

Министерство образования и науки РФ
Новосибирский государственный технический университет

Кафедра ТПИ

Лабораторная работа № 3
По Операционным системам и компьютерным сетям

Файловые системы ОС Windows

Факультет: ПМИ

Группа: ПМ-24

Бригада: 12

Студенты: Герасименко Вадим
Параскун Иван

Преподаватель: Сивак М. А.

Новосибирск
2024

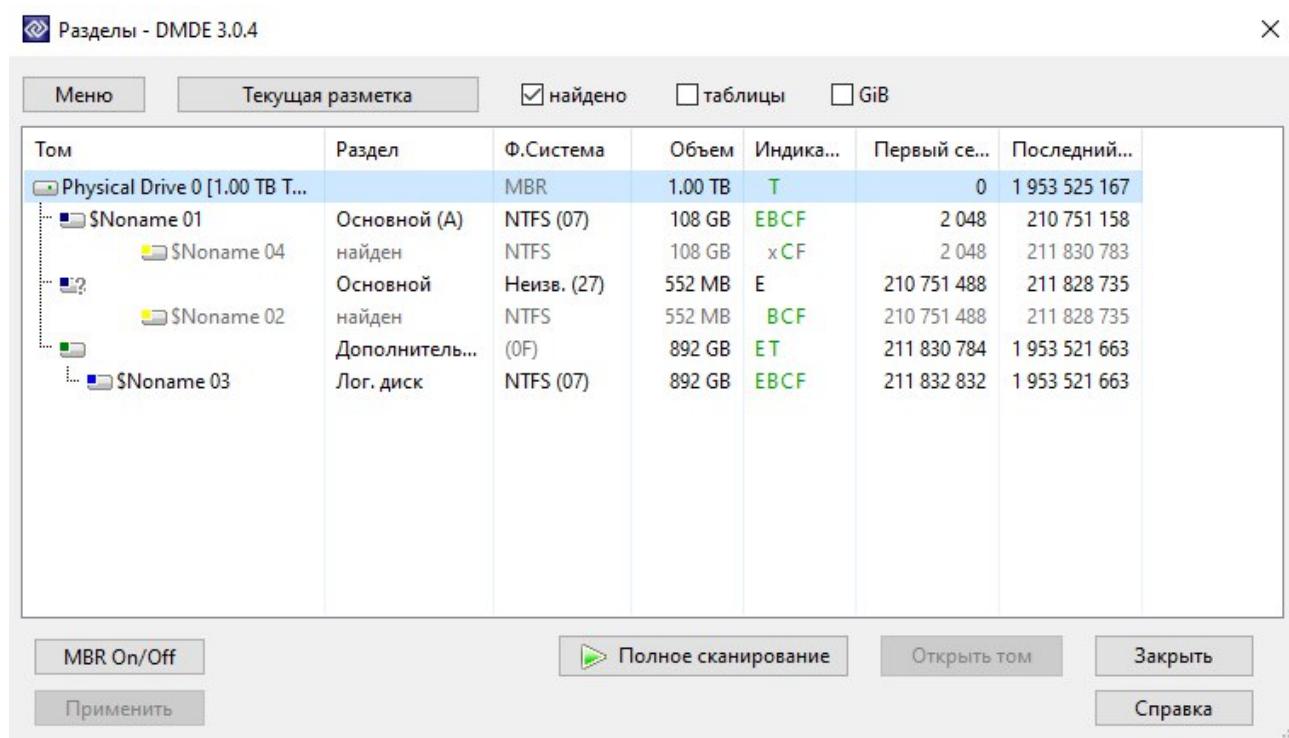
1. Цель работы

Целью работы является приобретение навыков анализа физической и логической структуры магнитных дисков и закрепление знаний по файловым системам FAT и NTFS.

2. Ход работы

1. Откройте дисковый редактор DMDE и определите параметры диска: общий объем, число и типы разделов, тип файловой установленной файловой системы. Для FAT - раздела определите размеры сектора и кластера; число секторов, выделенных для таблицы FAT и размер корневого каталога. Для NTFS - раздела определите размеры сектора и кластера, размер файла \$MFT и его адрес, размеры записи MFT и индексной записи. Занесите все параметры в отчет, подтверждая их скриншотами.

ПК:



The screenshot shows the 'Разделы' (Partitions) window of DMDE 3.0.4. The window displays the structure of Physical Drive 0, which has a total capacity of 1.00 TB. The drive contains three primary partitions and one logical volume. The primary partitions are: \$Noname 01 (Основной (A), NTFS (07), 108 GB, EBCF), \$Noname 02 (Основной, NTFS, 552 MB, EBCF), and \$Noname 03 (Лог. диск, NTFS (07), 892 GB, EBCF). The logical volume \$Noname 04 (найден) is part of the \$Noname 02 partition. The table also includes columns for Ф.Система (File System), Объем (Volume), Индика... (Indicator), Первый се... (First Sector), and Последний... (Last Sector).

Том	Раздел	Ф.Система	Объем	Индика...	Первый се...	Последний...
Physical Drive 0 [1.00 TB T...]		MBR	1.00 TB	T	0	1 953 525 167
\$Noname 01	Основной (A)	NTFS (07)	108 GB	EBCF	2 048	210 751 158
\$Noname 04	найден	NTFS	108 GB	xCF	2 048	211 830 783
\$Noname 02	Основной	Незав. (27)	552 MB	E	210 751 488	211 828 735
\$Noname 02	найден	NTFS	552 MB	BCF	210 751 488	211 828 735
\$Noname 03	Дополнитель...	(0F)	892 GB	ET	211 830 784	1 953 521 663
\$Noname 03	Лог. диск	NTFS (07)	892 GB	EBCF	211 832 832	1 953 521 663

Buttons at the bottom include: MBR On/Off, Полное сканирование (Full Scan), Открыть том (Open Volume), Закрыть (Close), Применить (Apply), and Справка (Help).

Общий объём: 1 ТВ,

Число разделов: 3,

Типы разделов: два первичных, один расширенный,

Тип файловой установленной системы: NTFS.

USB:

The screenshot shows the 'Разделы - DMDE 3.6.0' window. It displays a table of partitions on a drive. The table has columns: Том (Volume), Раздел (Partition), Ф.Система (File System), Объем (Volume), Индикат... (Indicator), Первый сект... (First Sector), and Последний с... (Last Sector). One partition is selected: 'Drive 3 - 8.05 GB - USB -...' with 'TOM' as its name. This partition is highlighted with a yellow icon and labeled 'Основной' (Primary) and 'найден' (Found). Its file system is FAT32 (0C), volume is 8.05 GB, and it starts at sector 2 048 and ends at 15 730 654. Other rows show the drive's capacity as 8.05 GB and the file system as Неизв. (Unknown). At the bottom, there are buttons for MBR On/Off, Full Scan, Open Volume, Close, Apply, and Help.

