УДК 004

Технология получения контрольных сумм файлов

Ленкин Алексей Викторович
Приамурский государственный университет имени Шолом-Алейхема.
Студент

Глаголев Владимир Александрович
Приамурский государственный университет имени Шолом-Алейхема
к.г.н., доцент кафедры информационных систем, математики и методик обучения

Аннотация
В данной статье описана технология контрольных сумм, а также продемонстрирована работа хеш-функций MD5 и SHA1.
Ключевые слова: контрольные суммы, хеш-суммы, хеш-функции, MD5, SHA1, HashTab

Technology for obtaining checksums of files

Lenkin Aleksei Viktorovich,
Sholom-Aleichem Priamursky State University
Student

Glagolev Vladimir Alexandrovich
Sholom-Aleichem Priamursky State University
candidate of geographical Sciences, associate professor of the Department of information systems, mathematics and teaching methods

Abstract
This article describes the checksum technology and illustrates the work of the MD5 and SHA1 hash functions.
Keywords: checksums, hash sums, hash functions, MD5, SHA1, HashTab

На сегодняшний день, в связи с сильно развитой инфраструктурой технологии интернет, каждый день генерируется, передается, удаляется и т.д. огромное количество файлов различных форматов и размеров. Но этим также активно начинают пользоваться злоумышленники, подменяя нужные пользователю файлы вирусами, при этом маскируя их под настоящие, изменив вес и название файла.

Для предотвращения таких подмен используется проверка контрольных сумм файлов (или хеш-суммы). Самыми популярными алгоритмами генерации хеш-сумм являются MD5 и SHA-1. Также контроль

сумм файлов может использоваться для проверки целостности скачанного файла.

Задачи исследования:

– изучить механизм реализации проверки контрольных сумм;

– показать на примере работу программ проверки контрольных сумм;

Цель исследования – описать технологию получения контрольных сумм и продемонстрировать её работу.

Исследованиями в данной теме занимались следующие авторы. Р.Корнийчук в своей работе описал механизм «Контрольной суммы. Проверка подлинности полученного файла»[1]. «Защита интернет-ресурсов методом контрольных сумм» демонстрируется в статье Б.С.Яковлев, Н.Е. Проскуряков [2]. А.Р. Кузьмин указал в своей работе контрольные суммы как «Актуальные методы обеспечения целостности данных облачной системы хранения»[3].

Контрольная сумма – это результат работы хеш-функций, позволяющих вычислить для файла любого размера уникальную короткую хеш-сумму. Контрольная сумма позволяет узнать тот ли файл вы скачали и является ли он целым или поврежден.

Технологии проверки контрольных сумм широко используется и в облачных технологиях, позволяя сократить время загрузки файлов пользователем на сервер, так как перед загрузкой происходит проверка хеш-суммы всех файлов и дупликаты не загружаются. Контрольные суммы также используются в технологии торрент, где она выполняется автоматически, защищая получаемую пользователем информацию. Последнее применение контрольных сумм это использование в качестве паролей, так как хеш-суммы достаточно криптоустойчивы.

Для проверки контрольной суммы используется большое количество алгоритмов хеш-функций и много программ генераций хеш-суммы. Самой популярной является HashTab компании Implibits [4].

Продемонстрируем пример работы программы.

Создадим два текстовых файла New.txt и Old.txt. Так как оба файла сейчас пустые можно сравнить их контрольные суммы (они должны быть одинаковы). Для этого необходимо зайти в свойства файла New.txt, перейти в «Хеш-суммы файлов», после чего нажать «Сравнить файл» и выбрать файл Old.txt. Результат работы виден на рисунке 1.

Программа показала идентичные контрольные суммы.

Теперь изменим содержание файлов, в файле New.txt напишем «New», а в Old.txt соответственно «Old», такие файлы будут иметь один размер и если им дать одно название, то будут казаться одинаковыми. Результат проверки модифицированных файлов представлен на рисунке 2.

