

Министерство науки и высшего образования Российской Федерации  
Федеральное государственное автономное образовательное  
учреждение высшего образования  
«Южно-Уральский государственный университет  
(национальный исследовательский университет)»  
Институт естественных и точных наук  
Факультет математики, механики и компьютерных технологий  
Кафедра прикладной математики и программирования  
Направление подготовки: 09.04.04 Программная инженерия

РАБОТА ПРОВЕРЕНА

Рецензент,

\_\_\_\_\_/\_\_\_\_\_  
« \_\_\_\_ » \_\_\_\_\_ 20 \_\_\_\_ г.

ДОПУСТИТЬ К ЗАЩИТЕ

Заведующий кафедрой, д.ф.-м.н.,  
доцент

\_\_\_\_\_/А.А. Замышляева  
« \_\_\_\_ » \_\_\_\_\_ 20 \_\_\_\_ г.

Использование контрольной точки во внутренней сети для анализа  
трафика в режиме реального времени

ПОЯСНИТЕЛЬНАЯ ЗАПИСКА  
К ВЫПУСКНОЙ КВАЛИФИКАЦИОННОЙ РАБОТЕ  
ЮУрГУ–09.04.04.2019.449.ПЗ ВКР

Руководитель работы, к.ф.-м.н.,  
доцент кафедры ПМиП

\_\_\_\_\_/С.М. Елсаков  
« \_\_\_\_ » \_\_\_\_\_ 2019 г.

Автор работы

Студент группы ЕТ-225

\_\_\_\_\_/Х.А. Флорес Б.  
« \_\_\_\_ » \_\_\_\_\_ 2019 г.

Нормоконтролер, ассистент

\_\_\_\_\_/Н.С. Мидоночева  
« \_\_\_\_ » \_\_\_\_\_ 2019 г.

Челябинск  
2019

## АННОТАЦИЯ

Флорес Бетанкур Х.А. Использование контрольной точки во внутренней сети для анализа трафика в режиме реального времени. – Челябинск: ЮУрГУ, ЕТ-225, 58 с., 31 ил. 9 табл., библиогр. список – 22 наим., 1 прил.

Целью данной работы является разработка приложения, отвечающего за анализ сетевого трафика сотрудников, подозреваемых в компьютерных преступлениях в венесуэльской компании CANTV (Национальная телефонная компания Венесуэлы).

В первом разделе был проведен анализ процесса компьютерной криминалистики, рассмотрены методы, применяющиеся для анализа сетевого трафика, проанализирована их связь с исследователем в реальном времени (мониторинг трафика).

Во втором разделе проанализирован актуальный процесс компьютерной криминалистики в компании Cantv.

Третий раздел был посвящен изучению технологии взаимодействия между системами с помощью языка Java.

В четвертом разделе описана разработанная система, пользовательский интерфейс программы и представлены результаты проверки ее работы на экспериментальных данных.

## ОГЛАВЛЕНИЕ

|                                                                                                    |    |
|----------------------------------------------------------------------------------------------------|----|
| ВВЕДЕНИЕ.....                                                                                      | 7  |
| 1 КОМПЬЮТЕРНЫЙ КРИМИНАЛИСТИЧЕСКИЙ АНАЛИЗ.....                                                      | 9  |
| 1.1 Информация о компании SANGV .....                                                              | 12 |
| 1.2 Процесс компьютерной криминалистики .....                                                      | 15 |
| 1.3 Методологии анализа компьютерной криминалистики .....                                          | 18 |
| 1.4 Информационная безопасность в реальном времени.....                                            | 19 |
| 1.5 Обоснование выбора средств разработки.....                                                     | 26 |
| 2 МОДЕЛЬ СИСТЕМЫ .....                                                                             | 30 |
| 2.1 Структура системы.....                                                                         | 30 |
| 2.2 Основной алгоритм программы.....                                                               | 31 |
| 2.3 Схема алгоритма пользовательского процесса.....                                                | 32 |
| 2.4 Схема алгоритма подключения к серверу протоколу TCP.....                                       | 33 |
| 2.5 Схема алгоритма анализа трафика в корпоративных приложениях.....                               | 34 |
| 2.6 Общая схема системы.....                                                                       | 35 |
| 3 РАЗРАБОТКА АРХИТЕКТУРЫ, ИНТЕРФЕЙСА СИСТЕМЫ .....                                                 | 37 |
| 3.1 Проектирование базы данных.....                                                                | 39 |
| 3.2 Окно подключения к приложению.....                                                             | 43 |
| 3.3 Главное окно приложения пользователя-исследователя .....                                       | 44 |
| 3.4 Главное окно приложения пользователя-координатора .....                                        | 45 |
| 3.5 Главное окно приложения пользователя-администратора .....                                      | 46 |
| 3.6 Окно добавления нового инцидента .....                                                         | 47 |
| 3.7 Окно редактирования инцидента .....                                                            | 48 |
| 3.8 Окно добавления пользователя.....                                                              | 49 |
| 3.9 Окно редактирования пользователя.....                                                          | 50 |
| 3.10 Окно анализа трафика сотрудника.....                                                          | 51 |
| 3.11 Окно экспорта в PDF.....                                                                      | 52 |
| 3.12 Эффективность подключения к серверу корпоративных<br>приложений с библиотекой FTPClient ..... | 52 |
| 3.13 Эффективность захвата трафика с помощью библиотекой Jscap.....                                | 53 |
| 3.14 Эффективность применения анализа времени по сравнению с<br>анализа в реальном времени .....   | 53 |
| ЗАКЛЮЧЕНИЕ .....                                                                                   | 55 |

|                                   |    |
|-----------------------------------|----|
| БИБЛИОГРАФИЧЕСКИЙ СПИСОК .....    | 56 |
| ПРИЛОЖЕНИЕ 1 Текст программы..... | 59 |

## ВВЕДЕНИЕ

В настоящее время, с ростом технологических достижений, человек проводит большую часть своего дня, используя телефон или компьютер. С помощью этих устройств осуществляется большинство рутинных действий, таких как интернет-покупки, банковские операции, общение с родственниками, отдых и другие ежедневные действия.

С увеличением пользователей современных технологий также увеличивается число преступников, которые используют эти технологии для совершенствования своего способа совершения преступления. Такие преступления в Венесуэле описаны в специальном законе о компьютерных преступлениях, в котором они считаются преступлением от неправомерного доступа к системе до мошенничества, фальсификации и компьютерного шпионажа. Самым большим недостатком в борьбе с этими преступлениями является анонимность правонарушителя, потому что в интернете его идентичность – это IP-адрес, который может быть скрыт или внутри компании скрывается за пользователем, который не имеет прямого отношения к человеку.

Информационная безопасность – это область, связанная с информатикой и телематикой, которая фокусируется на защите вычислительной инфраструктуры и всего, что связано с ней, и, особенно информации, содержащейся на компьютере [1]. Методы и процессы против компьютерных преступлений, такие как: предотвращение, защита информации и последующий анализ совершенного преступления, который называется компьютерной криминалистикой. Компьютерная криминалистика основана на применении научных методов и аналитики для идентификации, сохранения, анализа и представления данных.

Анализ в отделе компьютерной криминалистики проводится на оборудовании, которые подозреваются в совершении преступления,

возможно, оборудование не имеет соответствующей информации, поэтому процесс сбора данных является одним из самых важных в компьютерной криминалистике. Исследователи должны знать, где искать и иметь возможность получать наибольший объем информации в кратчайшие сроки, поскольку это может означать немедленное выявление правонарушителя.

В этом процессе анализа, где исследователь должен знать, что и где искать, тратится время и нет уверенности в получении ожидаемых результатов. В этой исследовательской работе в качестве эталона используется информация отдела компьютерной криминалистики компании CANTV.

Таким образом, целью данной работы является разработка приложения для исследования подозреваемых в режиме реального времени во внутренней сети компании CANTV.

Для достижения поставленной цели необходимо решить следующие задачи:

- 1) изучить и проанализировать методы, применяющиеся в компьютерной криминалистике и их использование в режиме реального времени;
- 2) ознакомиться с библиотеками, отвечающими за связи между системами и анализ трафика в внутренних сетях в языке Java;
- 3) проектировать структуры системы (схема классов, схема пользователей, схема системы, схема базы данных);
- 4) разработать компьютерную программу, реализующую разработанную структуру;
- 5) разработать пользовательский интерфейс;
- 6) подготовить подходящую среду для моделирования и тестирования системы (Установить и настроить сервер приложений Ubuntu 18);
- 7) проверить работу программы на экспериментальных данных.

## 1 КОМПЬЮТЕРНЫЙ КРИМИНАЛИСТИЧЕСКИЙ АНАЛИЗ

Компьютерная безопасность является актуальной задачей в наше время, так же как компьютерная криминалистика. Это объясняет большое разнообразие исследований на данную тему.

Первый закон, касающийся компьютерной криминалистики, был принят в 1978 году на форуме «Florida Computer Crimes Act». Где обсудили изменения и удаления данных в компьютерной системе, а также повреждения компьютерного оборудования [2].

С момента начала включения в правовую базу компьютерных преступлений многие компании разрабатывают цифровые и физические инструменты для анализа электронного оборудования.

В 1981 году была разработана первая программа сбора доказательств, которая отвечала за создание точной копии дискет.

В период с 1982 по 1984 год появляются различные инструменты, которые в принципе не были посвящены для экспертизы компьютерной криминалистики, такие как «Norton Utilities». Разработка приложения под названием UnErase, которое позволяет восстанавливать случайно удаленные файлы, но было полезно с точки зрения компьютерной криминалистики.

В настоящее время в течение всего года проводятся форумы, на которых обсуждаются новинки в области компьютерной криминалистики, такие как «Digital Forensic Research Workshop (DFRWS)» и «International Forensic Science Symposium», организуемые Интерполом.

30 октября 2001 года в Венесуэле был принят специальный закон «О борьбе с киберпреступностью», цель которого заключается в комплексной защите систем, использующих информационные технологии, а также в предупреждении и наказании за преступления, совершенные против таких систем или любого из их компонентов или совершенные с использованием таких технологий на условиях, предусмотренных законом [3].

8 августа 2014 открывается в Венесуэле CENIF (Национальный центр компьютерной криминалистики), который является первой и единственной лабораторией компьютерной криминалистики в Венесуэле и одной из самых важных лабораторий в Латинской Америке для приобретения, анализа, сохранения и представления доказательств, связанных с информационно-коммуникационными технологиями [4].

CENIF намерен создать службу технической поддержки всех государственных органов, обладающих компетенцией в области цифровых экспертиз.

Другим учреждением, которое поддерживает органы государства с помощью анализа цифровых экспертиз, является отдел компьютерной криминалистики компании CANTV, где анализируются внутренние инциденты, в которых отражаются мошенничество с предприятием, утечка информации, неправильное использование защищенных систем, среди других преступлений, совершаемых сотрудниками предприятия или внешними лицами. В CANTV также обрабатываются внешние инциденты, где запрашивают консультацию компьютерных экспертов для анализа оборудования, участвующего в делах, связанных с другими организациями.

Лаборатория Касперского в режиме реального времени отображает интерактивную карту глобальных кибератак, в которых мы будем выделять локальные атаки заражения, сетевые атаки и уязвимости, сделанные в Венесуэле.

