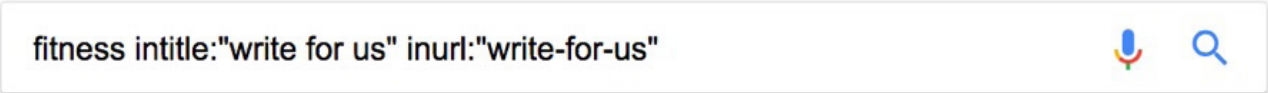


Комбинируя несколько операторов, можно одновременно выводить результаты для разных типов файлов.

Примечание. Этот оператор также поддерживает различные форматы .asp, .php, .html и др. Важно удалять подобные файлы или деиндексировать их для поисковых роботов.

Поиск возможностей для гостевой публикации

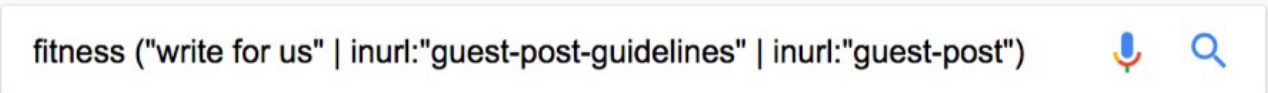
Возможно осуществить поиск сайта по его содержимому. Найдем блоги, которые просят опубликовать статью.



Применим более творческий подход. Не ограничивайтесь одной фразой, используйте подобные поисковые запросы:

- `[become a contributor]`
- `[contribute to]`
- `[write for me]`
- `[guest post guidelines]`
- `inurl:guest-post`
- `inurl:guest-contributor-guidelines`
- и др.

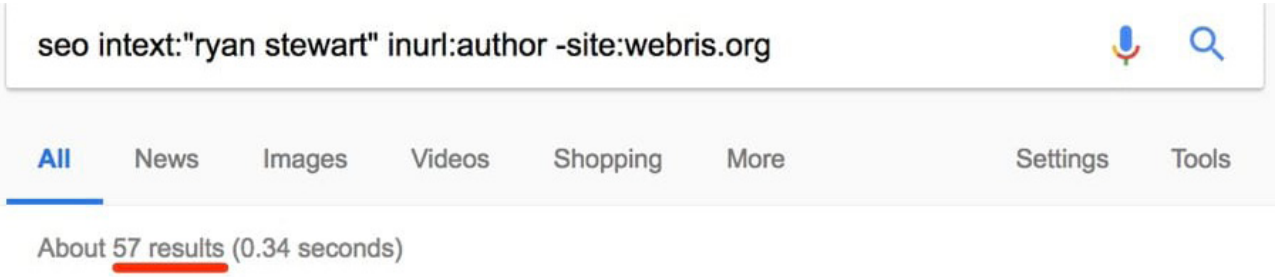
Можно искать всё сразу. Используем оператор (“|”) вместо AND, он делает то же самое.



Можно искать фразы с учётом необходимой тематики (сравните запрос выше и запрос представленный ниже).

Если необходимо сузить запрос до страны добавьте оператор site:.tld.

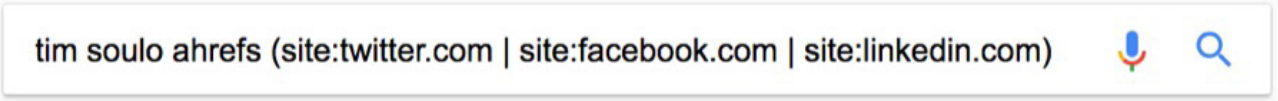
Если необходимо найти конкретного блогера.



Подобным образом найдутся все сайты, где публиковался данный автор.
Примечание. Был исключен сайт, которым владеет блогер.

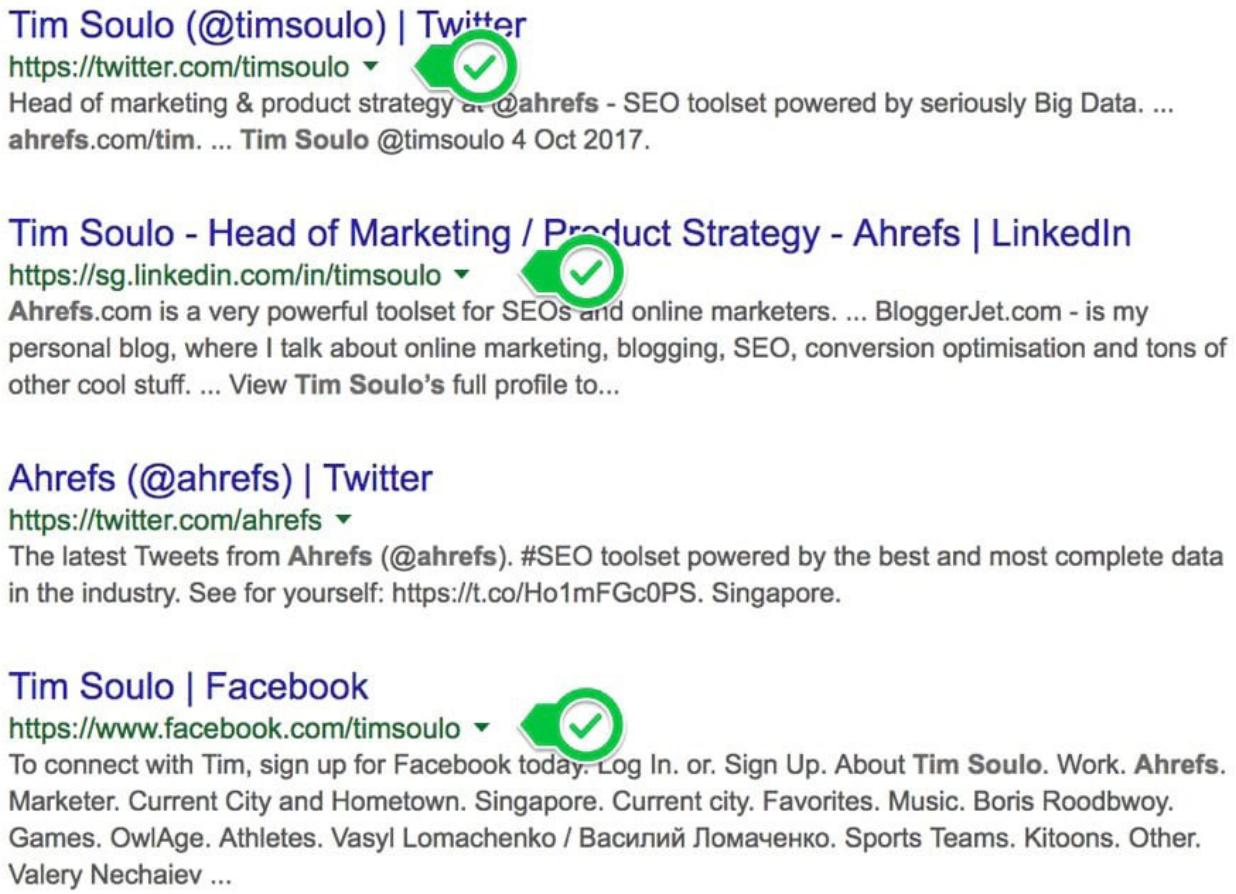
Поиск профилей в социальных сетях

Для поиска используйте следующий запрос:



Примечание. Имя человека обычно легко найти, а вот контактную информацию сложно.

Представим четыре лучших результата:



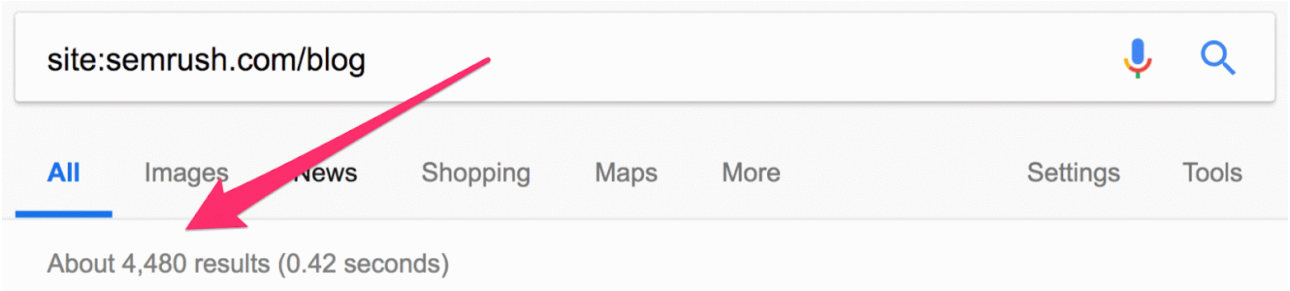
Попробуйте найти почту и осуществить поиск по почте. На каких сайтах зарегистрирован человек.

Проверка, как часто публикуется новый контент

Большинство блогов находятся в подпапке или поддомене, например:

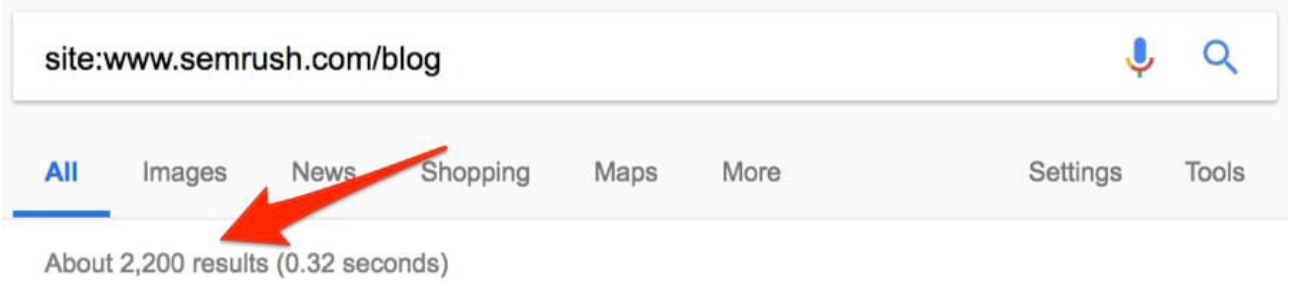
- `ahrefs.com/blog`
- `blog.hubspot.com`
- `blog.kissmetrics.com`

Это позволяет легко проверить, насколько регулярно конкуренты публикуют новый контент. Проверим на сайте SEMrush.

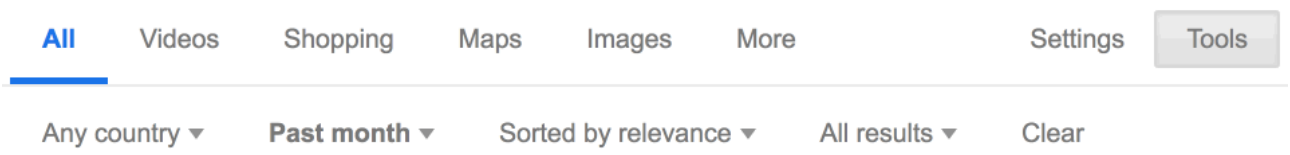


Похоже, у них уже около 4500 статей. Но это не совсем так. Сюда входят версии блога на разных языках, которые находятся на поддоменах.

Отфильтруем их.

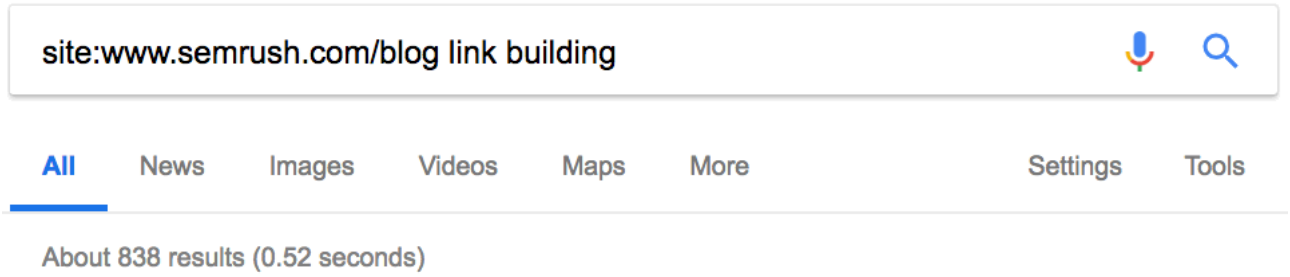


Это больше похоже на правду: около 2200 постов. Посмотрим, сколько опубликовано за последний месяц. Поскольку оператор daterange: больше не работает, используем встроенный фильтр Google.



Примечание. Можно указать любой диапазон дат. Просто выберите «Custom».

Оператор site: в сочетании с поисковым запросом покажет, сколько статей опубликовано по определённой теме.[1]



4. Способы работы с поисковиком DuckDuckGo

DuckDuckGo (сокр. DDG) – поисковая система, придающая особое значение обеспечиванию конфиденциальности пользователей и отказу от «пузыря фильтров» персонализированных результатов поиска. DuckDuckGo также уделяет особое внимание выдаче наилучших результатов, а не наибольшего их количества, и генерирует результаты, используя более 400 источников, включая ключевые краудсорсинговые сайты, такие как Википедия, а также другие поисковые системы, среди которых Bing, Yahoo!, Яндекс и Yummly.

Каждое посещение страницы, найденной поисковой системой Google, связано с тем фактом, что все ключевые слова, введенные пользователем для доступа к ней, и их IP-адрес отправляются на сервера поискового гиганта. Этой информации достаточно, чтобы идентифицировать пользователя Интернета. И нет, приватный режим вас не спасёт.

Работа поисковой системы DuckDuckGo основана на скрытности, предотвращает отправку IP-адреса и условий поиска на веб-сайт, который посещает пользователь. В результате владелец веб-сайта знает, что его посетил интернет-пользователь, но не имеет данных, позволяющих идентифицировать его, а также не знает, что он ввёл в поисковую строку, чтобы попасть на эту конкретную страницу.

DuckDuckGo получает результаты поиска двумя способами. Первый – это запатентованный робот DuckDuckBot, который просматривает Интернет в поисках веб-сайтов, наиболее релевантных запросу. В то же время поисковая система получает результаты примерно из 400 источников. Среди них есть и другие поисковые системы, такие как Bing или Yahoo, а также сервисы в виде Википедии.

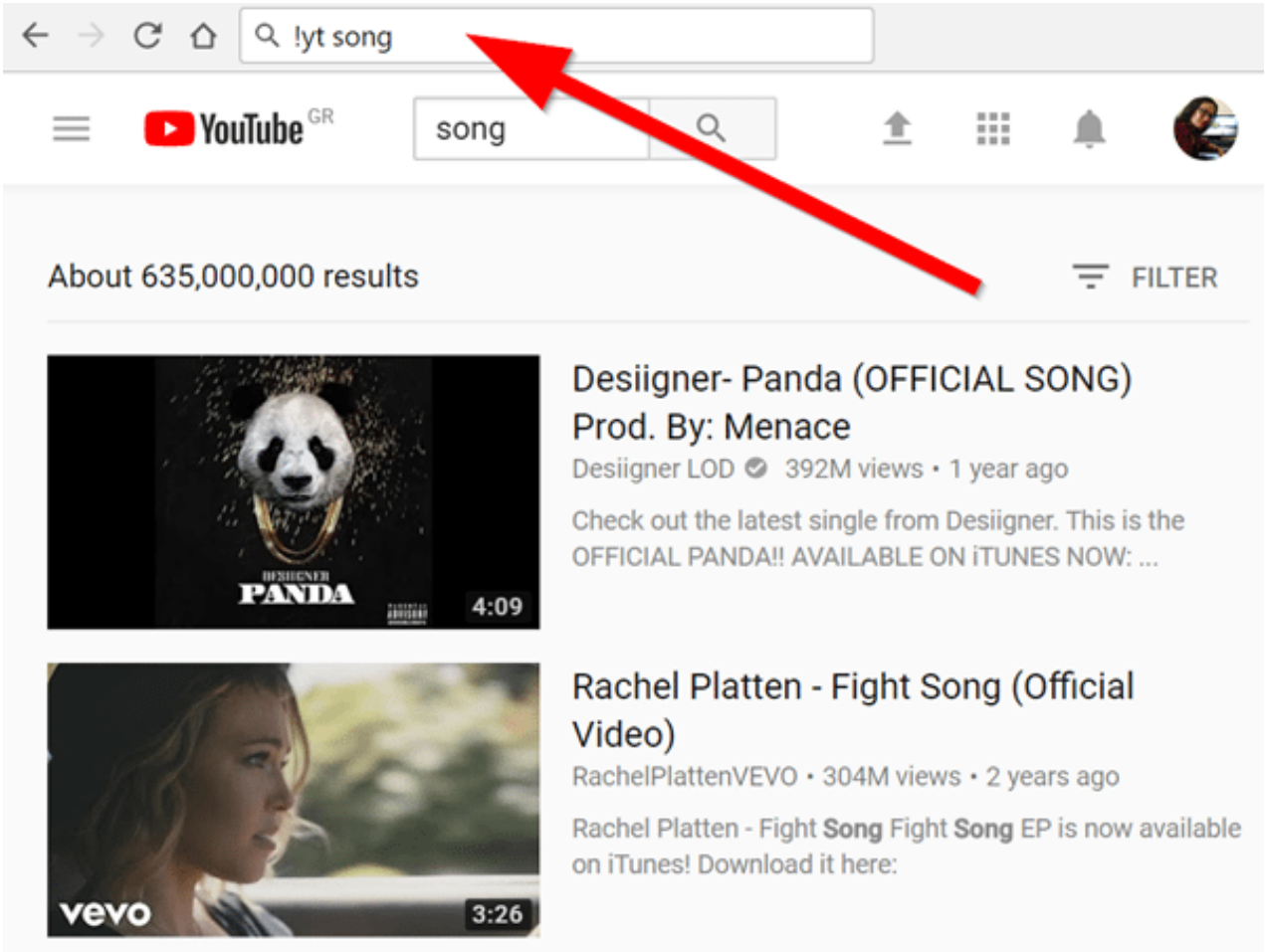
Bangs (Bangs запросы)

Bangs – одна из самых интересных функций, которые может предложить DuckDuckGo – конечно, помимо большей конфиденциальности поиска. Это ярлыки, которые сокращают путь поиска в интернет-магазинах или на порталах. Например, чтобы увидеть предложение айфонов на Amazon, просто введите в строку поиска «!a iPhone». Функция великолепна своей простотой и становится интуитивно понятной уже после нескольких применений.

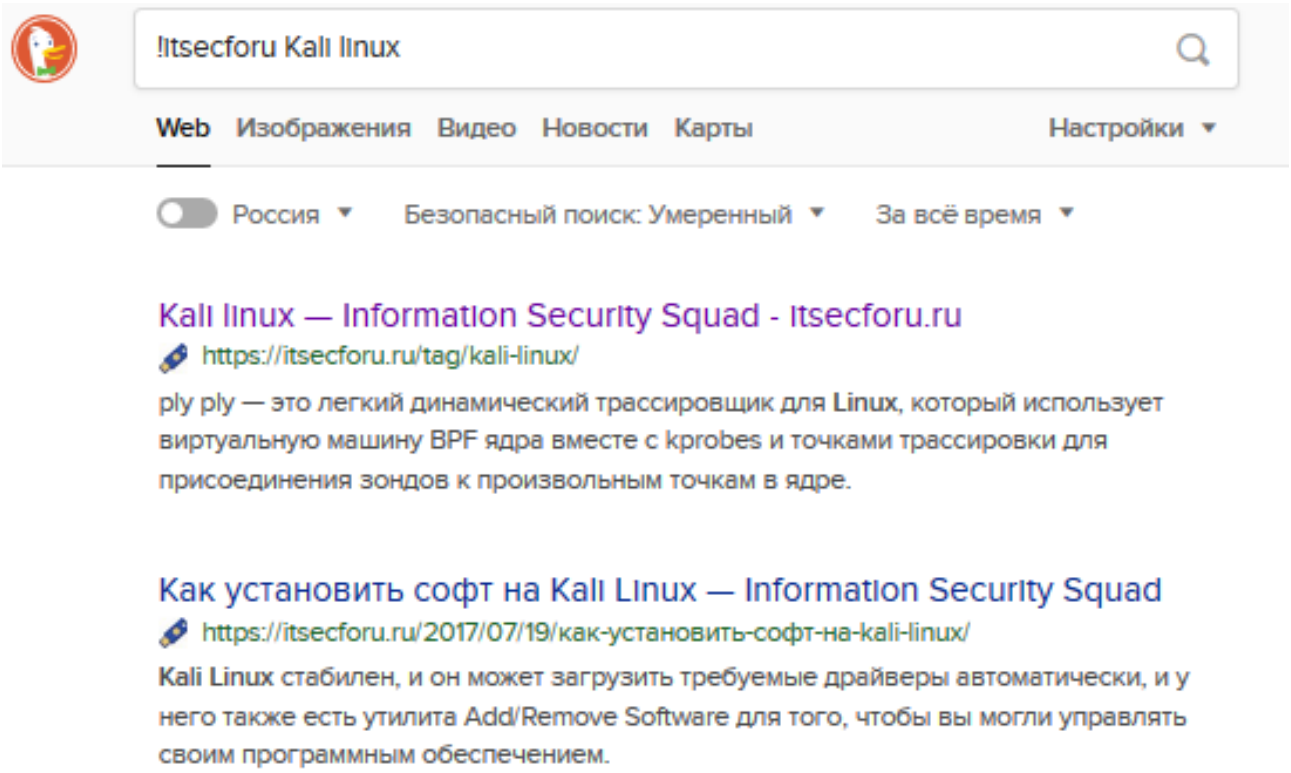
Рассмотрим несколько примеров использования *Bangs!* В DuckDuckGo необходимо использовать восклицательный знак в адресной строке, за которым следует поисковой запрос. Например, с помощью «!yt song» мы будем искать по ключевому слову «песня» только на YouTube.

---

1 Неизвестный GOOGLE: 42 оператора расширенного поиска Google. URL: https://oko-planet.su/politik/politwar/613911-neizvestnyy-google-42-operatora-rasshirennogo-poiska-google-polnyy-spisok.html.



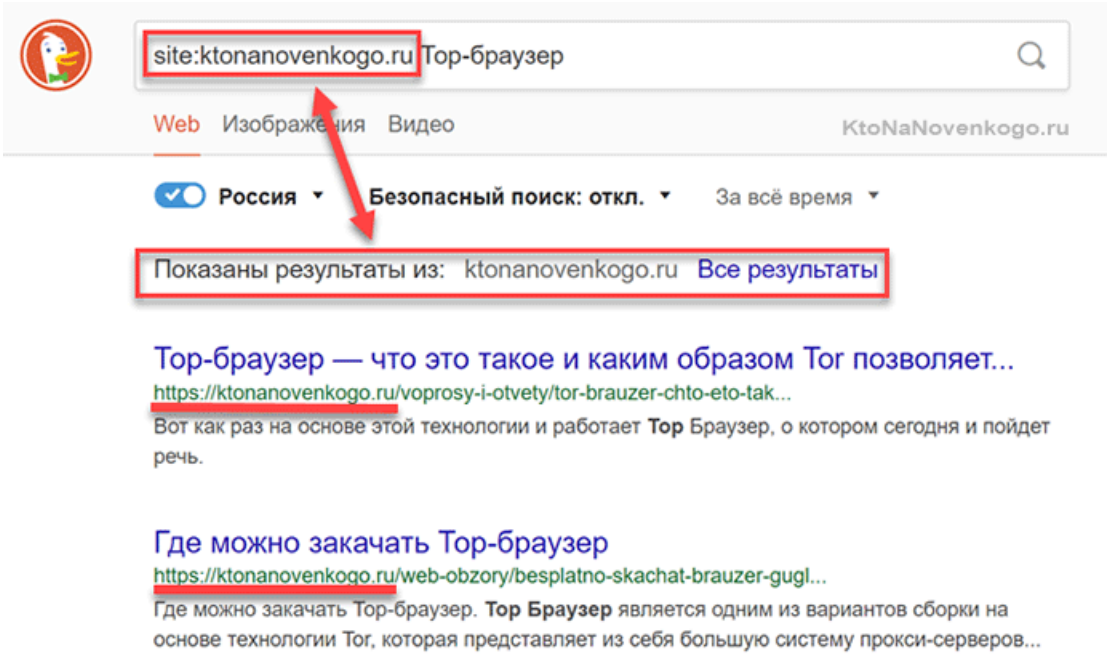
Поиск статей про Kali Linux в блоге «!itsecforu kali linux»



Для Wikipedia можно использовать «**!w linux**». Полный список, распределенный по категориям, представлен на сайте https://duckduckgo.com/bangs#bangs-list.

Продвинутые запросы DuckDuckGo

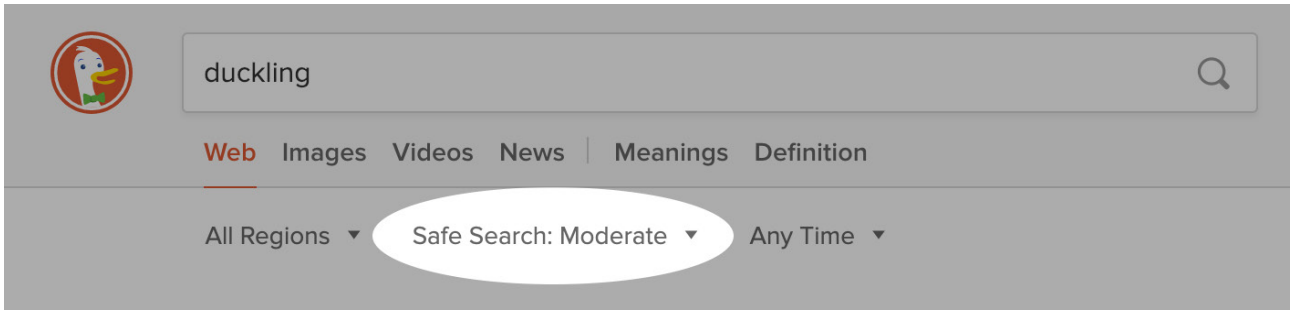
DuckDuckGo поддерживает синтаксис поиска, который можно использовать для точной настройки запросов, функциональность похожа на продвинутый поиск в Google, но имеет специфику.



Поисковые операторы

Пример	Описание
cats dogs	Поиск по запросу «кошки и собаки»
«cats and dogs»	Точный поиска по всем трем словам одновременно «кошки и собаки», если результаты не найдены будут предложены более подходящие
cats -dogs	Исключить из результатов собак
cats filetype:pdf	PDF-файлы о кошках. Поддерживаемые типы файлов: pdf, doc(x), xls(x), ppt(x), html
dogs site:example.com	Страницы о собаках с сайта example.com
cats -site:example.com	Страницы о кошках, кроме example.com
intitle:dogs	В заголовке страницы есть слово «собаки»
inurl:cats	URL страницы содержит слово «кошки»

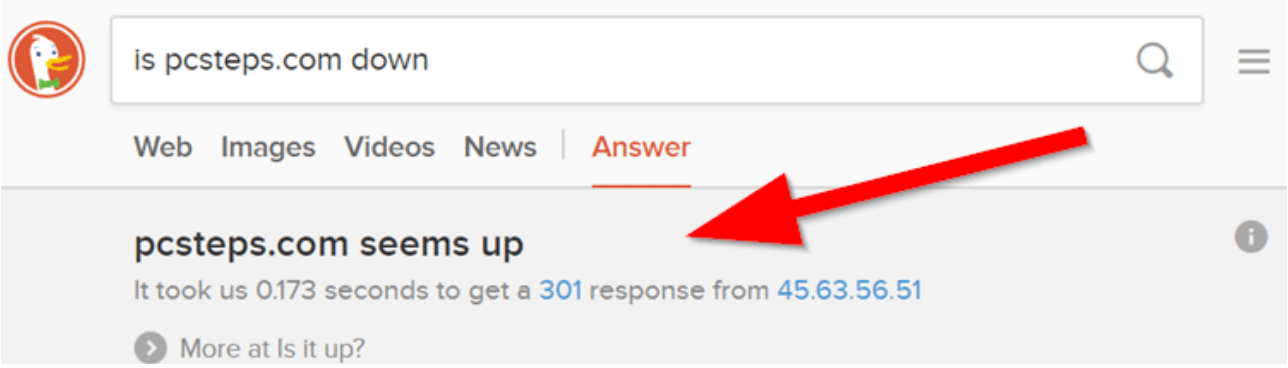
Добавьте **!safeon** или **!safeoff** в конец поиска, чтобы включить или выключить безопасный поиск для этого поиска(контент для взрослых).



