

Лабораторная №3

**«Использование программных
средств системного и прикладного
назначения»**

Кафедра ИУ-8

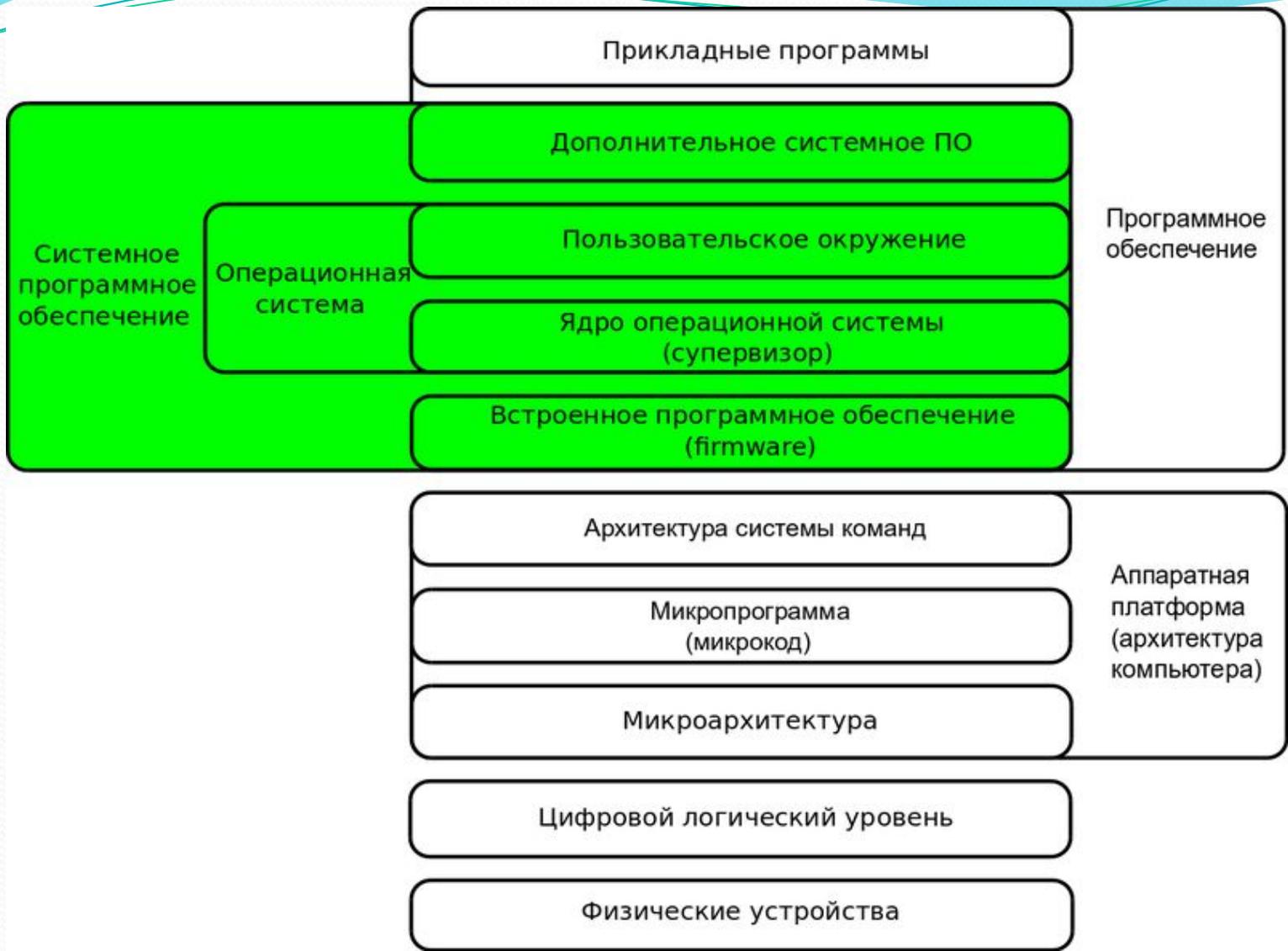
**Использование программных средств
форматирования,
дефрагментации,
архивации,
антивирусной защиты.**

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.



