Министерство образования и науки Российской Федерации

ФЕДЕРАЛЬНОЕ ГОСУДАРСТВЕННОЕ БЮДЖЕТНОЕ ОБРАЗОВАТЕЛЬНОЕ УЧРЕЖДЕНИЕ ВЫСШЕГО ОБРАЗОВАНИЯ «САРАТОВСКИЙ НАЦИОНАЛЬНЫЙ ИССЛЕДОВАТЕЛЬСКИЙ ГОСУДАРСТВЕННЫЙ УНИВЕРСИТЕТ ИМЕНИ Н.Г. ЧЕРНЫШЕВСКОГО»

Кафедра теоретических основ компьютерной безопасности и криптографии

Установление обстоятельств работы пользователей операционной системы Windows в сети Интернет

АВТОРЕФЕРАТ

дипломной работы

студента 6 курса 631 группы

специальности 10.05.01 Компьютерная безопасность

факультета компьютерных наук и информационных технологий

Светлова Ильдара Михайловича

Научный руководитель

доцент, к.юр.н. _____ А.В. Гортинский

31.12.2016 г.

Заведующий кафедрой

профессор, к.ф.-м.н. _____ В.Н. Салий

31.12.2016 г.

Саратов 2017

ВВЕДЕНИЕ

В современном мире очень актуальна проблема компьютерной безопасности. Благодаря широкому распространению различных электронных устройств и носителей информации сфера компьютерных технологий становится все более и более популярной. Многим современным людям уже сложно представить себе жизнь без Интернета, мобильного телефона или компьютера. Общение между людьми все больше и больше уходит в Глобальную сеть.

Как и в любой другой сфере, в сфере информационных технологий наравне с открытиями и изобретениями, направленными на улучшение и упрощение жизни людей, происходит множество событий, связанных с причинением вреда и нанесением урона отдельным гражданам, группам людей или даже целым государствам.

Рост числа пользователей компьютерных технологий порождает рост числа преступников в данной сфере, которые своими противоправными действиями всяческими способами пытаются получить выгоду, нанося материальный урон и моральный вред законопослушным гражданам.

Правоохранительные органы имеют на вооружении самые разнообразные средства и методы борьбы с преступлениями в сфере компьютерных технологий, которые позволяют им оперативно расследовать их и находить преступников.

Так как многие преступления совершаются с использованием сетевых технологий с устройств, находящихся на огромных расстояниях от объектов противоправных действий, то важную роль в расследовании таких преступлений играет умение точно определять все обстоятельства совершенных преступлений. Если в руках правоохранителей оказывается устройство, с которого возможно было совершено противоправное действие, их задача провести полное исследование данного устройства и извлечь из него

как можно больше различной информации, чтобы появилась возможность сделать правильные выводы о причастности или непричастности субъекта к преступлению.

На рынке программ для проведения компьютерных экспертиз и анализа сетевой активности существует множество разнообразных продуктов как отечественного («Forensic Assistant»), так и иностранного производства («Belkasoft Evidence Center», «Web Historian», «ChromeAnalysis», «FoxAnalysis»). Большинство из них являются платными, причем цены на них достаточно высоки для простых пользователей персональных компьютеров. Но даже у рядовых пользователей иногда возникает необходимость воспользоваться программами данной направленности.

Целью данной дипломной работы является изучение процесса следообразования и на основании его установления обстоятельств использования пользователем ПК с операционной системой Windows сетевых ресурсов и работы пользователя в сети Интернет, а также разработка программного обеспечения для сбора и агрегирования полученной информации о сетевом взаимодействии. В работе будут рассмотрены некоторые приложения и сервисы, которые являются носителями сведений о взаимодействии пользователя с ресурсами сети Интернет и использовании определенных интерфейсов операционной системы.

Дипломная работа состоит из введения, 7 разделов, заключения, списка использованных источников и 2 приложений. Общий объем работы – 62 страницы, из них 33 страницы – основное содержание, включая 8 рисунков, список использованных источников из 16 наименований.

КРАТКОЕ СОДЕРЖАНИЕ

Во введении формулируются цели дипломной работы: изучение способов установления обстоятельств использования пользователем ПК с операционной системой Windows сетевых ресурсов и работы пользователя в сети Интернет, а также разработка программного обеспечения для сбора и агрегирования полученной информации о сетевом взаимодействии.

В разделе 1 «Общая информация об исследуемых источниках сведений» представлены общие сведения об исследуемых источниках информации о сетевом взаимодействии. Приведено краткое описание конкретных данных, которые могут быть обнаружены в этих источниках.

Раздел 2 «Журнал событий Windows» посвящен журналу событий Windows Event Log. В начале раздела приведено описание данного журнала Windows, указаны пути до директорий, в которых располагаются его файлы. Далее в шести подразделах раздела 2 описаны службы и сервисы операционной системы Windows, которые прямо или косвенно принимают участие в процессе взаимодействия пользователя с сетью. Записи о работе этих служб в Windows Event Log представляют интерес для данного исследования.