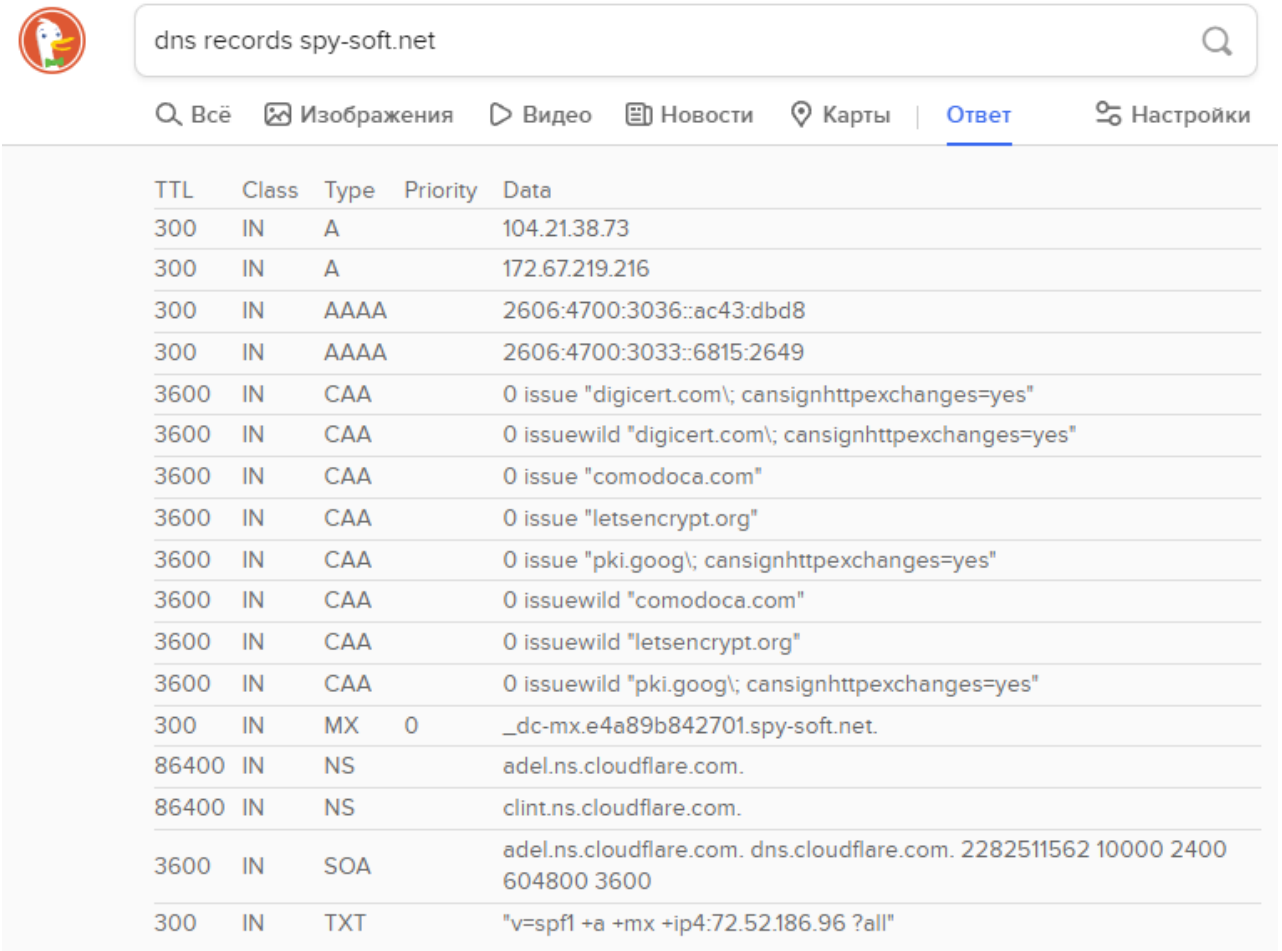
Вспомогательные функции

Простейший запрос к DDG будет выглядеть так «ip». Он выводит на экран ваш IP-адрес, местоположение и даже почтовый индекс.

Проверим работоспособность сайта. DDG ответит конкретными подробностями и информацией о пинге.



Более сложный запрос. Он покажет DNS-записи, которые относятся к домену spy-soft.net. **dns records spy-soft.net**



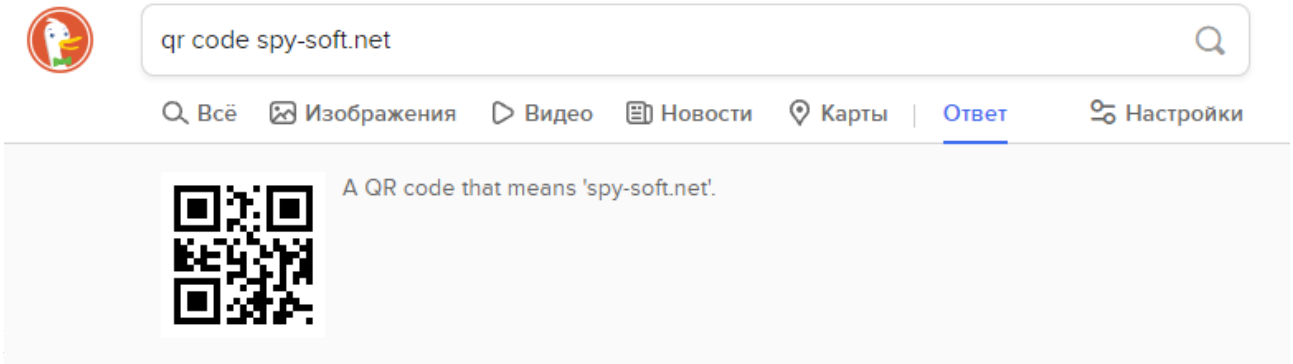
TTL	Class	Type	Priority	Data
300	IN	A		104.21.38.73
300	IN	A		172.67.219.216
300	IN	AAAA		2606:4700:3036::ac43:dbd8
300	IN	AAAA		2606:4700:3033::6815:2649
3600	IN	CAA		0 issue "digicert.com\; cansignhttpexchanges=yes"
3600	IN	CAA		0 issuewild "digicert.com\; cansignhttpexchanges=yes"
3600	IN	CAA		0 issue "comodoca.com"
3600	IN	CAA		0 issue "letsencrypt.org"
3600	IN	CAA		0 issue "pki.goog\; cansignhttpexchanges=yes"
3600	IN	CAA		0 issuewild "comodoca.com"
3600	IN	CAA		0 issuewild "letsencrypt.org"
3600	IN	CAA		0 issuewild "pki.goog\; cansignhttpexchanges=yes"
300	IN	MX	0	_dc-mx.e4a89b842701.spy-soft.net.
86400	IN	NS		adel.ns.cloudflare.com.
86400	IN	NS		clint.ns.cloudflare.com.
3600	IN	SOA		adel.ns.cloudflare.com. dns.cloudflare.com. 2282511562 10000 2400 604800 3600
300	IN	TXT		"v=spf1 +a +mx +ip4:72.52.186.96 ?all"

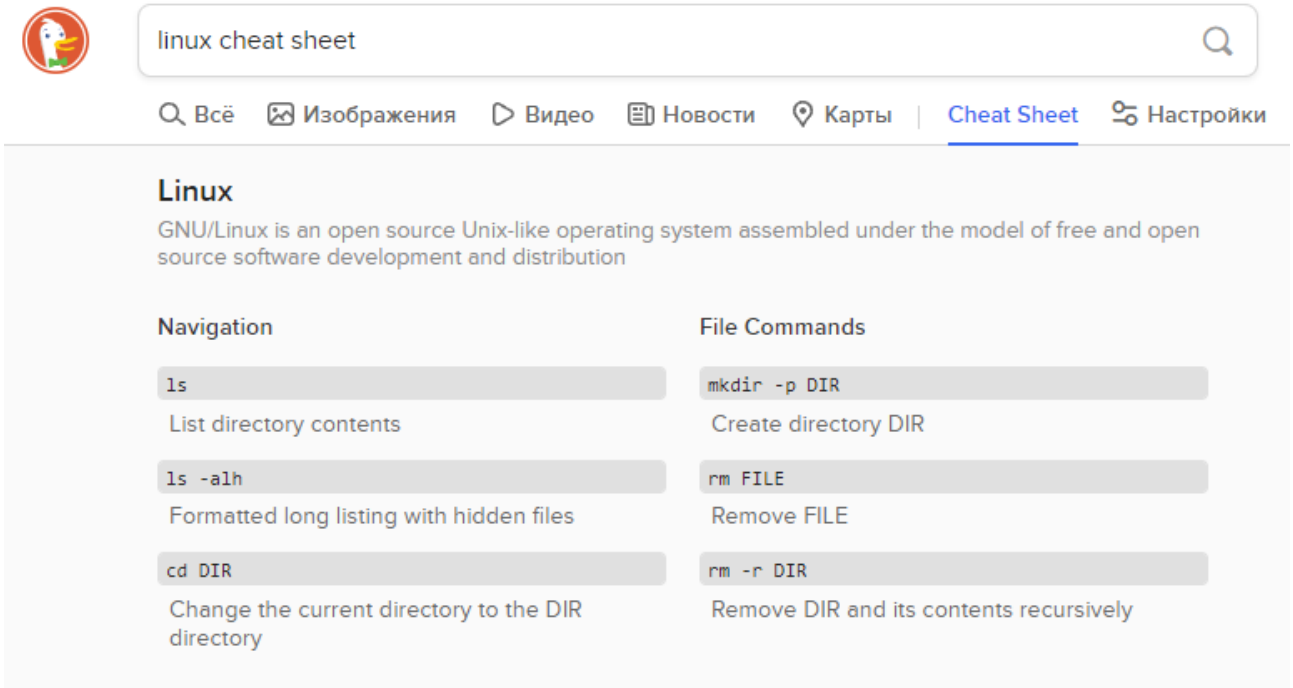
Получить информацию о твиттере сайта spy-soft.net: **@spysoftnet**.

Или проверить валидность электронного адреса одного из его редакторов: **validate spysoftnet@gmail.com**

Для сокращения ссылки на сайт воспользуйтесь контракцией **shorten https://spy-soft.net/xranenie-parolej-android/**

Существует возможность генерации QR кода «**qr code spy-soft.net**»





DuckDuckGo предоставляет еще ряд возможностей для разработчиков и администраторов например работа с HTML, цветом и CSS и др.

Генератор паролей и хешей в DuckDuckGo

DuckDuckGo поможет вам, если нужен стойкий пароль заданной длины:
password 10

DDG может сгенерировать кодовую фразу:
random passphrase

Или закодировать данные с помощью алгоритма Base64:
base64 encode <текст>

Генерация хеша:
md5 <текст>**sha** <текст>

Если хеш уже есть, но вы не знаете, каким алгоритмом он сгенерирован:
hash <хеш>

Горячие клавиши

Еще одна очень приятная особенность DDG – горячие клавиши. Это означает, что для управления внутри «утки» не требуется мышь, все действия можно осуществлять с помощью клавиатуры. Ниже приведен список доступных команд :

«j» – перемещаться по результатам вниз.
«k» – листать результаты вверх.
«v» – посмотреть выбранную ссылку.
«h» – быстро переместиться в строку для введения нового запроса.
«escape» – закрыть поисковую строку.
«t» – быстро переместиться наверх.
«m» – бысто выбрать первый результат из списка.
«d» – начать работу с конкретным сайтом (который выделен).

Практические задания

1. Найдите маму монстра на Amazon, используя Bangs запросы.
2. Найдите Bangs сайта dw.com и выберите новости за последние 24 часа, относящиеся к вашей стране.
3. Выполните примеры из таблицы поисковых операторов.
4. Найдите официальный сайт вашей любимой музыкальной группы.
5. Найдите сайт, посвящённый компьютерной технике и комплектующим.
6. Сгенерируйте qr-code для произвольного сайта и для него же сгенерируйте короткую ссылку.
7. Выполните запросы в поисковых системах Yandex, Baidu, Google, DuckDuckGo и заполните таблицу. При этом используйте продвинутые запросы:
   - найдите официальный сайт вашей любимой музыкальной группы;
   - найдите сайт, посвящённый компьютерной технике и комплектующим;
   - издателя и разработчика игры «Братья пилоты»;
   - в каком году и где родился Мишель Нострадамус.

	Вид запроса	*Yandex*	*Baidu*	*Google*	*DuckDuckGo*
Вопрос					

5. Прохождение интерактивной игры с сюжетной линией, которая заключается в решении различных головоломок и логических заданий

В правоохранительные органы поступила информация о том, что в одной из социальной сетей действует аккаунт лица, распространяющего информацию, содержащую агрессивные призывы к совершению экстремистских действий политического (религиозного или иного) содержания.

Задание 1. Получить доступ к аккаунту фигуранта

Данное задание предусматривает отработку и закрепление теоретических знаний и практических навыков мониторинга социальных сетей и мессенджеров в рамках следующих тем:

1.1. Понятие и общая характеристика преступлений в сфере компьютерной информации по законодательству Российской Федерации.

1.2. Криминологическая характеристика и профилактика компьютерных преступлений.

2.1. Сеть Интернет как источник информации. Веб-ресурсы и методы получения доступа к ним.

3.1. Криминалистическая характеристика преступлений в сфере компьютерной информации.

3.2. Особенности первоначального этапа расследования преступлений в сфере компьютерной информации.

5.1. Средства анонимизации и деанонимизации в сети Интернет.

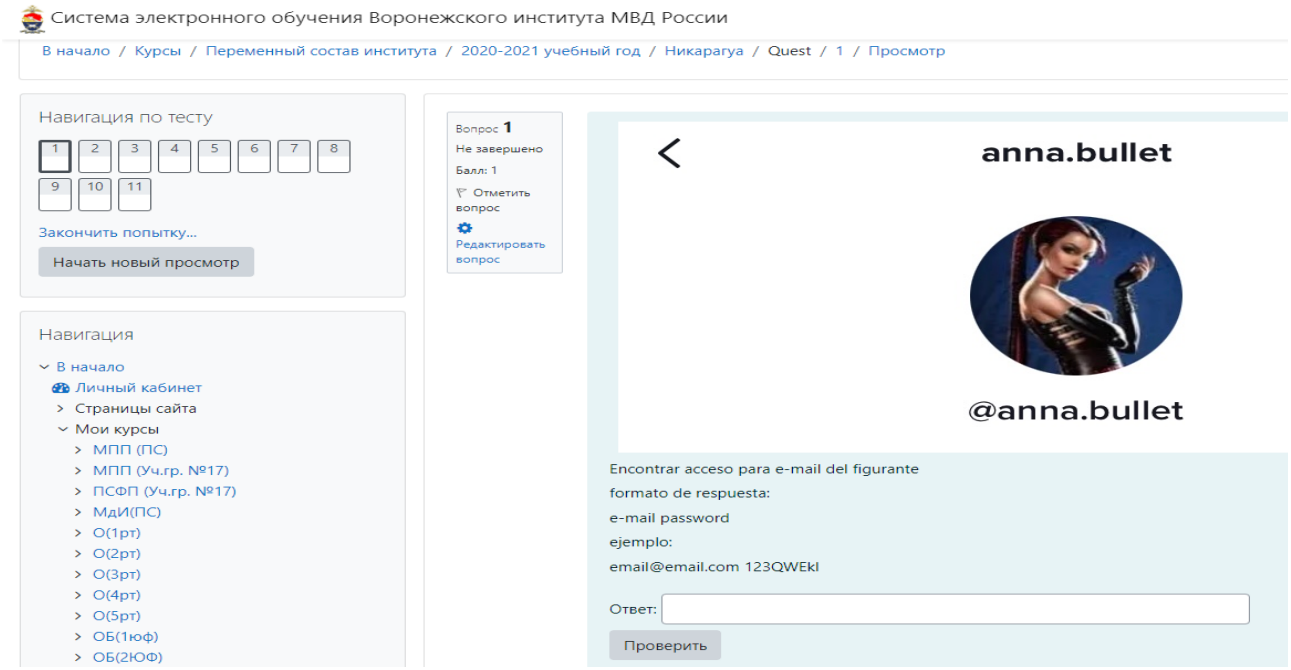
5.2. Использование веб-ресурсов для получения данных о недвижимости, транспорте, физических и юридических лицах.

5.3. Поиск и анализ информации в сети Интернет в целях выявления преступлений в сфере компьютерной информации.

Слушателям объявляется, что на ресурсах одной социальной сети неустановленные лица размещают материалы экстремистской и террористической направленности, необходимо установить их и привлечь к ответственности:

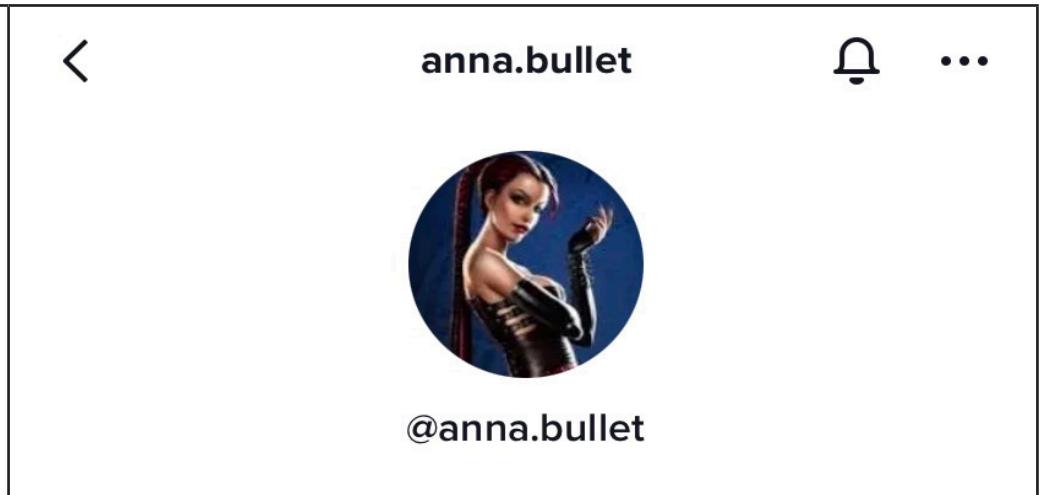
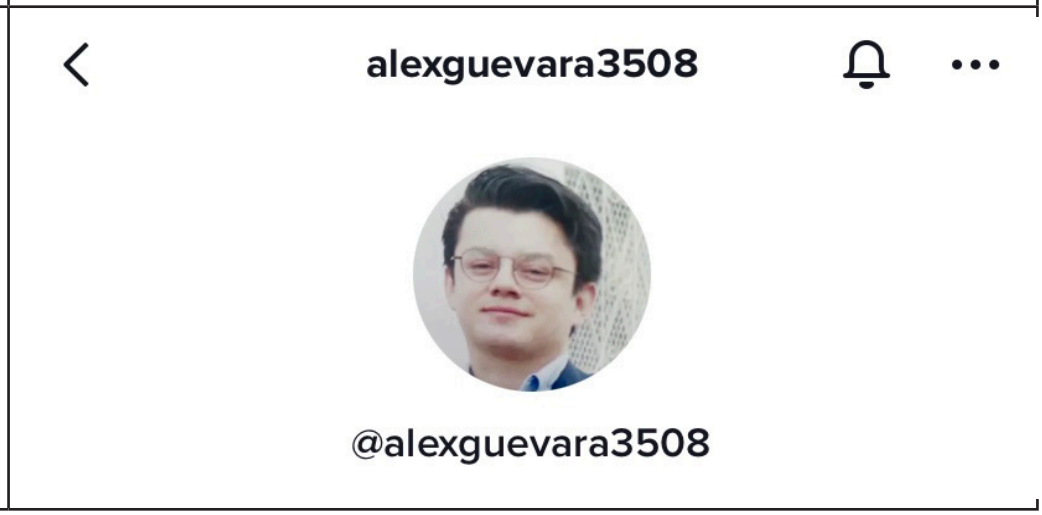
Encontrar acceso para e-mail del figurante.
formato de respuesta:
e-mail password
ejemplo:
email@email.com 123QWEkl

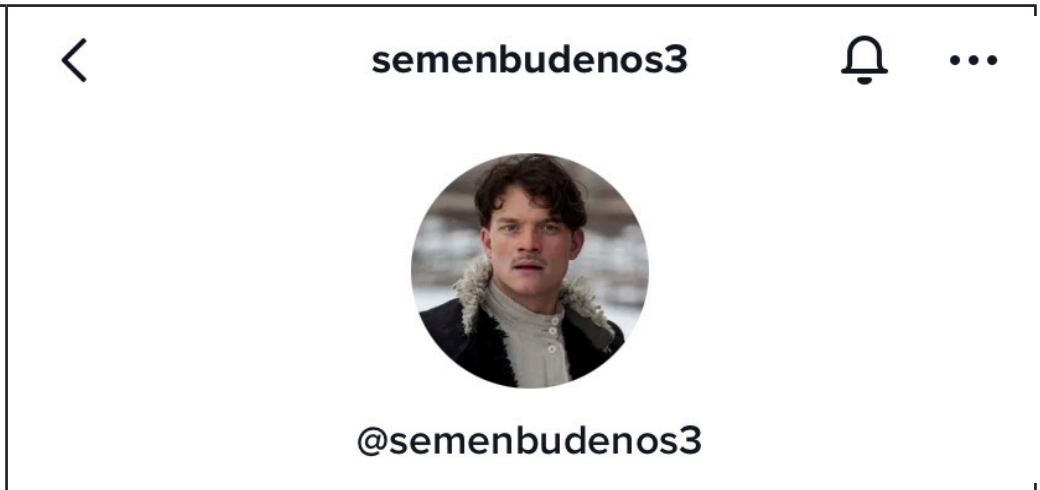
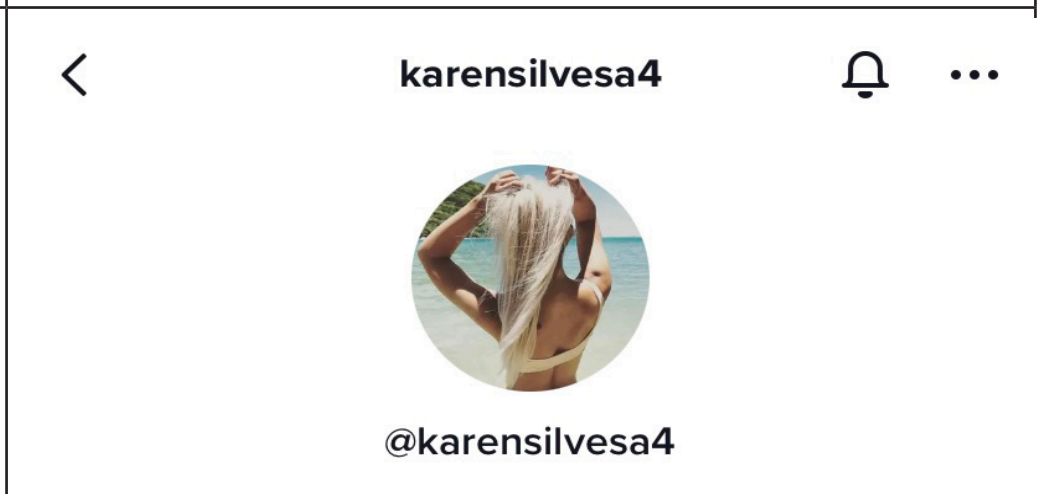
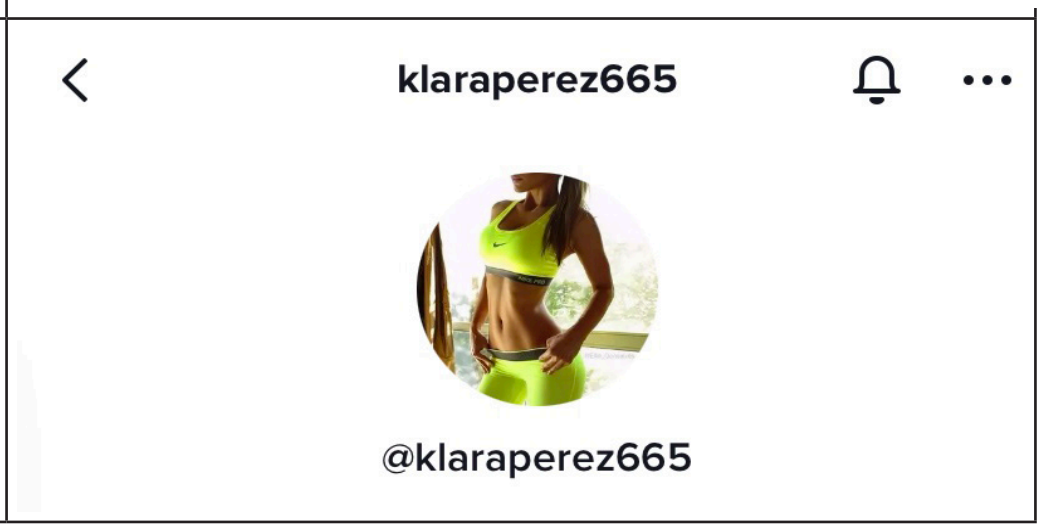
Перевод текста задания:
Получить доступ к **e-mail** фигуранта
Формат ответа:
e-mail password
Пример:
email@email.com 123QWEkl



Снимок экрана с первым заданием для сюжетной линии № 1

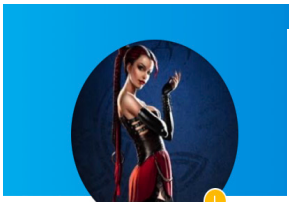
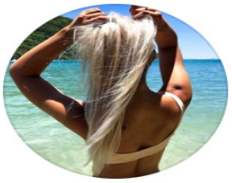
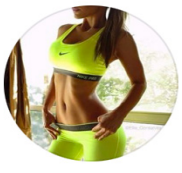
На данном этапе слушатель (подгруппа) на странице Системы электронного обучения Воронежского института МВД России в зависимости от выбранной сюжетной линии получает один из 5 снимков экрана из социальной сети TikTok:

Первая сюжетная линия:	
Вторая сюжетная линия:	

