



ОНЛАЙН-ОБРАЗОВАНИЕ

Меня хорошо слышно
&& видно?



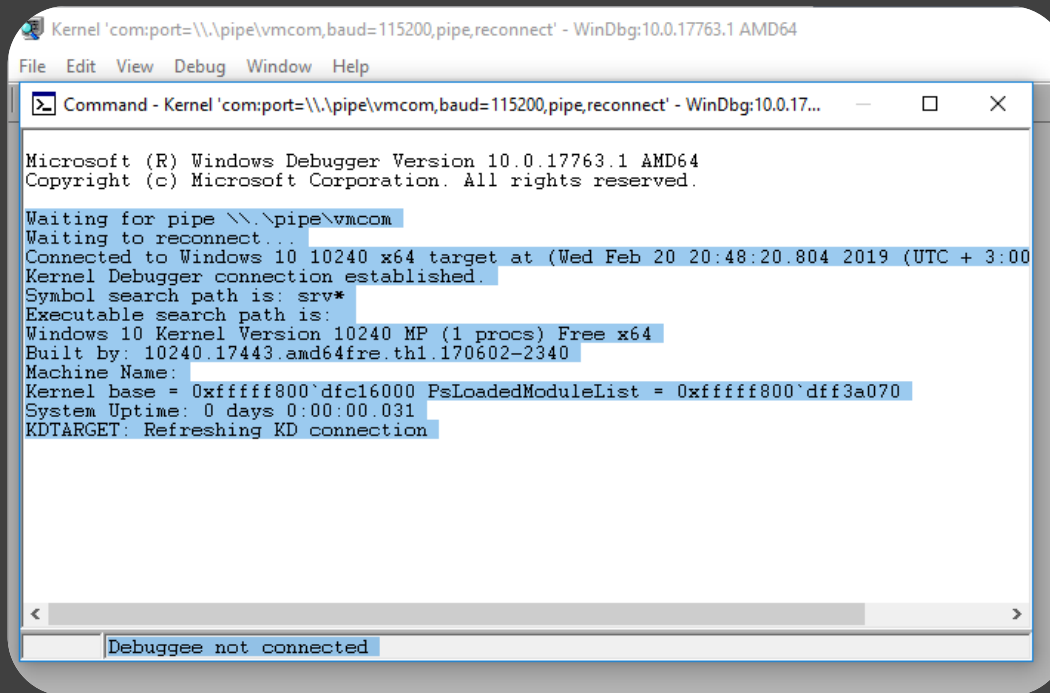
Напишите в чат, если есть проблемы!

Ставьте если все хорошо

Настройка рабочей среды для отладки драйверов режима ядра



Основная OS - Windows 7 x86



```
Kernel 'com:port=\\.\pipe\vmcom,baud=115200,pipe,reconnect' - WinDbg:10.0.17763.1 AMD64
File Edit View Debug Window Help
Command - Kernel 'com:port=\\.\pipe\vmcom,baud=115200,pipe,reconnect' - WinDbg:10.0.17...
Microsoft (R) Windows Debugger Version 10.0.17763.1 AMD64
Copyright (c) Microsoft Corporation. All rights reserved.
Waiting for pipe \\.\pipe\vmcom
Waiting to reconnect...
Connected to Windows 10 10240 x64 target at (Wed Feb 20 20:48:20.804 2019 (UTC + 3:00)
Kernel Debugger connection established.
Symbol search path is: srv*
Executable search path is:
Windows 10 Kernel Version 10240 MP (1 procs) Free x64
Built by: 10240.17443.amd64fre.th1.170602-2340
Machine Name:
Kernel base = 0xfffff800`dfc16000 PsLoadedModuleList = 0xfffff800`dff3a070
System Uptime: 0 days 0:00:00.031
KDTARGET: Refreshing KD connection
Debuggee not connected
```

