1. Министерство образования и науки Российской Федерации
2. Санкт-Петербургский Политехнический Университет Петра Великого
3. —
4. Институт кибербезопасности и защиты информации

**ЛАБОРАТОРНАЯ РАБОТА № 4**

**«ФАЙЛОВЫЕ СИСТЕМЫ»**

по дисциплине «Операционные системы»

1. Выполнил
2. студент гр. 4851003/10002 Галкин К. К.

1. Руководитель
2. К. т. н. Крундышев В. М.

Санкт-Петербург

2023

1. **ЦЕЛЬ РАБОТЫ**

Цель работы — изучение способов структуризации и организации

хранения данных на дисковых носителях, используемых в современных

операционных системах (ОС).

1. **ЗАДАЧИ**

* Проанализировать полученные RAW-дампы жестких дисков на предмет разделов. Расписать для каждого информацию, необходимую по заданию.
* Изучить снимок диска с ФС FATzz. Составить подробную таблицу для всех объектов на диске
* Изучить диск с ФС NTFS. Восстановить структуру объектов, проанализировать эти объекты. Результаты занести в таблицу
* Рассмотреть файловые системы ОС Linux и ОС FreeBSD. Расшифровать суперблок, восстановить структуру каталогов, описание объектов занести в таблицу.

1. **ХОД РАБОТЫ**
   1. **Часть первая. Разделы диска**

Для выполнения этой части лабораторной работы использовались следующие инструменты: терминальная команда fdisk в Ubuntu и AutoPsy.

Пример работы программ можно наблюдать на следующем рисунке:

Изображение выглядит как текст, электроника, снимок экрана, программное обеспечение

Автоматически созданное описание

Результаты работы представлены в таблице ниже:

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| Файл дампа | № раздела | ФС / Потенциальная ФС | Начало | Размер | Примечание |
| disk\_11.raw  Disk identifier: 0x63d3917f | 1 | DOS FAT16 | 2048 | 20480 | active, ID=0x04 |
| 2 | Linux | 22528 | 18432 | ID=0x83 |
| 3 | OpenBSD | 40960 | 12288 | ID=0xa6 |
| 4 | AIX Boot | 53248 | 22528 | ID=0x08 |
| disk\_12.raw  Disk identifier: 0x8bcd85dc | 1 | NTFS / exFAT | 2048 | 6144 | ID=0x07  Основной |
| 2 | BSD/386, 386BSD, NetBSD, FreeBSD | 98304 | 8192 | ID=0xa5  Основной |
| 5 | BeOS BFS | 10240 | 6144 | ID=0xeb  Логический |
| 6 | Unknown Type | 18432 | 8192 | ID=0xbf, The Solaris fdisk partition  Логический |
| 7 | BeOS BFS | 28672 | 6144 | ID=0xeb  Логический |
| 8 | Linux Swap / Solaris x86 | 36864 | 10240 | ID=0x82  Логический |
| 9 | EFI File System | 49152 | 12288 | ID=0xef  Логический |
| 10 | DOS FAT16 | 63488 | 10240 | ID=0x06  Логический |
| 11 | Mac OS X | 75776 | 8192 | ID=0xa8  Логический |
| 12 | NetBSD | 86016 | 8192 | ID=0xa9  Логический |
| disk\_13.raw  Disk identifier: 793078EB-FB25-465A-953D-A353012B49AC | GPTPart3 | FreeBSD swap | 2048 | 6144 | Type-UUID: 516E7CB5-6ECF-11D6-8FF8-00022D09712B |
| GPTPart2 | FreeBSD ZFS | 8192 | 16384 | Type-UUID: 516E7CBA-6ECF-11D6-8FF8-00022D09712B |
| GPTPart1 | FreeBSD swap | 24576 | 22528 | Type-UUID: 516E7CB5-6ECF-11D6-8FF8-00022D09712B |
| GPTPart8 | NetBSD FFS | 47104 | 12288 | Type-UUID: 49F48D5A-B10E-11DC-B99B-0019D1879648 |
| GPTPart5 | Apple TV recovery | 59392 | 12288 | Type-UUID: 5265636F-7665-11AA-AA11-00306543ECAC |
| GPTPart6 | Solaris backup | 71680 | 14336 | Type-UUID: 6A8B642B-1DD2-11B2-99A6-080020736631 |
| GPTPart0 | Solaris boot | 86016 | 20480 | Type-UUID: 6A82CB45-1DD2-11B2-99A6-080020736631 |
| GPTPart4 | FreeBSD ZFS | 106496 | 24576 | Type-UUID: 516E7CBA-6ECF-11D6-8FF8-00022D09712B |
| GPTPart7 | NetBSD FFS | 131072 | 18432 | Type-UUID: 49F48D5A-B10E-11DC-B99B-0019D1879648 |
| Защищенный раздел MacOS RAID | Apple RAID | 149504 | 14336 | Type-UUID: 52414944-0000-11AA-AA11-00306543ECAC |
| disk\_14.raw | a | 4.4LFS | 16 | 12256 | Раздел |
| b | Swap | 12272 | 6560 | Раздел |
| c | Unused | 0 | 39392 | Пустое пространство |
| d | Unknown | 18832 | 4704 | Раздел |
| e | Unknown | 23536 | 6208 | Раздел |
| f | ISO-9660 | 29744 | 5568 | Раздел |