Общий объём: 8.05 GB,

Число разделов: 1,

Типы разделов: один первичный (основной),

Тип файловой установленной системы: FAT32.

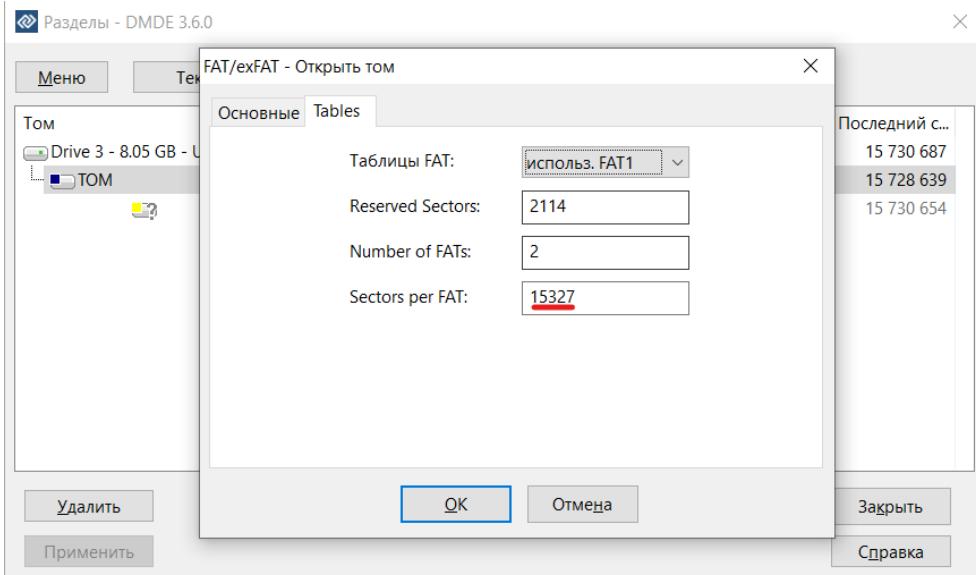
Раздел FAT32:

The screenshot shows the 'FAT/exFAT - Открыть том' (Open Volume) dialog box. It contains fields for basic volume parameters: Файловая система (File System) set to FAT32; Sector Size, Sec per Clust (Sector Size, Sectors per Cluster) set to 512 and 8 respectively; Root Dir Entries (Root Directory Entries) set to 0; Total Sectors (Total Sectors) set to 15726592; First Data Sector (First Data Sector) set to 32768; Root Cluster (Root Cluster) set to 2; Start offset (Start offset) set to 2048 with LBA indicator. A sidebar on the right shows the Last Sector values: 15 730 687, 15 728 639, and 15 730 654. At the bottom are OK, Cancel, Delete, and Apply buttons.

Размер сектора: 512 байт,

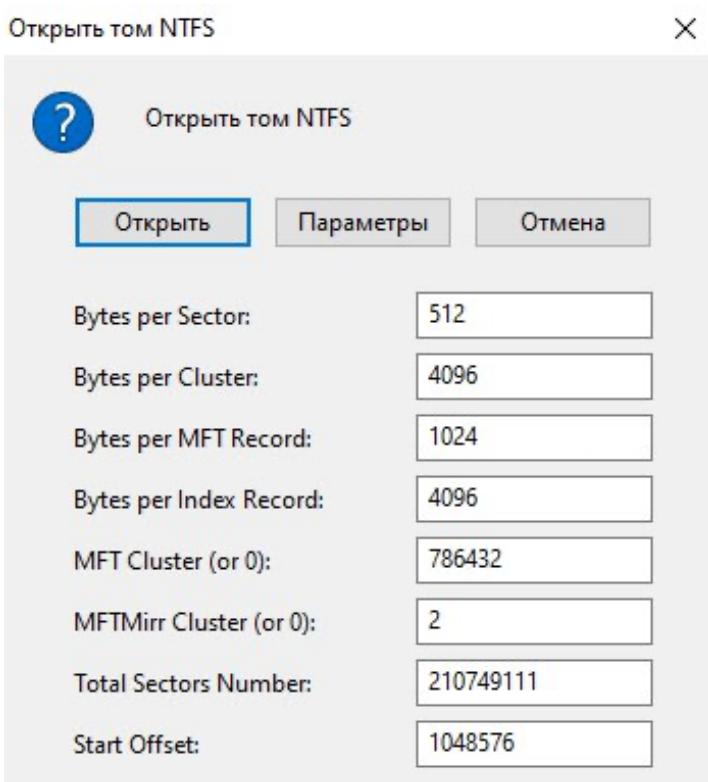
Размер кластера: 8 секторов (4096 байт),

Общее число секторов: 15726592.



Число секторов, выделенных для FAT: 15327.

Раздел NTFS:



Размер сектора: 512 байт,
Размер кластера: 4096 байт.

DMDE 3.0.4 Free Edition

Диск Сервис Окна Редактор Справка

Дерево папок

- [Другие результаты + полное сканирование]
- \$Noname 01
 - > [Все найденные + реконструкция]
 - MetaData
 - \$Extend
 - SAttrDef
 - SBadClus
 - SBadClus:\$Bad
 - SBitmap
 - SBitmap:\$SRAT
 - SBoot
 - SLogFile
 - \$MFT
 - \$MFTMirr
 - SSecure
 - SupCase
 - SupCase:\$Info
 - SVolume
- \$Root
 - driversinstall
 - Windows.old
 - SWinREAgent
 - SWindows.~WS
 - OneDriveTemp
 - vsstudio
 - Активатор
 - Documents and Settings
 - Recovery
 - WATCOM
 - System Volume Information
 - \$Recycle.Bin
 - PerfLogs
 - Program Files
 - Program Files (x86)
 - ProgramData
 - Users
 - Windows
 - Boot
 - Config.Msi
 - 82ace7d6-0197-474d-bf4b-a2043e72329b
 - AMD