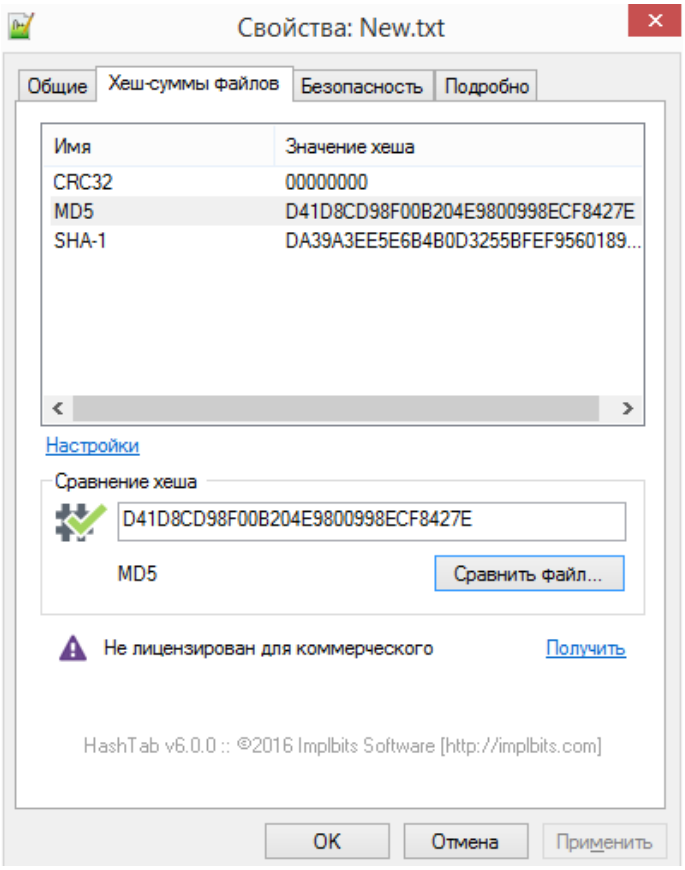

Рисунок 1. Проверка хеш-суммы одинаковых файлов в HashTab

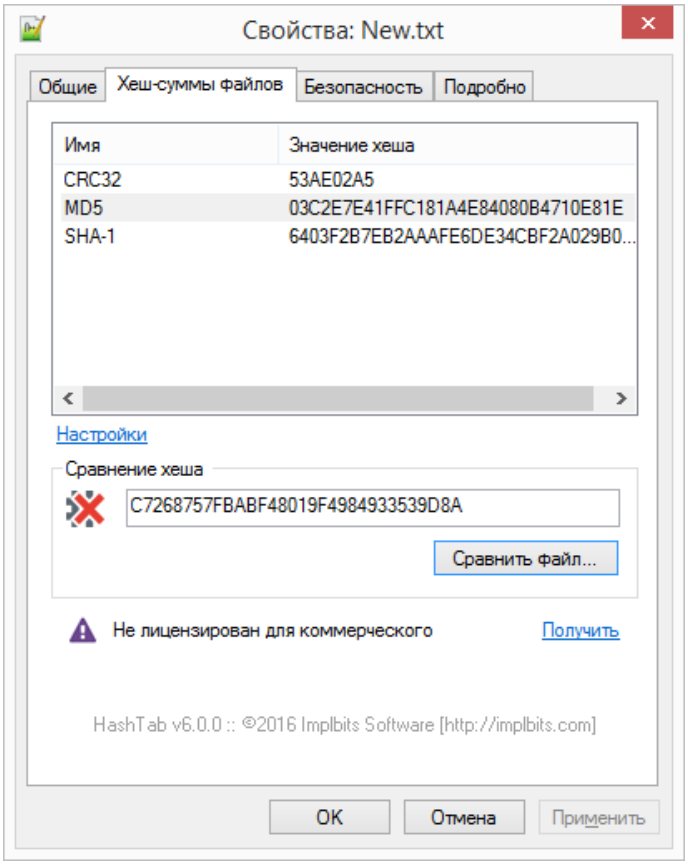

Рисунок 2. Проверка хеш-суммы файлов с разным содержанием

Результатом проверки стали различные контрольные суммы, сильно отличающиеся не только друг от друга, но и от своих пустых версий.

Таким образом, использование технологии контрольных сумм является важным средством безопасности при проверки любых файлов. И позволяет быстро вычислять какие файлы были модифицированы или повреждены. И хотя сами хэш-функции MD5 и SHA1 давно устарели и существую способы их обмана, они всё ещё могут использоваться для повседневных задач обычных пользователей.

Библиографический список

1. Корнийчук Р. Контрольная сумма. Проверка подлинности полученного файла. // Системный администратор. 2010. № 7-8 (92-93). С. 120-121.
2. Яковлев Б.С., Проскуряков Н.Е. Защита интернет-ресурсов методом контрольных сумм // Динамика систем, механизмов и машин. 2016. Т. 2. № 1. С. 311-317.
3. Кузьмин А.Р. Актуальные методы обеспечения целостности данных облачной системы хранения // Современная наука: актуальные проблемы теории и практики. Серия: Естественные и технические науки. 2017. № 2. С. 19-25.
4. HashTab [Электронный ресурс] URL: http://implbits.com/products/hashtab/ (дата обращения 12.01.2018)