
Лабораторная №3

# «Использование программных средств системного и прикладного назначения»

Кафедра ИУ-8

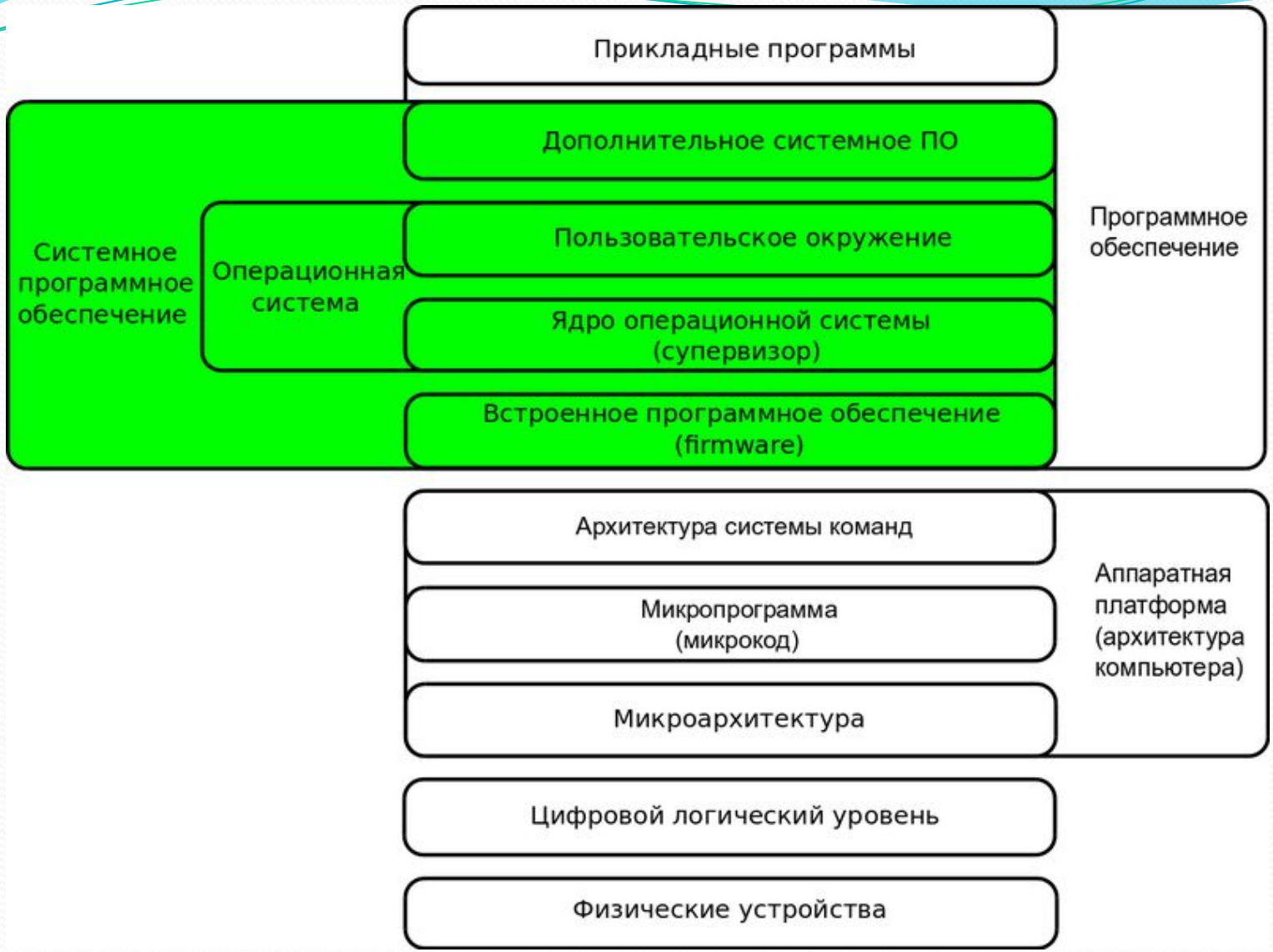
**Использование программных средств**
**форматирования,**
**дефрагментации,**
**архивации,**
**антивирусной защиты.**

Программное обеспечение можно условно разделить на системные и пользовательские программы.

**Системное программное обеспечение** выполняет функции «организатора» всех частей ПК, а также подключенных к нему внешних устройств.

**Программы для пользователей** служат для выполнения каких–либо конкретных задач во всех сферах человеческой деятельности.