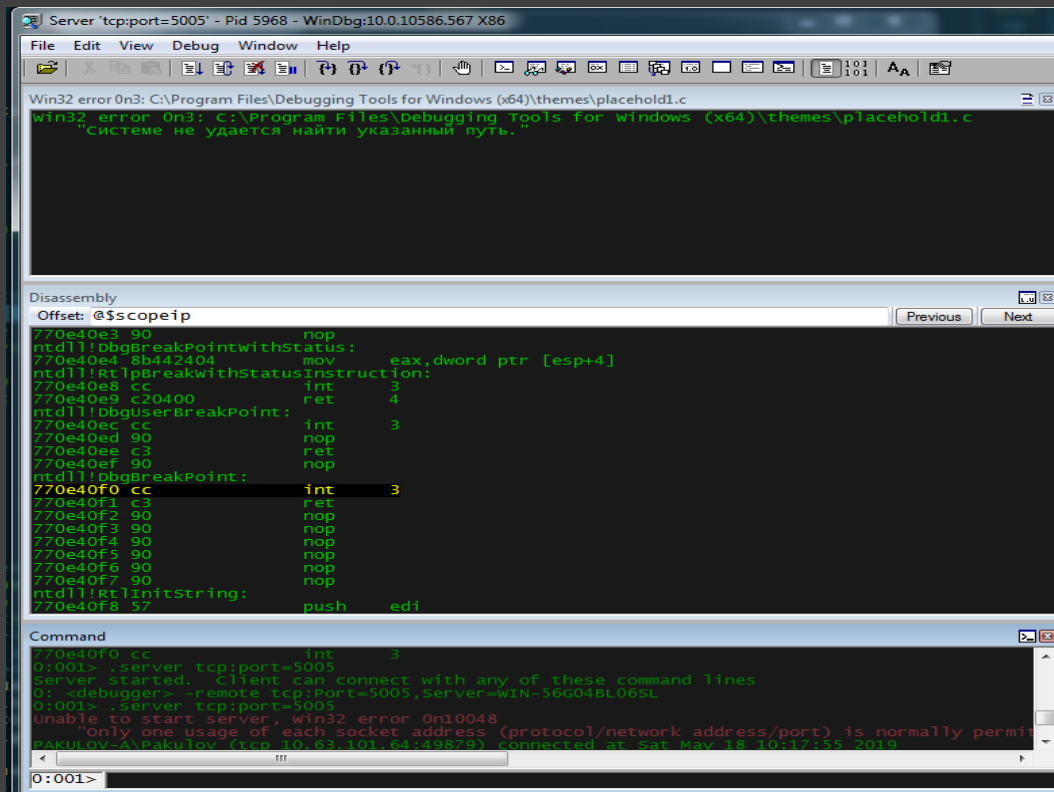
В каталоге Debuggers находится отладчик

```
D:\WinDDK\7600.16385.1
n
Name
..
bin
Catalog
Debug
Debuggers
help
inc
lib
MyDrivers
MyNativeApps
OACR
redis
src
tools
WDTF
blockdir
build
dirs
Green-krnl
install
license
project
redis
relnote
samples
dat
WEW
htm_
rtf_
mk
txt
htm_
txt
```

1

Отладка в режиме пользователя

1. Открываем Windbg
2. В нём открываем отлаживаемое приложение
3. В консоли пишем: `.server tcp:port=5005`



The screenshot shows the WinDbg interface with the following content:

Server 'tcp:port=5005' - Pid 5968 - WinDbg:10.0.10586.567 X86

File Edit View Debug Window Help

Win32 error 0n3: C:\Program Files\Debugging Tools for Windows (x64)\themes\placeholder1.c
Win32 error 0n3: C:\Program Files\Debugging Tools for Windows (x64)\themes\placeholder1.c
"Системе не удастся найти указанный путь."

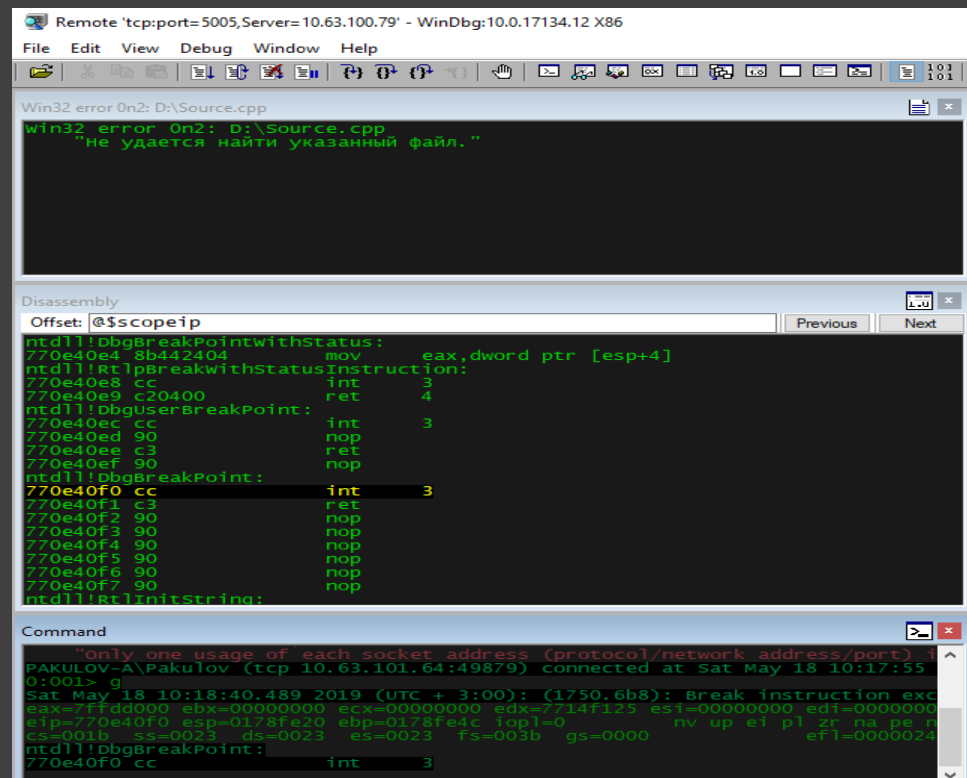
Disassembly
Offset: @\$scopeip

```
770e40e3 90      nop
ntdll!DbgBreakPointWithStatus:
770e40e4 8b442404 mov     eax,dword ptr [esp+4]
ntdll!RtlpBreakWithStatusInstruction:
770e40e8 cc      int     3
770e40e9 c20400  ret     4
ntdll!DbgUserBreakPoint:
770e40ec cc      int     3
770e40ed 90      nop
770e40ee c3      ret
770e40ef 90      nop
ntdll!pDbgBreakPoint:
770e40f0 cc      int     3
770e40f1 c3      ret
770e40f2 90      nop
770e40f3 90      nop
770e40f4 90      nop
770e40f5 90      nop
770e40f6 90      nop
770e40f7 90      nop
ntdll!RtlInitString:
770e40f8 57      push   edi
```

