Вариант 1.

Укажите содержимое байта по виртуальному адресу 0x01579333, если регистр CR3 содержит значение 0x13907000.

Перевод в двоичку:

0x01579333 - 0000 0001 0101 0111 1001 0011 0011 0011

0x13907000 - 0001 0011 1001 0000 0111 0000 0000 0000 - PGD

**Первое задание:**

Запишите виртуальный адрес в двоичном виде: 0000 0001 0101 0111 1001 0011 0011 0011

Дальше мы разбиваем наш адрес на 3 секции

Старшие 10 бит – индекс каталога страниц - PDI

Средние 10 бит – индекс таблицы страниц - PTI

Младшие 12 бит – смещение по странице

**Индекс каталога страниц:** 0000 0000 0101 – 0х005

**Индекс таблицы страниц: 00**01 0111 1001 – 0х179

Смещение по странице: 0011 0011 0011 – 0х333

CR3 содержит физический адрес самого верхнего уровня структуры страничной организации, называемого Page Global Directory (PGD).

Далле, с помощью смещения мы будем считать искомый физический адрес из адреса корневой таблицы страниц, то есть CR3.

Базовый адрес физической памяти страницы, мы смотрим по смещению с индексом каталога страниц:

Физический адрес записи в каталоге страниц = адрес корневой таблицы страниц + индекс каталога страниц \* 4(размер одной записи)

0x13907000 + 0х005 \* 4 = 0x13907000 + 14 = 0x13907014– далее ищем запись в нашем дампе памяти, по этому адресу

В зависимости от используемых функций процессора в регистре CR3 наряду с адресом PGD может храниться и дополнительная информация, поэтому более универсальный способ получения физического адреса PGD из регистра CR3 заключается в маскировании нижних 12 битов его содержимого.



Следовательно, дальше мы будем использовать адрес 0х13908127, так как смещение 0x5 (последние 3 байта)

По такому же принципу как вычислялся адрес таблицы страниц, вычисляем и адрес страницы:

Физический адрес страницы = Физический адрес таблицы страниц + (Индекс таблицы страниц \* размер страницы)

0х13908000 + 0х179\*4 = 0х13908000 + 0х5E4 = 0х139085E4



**Базовый адрес физической страницы памяти**: 0x25024000

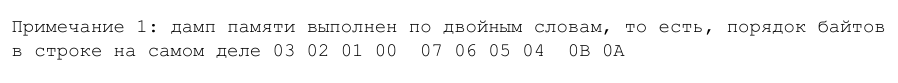
Искомый адрес мы находим по адресу страницы с использованием смещения по этой странице: 0x25024000 + 0х333

Искомый физический адрес: 0x25024333

Так как, нам представлены диапазоны адресов и адреса 0x25024333 в пуле нету, то смотрим диапазон, в который он будет входить, то есть диапазон начинающийся с 0x25024320. Такой диапазон в дампе присутствует. Рассмотрим его:  
 

Данный адрес предоставляет нам строку, содержащую 8 двухбайтовых слов с обратным (сначала младшие биты – потом старшие) порядком байтов.

По примеру:



Узнаем, что на месте 5, которое указывает на смещение, у нас находятся данные 0x75

Требуемые данные: 0x75