* 1. **Часть вторая. Файловые системы**

Информацию о ФС FAT32 можно найти на скриншоте ниже:

**Изображение выглядит как текст, снимок экрана, число, программное обеспечение

Автоматически созданное описание**

Из этих данных можно выделить OEM ID – MSDOS5.0, а так же тип ФС – FAT32 и сигнатура загрузочного диска (байты 0x55 0xAA)

Процесс получения этих данных был автоматизирован через R-Studio, однако стоит упомянуть, как эти данные можно получить без использования утилит – просмотр байтов через HxD или любой другой хексовые редактор. Пример работы:

Изображение выглядит как текст, снимок экрана, Шрифт, информация

Автоматически созданное описание

Информация обо всех объектах представлена в таблице ниже:

|  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- |
| Путь | Тип | Атрибуты | Размер | Создан | Изменен | Кластеры |
| \PHOTOED | Dir | -H-- |  |  |  | 0 |
| \PHOTOED\ILLMNTR | Dir | ---- |  |  |  | 0 |
| \PHOTOED\ILLMNTR\SHELF | Dir | -H-- |  |  |  | 0 |
| \PHOTOED\ILLMNTR\SHELF\PAGE-3.JPG | File | -HS- | 1.52 KB | 27.05.2002 7:01 | 22.12.2012 10:15 | 86-88 |
| \PHOTOED\ILLMNTR\TURNS | Dir | -HS- |  |  |  | 0 |
| \PHOTOED\ILLMNTR\PHOTO01.JPG | File | -HS- | 6.57 KB | 05.04.2012 15:10 | 25.12.2006 21:30 | 35-38 62-65 94 |
| \PHOTOED\SPECS | Dir | A-S- |  |  |  | 0 |
| \PHOTOED\SPECS\DBS | Dir | ---- |  |  |  |  |
| \PHOTOED\SPECS\DIR.CNF | File | ---- | 6.72 KB | 07.05.2008 10:34 | 16.11.2019 18:05 | 71-76 95-97 |
| \PHOTOED\SPECS\umělá.txt | File | AHS- | 11.1 KB | 02.06.1984 10:10 | 04.03.1992 18:11 | 91-94 97-101 127-129 |
| \System Volume Information | Dir | -HS- |  |  |  | 0 |
| \System Volume Information\IndexerVolumeGrid | File | A--- | 76 | 01.04.2018 3:00 | 01.04.2018 3:00 | 156 |
| \System Volume Information\WPSettings.dat | File | A--- | 12 | 01.04.2018 3:00 | 01.04.2018 3:00 | 19 |
| \UI | Dir | --S- |  |  |  | 0 |
| \UI\FETCH.TXT | File | --S- | 95 | 20.10.1985 15:27 | 18.02.1983 4:21 | 38 |
| \WINDOW | Dir | ---- |  |  |  | 0 |
| \WINDOW\Kiristдjд | Dir | ---- |  |  |  | 0 |
| \WINDOW\Kiristдjд\OSDEV | Dir | -H-- |  |  |  | 0 |
| \WINDOW\Kiristдjд\OSDEV\DATA.DB2 | File | --S- | 9.53KB | 24.06.2011 9:27 | 24.05.2019 15:31 | 51-55 65-66 82-86 |
| \WINDOW\Kiristдjд\WHEEL | Dir | -HS- |  |  |  | 0 |
| \WINDOW\Kiristдjд\WHEEL\PHONSFT | Dir | A-S- |  |  |  | 0 |
| \WINDOW\Kiristдjд\WHEEL\ πισίνα.txt | File | AHS- | 846 | 13.12.1989 17:37 | 23.04.2000 15:04 | 43 |
| \WINDOW\Kiristдjд\WHEEL\ausgewдhlten.txt | File | ---- | 8.11 KB | 21.02.1992 19:58:52 | 08.12.1990  17:18:38 | 39-43 67-71 76 |
| \WINDOW\Kiristдjд\WHEEL\CAPTURE.TXT | File | ---- | 9.29 KB | 19.09.2015 12:58 | 27.03.2009 18:55 | 4-10 28-32 |
| \WINDOW\Kiristдjд\WHEEL\SETUP.BIN | File | AH-R | 41.0 KB | 15.08.2005 2:53 | 10.02.2018 0:12 | 11–15  20–24  32–35  55–62  77–82  88–91  101–105  110–122 |
| CLEAR.SH | File | --S- | 37.9KB | 25.05.2019 3:48 | 24.12.2013 5:07 | 45–49  105–110  122–127  132–156 |

Пример получения списка кластеров для файла SETUP.BIN:

Изображение выглядит как текст, снимок экрана, программное обеспечение, Значок на компьютере

Автоматически созданное описание

В процессе решения было два возможных события: использование Active Disk Editor или дефрагментация сырых байтов и определение кластеров внутри фрагментов. Первый способ оказался намного проще, поэтому было принято решение работать с этим диском через названную утилиту. Более того, она показывает атрибуты файлов, даты создания и т. д.

