

<https://ssl.exelab.ru/f/index.php?action=vthread&forum=3&topic=20942>

diff_trace (Different TRACE) – программа для сравнения двух логов трассировки(Trace Log) отладчика **OllYDbg**. Идея сравнения возникла после того, как автор увидел отображение лога трассировки(далее по тексту **ТРЕЙСОВ**) в **Notepad++**, который нумерует строки.

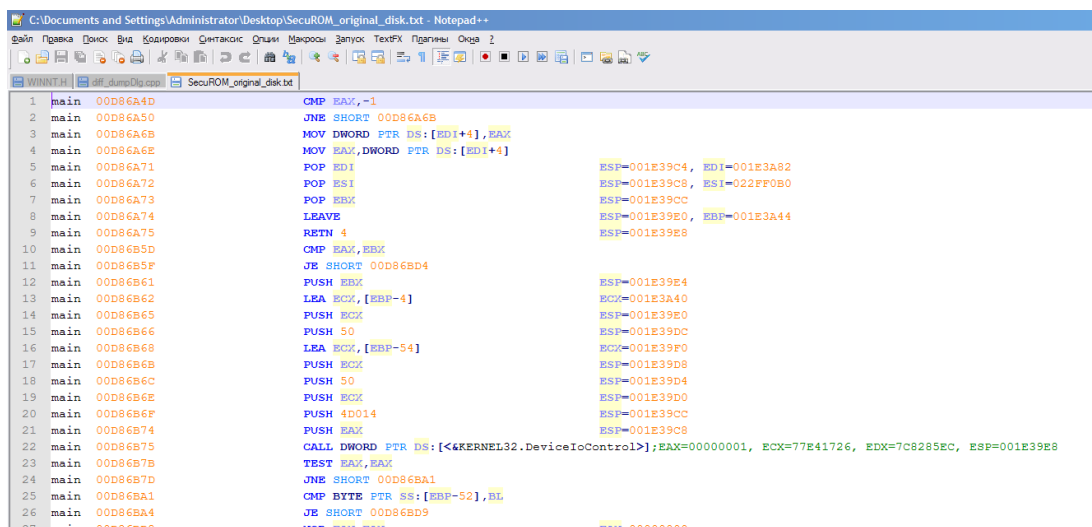
Красным выделена область, ответственная за загрузку трейсов.

Голубым выделена область настроек асинхронного режима работы. При снятой галочке активен **синхронный** режим.

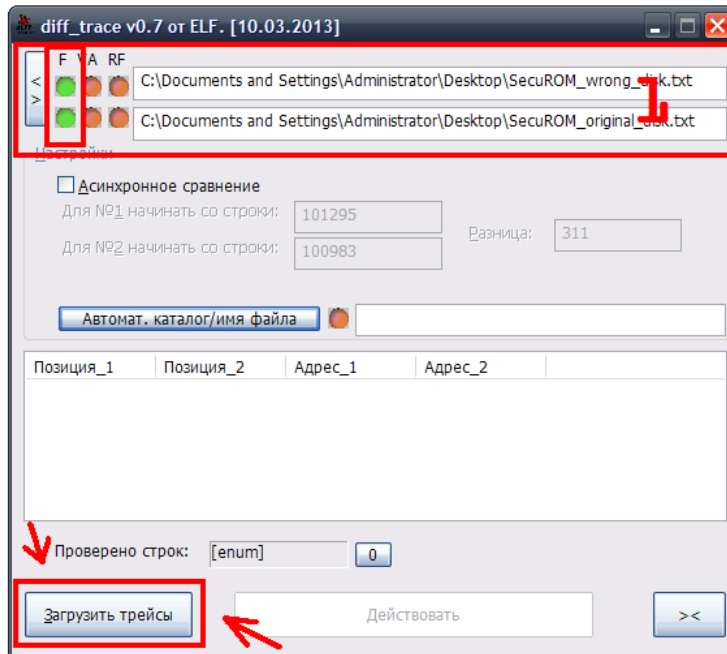
Синим выделена область настроек режима работы с исключениями. При нажатии кнопки **><**, происходит свертывание/развертывание (соответственно дезактивация/активация данного режима) панели настроек исключений.

Фиолетовым выделена область(listbox №1), вывода результатов.

