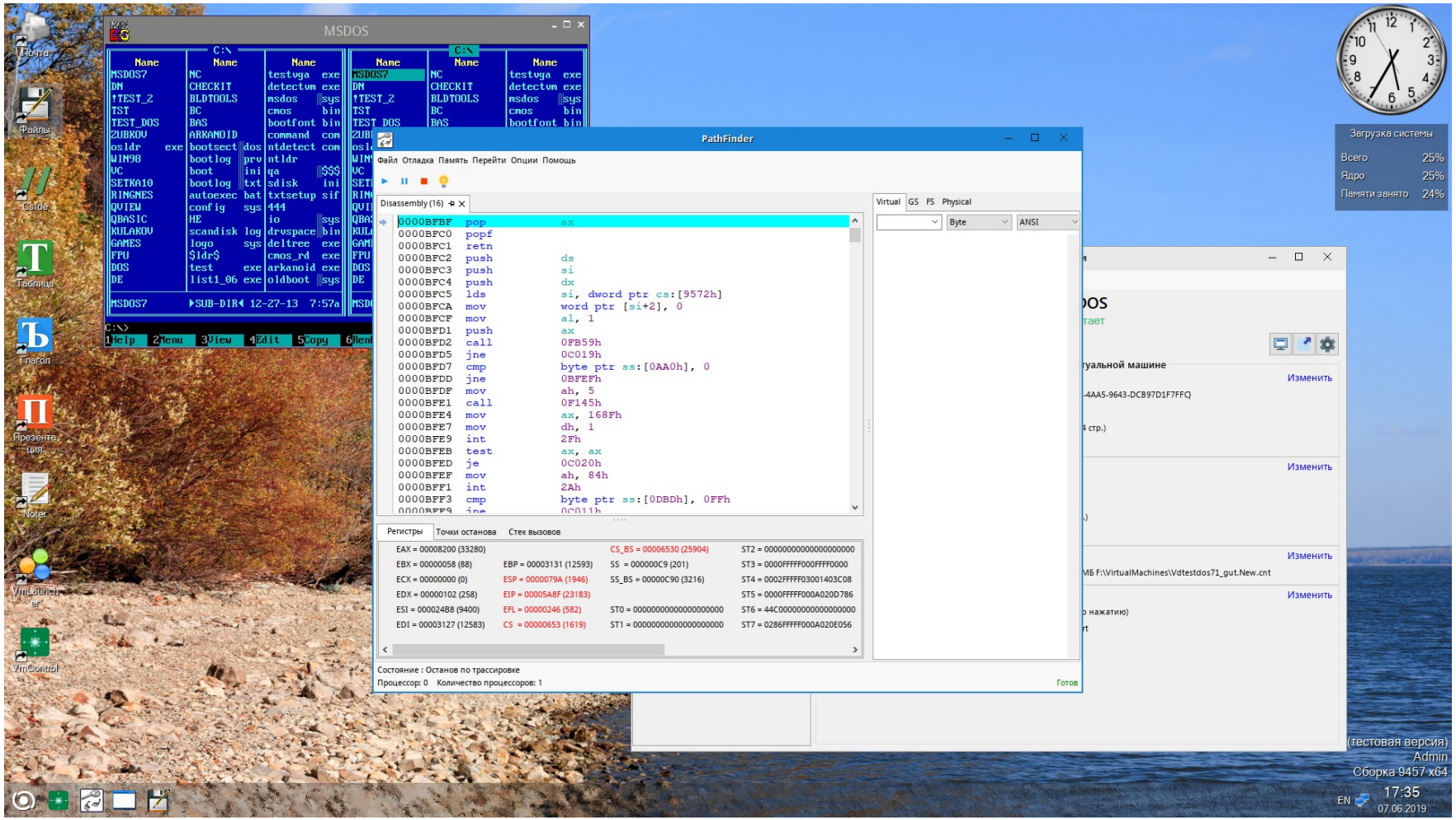
