Воронежский институт МВД России

А. В. Пучнин
Р. А. Солодуха

Использование современных информационных технологий в противодействии преступлениям (кейс-технология)

Учебно-методическое пособие

Воронеж

2022

ББК 67.4

Рецензенты: Кузнецов Е.Ю. – заместитель начальника Управления уголовного розыска ГУ МВД России по Воронежской области, полковник полиции; Суров О.А. – начальник Учебного центра (филиала) Сибирского юридического института МВД России в г. Манагуа, к.ю.н., полковник полиции.

Пучнин А.В.

Использование современных информационных технологий в противодействии преступлениям (кейс-технология) : учебно-методическое пособие [Электронный ресурс] / А.В. Пучнин, Р.А. Солодуха. – Электр. дан. и прогр. – Воронеж : Воронежский институт МВД России, 2022. –1 электр. опт. диск (CD-ROM) : 12 см. – Систем. требования: процессор Intel с частотой не менее 1,3 ГГц ; ОЗУ 512 Мб ; операц. система семейства Windows ; CD-ROM дисковод.

Методическая разработка предназначена для применения при организации и проведении занятий семинарского типа с использованием кейс-технологий.

Сценарий интерактивной игры предусматривает решение ситуационных задач с различными сюжетными линиями.

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

ISBN 978-5-88591-889-3

СОДЕРЖАНИЕ

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 них 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.

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 нормативным правовым актам 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;

– 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.

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 социальных 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

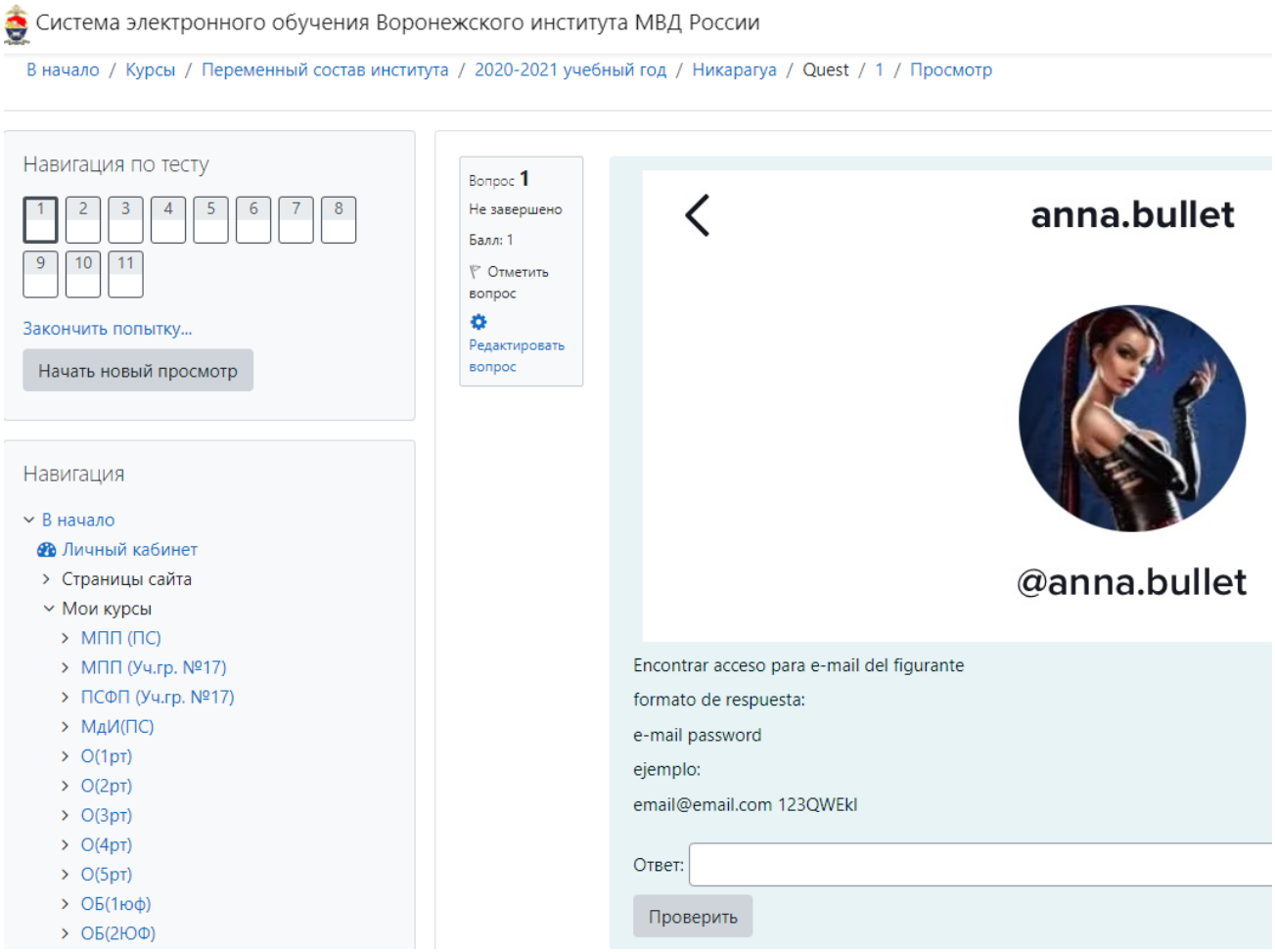
Данное задание предусматривает отработку и закрепление теоретических знаний и практических навыков мониторинга социальных сетей и мессенджеров в рамках следующих тем:

1. Понятие и общая характеристика преступлений в сфере компьютерной информации по законодательству Российской Федерации.
2. Криминологическая характеристика и профилактика компьютерных преступлений.
3. Сеть Интернет как источник информации. Веб-ресурсы и методы получения доступа к ним.
4. Криминалистическая характеристика преступлений в сфере компьютерной информации.
5. Особенности первоначального этапа расследования преступлений в сфере компьютерной информации.
6. Средства анонимизации и деанонимизации в сети Интернет.
7. Использование веб-ресурсов для получения данных о недвижимости, транспорте, физических и юридических лицах.
8. 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:

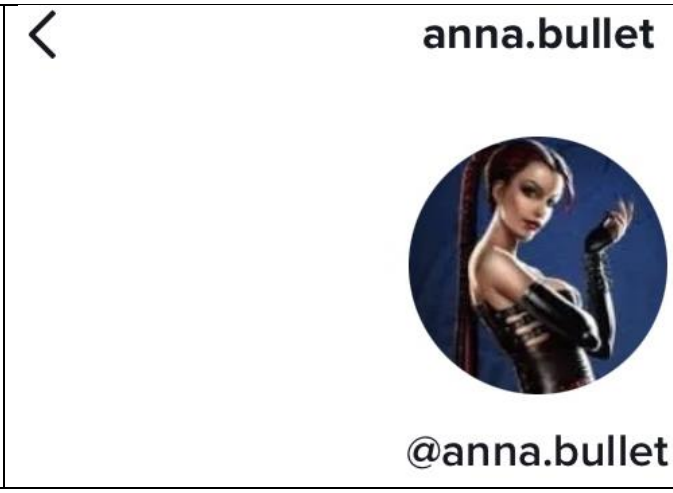
Encontrar acceso para e-mail del figurante.
formato de respuesta:
e-mail password
ejemplo:
email@email.com 123QWEkl

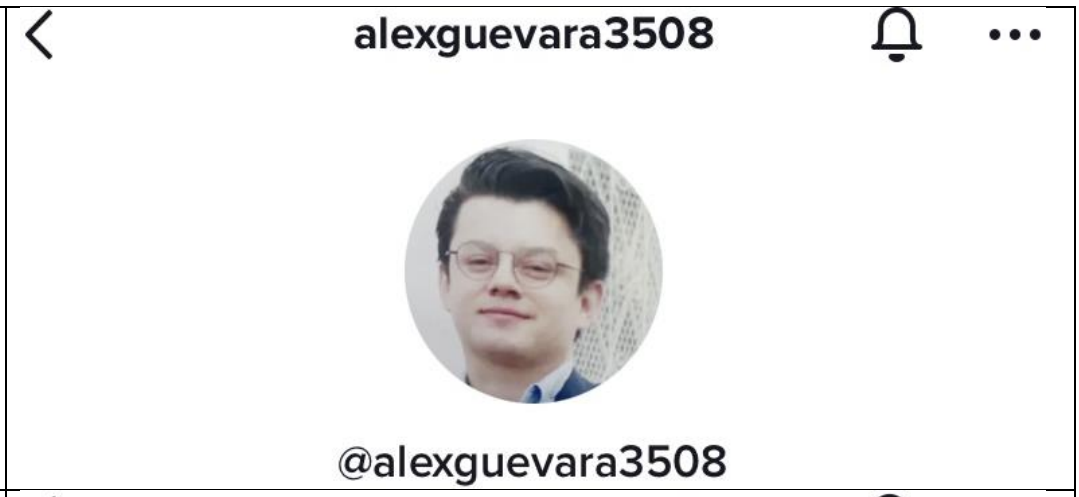
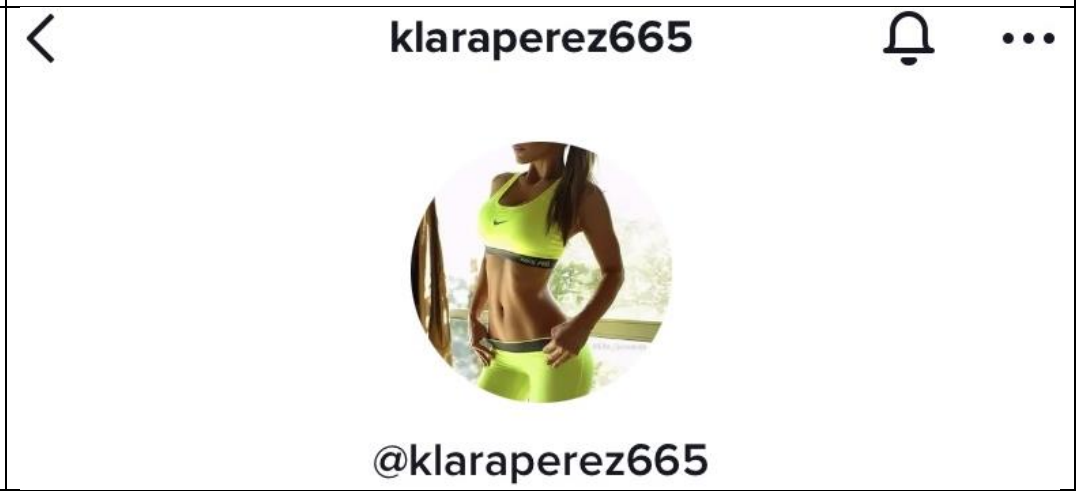
Перевод текста задания:
Получить доступ к e-mail фигуранта
Формат ответа:
e-mail password
Пример:
email@email.com 123QWEkl



Снимок экрана с первым заданием для сюжетной линии № 1

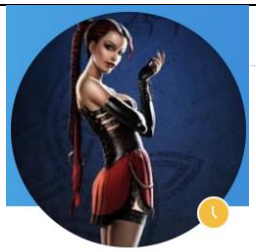
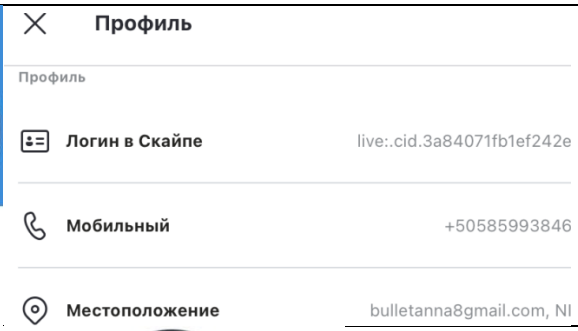
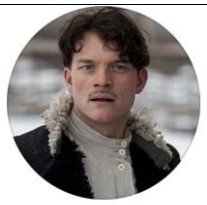
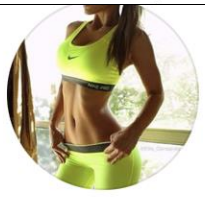
На данном этапе слушатель (подгруппа) на странице Системы электронного обучения Воронежского института МВД России в зависимости от выбранной сюжетной линии получает один из 5 снимков экрана из социальной сети TikTok:

Первая сюжетная линия:	

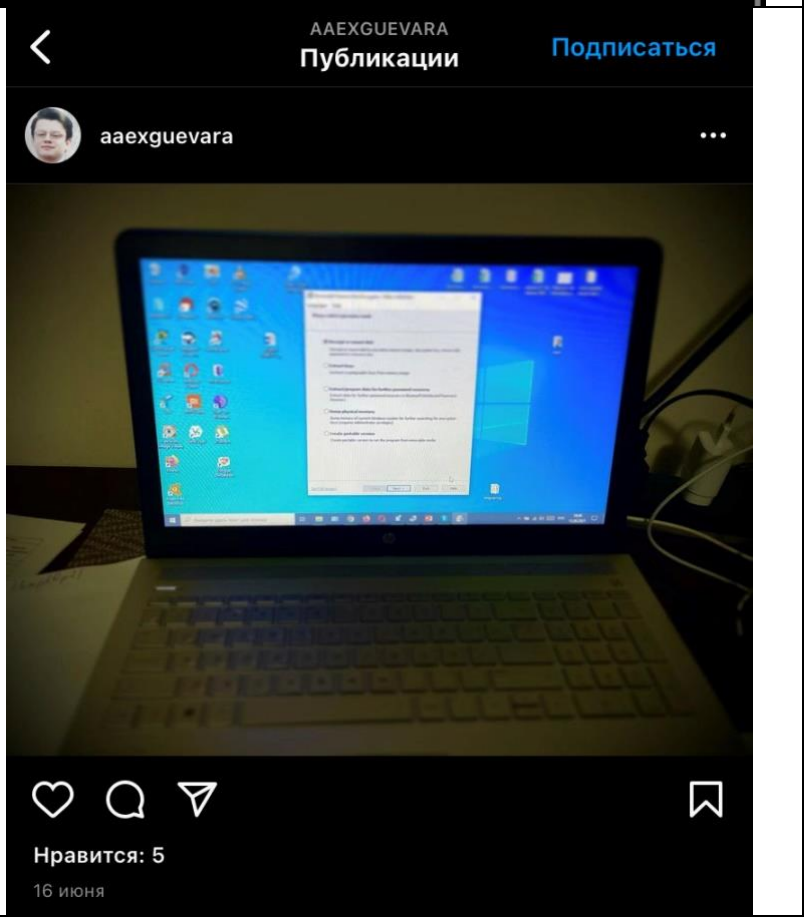
Вторая сюжетная линия:	
Третья сюжетная линия:	
Четвертая сюжетная линия:	
Пятая сюжетная линия:	

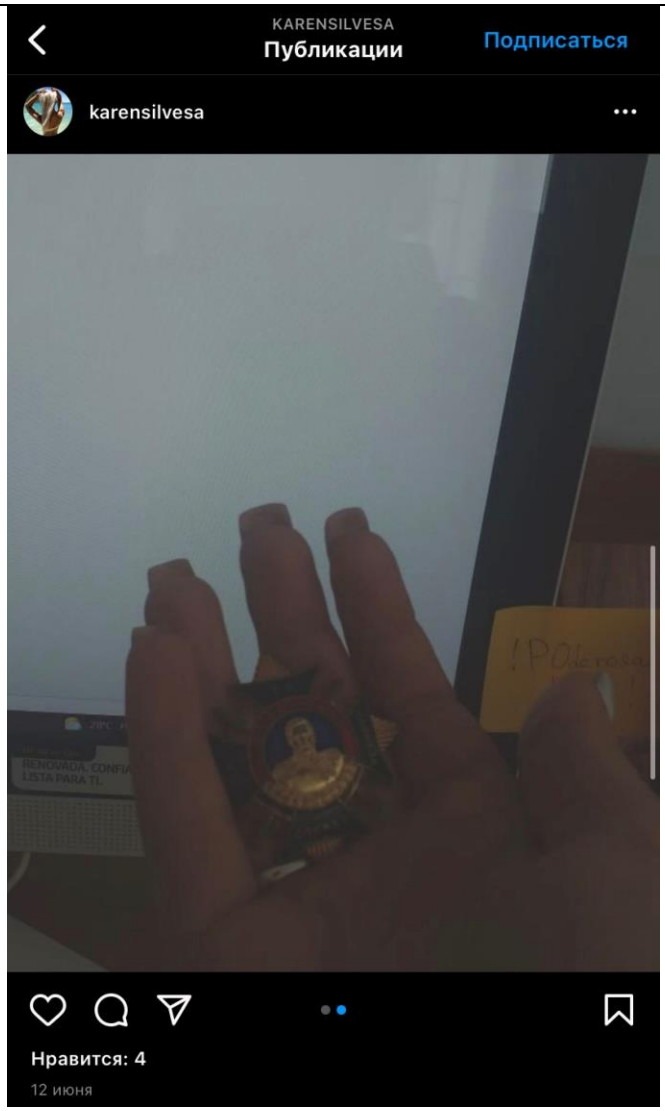
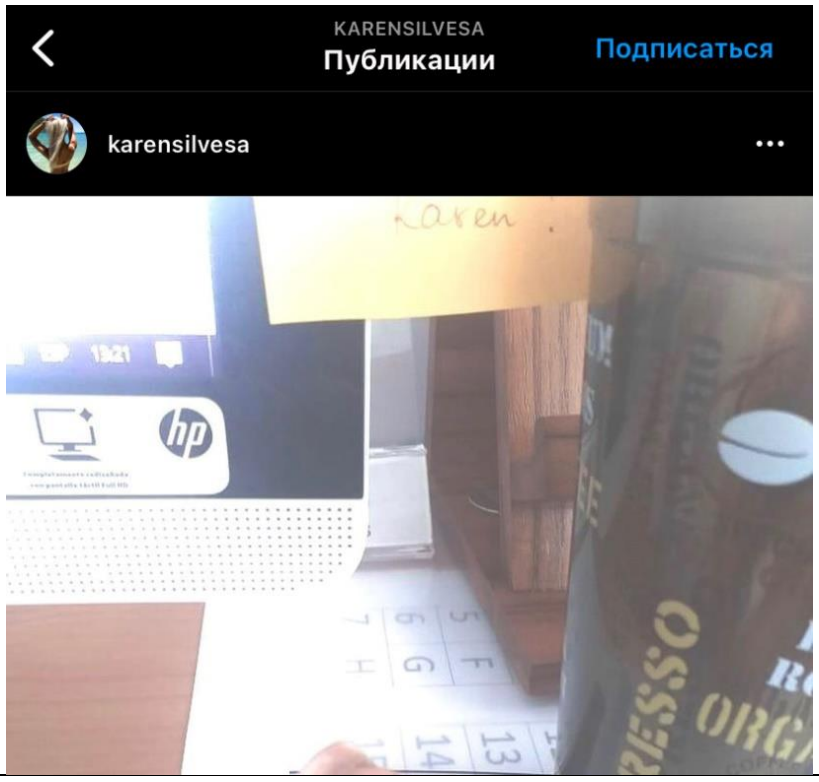
В ходе решения задания слушатели на основе имеющихся исходных данных (фотография, профиль и никнейм) должны обнаружить страницы игрового фигуранта на Facebook, Instagram, Twitter, WhatsApp, Skype, Viber и проанализировать их содержимое. Ответ на первое задание будет содержаться в открытом доступе на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