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.

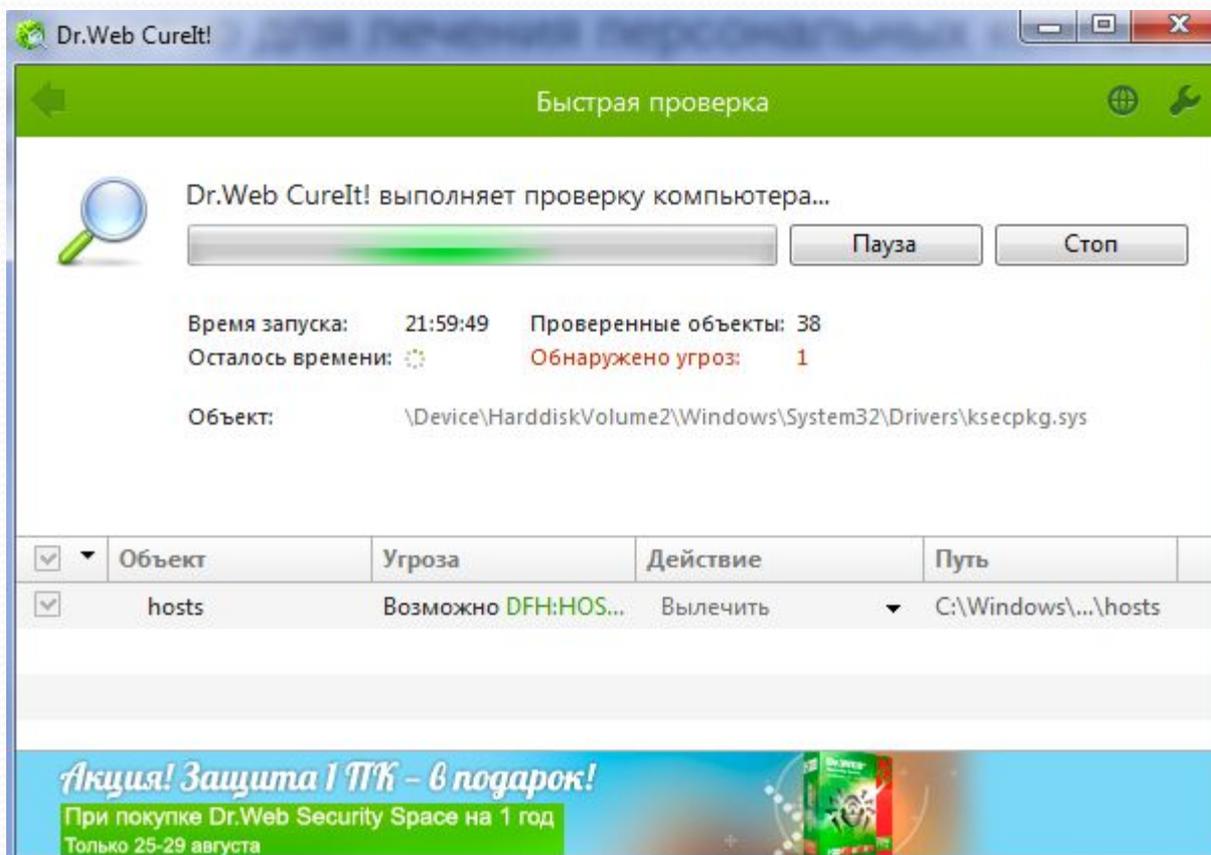
Полезные утилиты и основы борьбы с вредоносным ПО