Лаборатория Касперского каждый месяц проводит анализ статистических данных о вирусах в локальной сети. На рисунке 1.1 и на рисунке 1.2 показан процент атак в мае и июне 2019 года. В исследовании показано, что более 30% атак связаны с вредоносной троянской программой. Наиболее подвержена атаки платформа windows.



| Top - Local infections IN THE LAST MONTH |                                     |
|------------------------------------------|-------------------------------------|
| 1                                        | Trojan.WinLNK.Agent.gen 16.58%      |
| 2                                        | Trojan.WinLNK.Agent.qk 14.84%       |
| 3                                        | DangerousObject.Multi.Generic 9.77% |
| 4                                        | HackTool.MSIL.KMSAuto.di 7.69%      |
| 5                                        | Trojan.WinLNK.Runner.jo 6.92%       |
| 6                                        | Trojan.WinLNK.Starter.gen 6.78%     |
| 7                                        | HackTool.MSIL.KMSAuto.dh 6.78%      |
| 8                                        | Trojan.Win32.AutoRun.gen 3.71%      |
| 9                                        | Worm.Win32.Autoit.aky 3.69%         |
| 10                                       | Trojan.Win32.Swisyn.bner 3.51%      |

Рисунок 1.1 – Заражение локальной сети в Венесуэле

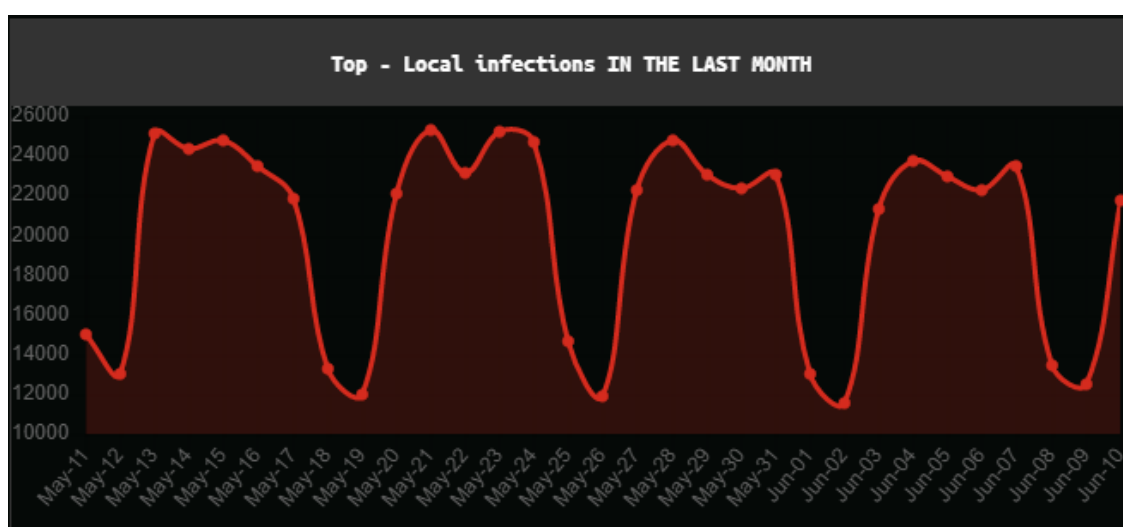


Рисунок 1.2 – Ежемесячное распределение зараженной локальной сети в Венесуэле

Помимо представления анализа статистических данных о вредоносных программах, лаборатория Касперского каждый месяц проводит анализ статистических данных об уязвимости программ. На рисунке 1.3 и на рисунке 1.4 показан процент уязвимости в мае и июне 2019 года. В исследовании показано, что более 30% атак связаны с уязвимостью The shadow broker - это уязвимость платформы Windows, через которую эксплойты получают несанкционированный доступ к системам семейства Windows.

| Top - Vulnerabilities IN THE LAST MONTH |                                |        |
|-----------------------------------------|--------------------------------|--------|
| 1                                       | Exploit.Win32.ShadowBrokers.ae | 32.27% |
| 2                                       | Exploit.AndroidOS.Lotoor.bg    | 12.66% |
| 3                                       | Exploit.AndroidOS.Lotoor.cd    | 7.25%  |
| 4                                       | Exploit.AndroidOS.Psneuter.a   | 5.7%   |
| 5                                       | Exploit.AndroidOS.Lotoor.bm    | 3.77%  |
| 6                                       | Exploit.Script.Generic         | 3.19%  |
| 7                                       | Exploit.Python.Agent.w         | 2.9%   |
| 8                                       | Exploit.Win32.MS17-010.shc     | 2.22%  |
| 9                                       | Exploit.Linux.Enoket.a         | 2.13%  |
| 10                                      | Exploit.Win32.ShadowBrokers.ab | 2.13%  |

Рисунок 1.3 – Уязвимость в Венесуэле

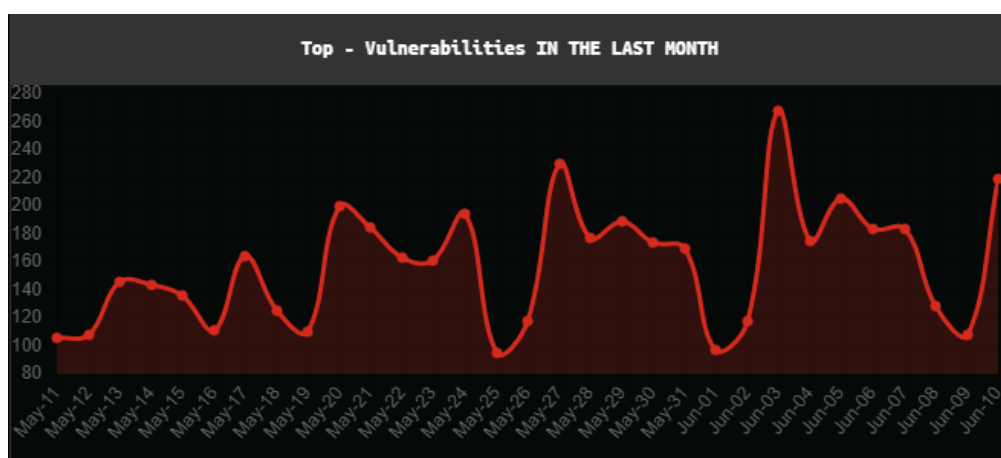


Рисунок 1.4 – Ежемесячное распределение уязвимости в Венесуэле

Анализ статистических данных о сетевых атаках представлен лабораторией касперского. В результате более 30% атак связаны с вторжениями в windows и android. Эти атаки пытаются удаленно использовать уязвимые или неправильно настроенные приложения, службы и операционные системы по сети для выполнения кода и выполнения несанкционированных сетевых действий. На рисунке 1.5, и на рисунке 1.6 показано распределение сетевых атак в мае и июне 2019 года.

### 1.1 Информация о компании CANTV

CANTV (Национальная телекоммуникационная компания Венесуэлы) является венесуэльской государственной телекоммуникационной компанией. Ее услуги варьируются от телефонии, которая является его основной сильной

стороной, до таких услуг, как продажа компьютеров, услуги по подключению к интернету. Гостям предоставляются услуги спутникового телевидения.

| Top - Network attacks IN THE LAST MONTH |                                                  |
|-----------------------------------------|--------------------------------------------------|
| 1                                       | Intrusion.Win.MS17-010.o 27.24%                  |
| 2                                       | BruteForce.Generic.Rdp.d 14.98%                  |
| 3                                       | BruteForce.Generic.Rdp.a 6.5%                    |
| 4                                       | BruteForce.Generic.MSSQL.a 1.64%                 |
| 5                                       | Intrusion.Win.EternalRomance.s 0.77%             |
| 6                                       | BruteForce.Generic.RDP 0.62%                     |
| 7                                       | BruteForce.Generic.Rdp.c 0.4%                    |
| 8                                       | Intrusion.Win.CVE-2017-0147.sa.leak 0.38%        |
| 9                                       | Intrusion.Win.EternalRomance.fish.nbt.leak 0.34% |
| 10                                      | Intrusion.Win.MS17-010.cf 0.25%                  |

Рисунок 1.5 – сетевая атака в Венесуэле

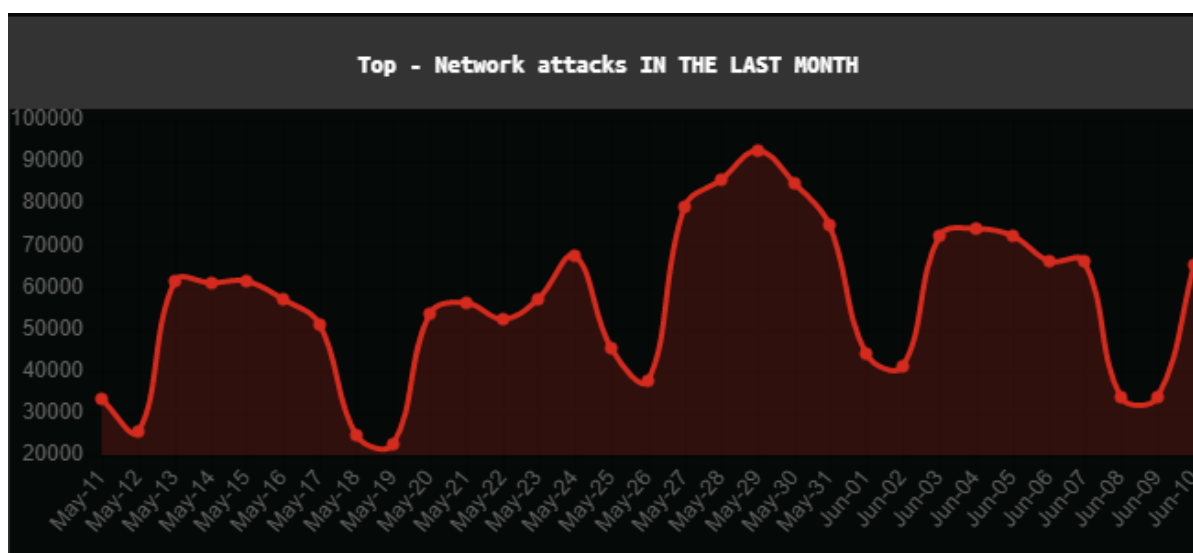


Рисунок 1.6 – ежемесячное распределение сетевой атаки в Венесуэле

Компания была основана 20 июня 1930 года, когда получили разрешение министерства развития на строительство и эксплуатацию телефонной сети в федеральном округе и других штатах страны. Компания начала приобретать несколько телефонных компаний по всей стране. С момента своего создания компания была сосредоточена на приобретении технологических ресурсов для модернизации и масштабирования своих услуг, поэтому в ноябре 1981 года она покупает и устанавливает двадцать цифровых станций, включая обучение операторов, необходимых для их надлежащего функционирования.

Доступ к электросвязи является ключевым фактором экономического роста и социального, политического и культурного развития, о чем уже свидетельствуют сотни технических докладов и исследовательских работ, подготовленных в самых разных национальных контекстах за последние два десятилетия. На глобальном уровне эта реальность была четко признана Организацией Объединенных Наций, включив в так называемые «цели в области развития, сформулированные в Декларации тысячелетия» обязательство предоставлять доступ к выгодам от новых технологий, особенно информационных и коммуникационных технологий.

Количество абонентов мобильной связи в Венесуэле увеличилось до 104,5%, 28 123 570 зарегистрированных абонентов. Таким образом, темпы расширения услуг были восстановлены пропорционально более высоким показателям проникновения. Дочерняя компания CANTV на данный момент имеет 65% абонентов. проникновения.

Процессы региональной интеграции в Латинской Америке в последнее время приобрели беспрецедентный темы. Формирование и укрепление ALBA (Боливарианский альянс для народов нашей Америки), расширение MERCOSUR (общий рынок стран Южной Америки) с предстоящим вступлением Венесуэлы в качестве полноправного партнера, запуск Южного Банка, несколько соглашений в области энергетики, культуры и других различных областях, выражают сильную волю интеграционистов. Еще можно выделить серьезные трудности в области сотрудничества и конвергенции в областях экономической и торговой интеграции, конвергенции в областях экономической и торговой интеграции.

Важной стратегией развития образования и телекоммуникации в Венесуэле является развитие компании CANTV, которая имеет наибольшее количество абонентов в стране.

В CANTV находится один из самых важных отделов компьютерной криминалистики в Венесуэле. Отдел компьютерной криминалистики

отвечает за проведение внутреннего расследования компании, в которых находятся дела, связанные с мошенничеством с компанией, манипулированием информацией, связанной с мобильными пользователями, утечкой жизненно важной информации компании или правительственной информацией, обрабатываемой в компании, также расследуются атаки, совершенные на сеть компании, ее веб-порталы.

Важность отдела компьютерной криминалистики в Венесуэле заключается в том, что он проводит расследование дел, связанных с другими государственными организациями и предприятиями. Отдел использует несколько платных приложений для компьютерной криминалистики, таких как EnCase Forensic, для сетевого или физического анализа.

## 1.2 Процесс компьютерной криминалистики

Приобретение информации – это первый этап, при получении данных, связанных с произошедшим инцидентом. Этот сбор данных должен быть выполнен безопасно и попытаться собрать всю информацию, связанную с инцидентом (доказательства). Таким образом, нужно избегать манипулирования оригинальными доказательствами, поэтому всегда следует делать копии информации, а затем анализировать эти копии, обычно в суде копия передается истцу и ответчику.

Эти копии используются цифровыми доказательствами. Инженер-вычислитель Ajoy Gosh в своей статье в 2004 [19] определяет ее как «любая информация, подлежащая вмешательству человека или иным образом, была извлечена с компьютера. Доказательства должны быть в человеческой читаемой форме или могут быть истолкованы людьми, которые умеют представлять такую информацию с помощью компьютерной программы».

Какие доказательства присутствуют, где и как они хранятся. Это имеет важное значение для определения того, какие процессы будут использоваться для облегчения их восстановления. Кроме того, эксперт криминалист должен

иметь возможность идентифицировать тип информации, хранящейся на устройстве, и формат, в котором она хранится, чтобы соответствующая технология могла использоваться для ее извлечения. На данном этапе существует два способа сбора информации.

Сбор доказательств с помощью электронных средств – это процесс осуществляется из захваченного электронного оборудования, обычно осуществляется в лабораториях компьютерной криминалистики. Существует множество систем, отвечающих за проведение этого сбора как forensic toolkit.