Изображение выглядит как снимок экрана, программное обеспечение, текст, Значок на компьютере

Автоматически созданное описание

**Теперь разберем диск с ФС NTFS.**

Расшифровка EBP и Extended EBP представлена ниже:

Изображение выглядит как текст, снимок экрана, число, программное обеспечение

Автоматически созданное описание

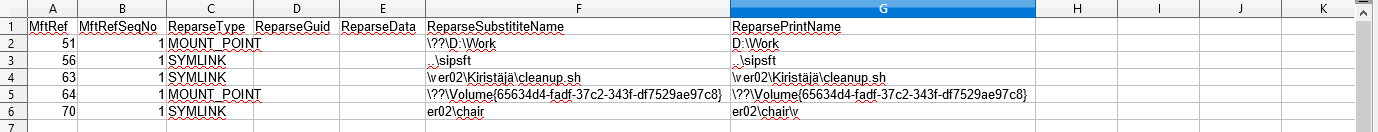
Файловая иерархия:

|  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- |
| Путь | Тип | Размер | Атрибуты | Создан | Изменен | Жестких ссылок | Номер в $MFT | Номера кластеров |
| \$Extend | Dir |  | HS |  |  |  | 11 |  |
| \$Extend\$Deleted | Dir |  | HS |  |  |  | 29 |  |
| \$Extend\$RmMetadata | Dir |  | HS |  |  |  | 27 |  |
| \$Extend\$RmMetadata\$Txf | Dir |  | HS |  |  |  | 31 |  |
| \$Extend\$RmMetadata\$TxfLog | Dir |  | HS |  |  |  | 30 |  |
| \$Extend\$RmMetadata\$TxfLog\$Tops | File | 0 | HSA | 01.04.2018 3:43 | 01.04.2018 3:43 | 1 | 32 | 0 |
| \$Extend\$RmMetadata\$TxfLog\$TxfLog.blf | File | 64.0 KB | A | 01.04.2018 3:43 | 01.04.2018 3:43 | 1 | 33 | 951-967 |
| \$Extend\$RmMetadata\$TxfLog\$TxfLogContainer00000000000000000001 | File | 2.0 MB | A | 01.04.2018 3:43 | 01.04.2018 3:43 | 1 | 34 | 967-1479 |
| \$Extend\$RmMetadata\$TxfLog\$TxfLogContainer00000000000000000002 | File | 2.0 MB | A | 01.04.2018 3:43 | 01.04.2018 3:43 | 1 | 35 | 1479-1991 |
| \$Extend\$RmMetadata\$Repair | File | 0 | HSA | 01.04.2018 3:43 | 01.04.2018 3:43 | 1 | 28 | 0 |
| \$Extend\$ObjId | File | 0 | HSA | 01.04.2018 3:43 | 01.04.2018 3:43 | 1 | 25 | 0 |
| \$Extend\$Quota | File | 0 | HSA | 01.04.2018 3:43 | 01.04.2018 3:43 | 1 | 24 | 0 |
| \$Extend\$Reparse | File | 0 | HSA | 01.04.2018 3:43 | 01.04.2018 3:43 | 1 | 26 | 0 |
| \inwork | Dir |  | H |  |  |  | 36 |  |
| \inwork\ošklivá.txt | File | 8.18 KB | - | 21.11.2013 11:36 | 14.02.2006 6:06 | 1 | 50 | 2006  2035  2365 |
| \inwork\pack.pkz | File | 31 | RSA | 19.09.2017 1:46 | 12.09.2008 5:32 | 2 | 40 | 24134032-24134063 |
| \sipsft | Dir |  | SA |  |  |  | 48 |  |
| \sipsft\brake | Dir, link |  | HI |  |  |  | 70 |  |
| \sipsft\drivers | Dir, link |  | RI |  |  |  | 56 |  |
| \sipsft\utils | Dir, link |  | - |  |  |  | 51 |  |
| \sipsft\support | Dir |  | HA |  |  |  | 54 |  |
| \sipsft\support\citybus | Dir |  | HA |  |  |  | 62 |  |
| \sipsft\support\citybus\police | Dir |  | HS |  |  |  | 66 |  |
| \sipsft\support\citybus\police\capture.txt | File | 177.0 KB | A | 12.10.1994 11:02 | 10.12.1983 22:04 |  | 69 | 2866-2868  2870-2872  2886  2889  2891  2893-2895  2899-2901  2909  2911  2930  2934-2936  2943  2945  2947  2949  2953-2955  2956  2958-2980 |
| \sipsft\support\citybus\police\content.txt | File | 10.2 KB | - | 22.10.1981 13:29 | 13.06.1992 17:43 | 1 | 68 | 2859-2861  2890 |
| \sipsft\support\citybus\data.myd | File | 5.27 KB | RHAI | 08.02.1986 4:29 | 20.09.1993 9:54 | 4 | 60 | 2046  2337 |
| \sipsft\support\citybus\free.dc | File | 125.0 KB | RSAI | 10.06.2016 13:11 | 04.01.1980 7:58 | 2 | 65 | 2366 – 2368  2376 – 2378  2868  2884 – 2886  2896 – 2899  2902  2904  2906  2910  2931 – 2934  2936 – 2943  2944  2946  2948  2950–2953 2955 |