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

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

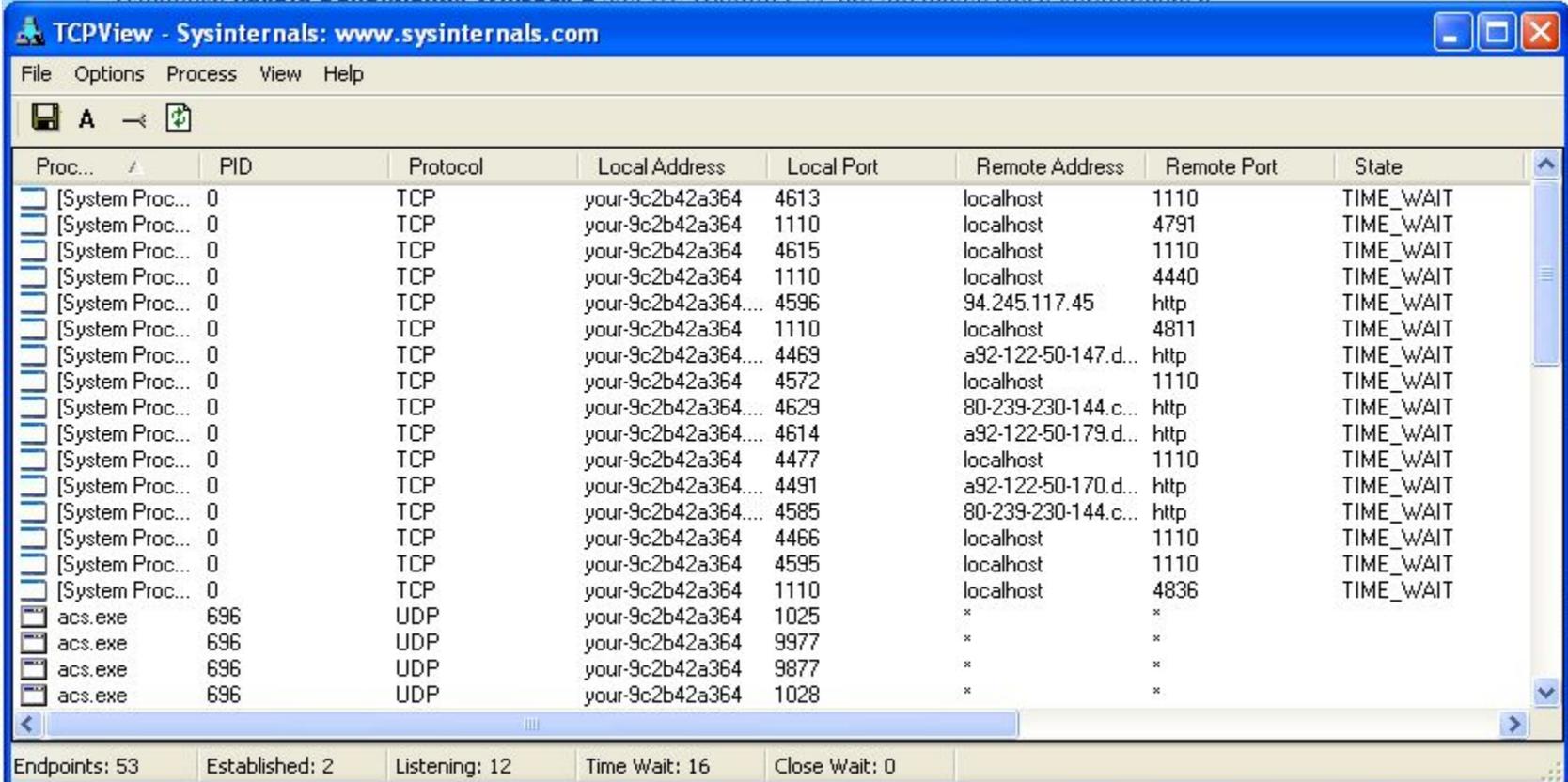
Dr.Web CureIt!

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.



The screenshot shows the TCPView application window with the following menu items: File, Options, Process, View, Help. The main display area contains a table of network connections. The status bar at the bottom indicates: Endpoints: 53, Established: 2, Listening: 12, Time Wait: 16, Close Wait: 0.