Forensic Toolkit – это криминалистическое компьютерное программное обеспечение, сделанное AccessData. позволяет сканировать жесткий диск. Например, можно находить удаленные электронные письма и сканировать диск для текстовых строк, чтобы использовать их в качестве словаря паролей для расшифровки шифрования.

Набор инструментов также включает в себя отдельную программу образа диска под названием FTK Imager. Этот инструмент сохраняет образ жесткого диска в файл или сегменты, которые могут быть впоследствии перестроены. Вычисляет хэш-значения MD5 и подтверждает целостность данных перед закрытием файлов. Результатом является файл, который может быть сохранен в нескольких форматах.

Сбор доказательств с помощью цифровых средств – этот процесс выполняется через сеть, и выполняется с компьютера исследователя компьютерной криминалистики и зависит от нескольких факторов. Исследуемый пользователь должен быть подключен к сети и иметь порт доступа, который использует инструмент (обычно порт 5554).

Неправильное обращение с собранными доказательствами может повлиять на вывод данных, поэтому так важно сохранять собранную информацию. Когда речь идет о цифровых доказательствах, различные процедуры, используемые для сохранения информации, могут быть использованы в качестве надежности доказательств. Когда доказательства

получены физически с компьютера, электронное оборудование должно быть защищено от беспроводных сигналов, которые могут повредить внутреннюю информацию, существуют инструменты, используемые для этой функции, такие как сумки Фарадея.

Анализ – это техническая часть процесса, в котором использованы инструменты, предназначенные для компьютерной криминалистики для получения информации из копий полученных устройств, исследователь должен знать, где и что искать в зависимости от типа инцидента. Существует множество систем, отвечающих за проведение этого анализа, такие как:

1) Autopsy – это цифровая криминалистическая платформа, которая содержит цифровые криминалистические инструменты. Она используется правоохранительными органами, военными и корпоративными экспертами для расследования того, что произошло на компьютере;

2) DEFT Linux – это программа Linux для свободного программного обеспечения на основе Ubuntu для использования, связанного с компьютерной криминалистикой и компьютерной безопасностью.

Документирование действий – это этап процесса, который гарантирует документирование каждого действия, которое было предпринято на этапе анализа, для обеспечения его надежности при использовании в процессе компьютерной криминалистики.

На этапе представления результатов проводится презентация полученных результатов, дается заключение анализа и составляется отчет с процессом и рекомендацией специалиста.

Программное обеспечение EnCase является лидером программных продуктов для E-Discovery. EnCase позволяет решать ряд задач присущих как E-Discovery, так и выполнять ряд задач стоящих перед отделом информационной безопасности любой организации. Программное обеспечение поставляется в нескольких продуктах, предназначенных для компьютерной криминалистики, кибербезопасности, аналитики безопасности

и использования e-discovery. Encase традиционно используется в криминалистике для восстановления доказательств с изъятых жестких дисков. Encase позволяет следователю проводить углубленный анализ пользовательских файлов для сбора доказательств, таких как документы, фотографии, история интернета и информация реестра Windows [5]. Процесс анализа Encase показан на рисунке 1.7.

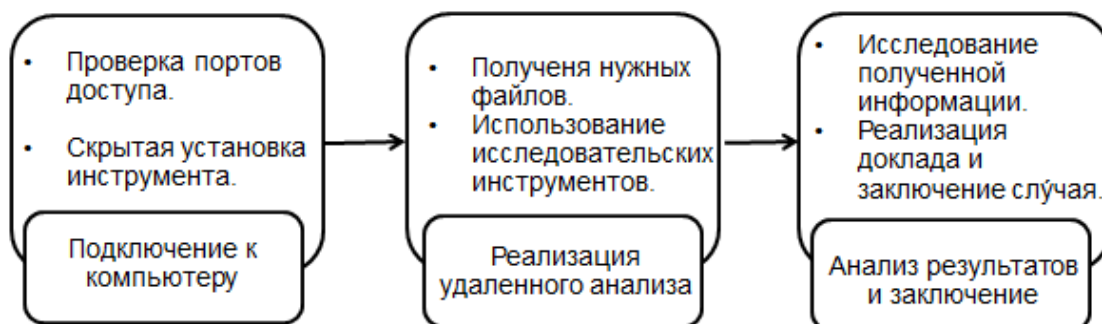


Рисунок 1.7 – Процесс анализа Encase

### 1.3 Методологии анализа компьютерной криминалистики

Методология министерства юстиции США (DOJ) отвечает за создание общей модели для применения к большинству электронных устройств и указывает четко определенную последовательность для выполнения каждого один из этапов, который предлагает, не проводит различия между криминалистическими компьютерными методами, применяемыми к компьютерам или другим электронным устройствам. Методология показан на рисунке 1.8 [6].

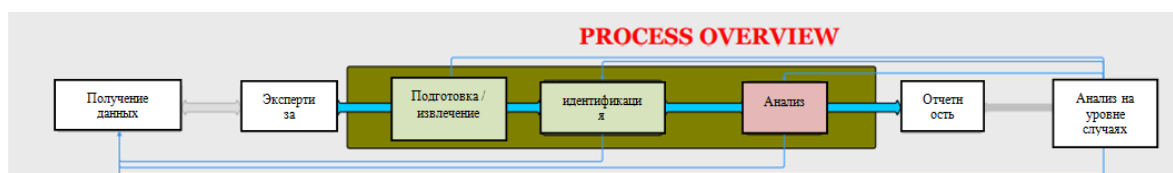


Рисунок 1.8 – Схема методологии DOJ

Методология Digital Forensics Research Workshop (DFRW) помогает определить и сфокусировать направление научного сообщества в отношении цифровой компьютерной криминалистики экспертизы. Содержит список



наиболее распространенных мест, где можно найти скрытую информацию. Предоставляет методы и действия для поиска скрытой информации [7] в качестве минуса можно отметить, что не предлагает конкретной процедуры для осуществления деятельности. Методология показана на рисунке 1.9 [8].

Институт SANS – это совместная научно-образовательная организация для специалистов в области безопасности. Для SANS надлежащее управление криминалистики и информатики экспертизой является ключом к борьбе с компьютерными преступлениями, требующими глубокого знания многих областей для надлежащего расследования. В методе SANS определяются форматы для установки цепочки хранения и определяются места, где можно найти скрытую информацию в операционных системах Windows и Linux.

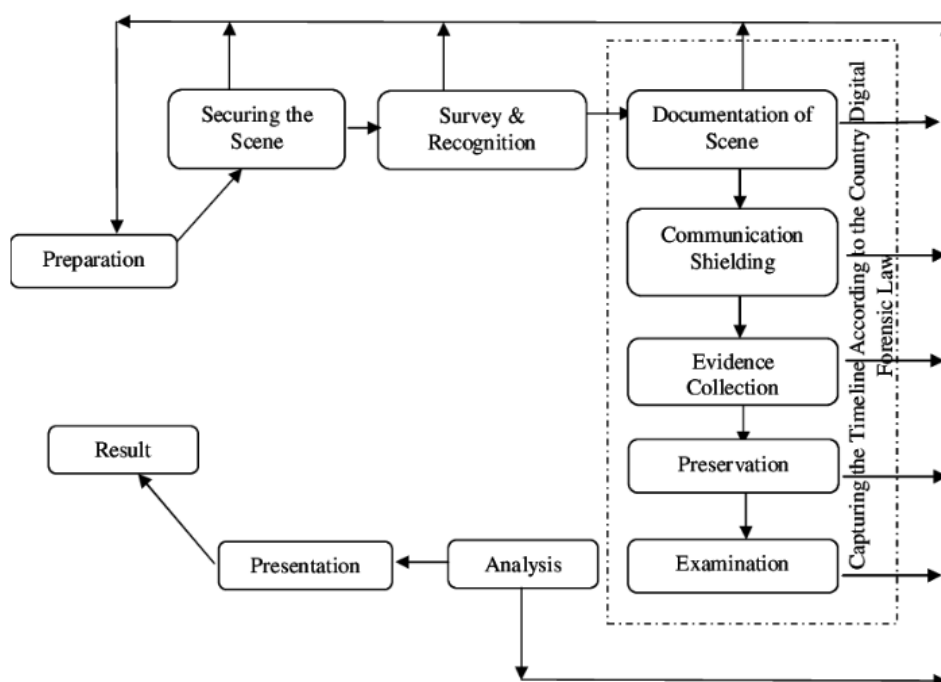


Рисунок 1.9 – Схема методологии DFRW

#### 1.4 Информационная безопасность в реальном времени

Система реального времени взаимодействует с вашей физической средой и реагирует на изменения окружающей среды в течение

определенного периода времени. Система реального времени должна быть напрямую связана с аппаратным и программным обеспечением.

В области компьютерной криминалистики используются методы «криминалистическая сеть» и «сеть мониторинга». Эти методы используются в расследовании в режиме реального времени и применяются в судебном процессе. Стоит отметить, что методы используются для расследования уже после совершения киберпреступления.

Сетевая криминалистика – это исследование анализа сетевой активности с целью выявления источника нарушений политики безопасности или информационной безопасности. Анализ отдельных потоков трафика и их содержимого имеет важное значение для полного понимания использования сети. Многие инструменты позволяют просматривать трафик в режиме реального времени, но мониторинг в режиме реального времени на любом уровне требует значительных людских и аппаратных ресурсов и не масштабируется до сетей больше одной рабочей группы [9]. Сетевая криминалистика имеет два применения:

1) безопасность: судебная экспертиза сети используется для повышения механизм защиты;

2) правоохранительные органы: сетевая криминалистика также используется чтобы получить доказательства по юридическим вопросам.

В компьютерной криминалистике необходимы методы для эффективного сбора данных. Первый метод связан с необходимостью захвата и хранения пакетов, проходящих через точку трафика в сети, и требуется большое количество памяти. Вторым методом является самым мощным и называется «Стоп, просмотр и прослушивание» пытается захватить только необходимую информацию с помощью фильтров и требует большой пропускной способности.

Мониторинг сети связан не только с мониторингом физической сети и хост-устройств, таких как маршрутизаторы, мосты, концентраторы и

компьютеры, но и с мониторингом служб, работающих на некоторых из этих устройств. Они предоставляют услуги хранения данных, манипуляции, презентации, услуги связи, и работают на сетевом уровне и выше. Фактически, мониторинговые службы контролируют службу прикладных уровней, службу доменных имен (DNS), протокол динамического управления хостом (DHCP), простой протокол передачи сообщений (SMTP) и протокол передачи гипертекста (HTTP) [10]. В настоящее время мониторинг сети подразделяется на несколько отдельных подсистем:

1) система обнаружения вторжений – следит за появлением угроз извне;

2) система мониторинга производительности сети (Network Performance Monitoring) «NPM» выявляет перегруженные устройства/каналы;

3) система мониторинга сети выполняет наблюдение за сетью в поисках проблем, вызванных отказавшими серверами, другими устройствами или сетевыми соединениями.

Брандмауэр – это специальный маршрутизатор, предназначенный для выполнения проверки сетевого трафика на то, что должно быть перенаправлено и какой трафик должен быть отброшен или пропущен. Это устоявшаяся и неотъемлемая часть сетевой безопасности. Он контролирует входящий и исходящий трафик на основе определенных правил безопасности. Маршрутизатор также определяет направление, в котором конкретный трафик может быть инициирован и разрешено проходить через него. Он работает как барьер между защищенной внутренней сетью и внешней сетью. На предприятии брандмауэры развертываются во внутренней сети для разделения сегментов. Брандмауэр может быть реализован на уровне пакетов IP[20].

honeypot – это компьютер или ловушка, которая содержит ценную информацию или ресурсы и кажется частью сети, но на самом деле изолирована и контролируется. Привлекая хакеров в систему, можно

собирать обновленные и ценные данные, которые помогают понять методологии и инструменты злоумышленников. Honeypot могут быть классифицированы в зависимости от их уровня взаимодействия на низкие, средние и высокие. Чем выше уровень взаимодействия, тем значительнее собираемые данные с соответственно возрастающими рисками. Кроме того, honeypots можно классифицировать в соответствии с их целями для исследования honeypots и производства honeypots. Другое возможное различие в области honeypots различает физические и виртуальные honeypots. С точки зрения расследования, honeypot является идеальным инструментом для тщательного изучения злоумышленников и мониторинга их движений [21].

Как правило, они считают приманок как инструмент или метод, который может быть развернут в процессе сетевой экспертизы.

E-mail экспертиза относится к исследованию источника и содержимого электронной почты в качестве доказательства, чтобы определить фактического отправителя и получателя сообщения, дата/время передачи, подробную запись электронной почты, намерения отправителя и т. д. Это исследование включает исследование метаданных, поиск, по ключевым словам, сканирование портов и т. д. для присвоения авторства и идентификации почтовых мошенников.