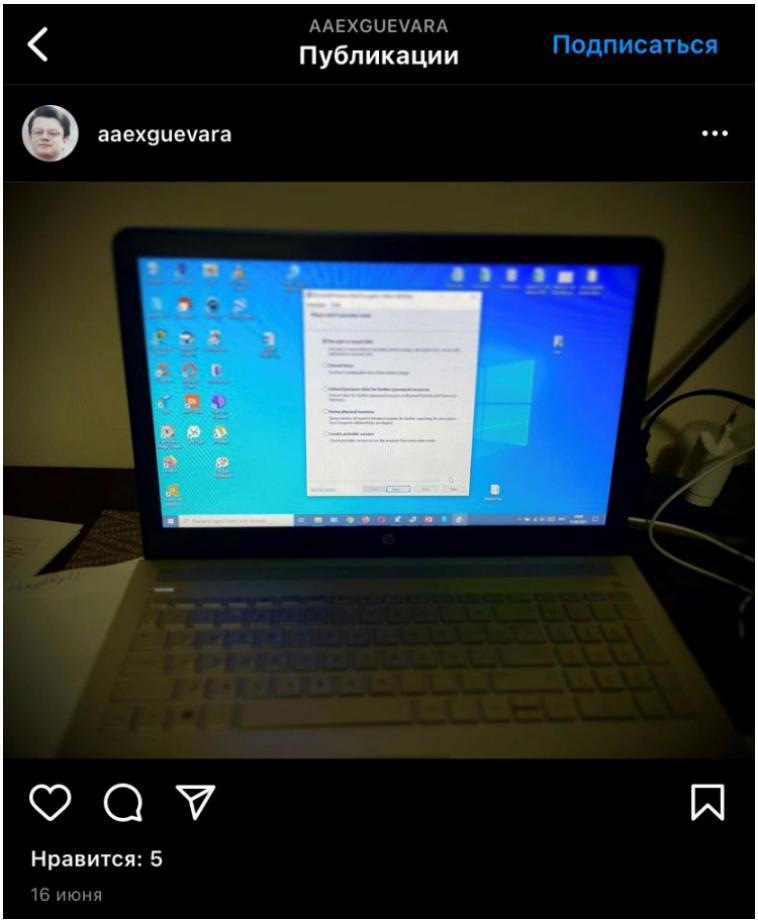
Третья сюжетная линия:	
Четвертая сюжетная линия:	
Пятая сюжетная линия:	

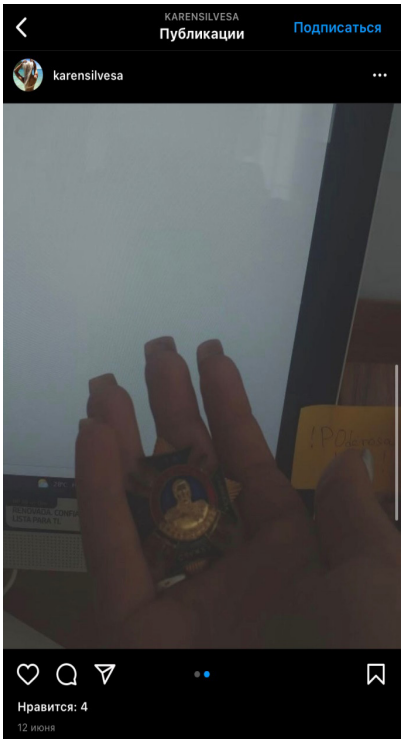
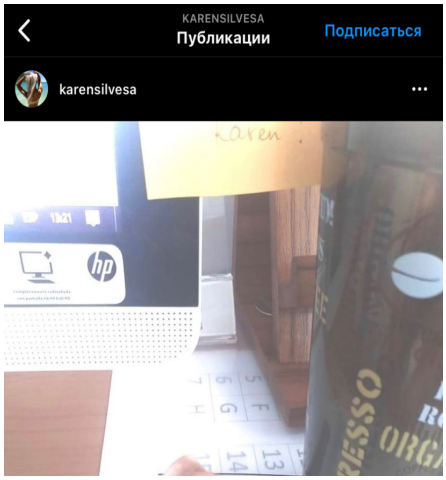
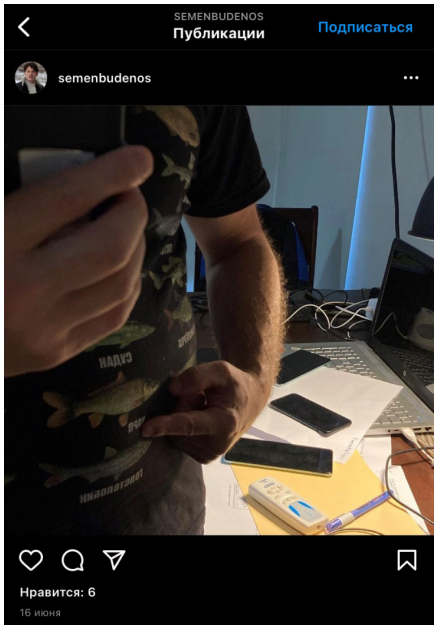
В ходе решения задания слушатели на основе имеющихся исходных данных (фотография, профиль и никнейм) должны обнаружить страницы игрового фигуранта на Facebook, Instagram, Twitter, WhatsApp, Skype, Viber и проанализировать их содержимое. Ответ на первое задание будет содержаться в открытом доступе на аккаунтах игрового персонажа в Skype и Instagram.

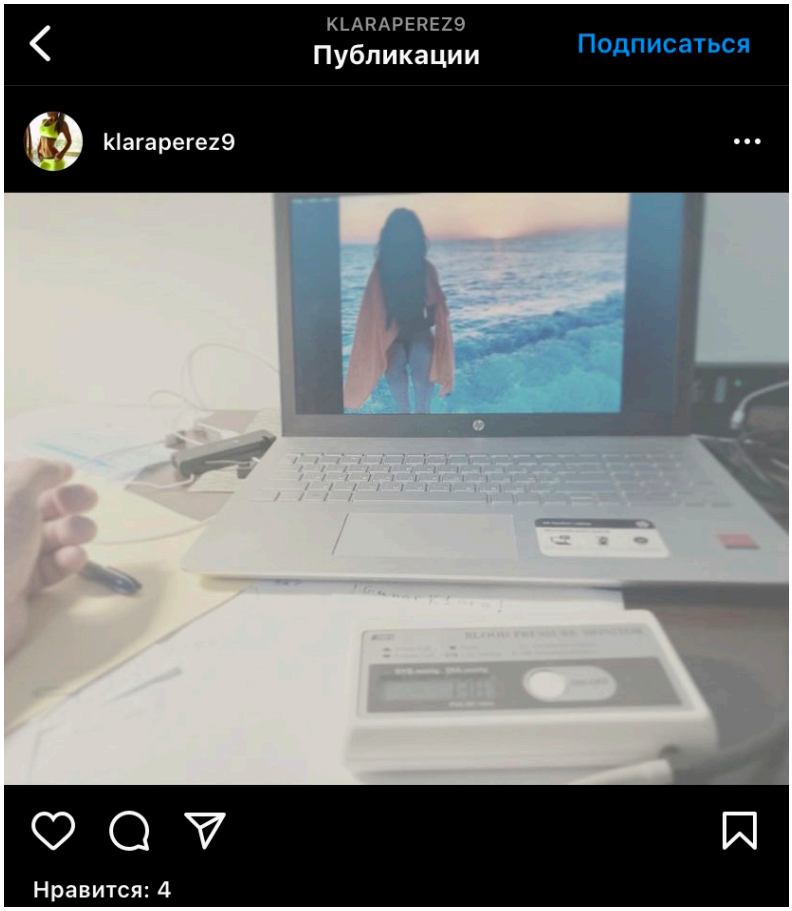
Учетные данные Skype содержат искомый адрес электронной почты с технической ошибкой, которую слушатели при дальнейшем прохождении должны выявить и устранить.

Первая сюжетная линия: (отсутствует символ «@» – коммерческое «эт»)	 Anna Bullet Была в сети несколько дней Логин в Скайпе live:.cid.3a84071fb1ef242e Мобильный +50585993846 Местоположение bulletanna8gmail.com, NI Дата рождения 10.04
Вторая сюжетная линия: (адрес электронной почты указан без ошибок)	 guevara alex Alex.guevara.lord@gmail.com
Третья сюжетная линия: (отсутствует символ «@» – коммерческое «эт»)	 Karen Silvesa Karensilvesa97gmail.com
Четвертая сюжетная линия (отсутствует символ «@» – коммерческое „эт“ и точка, отделяющая доменную зону «com»)	 Semen Budenos Semenbudenosgmailcom Нет общих контактов
Пятая сюжетная линия: (отсутствует символ «@» – коммерческое «эт» и доменная зона «com»)	 Perez Klara Kp578746gmail Нет общих контактов

На размещенных в Instagram фотографиях игрового персонажа содержится в визуально искажённом формате искомый пароль.

Первая сюжетная линия: (пароль указан справа от экрана ноутбука, требует корректировки резкости и контраста снимка)	
Вторая сюжетная линия: (пароль указан слева от ноутбука, требует корректировки резкости и контраста снимка)	

Третья сюжетная линия: (пароль размещен на двух фотографиях, требует корректировки резкости и контраста и объединения частей с двух снимков)	 
Четвертая сюжетная линия (пароль размещен вертикально между двумя телефонными аппаратами, требуется зеркально отобразить изображение)	

Пятая сюжетная линия: (пароль размещен у нижнего среза корпуса от ноутбука, требует корректировки резкости и контраста снимка)	

После ввода в Систему электронного обучения Воронежского института МВД России правильного ответа слушателям на экран выводится сообщение следующего содержания:

«El acceso al usuario es exelente! Seguramente hay muchas cosas interesantes! Es bueno, que hay programas especiales...»

Перевод: «Доступ к аккаунту – это замечательно! Наверняка там много интересного! Хорошо, что есть специальные программы...»)

Слушатели получают возможность перейти ко второму заданию.

ВАЖНО! В рамках решения данного задания слушатели должны обнаружить аккаунты игрового персонажа на многих ресурсах сети Интернет, осуществить анализ их содержимого. Данная информация будет необходима для решения последующих этапов интерактивной игры.

Задание 2. На основе переписки установить название группы в социальной сети, где выкладываются товары, подлежащие закупке

Данное задание предусматривает отработку и закрепление теоретических знаний и практических навыков по использованию социальных сетей и ресурсов Даркнет в рамках следующих тем:

2.1. Сеть Интернет как источник информации. Веб-ресурсы и методы получения доступа к ним.

2.2. Программные и программно-аппаратные средства, используемые для аналитической обработки информации. .

2.3. Обнаружение передачи скрытой информации и извлечение из содержащего её сообщения.

3.2. Особенности первоначального этапа расследования преступлений в сфере компьютерной информации.

4.1. Введение в информационную безопасность.

4.3. Методы и средства защиты от несанкционированного доступа к информации в компьютерных системах.

4.4. Выявление и сохранение значимой информации со средств вычислительной техники и программного обеспечения.

4.5. Основы информационной безопасности телекоммуникационных систем.

5.1. Средства анонимизации и деанонимизации в сети Интернет.

5.2. Использование веб-ресурсов для получения данных о недвижимости, транспорте, физических и юридических лицах.

5.3. Поиск и анализ информации в сети Интернет в целях выявления преступлений в сфере компьютерной информации.

Слушатели после успешного завершения первого задания переходят к решению второго:

En la base de la mensajeria encontrar el nombre del grupo en la red social, donde se colocan las mercancias,que seran compradas.

formato de respuesta:

nombre del grupo

ejemplo*:*

amantes del poder

Перевод текста задания:

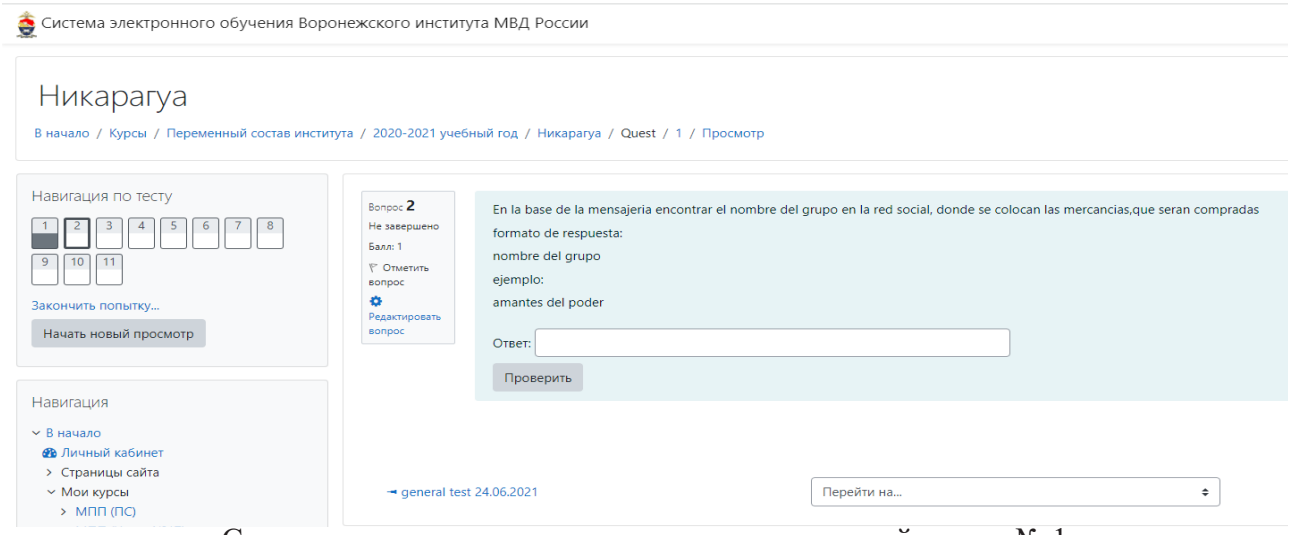
На основе переписки установить название группы в социальной сети, где выкладываются товары, подлежащие закупке

Формат ответа:

Имя группы

Пример:

Любители власти

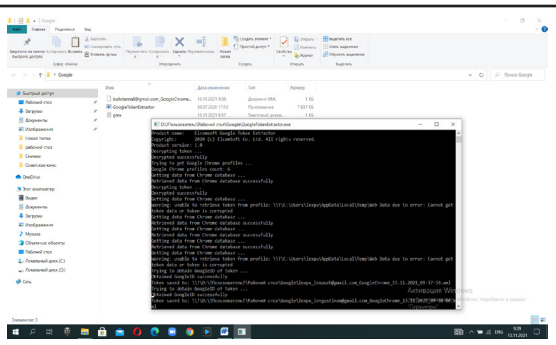
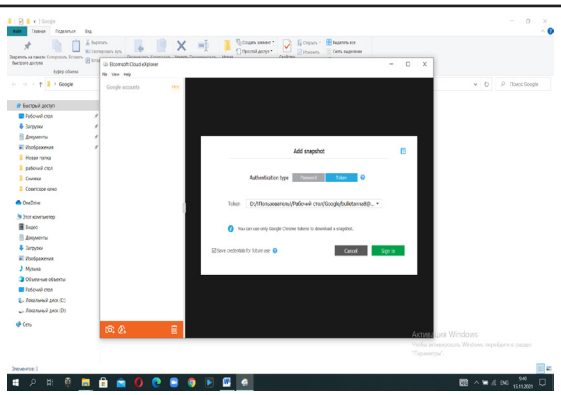
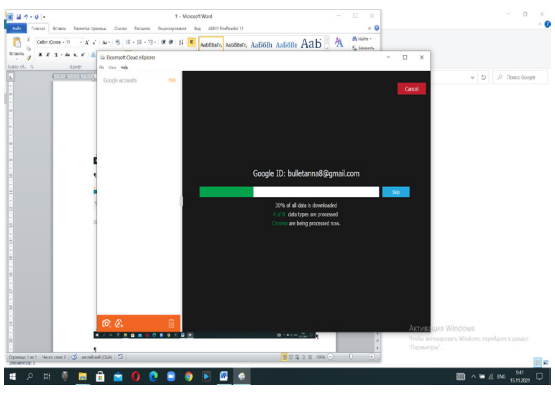


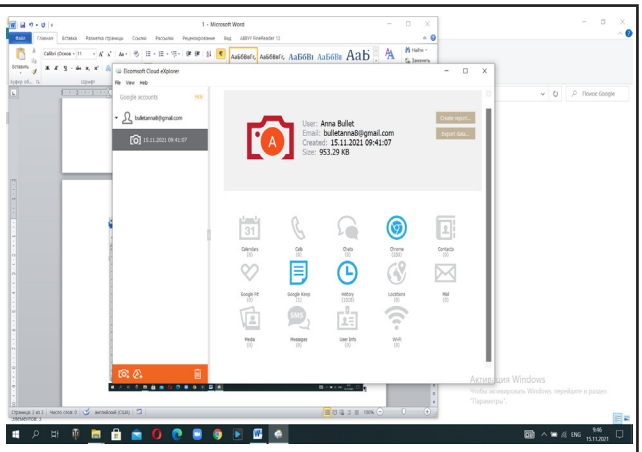
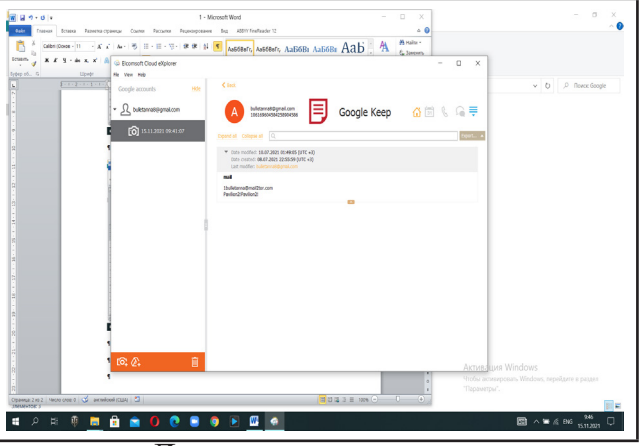
Снимок экрана со вторым заданием для сюжетной линии № 1

Основные этапы решения:

1. Анализ содержимого **Google-аккаунта:**

Слушателю необходимо авторизоваться с помощью браузера Chrome на ресурсах Gmail.com. Далее:

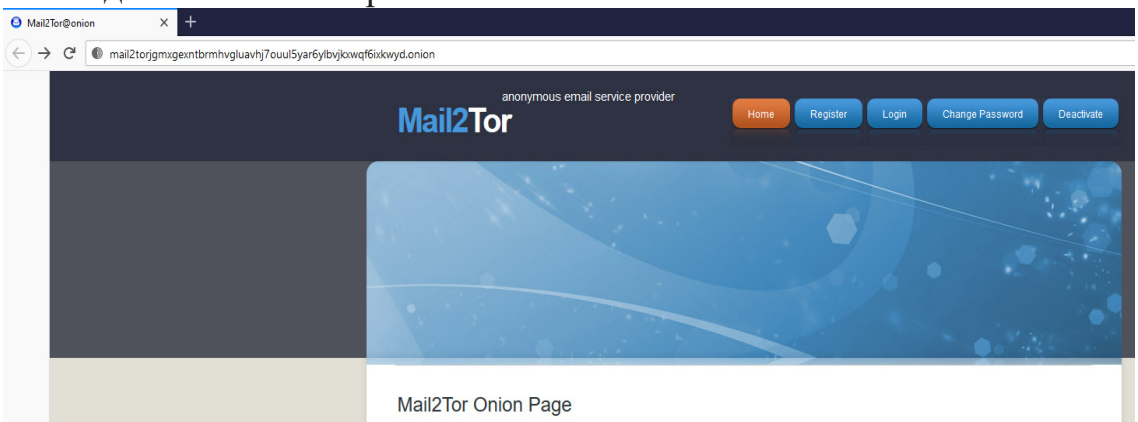
Решение на примере первой сюжетной линии	
с помощью специальной утилиты Elcomsoft Cloud eXplorer обнаруживает токен авторизации к облачным сервисам Google	
выбирает токен от учетной записи пользователей Google	
скачивает данные, доступные в учётной записи пользователей Google	

просматривает и анализирует данные, доступных в учётной записи пользователей Google, получив доступ к этой информации в программе «одного окна»	
в разделе Google Keep обнаруживает заметку с логином и паролем от почтового сервиса Mail2Tor	

2. Анализ содержимого почтового сервиса в Даркнете, для этого слушатель:

– исходя из названия почтового сервиса Mail2Tor, принимает решение о необходимости использования Tor-браузера,

– находит почтовый сервис Mail2Tor:



– с имеющимися данными авторизуется на данном почтовом сервисе:

– обнаруживает во вкладке отправленное письмо следующего содержания:

Первая сюжетная линия:	**Subject:** Una reunión **From:** 1bulletanna@mail2tor.com **Date:** Fri, July 9, 2021 10:44 pm **To:** pedro@secmail.pro **Priority:** Normal **Options:** View Full Header | View Printable Version ¡Hola! Publiqué una lista de armas y drogas en el grupo SurfNica$. Espero que todos recuerden cómo ver el archivo. reunirse en leon, como siempre, el último domingo del mes a la misma hora. adios hermanos) P.S. el poder y el dinero serán nuestros Привет! Я разместила список оружия и наркотиков в группе **SurfNica$.** Надеюсь, все помнят, как просматривать файл. Встретимся в Леоне, как всегда, в последнее воскресенье месяца в одно и то же время. До свидания, братья) P.S. Власть и деньги будут наши
Вторая сюжетная линия:	**Subject:** Una reunión **From:** alexguevara666@mail2tor.com **Date:** Thu, July 8, 2021 5:54 pm **To:** leon.sandero.mag@secmail.pro **Priority:** Normal **Options:** View Full Header | View Printable Version | Download this as a file ¡Hola! Publiqué una lista de armas y drogas en el grupo Mineros de Nicaragua. Espero que todos recuerden cómo ver el archivo. nos reunimos en nuestro lugar donde siempre descansamos, como siempre, el último domingo del mes a la misma hora. adios hermanos) P.S. el poder y el dinero serán nuestros Привет! Я опубликовал список оружия и наркотиков в группе **Mineros de Nicaragua.** Надеюсь, все помнят, как просматривать файл. Собираемся на своем месте, где всегда отдыхаем, как всегда, последнее воскресенье месяца в одно и то же время. До свидания, братья) P.S. Власть и деньги будут наши

<table>
<tr>
<td>Третья сюжетная линия:</td>
<td>
Subject: Una reunión
From: sembudenos3@mail2tor.com
Date: Thu, July 8, 2021 6:12 pm
To: frugel@mail.i2p
Priority: Normal
Options: View Full Header | View Printable Version | Download this as a file

¡Hola!
Publiqué una lista de armas y drogas en el grupo Caballería nicaragüense.
Espero que todos recuerden cómo ver el archivo.

nos reunimos en nuestro lugar donde siempre nos encontramos,
como siempre, el último domingo del mes a la misma hora.

adios hermanos)

P.S. El poder y el dinero serán nuestros

Перевод:
Привет! Я опубликовал список оружия и наркотиков в группе Caballería nicaragüense. Надеюсь, все помнят, как просматривать файл. Мы встречаемся у себя дома, где всегда встречаемся, как всегда, в последнее воскресенье месяца в одно и то же время.
До свидания, братья)
P.S. Власть и деньги будут наши
</td>
</tr>
<tr>
<td>Четвертая сюжетная линия:</td>
<td>
Message List | Unread | Delete | Edit Message as New

Subject: Una reunión
From: Ksilvesa4@mail2tor.com
Date: Thu, July 8, 2021 6:24 pm
To: fransec4@secmail.pro
Priority: Normal
Options: View Full Header | View Printable Version | Download this as a file

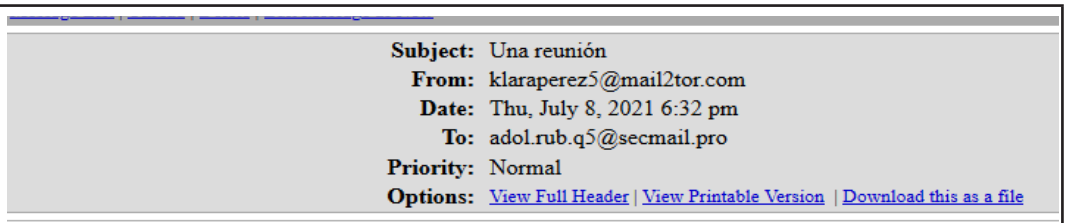
¡Hola!
Publiqué una lista de armas y drogas en el grupo Botella de pimienta.
Espero que todos recuerden cómo ver el archivo.

nos reunimos en el lugar donde nos encontramos para descansar regularmente,
como siempre, el último domingo del mes a la misma hora.

adios hermanos)

P.S. El poder y el dinero serán nuestros

Перевод:
Привет! Я разместил список оружия и наркотиков в группе Botella de pimienta. Надеюсь, все помнят, как просматривать файл. Мы встречаемся в том месте, где собираемся регулярно отдыхать, как всегда, в последнее воскресенье месяца в одно и то же время.
До свидания, братья)
P.S. Власть и деньги будут наши
</td>
</tr>
</table>

Пятая сюжетная линия:	 ¡Hola! Publiqué una lista de armas y drogas en el grupo Trompetistas alegres. Espero que todos recuerden cómo ver el archivo. nos reunimos en el lugar donde nos encontramos para descansar regularmente, como siempre, el último domingo del mes a la misma hora. adios hermanos) P.S. El poder y el dinero serán nuestros Перевод: Привет! Я разместил список оружия и наркотиков в группе **Trompetistas alegres**. Надеюсь, все помнят, как просматривать файл. Мы встречаемся там, где собираемся регулярно отдыхать, как всегда, в последнее воскресенье месяца в одно и то же время. До свидания, братья) P.S. Власть и деньги будут наши

После ввода в Систему электронного обучения Воронежского института МВД России правильного ответа слушателям на экран выводится сообщение следующего содержания:

«Valla, astutos, utilizan grupos abiertos, es interesante, en que estan esperanzados...»

Перевод: «Ишь, хитрецы, пользуются открытой группой, интересно, на что они надеются...»

Слушатели получают возможность перейти к третьему заданию.

ВАЖНО! В рамках выполнения данного задания слушатели должны обнаружить информацию, необходимую для решения заданий интерактивной игры на завершающем этапе:

– в почтовом сервисе Google аккаунта входящие сообщения от другого персонажа – Esperanza Grana (esper.grana@gmail.com) (задание № 11);

– в почтовом сервисе Mail2Tor факт направления неустановленному персонажу интерактивной игры (в каждой сюжетной линии отдельный фигурант) еще одного сообщения о необходимости перевода криптовалюты (задание № 9).

Задание 3. Извлечь содержимое заархивированного стегановложения

Данное задание предусматривает отработку и закрепление теоретических знаний и практических навыков по использованию стеганографических приложений и приложений для подбора паролей к файлам в рамках следующих тем:

2.1. Сеть Интернет как источник информации. Веб-ресурсы и методы получения доступа к ним.

2.2. Программные и программно-аппаратные средства, используемые для аналитической обработки информации. .

2.3. Обнаружение передачи скрытой информации и извлечение из содержащего её сообщения.

3.2. Особенности первоначального этапа расследования преступлений в сфере компьютерной информации.

4.3. Методы и средства защиты от несанкционированного доступа к информации в компьютерных системах.

4.4. Выявление и сохранение значимой информации со средств вычислительной техники и программного обеспечения.

5.2. Использование веб-ресурсов для получения данных о недвижимости, транспорте, физических и юридических лицах.

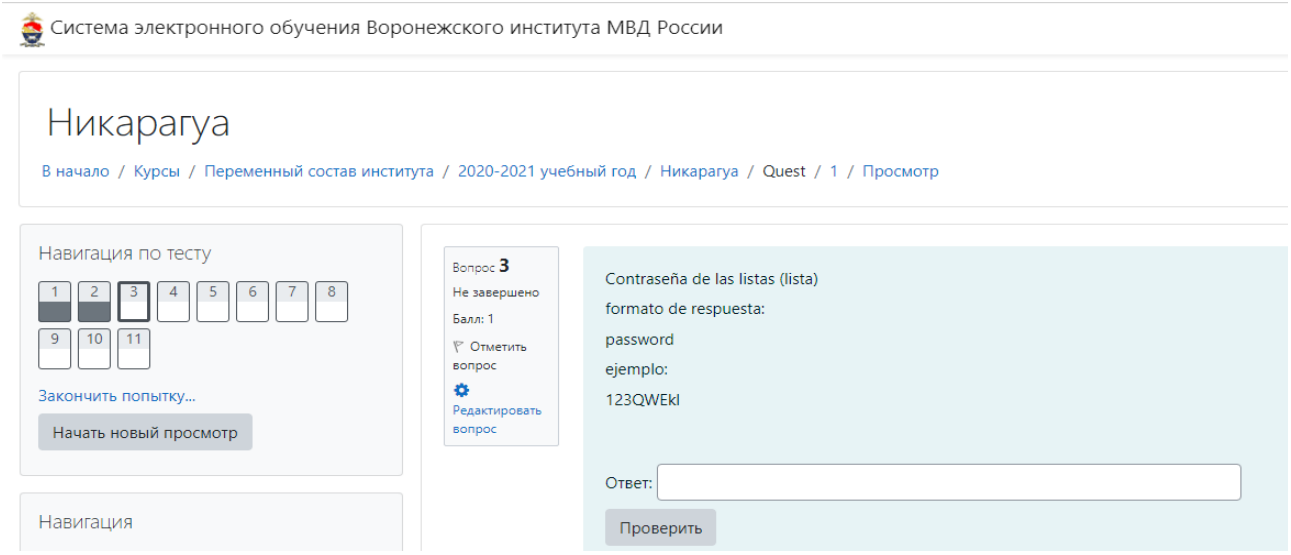
5.3. Поиск и анализ информации в сети Интернет в целях выявления преступлений в сфере компьютерной информации.