Имя Размер Изменен ID

...[+ найденные]	[Папка]		11 (11)
\$Extend	2 560	2018-04-25 09:...	4 (4)
SAttrDef	0	2018-04-25 09:...	8 (8)
SBadClus	107 903 541...	2018-04-25 09:...	8 (8)
SBadClus:\$Bad	3 292 960	2018-04-25 09:...	6 (6)
SBitmap	68	2018-04-25 09:...	6 (6)
SBitmap:\$SRAT	8 192	2018-04-25 09:...	7 (7)
SBoot	67 108 864	2018-04-25 09:...	2 (2)
SLogFile	1 546 387 456	2018-04-25 09:...	0 (1)
\$MFT	4 096	2018-04-25 09:...	1 (1)
\$MFTMirr	0	2018-04-25 09:...	9 (9)
SSecure	131 072	2018-04-25 09:...	10 (10)
SupCase	32	2018-04-25 09:...	10 (10)
SupCase:\$Info	0	2018-04-25 09:...	3 (3)
SVolume			

Файл "\$MFT" - Physical Drive 0 [1.00 TB TOSHIBA DT01ACA100 : MS20A750 : 95EYAGUNS]

LBA:6293504 лог.сек:6291456 Клас:786432 сек:0 (MFT 0)
 /секторов: 2 / MFT №: 0 (1)
 [0] 0x10 \$STANDARD_INFORMATION: 2018-04-25 09:25:54.775
 [3] 0x30 \$FILE_NAME: \$MFT
 [1] 0x80 \$DATA: Размер:1546387456 Занято:1546387456
 [5] 0x80 \$BITMAP: Размер:192520 Занято:196688
 [Конец списка атрибутов]
 LBA:6293506 лог.сек:6291458 Клас:786432 сек:2 (MFT 1)
 /секторов: 2 / MFT №: 1 (1)
 [0] 0x10 \$STANDARD_INFORMATION: 2018-04-25 09:25:54.775
 [2] 0x30 \$FILE_NAME: \$MFTMirr
 [1] 0x80 \$DATA: Размер:4096 Занято:4096
 Вид: Файл MFT | LBA: 0x00600800 = 6 293 504 Pos: 0x0038 = 56 | 0x0000000000038 = 56

[Enter]: открыть (редактор) [Ctrl+U]: восстановить...

Размер файла \$MFT: 1546387456 Б,
 Адрес файла \$MFT: LBA 6293504,
 Размер записи MFT: 1024 Б,
 Размер индексной записи: 4096 Б.

2. Откройте логический диск с файловой системой FAT32 и выполните следующие действия, подтверждая их скриншотами.

2.1 Создайте на диске каталог с именем, соответствующим Вашей учетной записи и в нем создайте структуру каталогов согласно заданию лабораторной работы № 1.

Дерево папок

- [Другие результаты + полное сканирование]
- ТОМ
 - > [Все найденные + реконструкция]
 - metaData
 - \$Root
 - System Volume Information
 - pml-b2412
 - ABC_12
 - HC1
 - HC2
 - (Новая папка, Новая папка)
 - TMP_12
 - TTT
 - (Новая папка)
 - TRASH_12
 - FONTS1
 - FONTS2
 - FONTS3
 - (Новая папка, Новая папка, Новая папка)
 - (Новая папка, Новая папка, Новая папка)
 - (Новая папка, _MI_, _ILE.TXT, Новый ярлык.lnk, Новый ярлык...)

2.2. В каталог *abc_kk* запишите три файла размером 40 – 60 Кбайт, имеющих форматы *.txt*, *.doc* и *.docx*, имена файлов должны содержать не менее 15 символов, например, *Лабораторная работа № 3*. Содержимое файлов должно быть записано с использованием символов кириллицы.

Содержимое папки				
Имя	Размер	Изменен	ID	Опции
<input type="checkbox"/> [..]			6	
<input type="checkbox"/> HC1	[папка]	2024-03-27	9	
<input type="checkbox"/> HC2	[папка]	2024-03-27	10	
<input type="checkbox"/> Новая папка	[папка]	2024-03-27	_000Fh	
<input type="checkbox"/> Новая папка	[папка]	2024-03-27 19:21	_0009h	
<input type="checkbox"/> Новая папка	[папка]	2024-03-27 19:22	_000Ah	
<input type="checkbox"/> Лабораторная работа № 4.doc	48 150	2024-03-27 19:29	27	
<input type="checkbox"/> Лабораторная работа № 4.docx	48 150	2024-03-27 19:29	39	
<input type="checkbox"/> Лабораторная работа № 4.txt	48 150	2024-03-27 19:29	15	

2.3. Для файла *Лабораторная работа № 4.txt* выполните следующие действия:
- определите число элементов каталога, выделенных для хранения информации по файлу:

Число элементов: 12 (с 15 по 26).

- занесите в таблицу 4 содержимое элемента, предназначенного для хранения короткого имени;

Имя	Расш.	Размер	Кластер	Атрибуты	Изменен	Создан	Доступ
HC2	>	0	10	---	2024-03-27 19:22:10	2024-03-27 19:22:08.07	2024-03-27
х 0	Новая папка .		0	RHSV----	EA		
х0ВАЯП~1	>	4096	15	---	2024-03-27 19:27:02	2024-03-27 19:27:01.67	2024-03-27
. 3	t.....		0	RHSV----	CB		
2	работа № 4.tx		0	RHSV----	CB		
1	Лабораторная		0	RHSV----	CB		
ЛАБОРА~1	TXT	48150	15	-----A--	2024-03-27 19:29:30	2024-03-27 19:27:07.83	2024-03-27
. 3	c.....		0	RHSV----	31		
2	работа № 4.do		0	RHSV----	31		
LBA:34849	лог.сек:32801 Клас:6 сек:1						
1	Лабораторная		0	RHSV----	31		
ЛАБОРА~1	DOC	48150	27	-----A--	2024-03-27 19:29:44	2024-03-27 19:27:20.79	2024-03-27
. 3	cx.....		0	RHSV----	92		
2	работа № 4.do		0	RHSV----	92		
1	Лабораторная		0	RHSV----	92		
Вид: Директория FAT	LBA: 0x00008820 = 34 848	Pos: 0x01a0 = 416		0x00000000001a0 = 416			

Таблица 4

Наименование поля	Значение поля
имя файла	ЛАБОРА~1
расширение имени	TXT
атрибуты	-----A--
время создания	19:27:07.83
дата создания	2024-03-27
номер начального кластера	15
размер файла	48150

- просмотрите содержимое и коды первых 16 байтов, занесите их в отчет;