Command

```
0:001> .server tcp:port=5005
Server started. Client can connect with any of these command lines
0: <debugger> -remote tcp:Port=5005,server=WIN-56G04BL065L
0:001> .server tcp:port=5005
unable to start server, win32 error 0n10048
"only one usage of each socket address (protocol/network address/port) is normally permitted"
bakulov-A\Bakulov (tcp 10.63.101.64:49879) connected at Sat May 18 10:17:55 2019
0:001>
```

1. Открываем Windbg
2. File->Connect to Remout Session (Ctrl+R)
3. Вводим tcp:port=5005,Server=192.168.17.130



The screenshot shows the WinDbg interface with a remote connection to a server. The title bar reads "Remote 'tcp:port=5005,Server=10.63.100.79' - WinDbg:10.0.17134.12 X86". The menu bar includes File, Edit, View, Debug, Window, and Help. The toolbar contains various debugging tools. A window titled "Win32 error 0n2: D:\Source.cpp" displays the error message: "win32 error 0n2: D:\Source.cpp 'Не удастся найти указанный файл.'" The Disassembly window shows the following code:

```
Offset: @$scope!ip
ntdll!DbgBreakPointwithStatus:
770e40e4 8b442404      mov     eax,dword ptr [esp+4]
ntdll!RtlpBreakwithStatusInstruction:
770e40e8 cc          int     3
770e40e9 c20400      ret     4
ntdll!DbgUserBreakPoint:
770e40ec cc          int     3
770e40ed 90          nop
770e40ee c3          ret
770e40ef 90          nop
ntdll!DbgBreakPoint:
770e40f0 cc          int     3
770e40f1 c3          ret
770e40f2 90          nop
770e40f3 90          nop
770e40f4 90          nop
770e40f5 90          nop
770e40f6 90          nop
770e40f7 90          nop
ntdll!RtlInitString:
```

