

Министерство образования и науки Российской Федерации

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

Кафедра теоретических основ
компьютерной безопасности и
криптографии

Исследование внутренней структуры мультимедиа-файлов

АВТОРЕФЕРАТ

дипломной работы

студентки 6 курса 631 группы

специальности 090102.65 «Компьютерная безопасность»

факультета компьютерных наук и информационных технологий

Чикатуевой Ольги Викторовны

Научный руководитель

старший преподаватель

И.Ю. Юрин

Заведующий кафедрой

профессор, к.ф.-м.н.

В.Н. Салий

Саратов 2016

ВВЕДЕНИЕ

В современном мире как никогда раньше распространено использование мультимедиа-файлов. Благодаря появлению социальных сетей, большому количеству видео- и аудио-хостингов, среди которых такие гиганты как youtube, rutube, kiwi, myspace, магазин itunes и другие, более быстрых способов передачи информации и более доступных устройств для съёмки цифрового видео и аудио, потоки цифровых данных захлестнули глобальную сеть. Заметим, что эти технологии развивались достаточно бурно на протяжении последних десятилетий. Вместе с технологиями записи и распространения мультимедиа появлялись и новые способы воспроизведения. Рост потребности в новых технологиях для работы с цифровым видео и аудио повышал и интерес к разработке всё более совершенных форматов хранения таких данных, что привело к появлению огромного количества разнообразных форматов и их разновидностей. У многих записывающих и генерирующих мультимедиа-контент программ появились свои уникальные способы записи таких данных в разных форматах, которые далеко не всегда подходят под описанные стандарты.

Мультимедиа используется не только для развлекательных целей. Например, запись с видеокamеры – это весомый аргумент при доказательстве чьей-либо вины в суде. Но технологии цифровой обработки мультимедиа тоже не стоят на месте, и любой злоумышленник, чтобы не оказаться за решёткой, вполне может попытаться подделать видео-улики. Тогда появляется очень важный вопрос – как же понять, подделано ли видео, которое предоставляют в качестве улики, или нет? Можно ли утверждать, что это видео было снято с помощью камеры марки Canon, а другое нет? Ответ кроется внутри самих файлов.

Не теряя общности, в этой работе будет рассмотрен один из самых популярных видео-форматов в мире – AVI и один из самых популярных аудио-

форматов – WAV. Будет описана разработанная программа, позволяющая визуально отобразить внутреннюю структуру этих файлов. С использованием этой программы будут выявлены интересные особенности разных устройств и программ, по которым можно определить с помощью чего был создан или изменён исследуемый файл.

КРАТКОЕ СОДЕРЖАНИЕ РАБОТЫ

Работа состоит из 5 разделов, а также списка основных определений и обозначений и приложения с листингом разработанной программы.

В первом разделе подробно рассматривается внутренняя структура формата RIFF, который является контейнером для мультимедиа-форматов AVI, WAV и других. Приведены определения основных элементов RIFF-структуры – блоков данных и блоков-списков, а также 2 таблицы, поясняющие строение этих элементов. Кроме того, описан способ вложения медиа-данных в контейнер и перечислены основные типы медиа-форматов, которые вкладываются в RIFF.

Раздел 2 посвящен формату AVI. Вначале дается определение формата AVI и приводится статистика использования этого и других форматов пользователями (по версии компании Movavi). В наиболее общем виде описывается структура формата, также приведено графическое представление. Далее следует подробное определение обязательных элементов формата AVI вместе с таблицами, описывающими структуры данных, которые содержатся в них. В последнем подразделе предложены необязательные элементы формата AVI, которые не определены документацией компании Microsoft, но были найдены в процессе исследования разных файлов, а также предложена информация об особенностях их появления в файле.

Раздел 3 содержит информацию о формате WAV. Приведено определение формата WAV, данные о возможностях использования, а также основная структура. По аналогии со вторым разделом изложены сведения об основных элементах WAV-структуры, а также об элементах, обнаруженных в ходе исследования файлов.

Описание программы, разработанной на основании полученных данных, представлено в разделе 4. Программа написана на языке Java 8 с использованием библиотеки JavaFX для реализации интерфейса пользователя и

позволяет исследовать внутреннюю структуру AVI- и WAV-файлов, а также проводить поиск следов использования оборудования или ПО для создания или изменения файла. В первом подразделе приведена подробная информация о возможностях программы и особенностях интерфейса, также приложены снимки экрана программы на всех этапах работы. Во втором подразделе дается информация о структуре программы, корневых пакетах и наиболее важных классах.

В пятом разделе предложено несколько примеров работы программы на различных файлах форматов AVI и WAV. Дается краткая информация о тестируемых файлах, а также снимки экрана работы программы с пояснениями.

Также в Приложении представлены фрагменты исходного кода программы, наиболее важные классы и интерфейсы, относящиеся к логике программы. Часть, касающаяся реализации пользовательского интерфейса, по возможности исключена.

ЗАКЛЮЧЕНИЕ

В результате проделанной работы была получена программа, способная визуально отображать внутреннее содержимое мультимедиа-файлов форматов AVI и WAV. Структура этих файлов была подробно изучена и описана. Было исследовано множество различных файлов для выявления особенностей, которые закладывают производители в свои устройства и программы. На основании этих особенностей в программу был добавлен модуль для автоматического исследования внутренней структуры файлов, чтобы более просто определять подозрительные места в файлах.

