ФЕДЕРАЛЬНОЕ АГЕНТСТВО СВЯЗИ

Федеральное государственное бюджетное образовательное учреждение

высшего образования

«Санкт-Петербургский государственный университет телекоммуникаций

им. проф. М.А. Бонч-Бруевича***»***

(СПБГУТ)

***\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_***

Факультет ИКСС

Кафедра ЗСС

Отчет по лабораторной работе №9

по дисциплине:

**«Цифровая криминалистика»**

Выполнили:

Студенты гр. ИКТБ-98м

Зеличенок И.Ю.

Щипцов Д.И.

Проверила:

Федорченко Е.В

Санкт-Петербург

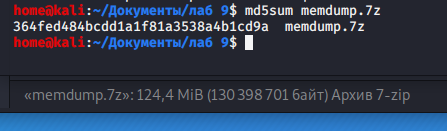
2020г.

Цель: извлечь и найти информацию

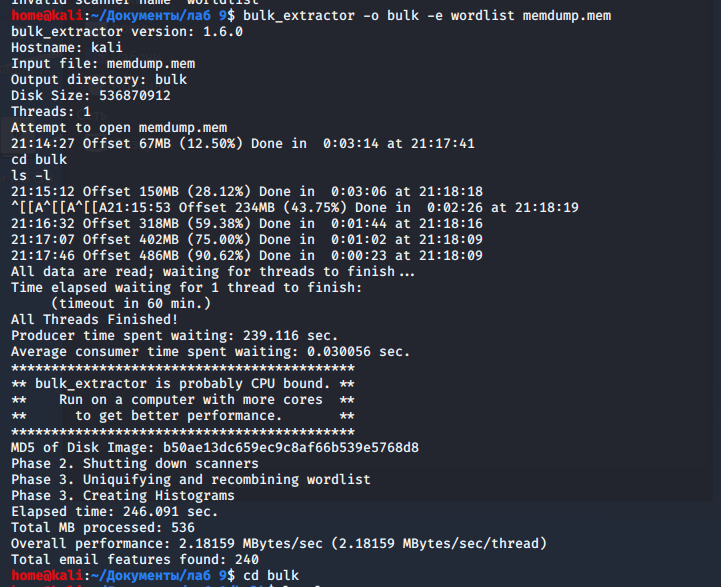
bulk\_extractor - это программа, которая извлекает такие функции, как адреса электронной почты, номера кредитных карт, URL-адреса и другие типы информации из цифровых файлов. Это полезный инструмент экспертизы для многих задач, таких как вредоносное и вторночное расследование, исследования личности и кибер-исследования, а также анализ изображений. Программа предоставляет несколько необычных возможностей, включая:

* Он находит адреса электронной почты, URL-адреса и номера кредитных карт, которые пропускают другие инструменты, поскольку он может обрабатывать сжатые данные (например, файлы ZIP, PDF и GZIP) и неполные или частично поврежденные данные. Он может вырезать JPEG, офисные документы и другие файлы из фрагментов сжатых данных. Он будет обнаруживать и вырезать зашифрованные файлы RAR.
* Он создает списки слов на основе всех слов, найденных в данных, даже в сжатых файлах, находящихся в нераспределенном пространстве. Эти списки слов могут быть полезны для взлома пароля.
* Он многопоточный; запуск bulk\_extractor на компьютере с удвоенным количеством ядер, как правило, заставляет запустить полчаса.
* Он создает гистограммы, показывающие наиболее распространенные адреса электронной почты, URL-адреса, домены, условия поиска и другие виды информации на диске.