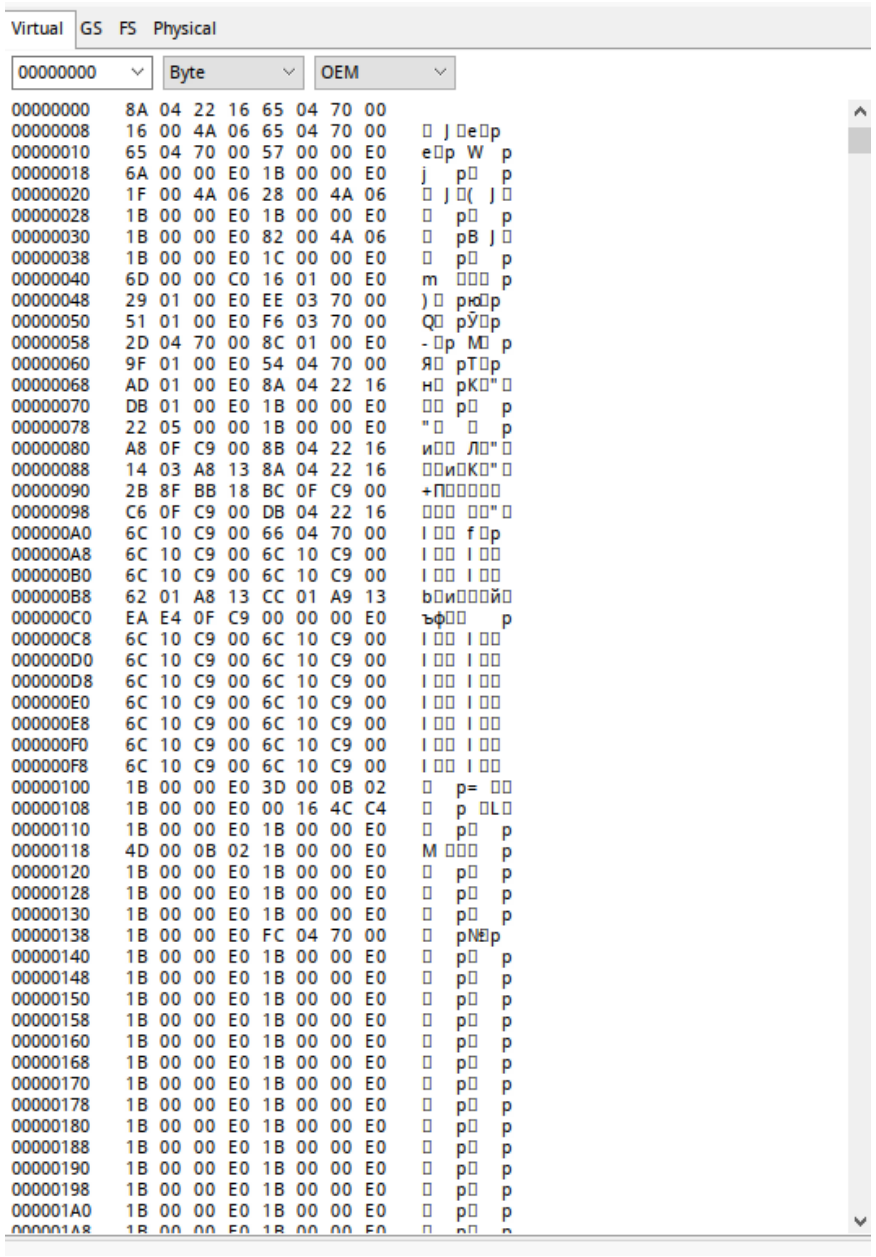
Отладчик виртуальных машин PathFinder