Файл "Лабораторная работа № 4.txt" - Physical Drive 3 - 8.05 GB - Generic Mass Storage : 1.0 : AEB77B70							
LBA:34920 лог.сек:32872 Клас:15 сек:0							
0000: 4C 6F 72 65 6D 20 49 70	73 75 6D 20 2D 20	D1 8D	Lorem Ipsum - CK				
0010: D1 82 D0 BE 20 01 82 D0	B5 D0 BA D1 81 D0 82 2D	C,Ps C,РµЕсCfC,-					
0020: 22 D1 80 D1 88 D0 B1 D0	B0 22 2C 20 D0 87 D0 B0	"Cfc<Р±Р°о, CР°о					
0030: D1 81 D1 82 D0 BE 20 00	B8 D1 81 D0 BF D0 BE D0	Cfc,Cps РёсCfР±Р±Р±Р					
0040: BB D1 8C D0 B7 D1 83 D0	B5 D0 BC D1 88 D0 B9 20	»CбР·CfРµРјC<РМ					
0050: D0 B2 20 D0 BF D0 B5 D1	87 D0 B0 D1 82 D0 B8 20	PI РІРµР±Р°C,Рё					
0060: D0 B0 20 D0 B2 D1 8D D0	B1 2D D0 B4 D0 B8 D0 B7	Pё PICRР±-PRРРР-					
0070: D0 B0 D9 D0 BD D0 B5	2E 20 4C 6F 72 65 6D 20	PºNWPSPu. Lorem					
0080: 49 70 73 75 6D 20 D1 8F	D0 B2 D0 6B D1 8F D0 B5	Ipsum CUPIP:CUPu					
0090: D1 82 D1 81 D1 BF 20 D1	81 D1 82 D0 B0 D0 BD D0	C,CfcU Cfc,PºPSP					
00a0: B4 D0 B0 D1 80 D1 82 D0	B0 D0 BE D0 B0 B9 20 22 D1	rР°CбC,РºР±Р±Р" C					
00b0: 80 D1 88 D0 B1 D0 BE D0	B9 22 20 D0 B4 D0 BB D1	БС<Р±Р±Р±Р" PrР±C					
00c0: 8F 20 D1 82 D0 B5 D0 BA	D1 81 D1 82 D0 BE D0 B2	U C,РµЕсCfC,РºР±					
00d0: 20 D0 D0 B0 20 D0 BB	D0 B0 D1 82 D0 BB D0 BD	PSPº PºР°C,РºР±					
00e0: D0 B0 D1 86 D0 B5 20 D1	81 20 D0 BD D0 B0 D1 87	PёсC+Рµ Cf PSPºC‡					
Вид: ANSI (141-115)	LBA: 0x00008868 = 34 920	Pos: 0x000f = 15		0x00000000000f = 15			

Коды: 4C 6F 72 65 6D 20 49 70 73 75 6D 20 2D 20 D1 8D

- определите используемую кодировку символов путем сравнения с кодировочными таблицами редактора;

Файл "Лабораторная работа № 4.txt" - Physical Drive 3 - 8.05 GB - Generic Mass Storage : 1.0 : AEB77B70							
Unicode							
Windows-1251 (Russian)	0	15	сек:0				
CP866 (DOS Russian)	1	2D 20 D1 8D	Lorem Ipsum - CK				
CP437 (DOS US)	2	81 D1 82 2D	C,Ps C,РµЕсCfC,-				
CP850 (DOS Western European)	3	91 D0 B7 D0 B0	"Cfc<Р±Р°о, CР°о				
CP852 (DOS Central European)	4	9BF D0 BE D0	Cfc,Cps РёсCfР±Р±Р±Р				
Windows-1250 (Central European)	5	98 B8 D0 B8 20	»CбР·CfРµРјC<РМ				
Windows-1252 (Western European)	6	98 D0 B0 D0 B0	PI РІРµР±Р°C,Рё				
Windows-1253 (Greek)	7	98 D0 B0 D0 B0	Pё PICRР±-PRРРР-				
Windows-1254 (Turkish)	8	98 D0 B0 D0 B0	PºNWPSPu. Lorem				
Windows-1255 (Hebrew)	9	98 D0 B0 D0 B0	Ipsum CUPIP:CUPu				
Windows-1256 (Arabic)	A	98 D0 B0 D0 B0	C,СfcU Cfc,PºPSP				
Windows-1257 (Baltic)	B	98 D0 B0 D0 B0	rР°CбC,РºР±Р±Р" C				
	C	98 D0 B0 D1 87	PrР±C				
	D	98 D0 B0 D1 87	PёсC+Рµ Cf PSPºC‡				
	E	98 D0 B0 D1 87	0x00000000000f = 15		0x00000000000f = 15		

Используемая кодировка: Windows-1251

- определите список кластеров этого файла, результаты занесите в таблицу 5;

Секторы тома 2 114 - 17 440 - Physical Drive 3 - 8.05 GB - Generic Mass Storage : 1.0 : AEB77B70											
LBA:4162 лог.сек:2114 FAT1 сек:0											^
[E]	F:[E]	[E]	[E]	[E]	[E]	[E]	[E]	[E]	[E]	[E]	[E]
[E]	[E]	16	[=]	[=]	[=]	[=]	[=]	[=]	[=]	[=]	[=]
[E]	[=]	[=]	[=]	[=]	[=]	[=]	[=]	[=]	[=]	[=]	[E]
[=]	[=]	[=]	[=]	[=]	[=]	[=]	[=]	[=]	[=]	[E]	0
0	0	0	0	0	0	0	0	0	0	0	0
0	0	0	0	0	0	0	0	0	0	0	0
0	0	0	0	0	0	0	0	0	0	0	0
0	0	0	0	0	0	0	0	0	0	0	0
0	0	0	0	0	0	0	0	0	0	0	0
0	0	0	0	0	0	0	0	0	0	0	0
LBA:4163 лог.сек:2115 FAT1 сек:1											
0	0	0	0	0	0	0	0	0	0	0	0
0	0	0	0	0	0	0	0	0	0	0	0
0	0	0	0	0	0	0	0	0	0	0	0
0	0	0	0	0	0	0	0	0	0	0	0
Вид: FAT32 [15]	LBA: 0x00001042 = 4 162 Pos: 0x003c = 60				0x000000000003c = 60						

Таблица 5

Логический номер кластера в файле	1	2	3	...	n
Номер кластера на диске	15	16	17	...	26
Значение элемента FAT	16	17	18	...	EOF

2.4. С помощью программы *Проводник* скопируйте файл *Лабораторная работа № 4.txt* в каталог *trash_kk*.