| \sipsft\support\check.sh | File | 2.07 MB | A | 01.04.2018 3:43 | 01.04.2018 3:43 | 1 | 67 | 2379-2459  2459-2859 |
| \sipsft\support\upload.sh | File | 1.49 MB | A | 01.04.2018 3:43 | 01.04.2018 3:43 | 1 | 61 | 2048-2128  2128-2256  2256-2336 |
| \sipsft\zip.txt | File | 5.27 KB | RHAI | 08.02.1986 4:29 | 20.09.1993 9:54 | 4 | 60 | 2046  2337 |
| \System Volume Information | Dir |  | HS | 01.04.2018 3:43 | 01.04.2018 3:43 |  | 37 |  |
| \System Volume Information\IndexerVolumeGuid | File | 76 | A | 01.04.2018 3:43 | 01.04.2018 3:43 | 1 |  | 24166704-24166780 |
| \System Volume Information\MountPointManagerRemoteDatabase | File | 0 | HSA | 01.04.2018 3:43 | 01.04.2018 3:43 | 0 | 71 | 0 |
| \System Volume Information\WPSettings.dat | File | 12 | A | 01.04.2018 3:43 | 01.04.2018 3:43 | 1 | 39 | 24132904-24132916 |
| \ver02 | Dir |  | A |  |  |  | 38 |  |
| \ver02\chair | Dir |  | HA |  |  |  | 41 |  |
| \ver02\chair\tesing | Dir |  | - |  |  |  | 43 |  |
| \ver02\chair\tesing\ausgewдhlten.txt | File | 8.57 KB | AI | 10.05.2012 1:19 | 12.04.2004 6:59 | 1 | 46 | 2002-2004  2047 |
| \ver02\chair\tesing\base.url | File | 102 KB | AC | 25.10.1987 16:45 | 23.07.1996 12:30 | 1 | 44 | 1993-1997  2862-2864 |
| \ver02\chair\ver01 | Dir |  | - |  |  |  | 64 |  |
| \ver02\Kiristдjд | Dir |  | - |  |  |  | 45 |  |
| \ver02\Kiristдjд\bonnet\ | Dir |  | S |  |  |  | 53 |  |
| \ver02\Kiristдjд\bonnet\install.cmd | File | 27 | - | 10.03.1993 2:34 | 20.05.1988 7:42 | 1 | 55 | 24149280-24149307 |
| \ver02\Kiristдjд\bonnet\people.txt | File | 11.7 KB | A | 14.07.2011 1:45 | 18.04.2003 16:30 | 1 | 59 | 2044-2046  2378 |
| \ver02\Kiristдjд\bonnet\variables.txt | File | 125 KB | RSAI | 10.06.2016 13:11 | 04.01.1980 7:58 | 2 | 65 | 2366-2368  2376-2378  2868  2884-2886  2896-2899  2902  2904  2906  2910  2931-2934  2936-2943  2944  2946  2948  2950-2953  2955  2957 |
| \ver02\Kiristдjд\cleanup.sh | File | 60.1 KB | RHS | 12.11.1992 7:11 | 22.11.2001 1:38 | 1 | 47 | 2004-2006  2007  2336  2368  2375  2887-2889  2892  2895  2901  2903  2905  2907-2909  2912 |
| \ver02\Kiristдjд\download.sh | File | 31 | RSA | 19.09.2017 1:46 | 12.09.2008 5:32 | 2 | 40 | 24134032-14134063 |
| \ver02\Kiristдjд\page05.jpg | File | 6.99 KB | HS | 25.04.1994 21:37 | 15.04.1982 10:28 | 1 | 58 | 2043  2869 |
| \ver02\Kiristдjд\κρεβάτια.txt | File | 1.36 KB | RHSA | 16.08.1990 7:22 | 01.03.1990 7:22 | 1 | 52 | 2008 |
| \ver02\lock | Dir |  | S |  |  |  | 42 |  |
| \ver02\lock\boot | Dir |  | - |  |  |  | 49 |  |
| \ver02\lock\boot\clear.sh | File | 91.8 KB | C | 20.10.2003 11:26 | 14.02.2015 7:03 | 1 | 57 | 2036-2040  2363-2365 |
| \ver02\lock\boot\photo03.jpg | File | 5.27 KB | RHAI | 08.02.1986 4:29 | 20.09.1993 9:54 | 4 | 60 | 2046  2337 |
| \ver02\lock\boot\values.txt | Link |  | R |  |  |  | 63 |  |
| \ver02\repack.sh | File | 5.27 KB | RHAI | 08.02.1986 4:29 | 20.09.1993 9:54 | 4 | 60 | 2046  2337 |

