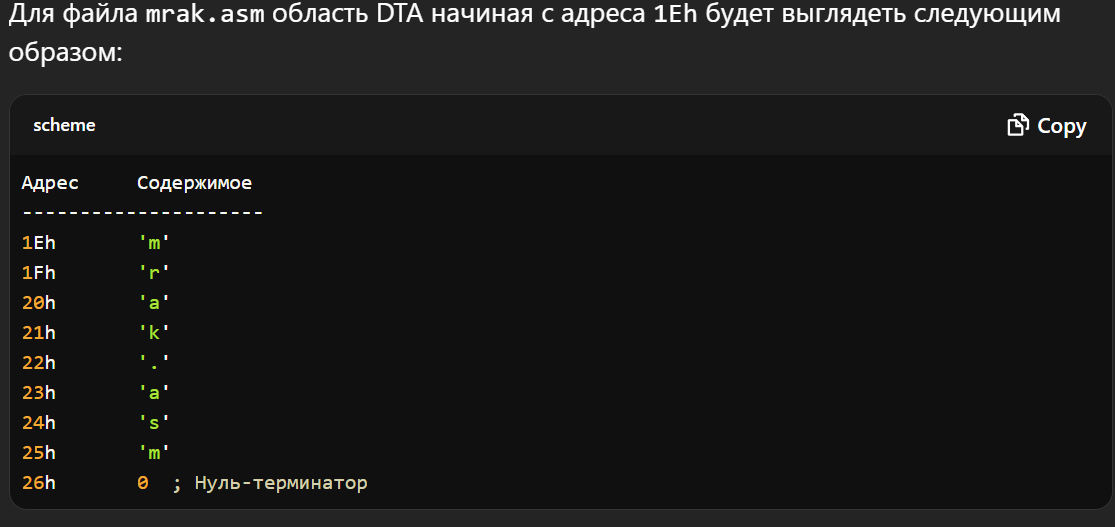
***ВОПРОС 7.1: ЧТО ЗА ЧИСЛО 140h – ОТКУДА ОНО БЕРЁТСЯ?***

Число 140h используется как адрес, указывающий на место в памяти, где хранится информация, необходимая для выполнения функции поиска файла. В данном случае, это адрес, по которому хранятся данные о файле, который требуется найти.**Вопрос 7.2. Что такое DTA. Какие три английских слова прячутся за буквами DTA. ГДЕ РАСПОЛАГАЕТСЯ ЭТА ОБЛАСТЬ.**

**DTA** расшифровывается как **Disk Transfer Area** (область передачи данных диска). Эта область располагается в конце сегмента Program Segment Prefix (PSP) и используется для хранения информации о найденных файлах.

**Вопрос 7.3. Нарисовать побайтно, каким образом в области памяти DTA начиная с адреса 1Eh, будет располагаться имя первого найденного файла, если первым найденным файлом будет файл mrak.asm. НАРИСОВАТЬ НА ЛИСТОЧКАХ!!!!**

******

***Вопрос 7.4. С помощью какой функции осуществляется ПОИСК СЛЕДУЮЩЕГО ЗА НАЙДЕННЫМ ФАЙЛА? КАКОВ КРИТЕРИЙ ОПРЕДЕЛЕНИЯ ПЕРВОГО ПОПАВШЕГОСЯ ФАЙЛА И ПОСЛЕДУЮЩИХ?***

***В задаче про mrak, папу с мамой, каждый из Вас имел «текущий каталог». Записать, какой из файлов будет первым найденным и затем записать какие файлы будут следующими, указав их ПОЛНЫЕ ИМЕНА И ИМЕНА СОКРАЩЕННЫЕ, КАК ОНИ БУДУТ ХРАНИТЬСЯ В ОБЛАСТИ DTA.***

Поиск следующего файла осуществляется с помощью функции 4Fh. Критерий определения следующего файла основан на маске, переданной в предыдущем вызове функции 4Eh. Следующий файл определяется по порядку, в котором они находятся в каталоге.