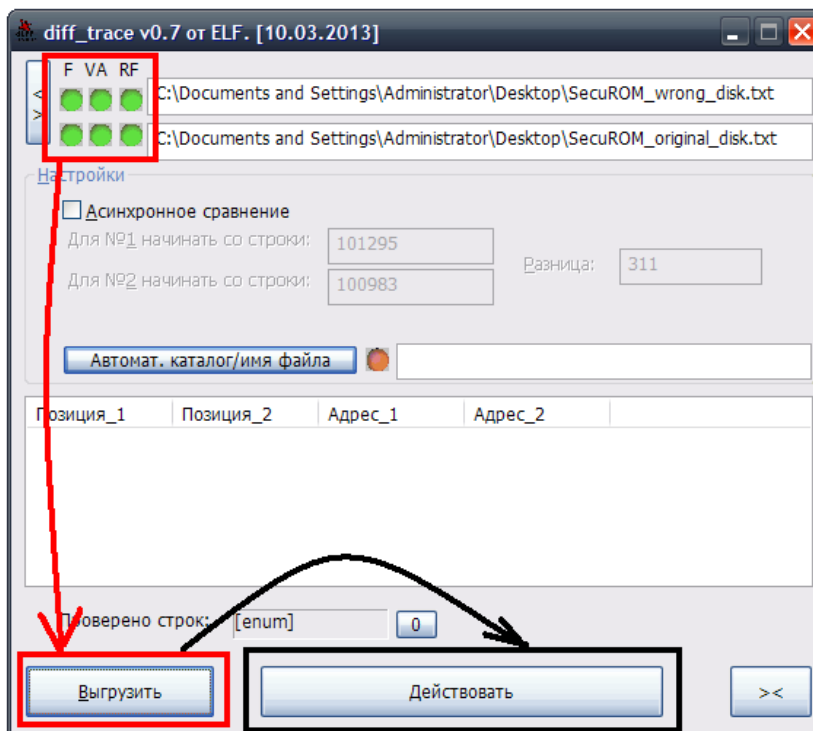
Черным обведена кнопка, при нажатии которой появляется результат(если трейсы не идентичны и оформлены по обычному стилю OllYDbg).



1. Начало работы



- 1.1 Вбейте пути к двум трейсам в edit'бохы (область, выделенная **красной** пиктограммой с цифрой **1**). Если оба пути верны, то будут гореть **зеленые** лампочки под буквой **F**(Флаг Find), в противном случае **красная** лампочка сигнализирует об ошибочном пути к файлу.
- 1.2 Флаги Find **зеленые**. Загружаем трейслоги. (кнопка, выделенная **красной** пиктограммой)

