С31. Принцип действия анализаторов пакетов - Wireshark

Wireshark – это программный инструмент для перехвата и анализа сетевого трафика. Сама программа, в первую очередь, предназначена для сбора информации о сетевых взаимодействиях и для обнаружения и устранения неполадок в сети. Анализаторы трафика применяются при разработке новых протоколов и программного обеспечения.

Установленная и запущенная на компьютере программа Wireshark позволяет обнаружить и изучить любой протокольный блок данных (Protocol Data Unit, PDU), который был отправлен и получен с помощью установленных на компьютере сетевых адаптеров (Network Interface Card, NIC). По мере движения потоков данных по сети анализатор перехватывает каждый протокольный блок данных (PDU), после чего расшифровывает или анализирует его содержание согласно соответствующему документу RFC или другим спецификациям.

Wireshark работает с подавляющим большинством известных протоколов, имеет понятный и логичный графический интерфейс на основе GTK+ и мощнейшую систему фильтров.

Кроссплатформенный, работает в таких ОС как Linux, Solaris, FreeBSD, NetBSD, OpenBSD, Mac OS X, и, естественно, Windows. Распространяется под лицензией GNU GPL v2. Доступен бесплатно на сайте **www.wireshark.org**.

Внешний вид программы Wireshark на экране представлен на рис.1.

Рис. 1. Вид окна «загрузка программы» Wireshark

При первой установке программы Wireshark на компьютер или в том случае, когда предыдущая версия была удалена, откроется мастер установки программы Wireshark. Нажмите кнопку «Next» (рис. 1.2).

Выполните все инструкции по установке. Когда откроется окно «License Agreement» (Лицензионное соглашение), нажмите кнопку «I accept» (Принять) (рис. 1.3).

При выборе компонентов оставьте настройки по умолчанию и нажмите кнопку «Next» (рис. 1.4).

Рис. 1.2. Мастер установки программы

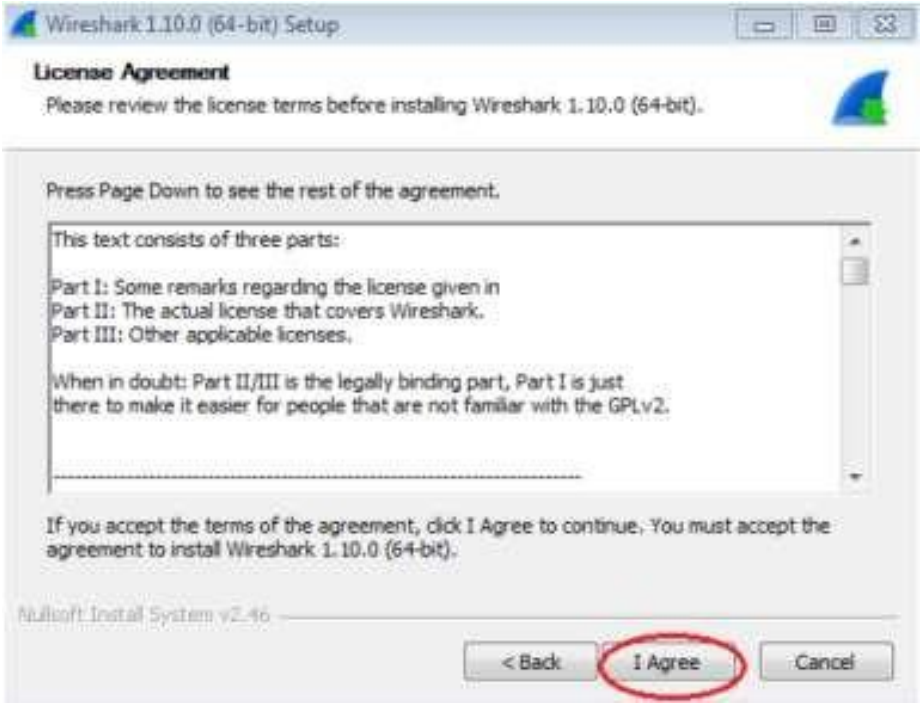

Рис. 1.3. Вид окна «Лицензионного соглашения»

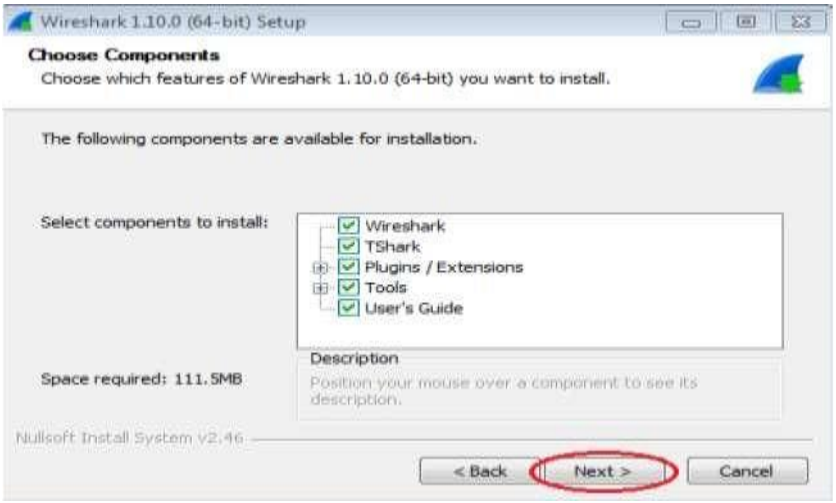

Рис. 1.4. Вид окна программы Wireshark «выбор компонентов»

Самостоятельная работа:

1) Установка программы Wireshark на виртуальную машину;
2) Основные функции программы Wireshark;
3) Основные функции панели инструментов