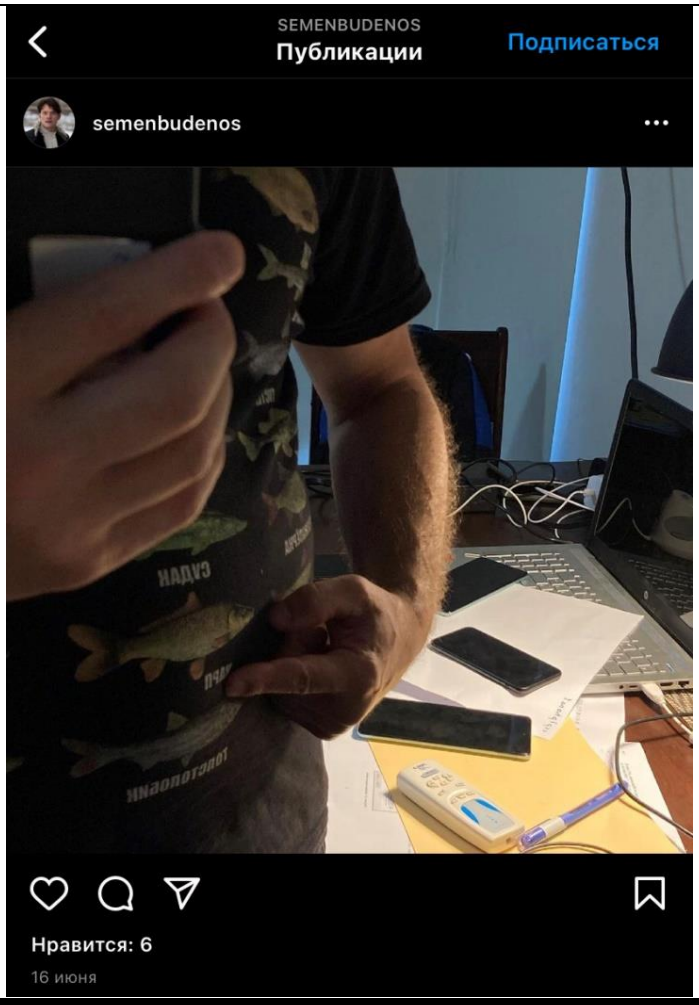
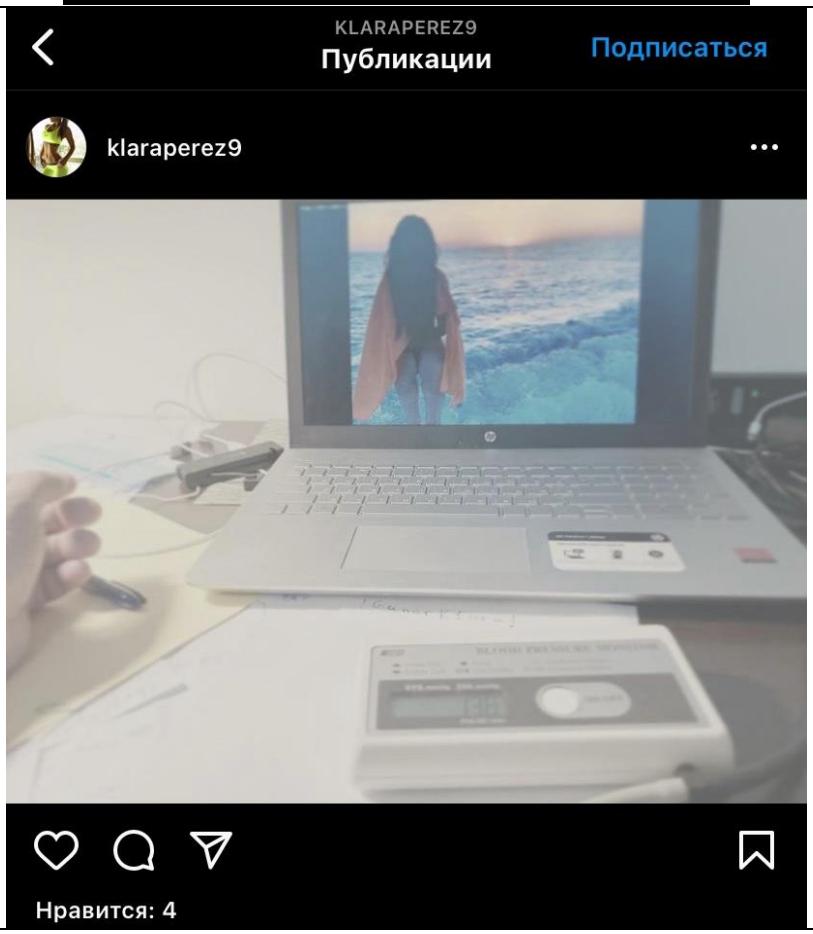
Учетные данные Skype содержат искомый адрес электронной почты с технической ошибкой, которую слушатели при дальнейшем прохождении должны выявить и устранить.

Первая сюжетная линия: (отсутствует символ «@» – коммерческое „эт“)	 Anna Bullet 
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
Пятая сюжетная линия: (отсутствует символ «@» – коммерческое „эт“ и доменная зона «com»)	 Perez Klara Kp578746gmail

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:

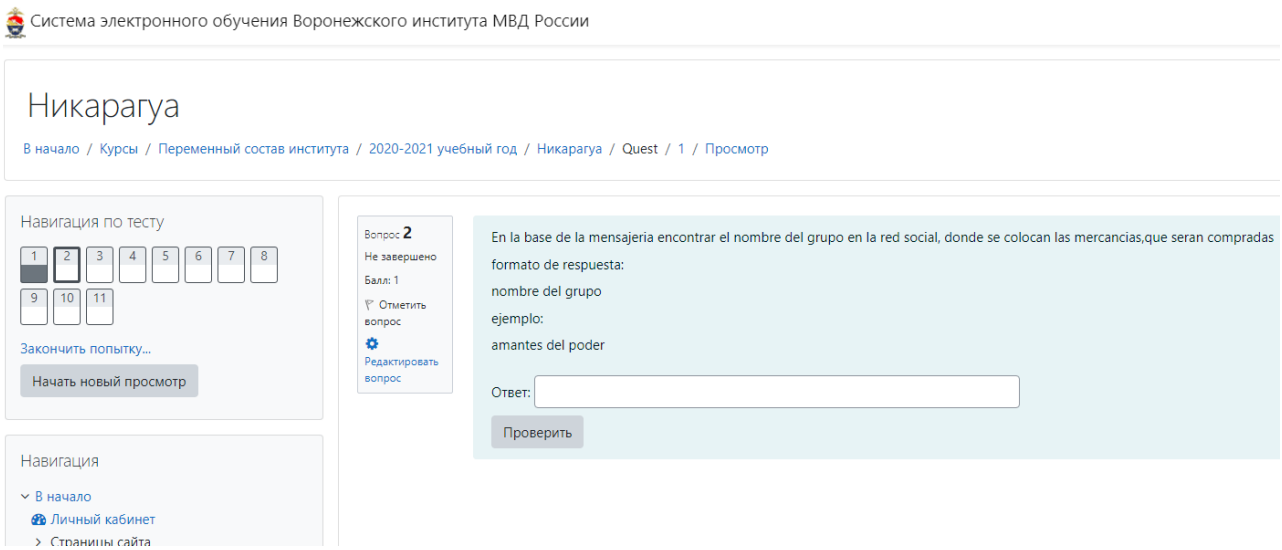
En la base de la mensajeria encontrar el nombre del grupo en la red social, donde se colocan las mercancias,que seran compradas.

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

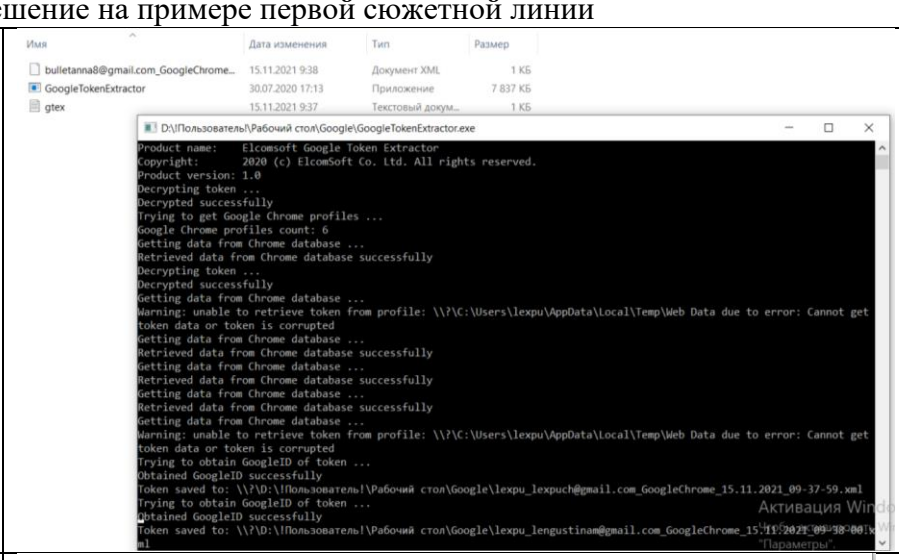
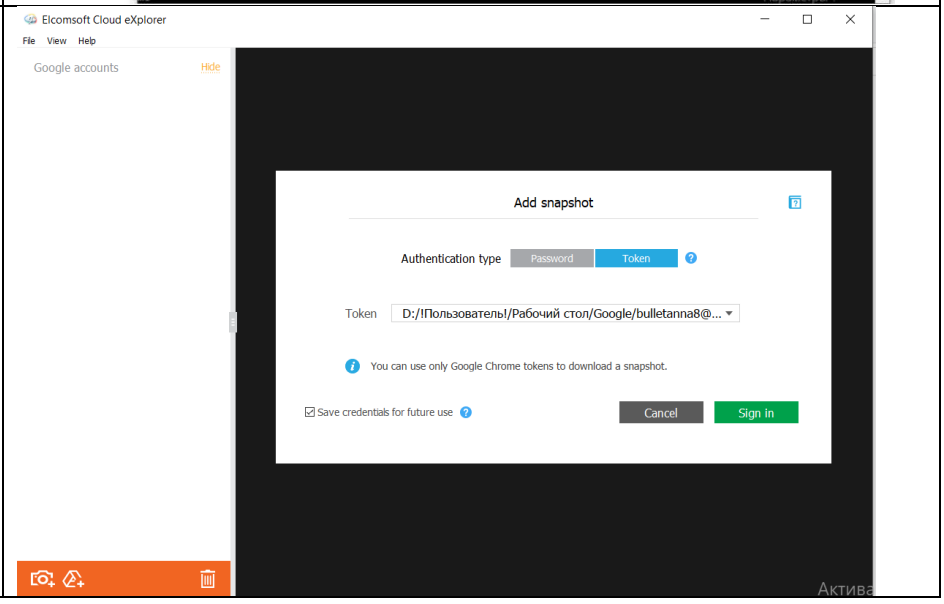


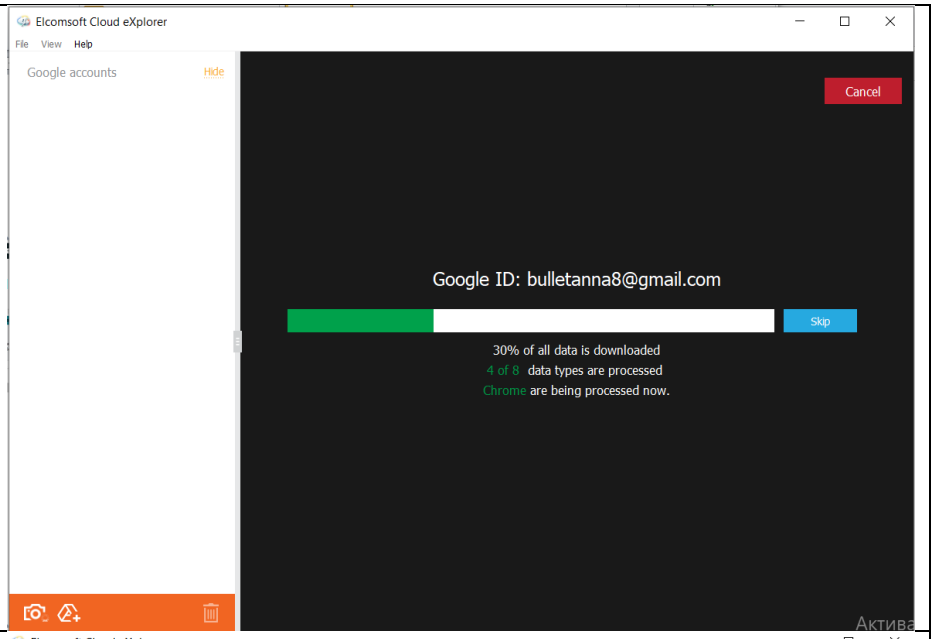
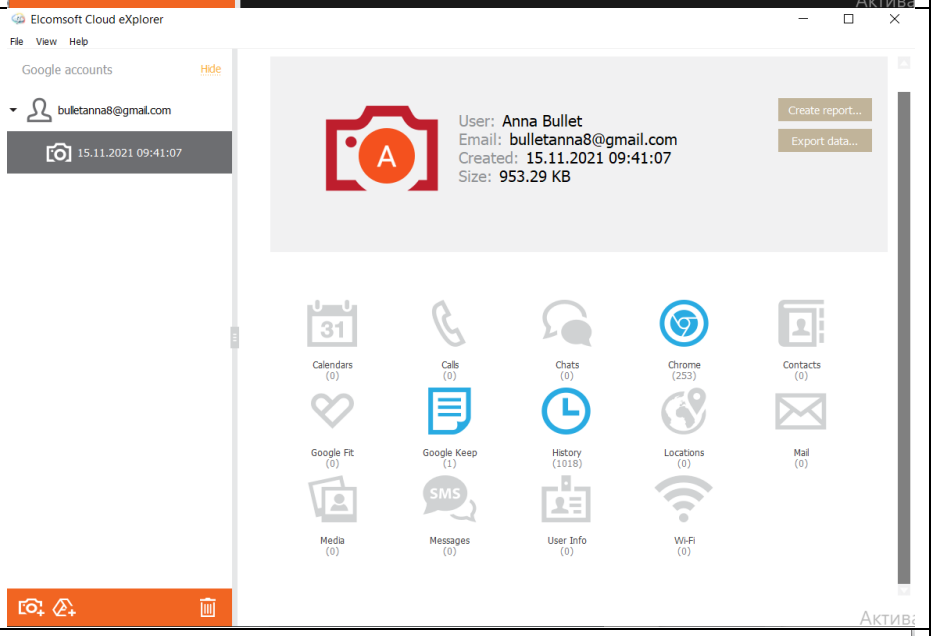
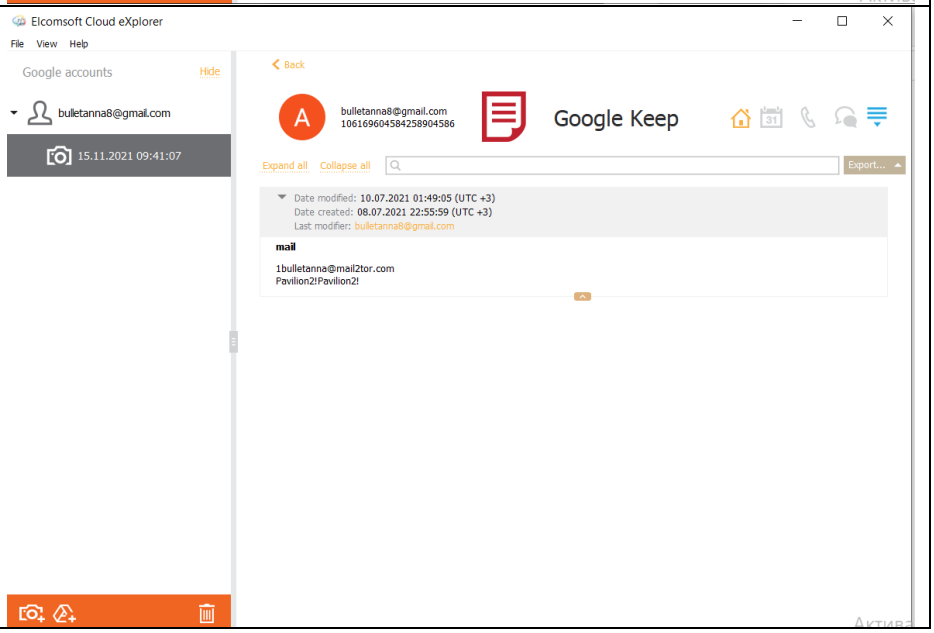
Снимок экрана со вторым заданием для сюжетной линии № 1

Основные этапы решения:

1. Анализ содержимого Google-аккаунта:

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

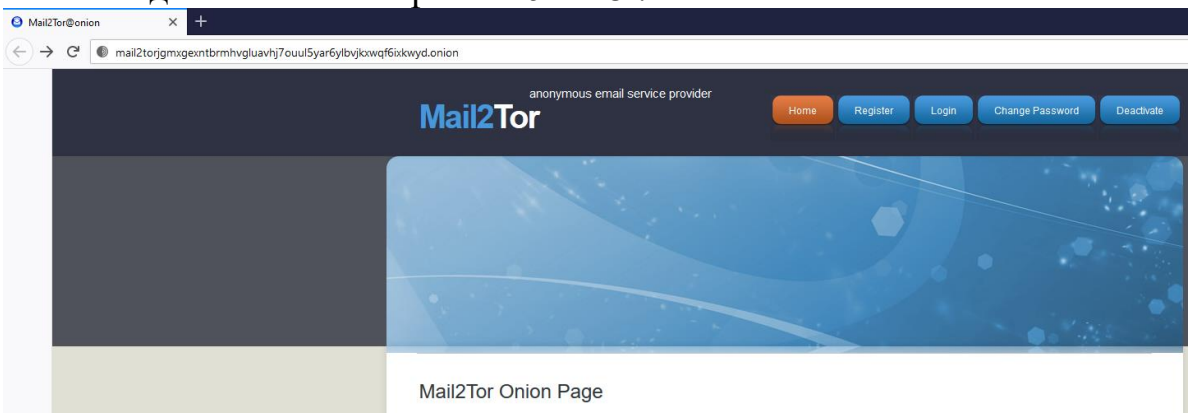
Решение на примере первой сюжетной линии	
с помощью специальной утилиты Elcomsoft Cloud eXplorer обнаруживает токен авторизации к облачным сервисам Google	
выбирает токен от учетной записи пользователей Google	

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	

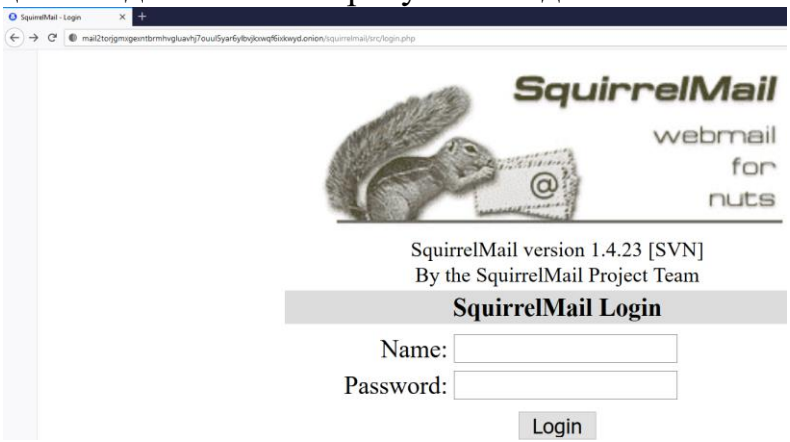
2. Анализ содержимого почтового сервиса в Даркнете, для этого слушатель:

– 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 | Download this as a file ¡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

<table>
<tr>
<td>Вторая сюжетная линия:</td>
<td>
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 <u>Mineros de Nicaragua.</u> 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
</td>
</tr>
<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>
</table>

Четвертая сюжетная линия:	**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
Пятая сюжетная линия:	**Subject:** Una reunión **From:** klaraperez5@mail2tor.com **Date:** Thu, July 8, 2021 6:32 pm **To:** adol.rub.q5@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 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.

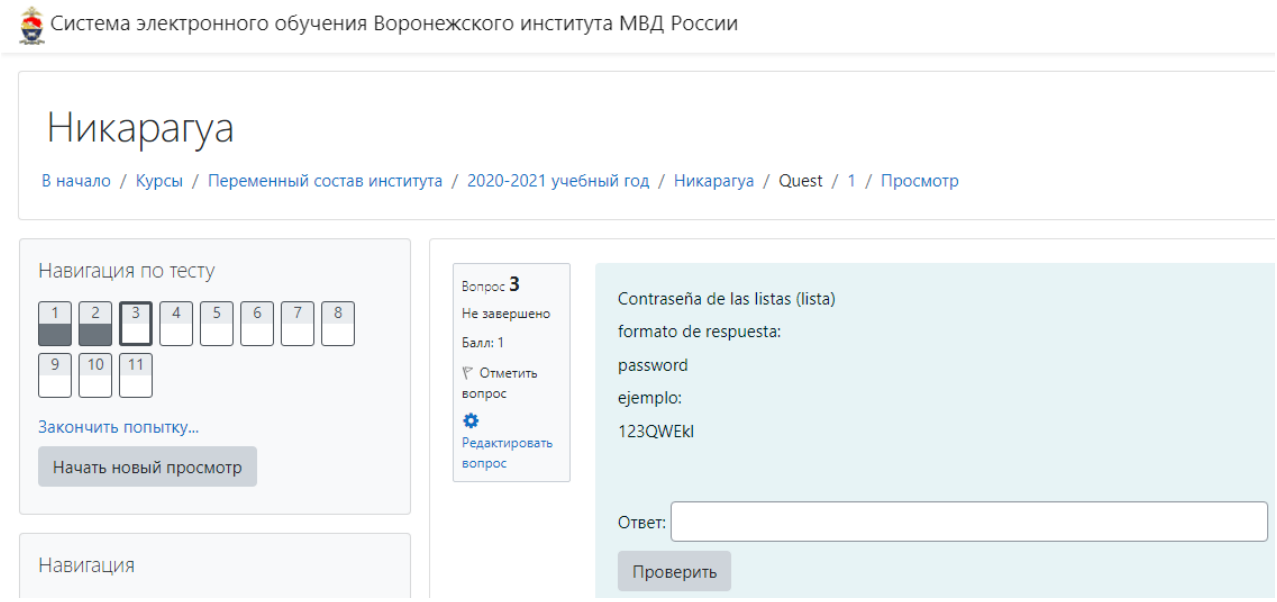
5.2. Использование веб-ресурсов для получения данных о недвижимости, транспорте, физических и юридических лицах.