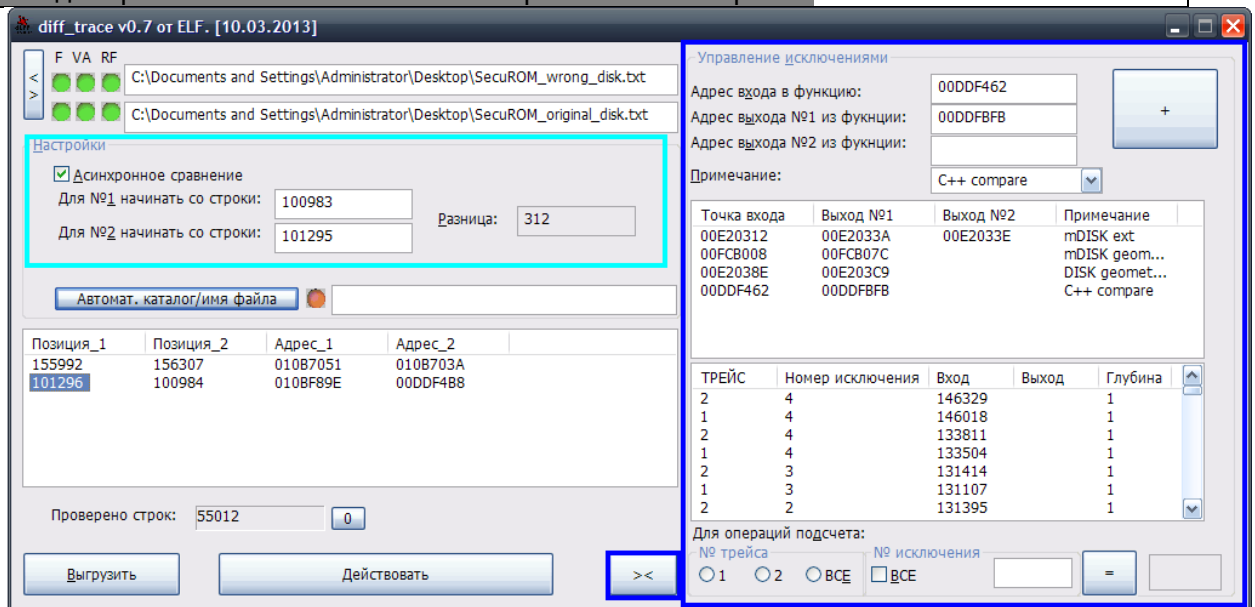


- 1.3 Если загрузка прошла в штатном режиме, все 6 лампочек будут гореть **зеленым** цветом. Также кнопка **Действовать** станет доступной.

Флаг VA	результат работы WinAPI VirtualAlloc
Флаг RF	результат работы WinAPI ReadFile

1.4 Выбираем режим работы.

Синхронный	Активен изначально. Деактивируется, если установлена галочка «Асинхронное сравнение».	Начинает процесс синхронного сравнения немедленно с первых строк (<i>адресов</i>) обоих трейсов до первого попавшегося различия по адресам.
Асинхронный	Активен, если установлена галочка «Асинхронное сравнение».	В соответствии с заданными строками (которые могут быть не равны) перемещается на указанные позиции и начинает процесс сравнения с них.
Синхронный/Асинхронный С исключениями	Взаимосвязан с первыми двумя режимами. Активен при развернутой панели настроек исключений.	Сочетает в себе возможности первых двух режимов с добавлением исключений .
Под каждый режим имеет свой оптимизированный алгоритм.		



Асинхронный с исключениями

1.4.1 Синхронный/Асинхронный с исключениями

Исключения задаются в виде hex-адреса

- **Обязательный параметр.** начала(входа) участка кода(функции), например *PUSH EBP*.

00DDF462	55	PUSH EBP	spirun.itoa_spez(guessed Arg1,Arg2,Arg3)
00DDF463	8DAC24 20FEF	LEA EBP,[LOCAL.128]	
00DDF46A	81EC 6002000	SUB ESP,260	
00DDF470	A1 C4C72E01	MOV EAX,DWORD PTR DS:[12EC7C4]	
00DDF475	8B8D F001000	MOV ECX,DWORD PTR SS:[EBP+1F0]	
00DDF47B	33C5	XOR EAX,EBP	
00DDF47D	8985 DC01000	MOV DWORD PTR SS:[EBP+1DC],EAX	
00DDF483	8B85 F001000	MOV EAX,DWORD PTR SS:[EBP+1E0]	

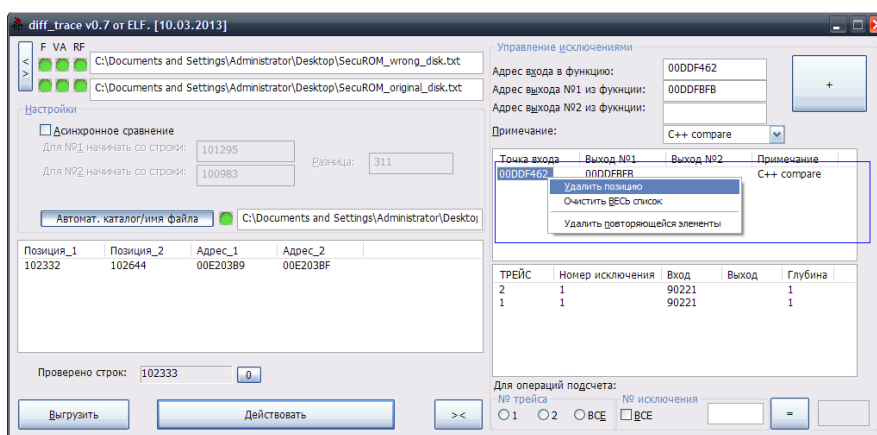
- **Обязательный параметр.** Окончания(выхода) №1 участка кода(функции), например *retn*.