Слушатели после успешного завершения второго задания переходят к решению третьего:

Contraseña de las listas (lista)
formato de respuesta:
password
ejemplo:
123QWEkl

Перевод текста задания:

Пароль от списка (**lista)**
Формат ответа:
password
Пример:
123QWEkl

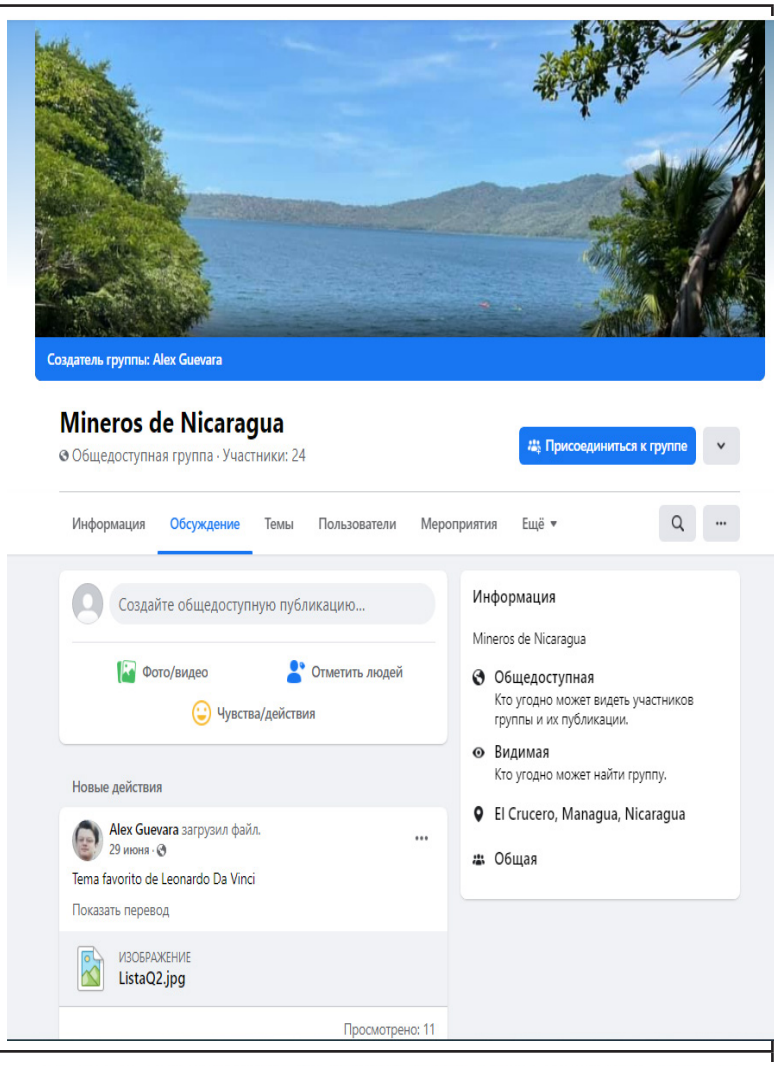
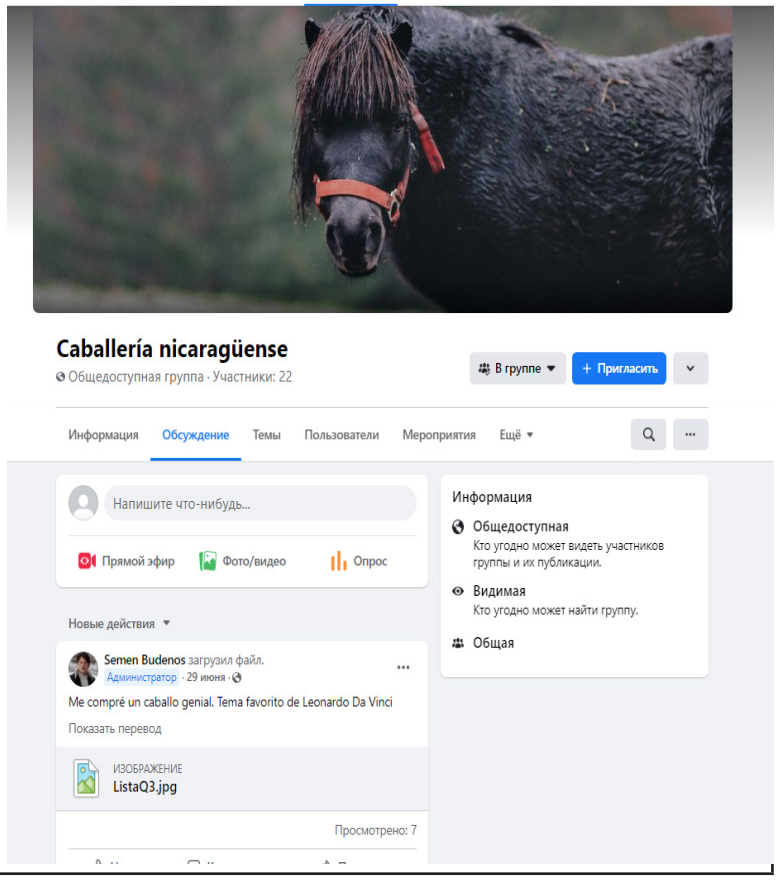


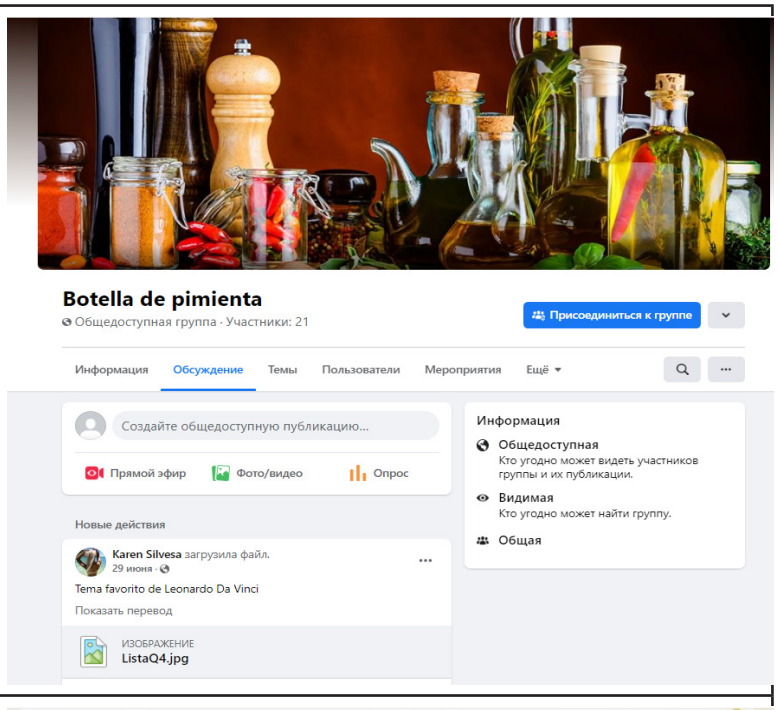
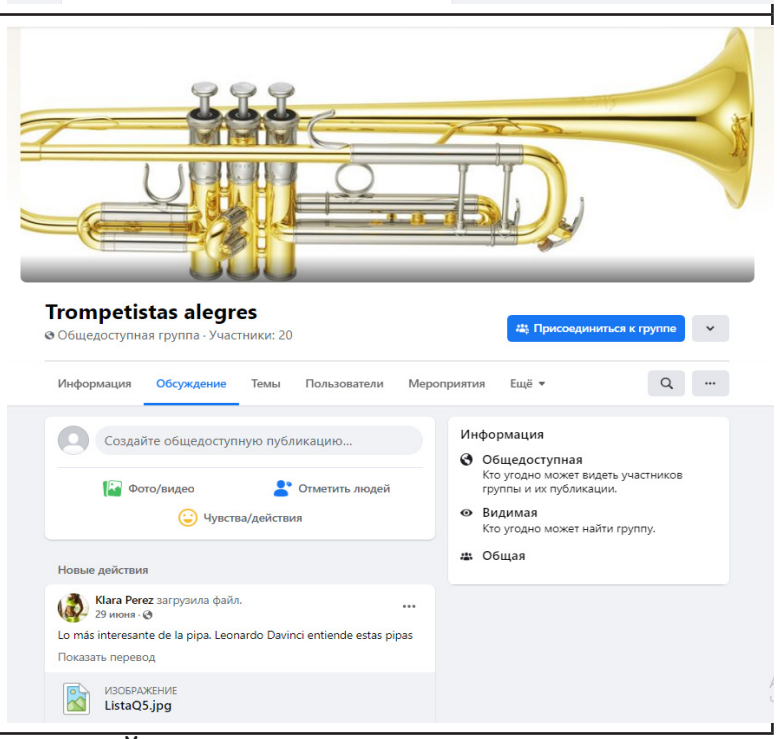
Снимок экрана с третьим заданием для сюжетной линии № 1

Основные этапы решения:

1. Мониторинг социальных сетей Интернета и обнаружение группы на **Facebook, в которой размещен искомый файл:**

Первая сюжетная линия:
Размещена публикация
с заголовком на испанском
языке «Это понравилось бы
Леонардо да Винчи»
и прикреплен искомый файл
«ListaQ1.jpg»

Вторая сюжетная линия: Размещена публикация с заголовком на испанском языке «Это понравилось бы Леонардо да Винчи» и прикреплен искомый файл «ListaQ2.jpg»	
Третья сюжетная линия: Размещена публикация с заголовком на испанском языке «Купил себе отличную лошадь. Она бы понравилась Леонардо да Винчи» и прикреплен искомый файл «ListaQ3.jpg»	

Четвертая сюжетная линия: Размещена публикация с заголовком на испанском языке «Это понравилось бы Леонардо да Винчи» и прикреплен искомый файл «ListaQ4.jpg»	
Пятая сюжетная линия: Размещена публикация с заголовком на испанском языке «Самое интересное в трубе. Леонардо да Винчи разбирается в этих трубах» и прикреплен искомый файл «ListaQ5.jpg»	

2. Анализ содержимого стегоконтейнеров**:**

При попытке открытия файла «ListaQ1.jpg» (цифра в названии соответствует номеру сюжетной линии) стандартными средствами слушатели увидят изображение, советующее тематике каждой из групп.

Первая сюжетная линия: файл «ListaQ1.jpg»	

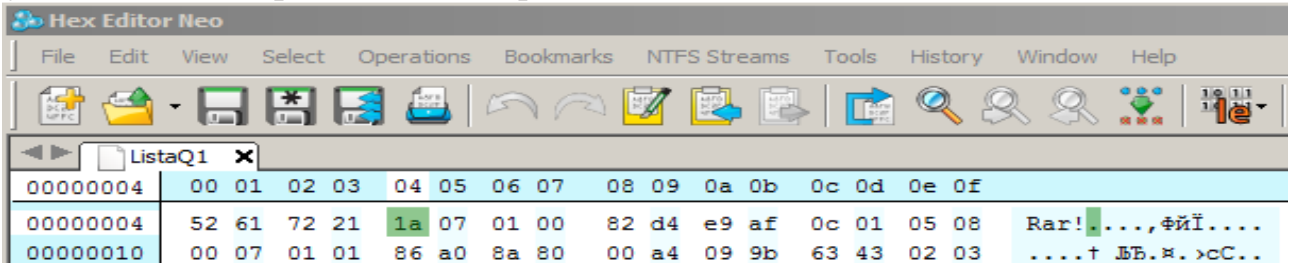
Вторая сюжетная линия: файл «ListaQ2.jpg»	
Третья сюжетная линия: файл «ListaQ3.jpg»	
Четвертая сюжетная линия: «ListaQ4.jpg»	
Пятая сюжетная линия: файл «ListaQ5.jpg»	

Слушатели должны обратить внимание на содержание текста в публикации, указывающего на имя известного художника Леонардо да Винчи, который прибегал к тайнописи и написал знаменитую картину «Мона Лиза» (Джоконда).

В связи с этим обучающиеся должны прийти к выводу, что данный файл является стегоконтейнером, созданным с помощью программы Secret Layer, так как ее иконка и интерфейс содержат изображение картины «Мона Лиза» (Джоконда). Открыть и выгрузить файл из стегоконтейнера.

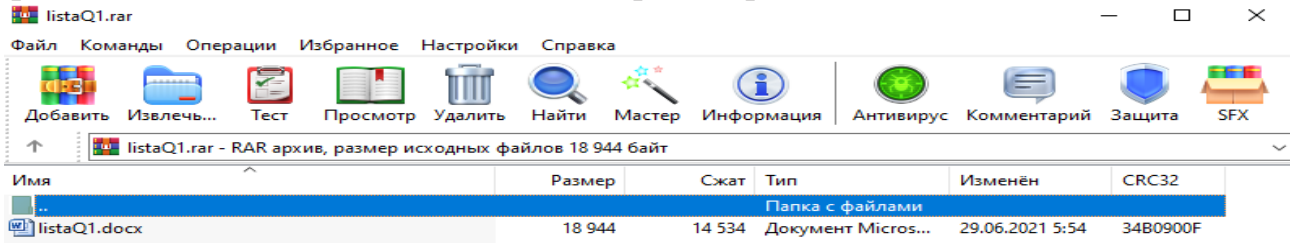
Интерфейс программы Secret Layer и содержимое файла сюжетной линии № 1

Если файл, содержащийся в стегоконтейнере, не имеет расширения, то слушатели должны определить его с помощью программы Hex Editor и установить, что файл является архивом RAR



Определение расширения «.rar» файла, содержащегося в стегоконтейнере
в рамках сюжетной линии № 1

Установив файлу разрешение «.rar» и открыв его, слушатели обнаружат там файл Microsoft Word, защищенный от просмотра.



Содержимое архива «ListaQ1.rar» в рамках сюжетной линии № 1

Слушатели должны вспомнить подсказку, содержащуюся в стегоконтейнере:

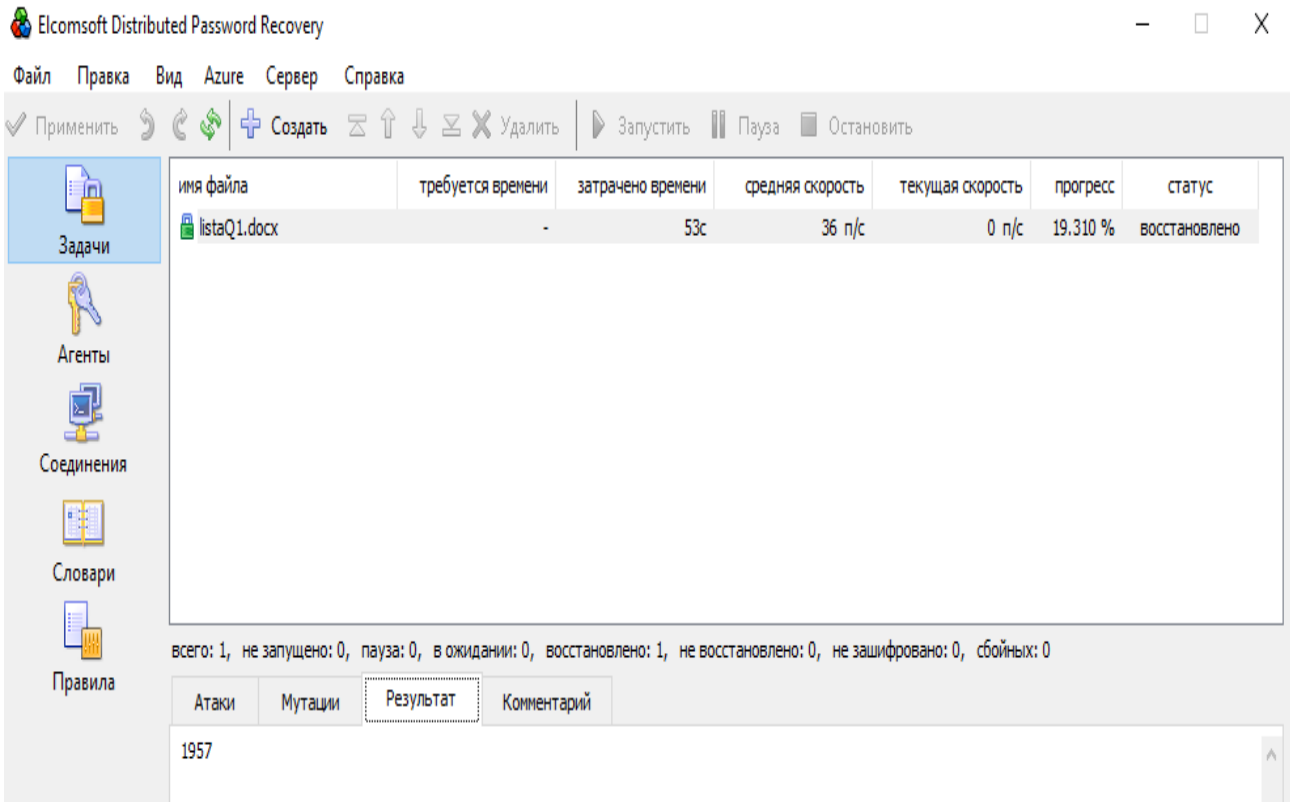
¡El secreto está adentro! Año de nacimiento del Primero: una pista sobre el contenido de la caja.

Перевод:

Секрет внутри! Год рождения Основателя: подсказка к содержимому коробки.

Подсказка сделана для того, чтобы слушатели пришли к выводу, что длина пароля – 4 цифры.

Файл Microsoft Word будет защищен от просмотра, в связи с этим слушатели с помощью Elcomsoft Distributed Password Recovery или иной программы должны осуществить подбор пароля, который и является ответом на третье задание интерактивной игры.



Результат подбора пароля к файлу «ListaQ1.docx» в рамках сюжетной линии № 1

Пароли от файлов Microsoft Word		Содержимое файлов
Первая сюжетная линия: «ListaQ1.docx»	1957	10 AK-47 5 pistolas Glock 500 gramos de cocaína
Вторая сюжетная линия: «ListaQ2.docx»	1962	7 AK-47 15 pistolas Glock 1500 gramos de cocaína
Третья сюжетная линия: «ListaQ3.docx»	1954	12 AK-47 3 pistolas Glock 400 gramos de cocaína
Четвертая сюжетная линия: «ListaQ4.docx»	1972	2 AK-47 4 pistolas Glock 100 gramos de cocaína
Пятая сюжетная линия: «ListaQ5.docx»	1971	2 AK-47 6 pistolas Glock 450 gramos de cocaína

После ввода в Систему электронного обучения Воронежского института МВД России правильного ответа слушателям на экран выводится сообщение следующего содержания:

«Ahora esta claro, a que se dedican... Como encontrar la personalidad de alguien???»

Перевод: «Теперь понятно, чем они занимаются... как бы установить чью-нибудь личность???»

Слушатели получают возможность перейти к четвертому заданию.

ВАЖНО! В рамках решения данного задания слушатели должны:

– обнаружить в файле Microsoft Word перечень закупаемого оружия и наркотиков;

– убедиться, что расследуют деятельность не просто экстремистской или террористической ячейки, занимающейся только распространением запрещённых идей и призывами к их реализации, а вооружённой организованной преступной группы.

Задание 4. Установить полное имя первого фигуранта

Данное задание предусматривает отработку и закрепление теоретических знаний и практических навыков извлечения метаданных документов MS Office в рамках следующих тем:

2.2. Программные и программно-аппаратные средства, используемые для аналитической обработки информации.

3.2. Особенности первоначального этапа расследования преступлений в сфере компьютерной информации.

4.4. Выявление и сохранение значимой информации со средств вычислительной техники и программного обеспечения.

5.1. Средства анонимизации и деанонимизации в сети Интернет.

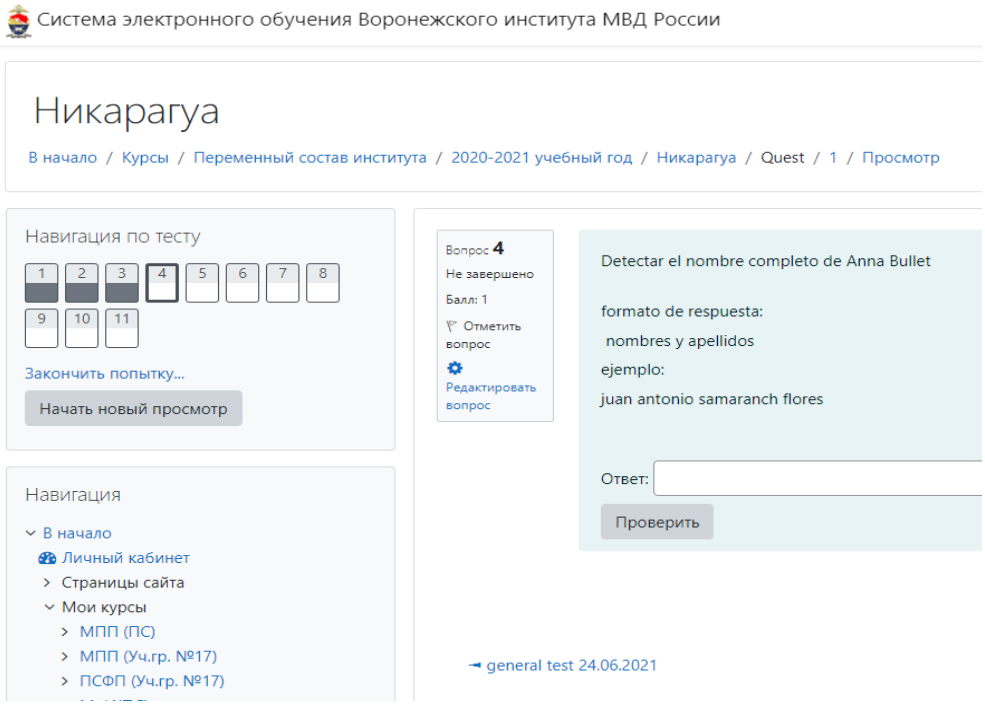
5.2. Использование веб-ресурсов для получения данных о недвижимости, транспорте, физических и юридических лицах.

5.3. Поиск и анализ информации в сети Интернет в целях выявления преступлений в сфере компьютерной информации.

Слушатели после успешного завершения третьего задания переходят к решению четвертого:

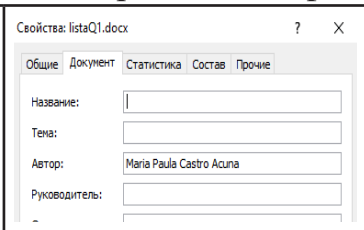
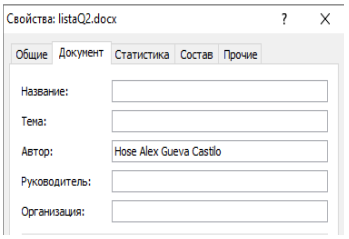
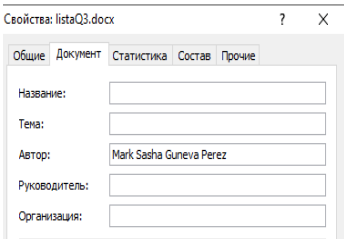
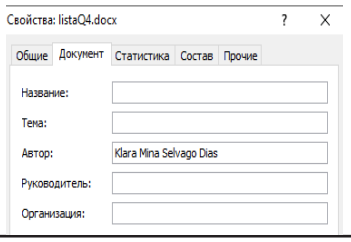
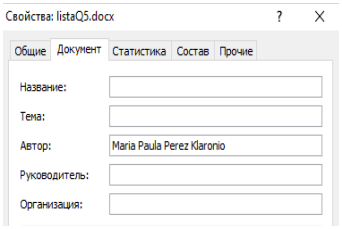
Detectar el nombre completo de **********
formato de respuesta:
nombres y apellidos
ejemplo:
juan antonio samaranch flores

Перевод текста задания:
Установить полное имя **********
Формат ответа:
Имя Имя Фамилия Фамилия
Пример:
Хуан Антонио Самаранч Флорес



Снимок экрана с четвертым заданием для сюжетной линии № 1

Задание предусматривает анализ метаданных файла Microsoft Word, слушателям необходимо просмотреть имя автора данного файла:

Первая сюжетная линия: «ListaQ1.docx»	
Вторая сюжетная линия: «ListaQ2.docx»	
Третья сюжетная линия: «ListaQ3.docx»	
Четвертая сюжетная линия: «ListaQ4.docx»	
Пятая сюжетная линия: «ListaQ5.docx»	

После ввода в Систему электронного обучения Воронежского института МВД России правильного ответа слушателям на экран выводится сообщение следующего содержания:

«Esto ya es algo! hay a quien arrestar en el mundo! al menos esto podemos hacer!!! Asi esta detenida, pero se retracta... No pudimos desbloquear el telefono... En la laptop tambien no hay nada... Nada, aparte de copia de reserva Iphone, pero que - ahi tambien hay contraseña!»

Перевод: «А это уже что-то! Есть кого арестовать в реальном мире! Уж это мы умеем!!! Итак, она задержана, но идет в отказ... Телефон разблокировать не удалось... на ноутбуке тоже ничего... Ничего, кроме резервной копии Iphone, но что толку - там тоже пароль!»

Слушатели получают возможность перейти к пятому заданию.

Задание 5. Извлечь содержимое резервной копии Iphone

Данное задание предусматривает отработку и закрепление теоретических знаний и практических навыков по подбору паролей к резервным копиям мобильных устройств под управлением iOS (Elcomsoft Phone Breaker Forensic Edition) в рамках следующих тем:

2.2. Программные и программно-аппаратные средства, используемые для аналитической обработки информации .

2.3. Обнаружение передачи скрытой информации и извлечение из содержащего её сообщения.

3.2. Особенности первоначального этапа расследования преступлений в сфере компьютерной информации.

3.3. Особенности последующего и заключительного этапов расследования преступлений в сфере компьютерной информации.

4.2. Основы криптографической защиты информации.

4.3. Методы и средства защиты от несанкционированного доступа к информации в компьютерных системах.

4.4. Выявление и сохранение значимой информации со средств вычислительной техники и программного обеспечения.