Иными словами, отличие от прикладного программного обеспечения, системное не решает конкретные прикладные задачи, а лишь обеспечивает работу других программ, управляет аппаратными ресурсами вычислительной системы и т.д.


Прикладные программы
Дополнительное системное ПО
Пользовательское окружение
Ядро операционной системы (супервизор)
Встроенное программное обеспечение (firmware)
Системное программное обеспечение
Операционная система
Программное обеспечение
Архитектура системы команд
Микропрограмма (микрокод)
Микроархитектура
Аппаратная платформа (архитектура компьютера)
Цифровой логический уровень
Физические устройства

# Форматирование диска

Форматирование диска - процесс разметки диска на сектора и дорожки для записи данных. Форматирование создает структуру диска, обеспечивающую запись/чтение файлов и программ операционной системой.

Форматирование диска на низком уровне (низкоуровневое форматирование). Это единственный «настоящий» метод форматирования диска. При этом процессе на жестком диске создаются физические структуры: треки (дорожки), сектора, управляющая информация. Этот процесс выполняется заводом-изготовителем на пластинах, которые не содержат ещё никакой информации.

Высокоуровневое форматирование. Этот процесс контролируется операционной системой и зависит как от типа операционной системы, так и от утилиты, используемой для форматирования. Процесс записывает логические структуры, ответственные за правильное хранение файлов, а также, в некоторых случаях, системные загрузочные файлы в начало диска. Это форматирование можно разделить на два вида: быстрое и полное. При быстром форматировании перезаписывается лишь таблица файловой системы, при полном же — сначала производится верификация (проверка) поверхности накопителя, а уже потом производится запись таблицы файловой системы.

Рассмотрим основные параметры форматирования средствами ОС Windows.

Файловая система:
NTFS ($2^{44}$ байт минус 64 килобайта, теоретически – $2^{64}$ байт)
FAT (поддерживает файлы размером не более 2 ГБ)
FAT32 (поддерживает файлы размером не более 4 ГБ)
exFAT (размер файла $2^{64}$ байт)

Размер кластера:
4096 байт
2048 байт
1024 байт
512 байт

Использовать сжатие

# Архивирование

Архивирование данных - сжатие и размещение файлов данных для их длительного хранения в памяти.

Архивирование можно проводить как средствами операционной системы, так и с помощью специальных программ (например, WinRAR).

Программы-архиваторы позволяют задать алгоритм сжатия, установить пароль на архив и другие дополнительные параметры.

# Дефрагментация

Дефрагментация — процесс обновления и оптимизации логической структуры раздела диска с целью обеспечить хранение файлов в непрерывной последовательности кластеров. После дефрагментации ускоряется чтение и запись файлов, а следовательно и работа программ, ввиду того, что последовательные операции чтения и записи выполняются быстрее случайных обращений (например, для жесткого диска при этом не требуется перемещение головки).
Другое определение дефрагментации: перераспределение файлов на диске, при котором они располагаются в непрерывных областях.

Длинные файлы занимают несколько кластеров. Если запись производится на незаполненный диск, то кластеры, принадлежащие одному файлу, записываются подряд. Если диск переполнен, на нём может не быть цельной области, достаточной для размещения файла. Тем не менее, файл все-таки запишется, если на диске много мелких областей, суммарный размер которых достаточен для записи. В этом случае файл записывается в виде нескольких фрагментов.

Процесс разбиения файла на небольшие фрагменты при записи на диск называется фрагментацией. Если на диске много фрагментированных файлов, скорость чтения носителя уменьшается, поскольку поиск кластеров, в которых хранятся файлы, на жёстких дисках требует времени. На флеш-памяти, например, время поиска не зависит от расположения секторов, и практически равно нулю, поэтому для них дефрагментация не требуется.

# Антивирусная защита

Антивирусная программа (антивирус) — любая программа для обнаружения компьютерных вирусов, а также нежелательных (считающихся вредоносными) программ вообще и восстановления зараженных (модифицированных) такими программами файлов, а также для профилактики — предотвращения заражения (модификации) файлов или операционной системы вредоносным кодом.

На данный момент антивирусное программное обеспечение разрабатывается в основном для ОС семейства Windows от компании Microsoft, что вызвано большим количеством вредоносных программ именно под эту платформу (а это, в свою очередь, вызвано большой популярностью этой ОС, также как и большим количеством средств разработки, в том числе бесплатных и даже "инструкций по написанию вирусов").