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

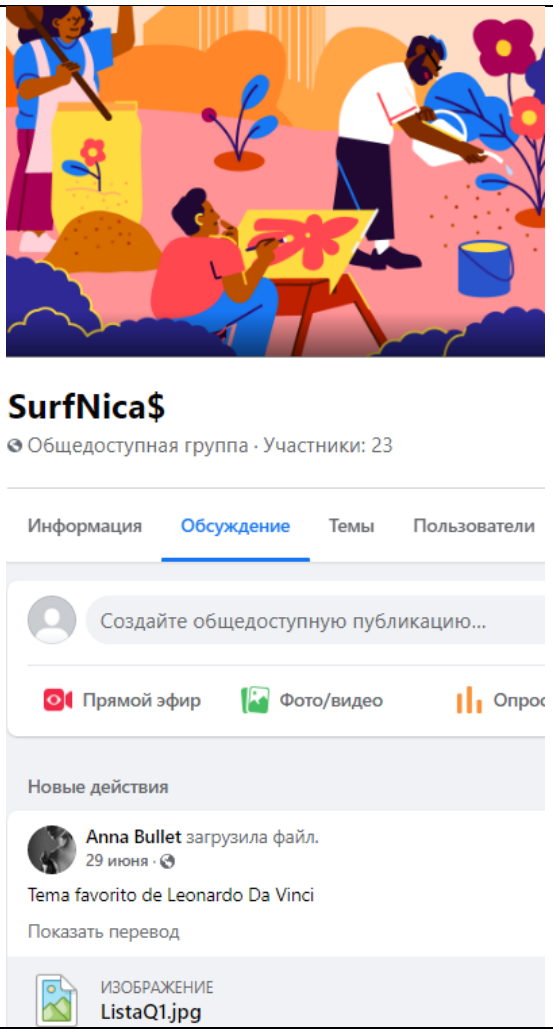
Перевод текста задания:
Пароль от списка (lista)
Формат ответа:
password
Пример:
123QWEkl

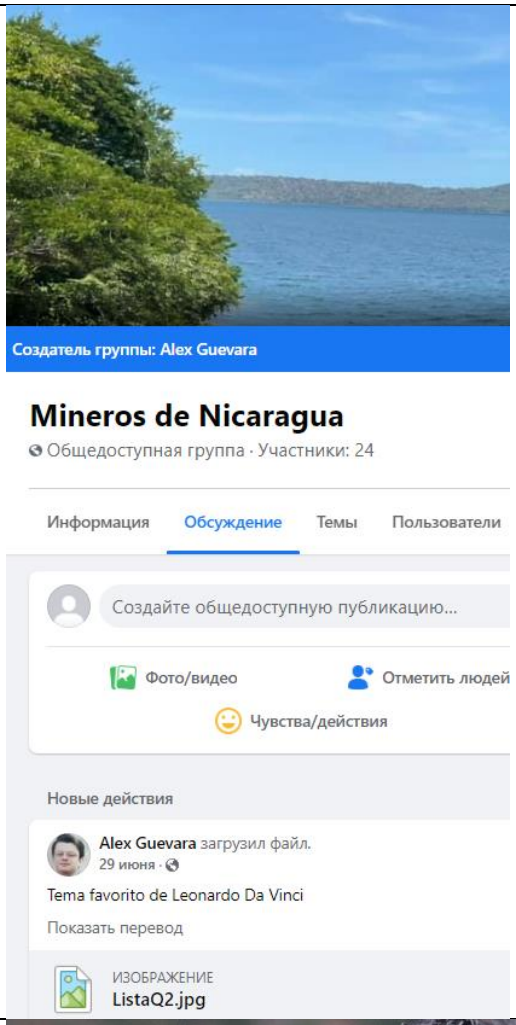


Снимок экрана с третьим заданием для сюжетной линии № 1

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»	 **Botella de pimienta** Общедоступная группа · Участники: 21 Информация Обсуждение Темы Пользователи Создайте общедоступную публикацию... Прямой эфир Фото/видео Опрос Новые действия Karen Silvesa загрузила файл. 29 июня · Tema favorito de Leonardo Da Vinci Показать перевод ИЗОБРАЖЕНИЕ 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»	 **Trompetistas alegres** Общедоступная группа · Участники: 20 Информация Обсуждение Темы Пользователи Создайте общедоступную публикацию... Фото/видео Отметить людей Чувства/действия Новые действия Klara Perez загрузила файл. 29 июня · Lo más interesante de la pipa. Leonardo Davinci entiende estas pipas Показать перевод ИЗОБРАЖЕНИЕ 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.

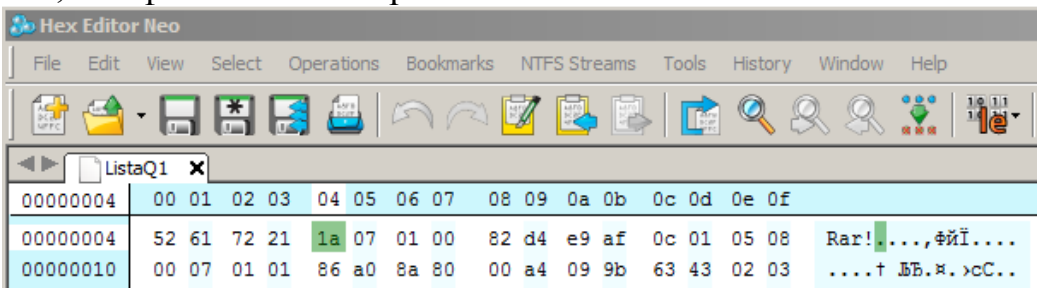
Первая сюжетная линия: файл «ListaQ1.jpg»	
Вторая сюжетная линия: файл «ListaQ2.jpg»	
Третья сюжетная линия: файл «ListaQ3.jpg»	
Четвертая сюжетная линия: «ListaQ4.jpg»	
Пятая сюжетная линия: файл «ListaQ5.jpg»	

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.

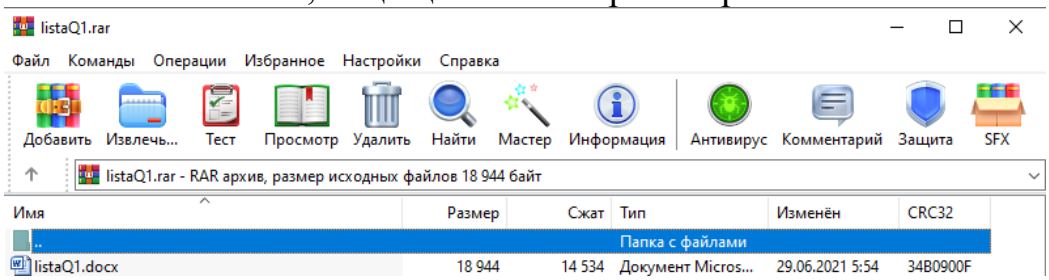
Интерфейс программы Secret Layer и содержимое файла сюжетной линии № 1

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:

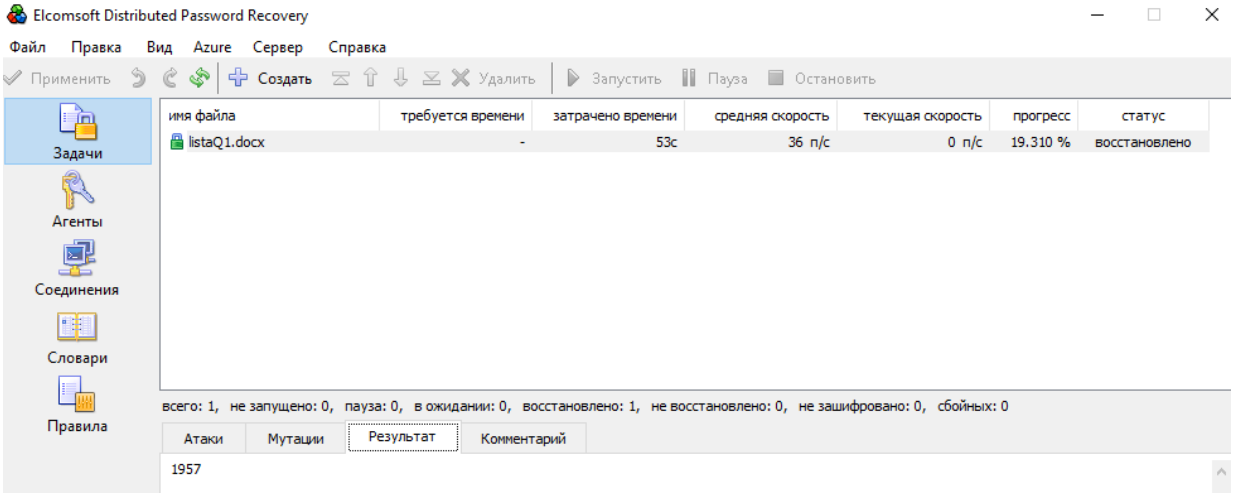
¡El secreto está adentro! Año de nacimiento del Primero: una pista sobre el contenido de la caja.

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.

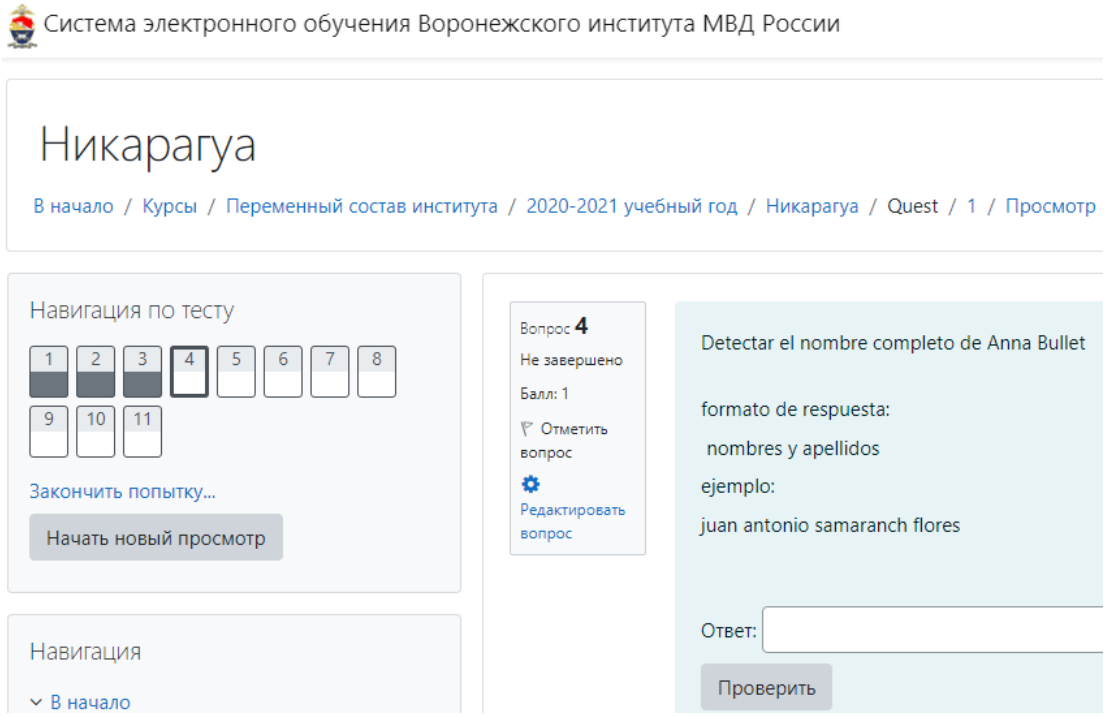
5.2. Использование веб-ресурсов для получения данных о недвижимости, транспорте, физических и юридических лицах.

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:

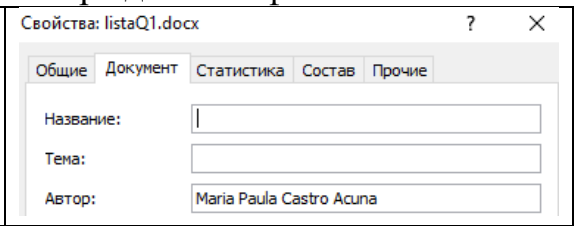
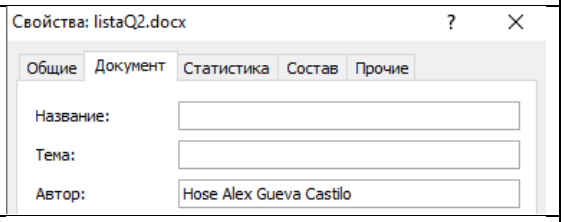
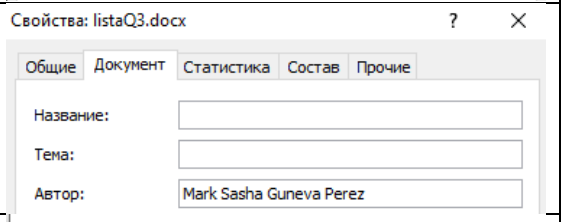
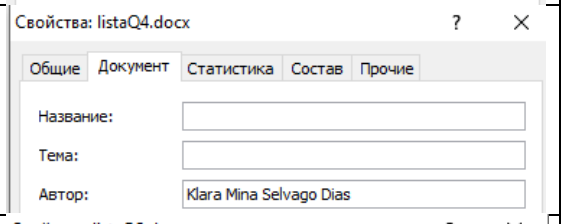
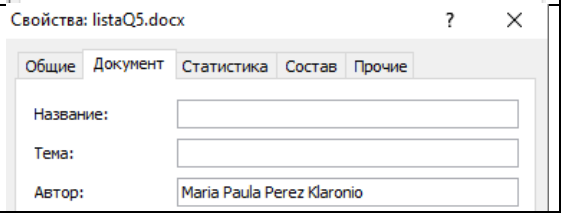
Detectar el nombre completo de **********
formato de respuesta:
nombres y apellidos
ejemplo:
juan antonio samaranch flores

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.

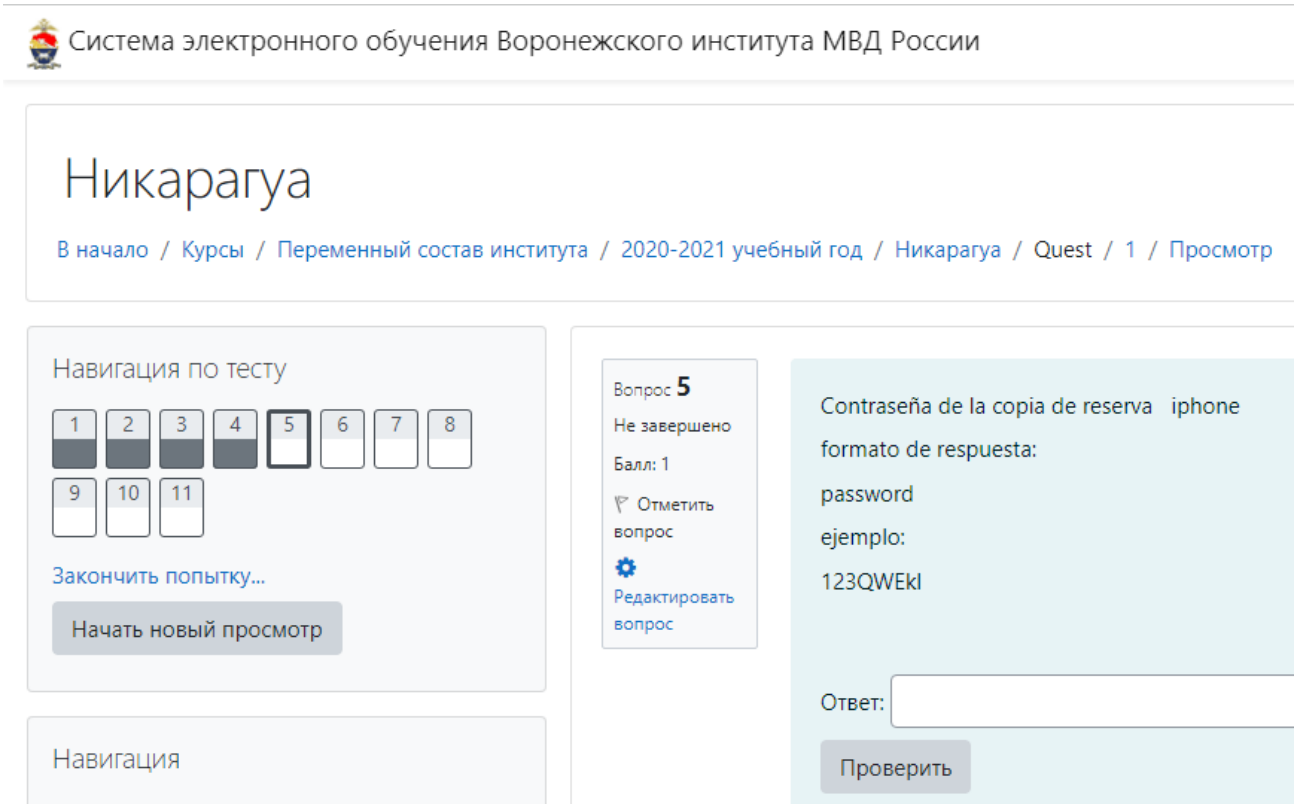
5.2. Использование веб-ресурсов для получения данных о недвижимости, транспорте, физических и юридических лицах.