Исходная цель создания отладчика

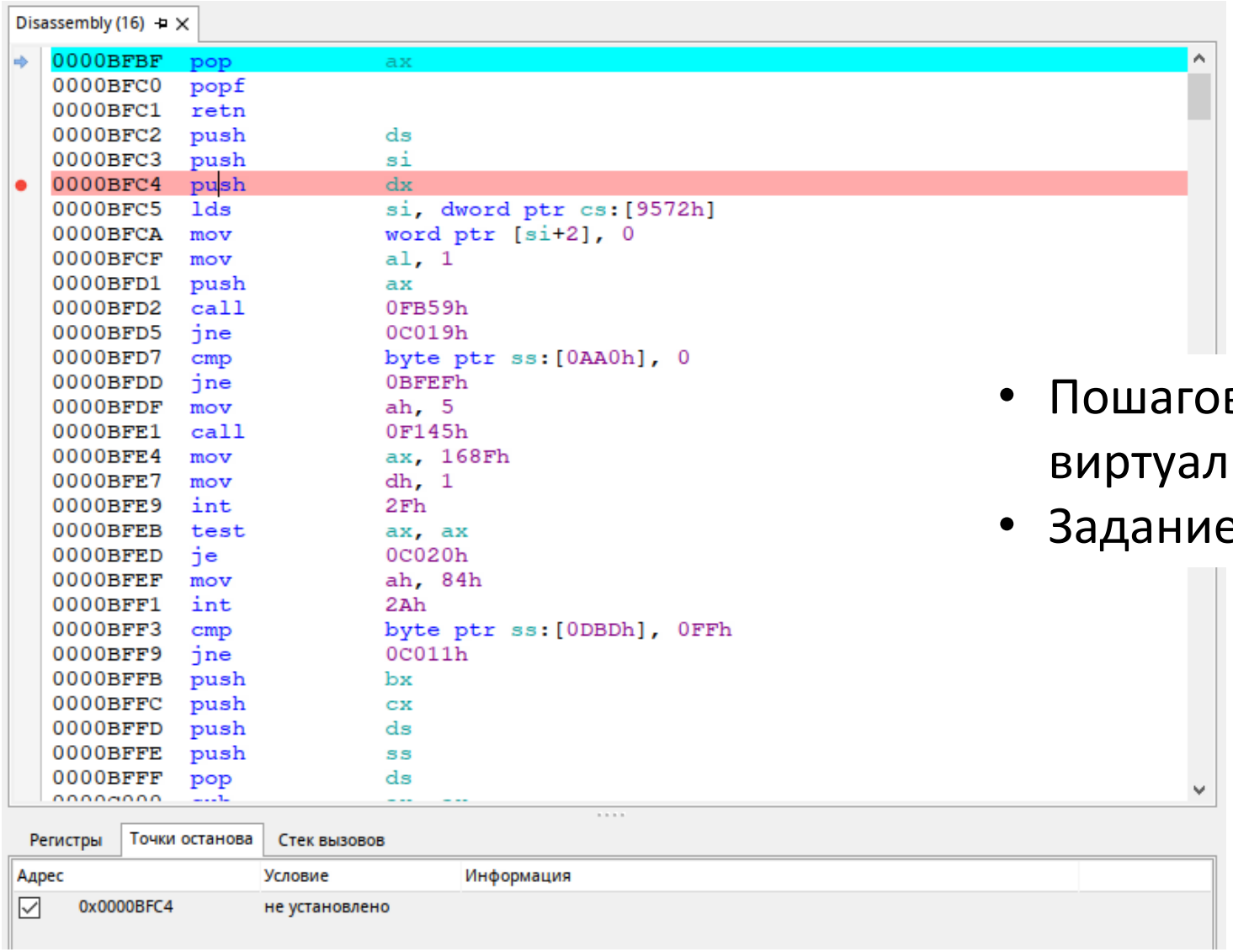
- Отладчик PathFinder создан в связи с необходимостью контроля за исполнением гипервизором инструкций виртуальной машины;
- Отладчик работает в связке с операционной системой QP ОС и гипервизором QP VMM;
- PathFinder является дополнительным инструментом и не входит в стандартную сборку гипервизора QP VMM.