Возвращаясь к вопросу, который был поставлен во введении, можно сделать следующий вывод – в большинстве случаев определить факт изменения файла удастся. Формально, подделать идеально видео-файл можно, но для этого нужно иметь очень большой опыт в этой области, и ни одна свободно распространяемая программа сейчас не способна это сделать в автоматическом режиме.

СПИСОК ИСПОЛЬЗОВАННЫХ ИСТОЧНИКОВ

1) RIFF [Электронный ресурс] // Универсальная энциклопедия [Электронный ресурс] URL: <http://unienc.ru/w/ru/903394-riff.html> (дата обращения 01.09.2015) Загл. с экрана.

2) AVI RIFF File Reference [Электронный ресурс] / Microsoft DirectShow 9.0 // Microsoft Documentation [Электронный ресурс] URL: <https://msdn.microsoft.com/en-us/library/ms779636.aspx> (дата обращения: 03.09.2015) Загл. с экрана. Яз. англ.

3) Audio Video Interleave [Электронный ресурс] // Академик [Электронный ресурс] URL: <http://dic.academic.ru/dic.nsf/ruwiki/716278> (дата обращения: 02.09.2015) Загл. с экрана.

4) Movavi [Электронный ресурс] URL: <http://www.movavi.ru/> (дата обращения: 20.09.2015)

5) Alexander Noé. AVI File Format / Alexander Noé [Электронный ресурс] URL: <http://www.alexander-noe.com/video/documentation/avi.pdf> (дата обращения: 04.09.2015) Загл. с экрана. Яз. англ.

6) John McGowan. AVI Overview [Электронный ресурс] / John McGowan // Solving Practical Problems with Mathematics [Электронный ресурс] URL: <http://www.jmcgowan.com/avi.html> (дата обращения: 10.09.2015) Загл. с экрана. Яз. англ.

7) AVI Research [Электронный ресурс] // URL: http://www.odec.ca/projects/2004/chia4a0/public_html/aviresearch.htm (дата обращения 11.09.2015) Загл. с экрана. Яз. англ.

8) RIFF [Электронный ресурс] // URL: <https://ru.wikipedia.org/wiki/RIFF> (дата обращения: 03.09.2015) Загл. с экрана.

9) RIFF Tags [Электронный ресурс] // The Sudbury Neutrino Observatory [Электронный ресурс] URL:

<http://www.sno.phy.queensu.ca/~phil/exiftool/TagNames/RIFF.html> (дата обращения: 04.09.2015) Загл. с экрана. Яз. англ.

10) Tag Mapping [Электронный ресурс] // Hydrogenaudio Knowledgebase [Электронный ресурс] URL: http://wiki.hydrogenaud.io/index.php?title=Tag_Mapping (дата обращения: 12.11.2015) Загл. с экрана. Яз. англ.

11) Josef Garvi. Extracting Recording Date & Time from AVI film clips [Электронный ресурс] / Josef Garvi // Eden Foundation [Электронный ресурс] URL: http://www.eden-foundation.org/products/code/film_date_stamp/ (дата обращения: 02.10.2015) Загл. с экрана. Яз. англ.

12) WAV [Электронный ресурс] // URL: <https://ru.wikipedia.org/wiki/WAV> (дата обращения: 04.11.2015) Загл. с экрана.

13) Формат WAV [Электронный ресурс] // Audio Coding [Электронный ресурс] URL: <http://audiocoding.ru/formats/wav/> (дата обращения: 03.11.2015) Загл. с экрана. Яз. англ.

14) Rob Ryan. RIFF WAVE (.WAV) file format [Электронный ресурс] / Rob Ryan // URL: <http://www.neurophys.wisc.edu/auditory/riff-format.txt> (дата обращения: 29.10.2015) Загл. с экрана. Яз. англ.

15) Microsoft. Multimedia. Standards Update. New Multimedia Data Types and Data Techniques [Электронный ресурс] / Microsoft Corporation // URL: <http://www-mmssp.ese.mcgill.ca/Documents/AudioFormats/WAVE/Docs/RIFFNEW.pdf> (дата обращения: 29.10.2015) Загл. с экрана. Яз. англ.

16) WAVE Module Specification [Электронный ресурс] / JHOVE2 // URL: https://bytebucket.org/jhove2/main/wiki/documents/JHOVE2-WAVE-module-спес-2_0_0.pdf (дата обращения: 05.11.2015) Загл. с экрана. Яз. англ.

17) Specification of the Broadcast Wave Format (BWF). A format for audio data files in broadcasting [Электронный ресурс] / EBU-UER // URL:

<https://tech.ebu.ch/docs/tech/tech3285.pdf> (дата обращения 10.11.2015) Загл. с экрана. Яз. англ.

18) WAVFormat [Электронный ресурс] // awesome-wav [Электронный ресурс] URL: <https://code.google.com/p/awesome-wav/wiki/WAVFormat> (дата обращения 14.11.2015) Загл. с экрана. Яз. англ.

19) Эккель, Б. Философия Java. Библиотека программиста / Эккель, Б. 4-е изд. СПб.: Питер, 2009. 640 с.

20) Мартин, Р. Чистый код: Создание, анализ и рефакторинг. Библиотека программиста / Мартин, Р. СПб.: Питер, 2010. 464 с.