Как можно заметить, в процессе парсинга иерархии было несколько ссылок. Одна из них – рекурсивная в саму себя, а вторая – пустая. Пример работы команды dir в Windows

Изображение выглядит как текст, снимок экрана, черный

Автоматически созданное описание



Описатели безопасности всех объектов хранятся в специальном файле $Secure. Файл хранит все уникальные описатели, их количество значительно меньше, чем количество объектов в разделе NTFS, поскольку разрешения дочерних объектов почти всегда наследуются от родительских каталогов. Каждый уникальный описатель безопасности имеет собственный уникальный идентификатор (SecurityId). Идентификатор описателя безопасности хранится по номеру в соответствующем поле атрибута объекта $STANDART\_INFORMATION.

Для определения описателей безопасности нужно посмотреть структуры атрибутов $SII и $SDH внутри файла $Secure. Пример битмапа для атрибута SDH представлен ниже(выделен темным цветом). Как можно заметить, биты внутри мапа нулевые, то есть описатели не установлены (не используются). Это подтверждают различные парсеры $Secure – структур.

Изображение выглядит как текст, снимок экрана, число, Шрифт

Автоматически созданное описание

Изображение выглядит как текст, снимок экрана, число, программное обеспечение

Автоматически созданное описание

У некоторых файлов есть дополнительные нестандартные NTFS-потоки данных. Через AutoPsy были найдены файлы с такими потоками (cleanup.sh и κρεβάτια.txt):

Изображение выглядит как текст, Шрифт, снимок экрана

Автоматически созданное описание

Изображение выглядит как текст, снимок экрана, документ

Автоматически созданное описание

Изображение выглядит как текст, снимок экрана

Автоматически созданное описание

Для нахождения дополнительных (расширенных) атрибутов нужно проверить атрибут $EA (тип 0xE0). В таком случае атрибут считается расширенным. В текущем диске существует несколько файлов с такими атрибутами:

|  |  |
| --- | --- |
| Файл | Атрибут |
| ošklivá.txt | $E0 |
| ausgewдhlten.txt | $E0 |

Атрибуты можно найти либо через AutoPsy, либо через Active Disk Editor. Ниже пример нахождения использования атрибута $EA внутри файла ausgewдhlten.txt

Изображение выглядит как текст, снимок экрана

Автоматически созданное описание

**Файловая система ext2/3/4:**

В R-Studio видим, что текущая ФС семейства ext:

Изображение выглядит как текст, снимок экрана, число, чек

Автоматически созданное описание

Значит, для расшифровки суперблока нам нужно посмотреть смещение 0x400 относительно диска. Основная информация о блоке представлена ниже:

Изображение выглядит как текст, снимок экрана, число, дисплей

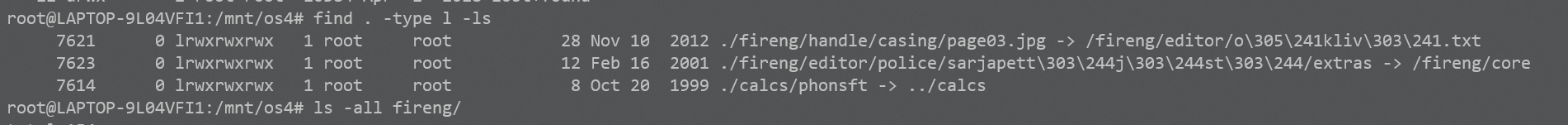
Автоматически созданное описание

* Block size – 1
* Block count – 45568
* Inode count – 22800
* Free inodes count – 22761