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

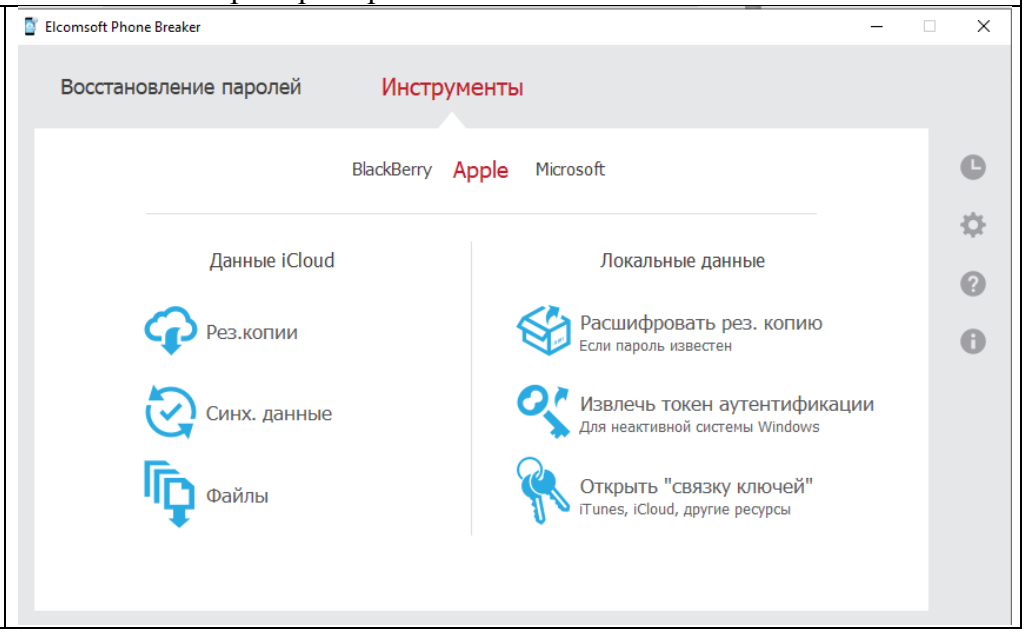
Перевод текста задания:
Пароль от резервной копии Iphone
Формат ответа:
password
Пример:
123QWEkl

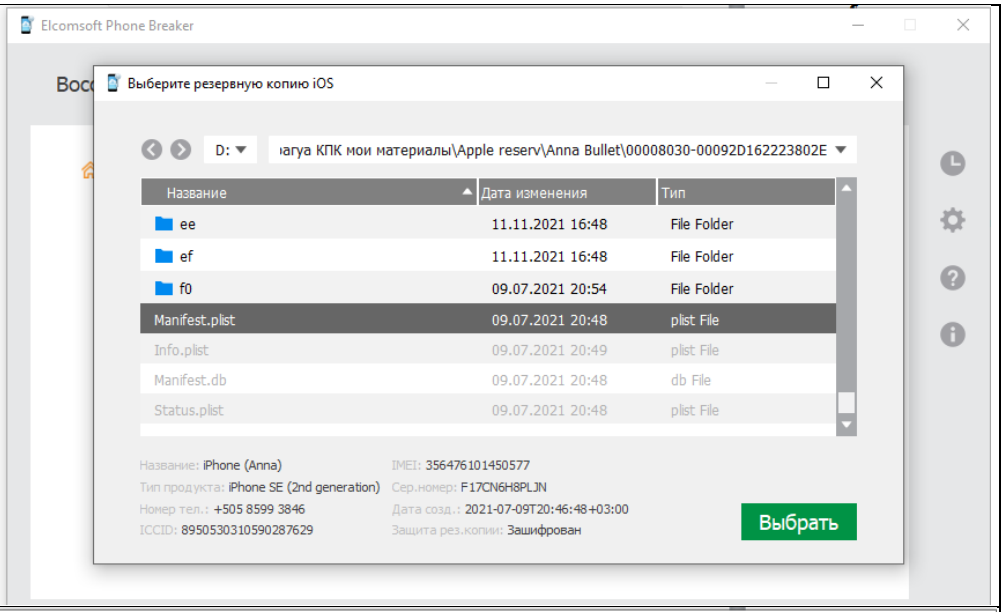
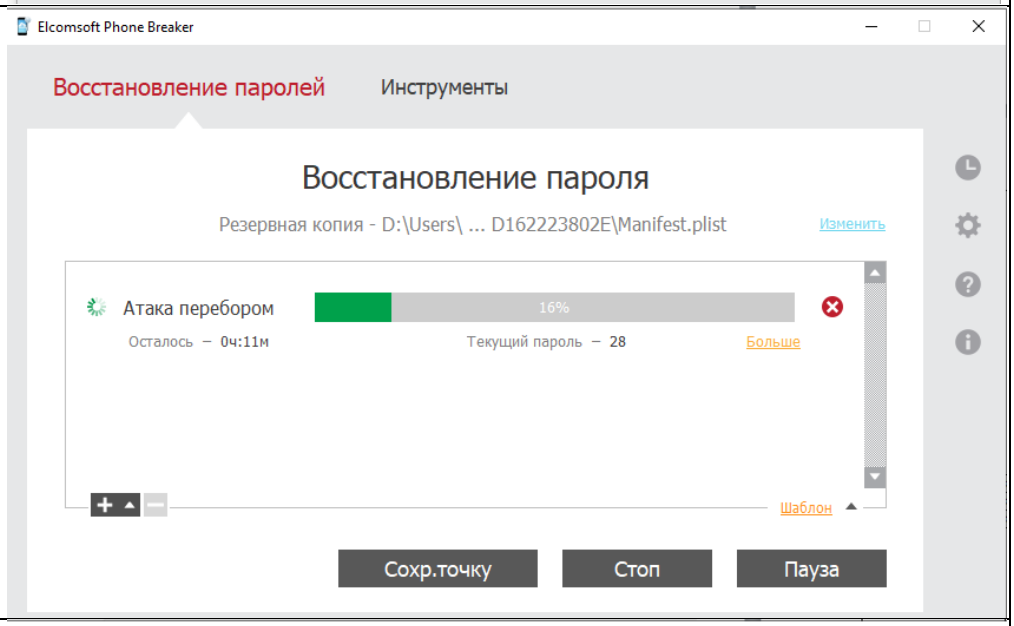
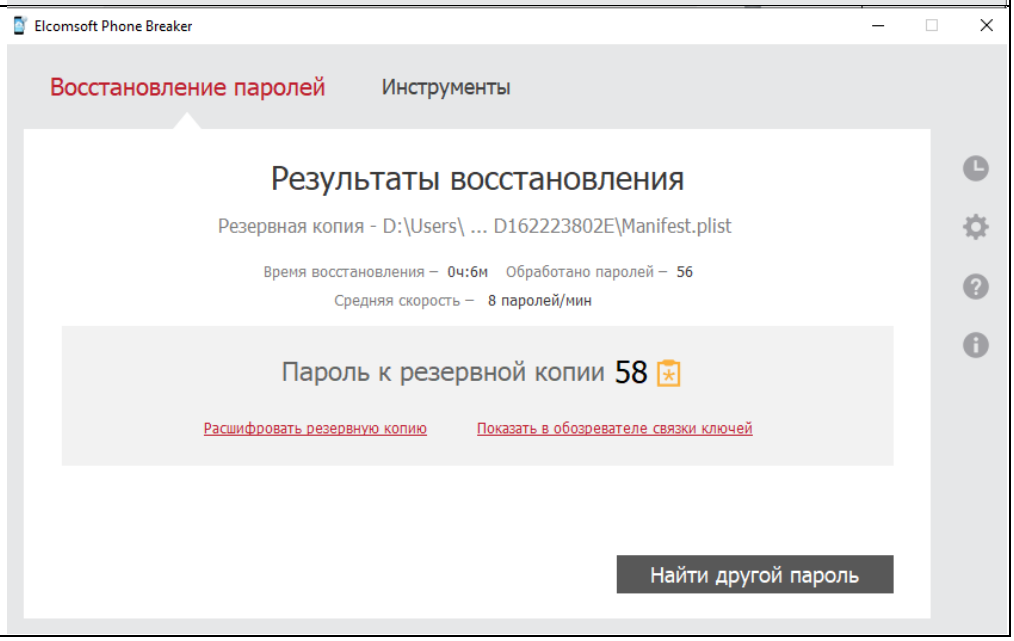


Снимок экрана с пятым заданием для сюжетной линии № 1

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.

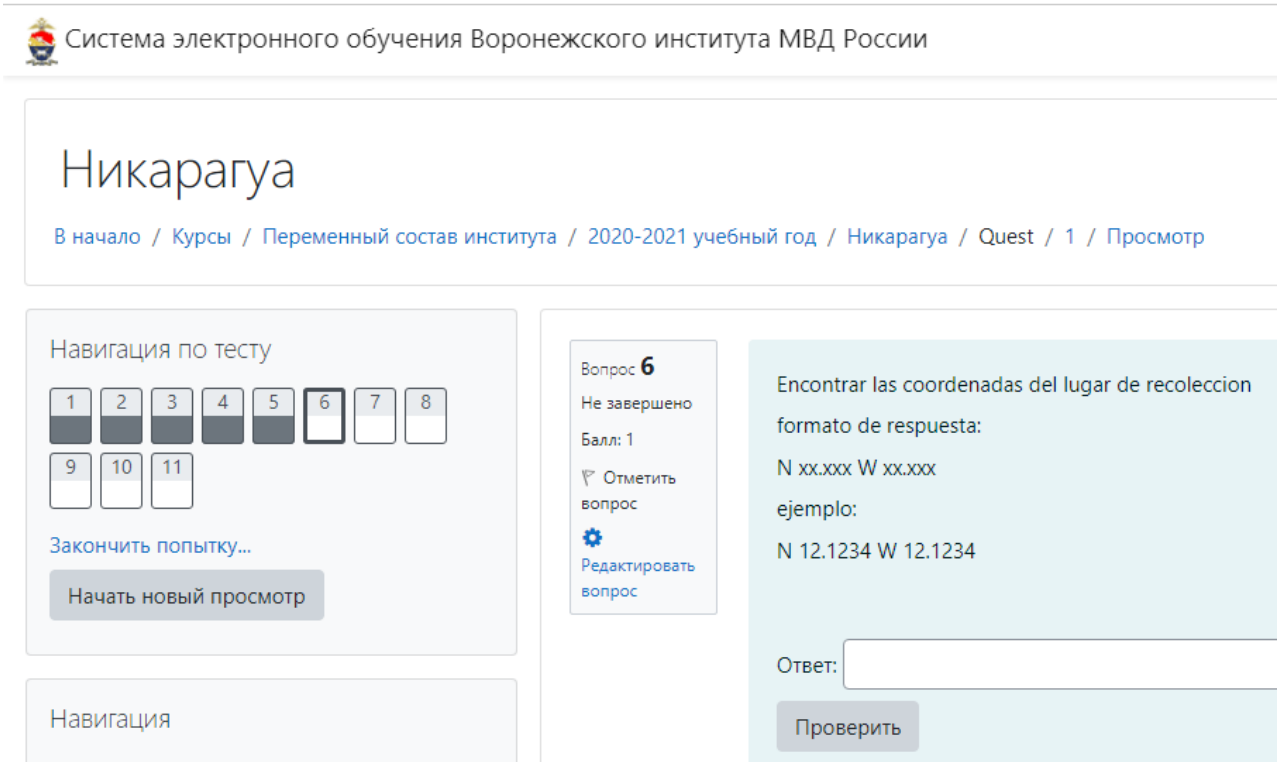
5.2. Использование веб-ресурсов для получения данных о недвижимости, транспорте, физических и юридических лицах.

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:

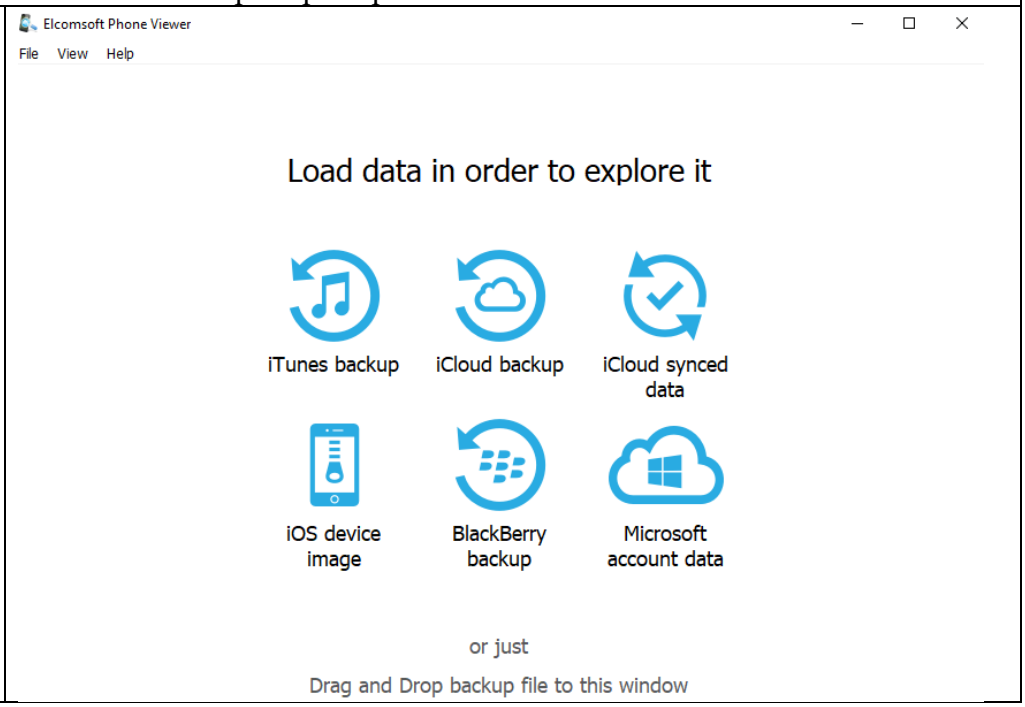
Encontrar las coordenadas del lugar de recoleccion
formato de respuesta:
N xx.xxx W xx.xxx
ejemplo:
N 12.1234 W 12.1234

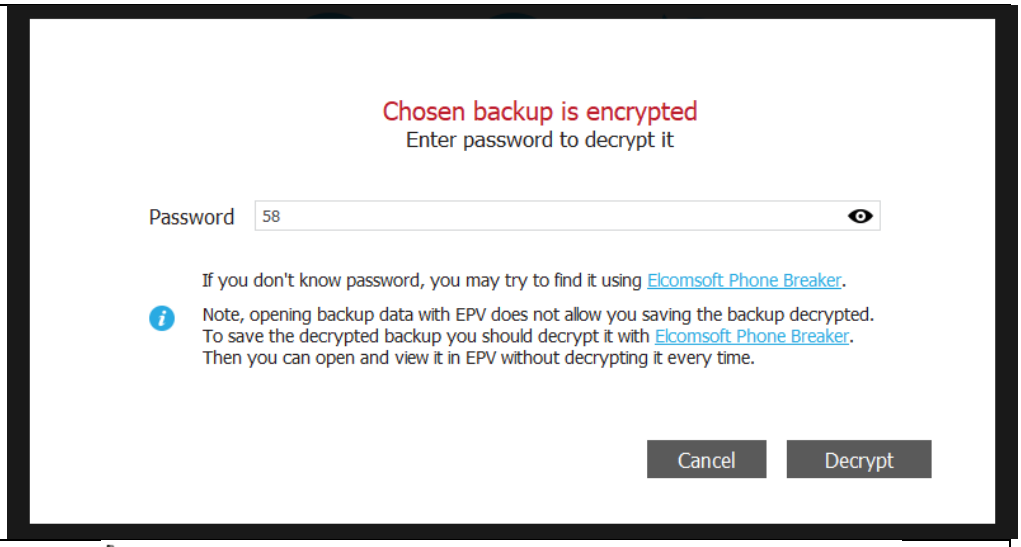
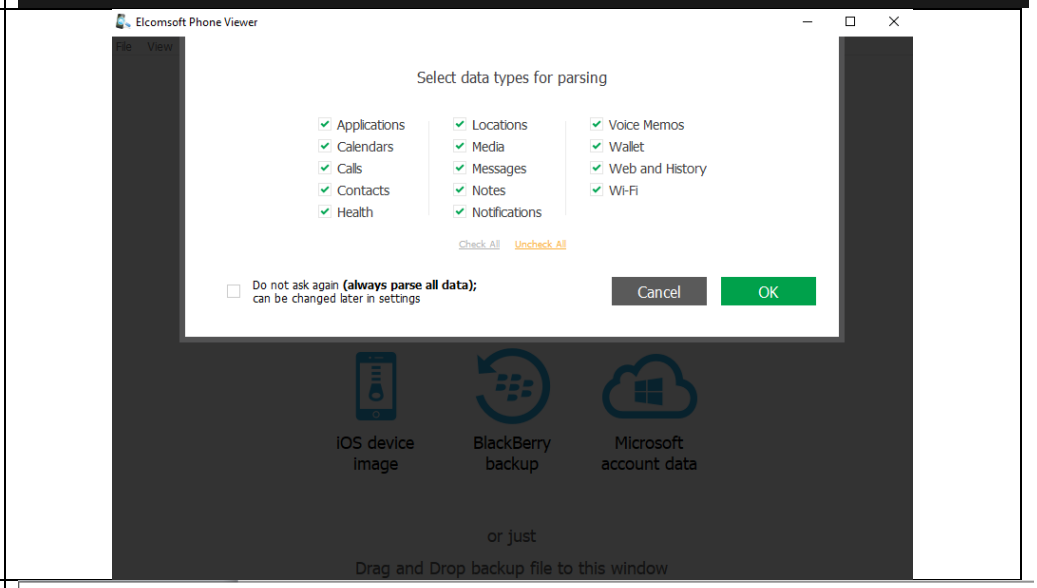
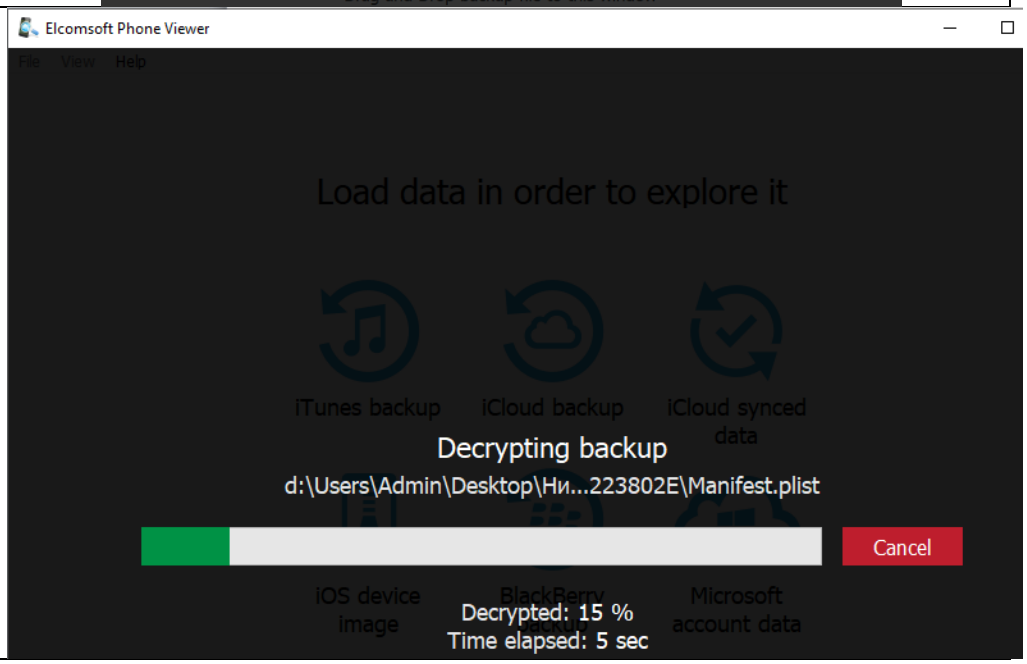
Перевод текста задания:
Установить координаты места сбора
Формат ответа:
N xx.xxx W xx.xxx
Пример:
N 12.1234 W 12.1234

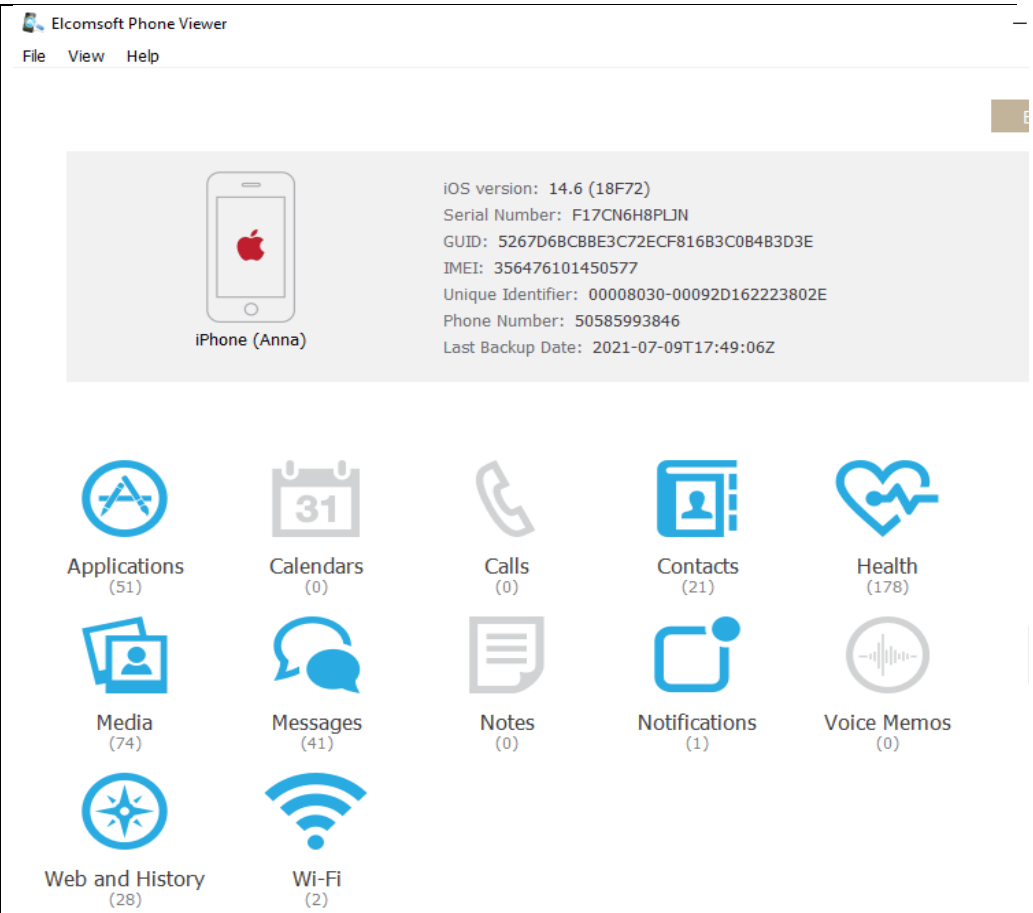
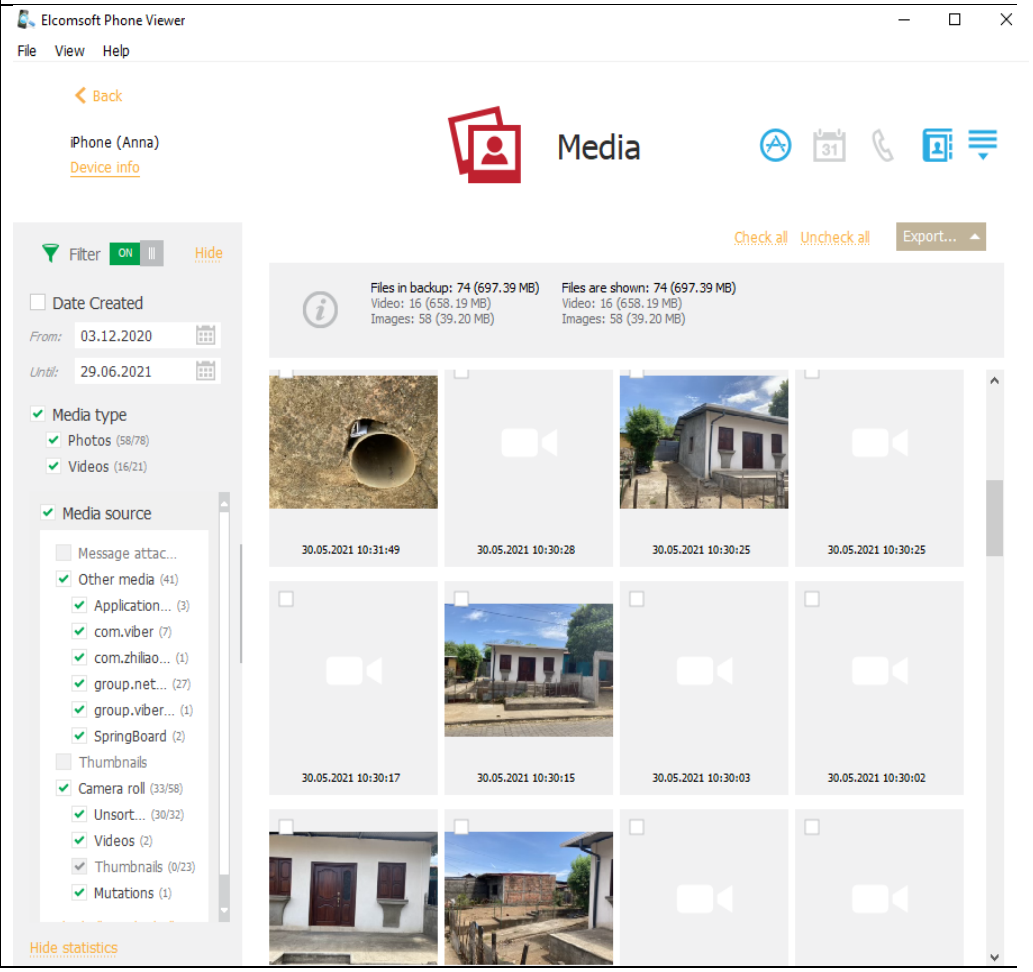