Классифицировать антивирусные продукты можно сразу по нескольким признакам, таким как: используемые технологии антивирусной защиты, функционал продуктов, целевые платформы.

*По используемым технологиям антивирусной защиты*:

- Классические антивирусные продукты (продукты, применяющие только сигнатурный метод детектирования)
- Продукты проактивной антивирусной защиты (продукты, применяющие только проактивные технологии антивирусной защиты);
- Комбинированные продукты (продукты, применяющие как классические, сигнатурные методы защиты, так и проактивные)

*По функционалу продуктов*:

- Антивирусные продукты (продукты, обеспечивающие только антивирусную защиту)
- Комбинированные продукты (продукты, обеспечивающие не только защиту от вредоносных программ, но и фильтрацию спама, шифрование и резервное копирование данных и другие функции)

По целевым платформам:

- Антивирусные продукты для ОС семейства Windows
- Антивирусные продукты для ОС семейства *UNIX (к данному семейству относятся ОС BSD, Linux, Mac OS X и др.)
- Антивирусные продукты для мобильных платформ (Windows Mobile, Symbian, iOS, BlackBerry, Android и др.)

Антивирусные продукты для корпоративных пользователей можно также классифицировать по объектам защиты:

- Антивирусные продукты для защиты рабочих станций
- Антивирусные продукты для защиты файловых и терминальных серверов
- Антивирусные продукты для защиты почтовых и Интернет-шлюзов
- Антивирусные продукты для защиты серверов виртуализации

и др.

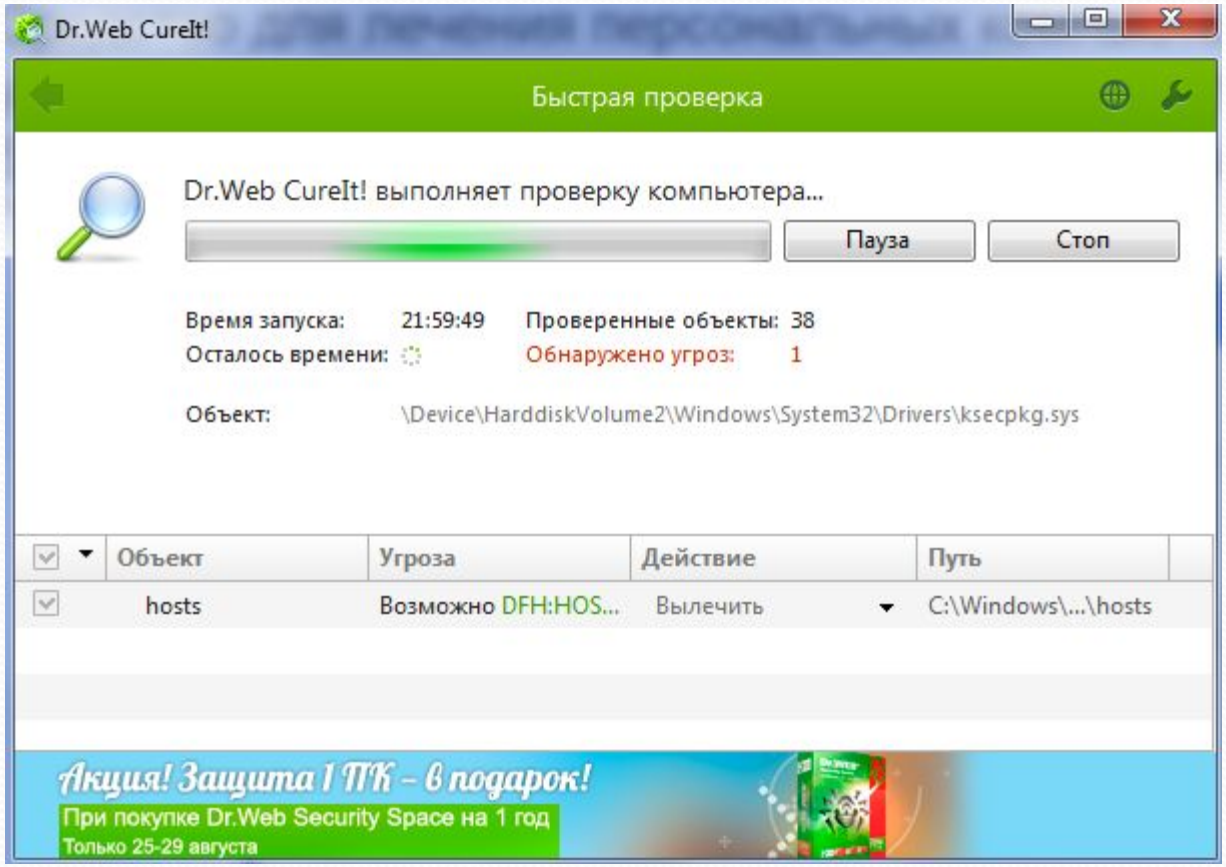
# Полезные утилиты и основы борьбы с вредоносным ПО