Структура каталогов диска представлена в таблице ниже

|  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- |
| Название | Inode | Тип, размер | Владелец  Группа | Атрибуты | Дата модификации | Дата обновления | Номера блоков | Количество жестких ссылок |
| \calcs | 7601 | Dir, 2048 | 8/2 | d----w-r-x | 1980-10-18 21:22:39 | 2002-06-22 21:00:40 | - | - |
| \calcs\photo1.jpg | 7610 | File, 9629 | 0/11 | rr-xr--rw- | 1996-05-16 07:03:00 | 2008-03-06 00:44:18 | 4168-4280 | 4 |
| \calcs\phonsft | 7614 | Link, 8 | 0/0 | lrwxrwxrwx | 1999-10-20 00:26:45 | 2003-12-01 21:16:11 | - | 1 |
| \fireng | |  | | --- | | 7602 | | Dir, 2048 | 4/27 | |  | | --- | | d-wx--x-wx | | |  | | --- | | 2008-06-13 05:07:34 | | |  |  | | --- | --- | |  | 2006-09-26 17:13:16 | | - | 5 |
| \fireng\capture.txt | 7605 | File, 7203 | 4/0 | |  | | --- | | rrwxr---w- | | |  |  | | --- | --- | |  | 1991-09-02 03:58:47 | | |  |  | | --- | --- | |  | 2013-07-13 13:32:09 | | 4136-4196  4288-4292 | 1 |
| \fireng\page05.jpg | 7604 | File, 129538 | 17/18 | |  | | --- | | r---rw---- | | |  | | --- | | 1998-09-08 01:41:33 | | |  |  | | --- | --- | |  | 2010-04-22 18:13:38 | | 4124-4136  4284-4288  4292-4308  …  16124-16128 | 1 |
| \fireng\rebuild.sh | 7603 | File, 5077 | 15/7 | rr-x-w--wx | 1984-07-27 20:39:30 | 1994-10-23 08:39:15 | 4108-4116  4156-4160 | 2 |
| \fireng\core | 7608 | Dir,  2048 | 1/41 | dr-xrw-rwx | 2011-11-16 09:21:37 | 2001-07-15 20:53:47 | - | 3 |
| \fireng\core\content.txt | 7625 | File, 191 | 4/39 | r--x-wxrwx | 1981-06-05 11:10:03 | 1994-09-27 20:14:32 | 4316-4320 | 2 |
| /fireng/core/illmntr | 7612 | Dir, 2048 | 10/17 | |  | | --- | | d---r---w- | | 2017-06-16 06:43:48 | 2016-04-22 21:55:50 | - | 2 |
| fireng/core/illmntr/values.txt | 7610 | File, 9629 | 0/11 | rr-xr--rw- | 1996-05-16 07:03:00 | 2008-03-06 00:44:18 | 4168-4176  4228-4332  4268-4272  4276-4280 | 4 |
| fireng/editor | 7606 | Dir, 2048 | 7/4 | dr-x---rwx | 1990-01-09 05:14:45 | 1990-03-05 01:17:50 | - | 3 |
| fireng/editor/ošklivá.txt | 7610 | File, 9629 | 0/11 | rr-xr--rw- | 1996-05-16 07:03:00 | 2008-03-06 00:44:18 | 4168-4176  4228-4332  4268-4272  4276-4280 | 4 |
| fireng/editor/pack.pkz | 7607 | File, 6281 | 18/15 | |  | | --- | | rr--rwx-w- | | 2014-08-22 06:41:50 | 2002-09-02 09:34:02 | 4148-4156  4184-4192 | 1 |
| fireng/editor/police | 7609 | Dir, 2048 | 8/29 | d---rw-r-x | 1994-06-14 01:55:03 | 1995-08-12 12:06:04 | - | 3 |
| fireng/editor/police/sarjapettдjдstд | 7622 | Dir, 2048 | 20/32 | d-w-r----- | 1983-06-02 16:01:26 | 1994-06-14 01:55:03 | - | 2 |
| fireng/editor/police/sarjapettдjдstд/check.sh | 7625 | File, 191 | 4/39 | r--x-wxrwx | 1981-06-05 11:10:03 | 1994-09-27 20:14:32 | 4316-4320 | 2 |
| fireng/editor/police/sarjapettдjдstд/ασφαλείας.txt | 7626 | File, 1965 | 0/18 | |  | | --- | | rrwxr-x-w- | | 2004-11-05 15:30:58 | 1983-06-02 16:01:26 | 4320-4324 | 1 |
| fireng/editor/police/sarjapettдjдstд/extras | |  | | --- | | 7623 | | Link, 12 | 0/0 | lrwxrwxrwx | 2001-02-16 20:58:11 | 1989-12-05 13:54:45 | - | 1 |
| /fireng/handle | 7611 | Dir, 2048 | 14/1 | drw-r-xrw- | 1982-10-22 01:28:57 | 2008-06-13 05:07:34 | - | 3 |
| /fireng/handle/niño.txt | 7616 | File, 9381 | 5/26 | rr----xrwx | 1989-09-18 04:22:17 | 1982-10-22 01:28:57 | 4176-4184  4244-4256 | 1 |
| fireng/handle/casing | 7615 | Dir, 2048 | 6/39 | drw----rw- | 2008-07-08 21:45:48 | 2005-01-06 13:54:59 | - | 3 |
| fireng/handle/casing/copyall.sh | 7619 | File, 87561 | 13/2 | r--xrwx--x | 1999-02-09 21:24:59 | 1988-03-02 17:13:35 | 168 блоков, начало -4208 | 1 |
| fireng/handle/casing/init.sh | 7618 | File, 16 | 17/40 | rr-x-w--wx | 1992-09-09 02:29:44 | 1990-10-16 17:33:45 | 4204-4208 | 1 |
| fireng/handle/casing/pack.sh | 7620 | File, 5032 | 7/1 | rr--rwx-w- | 1991-07-27 00:38:52 | 1991-10-22 01:01:49 | 4216-4228 | 1 |
| fireng/handle/casing/page03.jpg | 7621 | Link, 28 | 0/0 | lrwxrwxrwx | 2012-11-10 00:01:31 | 2018-01-22 01:46:35 | - | 1 |
| fireng/handle/casing/validate.txt | 7603 | File, 5077 | 15/7 | rr-x-w--wx | 1984-07-27 20:39:30 | 1994-10-23 08:39:15 | 4108-4116  4156-4160 | 2 |
| fireng/handle/casing/clients | 7624 | Dir, 2048 | 18/8 | drw-r-x--- | 2002-12-22 22:31:22 | 2008-07-08 21:45:48 | - | 2 |
| fireng/handle/casing/clients/get.txt | 7610 | File, 9629 | 0/11 | rr-xr--rw- | 1996-05-16 07:03:00 | 2008-03-06 00:44:18 | 4168-4176  4228-4232  4268-4272  4276-4280 | 4 |
| |  | | --- | | /lost+found | | 11 | Dir, 16384 | 0/0 | drwx------ | 2018-04-01 16:19:22 | 2018-04-01 16:19:22 | - | 2 |
| /data.myd | 12 | File, 149926 | 11/10 | rr-----rw- | 2007-06-19 05:34:19 | 2012-03-14 22:20:29 | 222 блока, начало - 4096 | 1 |