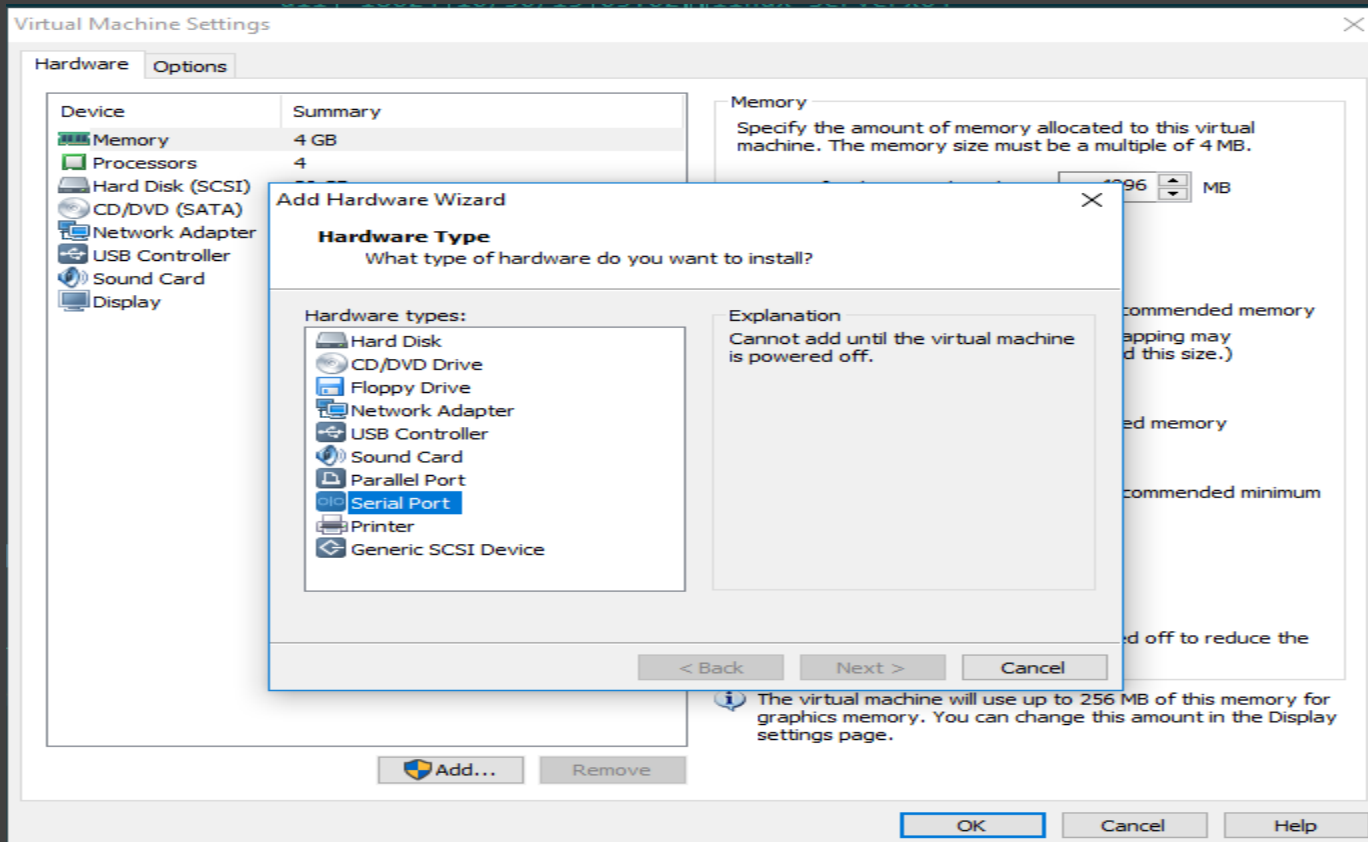
The Command window shows the following output:

```
"only one usage of each socket address (protocol/network address/port)
PAKULOV-A\Pakulov (tcp 10.63.101.64:49879) connected at Sat May 18 10:17:55
0:001> g
Sat May 18 10:18:40.489 2019 (UTC + 3:00): (1750.6b8): Break instruction exc
eax=7714f125 ebx=00000000 ecx=00000000 edx=7714f125 esi=00000000 edi=000000
eip=770e40f0 esp=0178fe20 ebp=0178fe4c iopl=0         nw up e1 pl zr na ps fi
cs=001b  ss=0023  ds=0023  es=0023  fs=003b  gs=0000             efl=0000024
ntdll!DbgBreakPoint:
770e40f0 cc          int     3
```