http://technet.microsoft.com/ru-ru/sysinternals

- Dr.Web CureIt!
- Wireshark
- TCPView
- Autoruns
- Process Explorer
- Process Monitor

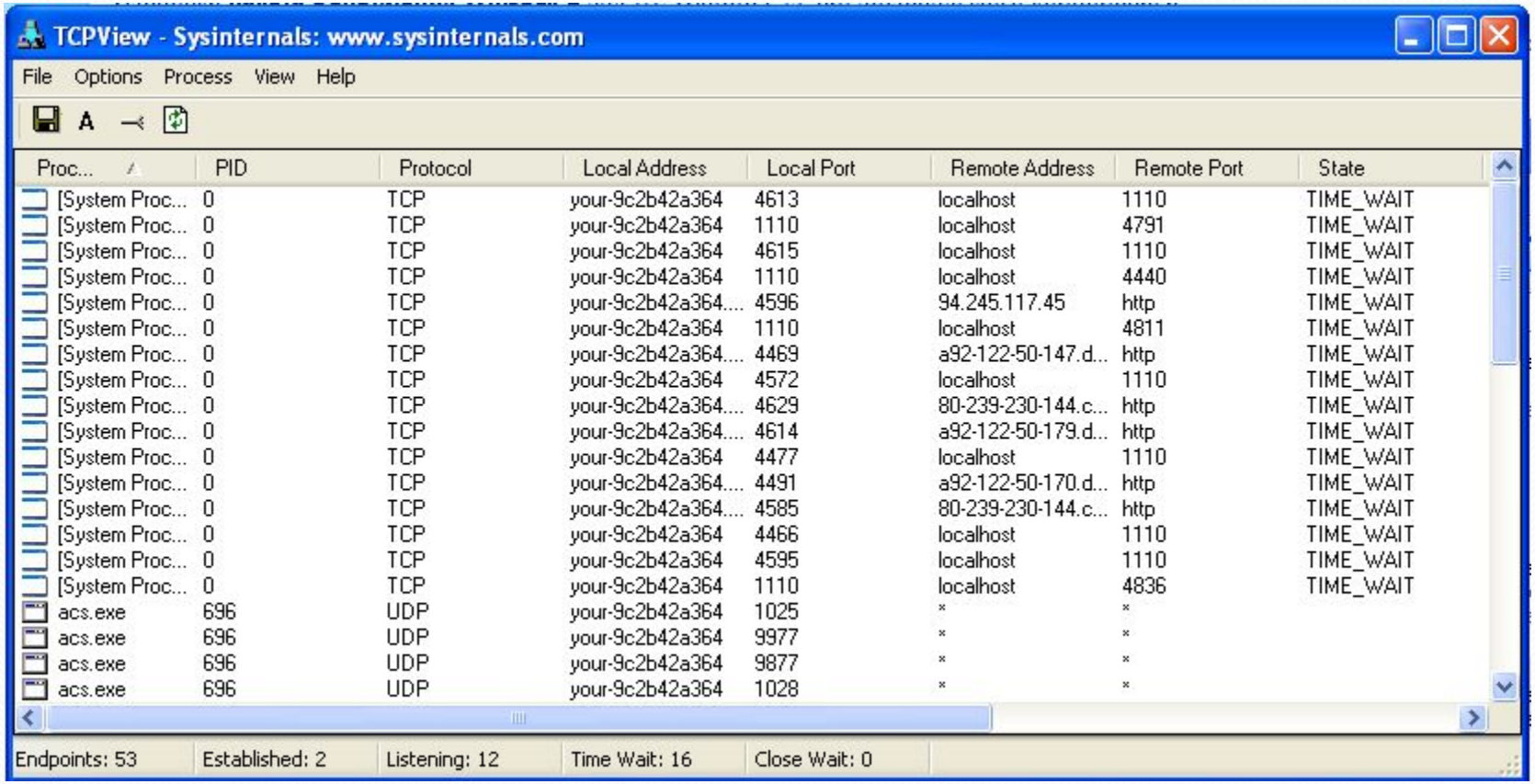
# Dr.Web CureIt!