Существует много инструментов, которые могут помочь в изучении источника и содержания сообщения электронной почты, чтобы можно было исследовать атаку или вторжений. Эти инструменты, предоставляя простой в использовании формат браузера, автоматизированные отчеты и другие функции, помогают идентифицировать источник и место назначения сообщения, отслеживать путь, пройденный сообщением; идентифицировать спам и фишинговые сети и т. д. В этом разделе представлены некоторые из этих инструментов [22]:

1) eMailTrackerPro, анализирует заголовки электронной почты, чтобы определить IP-адрес машины, отправившей сообщение, чтобы отправитель мог быть отслежен. Возможно отслеживать несколько писем одновременно и легко отслеживать их. Географическое расположение IP-адреса является ключевой информацией для определения уровня угрозы или действительности сообщения электронной почты. Этот инструмент может указать на наиболее вероятный город, откуда пришло письмо. Он идентифицирует поставщика сети отправителя и предоставляет контактную информацию для дальнейшего расследования. Фактический путь к IP-адресу отправителя сообщается в таблице маршрутизации, предоставляя дополнительную информацию о местоположении, чтобы определить истинное местоположение отправителя. EMailTrackerPro проверяет черные списки DNS, (Spamcop) для дальнейшей защиты от спама и вредоносных писем. Поддержка спам-фильтров на японском, русском и китайском языках в дополнение к английскому языку;

2) EmailTracer – это работа в области компьютерной криминалистики, проведенная центром ресурсов для кибер-криминалистики (RCCF), который является центром передового опыта для кибер-криминалистики в Индии. EmailTracer разрабатывает инструменты кибер-криминалистики, основанные на требованиях правоохранительных органов. Среди других компьютерных криминалистических инструментов он разработал инструмент отслеживания электронной почты под названием EmailTracer. Этот инструмент отслеживает исходный IP-адрес и другие заголовки электронной почты, генерирует подробный отчет по анализу заголовков электронной почты, находит провайдера на уровне города отправителя и отображает исходное географическое местоположение электронной почты;

3) Adcomplain – это инструмент для сообщений электронной почты и сообщений от неприемлемых коммерческих usenet, таких как сетевые письма и объявления. Adcomplain автоматически анализирует сообщение, составляет

отчет о злоупотреблениях и отправляет отчет поставщику интернет-услуг преступника, выполняя анализ заголовка;

4) Aid4Mail Forensic – это программное обеспечение для компьютерной криминалистической экспертизы. Это инструмент миграции и преобразования электронной почты, который поддерживает несколько почтовых форматов, включая Outlook (PST, MSG файлы), Windows Live Mail, Thunderbird, Eudora, e mbox. Возможность искать почту по дате, содержание заголовка, и по содержанию тела сообщения;

5) AbusePipe анализирует сообщения о злоупотреблениях и определяет, какой из клиентов ESP является спам-рассылка на основе информации о жалобах, отправленных по электронной почте. AbusePipe автоматически генерирует отчеты, которые сообщают клиентам, что они нарушают приемлемую политику пользователя ESP, поэтому действие для их закрытия может быть принято немедленно;

6) Sawmill-GroupWise – это анализатор журнала почтового агента, который может обрабатывать журнал файлы в формате GroupWise Post Office Agent и генерировать динамическую статистику из них, анализируя и сообщая о событиях;

Веб-браузеры, которые широко используются в настоящее время являются Microsoft's Internet Explorer (IE), Mozilla Firefox, Netscape family, Safari, Google Chrome и т. д. Каждый из этих браузеров показывает историю просмотра веб-страниц различных пользователей, которые имеют учетные записи на одной машине. Веб-браузеры устанавливают куки во время каждого посещения. IE сохраняет историю просмотра пользователя в файле dat, браузеры семейства Netscape сохраняют веб-активность в файле с именем History.dat. Эти два файла являются скрытыми файлами. Таким образом, для того, чтобы увидеть эти скрытые файлы, браузер должен быть установлен, чтобы показать, как скрытые файлы и системные файлы. Эти файлы не могут быть легко удалены.

Анализатор пакетов – это программное обеспечение, которое собирает трафик, проходящий в и из компьютера, подключенного к сети. Сниффер может анализировать только то, что проходит через его сетевую карту. Внутри одного сегмента сети, в локальной сети все пакеты рассылаются всем машинам, из-за этого возможно перехватывать чужую информацию.

Система обнаружения вторжений (IDS) – это система, которая занимается безопасностью в сети, проверяя весь входящий и исходящий трафик в сети. Система отслеживает сеть на наличие подозрительных шаблонов и предупреждают администраторов, когда такие шаблоны распознаются. Исторически они использовались для предупреждения или блокирования злоумышленников:

1) сетевая система обнаружения вторжений (NIDS) – развертывает датчики в стратегических местах и проверяет трафик, наблюдая за нарушениями протокола и необычными шаблонами соединений, и вредоносным контентом. Его функция заключается в выявлении аномального поведения сегмента сети;

2) Host Based Intrusion Detection System (HIDS) – использует механизм мониторинга ОС для поиска вредоносных программ в системе. HIDS контролирует команды оболочки и системные вызовы, выполняемые пользовательскими приложениями и системными программами. HIDS имеет наиболее полную информацию о программе для обнаружения и, следовательно, является точным;

3) сигнатурная система обнаружения вторжений (SIDS) – использует известные шаблоны неправильного использования или сигнатуры против потока событий для обнаружения. Имеет низкие пороги ложной тревоги и также имеет точные сообщения;

4) прикладная система обнаружения вторжений (AIDS) – имеет более высокую точность и точный контекст, но ее трудно развернуть.

Инструментарий компьютерной криминалистики Forensics Investigation Toolkit (FIT) – это инструментарий компьютерной криминалистики для чтения и анализа содержимого сырых данных из интернета в формате захвата пакетов (PCAP). FIT предоставляет административным сотрудникам по вопросам безопасности, аудиторам, следователям по мошенничеству и судебным экспертам, а также сотрудникам правоохранительных органов возможность проводить анализ контента и восстанавливать необработанные данные из интернета, ранее захваченные из кабельных или беспроводных сетей. Все проанализированные и перестроенные протоколы и службы отображаются в удобном для пользователя формате. Другая уникальность FIT заключается в том, что импортированные необработанные файлы данных могут быть немедленно проанализированы и перестроены. Поддерживает функции управления обращениями, подробную информацию, включая дату-время, IP-адрес источника, IP-адрес назначения, MAC-адрес источника и т. д.

### 1.5 Обоснование выбора средств разработки

В настоящее время язык Java является одним из самых гибких и мощных языков программирования, универсальный, параллельный и объектно-ориентированный. Java – это язык программирования и вычислительная платформа, впервые выпущенная Sun Microsystems в 1995 году. Существует множество приложений и веб-сайтов, которые не будут работать, если у вас не установлена Java, и каждый день создаются новые приложения. Java быстр, безопасен и надежен [11]. Java был создан с пятью основными целями:

- 1) использование парадигмы объектно-ориентированного программирования;
- 2) разрешить выполнение программы в нескольких операционных системах;
- 3) включить поддержку постоянного обновления контента;



4) предназначен для выполнения кода в удаленных системах безопасным способом;

5) быть простым в использовании и использовать лучшее из других объектно-ориентированных языков, таких как C ++.

IDE NetBeans – это модульная, основанная на стандартах, интегрированная среда разработки (IDE), написанная на языке программирования Java™. Проект NetBeans состоит из полнофункциональной IDE с открытым исходным кодом, написанной на языке программирования Java, и многофункциональной клиентской платформы приложений, которую можно использовать в качестве универсальной среды для создания приложений любого типа [12]. В среде IDE NetBeans 8.2 имеются готовые анализаторы и редакторы кода для работы с новейшими технологиями Java 8.

Pcap – это интерфейс программного приложения для захвата пакетов. Реализация для систем на основе Unix известна как libpcap. Порт для Windows в libpcap называется WinPcap.

WinPcap состоит из драйвера, расширяющего операционную систему для обеспечения низкоуровневого доступа к сети, и библиотеки, которая используется для легкого доступа к низкоуровневым сетевым уровням [13].

Tcpdump выводит описание содержимого пакетов на сетевом интерфейсе, которые соответствуют логическому выражению; описанию предшествует отметка времени, напечатанная по умолчанию в виде часов, минут, секунд и долей секунды с полуночи [14]. Пример библиотеки показан на рисунке 1.10.

```
gilb1993@aplicaciones:~$ sudo tcpdump -n icmp
tcpdump: verbose output suppressed, use -v or -vv for full protocol decode
listening on enp7s0, link-type EN10MB (Ethernet), capture size 262144 bytes
11:34:21.590380 IP 10.10.1.217 > 10.10.1.30: ICMP echo request, id 27948, seq 1, length 64
11:34:21.590434 IP 10.10.1.30 > 10.10.1.217: ICMP echo reply, id 27948, seq 1, length 64
11:34:27.680307 IP 10.10.1.159 > 10.10.1.1: ICMP 10.10.1.189 udp port 59619 unreachable, length 115
```

Рисунок 1.10 – Пример библиотеки Tcpdump

jNetPcap – это Java-библиотека, основанная как на libpcap, так и на WinPcap. API jNetPcap обеспечивает базовую реализацию на основе библиотеки API unix libpcap (org.jnetpcap), а также предоставляет дополнительную функциональность WinPcap в качестве расширения (org.jnetpcap.winpcap) см. рисунок 1.11. Основные классы, которые реализуют функции libpcap и WinPcap:

1) org.jnetpcap.Pcap класс – основные методы libpcap, доступные на всех платформах;

2) org.jnetpcap.winpcap.WinPcap класс – расширения на основе библиотеки WinPcap, как правило, доступны только в системе на базе Windows.

Функции JnetPcap:

- 1) находить полный список сетевых интерфейсов;
- 2) открывать сетевой интерфейс или файл захвата PCAP для чтения пакетов;
- 3) применять фильтр пакетов;
- 4) выгружать пакеты в файл захвата PCAP;
- 5) передавать необработанные пакеты канального уровня по сетевому интерфейсу;
- 6) собирать статистику о счетчиках сетевого интерфейса [15].

```
List<PcapIf> alldevs = new ArrayList<PcapIf>();  
StringBuilder errbuf = new StringBuilder();  
int r = Pcap.findAllDevs(alldevs, errbuf);
```

Рисунок 1.11 – Пример библиотеки JNetPcap в JAVA

FTPClient инкапсулирует все функции, необходимые для хранения и извлечения файлов с FTP-сервера. Этот класс заботится обо всех деталях низкого уровня взаимодействия с FTP-сервером и обеспечивает удобный интерфейс более высокого уровня. Как и во всех классах, производных от SocketClient, должно сначала подключиться к серверу с connect, прежде чем

что-либо делать, и, наконец, отключиться [16]. Подключение к серверу по протоколу FTP см. рисунок 1.12.

```
FTPClient ftpl=new FTPClient();
ftpl.connect(server);
boolean login=ftpl.login(user, pass);
ftpl.enterLocalPassiveMode();
ftpl.changeWorkingDirectory(remoteDIR);
FTPFile[] files1=ftpl.listFiles();
```

Рисунок 1.12 – Подключение к серверу по протоколу FTP

Захват файлов, локализованных на FTP-сервере см. рисунок 1.13.

```
ftpClient.initiateListParsing("");
FTPFile[] files = ftpClient.listFiles("/aplicaciones");
```

Рисунок 1.13 – Пример библиотеки Tcprdump

MySQL, самая популярная система управления базами данных SQL с открытым исходным кодом, разрабатывается, распространяется и поддерживается корпорацией Oracle.

SQL-часть «MySQL» означает «структурированный язык запросов». SQL является наиболее распространенным стандартизированным языком, используемым для доступа к базам данных. В зависимости от среды программирования можно ввести SQL напрямую (например, для создания отчетов), внедрить инструкции SQL в код, написанный на другом языке, или использовать API для конкретного языка, скрывающий синтаксис SQL.

## 2 МОДЕЛЬ СИСТЕМЫ

Для разработки приложения для расследования подозреваемых в режиме реального времени во внутренней сети, следует выделить отдельные модули, которые должны реализовывать определенную часть функций.

### 2.1 Структура системы

Контрольная точка – сигнал, после которого система начинает сбор информации. Контрольной точкой может быть IP-адрес сотрудника, также может использовать в качестве контрольной точки его данным. Эту информацию получают из двух серверов, первый сервер, где находятся приложения компании. Каждое приложение компании должно создать для каждого действия журнал такого действия (журнал приложения), с этой информацией интегрированная система анализирует действия, используя в качестве фильтра IP-адрес подозреваемого.

Вторым является сервер SMTP, в компании CANTV каждый сотрудник входит в сеть компании с корпоративной электронной почтой, поэтому каждый сотрудник при использовании компьютера компании всегда подключен к серверу SMTP, в этом аспекте SMTP-сервер может быть частью интегрированной системы с включением приложения, которое выполняет сетевой анализ на SMTP-сервере, который отвечает за выполнение анализа, чтобы отделить список IP от подозреваемых.