Proc...	PID	Protocol	Local Address	Local Port	Remote Address	Remote Port	State
[System Proc...	0	TCP	your-9c2b42a364	4613	localhost	1110	TIME_WAIT
[System Proc...	0	TCP	your-9c2b42a364	1110	localhost	4791	TIME_WAIT
[System Proc...	0	TCP	your-9c2b42a364	4615	localhost	1110	TIME_WAIT
[System Proc...	0	TCP	your-9c2b42a364	1110	localhost	4440	TIME_WAIT
[System Proc...	0	TCP	your-9c2b42a364...	4596	94.245.117.45	http	TIME_WAIT
[System Proc...	0	TCP	your-9c2b42a364	1110	localhost	4811	TIME_WAIT
[System Proc...	0	TCP	your-9c2b42a364...	4469	a92-122-50-147.d...	http	TIME_WAIT
[System Proc...	0	TCP	your-9c2b42a364	4572	localhost	1110	TIME_WAIT
[System Proc...	0	TCP	your-9c2b42a364...	4629	80-239-230-144.c...	http	TIME_WAIT
[System Proc...	0	TCP	your-9c2b42a364...	4614	a92-122-50-179.d...	http	TIME_WAIT
[System Proc...	0	TCP	your-9c2b42a364	4477	localhost	1110	TIME_WAIT
[System Proc...	0	TCP	your-9c2b42a364...	4491	a92-122-50-170.d...	http	TIME_WAIT
[System Proc...	0	TCP	your-9c2b42a364...	4585	80-239-230-144.c...	http	TIME_WAIT
[System Proc...	0	TCP	your-9c2b42a364	4466	localhost	1110	TIME_WAIT
[System Proc...	0	TCP	your-9c2b42a364	4595	localhost	1110	TIME_WAIT
[System Proc...	0	TCP	your-9c2b42a364	1110	localhost	4836	TIME_WAIT
acs.exe	696	UDP	your-9c2b42a364	1025	*	*	
acs.exe	696	UDP	your-9c2b42a364	9977	*	*	
acs.exe	696	UDP	your-9c2b42a364	9877	*	*	
acs.exe	696	UDP	your-9c2b42a364	1028	*	*	

Wireshark

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

(Untitled) - Wireshark

File Edit View Go Capture Analyze Statistics Help

Filter: + Expression... Clear Apply

No. .	Time	Source	Destination	Protocol	Info
13	3.684027	AsustekC_16:09:67	Broadcast	ARP	Who has 10.8.0.23? Tell 10.8.1.20
14	4.005863	Giga-Byt_2a:6d:dd	Broadcast	ARP	Who has 10.8.0.2? Tell 10.8.1.122
15	4.006422	Giga-Byt_2a:6d:dd	Broadcast	ARP	Who has 10.8.1.234? Tell 10.8.1.122
16	4.021983	Cisco_0c:16:8b	Spanning-tree-(for-br	STP	Conf. Root = 32769/00:12:80:0c:16:80 Cost = 0 Port =
17	4.198393	10.8.1.111	10.8.1.255	NBNS	Name query NB 401_WOJCIK<00>
18	4.457166	Giga-Byt_26:fb:97	Broadcast	ARP	who has 10.8.0.2? Tell 10.8.0.221
19	4.833274	00000001.00a0d2133ff5	00000001.ffffffffffff	IPX RIP	Response
20	4.948417	10.8.1.111	10.8.1.255	NBNS	Name query NB 401_WOJCIK<00>
21	5.347255	10.8.0.90	10.8.0.2	DNS	Standard query AAAA www.onet.pl
22	5.347647	10.8.0.2	10.8.0.90	DNS	Standard query response
23	5.347694	10.8.0.90	10.8.0.2	DNS	Standard query AAAA www.onet.pl
24	5.347874	10.8.0.2	10.8.0.90	DNS	Standard query response
25	5.347905	10.8.0.90	10.8.0.2	DNS	Standard query A www.onet.pl
26	5.348216	10.8.0.2	10.8.0.90	DNS	Standard query response A 213.180.130.200
27	5.348319	10.8.0.90	213.180.130.200	TCP	34348 > www [SYN] Seq=0 Len=0 MSS=1460 TSV=1086275 TSEF
28	5.358254	213.180.130.200	10.8.0.90	TCP	www > 34348 [SYN, ACK] Seq=0 Ack=1 Win=5792 Len=0 MSS=:
29	5.358297	10.8.0.90	213.180.130.200	TCP	34348 > www [ACK] Seq=1 Ack=1 Win=5840 Len=0 TSV=10862:

▶ Frame 18 (60 bytes on wire, 60 bytes captured)