Внешний вид PathFinder



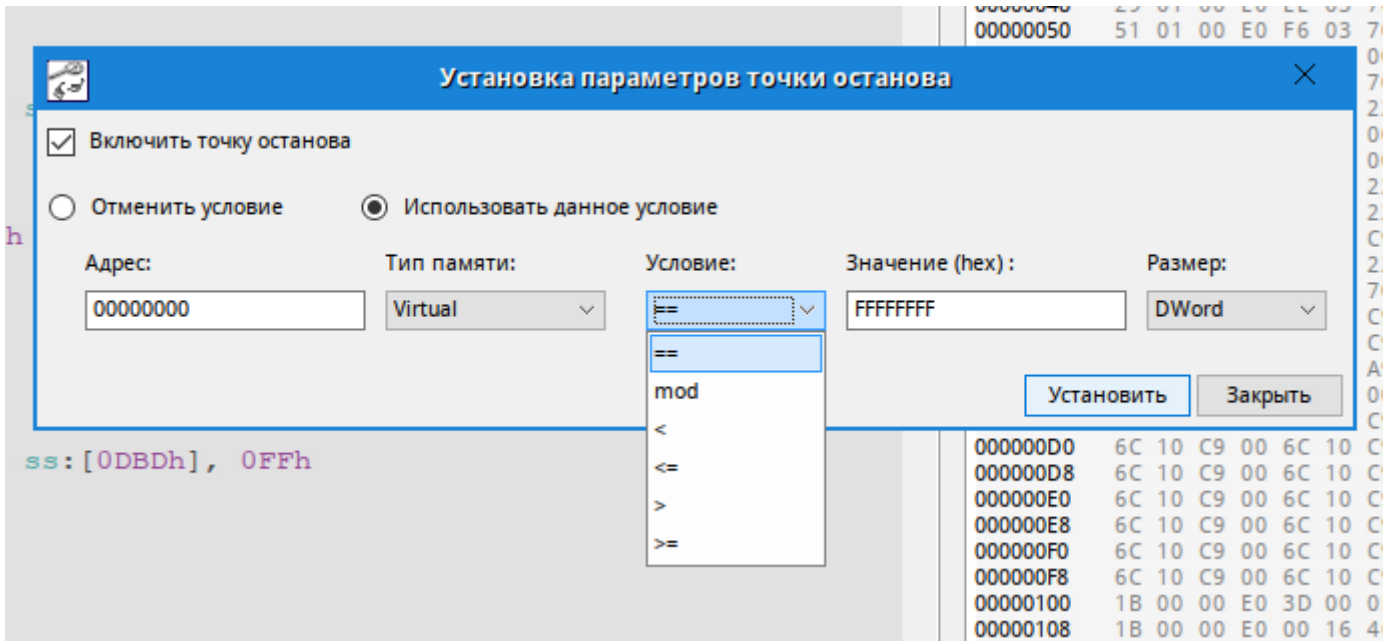


- Просмотр виртуальной и физической памяти



- Пошаговое исполнение виртуальной машины
- Задание точек останова

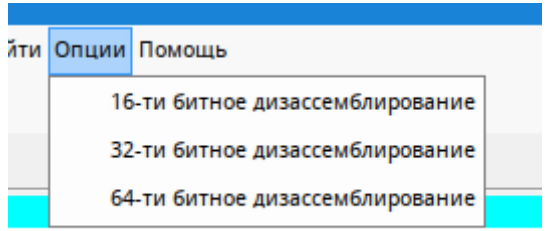
PathFinder



- Задание точек останова с условием

Disassembly (64)

```
000000000000BFBF  pop           rax
000000000000BFC0  popfq
000000000000BFC1  retn
000000000000BFC2  push          ds
000000000000BFC3  push          rsi
000000000000BFC4  push          rdx
000000000000BFC5  lds           esi, fword ptr [rsi]
000000000000BFC8  jb            000000000000BF5Fh
000000000000BFCA  mov           dword ptr [rdx+rax], 5001B000h
000000000000BFD2  call          000000004275FB5Bh
000000000000BFD7  cmp           byte ptr [rsi], 0A0h
000000000000BFDB  or            al, byte ptr [rax]
000000000000BFDD  jne           000000000000BFEFh
000000000000BFDF  mov           ah, 5
000000000000BFE1  call          0FFFFFFFF8FB8F147h
000000000000BFE6  push          ss
000000000000BFE7  mov           dh, 1
000000000000BFE9  int           2Fh
000000000000BFEB  test          eax, eax
000000000000BFED  je            000000000000C020h
000000000000BFEF  mov           ah, 84h
000000000000BFF1  int           2Ah
000000000000BFF3  cmp           byte ptr [rsi], 0BDh
000000000000BFF7  or            eax, 531675FFh
000000000000BFFC  push          rcx
000000000000BFFD  push          ds
000000000000BFFE  push          ss
000000000000BFFF  pop           ds
000000000000C000  sub           eax, eax
000000000000C002  call          0FFFFFFFFEBE8C307h
```



- Отладчик автоматически определяет режим дизассемблирования на основе анализа системных регистров;
- Режим дизассемблирования можно задать вручную

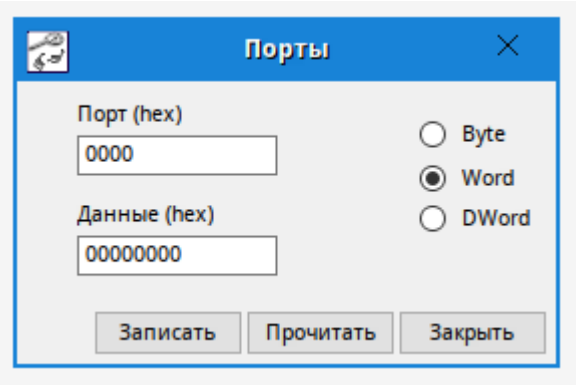
Регистры | Точки останова | Стек вызовов

