Вариант 3. Укажите содержимое байта по виртуальному адресу 0x001700A5, если регистр CR3 содержит значение 0x13907000.

0х означает что адреса нам представлены в шестнадцатиричной системе исчисления и мы по-быстрому всё переводим в двоичную:

0x001700A5 - 0000 0000 0001 0111 0000 0000 1010 0101

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

Первое задание сделано:

**Запишите виртуальный адрес в двоичном виде:** 0000 0000 0001 0111 0000 0000 1010 0101

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 00 – 0х0

**Индекс таблицы страниц:** 01 0111 0000 – 0х170

Смещение по странице: 0000 1010 0101 – 0хА5

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 + 0х0 \* 4 = 0x13907000 – 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 бу дем использовать адрес 0х13909127, так как нет смещения (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)

0х13909000 + 0х170\*4 = 0х13909000 + 0х05С0 = 0х139095С0

000101110000

000000000100

000000000000

000000000000

000101110000

00 0101 1100 0000



**Базовый адрес физической страницы памяти**: 0x2600300

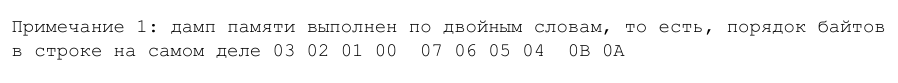
Искомый адрес мы находим по адресу страницы с использованием смещения по этой странице: 0x26003000 + 0хА5

Искомый физический адрес: 0x260030А5

Так как, нам представлены диапазоны адресов и адреса 0x260030А5 в пуле нету, то смотрим диапазон, в который он будет входить, то есть диапазон начинающийся с 0x260030А0. 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 F0

Требуемые данные: 0xF0