\\\pmi-b2412\TRASH_12			
Имя	Размер	Изменен	ID
□ 🗂 [...]			8
□ 🗂 FONTS1	[папка]	2024-03-27	12
□ 🗂 FONTS2	[папка]	2024-03-27	13
□ 🗂 FONTS3	[папка]	2024-03-27	14
□ 🗂 Новая папка	[папка]	2024-03-27 19:22	_000Ch
□ 🗂 Новая папка	[папка]	2024-03-27 19:22	_000Dh
□ 🗂 Новая папка	[папка]	2024-03-27 19:22	_000Eh
□ 📄 Лабораторная работа № 4.txt	48 150	2024-03-27 19:29	51

2.5. Удалите файл *Лабораторная работа № 4.txt* из каталога *abc_kk*, проведите анализ изменений в FAT и в каталоге *abc_kk*, результаты занесите в отчет в виде таблиц 22 и 23. Посмотрите содержимое начального кластера удаленного файла, результат занесите в отчет.

Имя	Расш.	Размер	Кластер	Атрибуты	Изменен	Создан	Доступ
хОВАЯП~1	>	0	10	----	2024-03-27 19:22:10	2024-03-27 19:22:08.07	2024-03-27
HC2	>	0	10	----	2024-03-27 19:22:10	2024-03-27 19:22:08.07	2024-03-27
x 0	Новая папка..			0 RHSV---	EA		
хОВАЯП~1	>	4096	15	----	2024-03-27 19:27:02	2024-03-27 19:27:01.67	2024-03-27
x 0	t.....			0 RHSV---	CB		
x 0	работа № 4.tx			0 RHSV---	CB		
x 0	Лабораторная			0 RHSV---	CB		
хБ0РР~1	TXT	48150	15	----A-	2024-03-27 19:29:30	2024-03-27 19:27:07.83	2024-03-27
.	3			0 RHSV---	31		
.	2			0 RHSV---	31		
LBA:34849	лог.сек:32801	Клас:6 сек:1					
1	Лабораторная			0 RHSV---	31		
ЛАБОРА~1	DOC	48150	27	----A-	2024-03-27 19:29:44	2024-03-27 19:27:20.79	2024-03-27
.	3			0 RHSV---	92		
.	2			0 RHSV---	92		

Файл "Лабораторная работа № 4.txt" - Physical Drive 3 - 8.05 GB - Generic Mass Storage : 1.0: AEB77B70
LBA:34920 лог.сек:32872 Клас:15 сек:0
0000: 4C 6F 72 65 6D 20 49 70 73 75 6D 20 2D 20 D1 8D Lorem Ipsum - СК
0010: D1 82 D0 20 D1 82 D0 B5 D0 BA D1 81 D1 82 2D C₂P₃C₄P₅E₆C₇-
0020: 22 D1 80 D1 88 D0 B1 D0 B8 22 2C 20 D1 87 D0 B0 "СБ₂С₃Р₄Р₅", С₆Р₇
0030: D1 81 D1 82 D0 BE 20 D0 B8 D1 81 D0 BF D0 BE D0 C₂C₃P₄S P₅E₆C₇P₈
0040: BB D1 8C D0 B7 D1 83 B5 D0 BC D1 88 D0 B9 20 »СБ₂С₃Р₄Р₅Д₆С₇М₈
0050: D0 B2 20 D0 BF D0 B5 D1 87 D0 B0 D1 82 D0 B8 20 Р₂Р₃Р₄С₅Р₆С₇Р₈, Р₉
0060: D0 B8 20 D0 B2 D1 8D D0 B1 2D D0 B4 D0 B8 D0 B7 Р₂Р₃К₄Р₅-Р₆Р₇-Р₈
0070: D0 B0 B9 D0 BD D0 B5 2E 20 4C 6F 72 65 6D 20 Р₂Р₃М₄Р₅С₆Р₇. Lorem
0080: 49 70 73 75 6D 20 D1 8F D0 B2 D0 B8 D1 8F D0 B5 Ipsum СУР₂И₃СУР₄
0090: D1 82 D1 81 D1 8F 20 D1 81 D1 82 D0 B8 D0 BD D0 C₂С₃С₄ С₅Р₆Р₇
00A0: B4 D0 B0 D1 80 D1 82 D0 BD D0 BE D0 B9 20 22 D1 Р₂Р₃С₄С₅Р₆Р₇М₈ "С
00B0: 80 D1 88 D0 B1 D0 BE D0 B9 22 20 D0 B4 D0 B8 D1 Т₂С₃Р₄Р₅М₆ Р₇Р₈С
00C0: 8F 20 D1 82 D0 B5 D0 BA D1 81 D1 82 D0 BE D0 B2 У C₂P₃E₄C₅Р₆Р₇
00D0: 20 D0 BD D0 B0 20 D0 BB D0 B0 D1 82 D0 B8 D0 BD Р₂Р₃Р₄ Р₅Р₆Р₇Р₈
00E0: D0 B8 D1 86 D0 B5 20 D1 81 20 D0 BD D0 B0 D1 87 Р₂С₃Р₄ С₅Р₆Р₇Р₈

2.6. Восстановите удаленный файл *Лабораторная работа № 4.txt*.

Всего файлов восстановлено:	1
Всего восстановлено:	48 150
Всего восстановлено:	48.2 kB

2.7. Определите используемую кодировку символов для файлов *Лабораторная работа № 4.doc* и *Лабораторная работа № 4.docx*, результаты занесите в отчет.

✓	Unicode	0	110 сек:5
	Windows-1251 (Russian)	1	распечат
	CP866 (DOS Russian)	2	образ
	CP437 (DOS US)	3	ки
	CP850 (DOS Western European)	4	цов
	CP852 (DOS Central European)	5	лог
	Windows-1250 (Central European)	6	ем
	Windows-1252 (Western European)	7	Ирсим
	Windows-1253 (Greek)	8	не толь
	Windows-1254 (Turkish)	9	ко успеш
	Windows-1255 (Hebrew)	A	но переж
	Windows-1256 (Arabic)	B	ил без э
		C	аметных
		D	изменени
		E	и
		F	пять в
		G	еков, но
		H	и переш
		I	агнул в
		J	электрон

Файл "Лабораторная работа № 4.docx" - Physical Drive 3 - 8.05 GB - Generic Mass Storage : 1.0 : AEB77B70	
✓ Unicode	0 180 сек:0
Windows-1251 (Russian)	0 00 21 00 DF A4 亂 . . . ! M 亂 Á - 亂 国 香
CP866 (DOS Russian)	1 00 08 02 5B 43 亂 . 亂 . 亂 亂 威 滴
CP437 (DOS US)	2 73 5D 2E 78 6D 漢 整 漢 烟 漢 漢 漢 漢 漢 漢 漢
CP850 (DOS Western European)	3 00 00 00 00 00 H 亂 亂 亂 亂 亂 亂 亂 亂 亂 亂 亂 亂
CP852 (DOS Central European)	4 00 00 00 00 .
Windows-1250 (Central European)	5 00 00 00 00 .
Windows-1252 (Western European)	6 00 00 00 00 .
Windows-1253 (Greek)	7 00 00 00 00 .
Windows-1254 (Turkish)	8 00 00 00 00 .
Windows-1255 (Hebrew)	9 00 00 00 00 .
Windows-1256 (Arabic)	A 00 00 00 00 .
Windows-1257 (Baltic)	B 00 00 00 00 .
	C 0 = 36 240 Pos: 0x0000 = 0 0x0000000000000000 = 0

Для расширения .doc: Unicode,
Для расширения .docx: Unicode.

