# Что такое переменные и как их искать?

## Что нужно знать для управления переменными в памяти

Роутер может получать доступ к симулятору в памяти и считывать или менять некоторые ячейки памяти. Нас интересуют переменные, принадлежащие как самому симулятору, так и приборам (файлы с расширением .GAU). Переменные могут иметь статический или динамический адрес. Переменные с динамическим адресом нас не интересуют, потому что они при каждой загрузке они будут находиться в новом месте. Переменные со статическим адресом для нас делятся на две части: те, что мы можем менять и те, что менять не удаётся. Следует учитывать, что неизменяемые извне переменные есть. Например, стандартные частоты COM1 и COM2, если менять их при помощи прямого доступа к памяти.

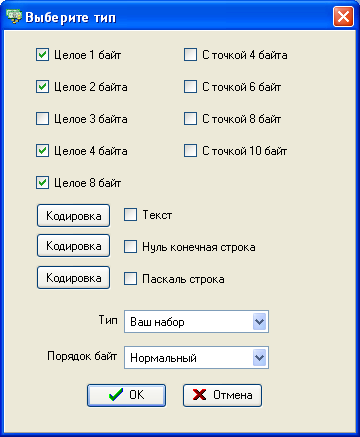
При загрузке самолёта, в память симулятора загружаются приборы «.GAU» по сути представляющие из себя обычные dll-библиотеки. Как правило, при каждой новой загрузке приборы будут загружаться по разным адресам. При поиске переменных при помощи программы artmoney, мы будем находить абсолютные смещения переменной относительно адреса, по которому загружен в данный момент симулятор. При следующей загрузке абсолютный адрес переменной будет другим, однако, относительно смещение от начала модуля в памяти для статической переменной останется тем же. Следовательно, для определения смещения переменной в модуле, нужно из её абсолютного адреса вычесть абсолютный адрес модуля в памяти. Для упрощения этого процесса в каждом окне добавления элемента типа «доступ к памяти» существует область «Определение модуля и относительного смещения». После ввода абсолютного смещения и нажатия кнопки «Определить», будут заполнены поля «Смещение» и «Модуль». Для того чтобы всё определялось правильно, поиск переменной и определение её относительного смещения должно производиться «в один приём» при работающем симуляторе и загруженном самолёте.

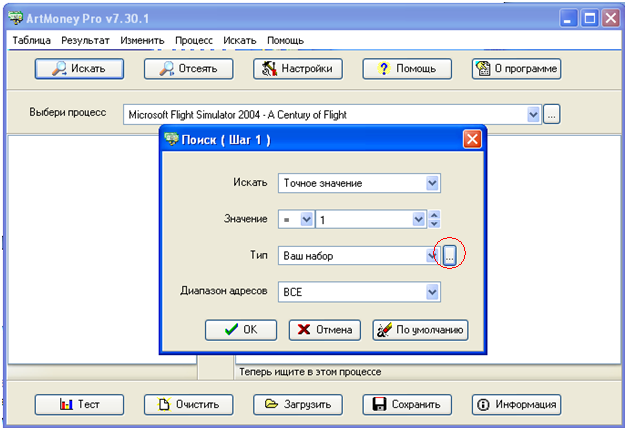


## Поиск переменных в памяти

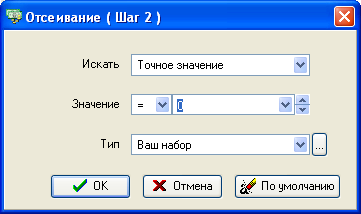
Сейчас я покажу, как можно найти переменную, а потом объясню некоторые подробности. Искать будем переменную «питание» на панели «НВУ» самолёта ПТ Ту-154М версии 2.02 для симулятора Microsoft Flight Simulator 2004. Итак, приступим. Загружаем симулятор и самолёт. Переводим симулятор для удобства в оконный режим (Alt+Enter). Включаем тумблер «Сеть». 

Запускаем ArtMoney, выбираем процесс «Microsoft Flight Simulator 2004 – A century of flight», нажимаем кнопку «Искать». Предполагаем, что тумблер, имеющий два положения, скорее всего в памяти будет представлен целыми числами 0 – выключено, 1 – включено. Жмём кнопку выбора типа данных (выделено красным), оставляем только целые значения длиной 1, 2, 4, 8 байт. И жмём «Ок» (Учитывайте, что чем больше выбрано типов данных, тем дольше производится поиск).