EAX = 00008200 (33280)	ES = 000028AD (10413)	DR7 = 00000400 (1024)	MM2 = 0000000000000000
EBX = 00000058 (88)	ES_BS = 00028AD0 (166608)		MM3 = FFFFF000FFFF0000
ECX = 00000000 (0)	FS = 00000000 (0)	ST0 = 00000000000000000000	MM4 = FFFFF03001403C08
EDX = 00000102 (258)	FS_BS = 00000000 (0)	ST1 = 00000000000000000000	MM5 = FFFFF000A020D786
ESI = 000024B8 (9400)	GS = 00000000 (0)	ST2 = 00000000000000000000	MM6 = 0000000000000000
EDI = 00003127 (12583)	GS_BS = 00000000 (0)	ST3 = 0000FFFFF000FFFF0000	MM7 = FFFFF000A020E056
		ST4 = 0002FFFFF03001403C08	
EBP = 00003131 (12593)	CR0 = 00000000 (0)	ST5 = 0000FFFFF000A020D786	XMM0 = 0000000000000000 0000000000000000
ESP = 0000079A (1946)	CR2 = 00000000 (0)	ST6 = 44C00000000000000000	XMM1 = 0000000000000000 0000000000000000
EIP = 00005A8F (23183)	CR3 = 00030000 (196608)	ST7 = 0286FFFFF000A020E056	XMM2 = 0000000000000000 0000000000000000
EFL = 00000246 (582)	CR4 = 00000000 (0)	FPS = FFFF (65535)	XMM3 = 0000000000000000 0000000000000000
CS = 00000653 (1619)	TR = 00000028 (40)	FPC = 0000 (0)	XMM4 = 0000000000000000 0000000000000000
CS_BS = 00006530 (25904)		FPT = 0000 (0)	XMM5 = 0000000000000000 0000000000000000
SS = 000000C9 (201)	DR0 = 00000000 (0)	FIP = 00000000 (0)	XMM6 = 0000000000000000 0000000000000000
SS_BS = 00000C90 (3216)	DR1 = 00000000 (0)	FDP = 00000000 (0)	XMM7 = 0000000000000000 0000000000000000
	DR2 = 00000000 (0)		MXCSR = 00000000 (0)
DS = 000000C9 (201)	DR3 = 00000000 (0)	MM0 = 0000000000000000	
DS_BS = 00000C90 (3216)	DR6 = FFFF0FF0 (4294905840)	MM1 = 0000000000000000	

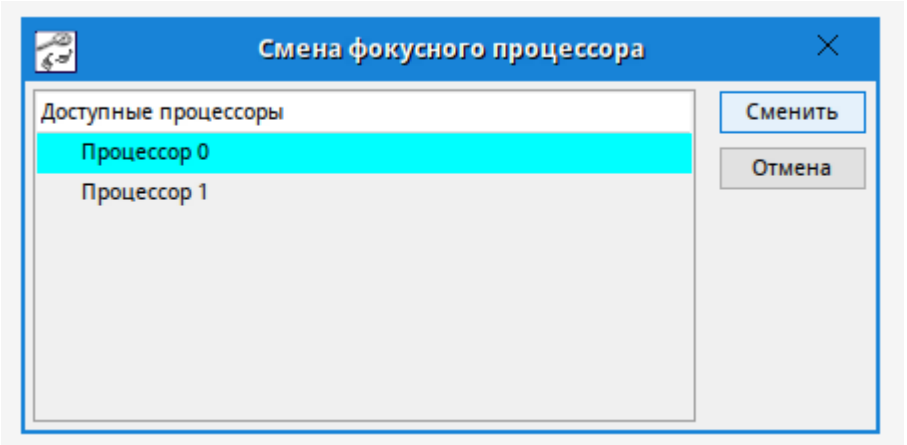
Регистры | Точки останова | Стек вызовов

EAX = 00008200 (33280)
EBX = 00000058 (88)
ECX = 00000000 (0)
EDX = 00000102 (258)
ESI = 000024B8 (9400)
EDI = 00003127 (12583)