Подключение приложения к серверу, где находятся внутренние приложения компании, для получения информации из журналов таких приложений и сохранение действий, выполняемых подозрительным сотрудникам с помощью библиотеки, отвечающей за соединение Ftp, в случае JAVA библиотека FTPClient. После подключения к серверам осуществляется передача журналов на сервер, где приложение локализовано, для дальнейшего анализа.

Приложение подключается к серверу SMTP, к которому должны подключаться все сотрудники компании. Приложение извлекает информацию из сети сервера SMTP, получает информацию от устройств, которые подключаются к серверу. Цель анализа - это использование сети сотрудника и получение информации о том, когда он находится в сети. С помощью библиотеки Jrcap (JAVA) осуществляется анализ сетевых интерфейсов, подключенных к компьютеру.

При эффективном соединении с серверами должна осуществляться передача информации с этих серверов на сервер, где хранится приложение, и таким образом сохранять информацию об использовании сети сотрудником и действиях, выполняемых в приложениях компании.

На главном экране пользователя-исследователя должны отображаться инциденты, которые были назначены этому пользователю, где отображаются данные инцидента, а также если подозрительный сотрудник находится в сети. Пользователю-координатору отображаются все инциденты в отделе, пользователь-координатор также может изменять инциденты и создавать новые инциденты.

После выбора случая, который требуется расследовать необходимо показать действия, выполненные во внутренних приложениях компании, которые сделал подозрительный сотрудник, этот трафик должен отображаться в режиме реального времени с задержкой в 30 секунд.

После анализа трафика сотрудника, исследователь может экспортировать отчет о результатах в формате PDF, это делается нажатием кнопки с логотипом экспорта.

## 2.2 Основной алгоритм программы

Настольное приложение разрабатывается под операционной системой Windows. Основной алгоритм работы всего приложения расположен на рисунке 2.1.



Рисунок 2.1 – Основной алгоритм

### 2.3 Схема алгоритма пользовательского процесса

После запуска приложения, запрашивается пользователя и пароль доступа к системе, проверяется база данных, что данные верны, а затем приступает к входу в систему. При запуске сеанса отображаются обращения, назначенные пользователю, второй шаг-выбор инцидента, который требуется

расследовать, отображение трафика подозреваемого и завершение процесса с экспортом отчета. Этот алгоритм показан на рисунке 2.2.

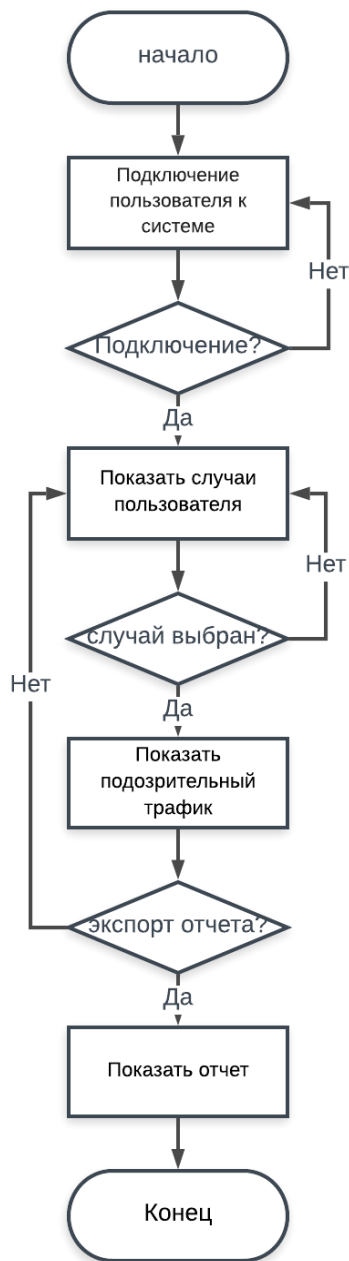


Рисунок 2.2 – Схема алгоритма пользовательского процесса

#### 2.4 Схема алгоритма подключения к серверу протоколу TCP

Анализ движения подозрительного сотрудника на сервере приложений компании, начинается с подключения приложения к серверу с помощью класса FTPClient, следующим шагом является захват и загрузка журналов

приложений и в конечном итоге фильтрация действий IP-адреса исследуемого сотрудника. Этот алгоритм показан на рисунке 2.3.



Рисунок 2.3 – Схема алгоритма подключения к серверу протоколу TSP

## 2.5 Схема алгоритма анализа трафика в корпоративных приложениях

Анализ сетевого трафика выполняется с помощью библиотеки Pcap, в которой перехватываются интерфейсы и сетевой трафик подозрительного сотрудника, на втором этапе сохраняется результат фильтра, выполненного с



IP подозреваемого, а затем показывает пользователю-следователю данные, связанные с трафиком, такие как IP-адрес прибытия, исходящий ip, результат действия, порт, используемый для соединения, и метод, выполненный для соединения Ftp, udp, sip, rtp и т. д. Этот алгоритм показан на рисунке 2.4.



Рисунок 2.4 – Схема алгоритма анализа трафика в корпоративных приложениях

## 2.6 Общая схема системы

Система разделена на 3 основных модуля, первый модуль – это сервер корпоративных приложений, приложение анализа трафика и подключение компьютера к сети.

Пользователь-следователь с помощью приложения собирает информацию о подозреваемых, расположенную на сервере корпоративных приложений, а затем передает их на сервер, где приложение сканирования, чтобы затем выполнить анализ трафика подозрительного сотрудника см. рисунок 2.5.

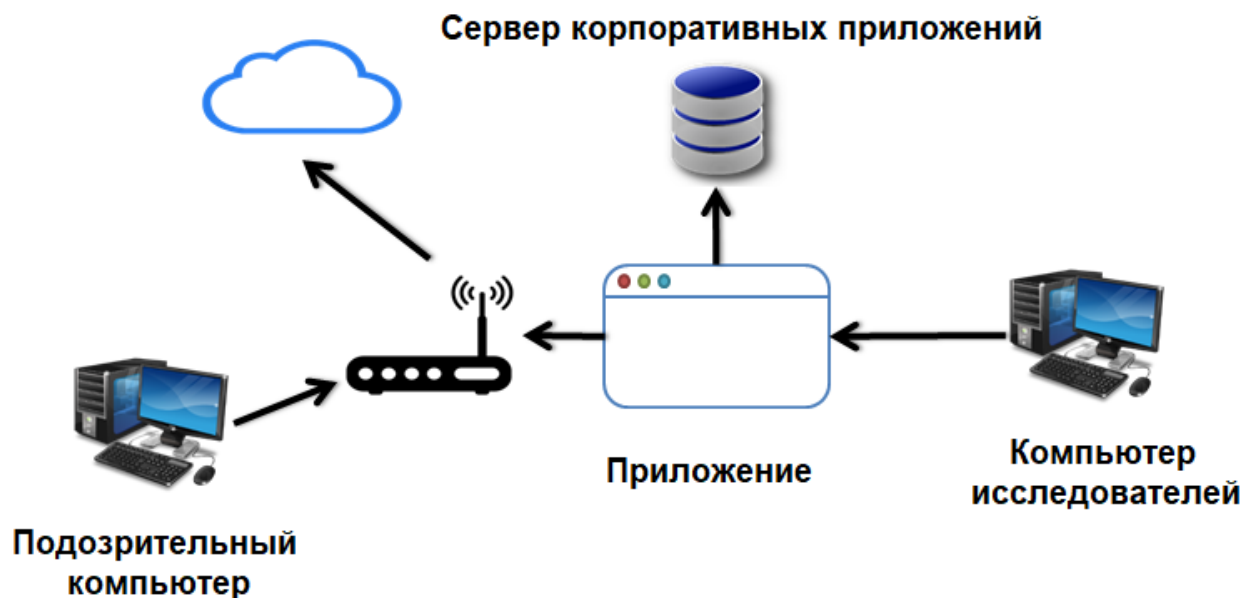


Рисунок 2.5 – Общая схема системы

### 3 РАЗРАБОТКА АРХИТЕКТУРЫ, ИНТЕРФЕЙСА СИСТЕМЫ

Вариант использования состоит из типичного взаимодействия между действующим лицом и приложением. Вариант использования определяется, прежде всего, своим именем и типом пользователя приложения, называемого действующим лицом [18].

Представления основной взаимоотношения между пользователем и системой см. рисунок 3.1:



Рисунок 3.1 – Диаграмма вариантов использования системы

1) подключение к системе, каждый пользователь должен подключиться к системе, используя логин и пароль, система проверяет информацию пользователя в базе данных, и если пароль и логин подходят, то входит в Главное окно и определяет тип пользователя;

2) для пользователя-исследователя, в главном окне системы отображаются инциденты, назначенные пользователю «исследователь», последний раз когда был в системе, и в каждом случае отображается, если сотрудник, участвующий в этом инциденте, находится в сети;

3) для пользователя-координатора, в главном окне системы пользователю-координатору отображаются все инциденты, которые активны в системе. В каждом случае отображается, если сотрудник, участвующий в этом инциденте, находится в сети. Также последний раз когда был в системе и в меню координатора, имеет возможность добавить новый инцидент или изменить существующий инцидент;

4) для пользователя- администратора, в главном окне системы отображаются все пользователи системы, последний раз когда был в системе, и в меню администратор имеет возможность добавить нового пользователя или изменить существующего пользователя;

5) открыть инцидент, когда пользователь находится в главном окне системы, он имеет возможность открыть инцидент, который хочет исследовать. Для этого пользователь выбирает имя сотрудника, которого хочет исследовать, и нажимает кнопку «ABRIR»;

б) показать трафик, когда пользователь выбирает инцидент и открывает его, открывается всплывающее окно, в котором отображается трафик подозрительного сотрудника и активность, которую сотрудник имел за последние 5 дней;

7) экспорт отчета, когда пользователь находится на экране системы, где отображается трафик выбранного подозрительного сотрудника, у него есть возможность экспортировать в pdf трафик, показанный на экране, это происходит, когда пользователь нажимает значок, который находится на экране или в меню;

8) показать отчет, при выборе опции экспорта, отчет отображается во всплывающем окне для проверки пользователя;

9) создать инцидент, только пользователь-координатор может выполнить опцию добавления нового инцидента, это происходит, когда пользователь находится на главном экране системы и нажимает кнопку Добавить инцидент или в меню опций;

10) изменить инцидент, пользователь-координатор имеет возможность изменить существующий инцидент, где может изменить тип инцидента, расследование или сотрудник;

11) загрузить случай, при создании или изменении инциденты должны быть загружены в базу данных, этот процесс выполняется путем подключения к базе данных;

12) создать пользователя, пользователь (администратор): в главном окне системы отображаются все пользователи системы, последнее раз когда был в системе, и в меню администратор имеет возможность добавить нового пользователя или изменить существующего пользователя. Администратор может добавить нового пользователя, нажав кнопку нового пользователя или в меню;

13) изменить пользователя, администратор имеет возможность изменить существующего пользователя, это происходит, когда администратор выбирает пользователя и нажимает кнопку «EDITAR»;

14) загрузить пользователя, при создании или изменении пользователя информация должна быть загружена в базу данных, этот процесс выполняется путем подключения к базе данных;

### 3.1 Проектирование базы данных

При разработке базы данных существуют принципы, которые определяют процесс создания базы данных. Первый принцип – это избежать дублирования информации или избыточных данных. Второй принцип – данные должны быть точными и интегрированными, если база данных

содержит неправильные данные, извлеченная информация приведет к ошибочным отчетам. Для хорошего проектирования базы данных:

- 1) необходимо определить цель базы данных;
- 2) необходимо найти и организовать необходимую информацию, определить типы используемой информации;
- 3) информация должна быть разделена на таблицы;
- 4) необходимо указать первичные ключи и настроить связи между таблицами с дочерними ключами.

Для разработки базы данных создается схема базы данных, в которой отображаются логика таблиц, взаимосвязи между ними и типы данных, включенные в каждую таблицу. Этот диаграмма показана на рисунке 3.2.