3. Откройте логический диск с файловой системой NTFS и выполните действия, подтверждая их скриншотами.

3.1. Создайте на диске структуру каталогов и файлов согласно п.3.1 и п.3.2.



3.2. Определите характеристики файла \$MFT (начальный адрес, число записей, размер в байтах и кластерах).

Файл "\$MFT" - Physical Drive 0 [1.00 TB TOSHIBA DT01ACA100 : MS20A750 : 95EYAGUNS]	
LBA:6293504	лог.сек:6291456 Клас:786432 сек:0 (MFT 0)
/секторов:	2 / MFT No: 0 (1)
[0] 0x10	\$STANDARD_INFORMATION: 2018-04-25 09:25:54.775
[3] 0x30	\$FILE_NAME: \$MFT
[1] 0x80	\$DATA: Размер:1546387456 Занято:1546387456
[5] 0x80	\$BITMAP: Размер:192520 Занято:196608
[Конец списка атрибутов]	
LBA:6293506	лог.сек:6291458 Клас:786432 сек:2 (MFT 1)
/секторов:	2 / MFT No: 1 (1)
[0] 0x10	\$STANDARD_INFORMATION: 2018-04-25 09:25:54.775
[2] 0x30	\$FILE_NAME: \$MFTMirr
[1] 0x80	\$DATA: Размер:4096 Занято:4096
[Конец списка атрибутов]	
LBA:6293508	лог.сек:6291460 Клас:786432 сек:4 (MFT 2)
/секторов:	2 / MFT No: 2 (2)
[0] 0x10	\$STANDARD_INFORMATION: 2018-04-25 09:25:54.775
[2] 0x30	\$FILE_NAME: \$LogFile
[1] 0x80	\$DATA: Размер:67108864 Занято:67108864
[Конец списка атрибутов]	
LBA:6293510	лог.сек:6291462 Клас:786432 сек:6 (MFT 3)
/секторов:	2 / MFT No: 3 (3)
[0] 0x10	\$STANDARD_INFORMATION: 2018-04-25 09:25:54.775
[1] 0x30	\$FILE_NAME: \$Volume
[6] 0x40	\$OBJECT_ID: размер:16
[4] 0x60	\$VOLUME_NAME: размер:0
[5] 0x70	\$VOLUME_INFORMATION: размер:12
[3] 0x80	\$DATA: размер:0

Начальный адрес: 6293504,
Число записей: $1546387456 / 1024 = 1510144$,
Размер в байтах: 1546387456,
Размер в кластерах: $1546387456 / 4096 = 377536$ (первый кластер: 0, последний кластер: 377535).

3.3. Определите число записей в файле \$MFTmirr.

SMFTMirr		4 096	2018-04-25 09:... 1 (1)
Файл "\$MFT" - Physical Drive 0 [1.00 TB TOSHIBA DT01ACA100 : MS2OA750 : 95EYAGUNS]			
LBA: 6293506	лог.сек: 6291458 Клас: 786432 сек: 2 (MFT 1)		
/секторов:	2 / MFT No: 1 (1)		
[0] 0x10	\$STANDARD_INFORMATION: 2018-04-25 09:25:54.775		
[2] 0x30	\$FILE_NAME: \$MFTMirr		
[1] 0x80	\$DATA: Размер: 4096 Занято: 4096		
[Конец списка атрибутов]			
Вид: Файл MFT	LBA: 0x00600802 = 6 293 506 Pos: 0x0000 = 0		0x0000000000

Число записей: $4096 / 1024 = 4$.

3.4. Проведите полный анализ записи MFT, соответствующей файлу *Лабораторная работа № 3.txt* и занесите в отчет описания всех атрибутов, включая расположение файла на диске.

\\pmi-b2412\abc_12\hc2			
Имя	Размер	Изменен	ID
..			533811 (12)
Лабораторная работа №3 Герасимен... 393 723 2024-03-27 10:... 398559 (25)			
Файл "\$MFT" - Physical Drive 0 [1.00 TB TOSHIBA DT01ACA100 : MS2OA750 : 95EYAGUNS]			
LBA: 128364806	лог.сек: 128362758 Клас: 16045344 сек: 6 (MFT 398559)		
/секторов:	2 / MFT No: 398559 (25)		
[0] 0x10	\$STANDARD_INFORMATION: 2024-03-27 10:59:30.083		
[5] 0x30	\$FILE_NAME: 3BCAF-1.TXT		
[4] 0x30	\$FILE_NAME: Лабораторная работа №3 Герасименко Параскун.txt		
[6] 0x40	\$OBJECT_ID: размер:16		
[7] 0x80	\$DATA: Размер: 393723 Занято: 458752 Сжато: 53248		
[Конец списка атрибутов]			
Вид: Файл MFT	LBA: 0x07a6b106 = 128 364 806 Pos: 0x0000 = 0		0x000018537c00 = 408 124 416

Расположение на диске: "C:\pmi-b2412\abc_12\hc2\Лабораторная работа №3 Герасименко Параскун.txt"

```

Файл "$MFT" - Physical Drive 0 [1.00 TB TOSHIBA DT01ACA100 : MS20A750 : 95EYAGUNS]
LBA:128364806 лог.сек:128362758 Клас:16045344 сек:6 (MFT 398559)
/секторов: 2 / MFT No: 398559 (25)
[ 0] 0x10 $STANDARD_INFORMATION: 2024-03-27 10:59:30.083
    Время создания: 2024-03-27 10:58:23.444
    Последнее изменение: 2024-03-27 10:59:30.083
    Последнее изменение в MFT: 2024-03-27 10:59:30.083
    Последний доступ: 2024-03-27 10:59:30.083
    Атрибуты файла: -----n-C----A-----
    Макс. число версий: 0x0
    Номер версии: 0x0
    Id класса: 0x0
    Id владельца: 0x0
    Security Id: 0x2cc6
    Назначенная квота: 0x0
    Update Sequence Number: 0x62b89d420