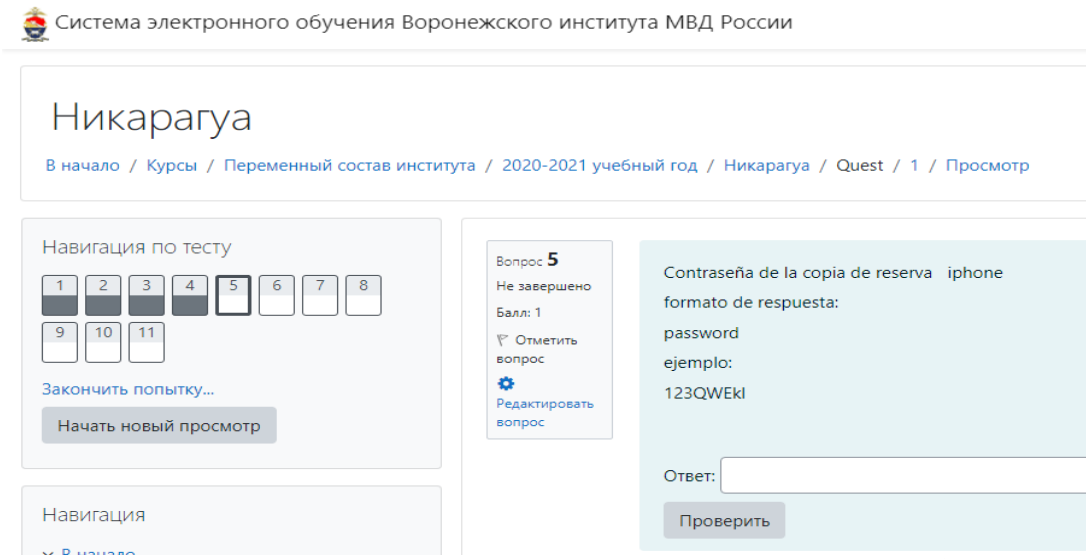
5.2. Использование веб-ресурсов для получения данных о недвижимости, транспорте, физических и юридических лицах.

5.3. Поиск и анализ информации в сети Интернет в целях выявления преступлений в сфере компьютерной информации

Слушатели после успешного завершения четвертого задания переходят к решению пятого:

Contraseña de la copia de reserva Iphone
formato de respuesta:
password
ejemplo:
123QWEkl

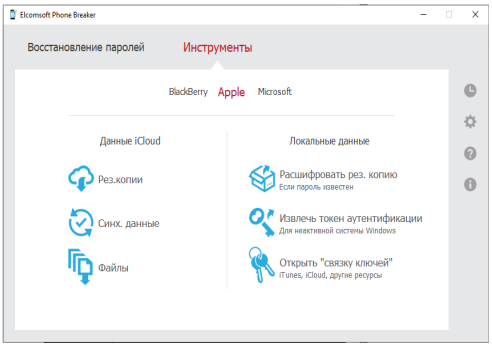
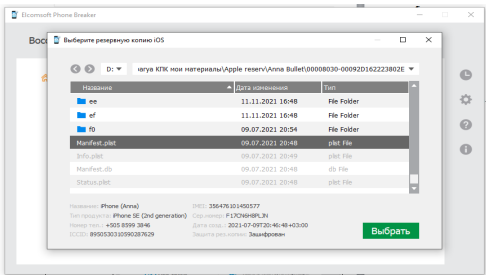
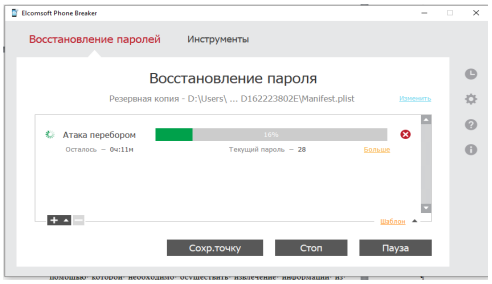
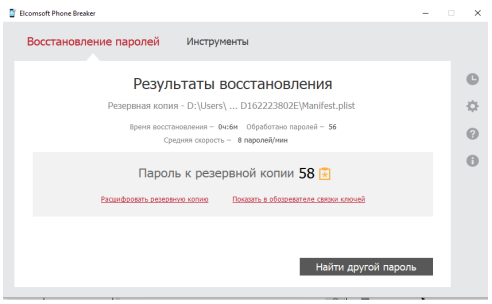
Перевод текста задания:
Пароль от резервной копии **Iphone**
Формат ответа:
password
Пример:
123QWEkl



Снимок экрана с пятым заданием для сюжетной линии № 1

Задание предусматривает использование Elcomsoft Phone Breaker, с помощью которой необходимо осуществить подбор пароля к резервной копии Apple iPhone, принадлежащего первому персонажу каждой сюжетной линии, путем ее расшифровки и подбора неизвестных паролей с использованием аппаратного ускорения.

Слушателям сообщается, что для ускорения процесса расшифровки резервной копии и подбора к ней пароля он состоит из 2 цифр.

Решение на примере первой сюжетной линии:	
Слушатель запускает Elcomsoft Phone Breaker и выбирает в меню «Расшифровать рез. копию»	
Слушатель выбирает файл «Manifest.plist», который находится в папке резервной копии	
Слушатель настраивает вид атаки и запускает процедуру восстановления пароля	
Слушатель получает искомый пароль от резервной копии	

После ввода в Систему электронного обучения Воронежского института МВД России правильного ответа слушателям на экран выводится сообщение следующего содержания:

«Urra, ahora tenemos acceso a la informacion del telefono... Seguramente ellos tienen casa de reunion... Interesante, donde esta???»

Перевод: «Ура, теперь у нас есть доступ к информации телефона... Наверняка у них есть явочная квартира... интересно, где она???»

Слушатели получают возможность перейти к шестому заданию.

Задание 6. Установить координаты места сбора фигурантов

Данное задание предусматривает отработку и закрепление теоретических знаний и практических навыков по анализу резервных копий мобильных устройств под управлением iOS (Elcomsoft Phone Viewer Forensic Edition) в рамках следующих тем:

2.2. Программные и программно-аппаратные средства, используемые для аналитической обработки информации.

2.3. Обнаружение передачи скрытой информации и извлечение из содержащего её сообщения.

3.2. Особенности первоначального этапа расследования преступлений в сфере компьютерной информации.

4.4. Выявление и сохранение значимой информации со средств вычислительной техники и программного обеспечения.

5.1. Средства анонимизации и деанонимизации в сети Интернет.

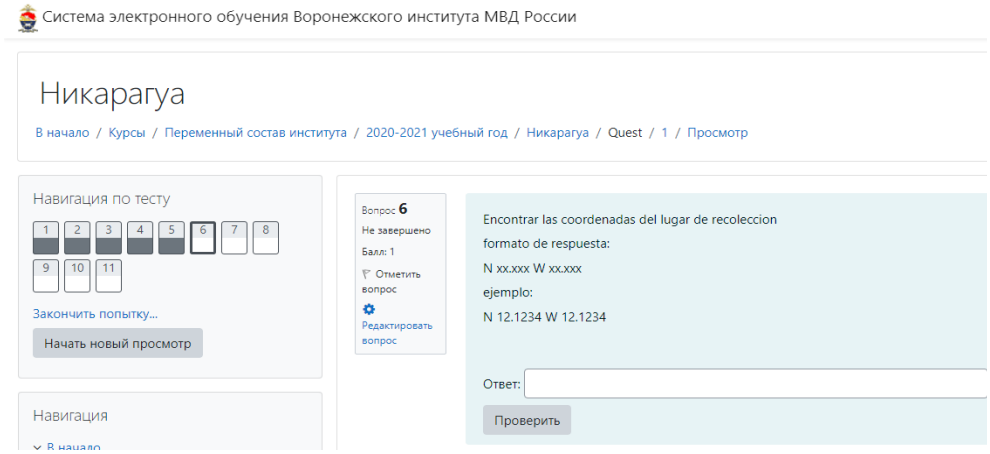
5.2. Использование веб-ресурсов для получения данных о недвижимости, транспорте, физических и юридических лицах.

5.3. Поиск и анализ информации в сети Интернет в целях выявления преступлений в сфере компьютерной информации.

Слушатели после успешного завершения пятого задания переходят к решению шестого:

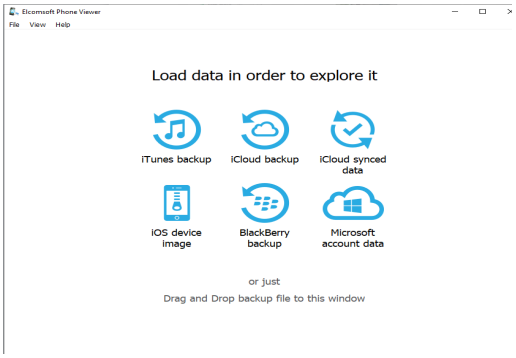
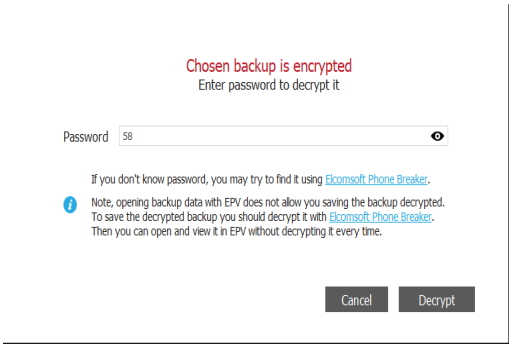
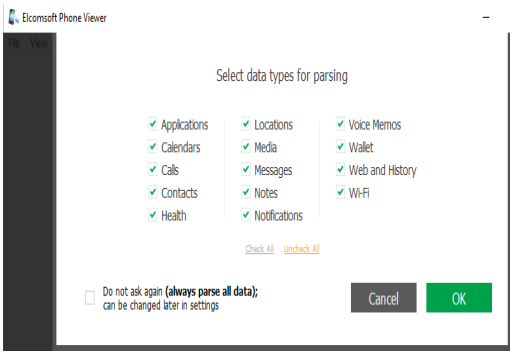
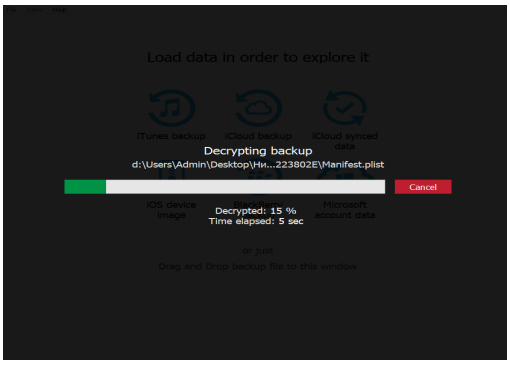
Encontrar las coordenadas del lugar de recoleccion
formato de respuesta:
N xx.xxx W xx.xxx
ejemplo:
N 12.1234 W 12.1234

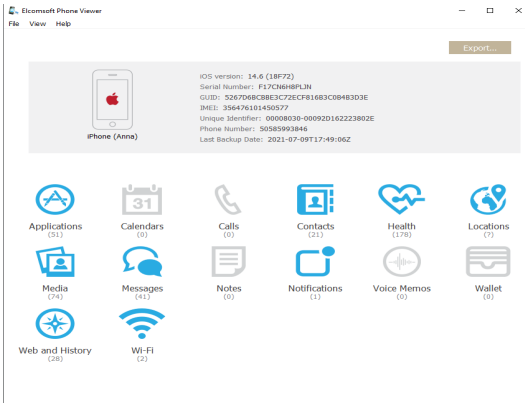
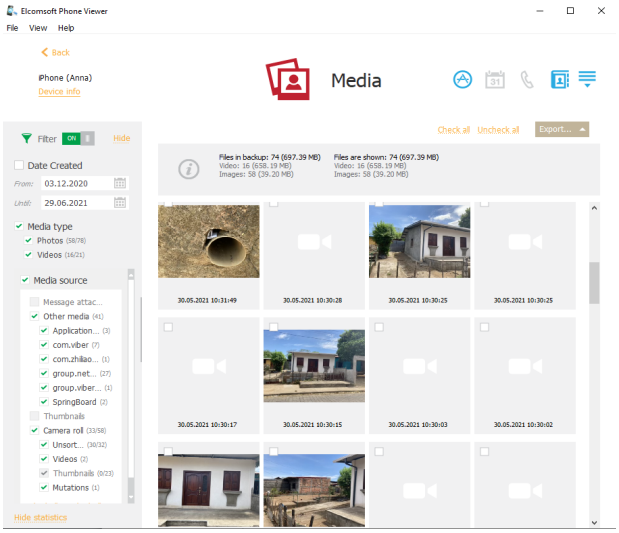
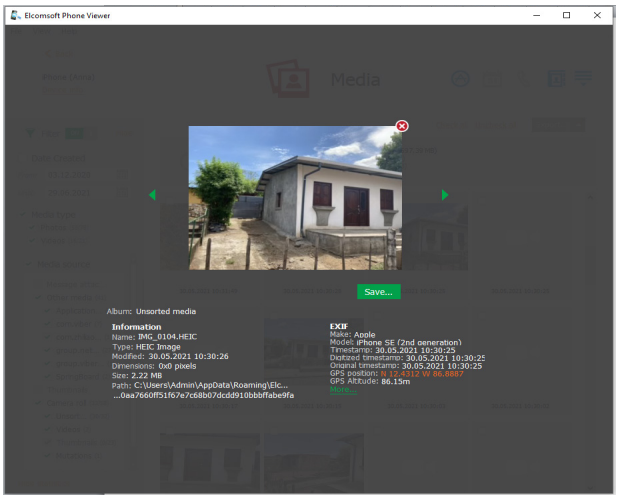
Перевод текста задания:
Установить координаты места сбора
Формат ответа:
N xx.xxx W xx.xxx
Пример:
N 12.1234 W 12.1234



Снимок экрана с шестым заданием для сюжетной линии № 1

Задание предусматривает использование программы Elcomsoft Phone Viewer, с помощью которой необходимо осуществить извлечение информации и осуществить анализ содержимого из резервной копии Apple iPhone, принадлежащего первому персонажу каждой сюжетной линии.

Решение на примере первой сюжетной линии	
Запустить Elcomsoft Phone Viewer и выбрать в меню «iTunes backup»	
Ввести пароль от резервной копии, который был получен в рамках решения 5 задания интерактивной игры	
Выбрать данные, подлежащие извлечению	
Осуществить извлечение данных из резервной копии	

Приступить к анализу содержимого резервной копии с целью установления координат места сбора персонажей интерактивной игры	
В разделе Media найти фотографии и видеозаписи, которые по датам и времени подходят под описание мест, которые были указаны в сообщении первого персонажа в почте Mail2Tor	
Раскрыть метаданные файла и установить координаты места сбора	

После ввода в Систему электронного обучения Воронежского института МВД России правильного ответа слушателям на экран выводится сообщение следующего содержания:

« Nosotros entramos inflagrante, pero solo habia una persona extraña... O un cuidador, o un conductor, o esta imitando. Que bueno, al menos no bloqueo el telefono... Que tiene aqui?»

Перевод: « Мы нагрянули внезапно, но там был только один чудило... То ли охранник, то ли водила, то ли прикидывается. Хорошо, хоть телефон не заблокировал... Что тут у него?»

Слушатели получают возможность перейти к седьмому заданию.

Задание 7. Установить координаты места хранения товара

Данное задание предусматривает отработку и закрепление теоретических знаний и практических навыков по анализу панорам местности с использованием ресурсов Google Street View и Яндекс.Панорамы в рамках следующих тем:

2.1. Сеть Интернет как источник информации. Веб-ресурсы и методы получения доступа к ним.

3.2. Особенности первоначального этапа расследования преступлений в сфере компьютерной информации.

3.3. Особенности последующего и заключительного этапов расследования преступлений в сфере компьютерной информации.

5.1. Средства анонимизации и деанонимизации в сети Интернет.

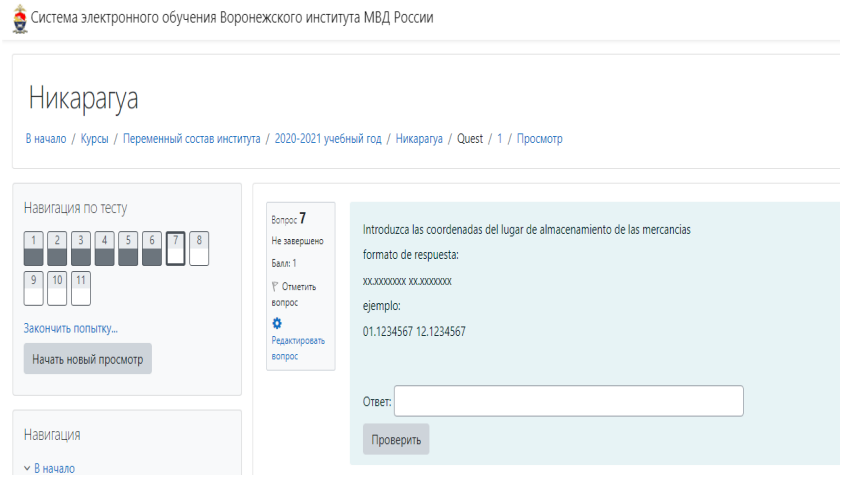
5.2. Использование веб-ресурсов для получения данных о недвижимости, транспорте, физических и юридических лицах.

5.3. Поиск и анализ информации в сети Интернет в целях выявления преступлений в сфере компьютерной информации.

Слушатели после успешного завершения шестого задания переходят к решению седьмого:

Introduzca las coordenadas del lugar de almacenamiento de las mercancias
formato de respuesta:
xx.xxxxxxx xx.xxxxxxx
ejemplo:
01.1234567 12.1234567

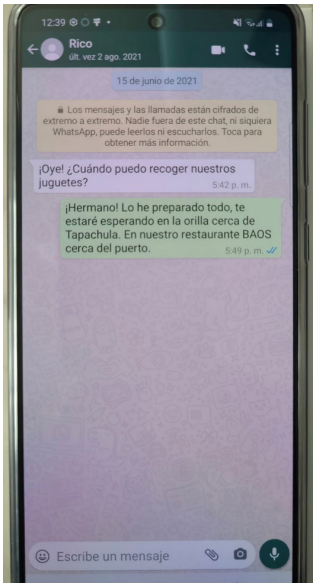
Перевод текста задания:
Ввести координаты места хранения товара
Формат ответа:
xx.xxxxxxx xx.xxxxxxx
Пример:
01.1234567 12.1234567



Снимок экрана с седьмым заданием для сюжетной линии № 1

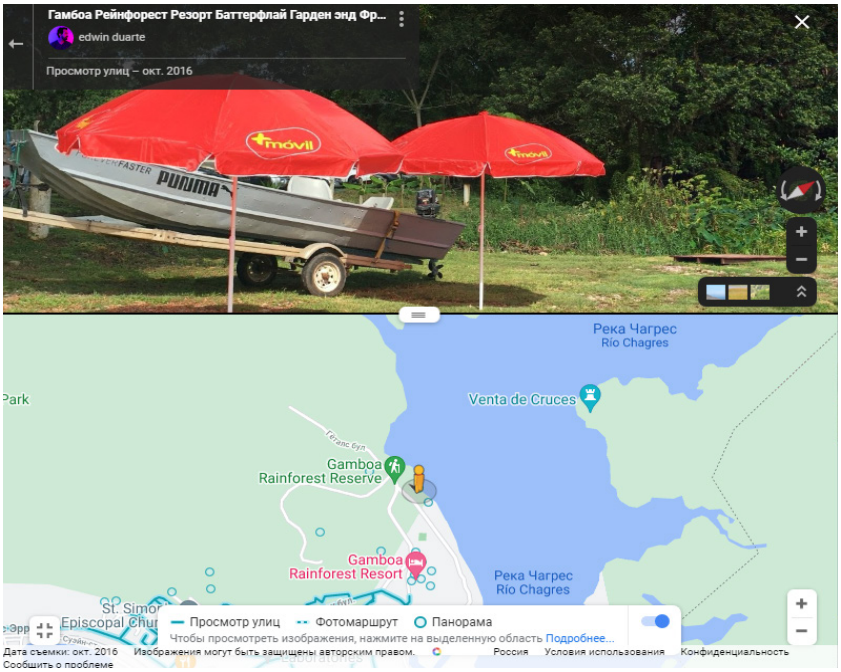
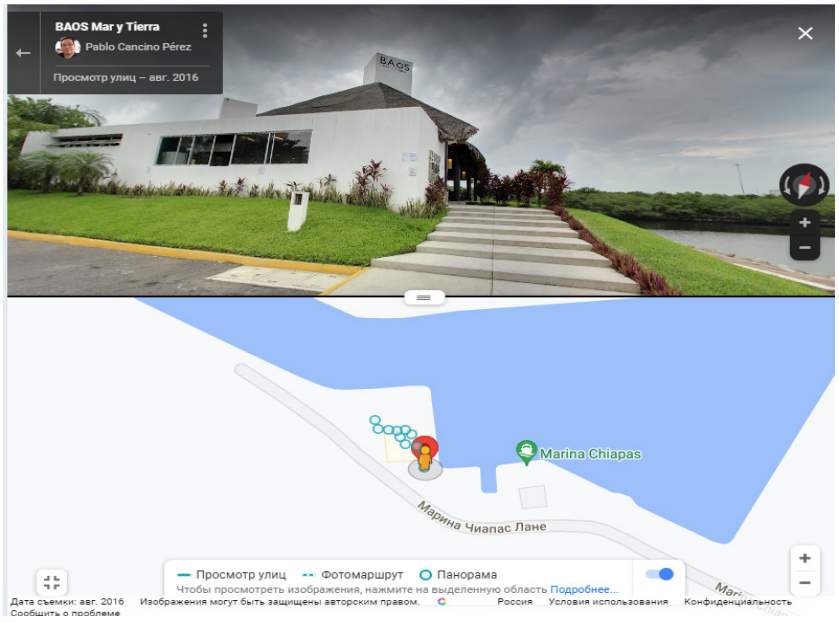
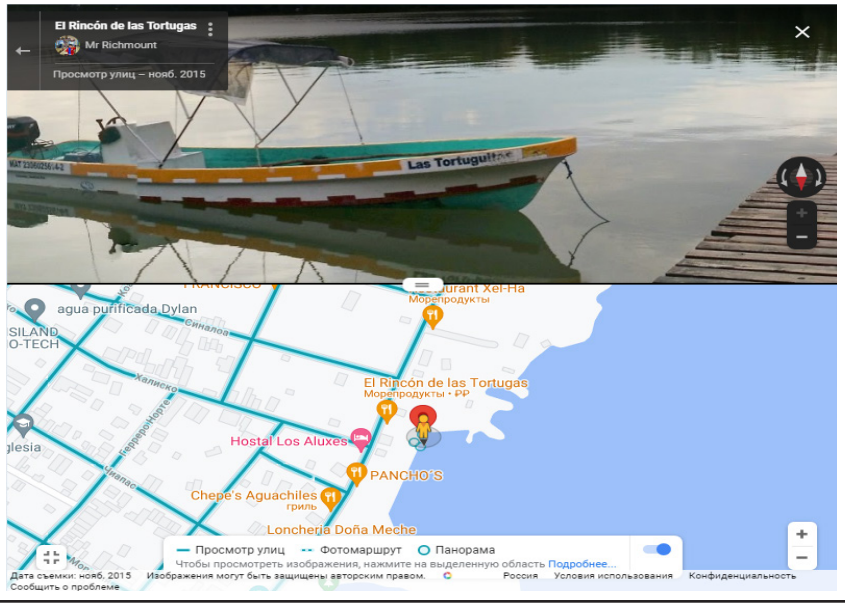
Слушателям выдается телефон, изъятый у второго персонажа, который по легенде был задержан в месте сбора.

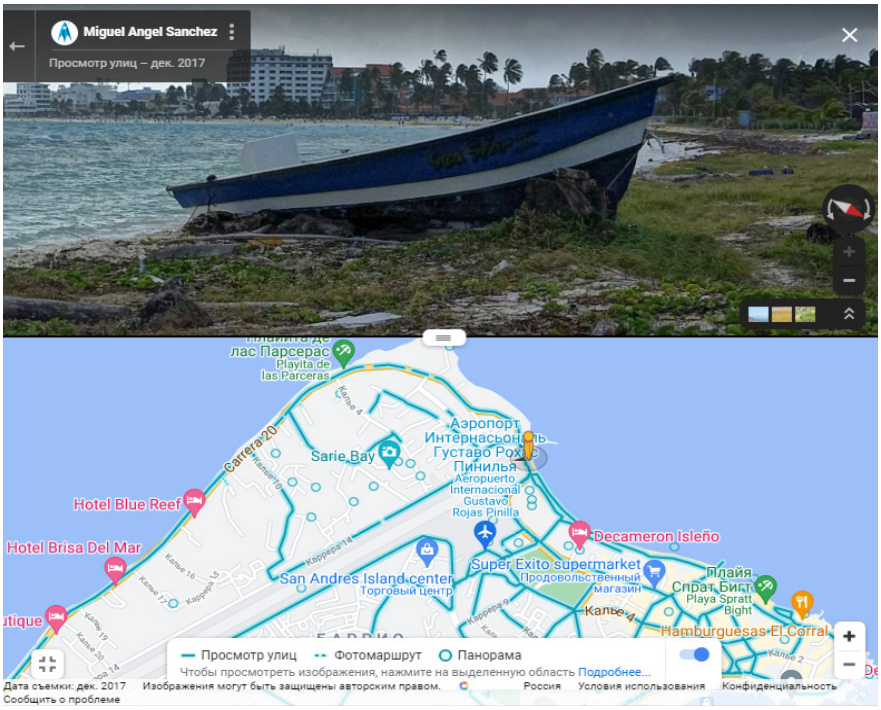
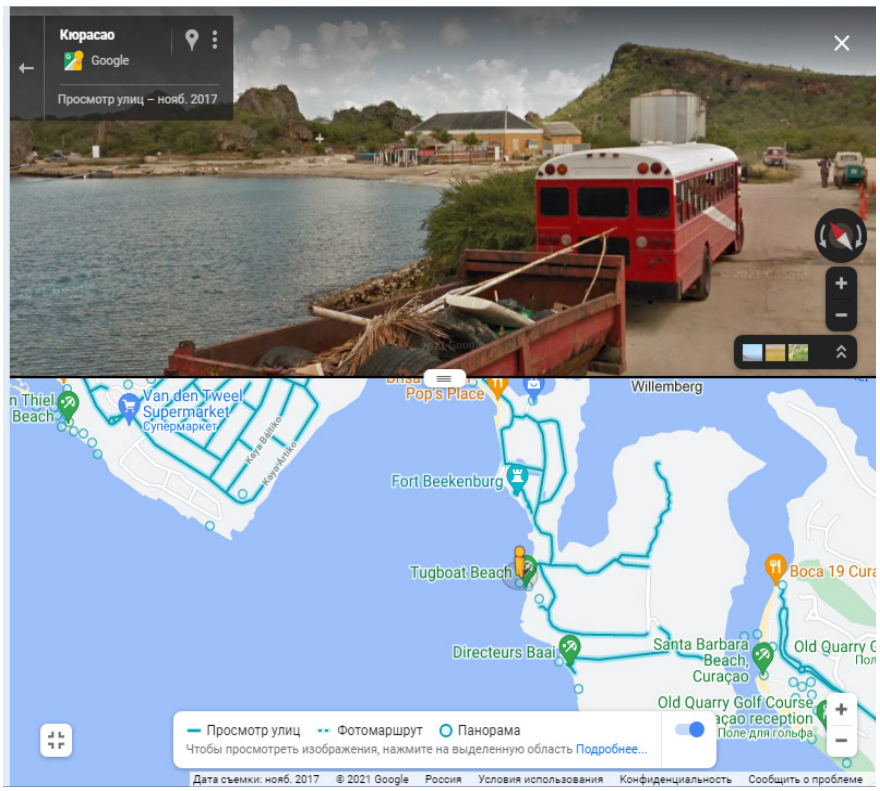
В рамках изучения и анализа содержимого они обнаруживают переписку в WhatsApp с еще одним игровым участником преступной группы:

Первая сюжетная линия Перевод: – Проверка связи. – Яволь. – Привет! Я все подготовил согласно списку. Жду тебя в панамской Гамбоа, на том же самом месте, где вы отдыхали в прошлый раз, у воды. Товар рядом, я за ним наблюдаю. Я положил его под навес у Серой Пумы, которая находится вблизи красных зонтов.	
Вторая сюжетная линия: Перевод: – Эй, когда могу забрать наши игрушки? – Брат, я все подготовил, буду ждать тебя на берегу, недалеко от Тапачулы. В нашем ресторане BAOS, недалеко от порта.	
Третья сюжетная линия: Перевод: – Эй, все готово? – Все готово, я с оружием и наркотиками на базе Четумаль. Все на берегу в бело-желтой Лас Тортугитас. Жду тебя.	

