УДК 004.056.53 **Технические науки**

Мешкова Елена Владимировна, *студентка 4 курса электротехнического факультета,*
Пермский национальный исследовательский политехнический университет

ПЕРЕХВАТ И АНАЛИЗ СЕТЕВОГО ТРАФИКА С ПОМОЩЬЮ «WIRESHARK»

Аннотация. В данной статье рассмотрен перехват и анализ сетевого трафика с помощью сниффера Wireshark.

Ключевые слова: сниффер, сетевые протоколы, анализ трафика.

Abstract. In this article discusses interception and the analysis of a network traffic by means of Wireshark sniffer.

Keywords: sniffer, network protocols recognition, traffic analysis.

Сейчас уже трудно представить наш современный мир без информационных технологий, наоборот, с каждым днем они развиваются и внедряются в больших количествах. Так и сфера сетевых технологий совершенствуется и появляются более новые сетевые протоколы, реализующиеся на прикладном уровне. В связи с этим становится актуальным мониторинг и анализ сетевого трафика.

Анализатор трафика — это программа, которая предназначена для перехвата, хранения и последующего анализа сетевого трафика, предназначенного для своих или других узлов. Также анализатор трафика имеет и другое название – сниффер. Сниффер может анализировать лишь те данные, которые проходят через его сетевую карту. Перехват сетевого трафика может осуществляться посредством:

- «прослушивания» сетевого интерфейса;
- подключением сниффера к разрыву канала;
- анализа побочных электромагнитных излучений;
- атаки на канальном или сетевом уровне, которая приводит к перенаправлению трафика жертвы или всего трафика сегмента на сниффер с последующим возвращением трафика в надлежащий адрес [1].

В данной статье будет рассмотрен перехват и анализ сетевого трафика с помощью сниффера Wireshark с целью выявления несанкционированного доступа к ресурсам сети и/или получения/передачи информации третьим лицам.

Wireshark – это программа, разработанная The Wireshark Team, которая имеет лицензию GNU General Public License и является свободно распространяемым продуктом. Данная программа поддерживают разбор большого количества различных сетевых протоколов, а также предоставляет возможность сортировки и фильтрации трафика. В режиме реального времени пользователь данного сниффера имеет возможность просматривать весь проходящий по сети трафик.

В качестве примера работы программы осуществим перехват изображения в сети. Для начала работы с продуктом необходимо скачать его с официального сайта и произвести установку на компьютер. Стартовое меню программы имеет вид, изображенный на рисунке 1.

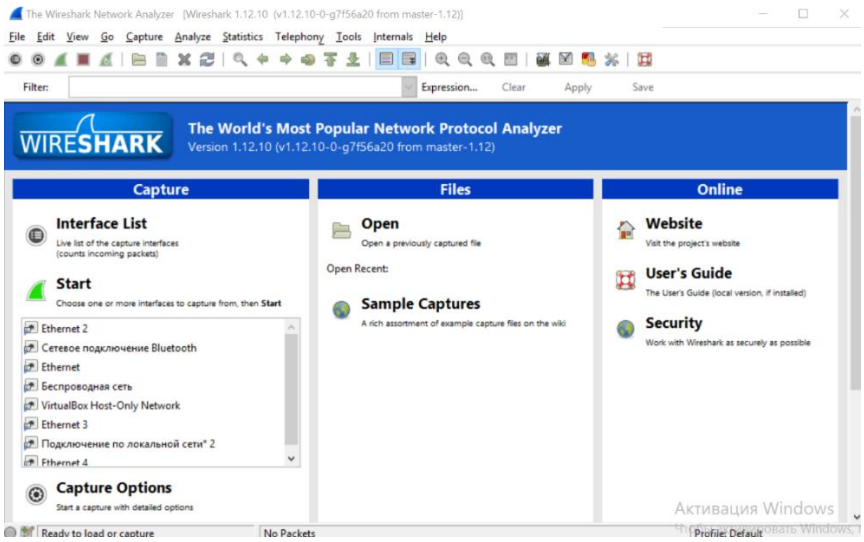

Рисунок 1 – Стартовое меню программы

Выбираем сетевой интерфейс, с помощью которого будет осуществляться захват пакетов и нажимаем «start». Выбор сетевого интерфейса представлен на рисунке 2.