```

Атрибут стандартной информации, резидентный, длина – 0x10 (16).

```

[ 5] 0x30 $FILE_NAME: ЗВСАФ~1.TXT
    Имя файла: ЗВСАФ~1.TXT
    Папка: 533811 (12)
    Время создания: 2024-03-27 10:58:23.444
    Последнее изменение: 2024-03-27 10:58:23.444
    Последнее изменение в MFT: 2024-03-27 10:58:23.444
    Последний доступ: 2024-03-27 10:58:23.444
    Занятое пространство: 0
    Размер: 0
    Атрибуты: -----n-C----A-----
    0x3C uint32: 0x00000000
    POSIX: 2

```

Атрибут короткого имени файла, резидентный, длина – 0x30 (48).

```

[ 4] 0x30 $FILE_NAME: Лабораторная работа №3 Герасименко Паракун.txt
    Имя файла: Лабораторная работа №3 Герасименко Паракун.txt
    Папка: 533811 (12)
    Время создания: 2024-03-27 10:58:23.444
    Последнее изменение: 2024-03-27 10:58:23.444
    Последнее изменение в MFT: 2024-03-27 10:58:23.444
    Последний доступ: 2024-03-27 10:58:23.444
    Занятое пространство: 0
    Размер: 0
    Атрибуты: -----n-C----A-----
    0x3C uint32: 0x00000000
    POSIX: 1

```

Атрибут полного имени файла, резидентный, длина – 0x30 (48).

```

[ 7] 0x80 $DATA: Размер:393723 Занято:458752 Сжато:53248
    Flags: 1
    первый вирт. кластер: 0
    послед.вирт. кластер: 111
        сжат. блок: 4
            занято: 458752
            размер: 393723
        инициализировано: 393723
            скжато: 53248
    +0:      2 cluster(s) @      947477
    +2:      14 cluster(s) @      -1
    +16:     2 cluster(s) @     948682
    +18:     14 cluster(s) @      -1
    +32:     2 cluster(s) @     950697
    +34:     14 cluster(s) @      -1
    +48:     2 cluster(s) @     950802
    +50:     14 cluster(s) @      -1
    +64:     2 cluster(s) @     953394
    +66:     14 cluster(s) @      -1
    +80:     2 cluster(s) @     954088
    +82:     14 cluster(s) @      -1
    +96:     1 cluster(s) @     976201
    +97:     15 cluster(s) @      -1
    [конец списка]
    [Конец списка атрибутов]

```

Атрибут данных файла, нерезидентный, длина 0x80 (128), выделенное количество памяти – 458952 байт, из которых используются 393723 байт, данные занимают 112 кластеров (с 0 по 111).

3.5. Удалите файл *Лабораторная работа № 3.txt*, проведите анализ изменений в MFT и в области данных. Результаты занесите в отчет.

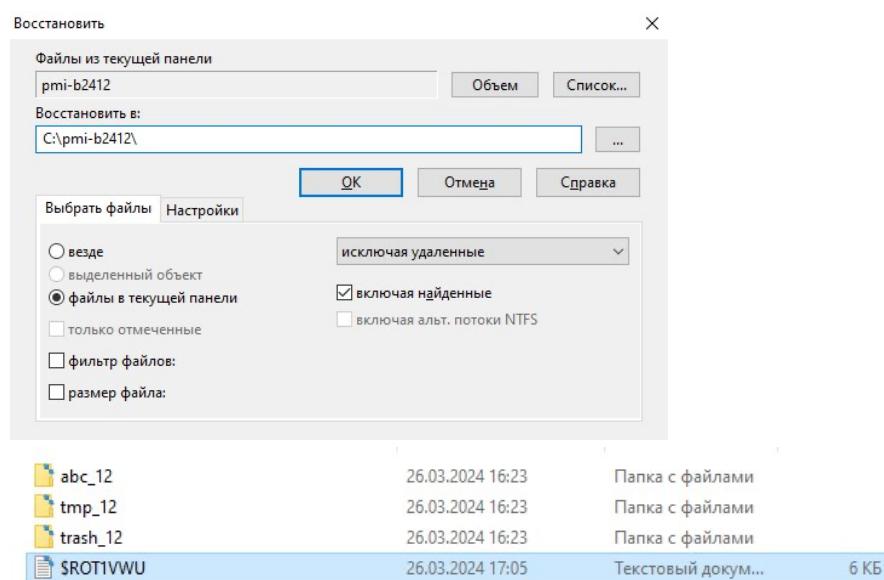
```
LBA:6304910      лог.сек:6302862 Клас:787857 сек:6 (MFT 5703)
/секторов: 2/ MFT No: 5703 (25)
[ 0] 0x10 $STANDARD_INFORMATION: 2024-03-26 10:05:00.316
[ 5] 0x30 $FILE_NAME: $ROT1VVU.txt
[ 1] 0x80 $DATA: Размер:5913 Занято:65536 Сжато:4096
[ 4] 0x80:Zone.Identifier $DATA: размер:115
```

Пропал атрибут полного имени файла и изменился атрибут короткого имени файла.

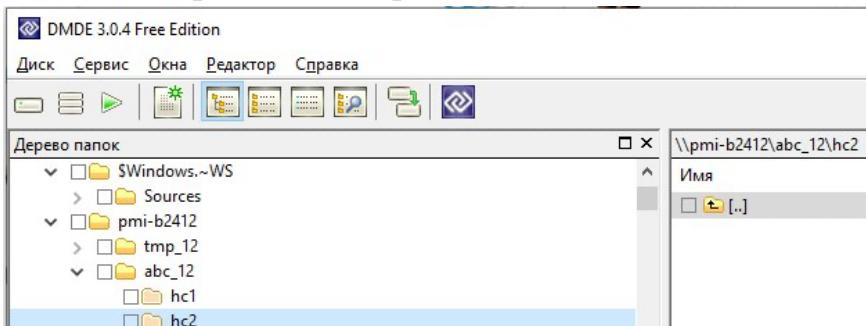
3.6. Восстановите удаленный файл.

Первая попытка:

Не вернуло имя, восстановилось с коротким названием.



Удаленный файл не отобразился.



3.7. С помощью программы Блокнот создайте текстовый файл **primer.txt**, записав в него фразу «Very good weather today!». Проведите анализ соответствующей записи MFT, определить адрес этого файла на диске.