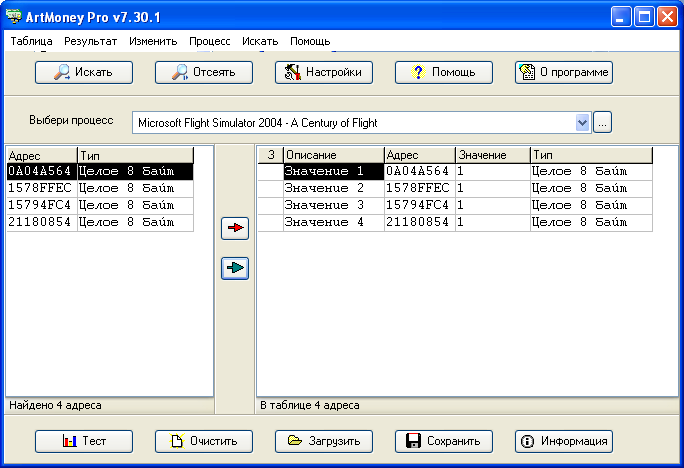




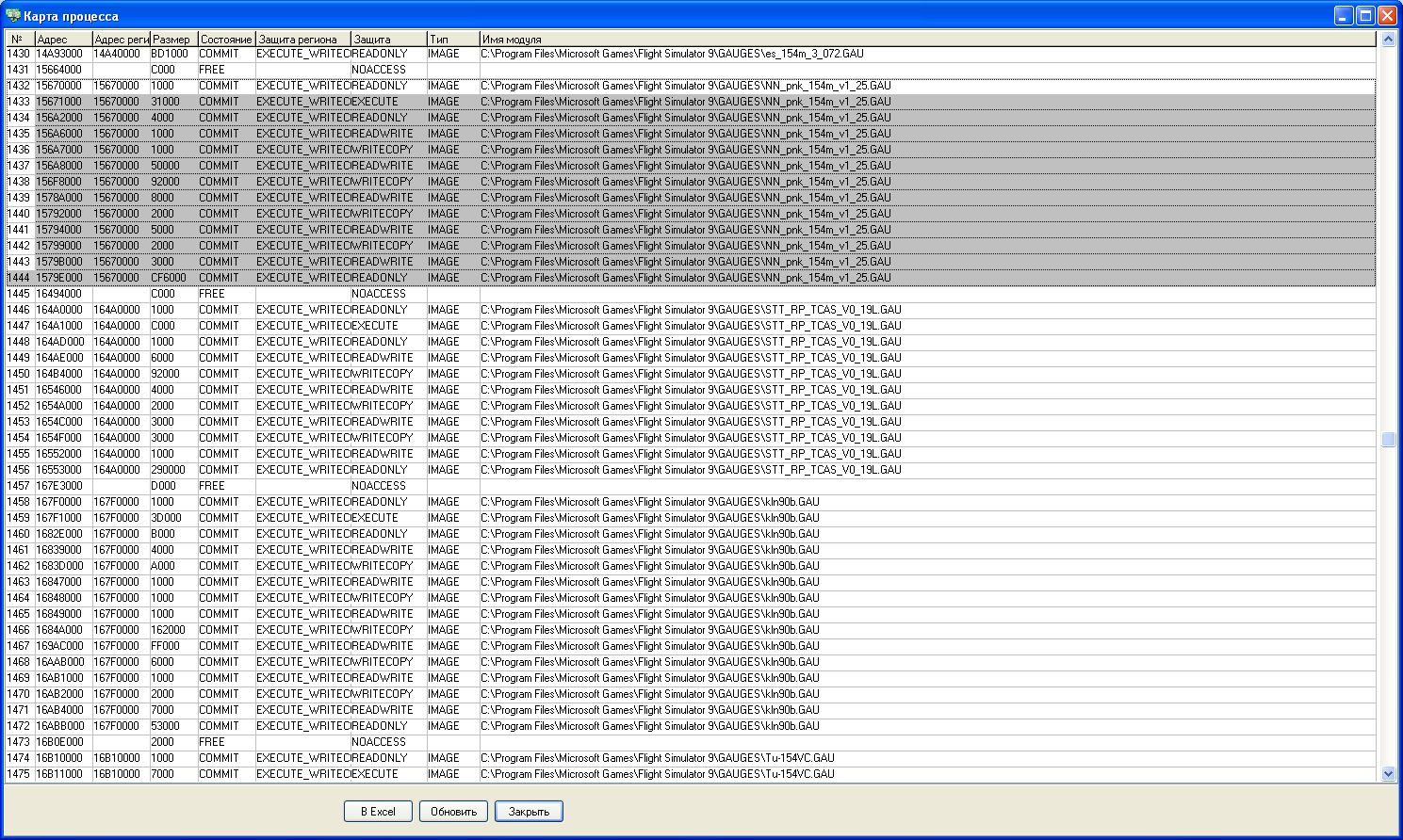
В поле «Значение» пишем «1». Жмём «Ок». Видим, что найдено много совпадений. Теперь выключаем тумблер «Сеть» в самолёте и жмём в ArtMoney «Отсеять», в поле «Значение» пишем «0» и нажимаем «Ок».