Средство для лечения персональных компьютеров и серверов под управлением MS Windows 2000/XP/2003/Vista/2008/Windows 7 (32- и 64-битные системы) от вирусов, руткитов, троянских программ, шпионского ПО и разного рода вредоносных объектов.



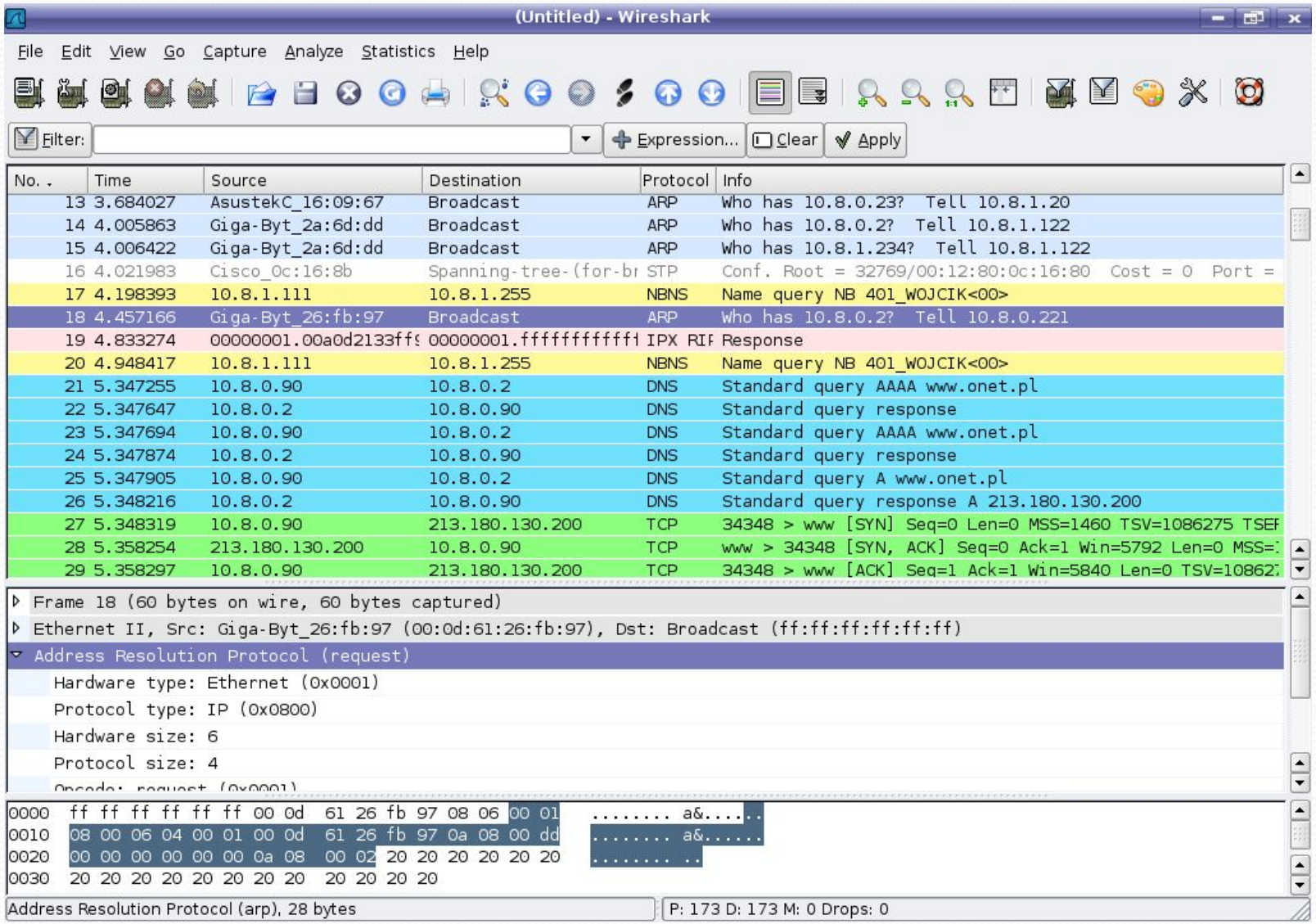
# TCPView

TCPView — это программа, предназначенная для операционной системы Windows, которая выводит на экран списки конечных точек всех установленных в системе соединений по протоколам TCP и UDP с подробными данными, в том числе с указанием локальных и удаленных адресов и состояния TCP-соединений. В операционных системах Windows NT, 2000 и XP программа TCPView также сообщает имя процесса, которому принадлежит конечная точка.