Четвертая сюжетная линия: Перевод: – Привет. – Привет. – Я уже оплатил покупку. Мне все привезли. Когда заберешь товар? – Куда надо подъехать? – Я все загрузил на лодку SeaSlar1, жду тебя как и всегда, рядом с аэропортом Густаво Рохас Пинийя.	
Пятая сюжетная линия: Перевод: – Все готово? – Да. – Где вы находитесь и где товар? – Там, где и всегда. Все в красном автобусе, рядом с кораблем, недалеко от Виллемстада. – Отлично!	

На основании полученной информации слушатель должен начать осматривать описанную в сообщении территорию с помощью Google Street View, после обнаружения места, подходящего под описание, – скопировать координаты в адресной строке.

Первая сюжетная линия 09.1251497 -79.6924538	
Вторая сюжетная линия 14.6985971 -92.3929973	
Третья сюжетная линия: 18.5606924 -88.2493121	

Четвертая сюжетная линия: 12.5899024 -81.7004998	
Пятая сюжетная линия: 12.0695119 -68.8619331	

После ввода в Систему электронного обучения Воронежского института МВД России правильного ответа слушателям на экран выводится сообщение следующего содержания:

« Lo encontramos, descubrimos a uno... Pero aparentemente es un simple corredor... Tambien es un ciudadano inocente - el telefono esta sin bloqueo! veamos...»

Перевод: «Нашли, хлопнули одного... Но это, кажется, простой курьер... Тоже весьма беспечный гражданин - телефон без блокировки! Посмотрим...»

Слушатели получают возможность перейти к восьмому заданию.

Задание 8. Установить получателя BTC-транзакции

Данное задание предусматривает отработку и закрепление теоретических знаний и практических навыков по осмотру мобильных устройств, использованию блокчейна криптовалют, на примере BTC, и мониторингу социальных сетей в рамках следующих тем:

2.1. Сеть Интернет как источник информации. Веб-ресурсы и методы получения доступа к ним.

3.2. Особенности первоначального этапа расследования преступлений в сфере компьютерной информации.

3.3. Особенности последующего и заключительного этапов расследования преступлений в сфере компьютерной информации.

5.1. Средства анонимизации и деанонимизации в сети Интернет.

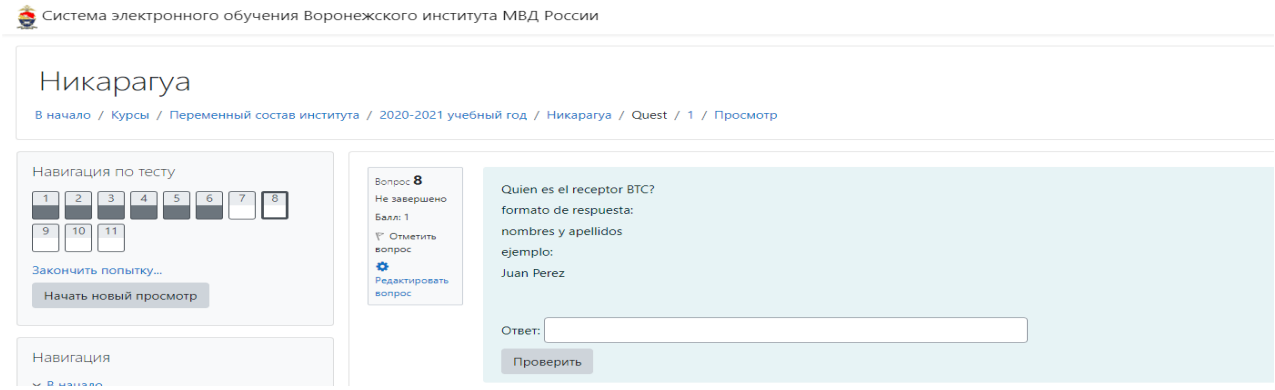
5.2. Использование веб-ресурсов для получения данных о недвижимости, транспорте, физических и юридических лицах.

5.3. Поиск и анализ информации в сети Интернет в целях выявления преступлений в сфере компьютерной информации.

Слушатели после успешного завершения седьмого задания переходят к решению восьмого:

Quien es el receptor BTC?
formato de respuesta:
nombres y apellidos
ejemplo:
Juan Perez

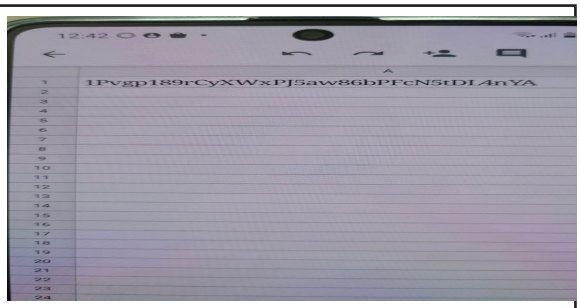
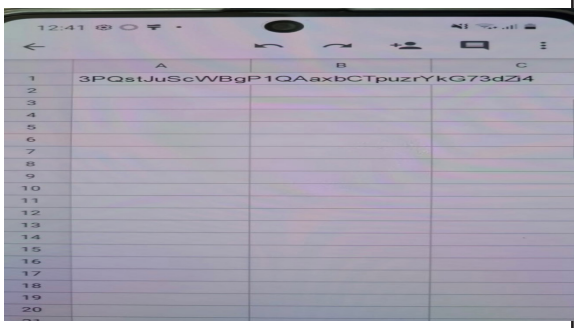
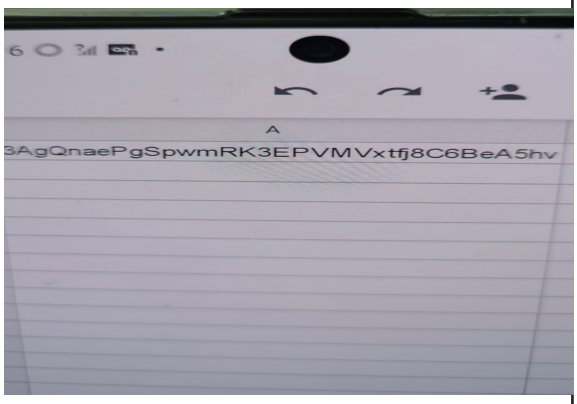
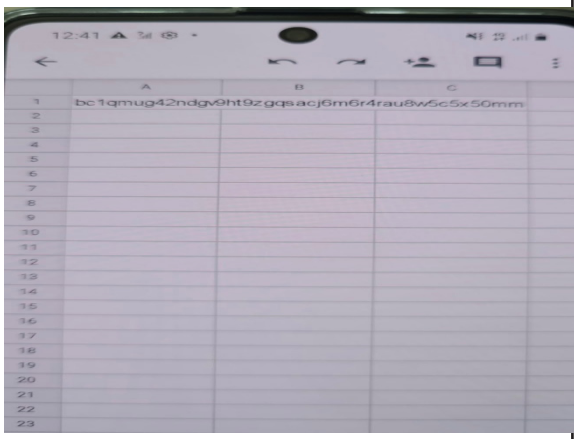
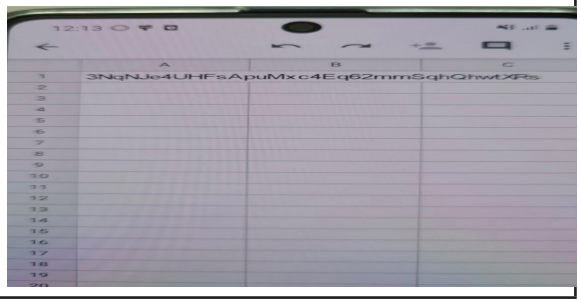
Перевод текста задания:
Кто же получатель BTC?
Формат ответа:
Имя Фамилия
Пример:
Хуан Перес



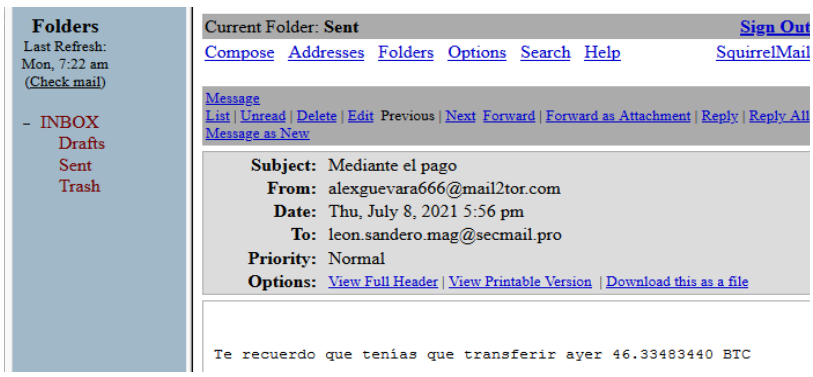
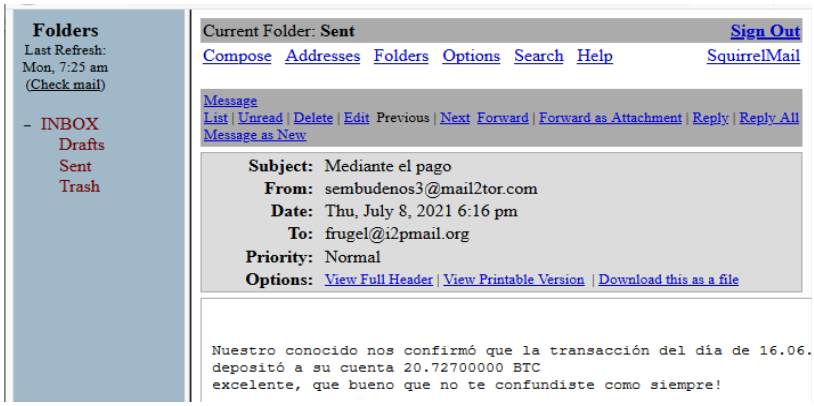
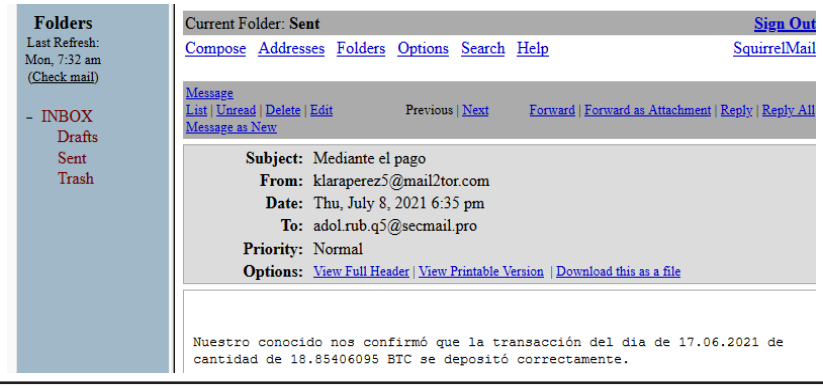
Снимок экрана с восьмым заданием для сюжетной линии № 1

Слушателям выдается еще один телефон, изъятый у третьего персонажа, который по легенде был задержан в месте хранения оружия и наркотиков.

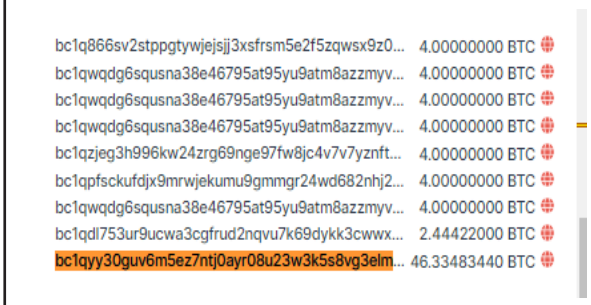
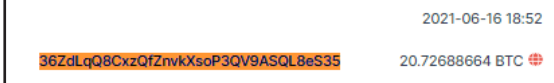
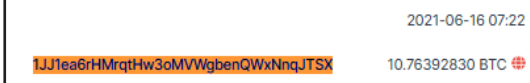
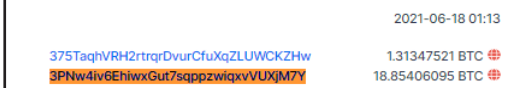
В рамках изучения и анализа содержимого они обнаруживают в приложении Google Tabs запись, содержащую комбинацию букв и цифр, которая является номером криптокошелька:

Первая сюжетная линия: 1Pvgp189rCyXWxPJ5aw86bPFcN5tDL4nYA	
Вторая сюжетная линия: 3PQstJuScWBgP1QAaxbCTpuzrYkG73dZi4	
Третья сюжетная линия: 3AgQnaePgSpwmRK3EPVMVxtfj8C6BeA5hv	
Четвертая сюжетная линия: bc1qmug42ndgv9ht9zgqsacj6m6r4rau8w5c5x50mm	
Пятая сюжетная линия: 3NqNJe4UHFsApuMxc4Eq62mmSqhQhwtXRs	

Слушатели должны вспомнить, что при решении второго задания при анализе содержимого учетной записи первого фигуранта на почтовом сервисе Mail2Tor были письма, адресованные собственнику исследуемого телефонного аппарата следующего содержания:

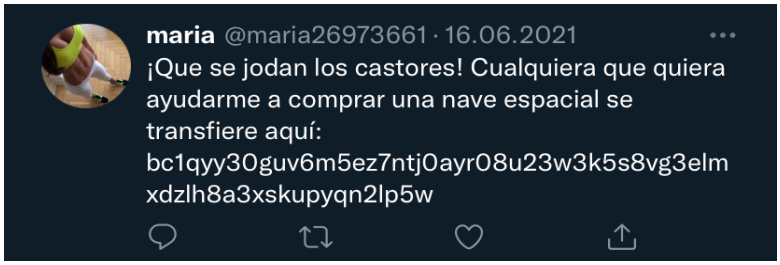
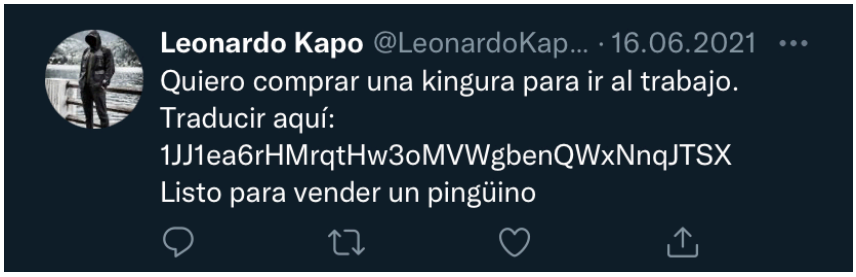
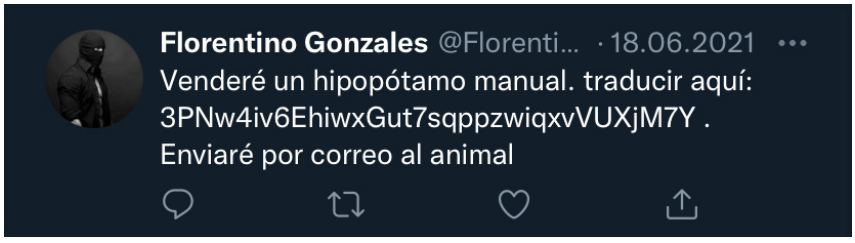
Первая сюжетная линия Перевод сообщения: «Молодец, что вчера перевел 2.21987085 BTC»	
Вторая сюжетная линия: Перевод сообщения: «Напоминаю, вчера нужно было перевести 46.33483440 BTC»	
Третья сюжетная линия: Перевод сообщения: «Наш знакомый подтвердил нам, что перевод от 16.06.2021 на его счет 20.72700000 BTC прошел, хорошо, что вы как всегда не перепутали!»	
Четвертая сюжетная линия: Перевод сообщения: «Наш знакомый подтвердил транзакцию депозита от 15.06.2021 10.76392830 BTC на его счет»	
Пятая сюжетная линия: Перевод сообщения: «Наш знакомый подтвердил нам, что сделка от 17.06.2021 18,85406095 BTC прошла успешно и битки зачислены»	

Располагая этой информацией, слушатели с использованием ресурса https://www.blockchain.com/ смогут установить номер криптокошелька, на который в указанные даты были переведены обозначенные суммы.

Первая сюжетная линия Перевод сообщения: «Молодец, что вчера перевел 2.21987085 BTC»	
Вторая сюжетная линия: Перевод сообщения: «Напоминаю, вчера нужно было перевести 46.33483440 BTC»	
Третья сюжетная линия: Перевод сообщения: «Наш знакомый подтвердил нам, что перевод от 16.06.2021 на его счет 20.72700000 BTC прошел, хорошо, что вы как всегда не перепутали!»	
Четвертая сюжетная линия: Перевод сообщения: «Наш знакомый подтвердил транзакцию депозита от 15.06.2021 10.76392830 BTC на его счет»	
Пятая сюжетная линия: Перевод сообщения: «Наш знакомый подтвердил нам, что сделка от 17.06.2021 18,85406095 BTC прошла успешно и битки зачислены»	

Далее слушатели в рамках мониторинга социальных сетей в Twitter смогут найти твит, благодаря которому установят личность человека, которому принадлежит найденный криптокошелек.

Первая сюжетная линия:	

Вторая сюжетная линия:	
Третья сюжетная линия:	
Четвертая сюжетная линия:	
Пятая сюжетная линия:	

После ввода в Систему электронного обучения Воронежского института МВД России правильного ответа слушателям на экран выводится сообщение следующего содержания:

«Y a este lo arrestaron. no habla... Pero tiene muchos rastros! como resolucion del juez le amputaron el dedo y desbloquearon su iPhone. Que se alegre, que el FaceID no fue necesario utilizarse - hubieramos trabajado con la cara... Y se incuto una memoria , pero en ell ano se encontro nada sospechoso... Aunque, hay que ver con que se reviso...»

Перевод: «И этого арестовали. Не колется... Но улик много! По решению суда ампутировали палец и разблокировали его iPhone. Пусть радуется, что FaceID не догадался использовать – пришлось бы работать с лицом... А ну и флешку изъяли, но на ней ничего подозрительного... Хотя, смотря чем посмотреть...»

Слушатели получают возможность перейти к девятому заданию.

Задание 9. Найти потенциальный криптоконтейнер

Данное задание предусматривает отработку и закрепление теоретических знаний и практических навыков по анализу носителей цифровой информации с использованием Belkasoft Evidence Center X в рамках следующих тем:

2.2. Программные и программно-аппаратные средства, используемые для аналитической обработки информации .

2.3. Обнаружение передачи скрытой информации и извлечение из содержащего её сообщения.

3.2. Особенности первоначального этапа расследования преступлений в сфере компьютерной информации.

3.3. Особенности последующего и заключительного этапов расследования преступлений в сфере компьютерной информации.

4.1. Введение в информационную безопасность.

4.2. Основы криптографической защиты информации.

4.3. Методы и средства защиты от несанкционированного доступа к информации в компьютерных системах.

4.4. Выявление и сохранение значимой информации со средств вычислительной техники и программного обеспечения.

4.5. Основы информационной безопасности телекоммуникационных систем.

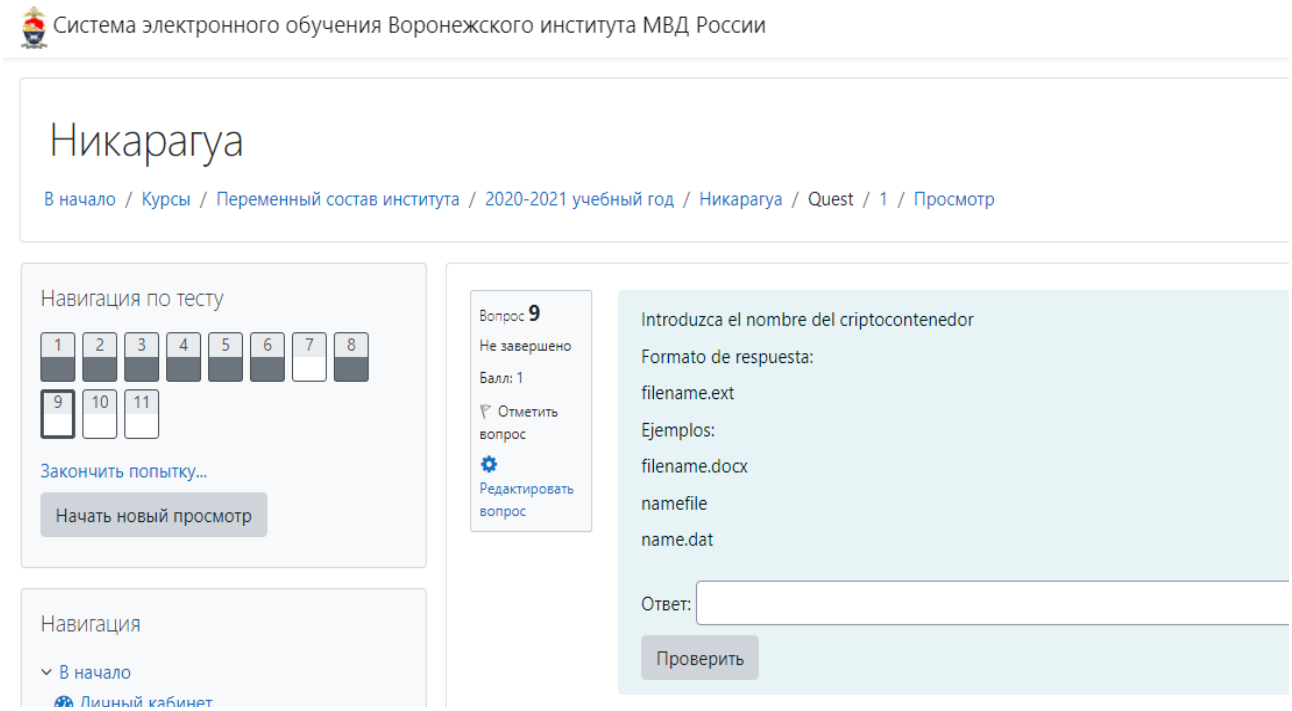
5.2. Использование веб-ресурсов для получения данных о недвижимости, транспорте, физических и юридических лицах.

5.3. Поиск и анализ информации в сети Интернет в целях выявления преступлений в сфере компьютерной информации

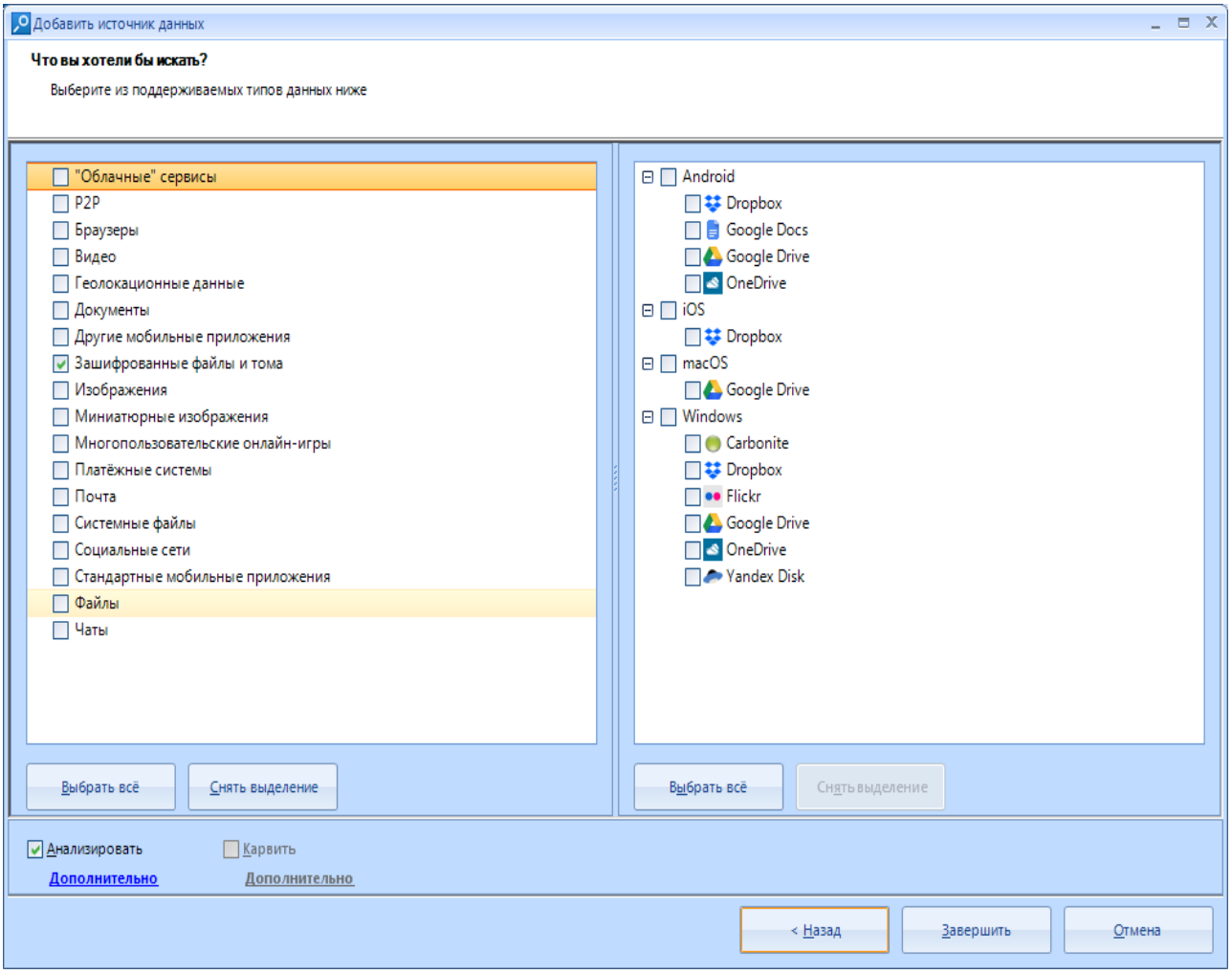
Слушатели после успешного завершения восьмого задания переходят к решению девятого:

Introduzca el nombre del criptocontenedor
Formato de respuesta:
filename.ext
Ejemplos:
filename.docx
namefile
name.dat

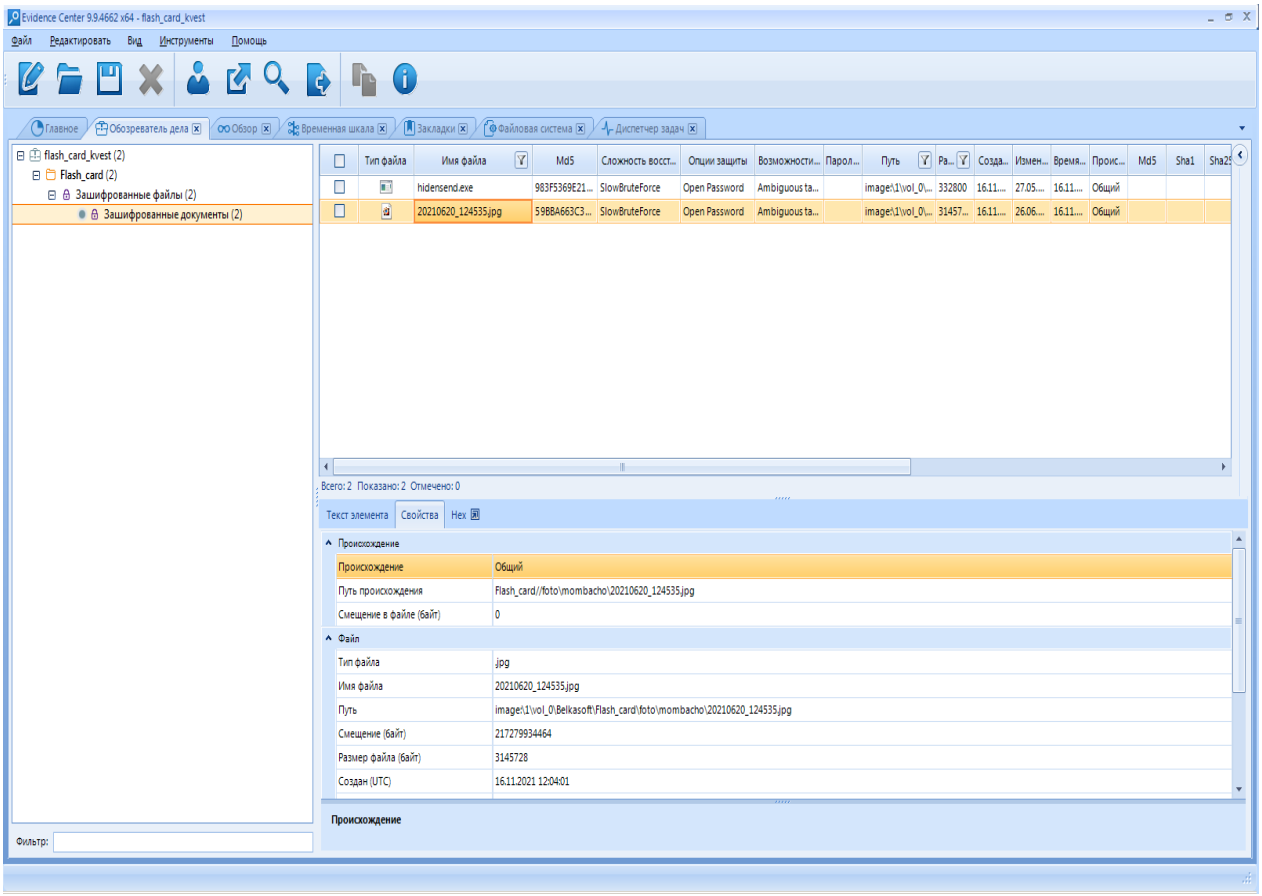
Перевод текста задания:
Введите имя криптоконтейнера
Формат ответа:
filename.ext
Примеры:
filename.docx
namefile
name.dat



Слушатели при помощи Belkasoft Evidence Center анализируют содержимое изъятой у подозреваемого флеш-карты на предмет наличия криптоконтейнеров, для чего включают поиск «Зашифрованные файлы и тома».