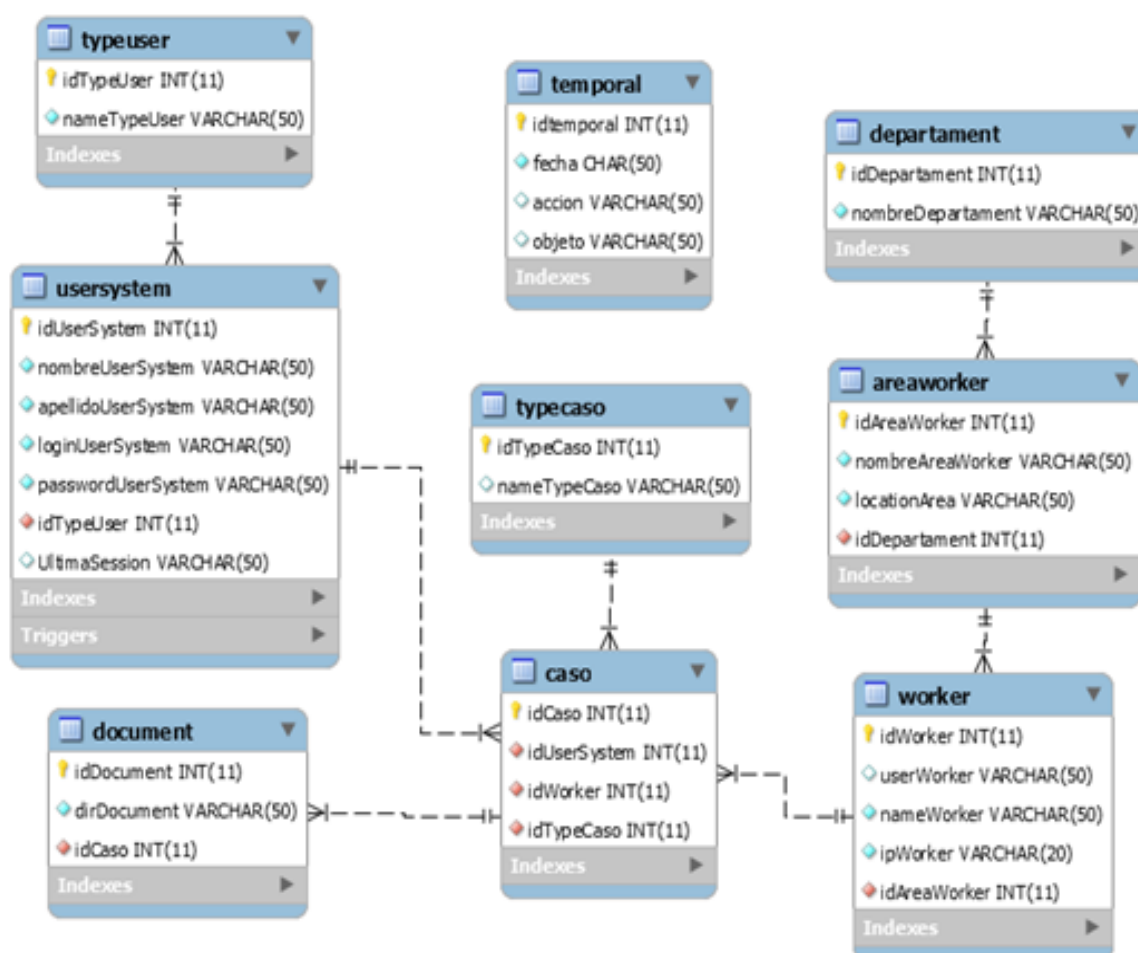


Рисунок 3.2 – Диаграмма базы данных

Таблицы определены следующим образом:

Таблица 3.1 – Информация о таблице «Caso»

| Имя          | Тип           | Размер | Комментарий                          |
|--------------|---------------|--------|--------------------------------------|
| idCaso       | целочисленный | 11     | первичный ключ                       |
| idUserSystem | целочисленный | 11     | вторичный ключ с таблицей UserSystem |
| idWorker     | целочисленный | 11     | вторичный ключ с таблицей worker     |
| idTypeCaso   | целочисленный | 11     | вторичный ключ с таблицей TypeCaso   |

Таблица 3.2 – Информация о таблице «TypeCaso»

| Имя          | Тип           | Размер | Комментарий        |
|--------------|---------------|--------|--------------------|
| idTypeCaso   | целочисленный | 11     | первичный ключ     |
| nameTypeCaso | строка        | 50     | имя типа обращения |

Таблица 3.3 – Информация о таблице «Document»

| Имя         | Тип           | Размер | Комментарий                    |
|-------------|---------------|--------|--------------------------------|
| idDocument  | целочисленный | 11     | первичный ключ                 |
| dirDocument | строка        | 50     | адрес расположения документа   |
| idCaso      | целочисленный | 11     | вторичный ключ с таблицей Caso |

Таблица 3.4 – Информация о таблице «Worker»

| Имя          | Тип           | Размер | Комментарий                          |
|--------------|---------------|--------|--------------------------------------|
| idWorker     | целочисленный | 11     | первичный ключ                       |
| userWorker   | строка        | 50     | Логин сотрудника                     |
| nameWorker   | строка        | 50     | Имя сотрудника                       |
| ipWorker     | строка        | 50     | ip-адрес сотрудника                  |
| idAreaWorker | целочисленный | 11     | вторичный ключ с таблицей AreaWorker |

Таблица 3.5 – Информация о таблице «AreaWorker»

| Имя              | Тип           | Размер | Комментарий                            |
|------------------|---------------|--------|----------------------------------------|
| idAreaWorker     | целочисленный | 11     | первичный ключ                         |
| nombreAreaWorker | строка        | 50     | Название области                       |
| locationArea     | строка        | 50     | Физический адрес области               |
| idDepartament    | целочисленный | 11     | вторичный ключ с таблицей Departament. |

Таблица 3.6 – Информация о таблице «Departament»

| Имя               | Тип           | Размер | Комментарий     |
|-------------------|---------------|--------|-----------------|
| idDepartament     | целочисленный | 11     | первичный ключ  |
| nombreDepartament | строка        | 50     | название отдела |

Таблица 3.7 – Информация о таблице «UserSystem»

| Имя                | Тип           | Размер | Комментарий                                 |
|--------------------|---------------|--------|---------------------------------------------|
| idUserSystem       | целочисленный | 11     | первичный ключ                              |
| nombreUserSystem   | строка        | 50     | имя пользователя                            |
| apellidoUserSystem | строка        | 50     | фамилия пользователя                        |
| loginUserSystem    | строка        | 50     | пользователь                                |
| passwordUserSystem | строка        | 50     | Пароль пользователя                         |
| idTypeUser         | целочисленный | 11     | вторичный ключ с таблицей TypeUser          |
| UltimaSession      | строка        | 50     | последняя сессия, проведенная пользователем |

Таблица 3.8 – Информация о таблице «TypeUser»

| Имя          | Тип           | Размер | Комментарий           |
|--------------|---------------|--------|-----------------------|
| idTypeUser   | целочисленный | 11     | первичный ключ        |
| nameTypeUser | строка        | 50     | имя типа пользователя |



Таблица 3.9 – информация о таблице «Temporal»

| Имя        | Тип           | Размер | Комментарий                                    |
|------------|---------------|--------|------------------------------------------------|
| idTemporal | целочисленный | 11     | первичный ключ                                 |
| Fecha      | строка        | 50     | дата выполнения действия                       |
| Acción     | строка        | 50     | действие, выполняемое над таблицей базы данных |
| objeto     | строка        | 50     | объект, который был изменен                    |

### 3.2 Окно подключения к приложению

Чтобы войти в систему, пользователь должен ввести свои данные в окне ввода см. рисунок 3.3.

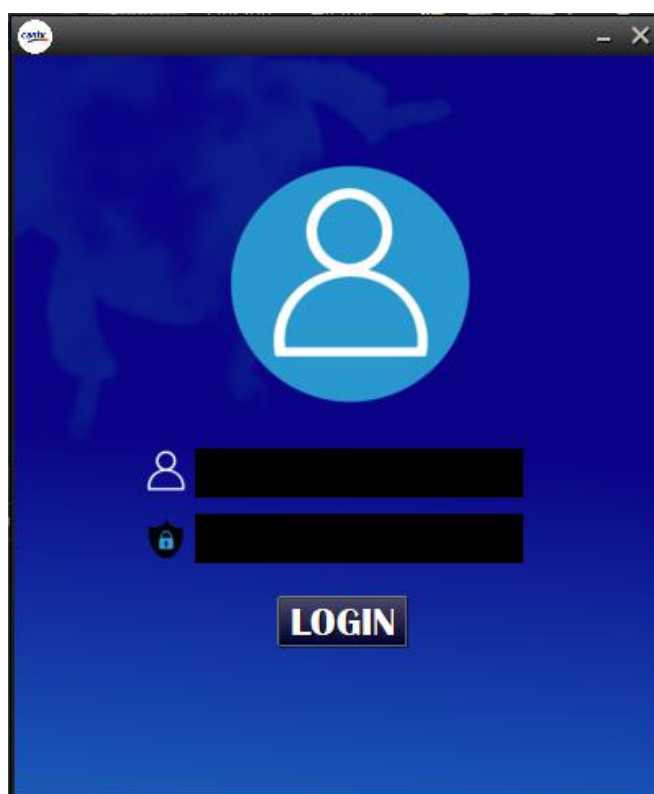


Рисунок 3.3 – Интерфейс окно подключения к приложению

Подключение пользователя осуществляется через этот экран, подключаясь к базе данных, разработанной в Mysql, есть два текстового поля первый для имени пользователя и второй для пароля.

### 3.3 Главное окно приложения пользователя-исследователя

Основные элементы главного окна (см. рисунок 3.4):

1) Панель мониторинга, где отображается таблица с данными подозрительных сотрудников, которые были назначены пользователю-следователю:

- online: Колонка, показывающая, если сотрудник находится в сети;
- idCaso: Код инцидента;
- user: Логин сотрудника;
- nombre: Имя сотрудника;
- IP: IP-адрес сотрудника;
- locacion: Физическое расположение сотрудника;
- tipo Caso: Тип инцидента;

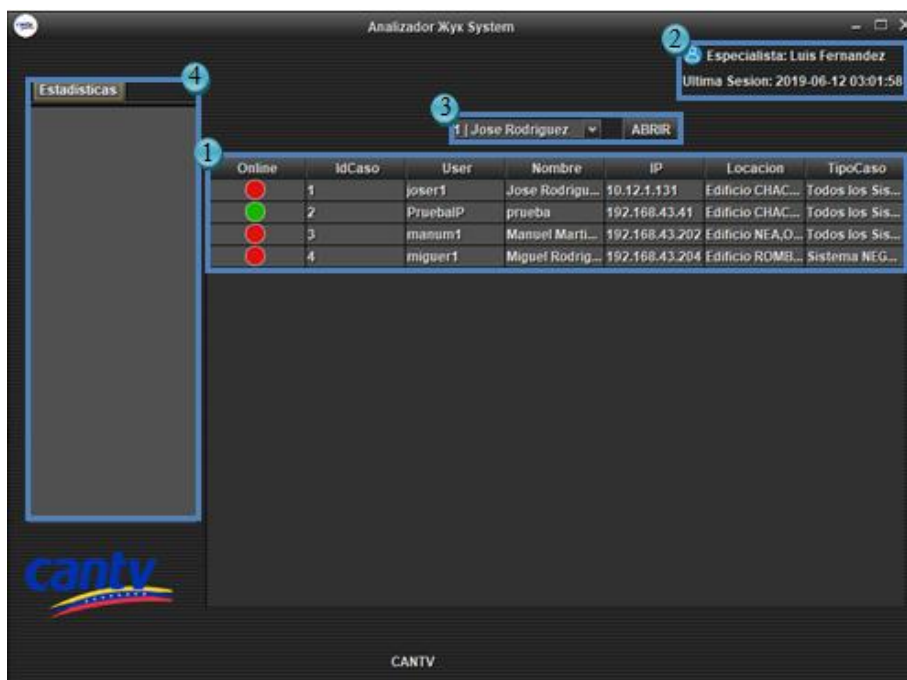


Рисунок 3.4 – Интерфейс главного окна приложения пользователя-исследователя

2) панель, в которой пользователю отображаются его данные (тип пользователя и имя) и последний раз, когда вошел в систему;

3) панель, где пользователь может выбрать сотрудника, который хочет исследовать и открыть инцидент для анализа трафика с помощью кнопки «ABRIR»;

4) панель, на которой отображается статистика, связанная с инцидентами.