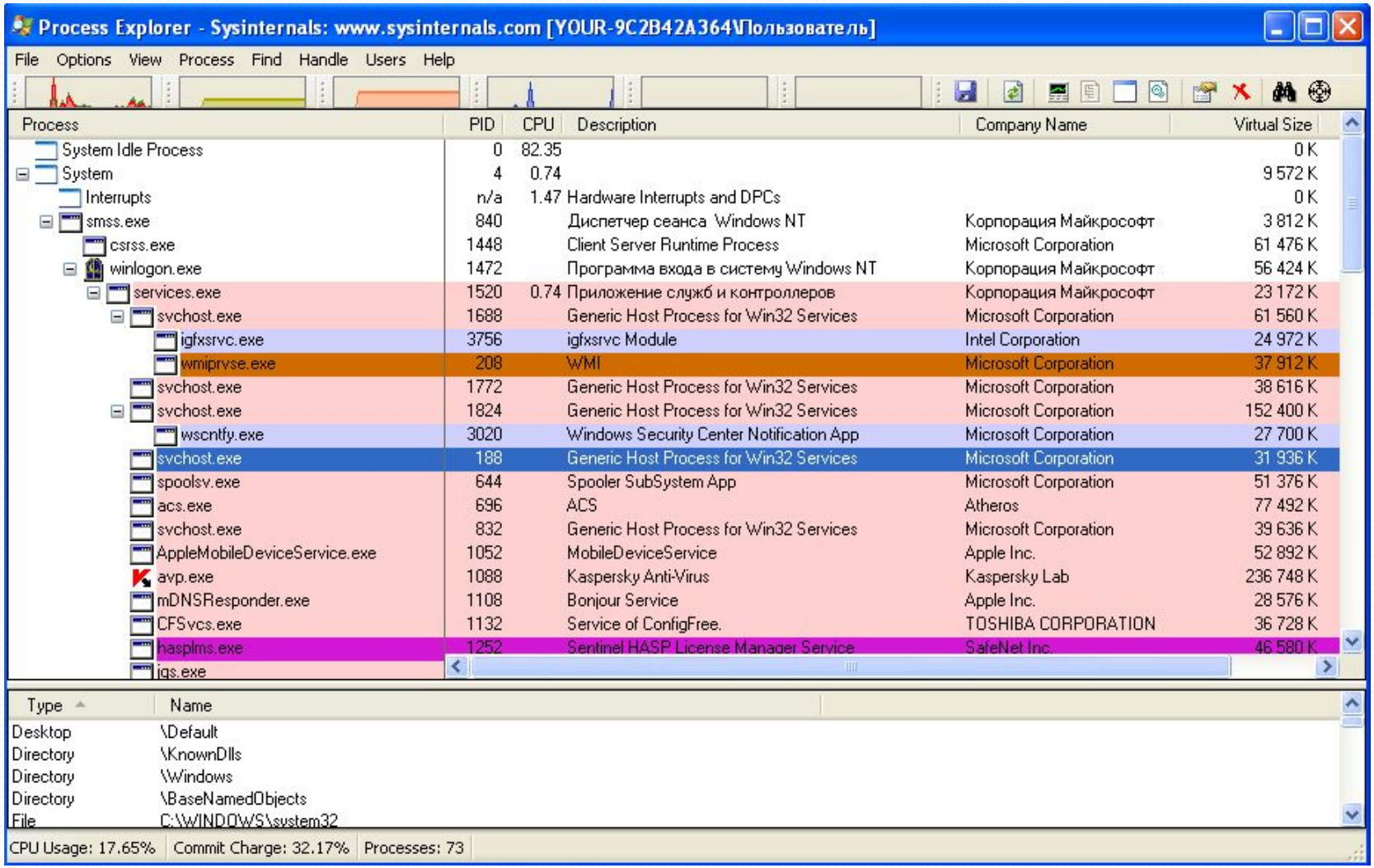
# Wireshark

Wireshark (ранее — Ethereal) — программа-анализатор трафика для компьютерных сетей Ethernet и некоторых других.