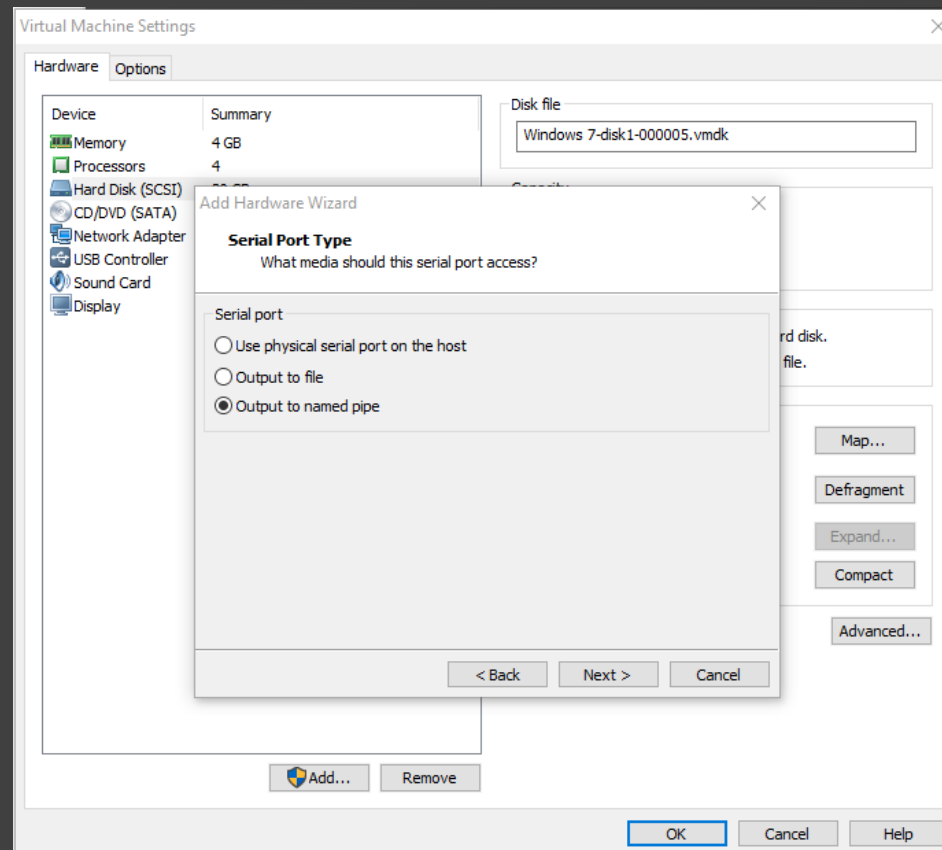

2

Отладка в режиме ядра

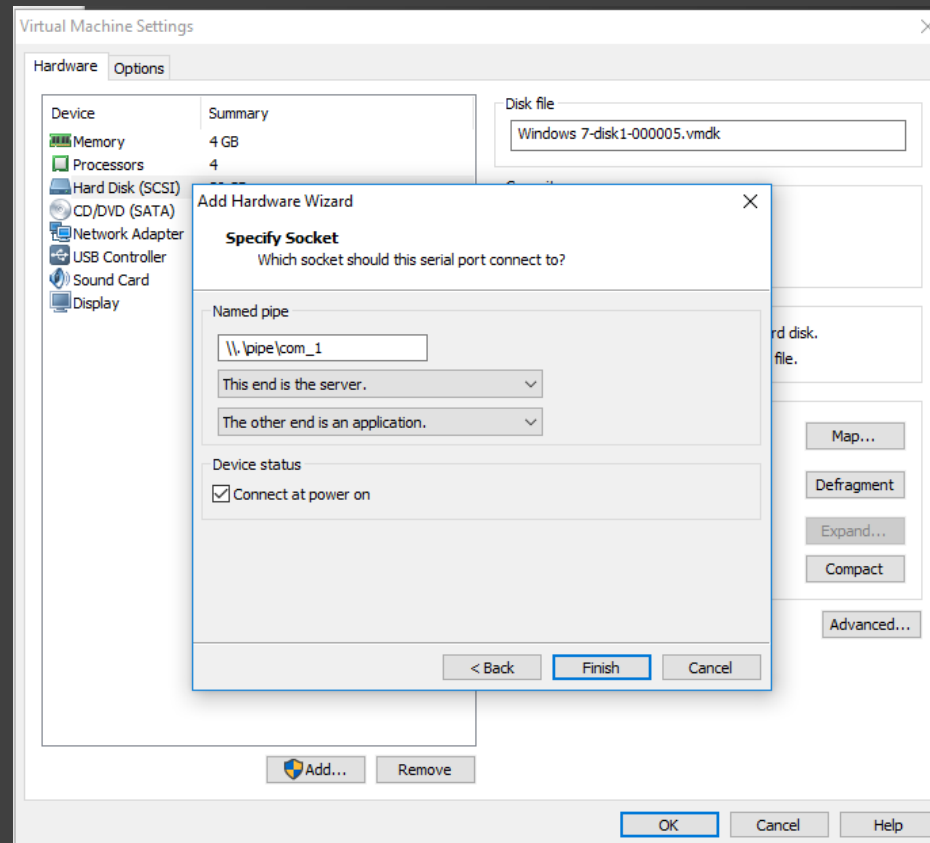
При добавлении проследить: в combo box нужно выбрать «This end is the server» и «The other end is an application»