Для определения значения ссылок можно было использовать плагины AutoPsy, или find на монтированный в Linux тестовый диск. Результат работы утилиты:



**Файловая система ОС FreeBSD:**

Информация о суперблоке в этой ФС должна лежать по смещению 0x10000, однако там пустой сектор. Через Active Disk Editor открываем весь дамп в байтовом виде и прыгаем по 4 сектора с шаблоном “UFS Superblock”. В конце концов, обнаруживаем необходимую информацию на смещении 0x00065536

Изображение выглядит как текст, снимок экрана, программное обеспечение, число

Автоматически созданное описание

Отсюда можно выяснить недостаток: Active Disk Editor не сможет прочитать ФС, т.к стартовые значения суперблока сбиты. Поэтому будем использовать AutoPsy для этого.

Иерархия файлов представлена ниже:

|  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- |
| Название | Inode | Тип, размер | Владелец  Группа | Атрибуты | Дата модификации | Дата обновления | Количество жестких ссылок |
| /.snap/ | 3 | Dir, 512 | 0/5 | drwxrwxr-x | 2002-01-02 09:18:45 | 2002-01-02 09:18:45 | 2 |
| /note02.avi | 5 | File, 116958 | 10/19 | rr-x-wxrw- | 2010-11-24 02:45:50 | 1993-10-13 21:59:01 | 1 |
| /χώρου.txt | 6 | File, 709 | 2/45 | rrwxrwx-w- | 2020-01-10 13:56:09 | 2004-11-24 05:15:24 | 1 |
| /casing | 1872 | Dir, 512 | 18/21 | d-w--w-rwx | 2015-04-04 17:11:30 | 2004-04-18 01:06:51 | 5 |
| /casing/bumper | 1888 | Link, 9 | 0/0 | lrwxr-xr-x | 2001-03-01 18:13:53 | 2001-03-01 18:13:53 | 1 |
| /casing/cleanup.sh | 1878 | File, 7932 | 5/14 | rr--r-xr-x | 2004-04-03 08:26:39 | 1994-03-10 10:21:51 | 2 |
| /casing/note01.avi | 1876 | File, 106 | 7/48 | r-wxr--rwx | 1992-05-28 09:22:19 | 2017-01-12 12:28:29 | 1 |
| /casing/inwork | 1883 | Dir, 512 | 17/29 | d--xrw---x | 2016-05-21 14:06:53 | 1985-05-28 23:14:35 | 2 |
| /casing/inwork/data.dbi | 1887 | File, 94 | 16/33 | rr-------x | 2000-08-03 02:09:48 | 2016-05-21 14:06:53 | 1 |
| /casing/links | 1879 | Dir, 512 | 18/8 | drwxr--r-x | 2009-01-01 04:10:56 | 2005-12-11 01:07:03 | 3 |
| /casing/links/dbs | 1880 | Dir, 512 | 11/7 | d-w--wxrw- | 2003-04-03 11:07:55 | 2009-01-01 04:10:56 | 3 |
| /casing/links/dbs/Cože.txt | 1882 | File, 7931 | 5/42 | r------rwx | 1993-04-13 08:28:48 | 2003-06-24 00:34:44 | 4 |
| /casing/links/dbs/file01.jpg | 1889 | Link, 27 | 0/0 | lrwxr-xr-x | 1980-07-15 01:47:25 | 1980-07-15 01:47:25 | 1 |
| /casing/links/dbs/install.cmd | 1895 | File, 161065 | 4/46 | rr----xrw- | 1981-05-18 20:12:03 | 2007-01-18 17:41:39 | 2 |
| /casing/links/dbs/photoed | 1884 | Dir, 512 | 4/30 | |  | | --- | | drwxr--r-x | | 1997-08-21 21:13:59 | 2019-06-28 04:41:03 | 2 |
| /casing/links/dbs/photoed/note03.avi | 1885 | File, 11153 | 7/9 | rr--r--rwx | 2010-09-23 13:14:23 | 2015-06-19 01:29:19 | 1 |
| /casing/links/dbs/photoed/scan.vld | 1892 | File, 11213 | 1/17 | rrw--wx-wx | 1991-05-13 05:10:28 | 2011-05-18 20:10:59 | 1 |