▶ Ethernet II, Src: Giga-Byt_26:fb:97 (00:0d:61:26:fb:97), Dst: Broadcast (ff:ff:ff:ff:ff:ff)

▼ Address Resolution Protocol (request)

- Hardware type: Ethernet (0x0001)
- Protocol type: IP (0x0800)
- Hardware size: 6
- Protocol size: 4
- Opcode: request (0x0001)

```
0000 ff ff ff ff ff ff 00 0d 61 26 fb 97 08 06 00 01 ..... a&.....
0010 08 00 06 04 00 01 00 0d 61 26 fb 97 0a 08 00 dd ..... a&.....
0020 00 00 00 00 00 00 0a 08 00 02 20 20 20 20 20 20 .....
0030 20 20 20 20 20 20 20 20 20 20 20 20
```

Address Resolution Protocol (arp), 28 bytes P: 173 D: 173 M: 0 Drops: 0

Process Explorer

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

The screenshot shows the Process Explorer window with the following data:

Process	PID	CPU	Description	Company Name	Virtual Size
System Idle Process	0	82.35			0 K
System	4	0.74			9 572 K
Interrupts	n/a	1.47	Hardware Interrupts and DPCs		0 K
smss.exe	840		Диспетчер сеанса Windows NT	Корпорация Майкрософт	3 812 K
csrss.exe	1448		Client Server Runtime Process	Microsoft Corporation	61 476 K
winlogon.exe	1472		Программа входа в систему Windows NT	Корпорация Майкрософт	56 424 K
services.exe	1520	0.74	Приложение служб и контроллеров	Корпорация Майкрософт	23 172 K
svchost.exe	1688		Generic Host Process for Win32 Services	Microsoft Corporation	61 560 K
igfxsrv.exe	3756		igfxsrv Module	Intel Corporation	24 972 K
wmiprvse.exe	208		WMI	Microsoft Corporation	37 912 K
svchost.exe	1772		Generic Host Process for Win32 Services	Microsoft Corporation	38 616 K
svchost.exe	1824		Generic Host Process for Win32 Services	Microsoft Corporation	152 400 K
wscntfy.exe	3020		Windows Security Center Notification App	Microsoft Corporation	27 700 K
svchost.exe	188		Generic Host Process for Win32 Services	Microsoft Corporation	31 936 K
spoolsv.exe	644		Spooler SubSystem App	Microsoft Corporation	51 376 K
acs.exe	696		ACS	Atheros	77 492 K
svchost.exe	832		Generic Host Process for Win32 Services	Microsoft Corporation	39 636 K
AppleMobileDeviceService.exe	1052		MobileDeviceService	Apple Inc.	52 892 K
avp.exe	1088		Kaspersky Anti-Virus	Kaspersky Lab	236 748 K
mDNSResponder.exe	1108		Bonjour Service	Apple Inc.	28 576 K
CFSvcs.exe	1132		Service of ConfigFree.	TOSHIBA CORPORATION	36 728 K
hasplms.exe	1252		Sentinel HASP License Manager Service	SafeNet Inc.	46 580 K
igs.exe					