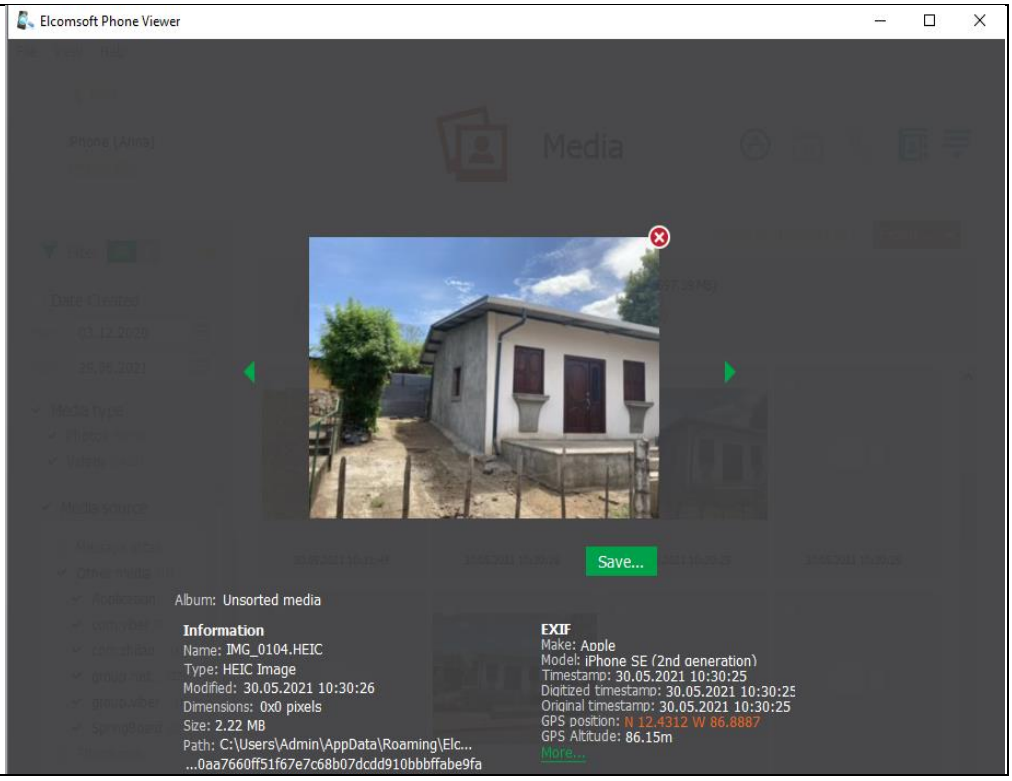
Снимок экрана с шестым заданием для сюжетной линии № 1

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.

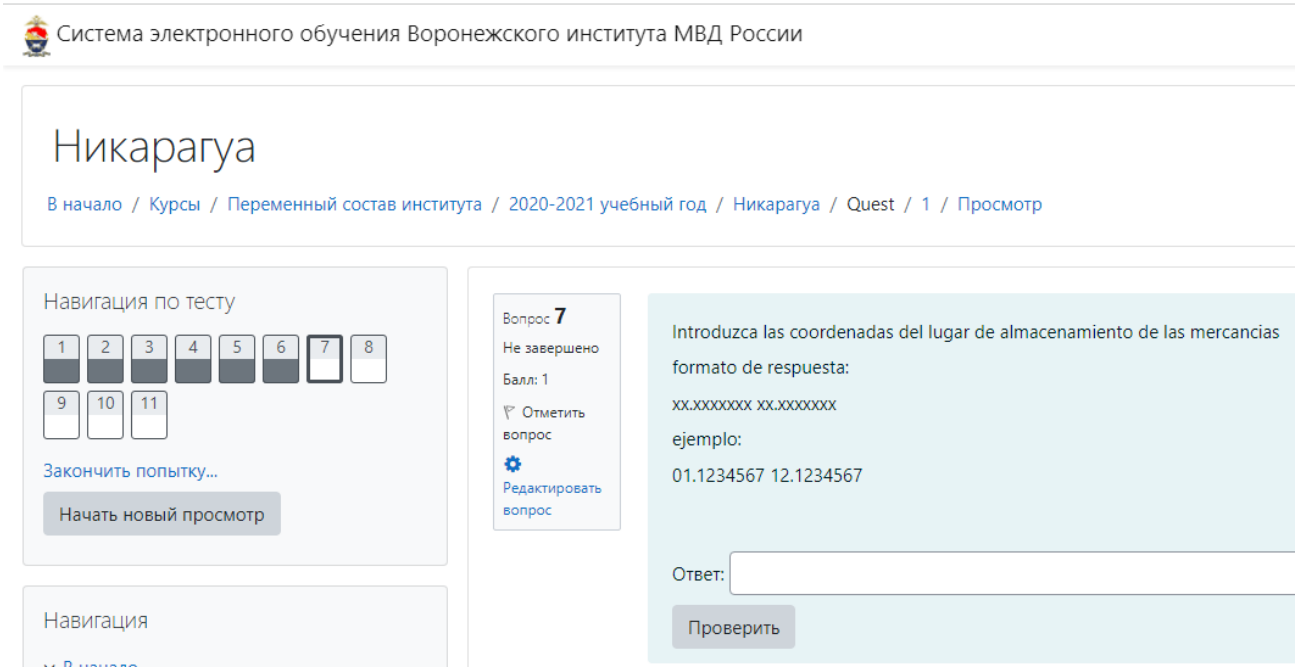
5.3. Поиск и анализ информации в сети Интернет в целях выявления преступлений в сфере компьютерной информации.

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:

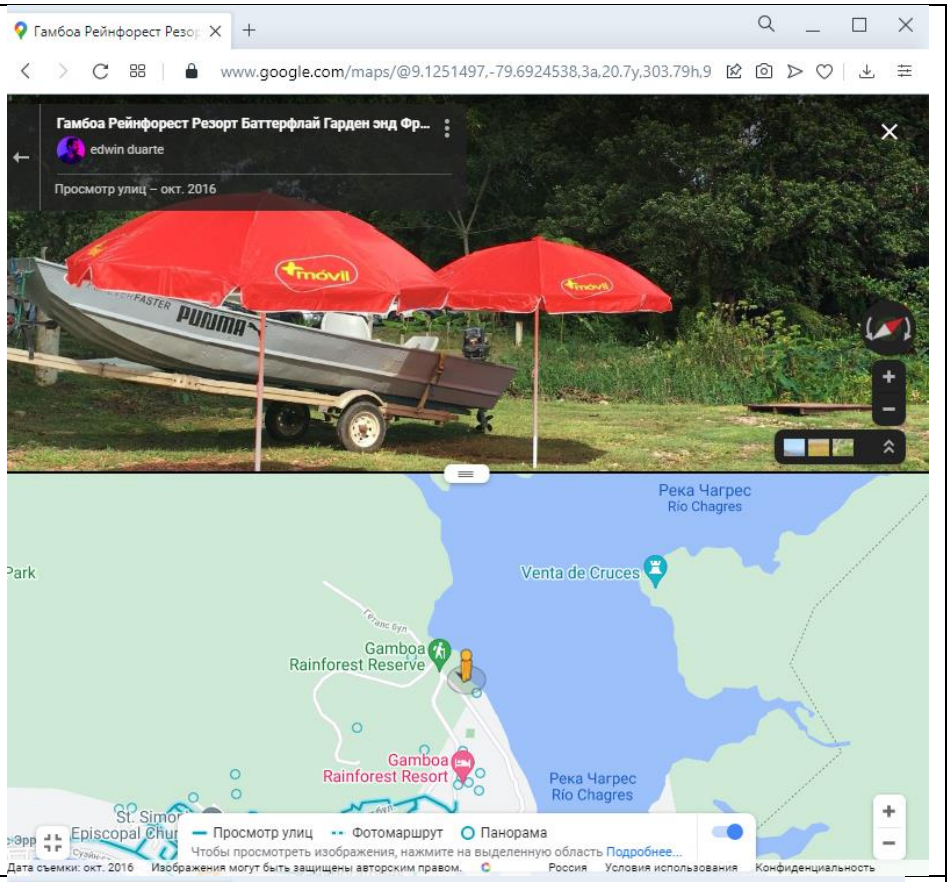
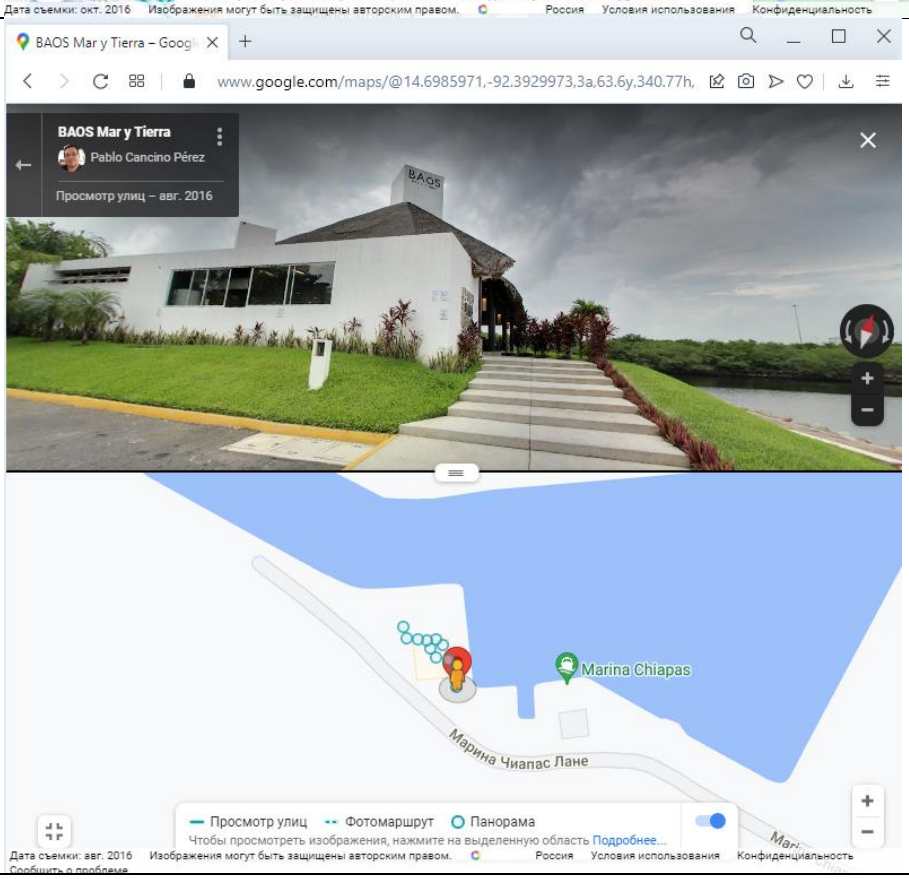
- Привет.
- Привет.
- Я уже оплатил покупку. Мне все привезли. Когда заберешь товар?
- Куда надо подъехать?
- Я все загрузил на лодку SeaSlar1, жду тебя как и всегда, рядом с аэропортом Густаво Рохас Пинийя.

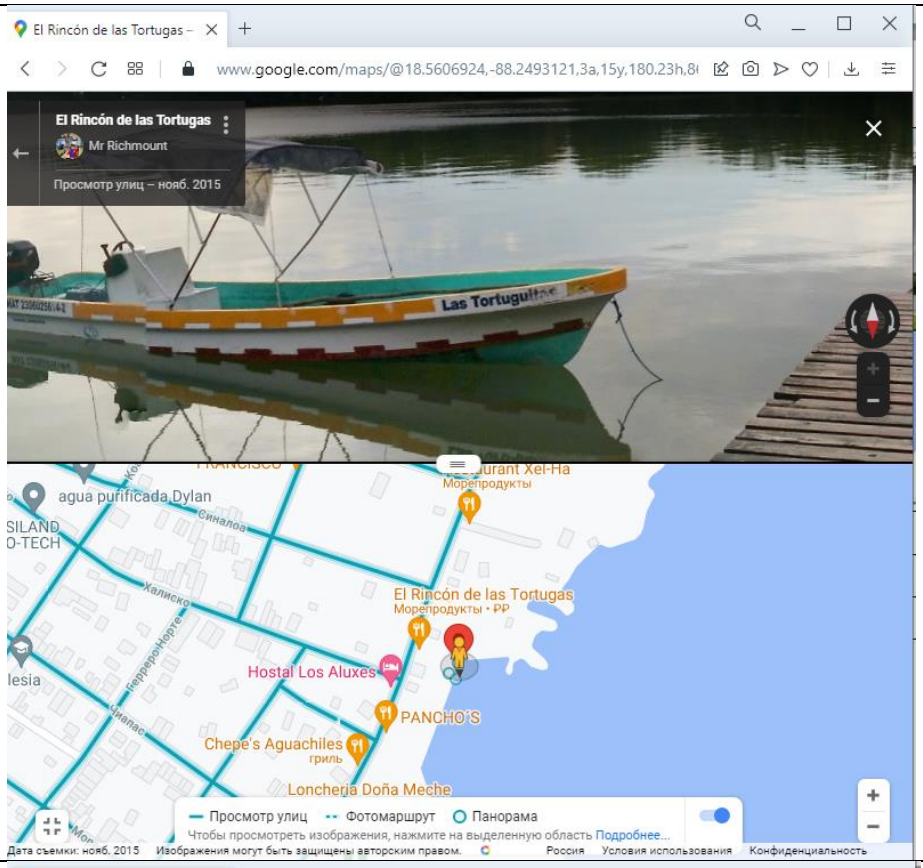
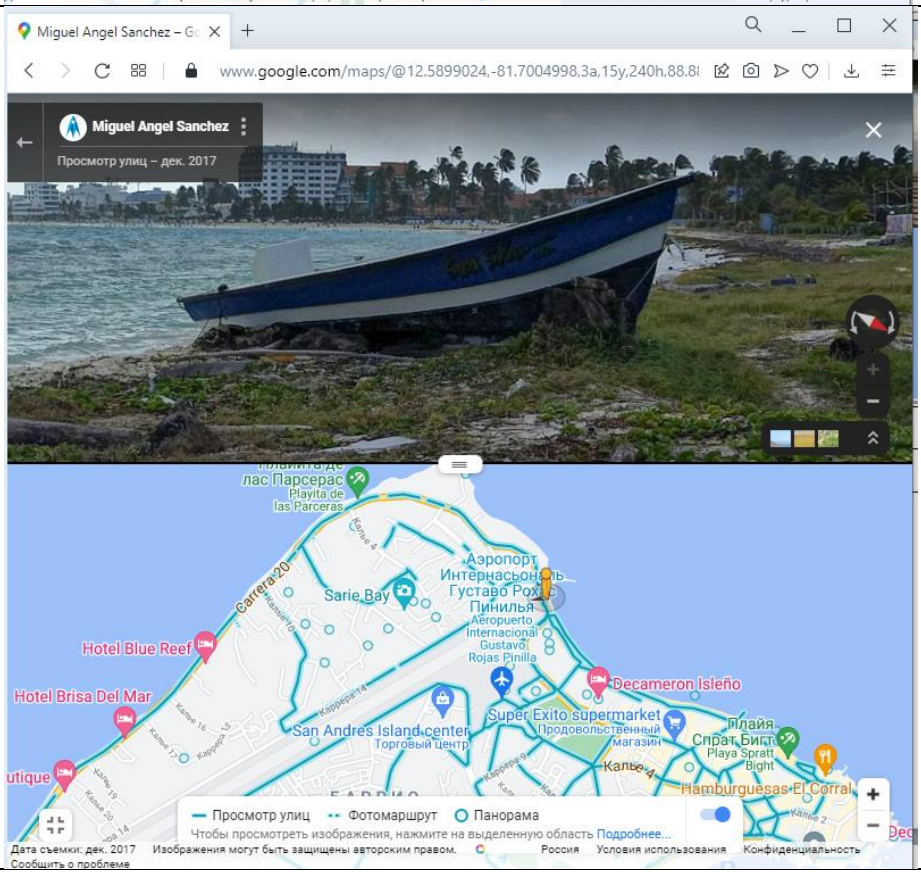
Пятая сюжетная линия:

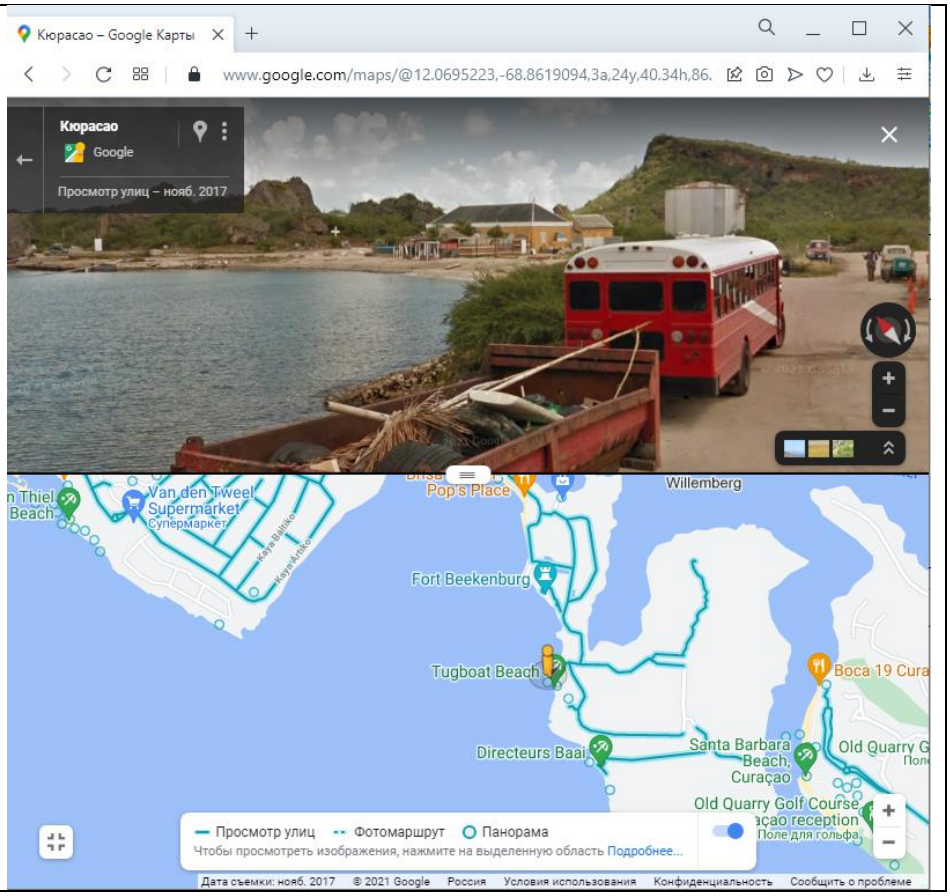
Перевод:

- 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.