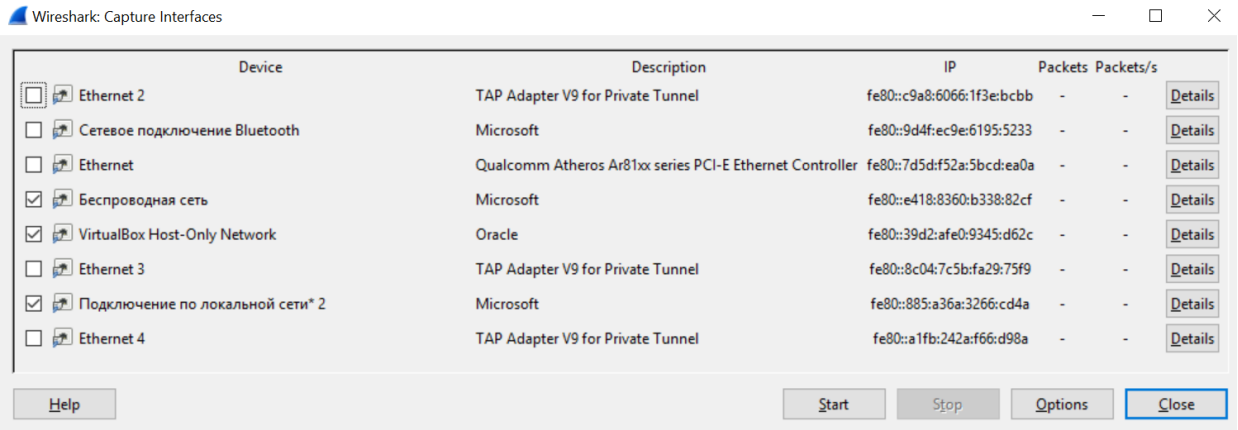

Рисунок 2 – Выбор сетевого интерфейса

После выбора сетевого трафика запускается основное меню программы, которое представлено на рисунке 3.

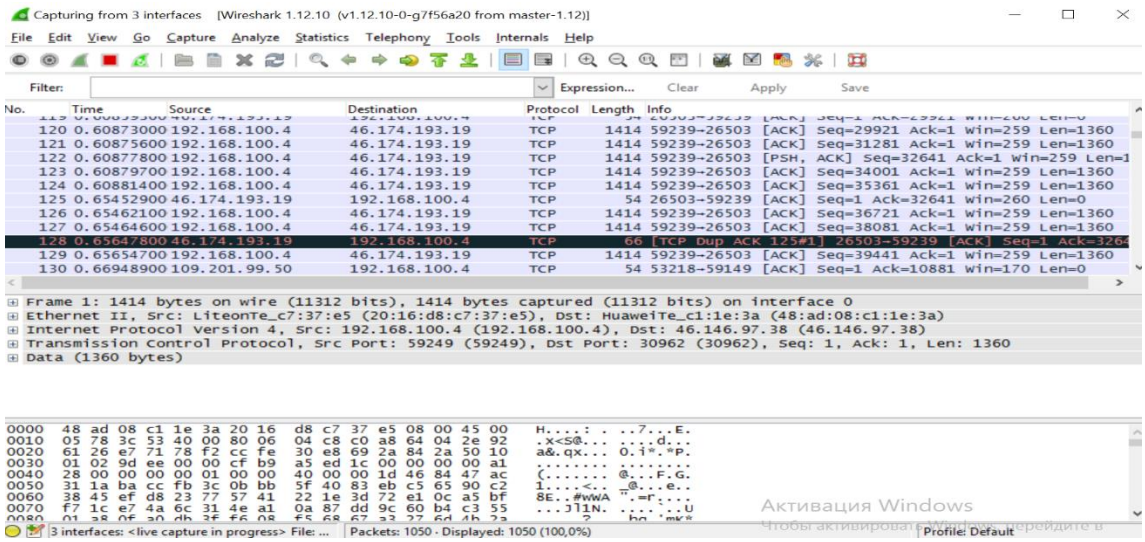

Рисунок 3 – Основное меню программы

Теперь произведем и сам перехват изображения. Для этого перейдем в меню File→ Export Objects → HTTP, в результате появится окно, которое показывает все захваченные http объекты – текстовые файлы, картинки и т.д. (Рисунок 4)