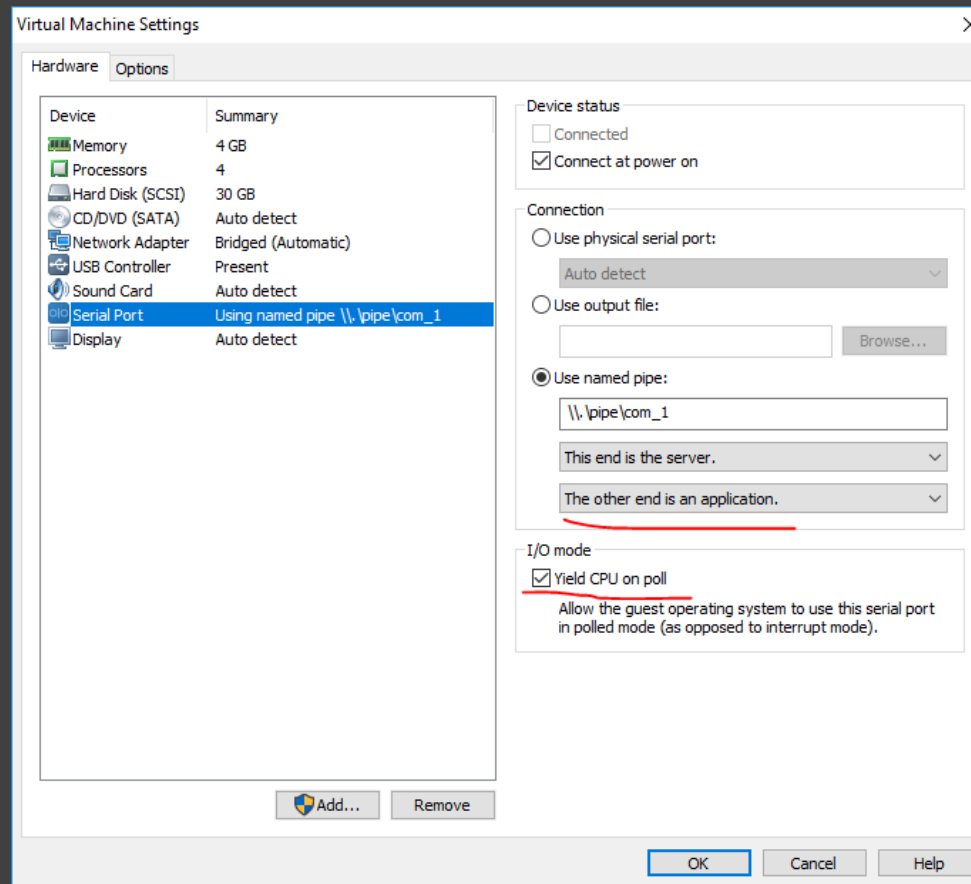
При добавлении проследить: в combo box нужно выбрать «This end is the server» и «The other end is an application»



При добавлении проследить: в combo box нужно выбрать «This end is the server» и «The other end is an application»

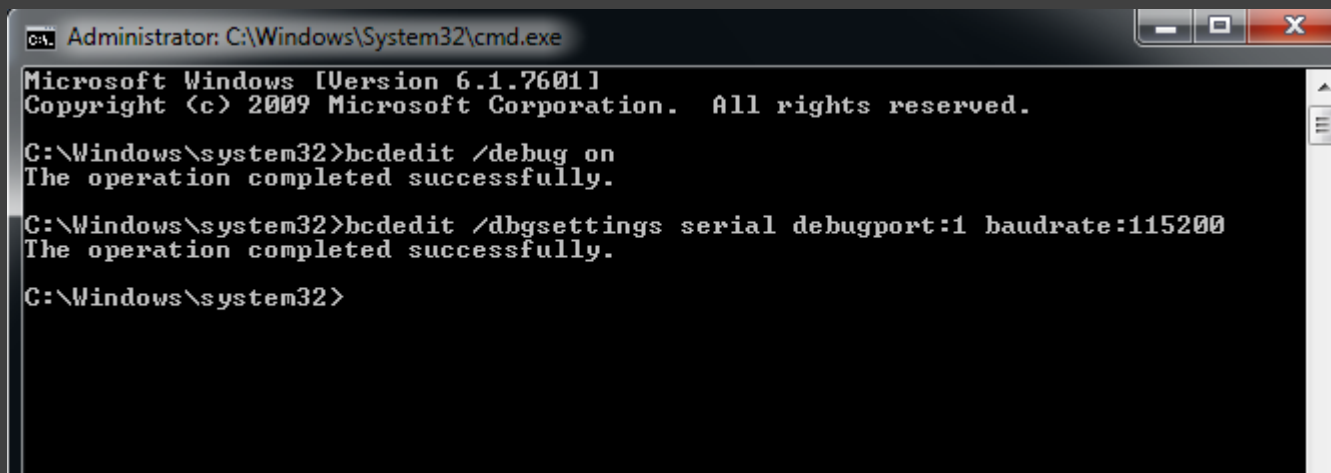


При добавлении проследить: в combo box нужно выбрать «This end is the server» и «The other end is an application»



Включаем режим отладки:

1. Открываем командную строку от имени администратора
2. `bcdedit /debug on`
3. `bcdedit /dbgsettings serial debugport:1 baudrate:115200`



```
Administrator: C:\Windows\System32\cmd.exe
Microsoft Windows [Version 6.1.7601]
Copyright (c) 2009 Microsoft Corporation. All rights reserved.

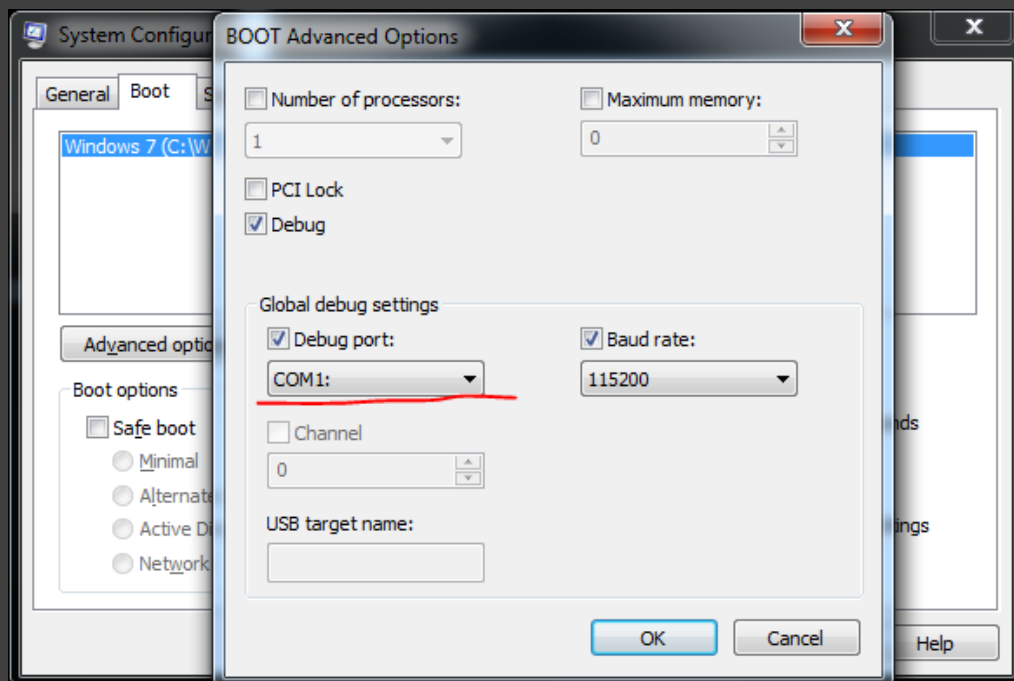
C:\Windows\system32>bcdedit /debug on
The operation completed successfully.

C:\Windows\system32>bcdedit /dbgsettings serial debugport:1 baudrate:115200
The operation completed successfully.

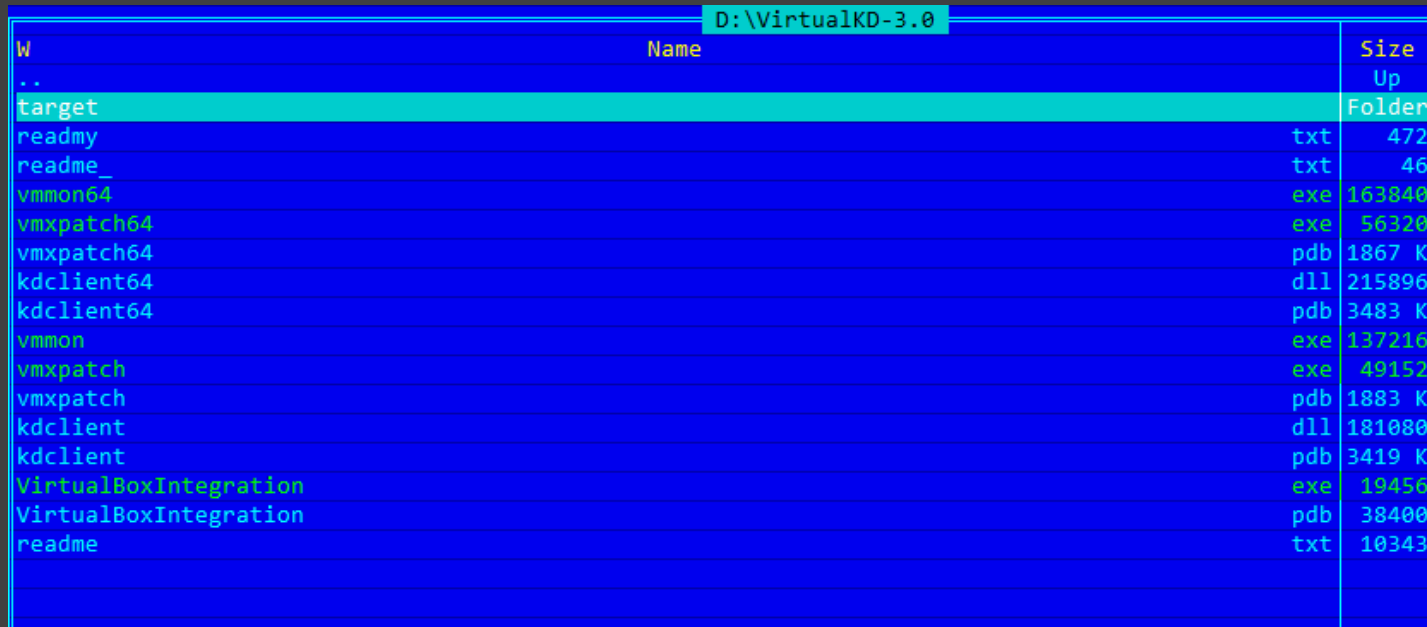
C:\Windows\system32>
```