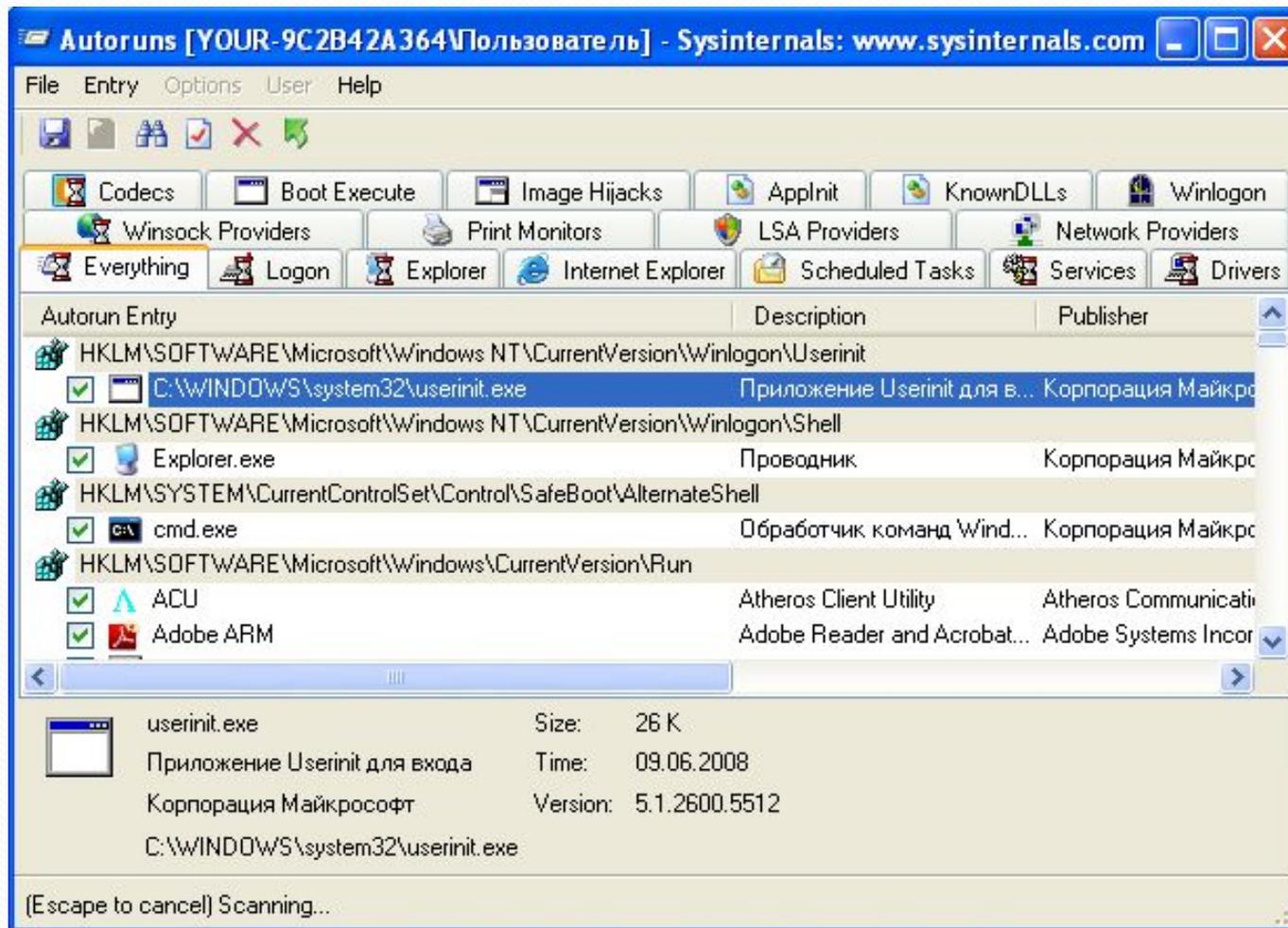
Below the process list, the 'Name' column shows the following paths:

Type	Name
Desktop	\Default
Directory	\KnownDlls
Directory	\Windows
Directory	\BaseNamedObjects
File	C:\WINDOWS\system32

At the bottom of the window, the status bar displays: CPU Usage: 17.65% | Commit Charge: 32.17% | Processes: 73