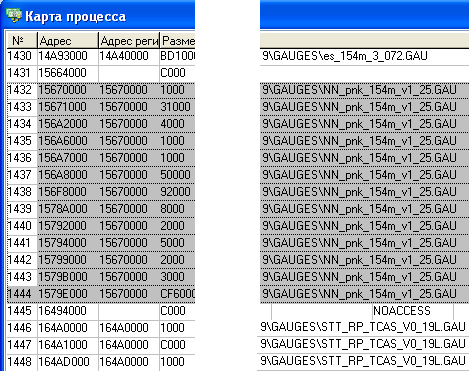


Опять включаем тумблер «Сеть», нажимаем кнопку «Отсеять», значение «1», далее «Ок», выключаем тумблер «Сеть», нажимаем кнопку «Отсеять», значение «0», далее «Ок». И так до тех пор, пока не останется несколько вариантов. У меня получилось 4. Жмём зелёную стрелку и варианты отображаются в правой части окна.

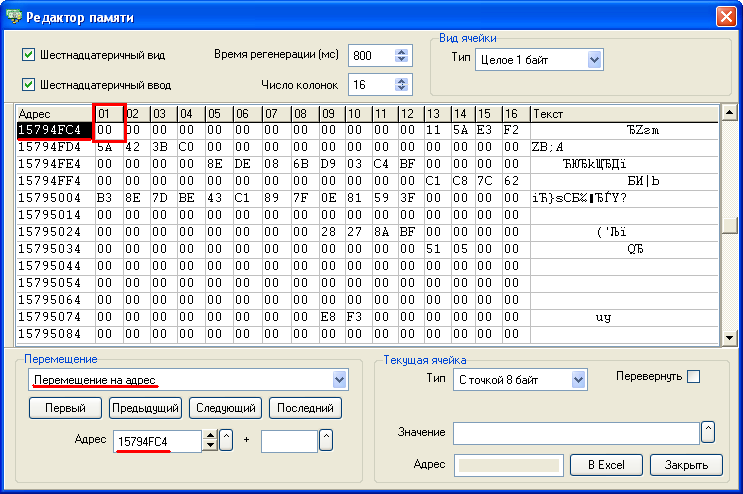


Теперь для того, чтобы узнать, какой из найденных адресов нам нужен, меняем значения в пределах 0-1 для каждого адреса. Если тумблер в самолёте перещёлкивается – это искомый адрес. В моём случае это «Значение 3». Запоминаем адрес 15794FC4 и открываем «Процесс»->«Карта процесса». Ищем, какому модулю принадлежит адрес.