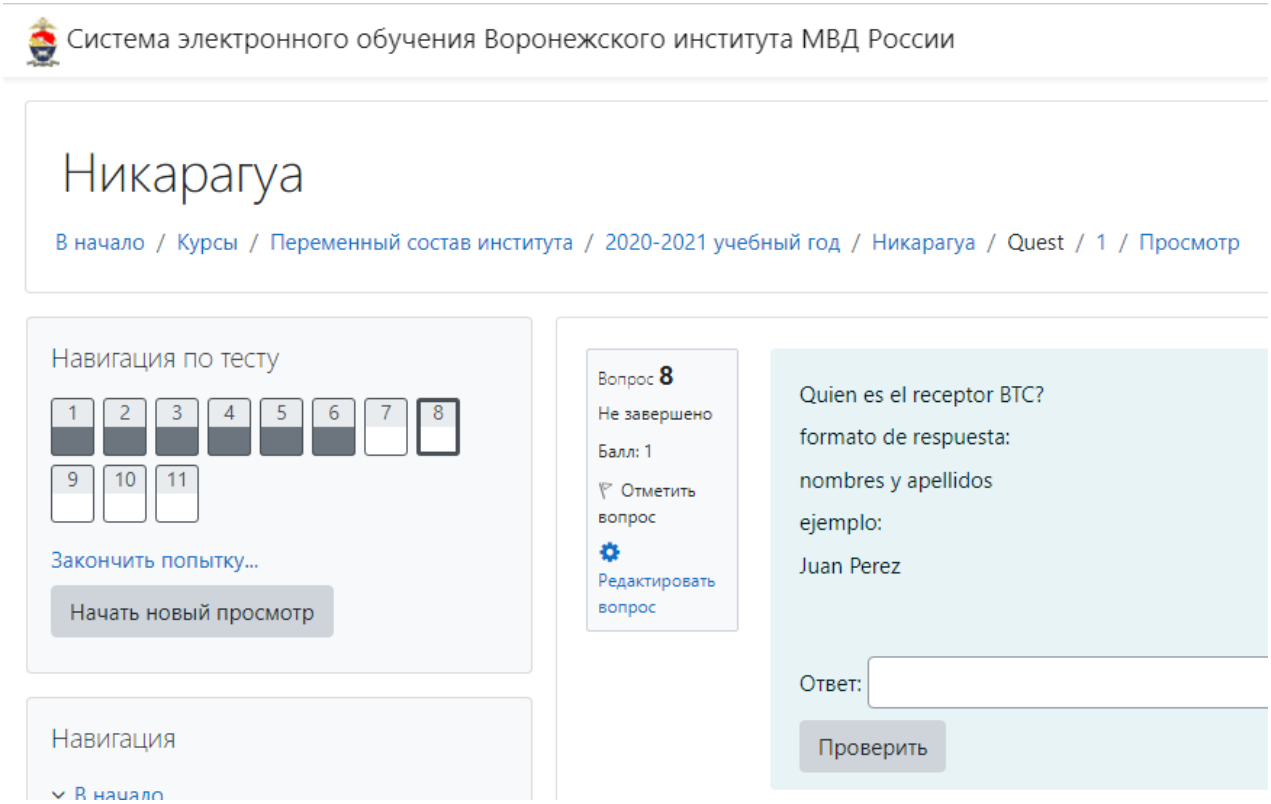
5.2. Использование веб-ресурсов для получения данных о недвижимости, транспорте, физических и юридических лицах.

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

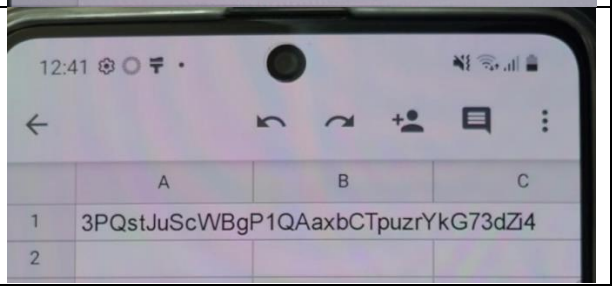
Перевод текста задания:
Кто же получатель BTC?
Формат ответа:
Имя Фамилия
Пример:
Хуан Перес

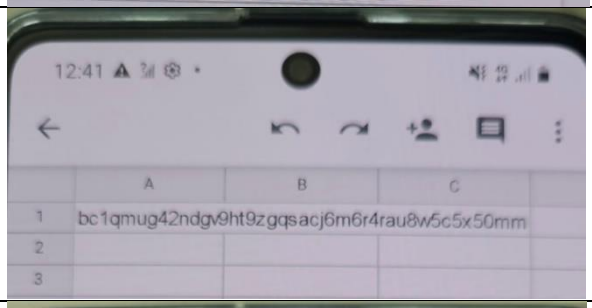
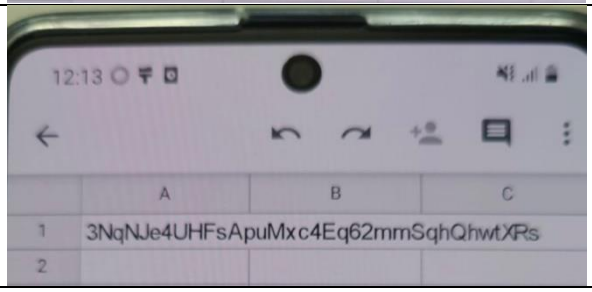


Снимок экрана с восьмым заданием для сюжетной линии № 1

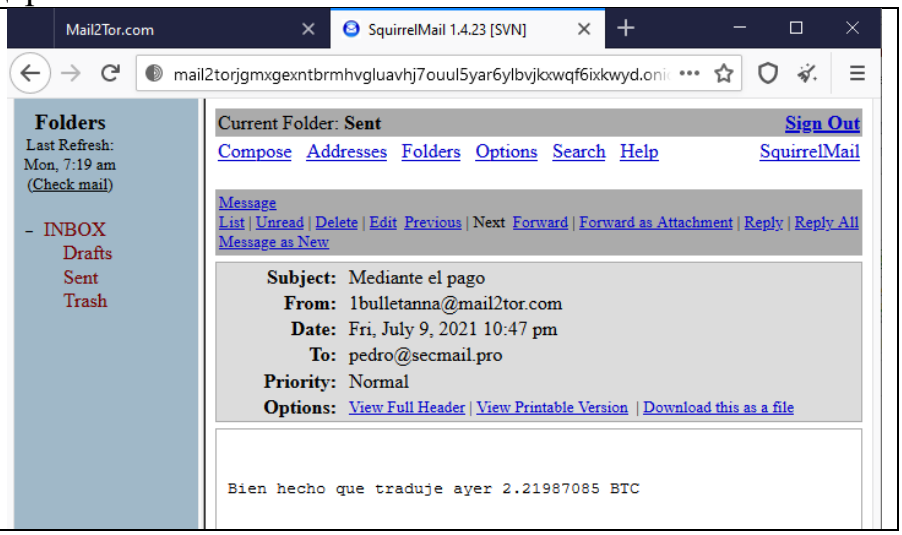
Слушателям выдается еще один телефон, изъятый у третьего персонажа, который по легенде был задержан в месте хранения оружия и наркотиков.

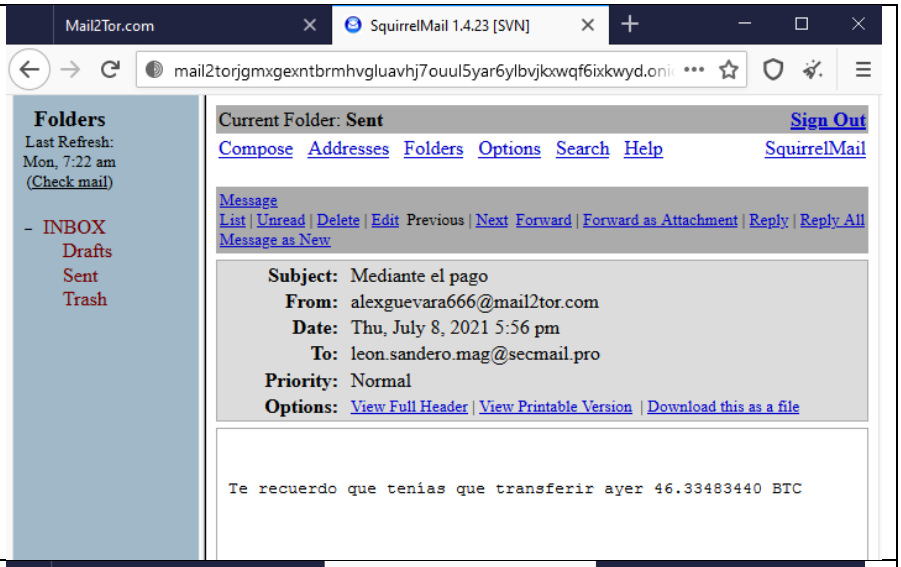
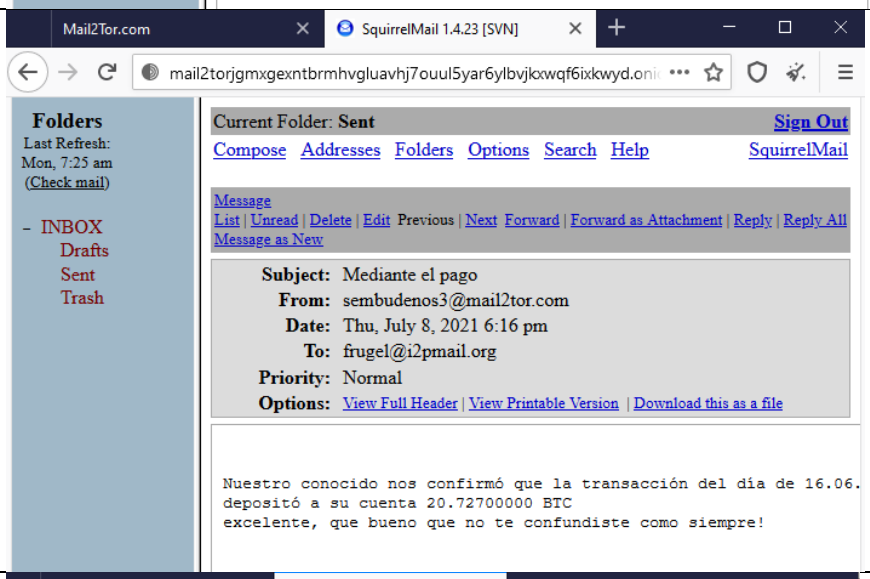
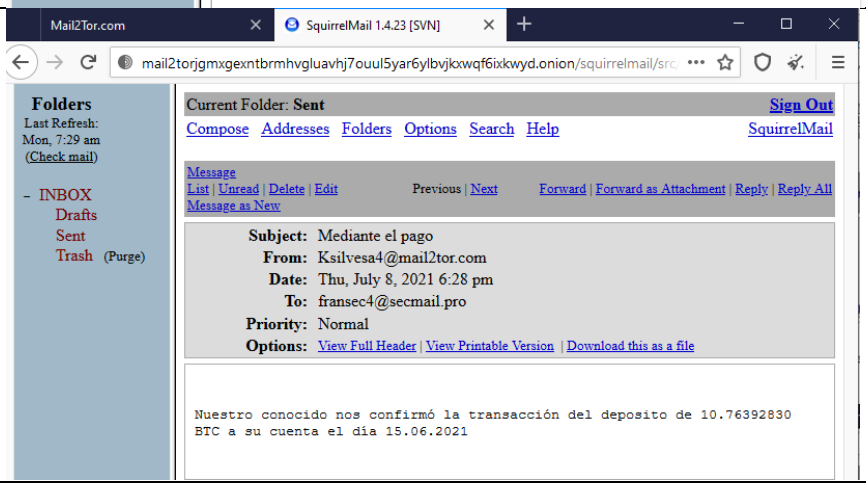
В рамках изучения и анализа содержимого они обнаруживают в приложении Google Tabs запись, содержащую комбинацию букв и цифр, которая является номером криптокошелька:

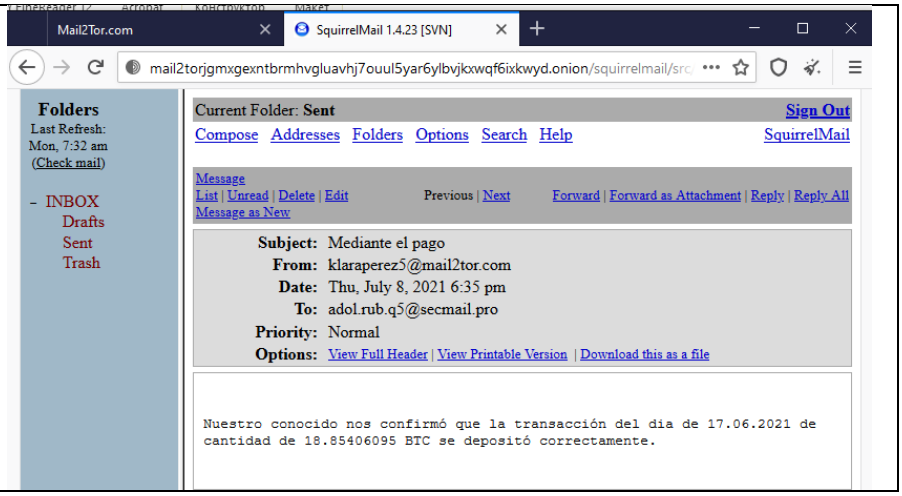
Первая сюжетная линия: 1Pvgp189rCyXWxPJ5aw86bPFcN5tDL4nYA	
Вторая сюжетная линия: 3PQstJuScWBgP1QAaxbCTpuzrYkG73dZi4	

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»	

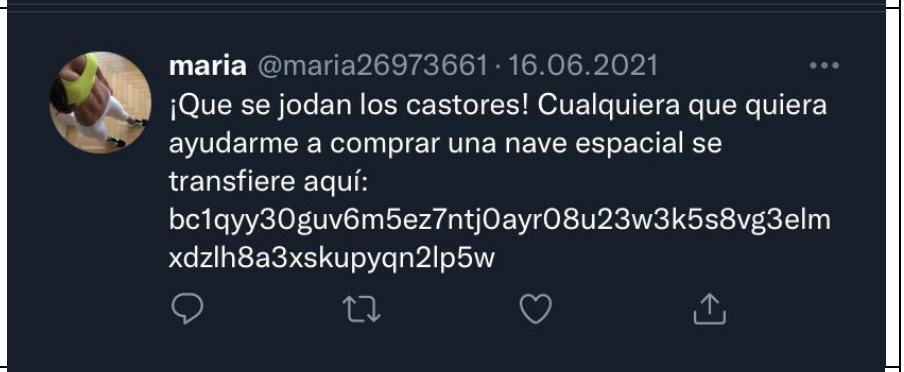
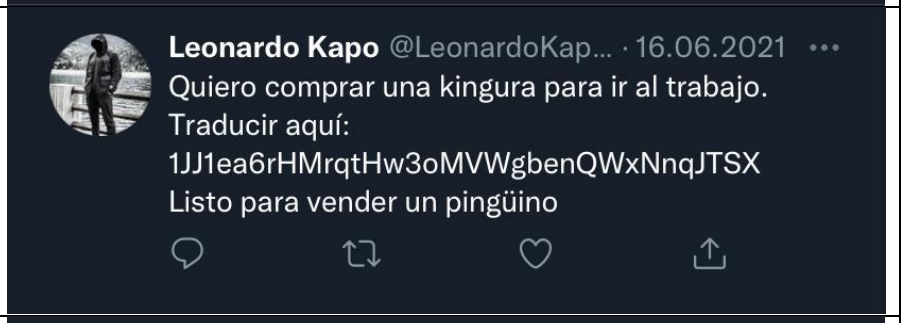
Вторая сюжетная линия: Перевод сообщения: «Напоминаю, вчера нужно было перевести 46.33483440 BTC»	
Третья сюжетная линия: Перевод сообщения: «Наш знакомый подтвердил нам, что перевод от 16.06.2021 г. на его счет 20.72700000 BTC прошел, хорошо, что вы как всегда не перепутали!»	
Четвертая сюжетная линия: 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 г. 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»	34cUiCLWRWNEQhBSH3K8fes7h3DwbdyTTZ 0.00550000 BTC 3KPTQFF9h3uzkaTSL3byc8hHUuaUYKNqsB 2.21987085 BTC
Вторая сюжетная линия: Перевод сообщения: «Напоминаю, вчера нужно было перевести 46.33483440 BTC»	bc1q866sv2stppgtywjejsjj3xsfrsm5e2f5zqwsx9z0... 4.00000000 BTC bc1qwqdg6squsna38e46795at95yu9atm8azzmyv... 4.00000000 BTC bc1qwqdg6squsna38e46795at95yu9atm8azzmyv... 4.00000000 BTC bc1qwqdg6squsna38e46795at95yu9atm8azzmyv... 4.00000000 BTC bc1qzjeg3h996kw24zrg69nge97fw8jc4v7v7yznft... 4.00000000 BTC bc1qpfsckufdjx9mrwjekumu9gmmgr24wd682nhj2... 4.00000000 BTC bc1qwqdg6squsna38e46795at95yu9atm8azzmyv... 4.00000000 BTC bc1qdl753ur9ucwa3cgfrud2nqvu7k69dykk3cwwx... 2.44422000 BTC bc1qyy30guv6m5ez7ntj0ayr08u23w3k5s8vg3elm... 46.33483440 BTC
Третья сюжетная линия: Перевод сообщения: «Наш знакомый подтвердил нам, что перевод от 16.06.2021 г. на его счет 20.72700000 BTC прошел, хорошо, что вы как всегда не перепутали!»	2021-06-16 18:52 36ZdLqQ8CxzQfZnvkXsoP3QV9ASQL8eS35 20.72688664 BTC
Четвертая сюжетная линия: Перевод сообщения: «Наш знакомый подтвердил транзакцию депозита от 15.06.2021 10.76392830 BTC на его счет»	2021-06-16 07:22 1JJ1ea6rHMrqtHw3oMVWgbenQWxNnqJTSX 10.76392830 BTC
Пятая сюжетная линия: Перевод сообщения: «Наш знакомый подтвердил нам, что сделка от 17.06.2021 г. 18,85406095 BTC прошла успешно и битки зачислены»	2021-06-18 01:13 375TaqhVRH2rtrqrDvurCfuXqZLUWCKZHw 1.31347521 BTC 3PNw4iv6EhiwxGut7sqppzwiqxvVUXjM7Y 18.85406095 BTC

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.