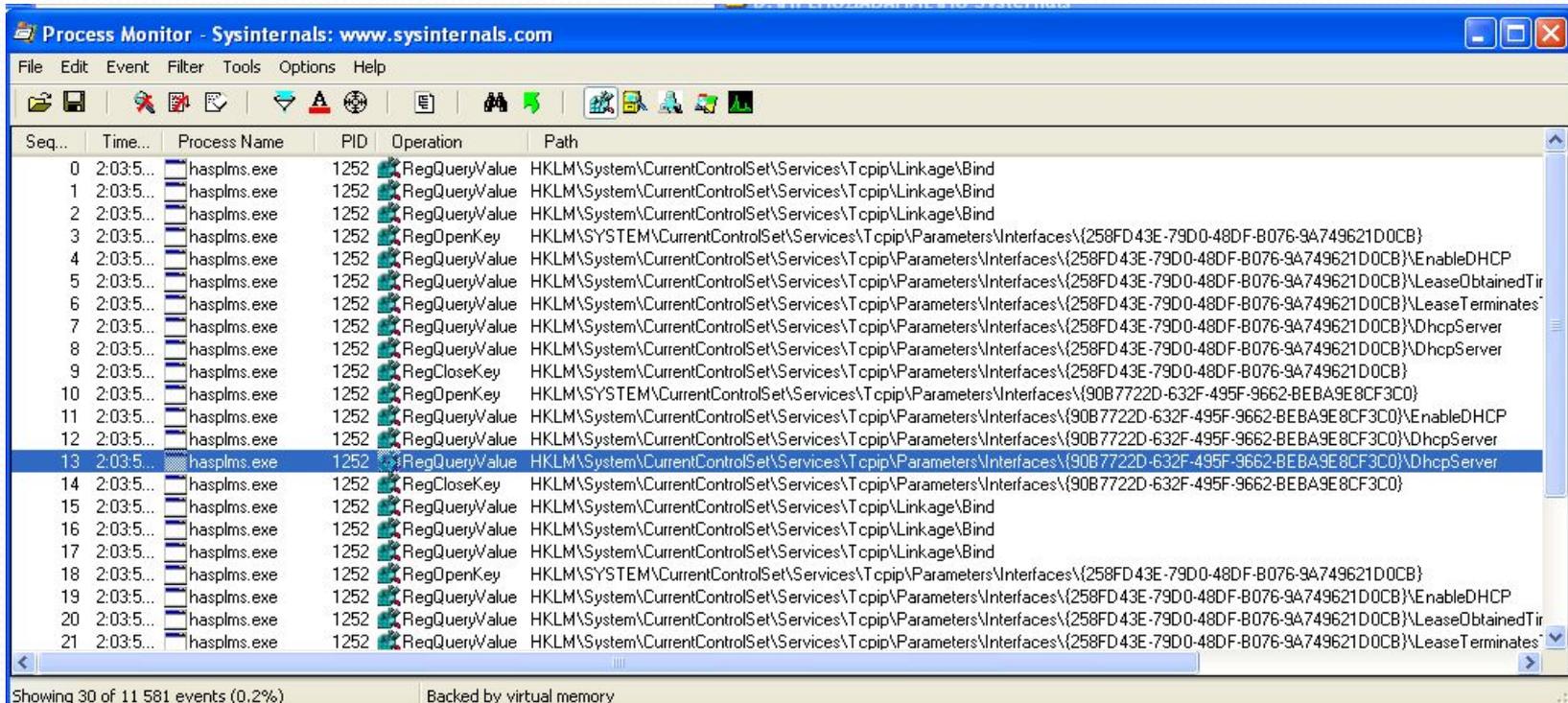
Autoruns

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.



The screenshot shows the Process Monitor application window with a list of 21 events. The columns are Seq., Time, Process Name, PID, Operation, and Path. The events show a sequence of registry operations performed by hasplms.exe (PID 1252). The operations include RegQueryValue, RegOpenKey, RegCloseKey, and RegOpenKey, all targeting paths under HKLM\System\CurrentControlSet\Services\Tcpip\Linkage\Bind and HKLM\System\CurrentControlSet\Services\Tcpip\Parameters\Interfaces.