\\pmi-b2412\temp_12			
Имя	Размер	Изменен	ID
□ [..]			466566 (9)
□ trash_12	[Папка]		533806 (12)
□ ttt	[Папка]		533809 (13)
□ primer.txt	24	2024-03-26 11:...	394217 (23)

Файл "\$MFT" - Physical Drive 0 [1.00 TB TOSHIBA DT01ACA100 : MS2OA750 : 95EYAGUNS]			
LBA:128356122	лог.сек:128354074	Клас:16044259	сек:2 (MFT 394217)
/секторов:	2 / MFT No: 394217 (23)		
[0] 0x10	\$STANDARD_INFORMATION: 2024-03-26 11:20:09.695		
[4] 0x30	\$FILE_NAME: primer.txt		
[5] 0x40	\$OBJECT_ID: размер:16		
[1] 0x80	\$DATA: размер:24		
[Конец списка атрибутов]			

Размер: 24,

Адрес: 128356122.

3.8. Запишите в файл **primer.txt** второй поток данных, используя для этого, например, любой текстовый файл размером не менее 50 Кбайт. Проведите анализ соответствующей записи MFT и определите расположение данных этого потока на диске. Определите размер файла, сравните с предыдущим пунктом.

C:\pmi-b2412\temp_12>type file.txt>primer.txt:file.txt

C:\pmi-b2412\temp_12>dir

Том в устройстве C не имеет метки.

Серийный номер тома: 3669-BB4E

Содержимое папки C:\pmi-b2412\temp_12

```
26.03.2024 18:24 <DIR> .
26.03.2024 18:24 <DIR> ..
26.03.2024 18:24           865 260 file.txt
26.03.2024 18:25           24 primer.txt
26.03.2024 16:23 <DIR>      trash_12
26.03.2024 16:23 <DIR>      ttt
```

2 файлов 865 284 байт
4 папок 60 009 414 656 байт свободно

```
Файл "$MFT" - Physical Drive 0 [1.00 TB TOSHIBA DT01ACA100 : MS20A750 : 95EYAGUNS]
LBA:128356122 лог.сек:128354074 Клас:16044259 сек:2 (MFT 394217)
/секторов: 2/ MFT No: 394217 (23)
[ 0] 0x10 $STANDARD_INFORMATION: 2024-03-26 11:37:08.340
[ 4] 0x30 $FILE_NAME: primer.txt
[ 5] 0x40 $OBJECT_ID: размер:16
[ 1] 0x80 $DATA: размер:24
[ 7] 0x80:file.txt $DATA: Размер:865260 Занято:917504 Сжато:110592
Flags: 1
первый вирт. кластер: 0
послед.вирт. кластер: 223
сжат. блок: 4
занято: 917504
размер: 865260
инициализировано: 865260
скжато: 110592
+0: 2 cluster(s) @ 1737830
+2: 14 cluster(s) @ -1
+16: 2 cluster(s) @ 1737832
+18: 14 cluster(s) @ -1
+32: 2 cluster(s) @ 1737834
+34: 14 cluster(s) @ -1
+48: 2 cluster(s) @ 1737836
+50: 14 cluster(s) @ -1
+64: 2 cluster(s) @ 1737838
+66: 14 cluster(s) @ -1
+80: 2 cluster(s) @ 1737840
+82: 14 cluster(s) @ -1
+96: 2 cluster(s) @ 1737842
+98: 14 cluster(s) @ -1
+112: 2 cluster(s) @ 1737844
+114: 14 cluster(s) @ -1
+128: 2 cluster(s) @ 1737846
+130: 14 cluster(s) @ -1
+144: 2 cluster(s) @ 1737848
+146: 14 cluster(s) @ -1
+160: 2 cluster(s) @ 1737850
+162: 14 cluster(s) @ -1
+176: 2 cluster(s) @ 1737852
+178: 14 cluster(s) @ -1
+192: 2 cluster(s) @ 1737854
+194: 14 cluster(s) @ -1
+208: 1 cluster(s) @ 1737856
+209: 15 cluster(s) @ -1
[конец списка]
```

Появилась запись MFT альтернативного потока.

Адрес: 128356122 – остался прежним.

Размер: 24 – остался прежним.

3.9. Запишите в файл **primer.txt** третий поток данных, используя для этого любой графический файл (например, фотографию). Проведите анализ соответствующей записи MFT и определите расположение данных этого потока на диске. Определите размер файла, сравните с предыдущим пунктом.

C:\pmi-b2412\tmp_12>type graphic.jpg>primer.txt:graphic.jpg

C:\pmi-b2412\tmp_12>dir

Том в устройстве C не имеет метки.

Серийный номер тома: 3669-BB4E

Содержимое папки C:\pmi-b2412\tmp_12

26.03.2024 18:35 <DIR>	.
26.03.2024 18:35 <DIR>	..
26.03.2024 18:24	865 260 file.txt
26.03.2024 18:35	118 095 graphic.jpg
26.03.2024 18:37	24 primer.txt
26.03.2024 16:23 <DIR>	trash_12
26.03.2024 16:23 <DIR>	ttt
	3 файлов 983 379 байт
4 папок	60 011 675 648 байт свободно

```
Файл "$MFT" - Physical Drive 0 [1.00 TB TOSHIBA DT01ACA100 : MS2OA750 : 95EYAGUNS]
LBA:128356122 лог.сек:128354074 Клас:16044259 сек:2 (MFT 394217)
/секторов: 2/ MFT No: 394217 (23)
[ 0] 0x10 $STANDARD_INFORMATION: 2024-03-26 11:37:08.340
[ 4] 0x30 $FILE_NAME: primer.txt
[ 5] 0x40 $OBJECT_ID: размер:16
[ 1] 0x80 $DATA: размер:24
[ 7] 0x80:file.txt $DATA: Размер:865260 Занято:917504 Сжато:110592
[ 9] 0x80:graphic.jpg $DATA: Размер:118095 Занято:131072 Сжато:118784
Flags: 1
первый вирт. кластер: 0
послед.вирт. кластер: 31
сжат. блок: 4
занято: 131072
размер: 118095
инициализировано: 118095
сжато: 118784
+0: 29 cluster(s) @ 1003237
+29: 3 cluster(s) @ -1
[конец списка]
[Конец списка атрибутов]
```

Адрес: 128356122 – остался прежним.

Размер: 24 – остался прежним.

3. Выводы

В ходе выполнения работы были приобретены навыки анализа физической и логической структуры магнитных дисков и закреплены знания по файловым системам FAT и NTFS. Контрольные вопросы проработаны.