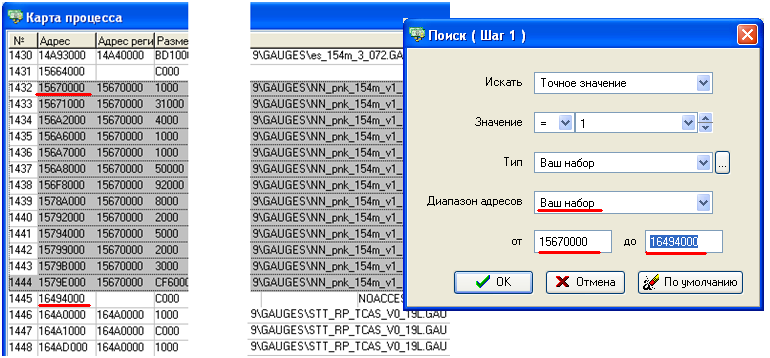




Обнаруживаем, что это процесс NN\_pnk\_154m\_v1\_25.GAU, который начинается с адреса 15670000 (шестнадцатеричная система счисления). Открываем калькулятор, переводим его в «инженерный режим», выбираем шестнадцатеричную систему счисления «Hex». Вычитаем из найденного нами адреса адрес начала процесса NN\_pnk\_154m\_v1\_25.GAU. 15794FC4-15670000=124FC4. 124FC4 – это смещение переменной в модуле NN\_pnk\_154m\_v1\_25.GAU. Статичность переменной можно проверить следующим образом: перезагрузить самолёт, в «карте процесса» убедиться, что модуль загружен по другому адресу и запомнить его адрес. В ArtMoney открыть «Процесс»->«редактор памяти», перейти на адрес (адрес модуля + найденное нами смещение). Попробовать поменять значение и убедиться, что тумблер в самолёте щёлкает.



Теперь, зная модуль, в котором реализована система «НВУ», можно искать переменные быстрее. Указав диапазон адресов, среди которых нужно искать.



## Выбор размера переменных и значений для поиска

Самые распространённые типы целых переменных: 1,2,4,8 байт, самый распространённый тип значений с точкой (запятой) – 8 байт.

## Примеры, с которыми я столкнулся при поиске переменных для ПТ Ту-154М

1. Основная масса двухпозиционных переключателей (тумблеров) принимает значения 0 и 1. Однако значения некоторых тумблеров перевёрнуты. То есть в том положении тумблера, при котором я предполагал найти ноль, на самом деле была единица.
2. Один из переключателей имел значения 0 и 2.
3. Трёхпозиционные тумблеры принимали значения -1, 0, 1 или 0, 1, 2. И иногда прядок следования цифр не соответствовал порядку следования положений тумблера.
4. Галетные переключатели, как правило, принимали значения от нуля и выше с шагом 1. Однако на панели НВУ они имели и отрицательные значения. На картинке левый переключатель принимает значения от -4 до +4, правый от -1 до +5.

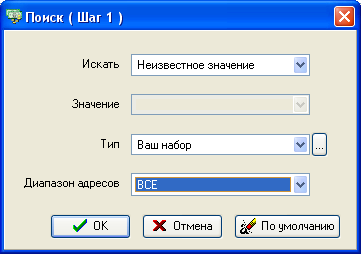


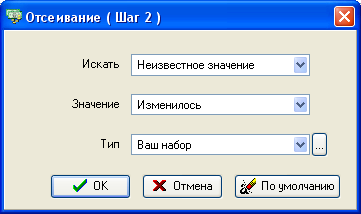
1. Расстояния на панели НВУ были 8 байтными числами с точкой и оперировали метрами. Единица на табло – это 1 километр. В переменную записывалось 1000 метров. Один щелчок мыши добавлял или отнимал по 10 метров.
2. Нефиксируемые тумблеры и кнопки я искал так: нажимаем на тумблер или кнопку, жмём Esc. Ищем переменную кнопки в нажатом состоянии. Нажимаем Esc ещё раз и ищем переменную кнопки в отжатом состоянии.

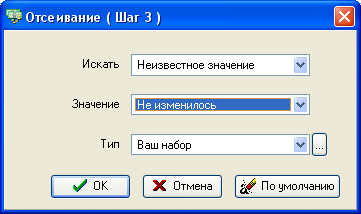
Для более глубокого понимания рекомендую изучить документацию к ArtMoney.

## Более точный способ поиска переменных

Практика показывает, что не всегда можно угадать значения, которые принимает переменная, а также не всегда, например, переключение тумблера использует только одну переменную. Например, тумблер «Аккумулятор №1» на панели бортинженера в самолёте ПТ Ту-154М управляет двумя переменными. Первая – положение тумблера, вторая – собственно, включение аккумулятора в сеть. Для того чтобы найти все переменные, которые изменяются при, например, нажатии кнопки, можно воспользоваться поиском неизвестного значения. Суть в следующем: ищем неизвестное значение, переключаем тумблер, выбираем «Отсеять»-> «Неизвестное значение»-> «Изменилось». Следующим шагом, например, не переключаем тумблер и выбираем «Отсеять»-> «Неизвестное значение»-> «Не изменилось»







Таким образом, будут найдены все изменяемые значения. Скорее всего, будут найдены две группы переменных, те, которые нужно изменять принудительно и те, некоторые будут изменяться сами в зависимости от состояния изменяемых принудительно.