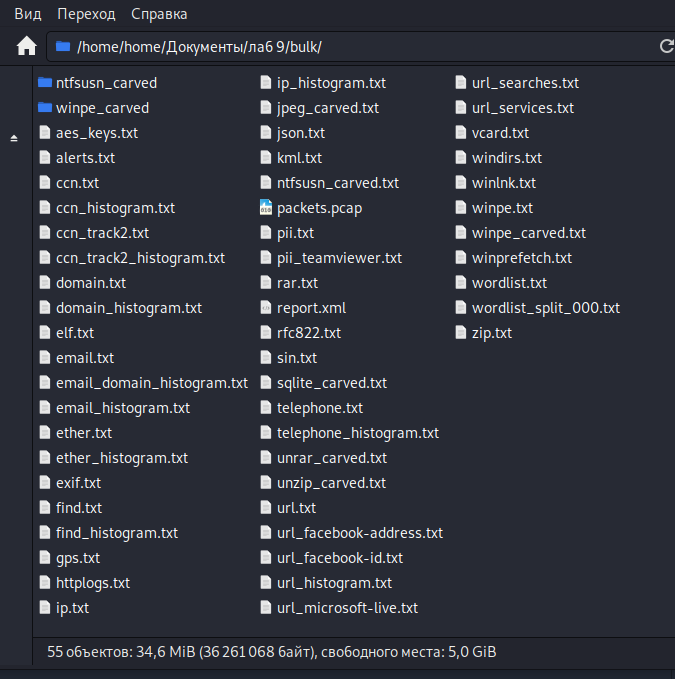
проверка архива



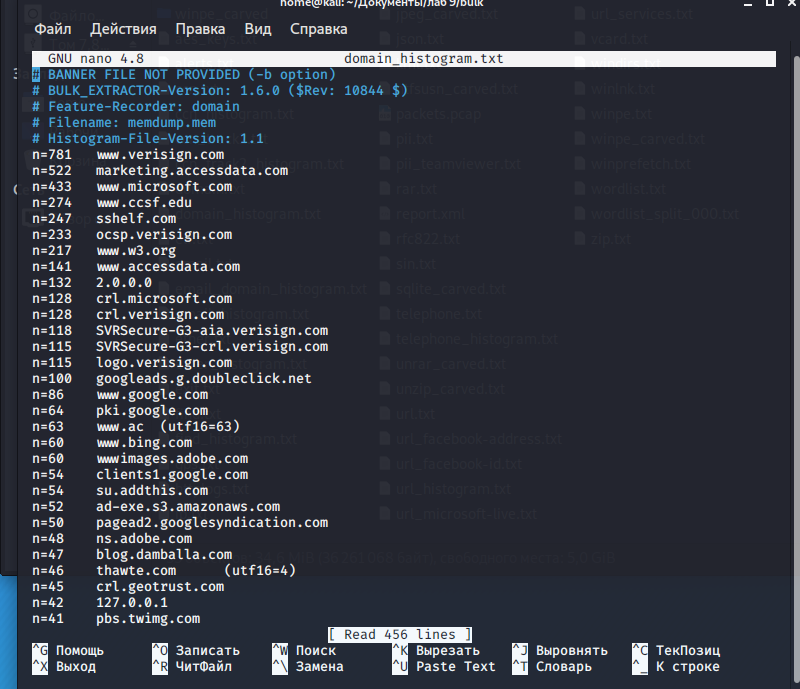
произведем экстракт



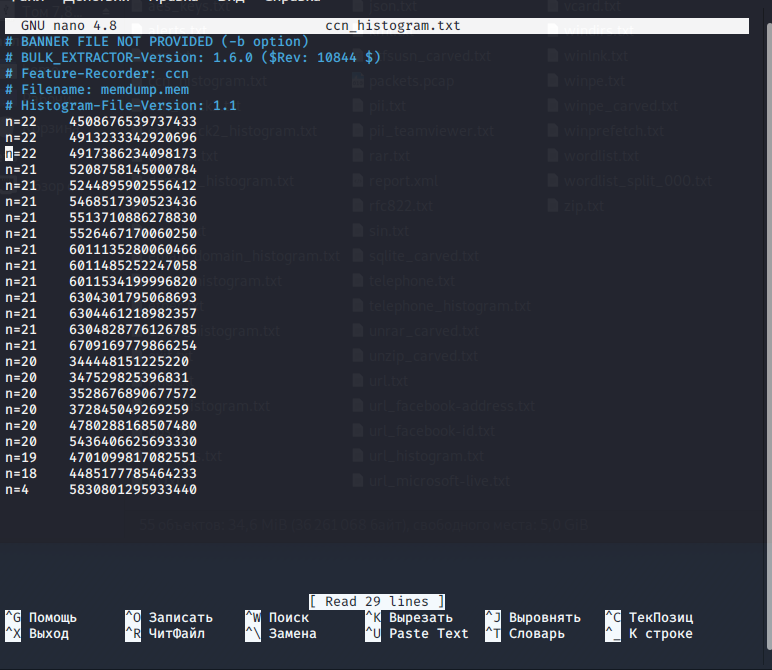
Получили результат



Проверим посещение сайтов

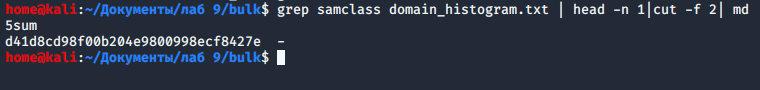


Проверим номера кредитных карт

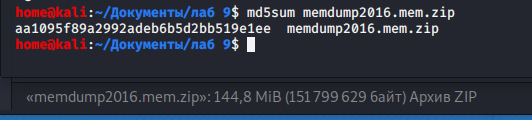


Искомая карта





Проверка архива



Адрес найденный в 2016



Вывод: bulk\_extractor позволяет извлекать полезную информацию для криминалистики так и для злоумышлеников.