Проверка:

1. Win+R: msconfig
2. Вкладка “boot” -> Advanced options
3. Видим активный checkbox “Debug”



1. Устанавливаем на хостовой машине
2. На гостевую копируем папку target

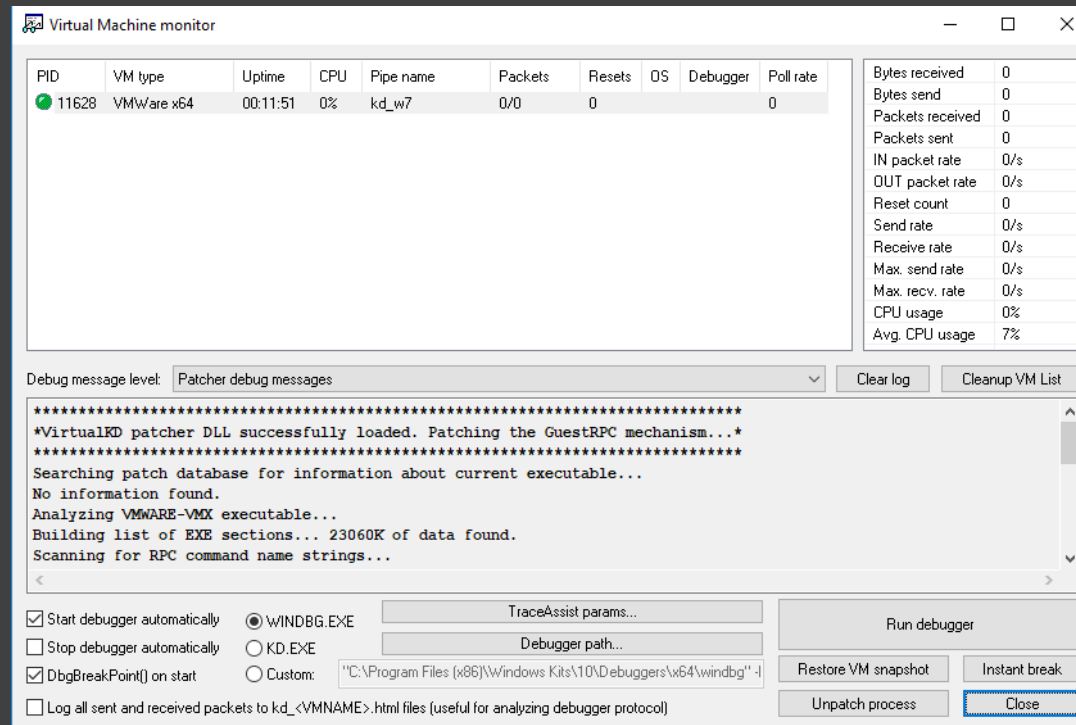


D:\VirtualKD-3.0

W	Name		Size
.	.		Up
	target	Folder	
	readmy	txt	472
	readme_	txt	46
	vmmon64	exe	163840
	vmxpatch64	exe	56320
	vmxpatch64	pdb	1867 K
	kdclient64	dll	215896
	kdclient64	pdb	3483 K
	vmmon	exe	137216
	vmxpatch	exe	49152
	vmxpatch	pdb	1883 K
	kdclient	dll	181080
	kdclient	pdb	3419 K
	VirtualBoxIntegration	exe	19456
	VirtualBoxIntegration	pdb	38400
	readme	txt	10343

1. На гостевой запускаем vminstall.exe

2. На хостовой - vmmon64.exe → Run Debugger



Вопросы???





Пакулов Артур

A.Pakulov.Otus@Gmail.com

Спасибо
за внимание!