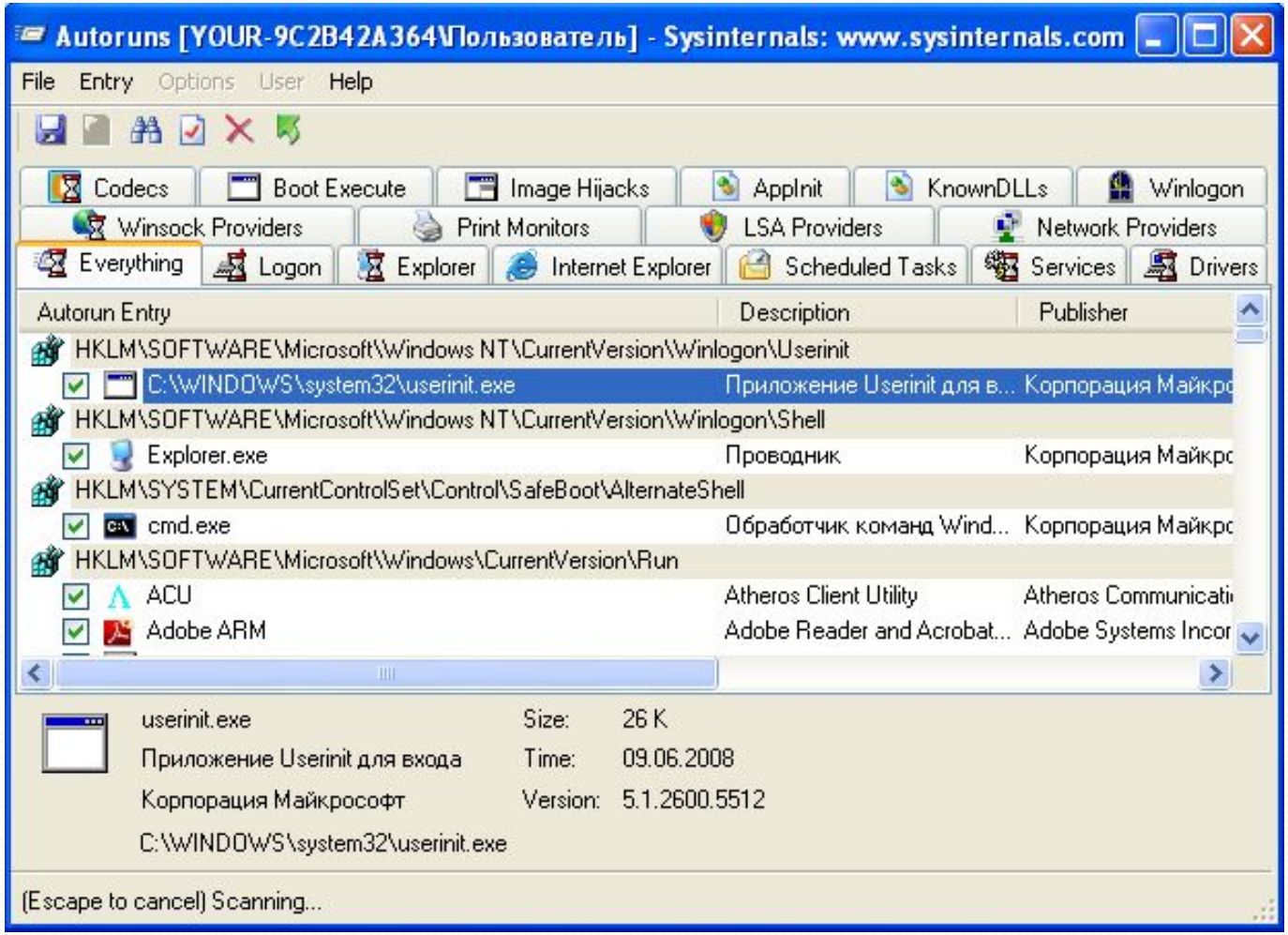
# Process Explorer

Программа *Process Explorer* отображает информацию об открытых процессом дескрипторах и загруженных им библиотеках DLL.