Раздел 3 «Следы использования браузеров» посвящен следообразованию в браузерах. В начале раздела приведено общее описание программ-браузеров, описаны их функции, дана общая информация об исследуемых браузерах.

В подразделе 3.1 «Кэш браузеров» раздела 3 дано понятие кэша браузеров, приведены функции кэша и механизм работы.

Подраздел 3.2 «Следы использования Google Chrome» раздела 3 посвящен следообразованию в браузере Google Chrome. В данном подразделе приведены краткие сведения об этом браузере, описаны пользовательские директории данной программы в операционных системах семейства Windows. Также в этом подразделе описаны базы данных пользовательских директорий

браузера Google Chrome, представляющие интерес для исследования, представлена их структура и местоположение.

Подраздел 3.3 «Следы использования Mozilla Firefox» раздела 3 посвящен следообразованию в браузере Mozilla Firefox. В данном подразделе приведены краткие сведения об этом браузере, описаны пользовательские директории данной программы в операционных системах семейства Windows. Также в этом подразделе описаны базы данных пользовательских директорий браузера Mozilla Firefox, представляющие интерес для исследования, представлена их структура и местоположение.

Подраздел 3.4 «Следы использования Opera» раздела 3 посвящен следообразованию в браузере Opera. В данном подразделе приведены краткие сведения об этом браузере, описаны пользовательские директории данной программы в операционных системах семейства Windows. Также в этом подразделе описаны базы данных пользовательских директорий браузера Opera, представляющие интерес для исследования, представлена их структура и местоположение.

В разделе 4 «Следы использования Skype» описана программа для обеспечения текстовой, голосовой и видеосвязи Skype. Сформулированы основные ее преимущества и недостатки, рассмотрена структура пользовательской директории данной программы. Описана важная особенность данного приложения, которая заключается в том, что содержимое основной пользовательской базы данных Skype представлено в открытом незашифрованном виде и не удаляется после выхода пользователя из учетной записи Skype на компьютере (настройка по умолчанию). По этой причине вне зависимости от того, выполнен ли вход в учетную запись пользователя, имеется возможность просмотреть сведения о его переписках и звонках.

В следующих трех подразделах раздела 4 приводится информация о местоположении и структуре таблиц основной базы данных Skype, которые представляют интерес для данного исследования. Это таблицы, содержащие

сведения о переписках пользователя, голосовых и видео звонках и пользователях из списка контактов.

В разделе 5 «Следы использования Viber» описана программа для обеспечения текстовой, голосовой и видеосвязи Viber. Сформулированы основные ее преимущества и недостатки, рассмотрена структура пользовательской директории данной программы.

В следующих трех подразделах раздела 5 приводится информация о местоположении и структуре таблиц основной базы данных Viber, которые представляют интерес для данного исследования. Это таблицы, содержащие сведения о переписках пользователя, голосовых и видео звонках и пользователях из списка контактов.

В разделе 6 «Сбор и агрегирование информации о сетевом взаимодействии» описана идея сбора сведений о сетевом взаимодействии из вышеописанных источников.

В подразделе 6.1 «Выборка событий из Windows Event Log» раздела 6 описан механизм выборки событий из журнала событий Windows. Приведены сведения о правилах, на основании которых производится выборка.

В подразделе 6.2 «Выборка записей из баз данных браузеров» раздела 6 описан механизм выборки записей из баз данных браузеров.

В подразделе 6.3 «Распознавание файлов кэша браузеров» раздела 6 описан способ распознавания файлов кэша браузеров и присвоения им расширений.

В подразделе 6.4 «Выборка записей из баз данных Skype и Viber» раздела 6 описан механизм выборки записей из баз данных Skype и Viber.

В разделе 7 «Программа для сбора и агрегирования информации о работе в сети» приведена техническая информация о разработанной программе (язык программирования, общая структура, использованные сторонние библиотеки, формат выходных данных).

Подраздел 7.1 «Описание модулей программы» раздела 7 посвящен описанию всех модулей разработанной программы.

Подраздел 7.2 «Пример работы программы» раздела 7 содержит подробное описание процесса взаимодействия пользователя с программой. Подраздел включает в себя 5 рисунков, на которых продемонстрированы основные функции программы.

В заключении содержатся выводы по результатам работы.

В приложении А «Листинг программы» приведен код разработанной программы.

В приложении Б «Конфигурационные файлы» приведены необходимые для работы программы конфигурационные файлы, их структура и содержимое.

ЗАКЛЮЧЕНИЕ

В данной работе был изучен процесс следообразования и основанные на нем методы установления обстоятельств использования пользователем ПК с ОС Windows сетевых ресурсов и работы пользователя в сети Интернет, а также была разработана программа для сбора и агрегирования информации о сетевом взаимодействии. Были рассмотрены некоторые популярные приложения и сервисы, которые являются носителями сведений о взаимодействии пользователя с ресурсами сети Интернет и использовании определенных интерфейсов операционной системы.