Seq...	Time...	Process Name	PID	Operation	Path
0	2:03:5...	hasplms.exe	1252	RegQueryValue	HKLM\System\CurrentControlSet\Services\Tcpip\Linkage\Bind
1	2:03:5...	hasplms.exe	1252	RegQueryValue	HKLM\System\CurrentControlSet\Services\Tcpip\Linkage\Bind
2	2:03:5...	hasplms.exe	1252	RegQueryValue	HKLM\System\CurrentControlSet\Services\Tcpip\Linkage\Bind
3	2:03:5...	hasplms.exe	1252	RegOpenKey	HKLM\SYSTEM\CurrentControlSet\Services\Tcpip\Parameters\Interfaces\{258FD43E-79D0-48DF-B076-9A749621D0CB}
4	2:03:5...	hasplms.exe	1252	RegQueryValue	HKLM\System\CurrentControlSet\Services\Tcpip\Parameters\Interfaces\{258FD43E-79D0-48DF-B076-9A749621D0CB}\EnableDHCP
5	2:03:5...	hasplms.exe	1252	RegQueryValue	HKLM\System\CurrentControlSet\Services\Tcpip\Parameters\Interfaces\{258FD43E-79D0-48DF-B076-9A749621D0CB}\LeaseObtainedTir
6	2:03:5...	hasplms.exe	1252	RegQueryValue	HKLM\System\CurrentControlSet\Services\Tcpip\Parameters\Interfaces\{258FD43E-79D0-48DF-B076-9A749621D0CB}\LeaseTerminates
7	2:03:5...	hasplms.exe	1252	RegQueryValue	HKLM\System\CurrentControlSet\Services\Tcpip\Parameters\Interfaces\{258FD43E-79D0-48DF-B076-9A749621D0CB}\DhcpServer
8	2:03:5...	hasplms.exe	1252	RegQueryValue	HKLM\System\CurrentControlSet\Services\Tcpip\Parameters\Interfaces\{258FD43E-79D0-48DF-B076-9A749621D0CB}\DhcpServer
9	2:03:5...	hasplms.exe	1252	RegCloseKey	HKLM\System\CurrentControlSet\Services\Tcpip\Parameters\Interfaces\{258FD43E-79D0-48DF-B076-9A749621D0CB}
10	2:03:5...	hasplms.exe	1252	RegOpenKey	HKLM\SYSTEM\CurrentControlSet\Services\Tcpip\Parameters\Interfaces\{90B7722D-632F-495F-9662-BEBA9E8CF3C0}
11	2:03:5...	hasplms.exe	1252	RegQueryValue	HKLM\System\CurrentControlSet\Services\Tcpip\Parameters\Interfaces\{90B7722D-632F-495F-9662-BEBA9E8CF3C0}\EnableDHCP
12	2:03:5...	hasplms.exe	1252	RegQueryValue	HKLM\System\CurrentControlSet\Services\Tcpip\Parameters\Interfaces\{90B7722D-632F-495F-9662-BEBA9E8CF3C0}\DhcpServer
13	2:03:5...	hasplms.exe	1252	RegQueryValue	HKLM\System\CurrentControlSet\Services\Tcpip\Parameters\Interfaces\{90B7722D-632F-495F-9662-BEBA9E8CF3C0}\DhcpServer
14	2:03:5...	hasplms.exe	1252	RegCloseKey	HKLM\System\CurrentControlSet\Services\Tcpip\Parameters\Interfaces\{90B7722D-632F-495F-9662-BEBA9E8CF3C0}
15	2:03:5...	hasplms.exe	1252	RegQueryValue	HKLM\System\CurrentControlSet\Services\Tcpip\Linkage\Bind
16	2:03:5...	hasplms.exe	1252	RegQueryValue	HKLM\System\CurrentControlSet\Services\Tcpip\Linkage\Bind
17	2:03:5...	hasplms.exe	1252	RegQueryValue	HKLM\System\CurrentControlSet\Services\Tcpip\Linkage\Bind
18	2:03:5...	hasplms.exe	1252	RegOpenKey	HKLM\SYSTEM\CurrentControlSet\Services\Tcpip\Parameters\Interfaces\{258FD43E-79D0-48DF-B076-9A749621D0CB}
19	2:03:5...	hasplms.exe	1252	RegQueryValue	HKLM\System\CurrentControlSet\Services\Tcpip\Parameters\Interfaces\{258FD43E-79D0-48DF-B076-9A749621D0CB}\EnableDHCP
20	2:03:5...	hasplms.exe	1252	RegQueryValue	HKLM\System\CurrentControlSet\Services\Tcpip\Parameters\Interfaces\{258FD43E-79D0-48DF-B076-9A749621D0CB}\LeaseObtainedTir
21	2:03:5...	hasplms.exe	1252	RegQueryValue	HKLM\System\CurrentControlSet\Services\Tcpip\Parameters\Interfaces\{258FD43E-79D0-48DF-B076-9A749621D0CB}\LeaseTerminates

Showing 30 of 11 581 events (0.2%)

Backed by virtual memory

Спасибо за внимание