00DDFBDB	84DB	TEST BL,BL	
00DDFBDB	0F85 D3F8FFF	JNE 00DDF4B4	
00DDFBE1	5F	POP EDI	
00DDFBE2	5E	POP ESI	
00DDFBE3	8B8D DC01000	MOV ECX,DWORD PTR SS:[EBP+1DC]	
00DDFBE9	8B45 BC	MOV EAX,DWORD PTR SS:[EBP-44]	
00DDFBEC	33CD	XOR ECX,EBP	
00DDFBEE	5B	POP EBX	
00DDFBEF	E8 F6000000	CALL 00DDFCEA	
00DDFBF4	81C5 E001000	ADD EBP,1E0	
00DDFBFA	C9	LEAVE	
00DDFBFB	C3	RETN	

- **По усмотрению.** Окончания(выхода) №2 участка кода(функции), если функция имеет два выхода.

- **По усмотрению.** Комментарии к участку кода (функции).

Добавление осуществляется большой кнопкой «+».



Удаление осуществляется вызовом меню правой кнопкой на выбранном элементе. Меню присутствует во всех трех listbox.

1.5 «Действовать»

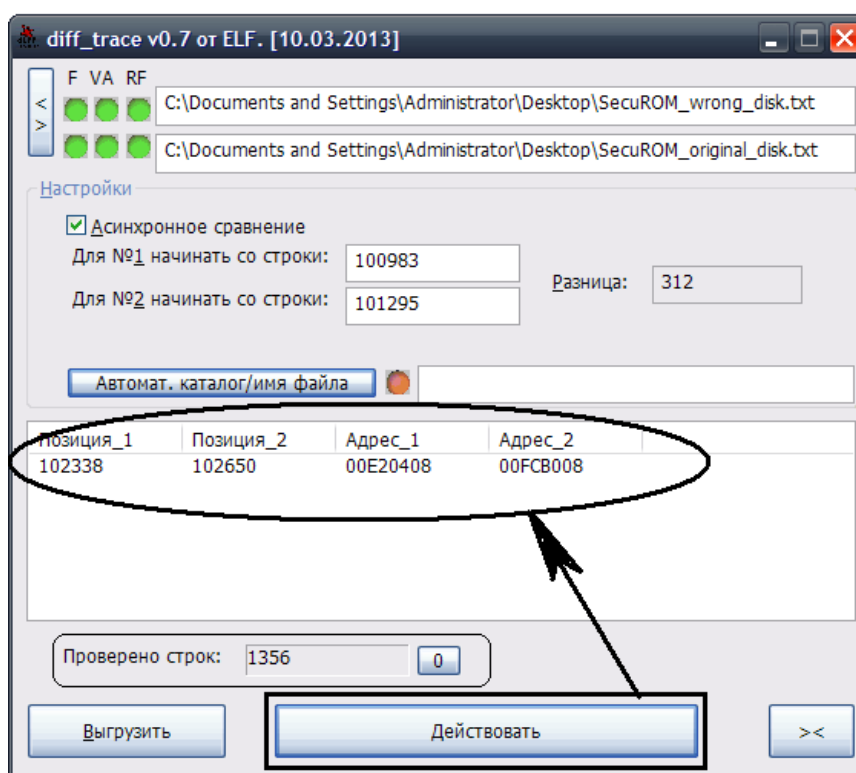
Трейслоги загружены. Режим выбран. Жмем кнопку **«действовать»**.

В версии 0.7 идентификация строк происходит по слову **main**.

main 00D86A71 POP EDI ESP=001E39C4, EDI=001E3A82

Между *main* и адресом в идеале должно быть ровно 2 пробела. По крайней мере OllyDbg 2.0 оставляет 2 пробела.

В основном **listbox**'е должен появиться результат, если логи трассировки не идентичны.



Позиция_1 указывает на номер строки от начала файла (асм инструкции) в логе трассировки №1 (верхний **exitbox**- C:\Documents and Settings\Administrator\Desktop\SecuROM_original_disk.txt). Соответственно, **Позиция_2** указывает на номер строки от начала файла (асм инструкции) в логе трассировки №2 (**exitbox** ниже - C:\Documents and Settings\Administrator\Desktop\SecuROM_wrong_disk.txt). То же самое и с адресами.

1.6 Окончание работы

Выгружаем трейслоги(*VirtualFree*) с памяти соответствующей кнопкой. При необходимости, сохраняем в файл результаты. Если путь не указан предварительно или не была задействована автомат. генерация пути/фала, возникает диалоговое окно «Save as»(Сохранить как).