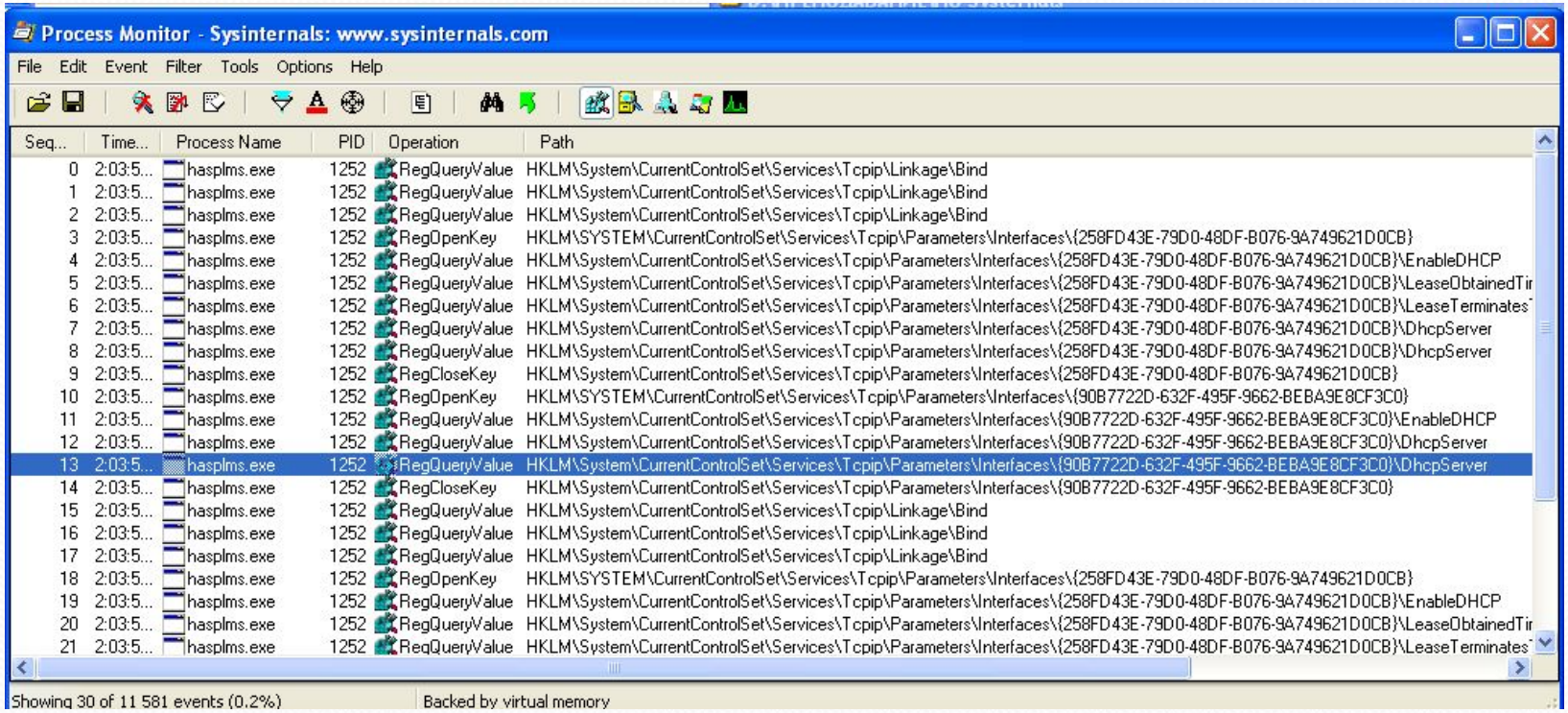
# Autoruns

Это средство проверяет большее количество мест, из которых происходит автозапуск программ, чем любой другой монитор автозагрузки. Оно показывает, какие программы настроены на запуск в процессе загрузки или входа в систему, причем эти программы отображаются в том порядке, в каком система Windows обрабатывает их.



# Process Monitor

Программа Process Monitor является усовершенствованным инструментом отслеживания для Windows, который в режиме реального времени отображает активность файловой системы, реестра, а также процессов и потоков.В этой программе сочетаются возможности двух ранее выпущенных программ от Sysinternals: Filemon и Regmon, а также огромный ряд улучшений, включая расширенную и безвредную фильтрацию, всеобъемлющие свойства событий, такие как ID сессий и имена пользователей, достоверную информацию о процессах, полноценный стек потока со встроенной поддержкой всех операций, одновременную запись информации в файл и многие другие возможности. Эти уникальные возможности делают программу Process Monitor ключевым инструментом для устранения неполадок и избавления от вредоносных программ.



# Спасибо за внимание