### 3.4 Главное окно приложения пользователя-координатора

Рассмотрим главное окно приложения пользователя-координатора см. рисунок 3.5:

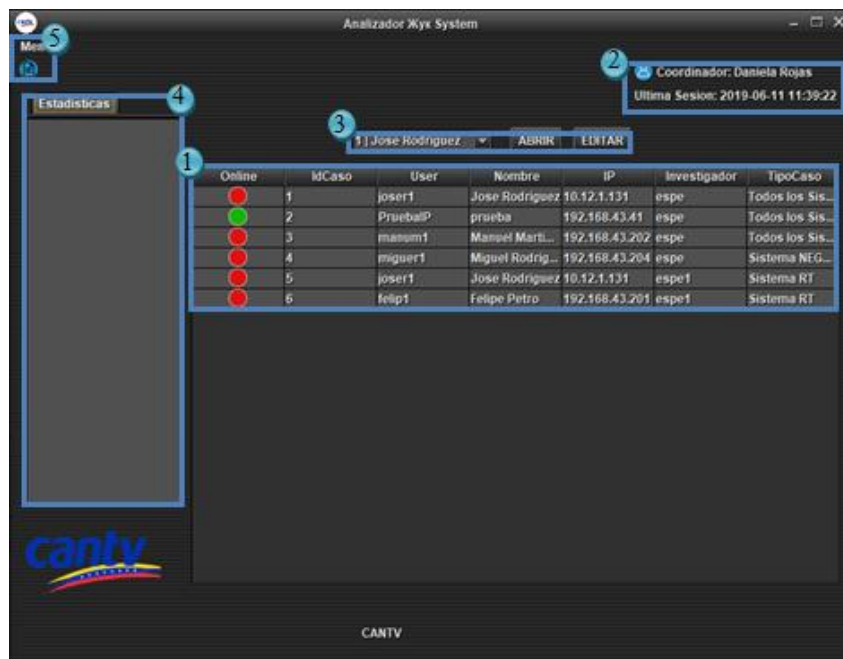


Рисунок 3.5 – Интерфейс главного окна приложения пользователя-координатора

1) панель мониторинга, которая отображает таблицу с данными все инциденты отдела:

- online: Колонка, показывающая, если сотрудника находится в сети;
- idCaso: Код инцидента;
- user: Логин сотрудника;
- nombre: Имя сотрудника;

- IP: IP-адрес сотрудника;
- locacion: Физическое расположение сотрудника;
- tipo Caso: Тип инцидента;

2) панель, в которой пользователю отображаются его данные (тип пользователя и имя) и последний раз, когда вошел в систему;

3) панель, где пользователь может выбрать сотрудника, который хочет исследовать и открыть инцидент для анализа трафика с помощью кнопки «ABRIR». Имеет возможность изменить выбранный инцидент с помощью кнопки «EDITAR»;

4) панель, на которой отображается статистика, связанная с инцидентами;

5) панель, где находится кнопка, ответственная за открытие нового инцидент.

### 3.5 Главное окно приложения пользователя-администратора

Рассмотрим главное окно приложения пользователя- администратора см. рисунок 3.6:

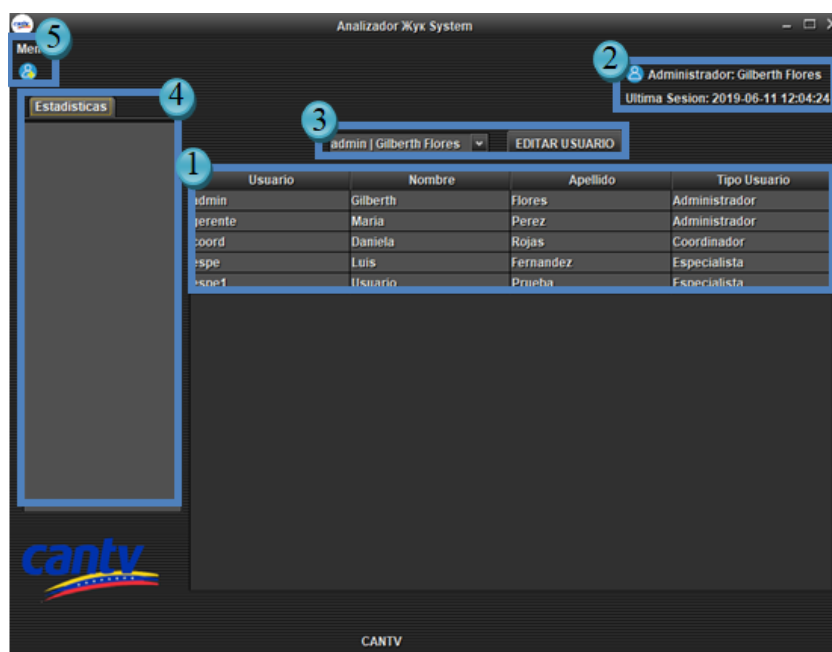


Рисунок 3.6 – Интерфейс главного окна приложения пользователя-администратора

1) панель мониторинга, которая отображает таблицу с данными все пользователи приложения;

– usuario: Пользователь приложения;

– nombre: Имя пользователя;

– apellido: Фамилия пользователя;

– tipo de usuario: Тип пользователя;

2) панель, в которой пользователю отображаются его данные (тип пользователя и имя) и последний раз, когда вошел в систему;

3) панель, где пользователь может выбрать пользователь, который хочет поменять с помощью кнопки «EDITAR USUARIO»;

4) панель, на которой отображается статистика, связанная с инцидентами;

5) панель, где находится кнопка, ответственная за открытие нового инцидент.

### 3.6 Окно добавления нового инцидента

Рассмотрим главное окно приложения нового инцидента см. рисунок

3.7:




Рисунок 3.7 – Интерфейс окна добавления инцидента

1) комбинированный список, на котором отображаются пользователи-специалисты, для назначения инцидента;

2) комбинированный список, на котором отображаются сотрудники компании;

3) при выборе сотрудника немедленно отображаются следующие данные этого сотрудника:

- логин сотрудника;
- IP-адрес сотрудника;
- физическое расположение сотрудника;
- отдел, где работает сотрудник;

4) комбинированный список, в которой выбирается тип инцидента.

### 3.7 Окно редактирования инцидента

Рассмотрим главное окно приложения для редактирования инцидента см. рисунок 3.8:



Рисунок 3.8 – Интерфейс окна редактирования инцидента

1) комбинированный список, на котором отображаются пользователи-специалисты, для назначения инцидента;

2) комбинированный список, на котором отображаются сотрудники компании;

3) при выборе сотрудника немедленно отображаются данные этого сотрудника;

- логин сотрудника;
- IP-адрес сотрудника;
- физическое расположение сотрудника;
- отдел, где работает сотрудник;

4) комбинированный список, в котором выбирается тип инцидента.

### 3.8 Окно добавления пользователя

Рассмотрим главное окно приложения для добавления пользователя см. рисунок 3.9:



Рисунок 3.9 – Интерфейс окна добавления пользователя

- 1) текстовое поле для ввода имени пользователя;
- 2) текстовое поле для ввода имени исследователя;
- 3) текстовое поле для ввода фамилии исследователя;
- 4) комбинированный список, на котором выбирается тип пользователя.

### 3.9 Окно редактирования пользователя

Рассмотрим главное окно приложения для редактирования пользователя см. рисунок 3.10:

The screenshot shows a window titled 'Editar' with a dark background. At the top left is a small logo. Below the title bar, there is a blue header with a user icon and the word 'Editar'. The main area contains five input fields, each with a blue circle containing a number (1-5) next to it. The fields are: 'ID USUARIO:' with the value '1'; 'USUARIO:' with the value 'admin'; 'NOMBRE:' with the value 'Gilberth'; 'APELLIDO:' with the value 'Flores'; and 'TIPO DE USUARIO:' with a dropdown menu showing 'Administrador'. At the bottom of the form is a button labeled 'MODIFICAR'.

Рисунок 3.10 – Интерфейс окно редактирования пользователя

- 1) текстовое поле для отображения идентификатора пользователя;
- 2) текстовое поле для ввода имени пользователя;
- 3) текстовое поле для ввода имени исследователя;
- 4) текстовое поле для ввода фамилии исследователя;
- 5) комбинированный список, на котором выбирается тип пользователя.



### 3.10 Окно анализа трафика сотрудника

Рассмотрим главное окно приложения для анализа трафика сотрудника см. рисунок 3.11:

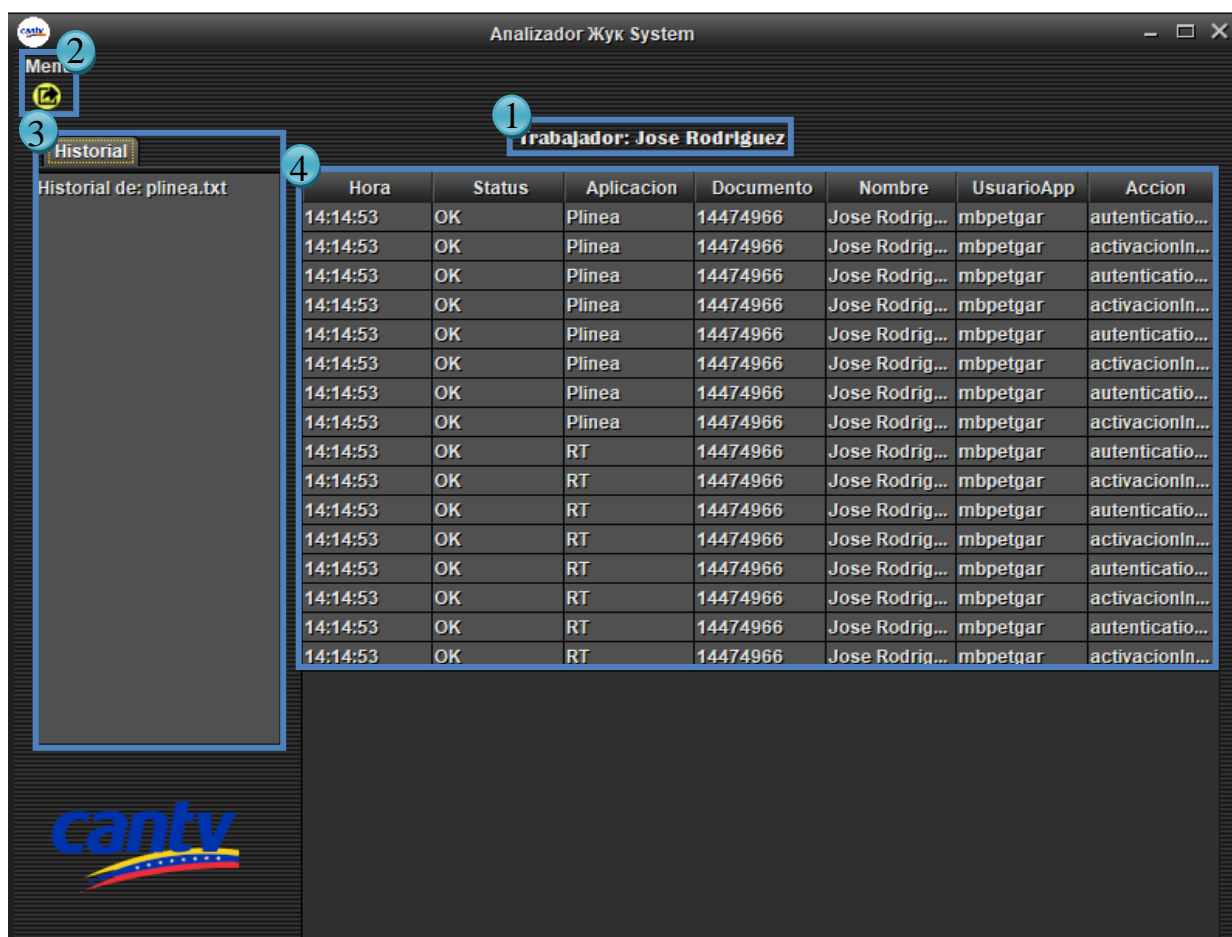


Рисунок 3.11 – Интерфейс окно анализа трафика пользователя

- 1) панель, на которой отображается имя сотрудника;
- 2) панель, где находится кнопка действия экспорт отчета;
- 3) панель, на которой отображается статистика, связанная с инцидентами;

4) панель мониторинга, где отображается таблица с данными трафика сотрудников в сети:

- hora: время действия выполнено;
- status: состояние действия;
- aplicacion: приложение, в котором сотрудник выполняет действие;
- documento: национальный документ сотрудника;

- nombre: имя сотрудника;
- usuarioapp: логин сотрудника в приложении компании;
- acción: действие осуществляется в применении компании.

### 3.11 Окно экспорта в PDF

Рассмотрим главное окно приложения для экспорта в PDF см. рисунок 3.12.

