|  |
| --- |
| Федеральное государственное бюджетное образовательное учреждение высшего профессионального образования МОсковский государственный технический университет имени баумана (Мгту им. н. э. баумана) |

|  |
| --- |
| Приложение - анализатор трафика  для Windows  "MyWireshark" |

Руководство пользователя

Автор: Стаселович Олег

Группа: ИУ8-33

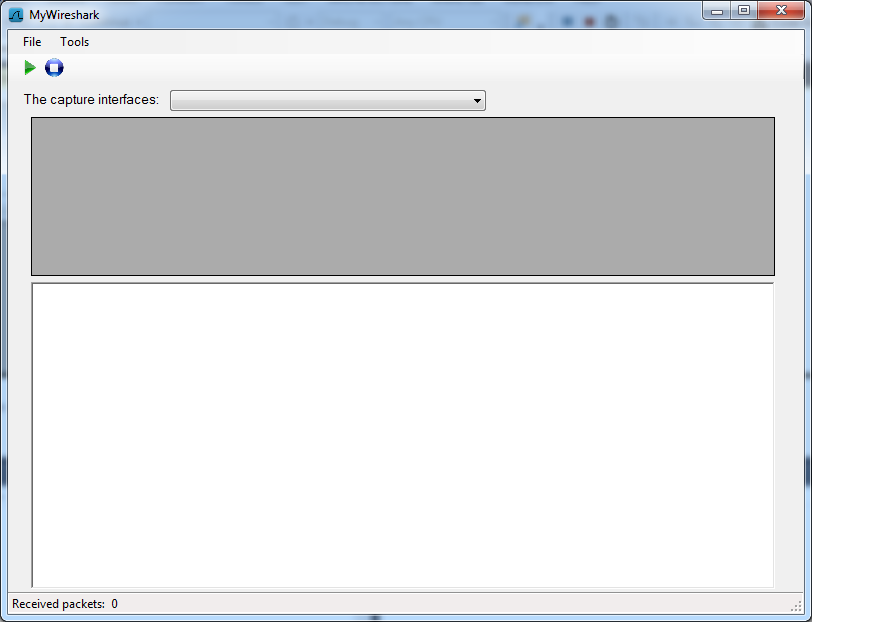
Москва, 2015

**Системные требования:**

* ОС: Windows 7, 8, 8.1, 10
* Microsoft .NET Framework 4.5
* 1 Гб свободного места на жестком диске;
* CPU: 1 ГГц и выше;
* RAM: 512 Мб и выше;
* Видеокарта: карта с 256 Мб видеопамяти;
* Наличие сетевого адаптера

**Главное окно программы:**

После запуска приложения появится окно, представленное ниже.

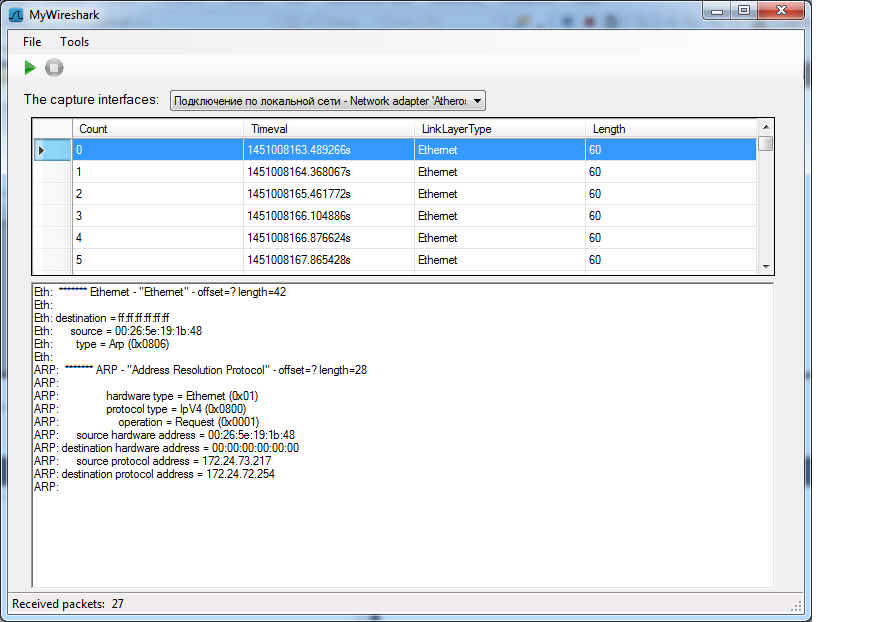


Оно включает в себя:

* Область вывода перехватываемых пакетов (серая область)
* Область вывода информации о пакете (белая область)
* Выпадающий список доступных устройств
* Кнопки "Старт" и "Стоп"
* Меню, состоящее из двух пунктов - "File" и "Tools"
* Строку состояния, выводящую количество перехваченных пакетов

**Работа с программой.**

Перед началом перехвата пакетов необходимо выбрать устройство, которое будет прослушиваться. Для этого необходимо кликнуть по выпадающему списку "The capture interfaces". Появятся доступные подключения с именами адаптера. Выберите один из них. После этого кликните по кнопке "Старт" (зеленый треугольник на панели инструментов). Начнется перехват пакетов.

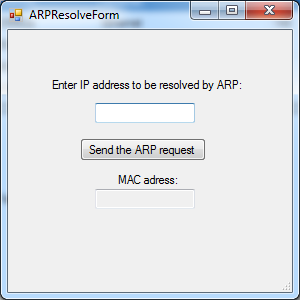


В верхнем поле отображается список всех пакетов. В столбцах указывается номер пакета, время, тип протокола канального уровня, длина. В нижнем поле приводится дополнительная информация по выбранному пакету. Например, на приведенной картинке видно, что выбранный пакет - ARP-запрос. Он пришел на сетевой адаптер компьютера по протоколу Ethernet, и поднялся выше до уровня сетевого протокола.

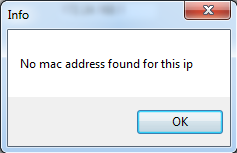
При нажатии на кнопку "Стоп" (белый прямоугольник в синем круге) захват пакетов остановится, можно подробно рассмотреть захваченный пакеты.

При выборе пункта меню File - Quit происходит закрытие приложения.

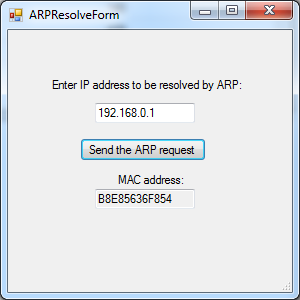
При выборе пункта меню Tools - ARPResolve открывается новое окно для отправки ARP-запроса. Его внешний вид приведен ниже.



В текстовое поле вводится IP-адрес, по которому нужно определить MAC-адрес. В случае неудачи будет выведено следующее сообщение:



При вводе корректного IP-адреса в поле "MAC address" будет выведен MAC-адрес устройства по указанному IP-адресу.



После закрытия этой формы можно продолжить просматривать перехватываемый трафик.