Обнаруживают 2 файла, имеющих признаки криптоконтейнера. Имя файла с расширением .jpg – правильный ответ.



После ввода в Систему электронного обучения Воронежского института МВД России правильного ответа слушателям на экран выводится сообщение следующего содержания:

«Emmm. Contenedor encontrado, y como lo abrimos? Será que es todo... El tope???»

Перевод: «Мда. Контейнер найден, а вот как его открыть? Неужели все... Тупик???»

Слушатели получают возможность перейти к десятому заданию.

Задание 10. Определить место встречи с куратором

Данное задание предусматривает отработку и закрепление теоретических знаний и практических навыков по структуризации, форматированию и группировке больших информационных массивов в рамках следующих тем:

2.1. Сеть Интернет как источник информации. Веб-ресурсы и методы получения доступа к ним.

2.2. Программные и программно-аппаратные средства, используемые для аналитической обработки информации .

3.2. Особенности первоначального этапа расследования преступлений в сфере компьютерной информации.

3.3. Особенности последующего и заключительного этапов расследования преступлений в сфере компьютерной информации.

4.4. Выявление и сохранение значимой информации со средств вычислительной техники и программного обеспечения.

5.1. Средства анонимизации и деанонимизации в сети Интернет.

5.2. Использование веб-ресурсов для получения данных о недвижимости, транспорте, физических и юридических лицах.

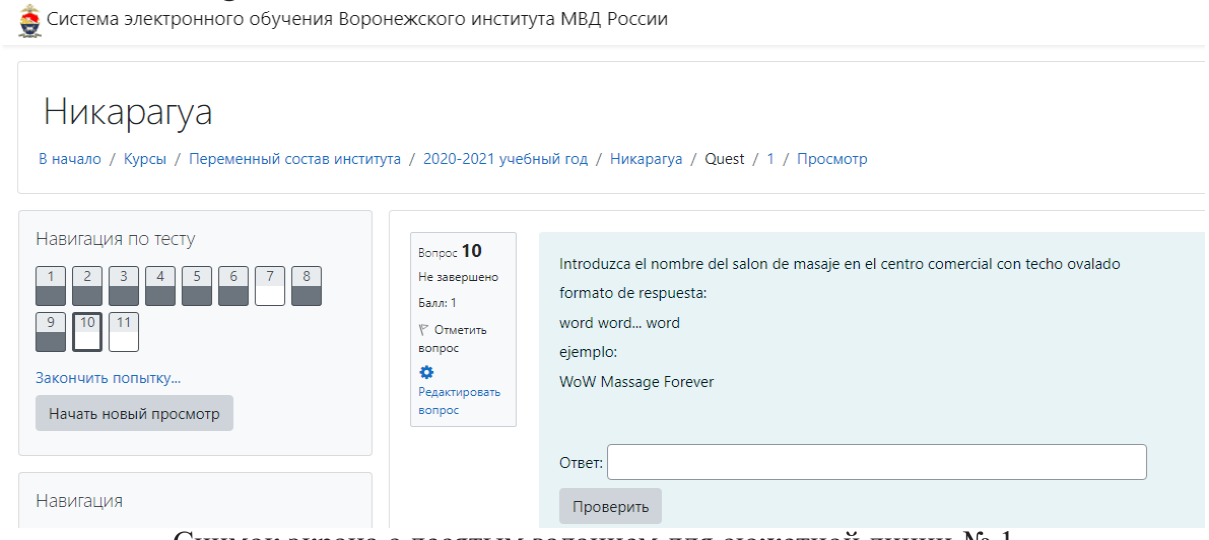
5.3. Поиск и анализ информации в сети Интернет в целях выявления преступлений в сфере компьютерной информации

Слушатели после успешного завершения девятого задания переходят к решению десятого:

Introduzca el nombre del salon de masaje en el centro comercial con techo ovalado

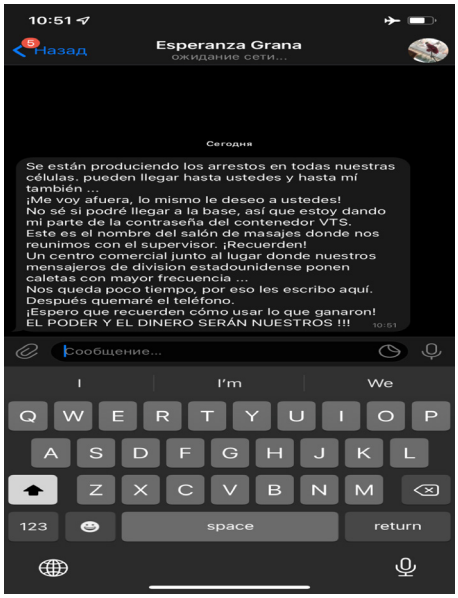
formato de respuesta:
word word... word
ejemplo:
WoW Massage Forever

Перевод текста задания:
Введите название массажного салона в торговом центре с овальной крышей
Формат ответа:
word word... word
Пример:
WoW Massage Forever

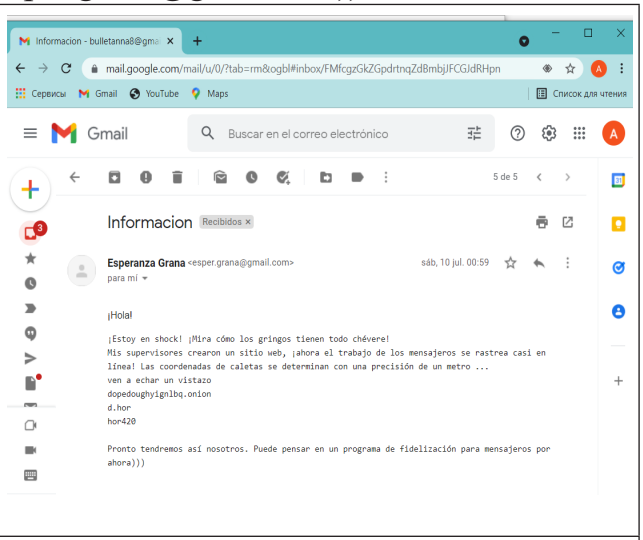
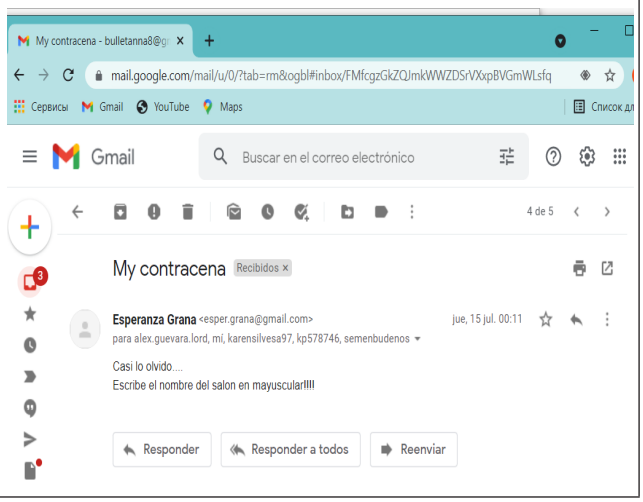


Снимок экрана с десятым заданием для сюжетной линии № 1

1. Слушателям выдаются Iphone четвёртых персонажей, в приложении Telegram они обнаружат сообщение от Esperanza Grana следующего содержания:

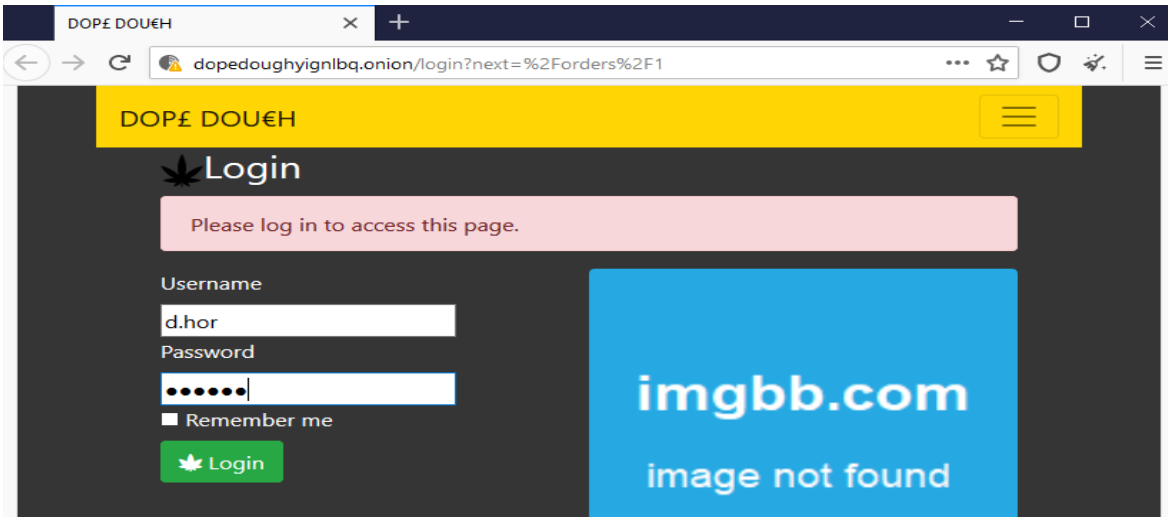
Во всех наших ячейках проходят аресты, могут добраться до вас и до меня тоже... Я сваливаю за бугор, чего и вам желаю! Не знаю, удастся ли добраться до базы, поэтому сообщаю свою часть пароля от контейнера BTC. Это название массажного салона, где мы с вами встречались у куратора. Вспоминайте! Торговый центр рядом с местом, где курьеры нашего американского подразделения чаще всего делают закладки... Времени мало, поэтому пишу сюда. Потом телефон сожгу. Надеюсь, вы помните, как надо использовать заработанное! ВЛАСТЬ И ДЕНЬГИ БУДУТ НАШИ!!!	

2. Слушатели должны обратиться к сообщениям, полученным в рамках второго задания интерактивной игры, в почтовом сервисе Google аккаунта первого персонажа (входящие сообщения от Esperanza Grana (esper.grana@gmail.com))

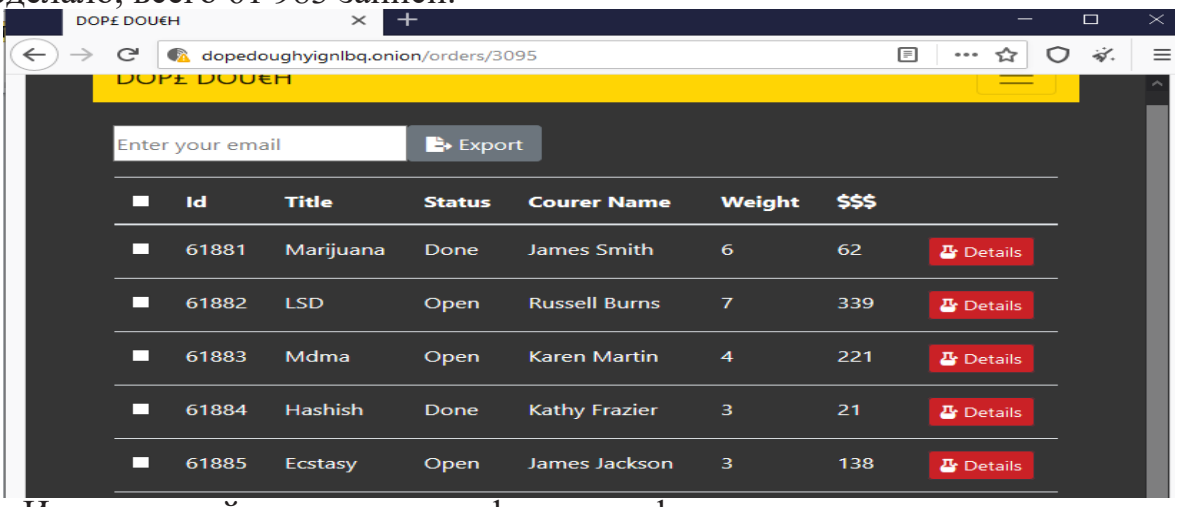
Перевод: Привет! Я в шоке! Смотри, как у американцев все четко! Мои кураторы сделали сайт – теперь работу курьеров отслеживают практически онлайн! Координаты закладок с точностью до метра определяют ... зайди глянь dopedoughyignlbq.onion d.hor hor420 Скоро и у нас так будет. Можешь пока программу лояльности для курьеров придумать)))	
Перевод: Я почти забыл… Напиши название салона заглавными буквами!!![1]	

1 На основе которых слушатели делают вывод, что ответ необходимо вводить заглавными буквами.

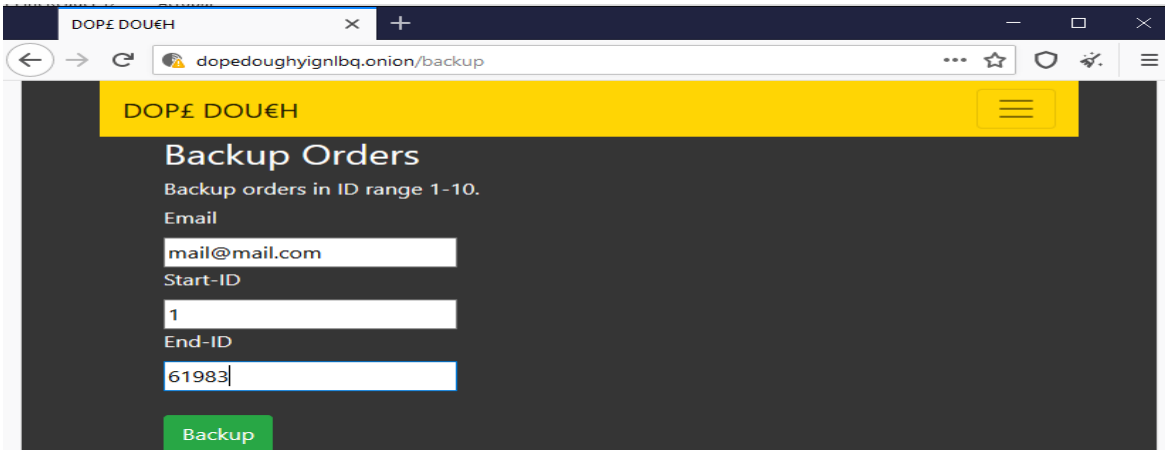
Слушатели переходят на ресурс в Даркнете dopedoughyignlbq.onion, на котором авторизуются с указанным логином и паролем.



На ресурсе имеются данные о статусе закладки с наркотиком и лице, которое ее сделало, всего 61 983 записи.



Исследуемый ресурс имеет функцию формирования выгрузки данных на e-mail.

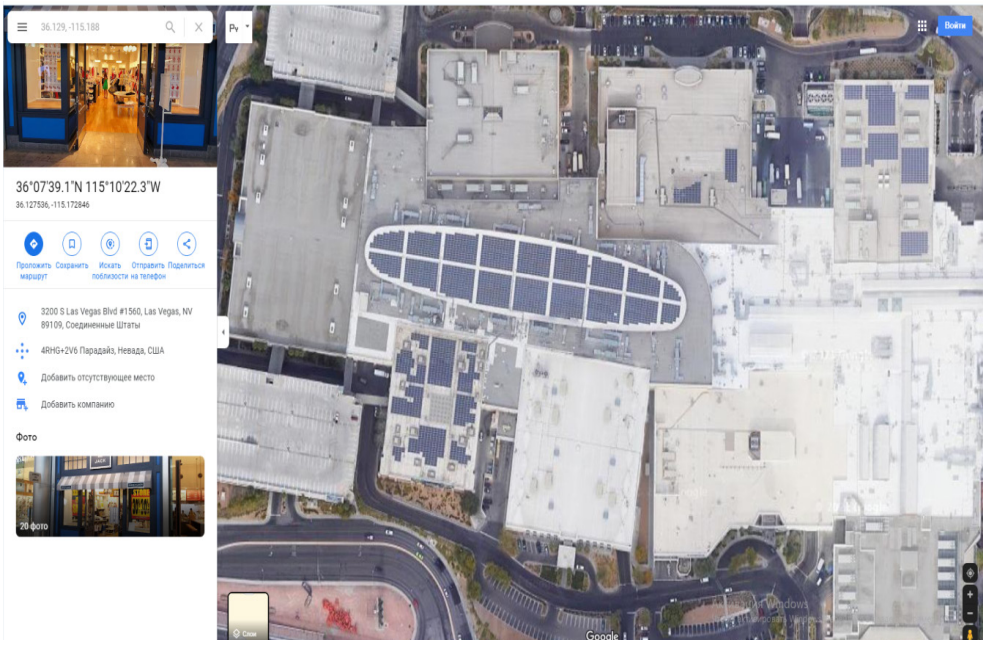


Выгружаемый файл «backup.csv» **содержит в себе больше данных о каждой закладке, в том числе геолокацию**. Слушателям необходимо определить территорию, на которой больше всего сделано закладок наркотических веществ.

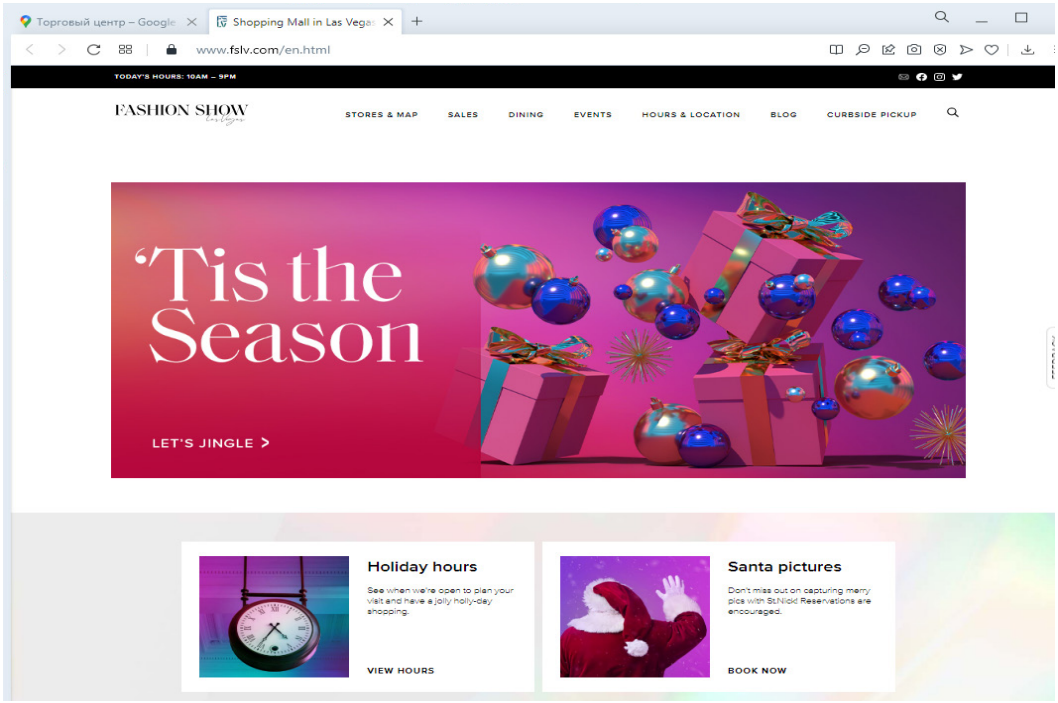
Для этого следует с использованием инструментов Microsoft Excel **совершить примерно следующие действия:**

Оригинальное содержание файла «backup.csv»	ID,Title,Description,Location,Status,Weight,Price,CourerName,Date 1,Ecstasy,Ecstasy elite shipment,39.98085632557801,-82.95365497895132,Done,7,327,Russell Burns,2020-06-25 20:33:04 2,Heroin,Heroin vip distribution,36.17701739283456,-115.13329422609739,Done,7,974,James Melton,2020-06-25 20:48:54 3,Meth,Meth budget request,33.3862661178935555,-112.24316504855486,Done,4,221,James Jackson,2020-06-25 20:49:57 4,LSD,LSD elite shipment,39.90408713025035,-82.96621025166684,Done,8,385,Lisa Lewis,2020-06-25 20:50:03 5,Marijuana,Marijuana smart order,36.11016486063127,-115.13129284212239,Done,6,54,Brittany Young,2020-06-25 20:51:34 6,Hashish,Hashish powerful distribution,36.1596409061663,-86.81444291754462,Done,4,25,Kathy Frazier,2020-06-25 20:55:38 7,Hashish,Hashish fast request,40.002169676556534,-82.97526423523703,Done,9,48,Jennifer Cooley,2020-06-25 20:58:24 8,Marijuana,Marijuana vip deliver,39.752973123462645,-86.15650324080367,Done,6,65,Jill Jenkins,2020-06-25 20:59:32 9,Meth,Meth low-cost distribution,39.94553591496814,-83.00085632582581,Done,9,509,James Adams,2020-06-25 21:00:04 10,Marijuana,Marijuana powerful transport,39.76454775966529,-86.21277821606803,Done,8,70,James Smith,2020-06-25 21:23:02 11,Marijuana,Marijuana discounted distribution,39.78416472508656,-86.16404113619183,Done,7,64,Joe Vazquez,2020-06-25 21:27:29 12,Amphetamine,Amphetamine secure request,33.46366181709506,-112.32097948324537,Done,4,48,Michael Adams,2020-06-25 21:39:57 13,Meth,Meth discounted transport,39.78477506429844,-86.10680681225453,Done,7,395,Joe Vazquez,2020-06-25 21:44:21 14,Marijuana,Marijuana express request,36.15467281221279,-115.28348673679317,Done,5,47,Brittany Young,2020-06-25 21:49:28
Разделить и перевести сведения в сводную таблицу	5 Marijuana Marijuana smart order 36,11016486 -115,1312928 Brittany Young 25.06.2020 6 Hashish Hashish powerful distribution 36,1596409 -86,81444292 Kathy Frazier 25.06.2020 7 Hashish Hashish fast request 40,00216968 -82,97526424 Jennifer Cooley 25.06.2020 8 Marijuana Marijuana vip deliver 39,75297312 -86,15650324 Jill Jenkins 25.06.2020 9 Meth Meth low-cost distribution 39,94553591 -83,00085633 James Adams 25.06.2020 10 Marijuana Marijuana powerful transport 39,76454776 -86,21277822 James Smith 25.06.2020 11 Marijuana Marijuana discounted distribution 39,78416473 -86,16404114 Joe Vazquez 25.06.2020 12 Amphetamine Amphetamine secure request 33,46366182 -112,3209795 Michael Adams 25.06.2020 13 Meth Meth discounted transport 39,78477506 -86,10680681 Joe Vazquez 25.06.2020 14 Marijuana Marijuana express request 36,15467281 -115,2834867 Brittany Young 25.06.2020 15 Crack Crack premium distribution 39,95016813 -82,96437788 Jennifer Cooley 25.06.2020
С использованием функций в колонках с широтой и долготой сократить количество знаков после запятой до 3	4 3 Meth Meth budget request 33,386 -112,243 James Jackson 25.06.2020 5 4 LSD LSD elite shipment 39,904 -82,966 Lisa Lewis 25.06.2020 6 5 Marijuana Marijuana smart order 36,110 -115,131 Brittany Young 25.06.2020 7 6 Hashish Hashish powerful distribution 36,160 -86,814 Kathy Frazier 25.06.2020 8 7 Hashish Hashish fast request 40,002 -82,975 Jennifer Cooley 25.06.2020 9 8 Marijuana Marijuana vip deliver 39,753 -86,157 Jill Jenkins 25.06.2020 10 9 Meth Meth low-cost distribution 39,946 -83,001 James Adams 25.06.2020 11 10 Marijuana Marijuana powerful transport 39,765 -86,213 James Smith 25.06.2020 12 11 Marijuana Marijuana discounted distribution 39,784 -86,164 Joe Vazquez 25.06.2020 13 12 Amphetamine Amphetamine secure request 33,464 -112,321 Michael Adams 25.06.2020 14 13 Meth Meth discounted transport 39,785 -86,107 Joe Vazquez 25.06.2020
Объединить колонки с широтой и долготой	1 Ecstasy Ecstasy elite shipment 39.981, -82.954 2 Heroin Heroin vip distribution 36.177, -115.133 3 Meth Meth budget request 33.386, -112.243 4 LSD LSD elite shipment 39.904, -82.966 5 Marijuana Marijuana smart order 36.11, -115.131 6 Hashish Hashish powerful distribution 36.16, -86.814 7 Hashish Hashish fast request 40.002, -82.975 8 Marijuana Marijuana vip deliver 39.753, -86.157 9 Meth Meth low-cost distribution 39.946, -83.001 10 Marijuana Marijuana powerful transport 39.765, -86.213
Определить координаты, которые чаще всего повторяются	Названия строк Количество по полю 36.129, -115.188 77 36.13, -115.188 59 36.129, -115.187 32 36.13, -115.189 31 36.129, -115.189 29 36.13, -115.187 18 36.169, -86.798 15 36.151, -86.79 13 36.16, -86.772 13 36.165, -86.773 13 36.173, -86.779 13 36.128, -115.189 12 36.164, -86.794 12 36.154, -86.8 11

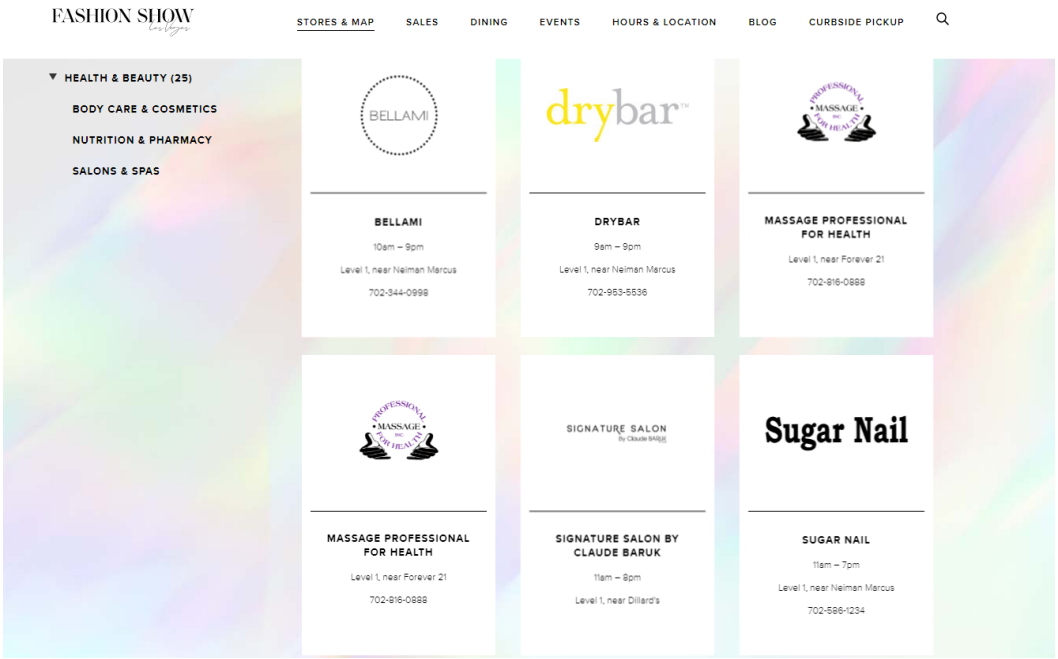
На основании полученной информации слушатель должен начать осматривать с помощью ресурсов GoogleКарты или ЯндексКарты территорию по найденным координатам для установления торгового центра с овальной крышей:



Далее следует перейти на сайт данного торгового центра.