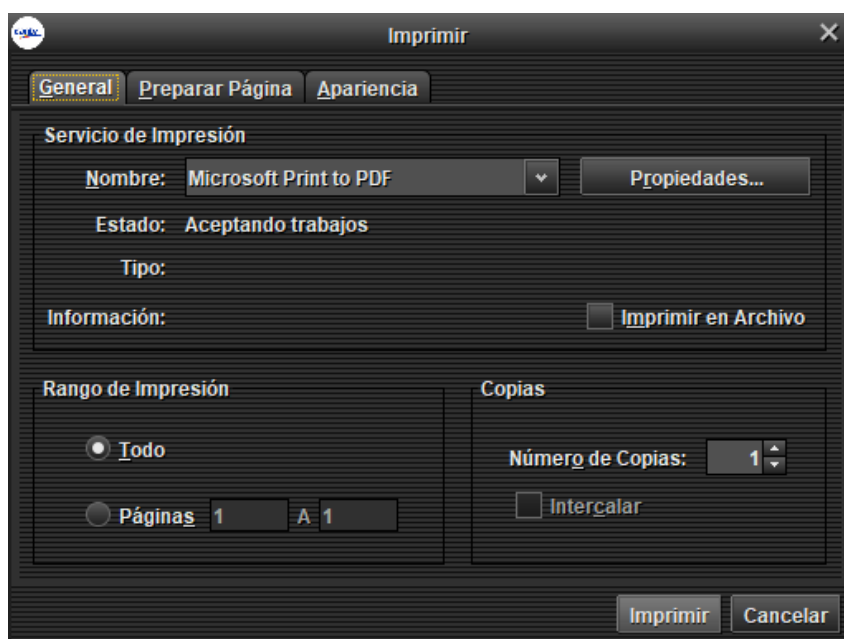


Рисунок 3.12 – Окно экспорта в PDF

3.12 Эффективность подключения к серверу корпоративных приложений с библиотекой FTPClient

Для проверки эффективности подключения к серверу коорпоративных приложений была установлена виртуальная машина с Ubuntu server 18, на которой были настроены службы FTP и другие основные службы.

После создания среды выполнения приложения тест соединения выполняется с помощью приложения java с библиотекой FTPClient путем достижения подключения к папке, предназначенной для пользователя, созданного для подключения приложения под названием «app», этот

пользователь имеет доступ только к каталогу /aplicaciones, в которых находятся файлы, имитирующие журналы корпоративных приложений.

Из приложения журналы загружаются с сервера с помощью FileOutputStream. Это действие автоматически каждые 10 секунд сохраняет на сервере приложения файлы журналов с информацией о действиях сотрудника.

При выборе подозреваемого для расследования проверяются сохраненные файлы журналов и отображаются действия подозреваемого.

### 3.13 Эффективность захвата трафика с помощью библиотекой Jrcap

Для этого процесса необходимо установить вторую виртуальную машину с Ubuntu server 18, которая имитировала бы SMTP - сервер компании CANTV, так как все сотрудники компании, чтобы использовать свои компьютеры, должны войти со своей корреспонденцией, которая немедленно подключается к SMTP-серверу.

С помощью библиотеки Jrcap разрабатывается второе приложение, которое находится на SMTP-сервере и работает каждую минуту с помощью crontab, это приложение анализирует трафик сервера с фильтром подозрительных сотрудников.

Затем из приложения анализа и с помощью библиотеки FTPClient загружается трафик с сервера.

### 3.14 Эффективность применения анализа времени по сравнению с анализа в реальном времени

После тестирования соединения с приложением и имитации с помощью FileZilla вариантов действий на сервере корпоративного приложения были получены графики трафика в режиме реального времени см. рисунок 3.13.

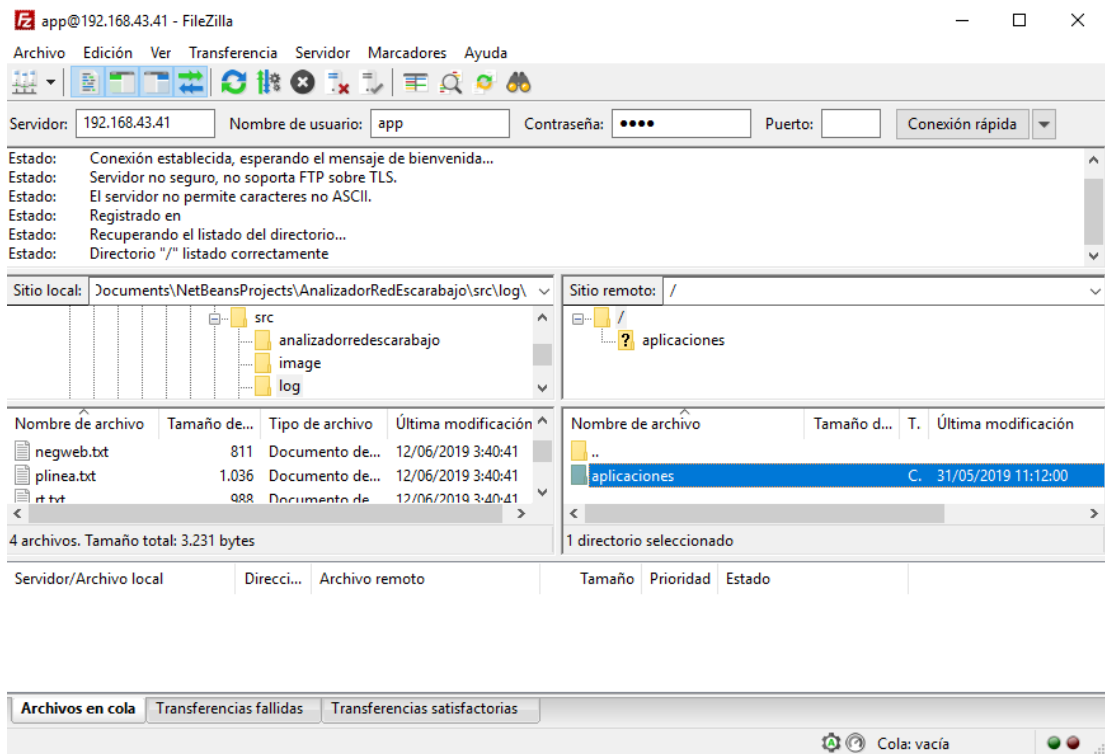


Рисунок 3.13 – Окно приложения FileZilla

## ЗАКЛЮЧЕНИЕ

В данной работе для обеспечения защищенности системы было разработано приложение для расследования инцидентов режиме реального времени во внутренней сети организации.

Исследована информация, связанная с компьютерной криминалистикой, ее текущими методами, процедурами и инструментами для анализа полученных доказательств.

В частности, была исследована информация о расследованиях в режиме реального времени, ориентированная на анализ внутреннего сетевого трафика компании, поскольку исследовательская работа сосредоточена на анализе сетевого трафика подозреваемых сотрудников в компании CANTV.

Были проанализированы требования приложения, разработанного на JAVA для подключения к внутренней сети и получения трафика сети подозреваемых, рассмотрены существующие решения для работы с библиотеками, предлагаемыми Java, такими как Jrcar и FTPClient, описаны его достоинства и недостатки.

Разработана архитектура и интерфейс системы, представлены схемы основных алгоритмов, обеспечивающих правильную работу системы. Для тестирования и отладки были разработаны тесты с фиктивными данными.

В результате было разработано программное обеспечение для анализа трафика подозреваемых сотрудников, выполняемого исследователями отдела компьютерной криминалистики компании CANTV.

Были смоделированы данные сотрудников и среды, имитирующей внутреннюю сеть компании CANTV для проведения тестирования приложения.

Данная система универсальна и может быть интегрирована и адаптирована в разные компании по всему миру.

## БИБЛИОГРАФИЧЕСКИЙ СПИСОК

1 Что такое кибербезопасность? / Касперский латиноамерика. – Дата обновления: 05.04.2019. URL: <https://latam.kaspersky.com/resource-center/definitions/what-is-cyber-security> (дата обращения: 25.09.2018).

2 Prosecuting Computer Crimes/ Н. М. Jarrett и М. W. Bailie. United states – Дата обновления: 14.01.2015 URL: <https://www.justice.gov/sites/default/files> (дата обращения: 27.09.2018).

3 Ley especial contra los delitos informáticos / Gaceta Oficial. Venezuela – Дата обновления: 31.10.2001 URL: <https://www.wipo.int/edocs/lexdocs/laws/es/ve/ve041es.pdf> (дата обращения: 28.09.2018).

4 Cenif: Primer y único laboratorio de Informática Forense de Venezuela / Centro nacional de tecnologías de información. Venezuela – Дата обновления: 08.08.2014 URL: <https://www.cnti.gob.ve/noticias/actualidad/nacionales/3969-2014-08-08-23-47-07.html> (дата обращения: 28.09.2018).

5 Руководство по EnCase. – Дата обновления: 26.03.2018 URL: <https://www.guidancesoftware.com/encase-forensic> (дата обращения: 28.09.2018).

6 Digital forensic analysis methodology / Departament of justice. United states – Дата обновления: 26.03.2015 URL: [https://www.justice.gov/sites/default/files/criminalccips/legacy/2015/03/26/forensics\\_chart.pdf](https://www.justice.gov/sites/default/files/criminalccips/legacy/2015/03/26/forensics_chart.pdf) (дата обращения: 30.09.2018).

7 Metodología de análisis forense orientada a incidentes en dispositivos Móviles / Diego Pinto. – Ecuador: Universidad de las fuerzas armadas – Дата обновления: 17.10.2014 URL: <https://publicaciones.ucuenca.edu.ec/ojs/index.php/maskana/article/download/721/641/> (дата обращения: 01.10.2018).

8 Systematic Digital Forensic Investigation Model. Gupta International Journal of Computer Science and Security / Agarwal, Ankit, Megha. India – Дата обновления: 01.01.2011 URL: [https://www.researchgate.net/publication/228410430\\_Systematic\\_Digital\\_Forensic\\_Investigation\\_Model](https://www.researchgate.net/publication/228410430_Systematic_Digital_Forensic_Investigation_Model) (дата обращения: 02.10.2018).

9 T. Manesh. Network Forensic Investigation of HTTPS Protocol / Доклад Инженерно- Shankara Centre for Research in Information Science. India 2013. URL: [https://www.researchgate.net/publication/273297472\\_Network\\_Forensic\\_Investigation\\_of\\_HTTPS\\_Protocol](https://www.researchgate.net/publication/273297472_Network_Forensic_Investigation_of_HTTPS_Protocol) (дата обращения: 03.10.2018).

10 K. Ahmed, M. Kisangiri. A Step on Developing Network Monitoring Tools / Доклад IISTE. Tanzania 2014 URL: [https://www.researchgate.net/publication/283210566\\_A\\_Step\\_on\\_Developing\\_Network\\_Monitoring\\_Tools](https://www.researchgate.net/publication/283210566_A_Step_on_Developing_Network_Monitoring_Tools) (дата обращения: 04.10.2018).

11 Руководство по Java. – Дата обновления: 27.01.2010 URL: <https://www.java.com/ru/> (дата обращения: 05.10.2018).

12 Руководство по Netbeans. – Дата обновления: 23.09.2016 URL: <https://netbeans.org/community/releases/> (дата обращения: 05.10.2018).

13 Руководство по WinPcap. – Дата обновления: 02.07.2010 URL: <https://www.winpcap.org/> (дата обращения: 05.10.2018).

14 Руководство по TCPDump. – Дата обновления: 03.09.2017 URL: <https://www.tcpdump.org/#documentation> (дата обращения: 05.10.2018).

15 Руководство по Jpcap. URL: <http://jpcap.sourceforge.net/javadoc/help-doc.html> (дата обращения: 05.10.2018).

16 Руководство по FTPClient. URL: <https://commons.apache.org/proper/commons-net/apidocs/org/apache/commons/net/ftp/FTPClient.html> (дата обращения: 05.10.2018).

17 Руководство по Mysql. URL: <https://dev.mysql.com/doc/FTPClient.html> (дата обращения: 09.10.2018).

18 Э. Брауде. Технология разработки программного обеспечения [Электронный ресурс]: учебное пособие / Э. Брауде. – Москва, 2004. 659 с. URL: [http://www.immsp.kiev.ua/postgraduate/Biblioteka\\_trudy/Tekhnologiya\\_RazrabProgrBraude2004.pdf](http://www.immsp.kiev.ua/postgraduate/Biblioteka_trudy/Tekhnologiya_RazrabProgrBraude2004.pdf) (дата обращения: 09.10.2018).

19 Ajoy Ghosh. Guidelines for the Management of IT Evidence / Доклад АРЕС Telecommunications and Information Working Group. China. 2004. URL:

<http://unpan1.un.org/intradoc/groups/public/documents/APCITY/UNPAN016411.pdf> (дата обращения: 01.11.2018).

20 Udo Payer. Realtime Intrusion-Forensics, A First Prototype Implementation(based on a stack-based NIDS) / Доклад University of Technology. Austria. 2004 URL: <https://www.terena.org/publications/tnc2004-proceedings/papers/payer.pdf> (дата обращения: 05.11.2018).

21 Q. Nasir. Honeypots Aiding Network Forensics: Challenges and Notions / Доклад University of Sharjah. United Arab Emirates. 2013 URL: <https://pdfs.semanticscholar.org/c480/6c1f45c8f81b5dea3c9e60e6a4039abb64ed.pdf> (дата обращения: 06.11.2018).

22 M. Tariq. Techniques and tools for forensic investigation of e-mail / Доклад University of Kashmir. India 2011 URL: <https://pdfs.semanticscholar.org/8625/a3b17d199e5cabbb796bad0df56a7979c77c.pdf> (дата обращения: 07.11.2018).



## ПРИЛОЖЕНИЕ 1

Текст программы