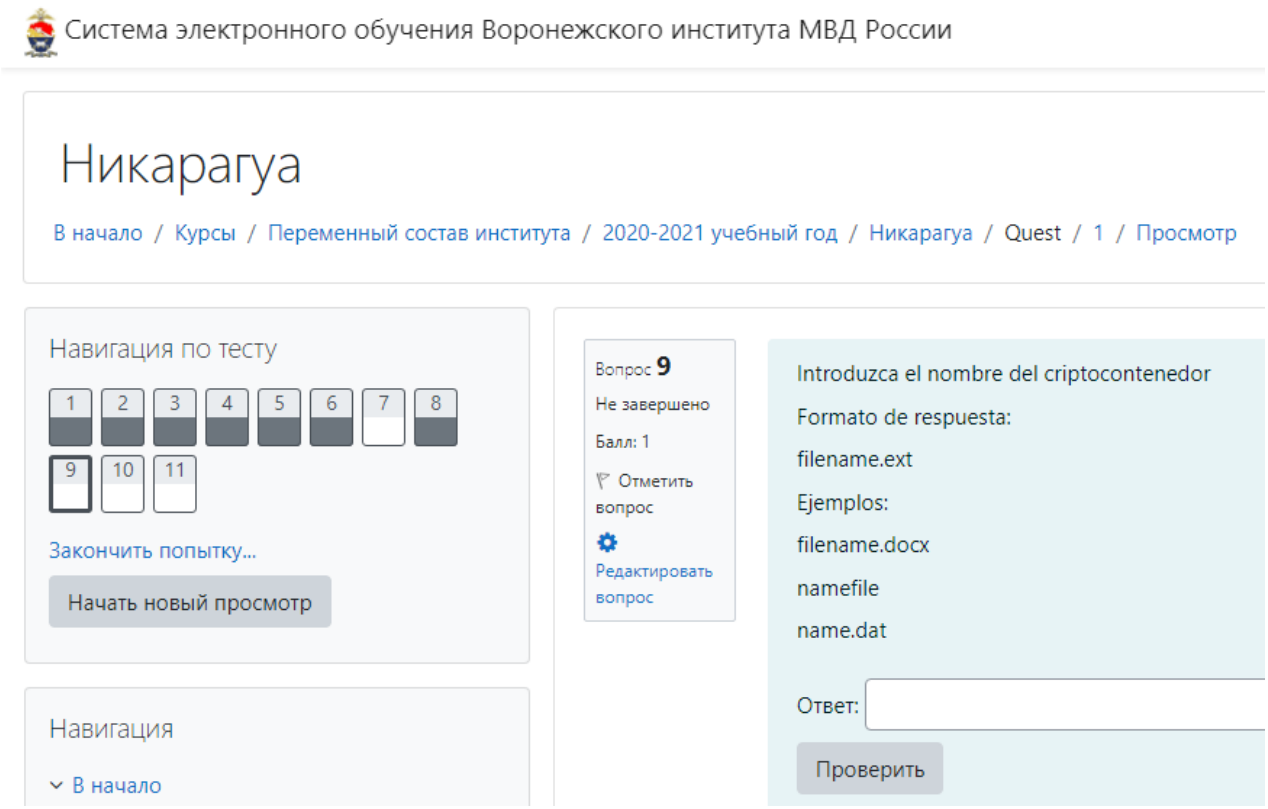
5.2. Использование веб-ресурсов для получения данных о недвижимости, транспорте, физических и юридических лицах.

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:

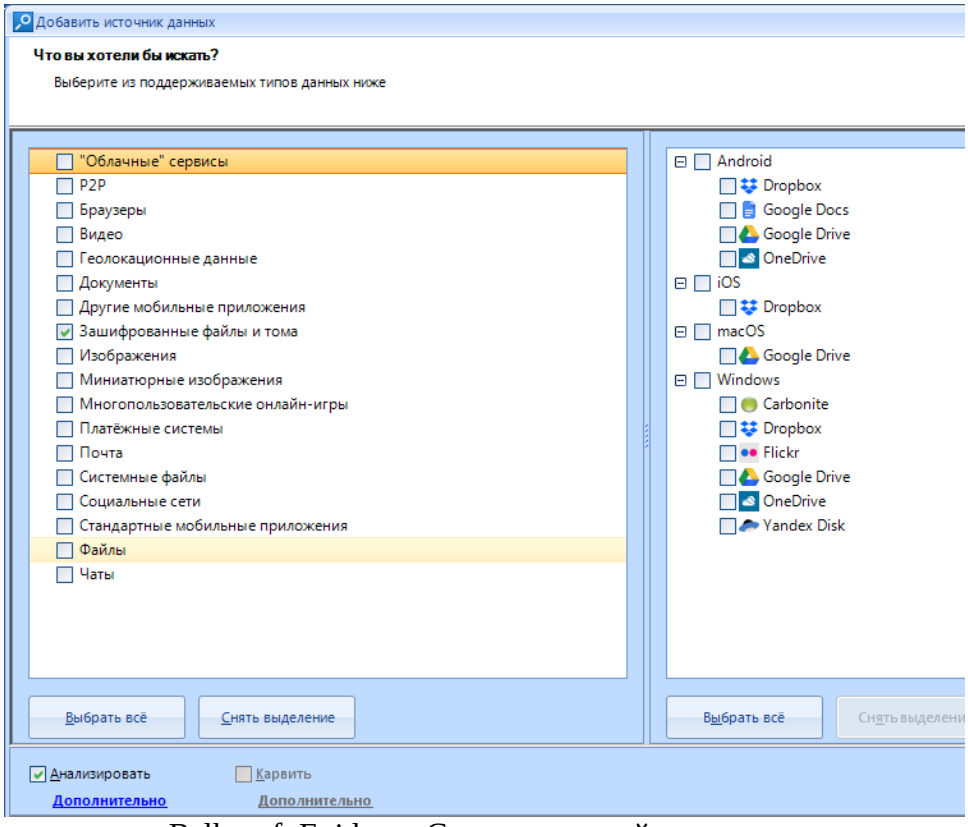
Introduzca el nombre del criptocontenedor
Formato de respuesta:
filename.ext
Ejemplos:
filename.docx
namefile
name.dat

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



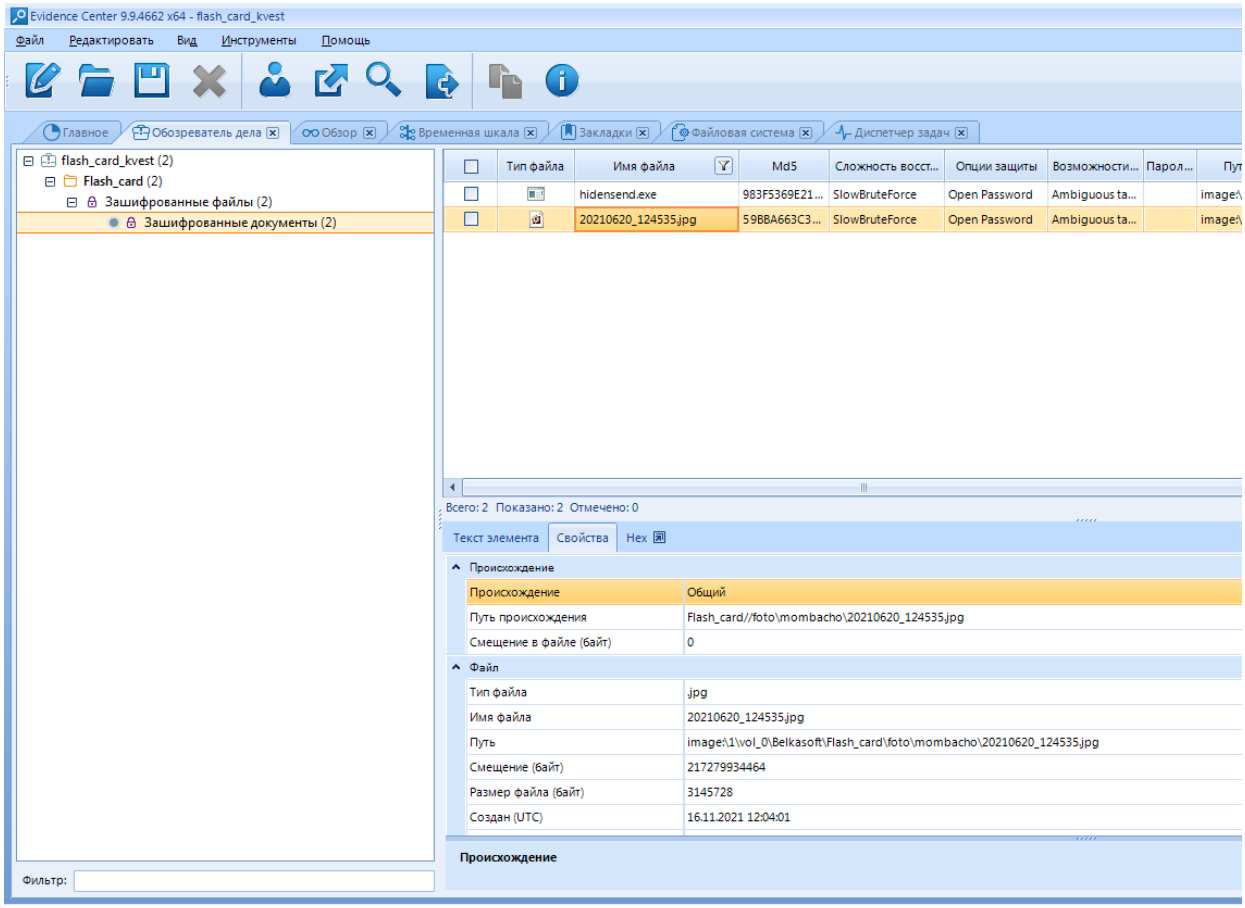
Снимок экрана с девятым заданием для сюжетной линии № 1

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».



Снимок экрана Belkasoft Evidence Center с настройками для поиска криптоконтейнеров

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



Снимок экрана Belkasoft Evidence Center с найденными криптоконтейнерами

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:

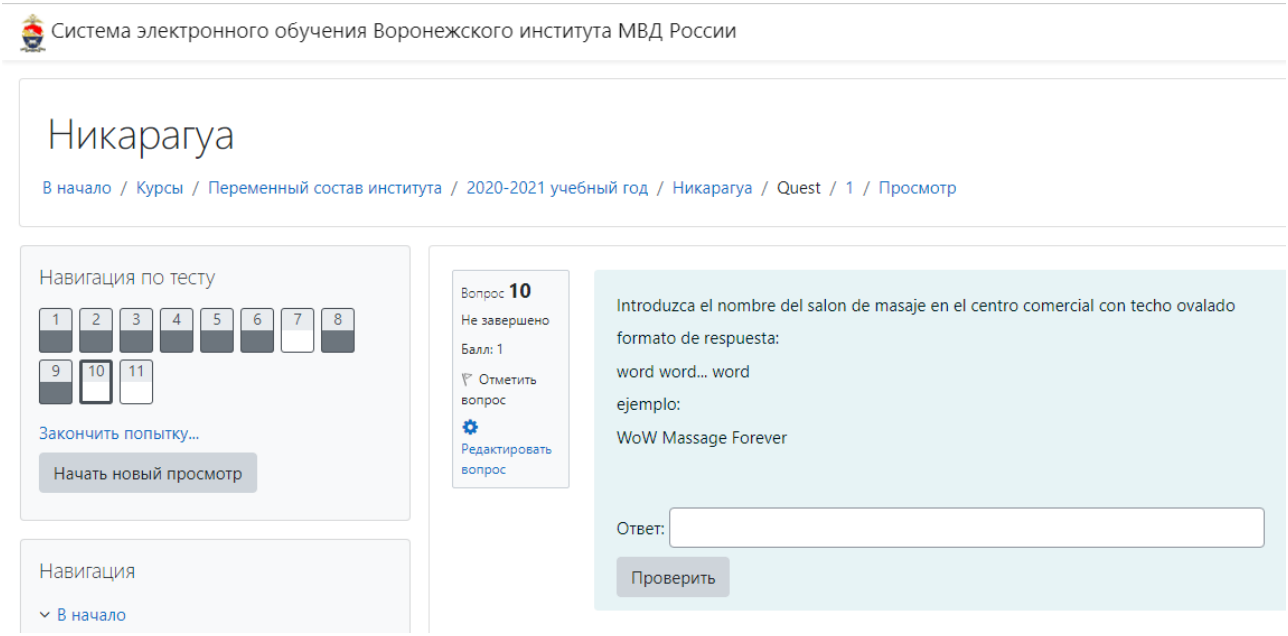
Introduzca el nombre del salon de masaje en el centro comercial con techo ovalado

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

Перевод текста задания:

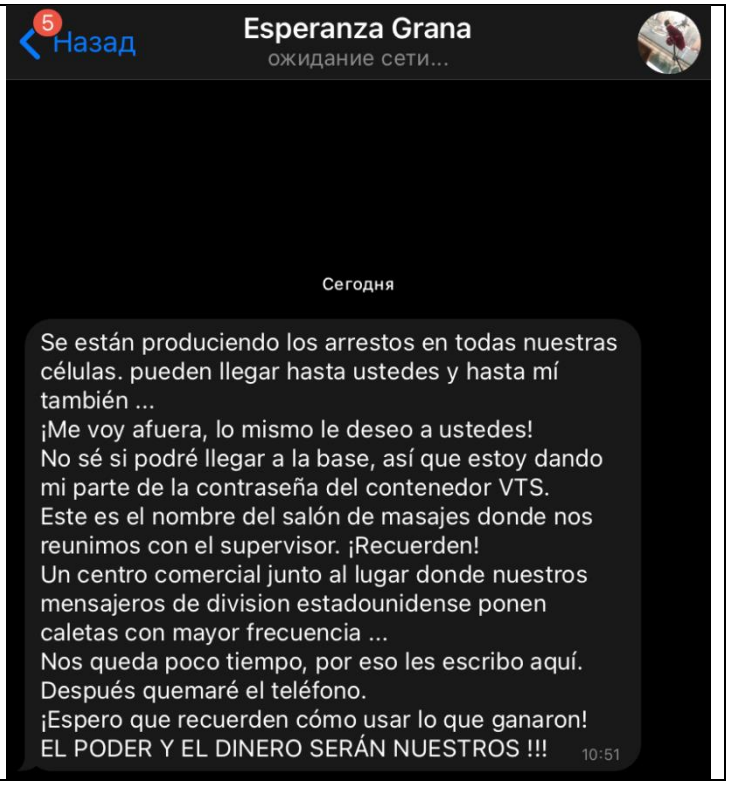
Введите название массажного салона в торговом центре с овальной крышей

Формат ответа:
word word... word
Пример:
WoW Massage Forever

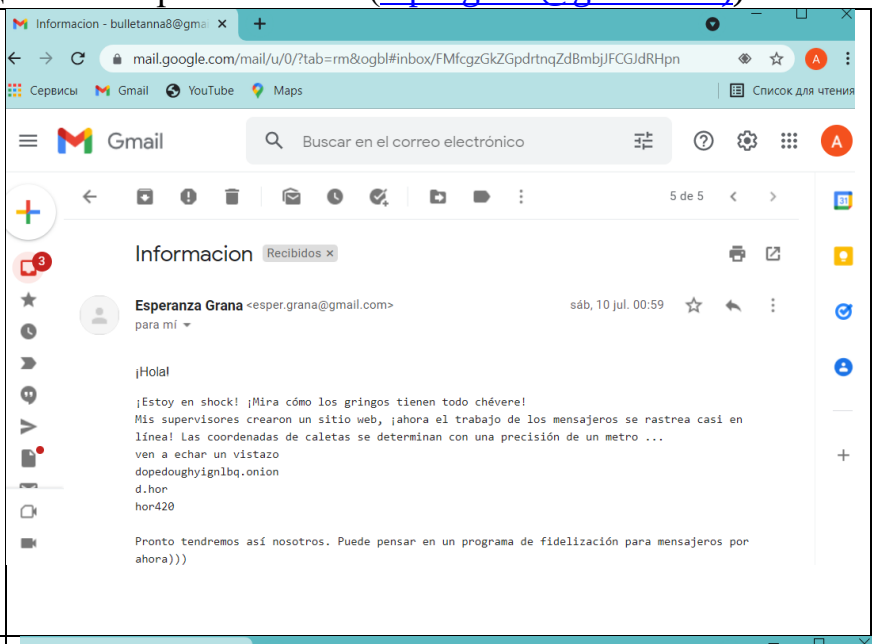
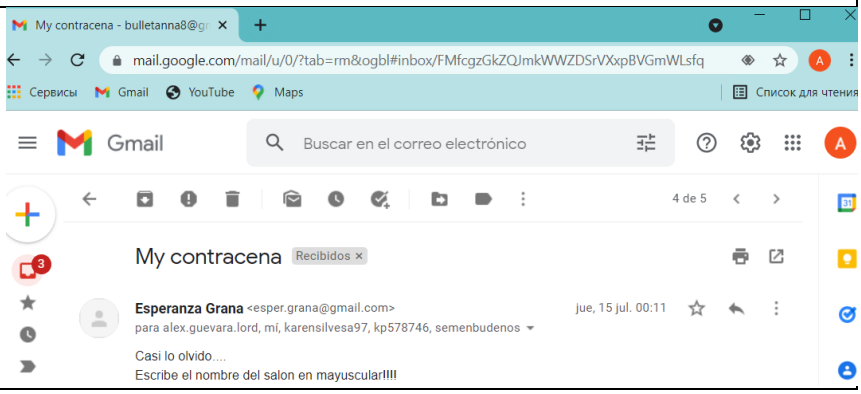


Снимок экрана с десятым заданием для сюжетной линии № 1

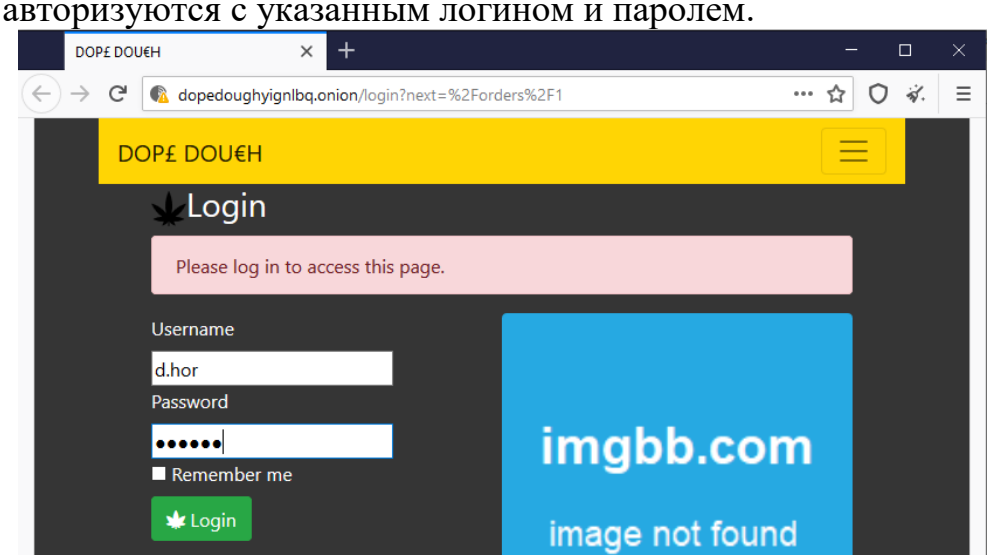
1. Слушателям выдаются Iphone четвёртых персонажей, в приложении Telegram они обнаружат сообщение от Esperanza Grana следующего содержания:

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))

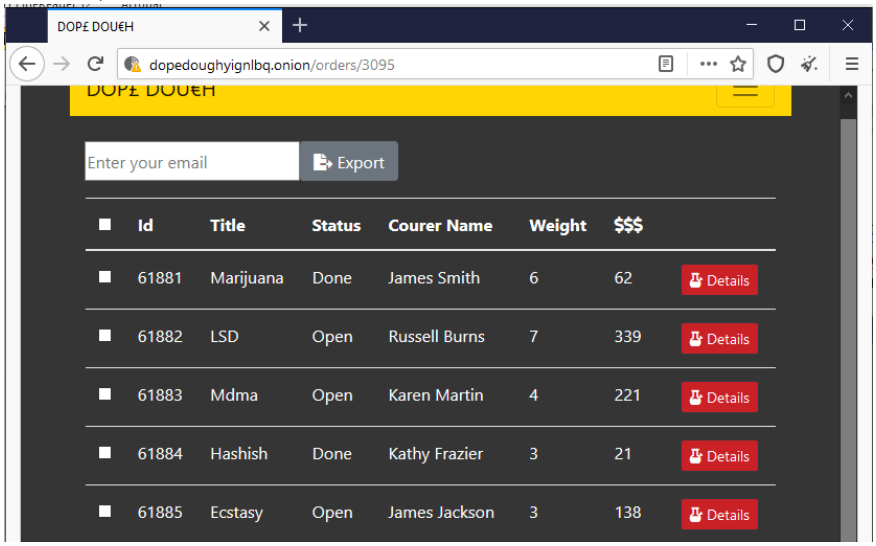
Перевод: Привет! Я в шоке! Смотри, как у американосов все четко! Мои кураторы сделали сайт - теперь работу курьеров отслеживают практически онлайн! Координаты закладок с точностью до метра определяют ... зайди глянь dopedoughyignlbq.onion d.hor hor420 Скоро и у нас так будет. Можешь пока программу лояльности для курьеров придумать)))	 Informacion - bulletanna8@gmail mail.google.com/mail/u/0/?tab=rm&ogbl#inbox/FMfcgzGkZGpdrtnqZdBmbjJFCGJdRHpn Gmail Buscar en el correo electrónico Informacion Esperanza Grana <esper.grana@gmail.com> sáb, 10 jul. 00:59 ¡Hola! ¡Estoy en shock! ¡Mira cómo los gringos tienen todo chévere! Mis supervisores crearon un sitio web, ¡ahora el trabajo de los mensajeros se rastrea casi en línea! Las coordenadas de caletas se determinan con una precisión de un metro ... ven a echar un vistazo dopedoughyignlbq.onion d.hor hor420 Pronto tendremos así nosotros. Puede pensar en un programa de fidelización para mensajeros por ahora)))
Перевод: Я почти забыл… Напиши название салона заглавными буквами!!![1]	