**Пример:**

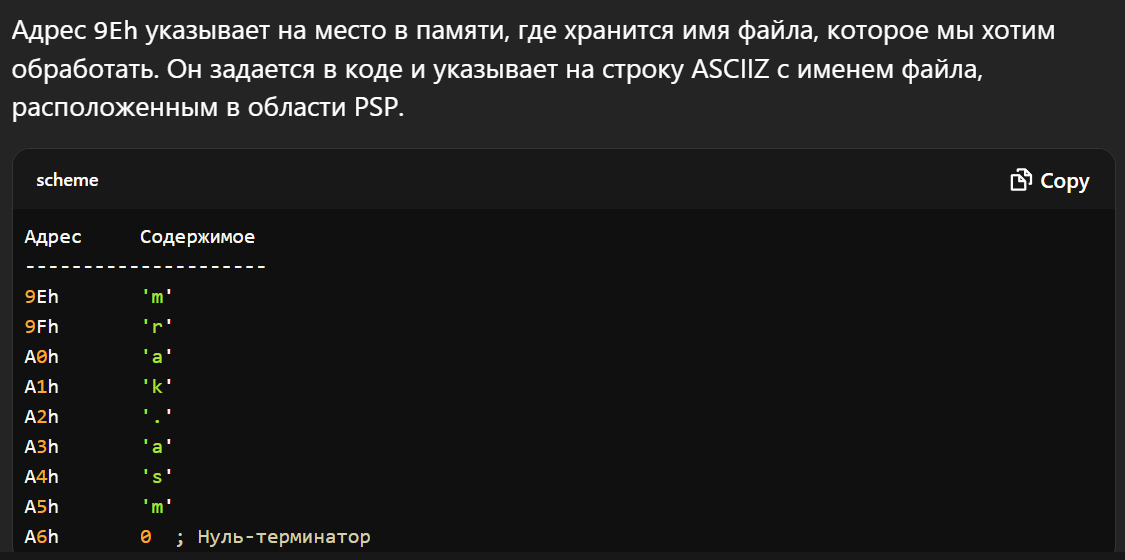
1. Первый найденный файл: mrak.asm
2. Следующие файлы могут быть, например:
   * Полное имя: test.txt, Сокращенное имя: TEST.TXT
   * Полное имя: example.doc, Сокращенное имя: EXAMP~1.DOC

**ВОПРОС 7.5: После выполнения функции 4Eh в области DTA, начиная с адреса +15h получено значение, равное 6. Что это за файл? Точнее, какие атрибуты имеет этот файл. Ответ дать на русском языке.**

Значение 6 в области DTA указывает на атрибуты файла. В двоичной форме это обозначает, что:

* Бит 2 (системный файл) установлен в 1.
* Бит 1 (скрытый файл) установлен в 1.  
  Таким образом, данный файл является скрытым и системным.

***ВОПРОС 7.6 : КАК ПОЛУЧАЕТСЯ 9Eh. Нарисовать.***

******

**Вопрос 7.7. Что такое Handle? Что значит «Открыть файл»?**

**Handle** — это дескриптор файла, который используется для управления открытым файлом в операционной системе. «Открыть файл» означает получение доступа к файлу для чтения или записи, что позволяет выполнять операции с ним, используя этот дескриптор.

***Вопрос 7.8. Что это за команда NOP? Для чего они здесь нужны? Что будет, если их убрать?***

**NOP** (No Operation) — это команда, которая ничего не делает и используется для выравнивания кода или создания задержек. Если убрать команды NOP, это может повлиять на выполнение программы, особенно если они нужны для корректного выравнивания инструкций или задержек.

***Вопрос 7.9. «…следующий совпадающий по маске файл» - «следующий» - это какой? Какие критерии «следующности»?***

«Следующий» файл — это файл, который найден в каталоге после текущего совпадения. Критерии «следующности» основаны на порядке файлов в каталоге, соответствующих заданной маске.

***Вопрос 7.10. Какая разница между командами JNB и JNL?***

**JNB** (Jump if Not Below) используется для перехода, если флаг ниже (CF=0), а **JNL** (Jump if Not Less) используется для перехода, если флаги меньше (CF=0 и ZF=0). Таким образом, JNL учитывает также условие равенства.

**Вопрос 7.11: Как известно, описание функции 31h следующее:**

**31h выходит в родительский процесс, сохраняя код выхода в AL.** Программная часть операционной системы **устанавливает распределение памяти, как определено в DX, и возвращает управление родительскому процессу, оставляя указанную память резидентной (число байт = DX \* 16).**

Функция 31h завершает выполнение текущей программы и возвращает управление родительскому процессу, сохраняя код выхода и выделяя указанное количество памяти.

**Вопрос 7.11.1. Что является «родительским процессом» когда вирус функционирует – исполняется.**

Родительским процессом является тот процесс, который запустил вирус; это может быть, например, командная оболочка или другой исполняемый файл.

**Вопрос 7.11.2. Что такое параграф и чему он равен?**

Параграф — это единица адресации в памяти, равная 16 байтам. Это означает, что адресация в памяти происходит по параграфам, и каждый параграф содержит 16 байтов.