| /casing/links/dbs/photoed/totiž.txt | 1890 | File, 9348 | 12/30 | rr-x---r-- | 1982-02-14 18:49:35 | 1994-10-07 05:51:38 | 1 |
| /casing/links/dbs/photoed/values.txt | 1882 | File, 7931 | 5/42 | r------rwx | 1993-04-13 08:28:48 | 2003-06-24 00:34:44 | 4 |
| /casing/stand | 1873 | Dir, 512 | 15/10 | drwxrwxrwx | 1999-09-11 07:03:46 | 1985-01-13 01:57:21 | 5 |
| /casing/stand/brake | 1874 | Dir, 512 | 13/31 | d-----x-wx | 2017-08-18 19:12:46 | 2007-02-12 05:30:53 | 2 |
| /casing/stand/brake/pack.pkz | 1882 | File, 7931 | 5/42 | r------rwx | 1993-04-13 08:28:48 | 2003-06-24 00:34:44 | 4 |
| /casing/stand/sites | 1877 | Dir, 512 | 2/1 | d---r---w- | 2020-03-13 09:30:02 | 1993-10-08 05:50:47 | 2 |
| /casing/stand/sites/data.db2 | 1882 | File, 7931 | 5/42 | r------rwx | 1993-04-13 08:28:48 | 2003-06-24 00:34:44 | 4 |
| /casing/stand/sites/scansft | 1881 | Link, 19 | 0/0 | lrwxr-xr-x | 1993-12-06 03:38:58 | 1993-12-06 03:38:58 | 1 |
| /casing/stand/Venäjän | 1891 | Dir, 512 | 16/10 | d--x--x-wx | 2007-01-18 17:41:39 | 1999-09-11 07:03:46 | 3 |
| /casing/stand/Venäjän/file03.jpg | 1895 | File, 161065 | 4/46 | rr----xrw- | 1981-05-18 20:12:03 | 2007-01-18 17:41:39 | 2 |
| /casing/stand/Venäjän/xmlrdr | 1893 | Dir, 512 | 0/5 | drwxrwx-wx | 1982-05-14 10:37:03 | 2014-05-01 06:04:15 | 2 |
| casing/stand/Venäjän/xmlrdr/check.txt | 1894 | File, 95079 | 10//50 | r--x------ | 1999-01-12 09:52:26 | 2000-05-09 12:21:48 | 1 |
| /casing/stand/Venäjän/xmlrdr/download.sh | 1896 | File, 9539 | 1/40 | rr-xrw-r-- | 1985-12-13 01:17:37 | 1982-05-14 10:37:03 | 1 |
| /casing/stand/Venäjän/xmlrdr/zip.txt | 1878 | File, 7932 | 5/14 | rr--r-xr-x | 2004-04-03 08:26:39 | 1994-03-10 10:21:51 | 2 |

В этом задании не получится смонтировать UFS под Linux без дополнительных модулей, поэтому можно руками получить значения ссылок из AutoPsy:

|  |  |
| --- | --- |
| Ссылка | Значение |
| /casing/stand/sites/scansft | /casing/stand/brake |
| /casing/links/dbs/file01.jpg | /casing/links/dbs/Co?e.txt |
| /casing/bumper | ../casing |

1. **ВЫВОД**

В процессе выполнения лабораторной работы исследовались основные файловые системы, поддерживаемые в Windows и Linux. Кроме организации файлов, были рассмотрены атрибуты безопасности и дополнительные возможности объектов. Были получены знания об организации структуры данных, которая содержит информацию о диске, файловой системе и объектах, таких как суперблок, таблица $MFT, BPB и Extended BPB.

Система NTFS имеет большее количество дополнительных данных, чем другие системы, в то время как FAT, также созданная Microsoft, менее нагружена. Задание для FAT выполнялось так же легко и быстро, как и для Linux и FreeBSD.

Так же стоит отметить, что при парсинге структуры файлов опускались некоторые системные файлы (например, в таблицу не попали файлы с данными $Secure, $MFT и им подобные в ФС NTFS). Более того, было решено не заниматься переписыванием всех используемых блоков у больших файлов, так как это не имеет сильного значения.