В подразделе «Салоны и спа» раздела «Здоровье и красота» перечислены все имеющиеся салоны.



Путем перебора возможных вариантов слушатели находят правильный ответ.

После ввода в Систему электронного обучения Воронежского института МВД России правильного ответа слушателям на экран выводится сообщение следующего содержания:

«Felicitaciones, probablemente escontramos la contraseña! Y ahora, queda ver, que hay en el contenedor!»

Перевод: «Поздравляю, пароль вроде нашли! Ну что, осталось посмотреть, что в контейнере!»

Слушатели получают возможность перейти к одиннадцатому заданию.

Задание 11. Открыть контейнер с помощью пароля и ключевого файла

Данное задание предусматривает отработку и закрепление теоретических знаний и практических навыков по использованию приложений для работы с криптоконтейнерами на примере VeraCrypt в рамках следующих тем:

2.1. Сеть Интернет как источник информации. Веб-ресурсы и методы получения доступа к ним.

2.2. Программные и программно-аппаратные средства, используемые для аналитической обработки информации. .

3.2. Особенности первоначального этапа расследования преступлений в сфере компьютерной информации.

3.3. Особенности последующего и заключительного этапов расследования преступлений в сфере компьютерной информации.

4.4. Выявление и сохранение значимой информации со средств вычислительной техники и программного обеспечения.

5.1. Средства анонимизации и деанонимизации в сети Интернет.

5.2. Использование веб-ресурсов для получения данных о недвижимости, транспорте, физических и юридических лицах.

5.3. Поиск и анализ информации в сети Интернет в целях выявления преступлений в сфере компьютерной информации.

Слушатели после успешного завершения десятого задания переходят к решению одиннадцатого**:**

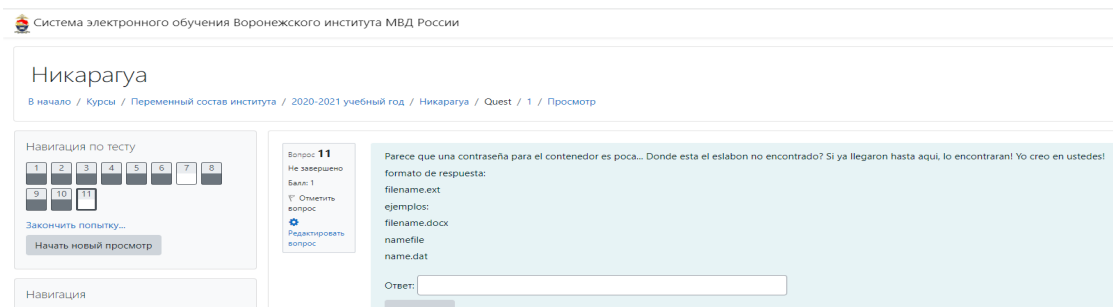
Parece que una contraseña para el contenedor es poca... Donde esta el eslabon no encontrado? Si ya llegaron hasta aqui, lo encontraran! Yo creo en ustedes!

formato de respuesta:
filename.ext
ejemplos:
filename.docx
namefile
name.dat

Перевод текста задания:

Кажется одного пароля для контейнера мало**...** где же это недостающее звено? Уж если вы сюда добрались, то точно найдете!

Формат ответа:
filename.ext
Примеры:
filename.docx
namefile
name.dat



Путем анализа содержимого флеш карты слушатели должны найти файл под названием «el gato elena vera.jpg», слово «vera» является ключевым и должно натолкнуть их на мысль, что оно и является ключевым.

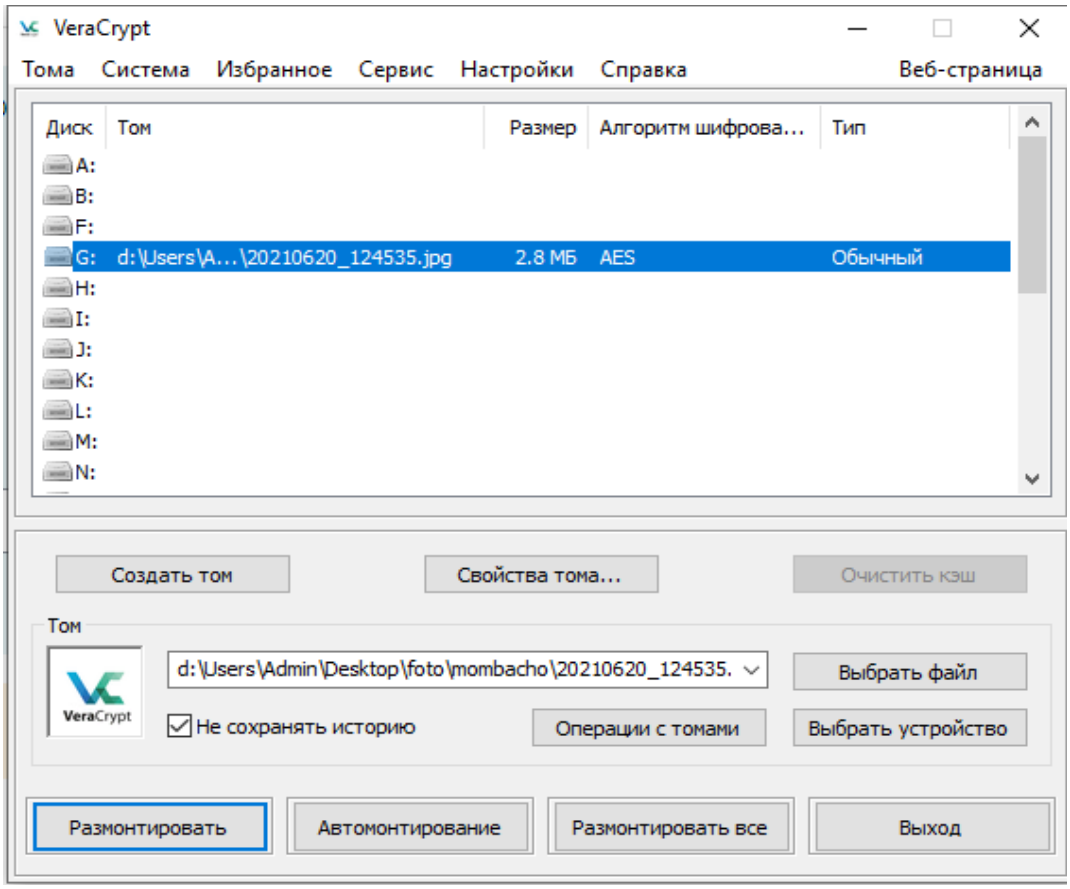
..			Папка с файлами		
a mi madre.jpeg	335 194	248 576	Файл "JPEG"	27.06.2021 21:34	A3E24FB4
amor en Esplendor.jpg	105 678	105 678	Файл "JPG"	27.06.2021 20:59	98455D6C
Antonio Machado.docx	12 061	9 337	Документ Micros...	27.06.2021 21:11	7FBC8155
Bilingüe-Porque-hablo-español.png	99 569	99 569	Файл "PNG"	27.06.2021 21:31	0914A3F1
como si fuera.png	275 731	275 731	Файл "PNG"	27.06.2021 21:04	846F9562
cuando pienso en ti.jpeg	269 517	211 906	Файл "JPEG"	27.06.2021 21:34	06E3EA09
cuanto.jpg	192 458	191 393	Файл "JPG"	27.06.2021 21:29	1E5AE068
donde tu no Estas.jpg	278 255	207 194	Файл "JPG"	27.06.2021 21:01	DA4A36E6
el gato elena vera.jpg	28 303	28 195	Файл "JPG"	26.06.2021 21:15	50825925
el primer Beso.jfif	14 907	14 907	Файл "JFIF"	27.06.2021 21:00	15DC40C4
Es muy importante.docx	11 911	9 188	Документ Micros...	27.06.2021 21:06	A331264A
fabian ruiz.jpeg	307 250	249 490	Файл "JPEG"	27.06.2021 21:35	1FDEA03C
FRANCISCO DE QUEVEDO.docx	12 136	9 410	Документ Micros...	27.06.2021 21:09	E86ED3DA
Julio Cortázar.docx	11 967	9 242	Документ Micros...	27.06.2021 21:08	94895815
La guitarra.docx	12 001	9 273	Документ Micros...	27.06.2021 21:07	8ED4EDB3
LA LENGUA CASTELLANA.docx	12 058	9 343	Документ Micros...	27.06.2021 21:08	4DD976AB
LOPE DE VEG1.docx	12 062	9 342	Документ Micros...	27.06.2021 21:12	4F99E03C
LOPE DE VEGA.docx	12 055	9 328	Документ Micros...	27.06.2021 21:07	806C317D
Oriza Martins.jpg	102 967	102 967	Файл "JPG"	27.06.2021 21:03	4B2F2326
Pablo Neruda.docx	12 266	9 545	Документ Micros...	27.06.2021 21:11	E7626731
paisaje-en-espa-ol-e-ingl-s-federico-garc-a-lorca.j...	321 456	284 086	Файл "JPG"	27.06.2021 21:00	184038CC
Pasa el otoño en Madrid y el color ocre se funde a ...	12 083	9 368	Документ Micros...	27.06.2021 21:08	7E5D9B6D
poemmyfamily.jpg.crdownload	81 619	75 667	Файл "CRDOWNL...	27.06.2021 21:01	5021C171

После ввода в Систему электронного обучения Воронежского института МВД России правильного ответа слушателям на экран выводится сообщение следующего содержания:

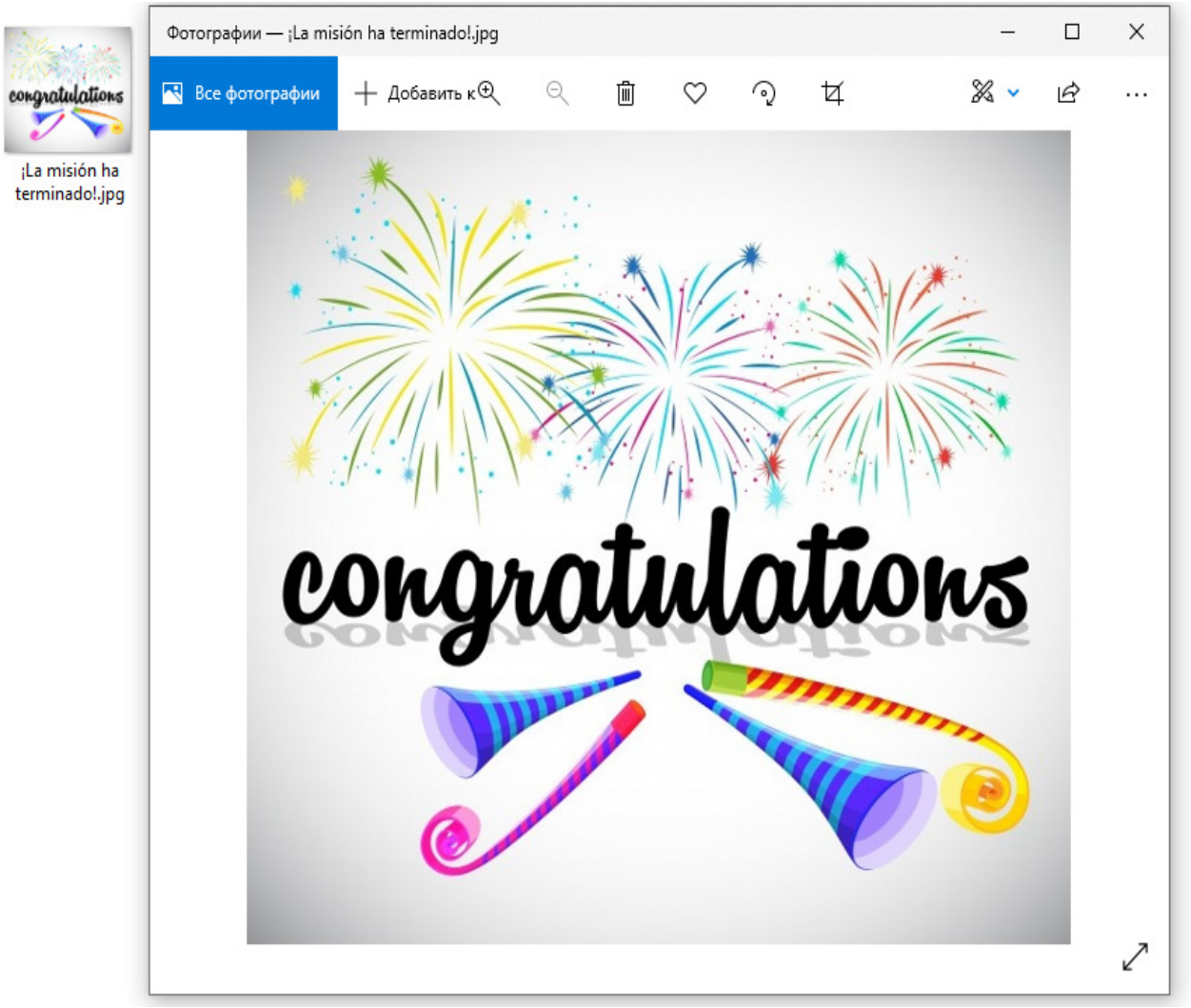
«Es todo - monten el contenedor!»

Перевод: «Ну всё - монтируйте контейнер!»

Слушатели получают возможность воспользоваться ключевым файлом, паролем (задание № 10), чтобы открыть криптоконтейнер (задание № 9).



В контейнере находится файл поздравления с успешным прохождением интерактивной игры



Заключение

Современные кейс-технологии позволяют слушателям овладеть знаниями в сфере поиска и фиксации информации относительно динамичных взаимосвязанных объектов на ресурсах сетей Интернет и Даркнет и выработать соответствующие навыки в фактически реальных условиях.

Использование данного метода обучения способствует:

– формированию у слушателей навыков использования методов конкурентной разведки, свободно распространяемого и специализированного программного обеспечения в реальных условиях и на реальных объектах информатизации;

– развитию у слушателей способностей к саморазвитию и формированию навыков самостоятельной интерпретации полученных результатов.

Участие в интерактивной игре позволяет слушателю демонстрировать личный уровень компетенций в сфере противодействия преступлениям, совершенным с использованием информационных технологий, а также стимулирует его к достижению лучших показателей в учебно-служебной деятельности.

Использование в учебном процессе Системы электронного обучения Воронежского института МВД России позволяет преподавателю осуществлять:

– дистанционный мониторинг вводимых ответов;

– контроль хода решения задания, не привлекая внимания слушателей;

– корректировку направления прохождения интерактивной игры;

– ранжирование достижений обучающихся;

– при необходимости оценку результатов выполнения каждого задания отдельно.

Условия и требования

Время: 900 мин.

Место проведения занятия:

Аудиторный фонд, предназначенный для проведения лекционных и практических занятий, оборудованный необходимыми техническими средствами обучения, мультимедийной и компьютерной техникой с доступом к сети Интернет.

Программное обеспечение:

Операционная система Microsoft Windows 7 Professional (x64);

Пакет офисных программ Microsoft Office;

Браузеры Tor, Chrome, Yandex, Opera;

Действующие аккаунты Facebook, Google, Instagram, Skype, Telegram, Twitter, Viber, WhatsApp, Yandex;

Приложения Telegram, WhatsApp, Skype, Viber для OS Windows и мобильные версии;

Специализированное программное обеспечение «Belkasoft» версия не ниже «Belkasoft Evidence Center 9.9800 сборка 5195» (производитель ООО «Белкасофт»);

Специализированное программное обеспечение «ElcomSoft» версия не ниже «Elcomsoft Premium Forensic Bundle» (производитель ООО «Элкомсофт»);

Утилиты работы с архивными файлами (WinZip, WinRar, Advanced Archive Password Recovery: Professional Edition 4.5x);

– Secret Layer версия не ниже 2.8.1;

– IBM I2 Analyst Notebook;

– VeraCrypt 1.24.

Материально-технические условия реализации программы

1. Персональные компьютеры, объединенные в локальную сеть с выходом в Интернет.
2. Смартфоны с операционной системой Android (11 шт.).
3. Смартфоны с операционной системой iOS (10 шт.).
4. Активные SIM-карты с положительным балансом (по количеству смартфонов).

Список использованных источников

Нормативные правовые акты и иные официальные документы

1. Уголовный кодекс Республики Никарагуа : Закон Республики Никарагуа № 641, с изм., внесенными законом Республики Никарагуа № 952 [es.]. URL: https://www.asamblea.gob.ni.

2. Уголовно-процессуальный кодекс Республики Никарагуа : Закон Республики Никарагуа № 406 [es.]. URL: https://www.asamblea.gob.ni.

3. Специальный Закон Республики Никарагуа «О Киберпреступлениях» № 1042, утвержденный 27.10.2020 // La Gaceta, Diario Oficial.2020. № 201.

Научная и учебная литература:

1. Аббазова, А.Р. Промышленный шпионаж, конкурентная разведка /А.Р. Аббазова, С.А. Сулейманова // Академическая публицистика. – 2019. – № 5. – С. 130-133.

2. Алавердов, А.Р. Управление кадровой безопасностью организации : учебник / А.Р. Алавердов. – М.: Маркет ДМ, 2008. – 176 с.

3. Анонимизация и деанонимизация в сети Интернет. URL: https://habr.com/ru/articles/137416/.

4. Баяндин, Н. Конкурентная разведка как основной элемент информационного противоборства в бизнесе / Н. Баяндин, В. Креопалов, С. Куликова // Риск: Ресурсы, Информация, Снабжение, Конкуренция. – 2017.– № 1. – С. 38-42.

5. Бондарчук, Н.В. Бизнес-разведка. Практикум : учебное пособие / Н.В. Бондарчук, А.А. Курашова. – 2-е изд. – М., 2020. – 138 с.

6. Артамонов, В.А. Методы анонимизации в сети интернет / А.В. Артамонов, Е.В. Артамонова. URL: http://itzashita.ru/publications/metodyi-anonimizatsii-v-seti-internet.html.

7. Важенина, И.С. Особенности и перспективы создания службы конкурентной разведки в структуре российских компаний / И.С. Важенина, С.Г. Важенин, В.Е. Ющук // Менеджмент в России и за рубежом. – 2019. – № 4. – С. 72-81.

8. Иванов, Д.Д. Классификация методов осуществления конкурентной разведки на предприятии / Д.Д. Иванов // Санкт-Петербургский научный вестник. – 2021. – № 2 (11). – С. 3.

9. Иванов, С. А. Основы деловой (конкурентной) разведки : учебное пособие / С.А. Иванов, С.Ю. Микадзе. – СПб.: Санкт-Петербургский государственный экономический университет, 2020.

10. Илякова, И.Е. Конкурентная разведка / И.Е. Илякова, С.Э. Майкова. – Саранск, 2018.

11. Коваленко, А.П. Некоторые направления добывания компьютерной информации при проведении конкурентной (экономической) разведки / А.П. Коваленко, Г.И. Москвитин // Вопросы защиты информации. – 2017. –№ 3 (118). – С. 54-56.

12. Конкурентная разведка в интернете: технологии и инструменты поиска информации / Д.Г. Маслов, А.А. Тусков, З.А. Дивненко [и др.] // Фундаментальные исследования. – 2015. – № 5-3. – С. 631-634.

13. Конкурентная разведка. Ч. 2 / Е.Л. Ющук [и др.]. – Екатеринбург, 2016.

14. Конкурентная разведка: технологии и противодействие / В.И. Аверченков [и др.]. – 2-е изд., стереотип. – М., 2017.

15. Кравцов, А.А. Особенности профессионально-педагогического целеполагания при преподавании студентам дисциплины «конкурентная разведка» / А.А. Кравцов // Вестник Московского государственного лингвистического университета. Образование и педагогические науки. – 2016. – № 8 (747). – С. 85-92.

16. Миненко, П.В. Массивы компьютерной информации как объект оперативно-розыскных мероприятий / П.В. Миненко, А.В. Пучнин // Общество и право. – 2020. – № 4 (74). – С. 87-91.

17. Неизвестный GOOGLE: 42 оператора расширенного поиска Google. URL: https://oko-planet.su/politik/politwar/613911-neizvestnyy-google-42-operatora-rasshirennogo-poiska-google-polnyy-spisok.html.

18. Павлов, А.В. Конкурентная разведка : учебное пособие / А.В. Павлов, Б.И. Ткаченко, А.М. Шунаев. – СПб.: Санкт-Петербургский государственный экономический университет, 2020.

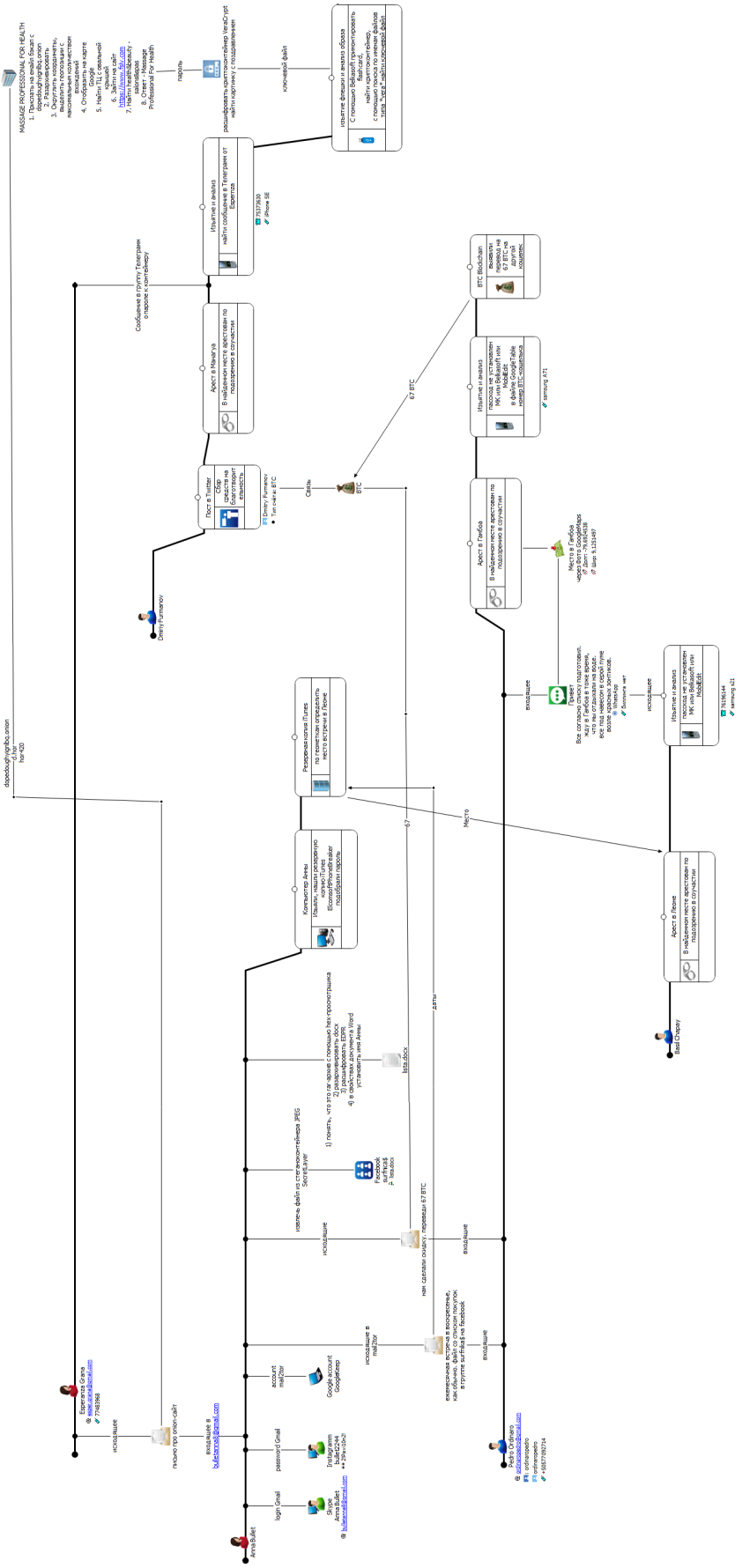
19. Пучнин, А.В. Создание и развитие «фермы аккаунтов» в социальных сетях как этап подготовки к противоправному деянию / А.В. Пучнин, П.В. Миненко // Вестник Воронежского института МВД России. – 2020. – № 3. – С. 219-228.

20. Федосеев, А.Э. Конкурентная разведка в деятельности правоохранительных органов / А.Э. Федосеев, И.Н. Архипцев // Преступность в сфере информационных и телекоммуникационных технологий: проблемы предупреждения, раскрытия и расследования преступлений. – 2021. – № 7. – С. 91-96.

21. Шумков, Е.А. Конкурентная разведка в сети Интернет для вуза / Е.А. Шумков // Научные труды КубГТУ. – 2016. – № 3. – С. 67-72.

22. Ющук, Е.Л. Интернет-разведка: руководство к действию / Е.Л. Ющук. – М., 2007.

Схема взаимодействия участников преступной группы (персонажей интерактивной игры) на примере сюжетной линии № 1



План-график
выпуска учебных и научных издания № 31

А.В. Пучинин,
А.Д. Попов,
В.А. Цилик

Применение современных методов обучения иностранных слушателей по программам противодействия преступлениям, совершаемым с использованием информационно-телекоммуникационных технологий

Учебно-методическое пособие

Подготовлено к изданию А.О. Скудрой, Ю.В. Леонтьевой.

Подписано в печать *19.10.2023*
Формат Р 60х84. Бумага типографская. Гарнитура Times.
Печать офсетная. 5,0 усл.печ.л.
Тираж 100 экз. Заказ XXX.

Научно-исследовательский и редакционно-издательский отдел.
Сибирский юридический институт МВД России.
660131, г. Красноярск, ул. Рокоссовского, 20.

Отпечатано в типографии НИРИО СибЮИ МВД России.
660050, г. Красноярск, ул. Кутузова, 6.