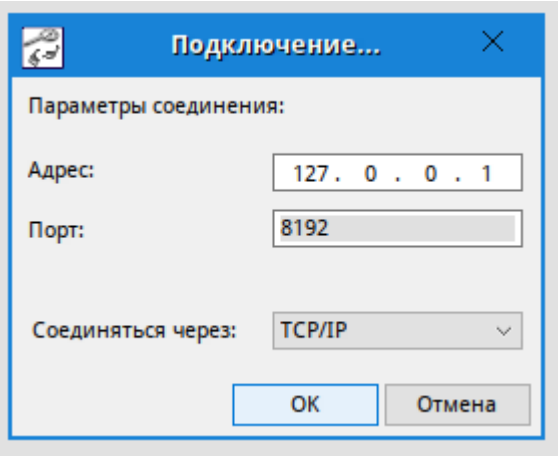
- Отладчик отображает и позволяет управлять большинством регистров процессора;
- Отображение регистров можно настраивать.



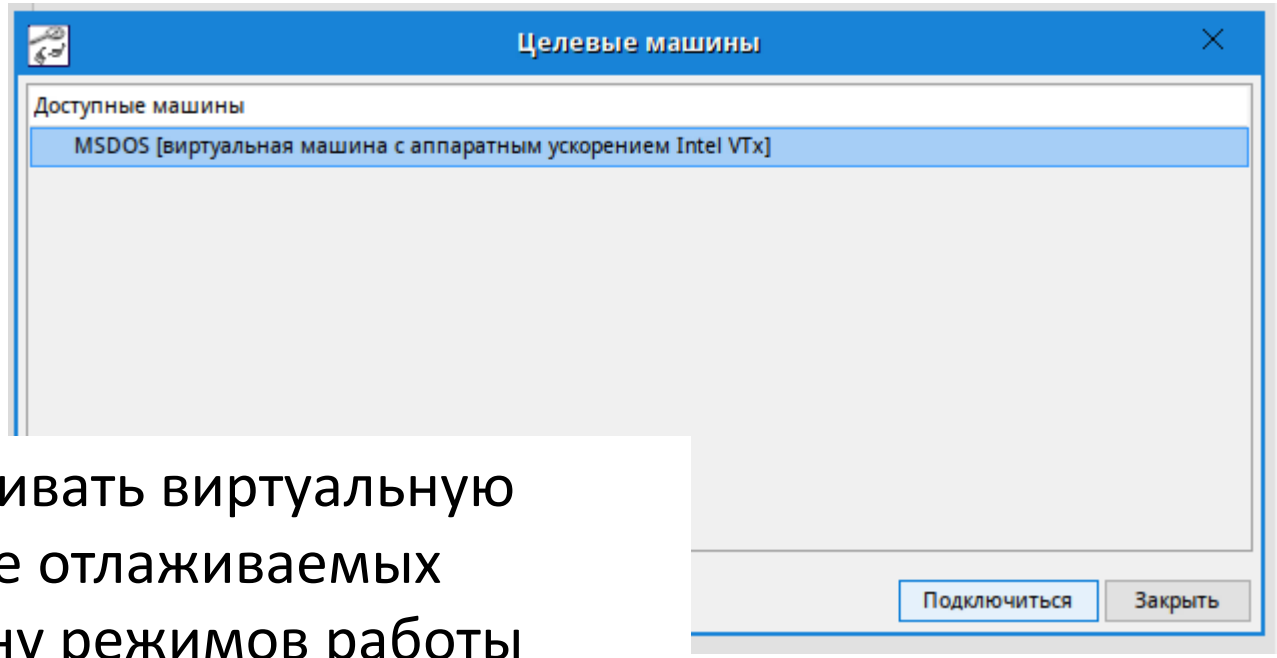
- Можно выполнять операции с портами ввода вывода.



- Можно переключаться между процессорами виртуальной машины.



- PathFinder связывается с гипервизором по протоколу TCP



- PathFinder позволяет отлаживать виртуальную машину на участках кода, не отлаживаемых другими отладчиками: смену режимов работы процессора, настройку виртуальной памяти, переключение TSS и.т.д.

- PathFinder находится в состоянии бета-версии. Он может быть доработан до коммерческого продукта при наличии заинтересованных организаций и предприятий.

Благодарю за внимание!

Вопросы?