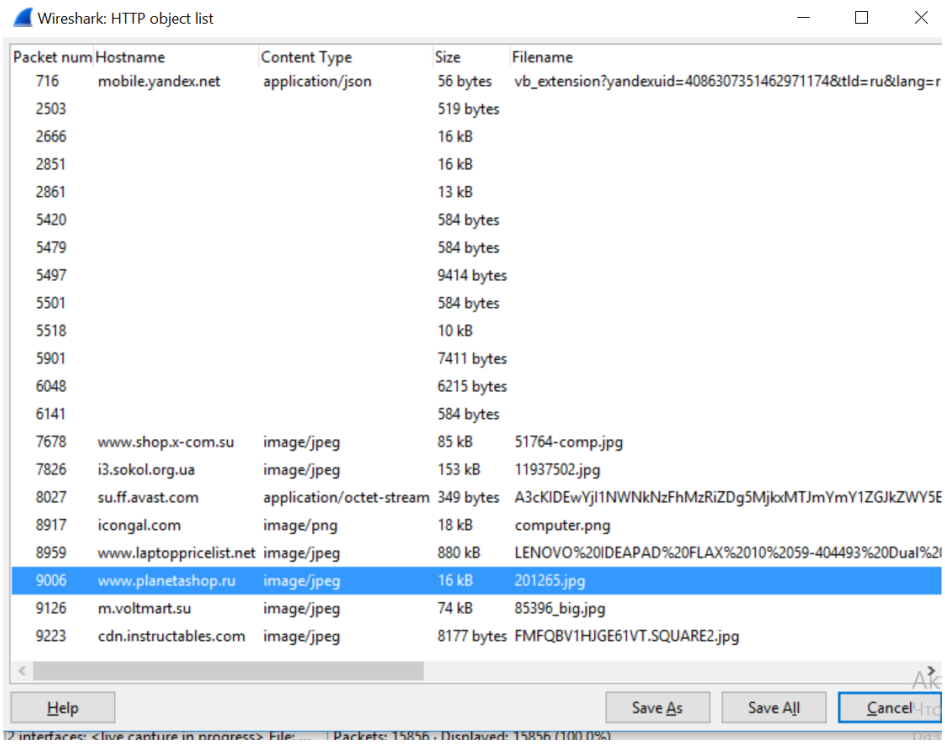

Рисунок 4 – Захваченные объекты

Для того чтобы извлечь нужный файл из списка, достаточно просто выделить его и нажать «Save As». Далее сохраняем файл и открываем его для просмотра. (Рисунок 5)

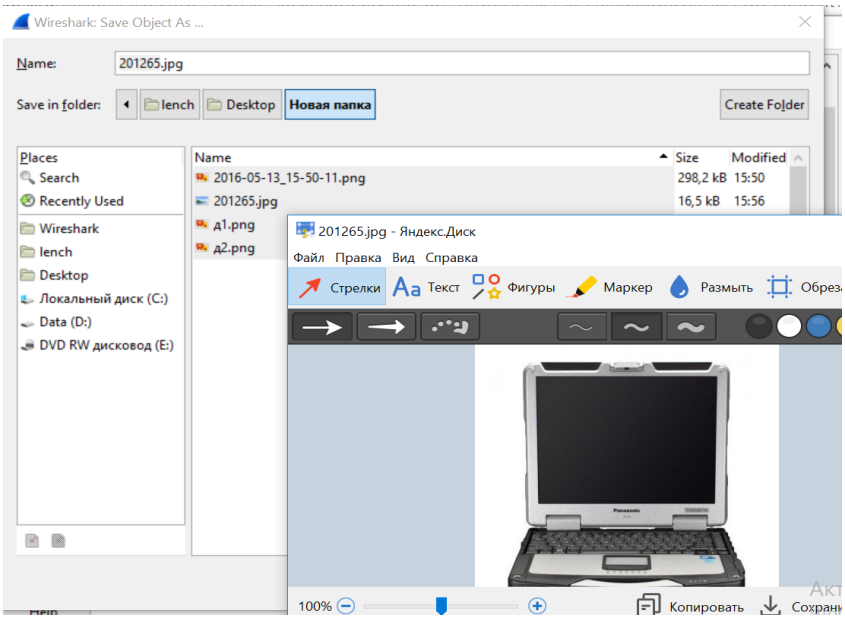

Рисунок 5 – Перехваченное изображение

Также программа позволяет перехватить и текстовый файл, и персональные данные пользователя в сети широковещательной передачей трафика (в сети с концентратором).

Wireshark представляет пользователю удобный интерфейс для работы и поддерживает разбор и распознавание более 100 сетевых протоколов.

При возникновении сложных, повторяющихся нерегулярно проблем, связанных с нарушением безопасности, а также для их решения, необходим анализ сетевого трафика, который позволяет выявить данные проблемы в сети, восстановить потоки данных, предотвратить различного рода сетевые атаки, накапливать статистику.

Библиографический список

1. Маркин Ю. В., Санаров А. С. Обзор современных инструментов анализа сетевого трафика. http://www.ispras.ru/preprints/docs/prep_27_2014.pdf, дата обращения 17.08.2016

2. Wireshark Trace Files. Режим доступа: http://www.wiresharkbook.com/studyguide_supplements/9781893939943_traces.zip, дата обращения 17.08.2016

3. Wireshark. Режим доступа: http://www.wireshark.org/ , дата обращения 17.08.2016