Разработанная программа является удобным средством для быстрого и комплексного сбора сведений о сетевом взаимодействии на ПК с ОС Windows. В любой момент можно расширить ее функционал путем добавления новых правил сбора данных и модулей.

Таким образом, поставленные цели были достигнуты и решены все необходимые для их достижения задачи.

СПИСОК ИСПОЛЬЗОВАННЫХ ИСТОЧНИКОВ

1 «Forensic Assistant» («0xFA») v1.3.2 [Электронный ресурс] // National Hi-Tech Crime Unit.RU [Электронный ресурс]. URL: http://www.nhtcu.ru/fa_ru (дата обращения: 10.12.2016). Загл. с экрана. Яз. рус.

2 Belkasoft Evidence Center 2017 [Электронный ресурс] // Belkasoft [Электронный ресурс]. URL: https://belkasoft.com/ec (дата обращения: 10.12.2016). Загл. с экрана. Яз. англ.

3 Visualize your web use to understand your habits [Электронный ресурс] // Web Historian [Электронный ресурс]. URL: http://www.webhistorian.org/ (дата обращения: 10.12.2016). Загл. с экрана. Яз. англ.

4 ChromeAnalysis [Электронный ресурс] // foxton FORENSICS [Электронный ресурс]. URL: https://www.foxtonforensics.com/chromeanalysis/ (дата обращения: 10.12.2016). Загл. с экрана. Яз. англ.

5 FoxAnalysis [Электронный ресурс] // foxton FORENSICS [Электронный ресурс]. URL: https://www.foxtonforensics.com/foxanalysis/ (дата обращения: 10.12.2016). Загл. с экрана. Яз. англ.

6 About Event Logging [Электронный ресурс] // Microsoft [Электронный ресурс]. URL: https://msdn.microsoft.com/en-us/library/windows/desktop/aa363632.aspx (дата обращения: 15.09.2016). Загл. с экрана. Яз. англ.

7 Web Browser History [Электронный ресурс] // Livinginternet [Электронный ресурс]. URL: http://www.livinginternet.com/w/wi_browse.htm (дата обращения: 17.09.2016). Загл. с экрана. Яз. англ.

8 Что такое кэш в браузере и зачем нужно его чистить? [Электронный ресурс] // Заметки пользователям [Электронный ресурс]. URL: http://inck.in.ua/articles/33-chto-takoe-kjesh-v-brauzere-i-zachem-ego-nuzhno-chistit (дата обращения: 17.09.2016). Загл. с экрана. Яз. рус.

9 Top 5 Desktop, Tablet & Console Browsers from Jan to Dec 2016 [Электронный ресурс] // StatCounter [Электронный ресурс]. URL:

http://gs.statcounter.com/#browser-ww-monthly-201601-201612 (дата обращения: 18.12.2016). Загл. с экрана. Яз. англ.

10 Отчет: Количество посетителей с разными браузерами [Электронный ресурс] // Liveinternet [Электронный ресурс]. URL: https://www.liveinternet.ru/stat/ru/browsers.html (дата обращения: 18.12.2016). Загл. с экрана. Яз. англ.

11 Функции Chrome [Электронный ресурс] // Chrome [Электронный ресурс]. URL: https://www.google.ru/chrome/browser/features.html (дата обращения 16.09.2016). Загл. с экрана. Яз. рус.

12 Mozilla Firefox [Электронный ресурс] // Mozilla Россия [Электронный ресурс]. URL: https://mozilla-russia.org/products/firefox/ (дата обращения 21.09.2016). Загл. с экрана. Яз. рус.

13 Браузер Opera для ПК с Windows [Электронный ресурс] // Opera [Электронный ресурс]. URL: http://www.opera.com/ru/computer (дата обращения 22.09.2016). Загл. с экрана. Яз. рус.

14 Skype [Электронный ресурс] // TechTarget SearchUnified Communications [Электронный ресурс]. URL: http://searchunifiedcommunications.techtarget.com/definition/Skype (дата обращения: 10.12.2016). Загл. с экрана. Яз. рус.

15 «Это такая штука, где можно подглядывать за другими в замочную скважину» [Электронный ресурс] // афишаDaily [Электронный ресурс]. URL: https://daily.afisha.ru/archive/vozduh/technology/eto-takaya-shtuka-gde-mozhno-podglyadyvat-za-drugimi-v-zamochnuyu-skvazhinu/ (дата обращения: 05.12.2016). Загл. с экрана. Яз. рус.

16 Most popular mobile messaging apps worldwide as of April 2016 [Электронный ресурс] // statista [Электронный ресурс]. URL: https://www.statista.com/statistics/258749/most-popular-global-mobile-messenger-apps/ (дата обращения: 10.12.2016). Загл. с экрана. Яз. англ.