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

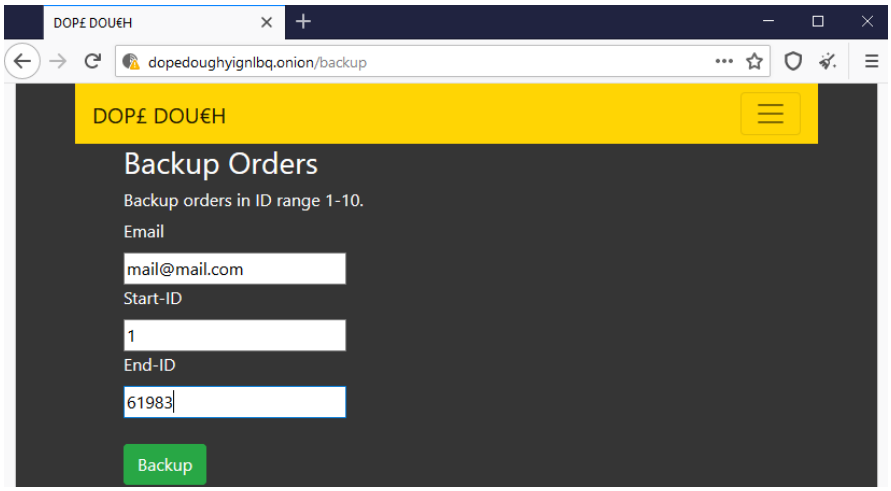


[1] На основе которых слушатели делают вывод, что ответ необходимо вводить заглавными буквами

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»	Файл Главная Вставка Разметка страницы Формулы Данные Рецензирование Вид ABBYY FineReader 12 Acrobat W25 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,33.386266117893555,-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,36.15964090061663,-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	

3	Meth	Meth budget request	33,386	-112,243
4	LSD	LSD elite shipment	39,904	-82,966
5	Marijuana	Marijuana smart order	36,110	-115,131
6	Hashish	Hashish powerful distribution	36,160	-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
11	Marijuana	Marijuana discounted distribution	39,784	-86,164
12	Amphetamine	Amphetamine secure request	33,464	-112,321
13	Meth	Meth discounted transport	39,785	-86,107

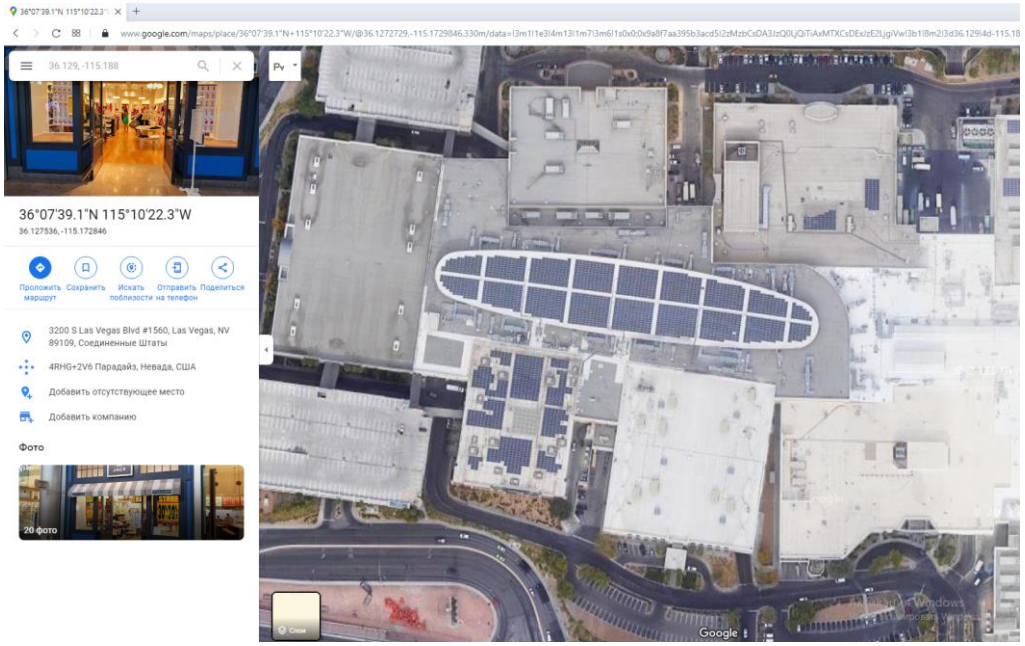
Объединить колонки с широтой и долготой	

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

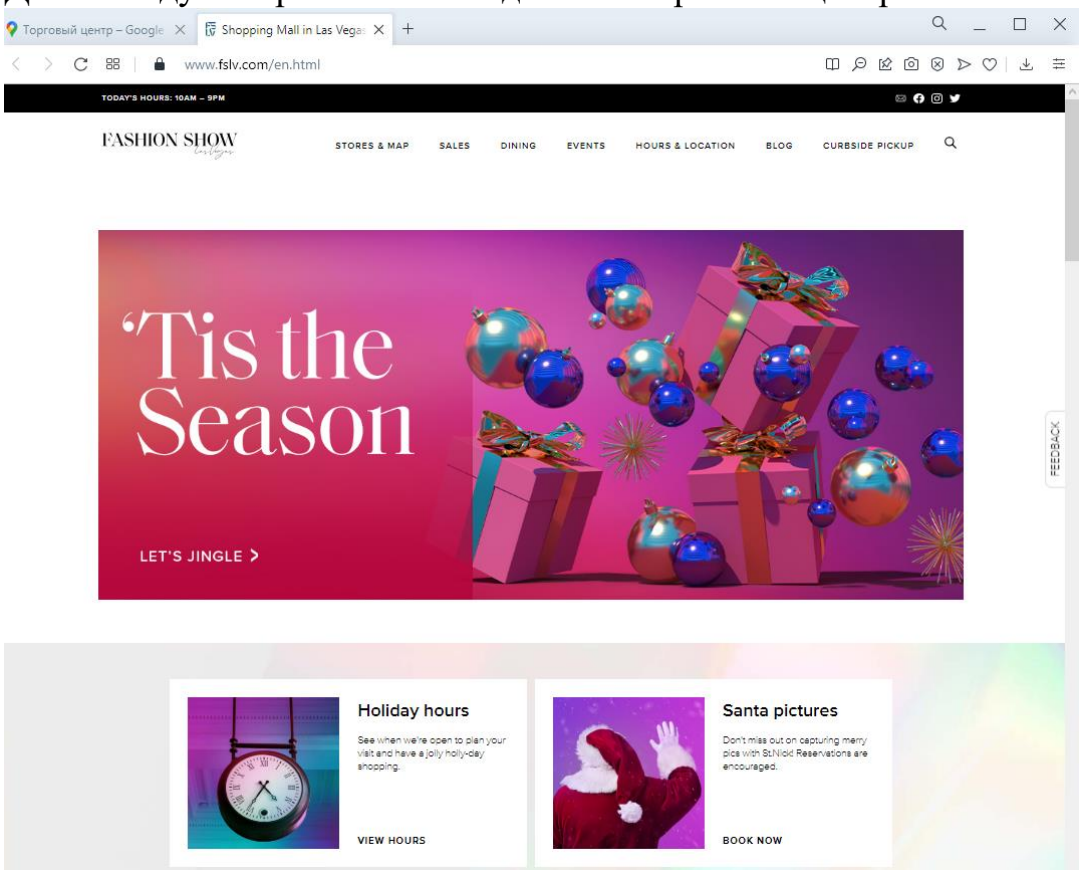
Определить координаты, которые чаще всего повторяются		

1	Названия строк	Количество по полю
2	36.129, -115.188	77
3	36.13, -115.188	59
4	36.129, -115.187	32
5	36.13, -115.189	31
6	36.129, -115.189	29
7	36.13, -115.187	18
8	36.169, -86.798	15
9	36.151, -86.79	13
10	36.16, -86.772	13
11	36.165, -86.773	13
12	36.173, -86.779	13
13	36.128, -115.189	12
14	36.164, -86.794	12
15	36.154, -86.8	11

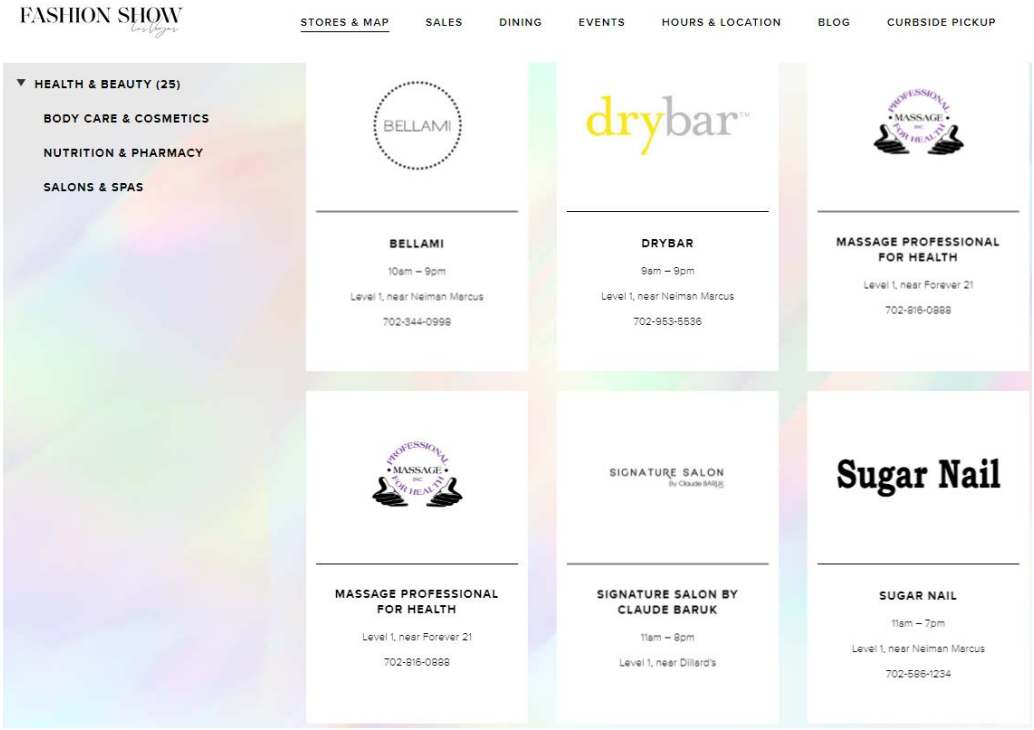
На основании полученной информации слушатель должен начать осматривать с помощью ресурсов GoogleКарты или ЯндексКарты территорию по найденным координатам для установления торгового центра с овальной крышей:



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:

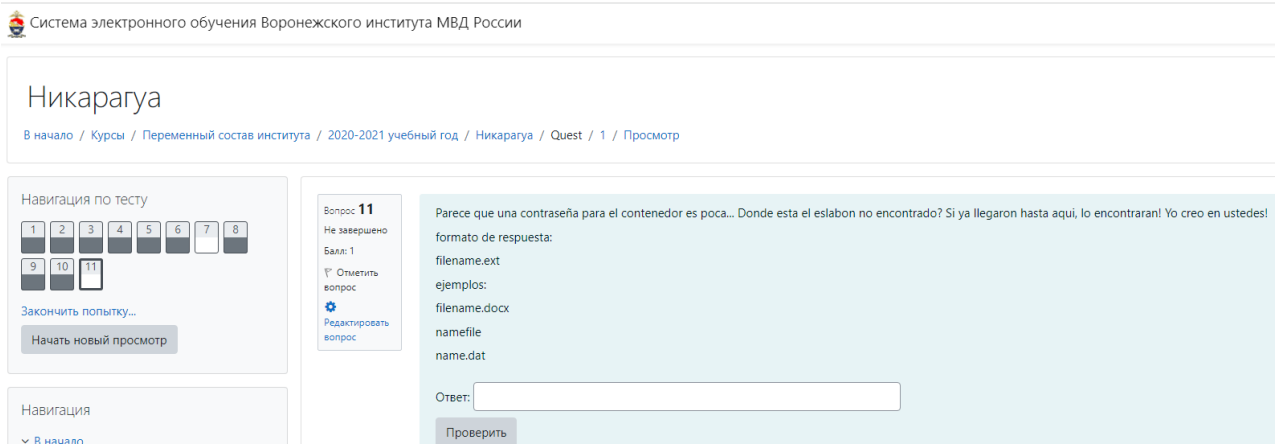
Parece que una contraseña para el contenedor es poca... Donde esta el eslabon no encontrado? Si ya llegaron hasta aqui, lo encontraran! Yo creo en ustedes!

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



Снимок экрана с одиннадцатым заданием для сюжетной линии № 1

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.

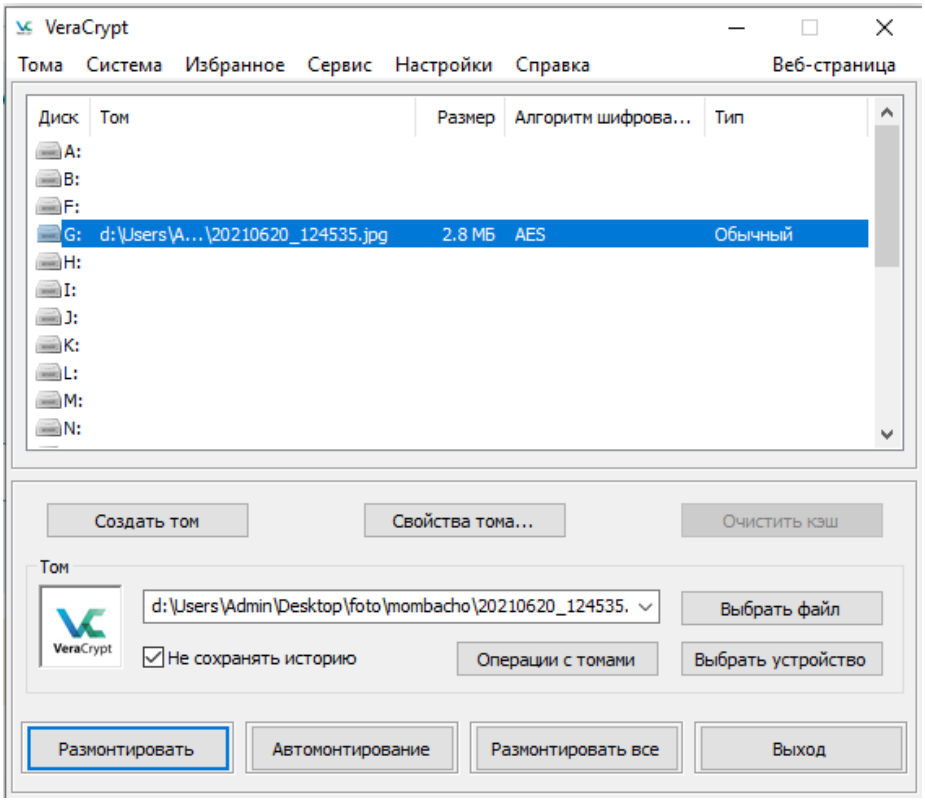
Имя	Размер	Сжат	Тип	Изменён	CRC32
..			Папка с файлами		
a mi madre.jpeg	335 194	248 576	Файл "JPEG"	27.06.2021 21:34	A3E24FB4
amor en Esplendor.jpg	105 678	105 678	Файл "JPG"	27.06.2021 20:59	98455D6C
Antonio Machado.docx	12 061	9 337	Документ Micros...	27.06.2021 21:11	7FBC8155
Bilingüe-Porque-hablo-español.png	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

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

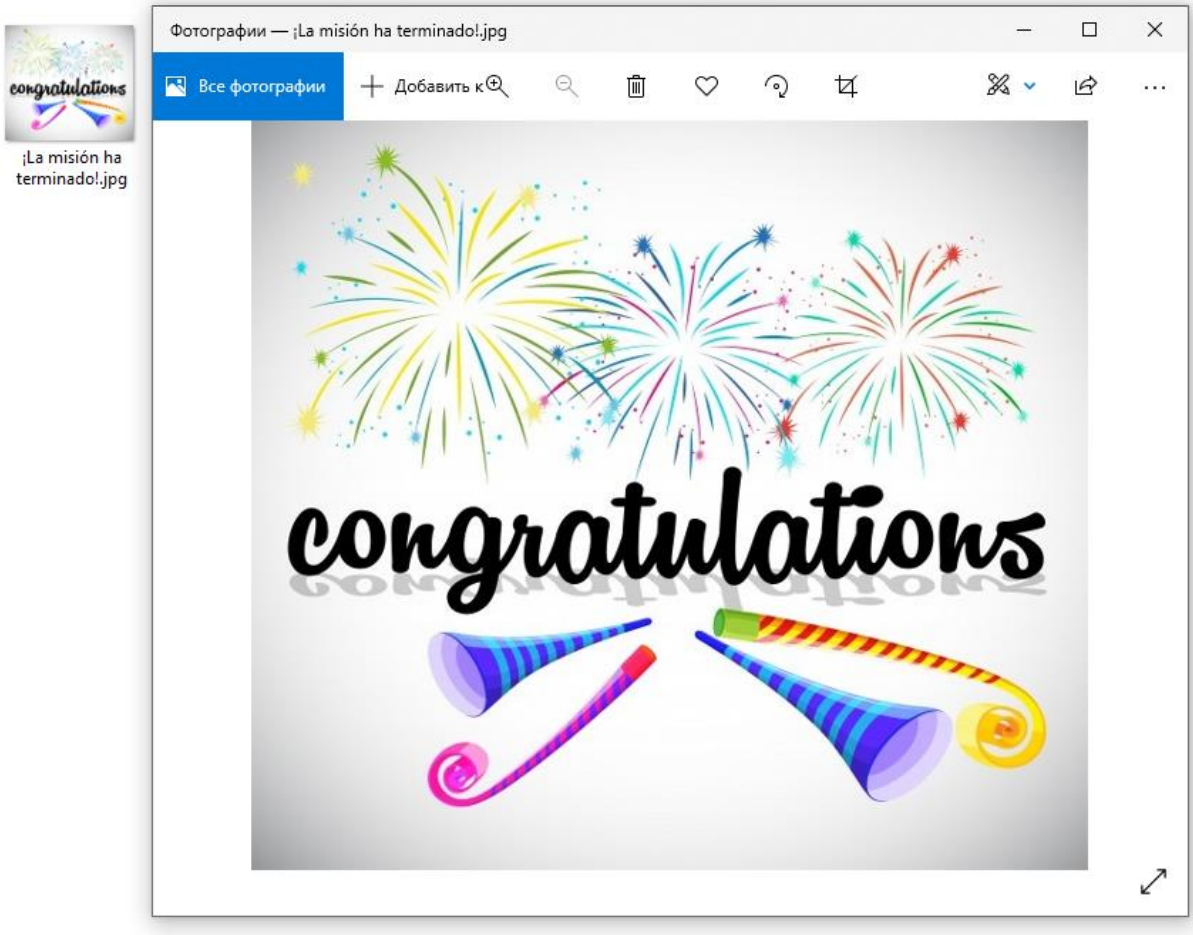
«Es todo - monten el contenedor!»

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 позволит 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

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).

Основная литература

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

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

3. Иванов С. А. Основы деловой (конкурентной) разведки : учебное пособие / С. А. Иванов, С. Ю. Микадзе. – Санкт-Петербург : Санкт-Петербургский государственный экономический университет, 2020. – 182 с.

4. Конкурентная разведка: технологии и противодействие / В. И. Аверченков [и др.]. – 2-е изд., стереотипное. – Москва, 2017.

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

6. Павлов А. В. Конкурентная разведка : учебное пособие / А. В. Павлов, Б. И. Ткаченко, А. М. Шунаев. – Санкт-Петербург : Санкт-Петербургский государственный экономический университет, 2020. – 102 с.

Дополнительная литература

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

2. 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.

3. 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.

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

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

6. 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.

7. 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.

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

9. 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.

10. 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.

11. 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.

12. Шумков Е. А. Конкурентная разведка в сети Интернет для вуза / Е. А. Шумков // электронный сетевой политематический журнал. Научные труды КубГТУ: – 2016. – № 3. – С. 67–72.

13. Ющук Е. Л. Интернет-разведка: руководство к действию / Е. Л. Ющук. – Москва : Вершина, 2007. – 256 с.

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