Debugging.TV

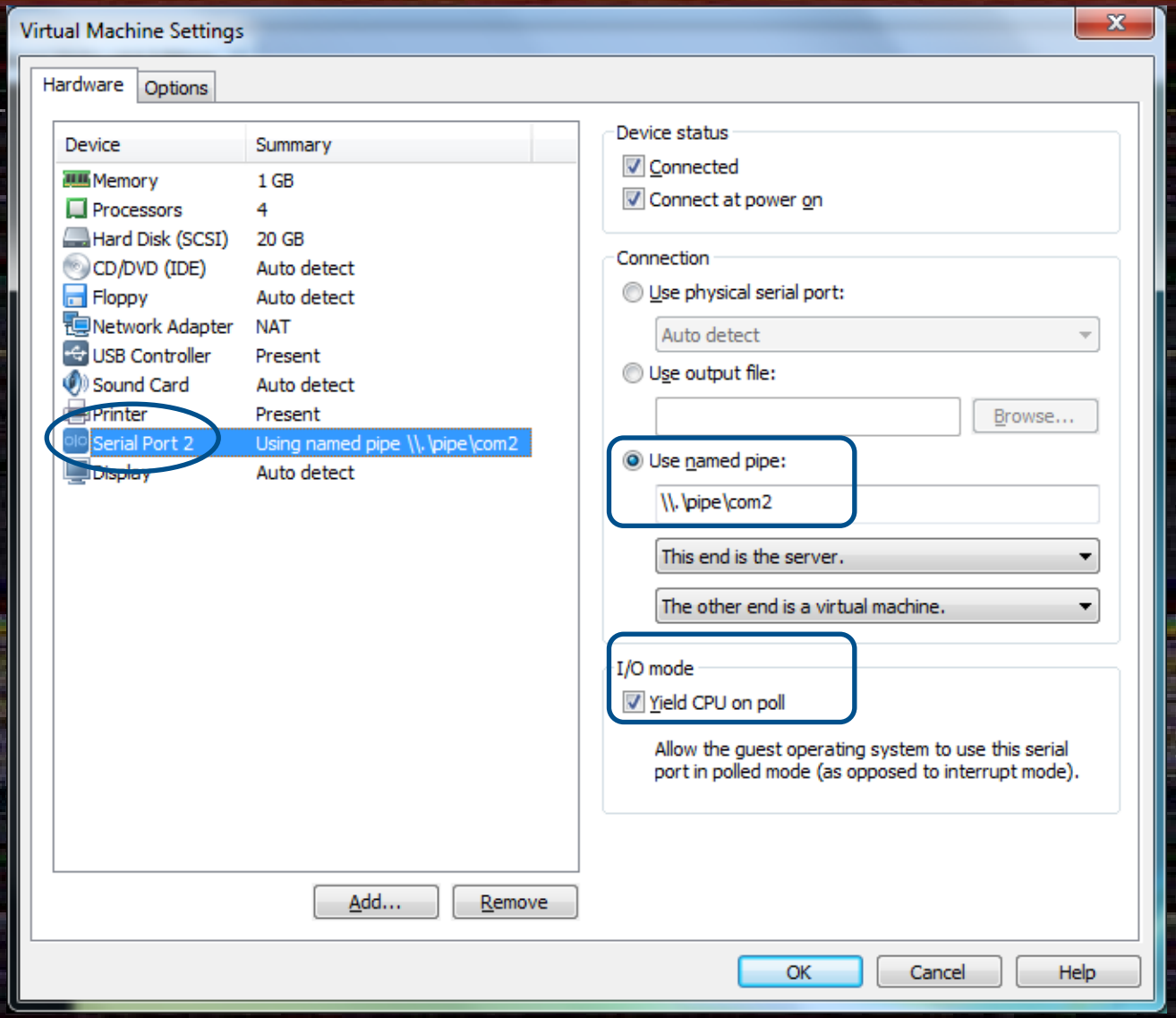
Frame 0x25

Presenter: Dmitry Vostokov

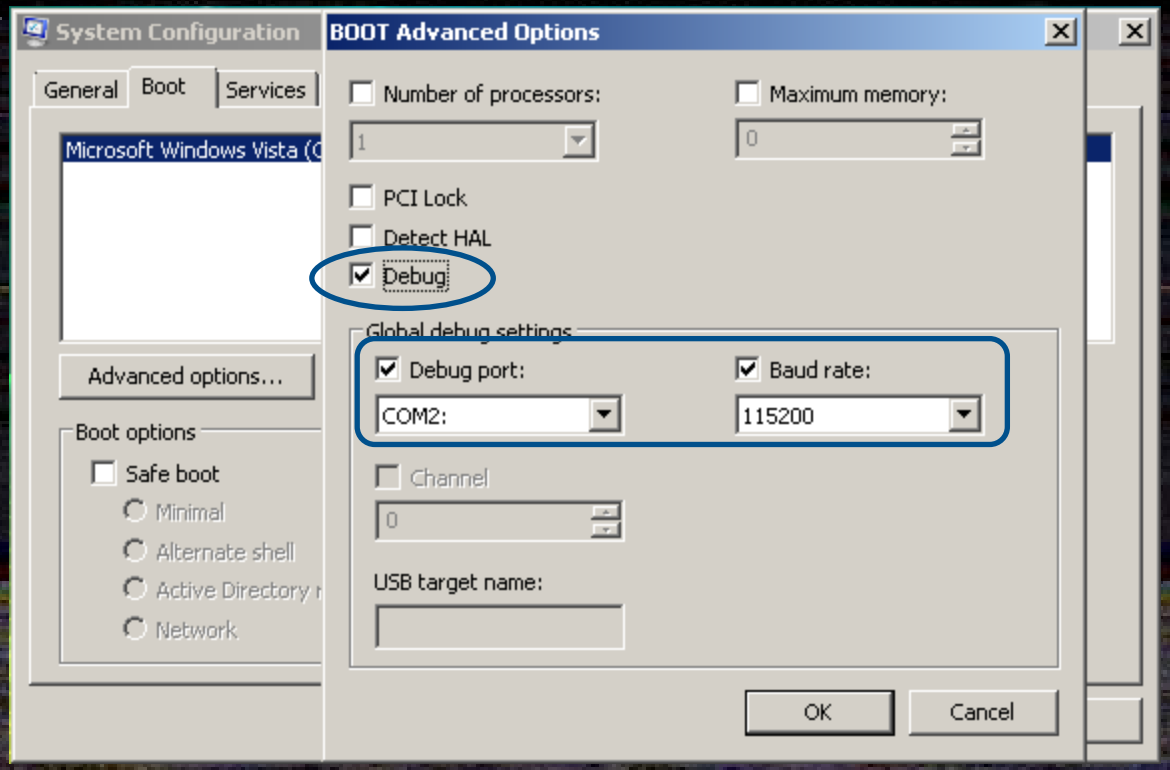
Topics

- Setting guest OS and virtual machine for kernel debugging
- Configuring host WinDbg for kernel debugging
- Examining the guest system
- Simulating a double fault

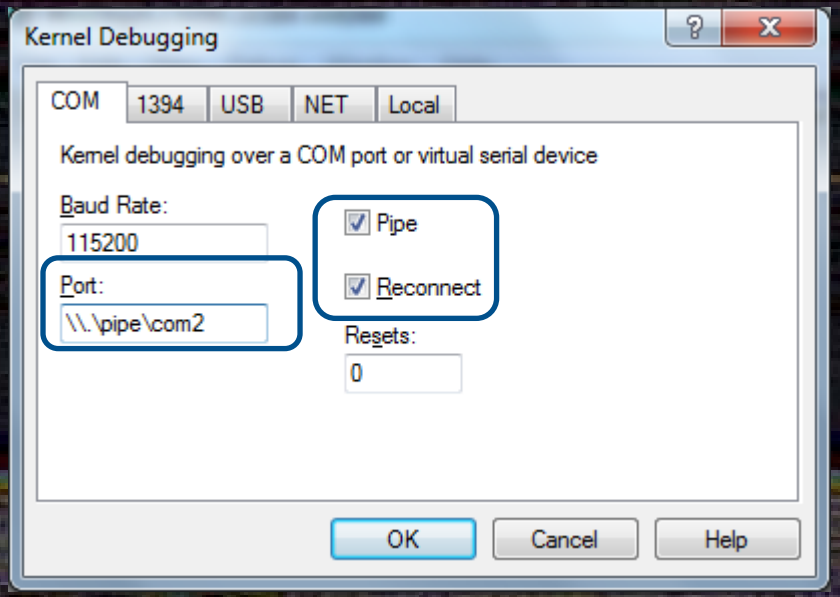
Virtual Machine Setup



Guest OS Setup



Host WinDbg Setup



Double Fault

```
1: kd> k
Child-SP          RetAddr           Call Site
fffff980`00a9e968 fffff800`0184d8f3 nt!KeBugCheckEx
fffff980`00a9e970 fffff800`0184c138 nt!KiBugCheckDispatch+0x73
fffff980`00a9eab0 fffff800`0184b754 nt!KiDoubleFaultAbort+0xb8
fffff980`00ce4f80 fffff800`0184d900 nt!KiDebugTrapOrFault+0x14
fffff980`00ce5118 fffff800`0184b871 nt!KiExceptionDispatch
fffff980`00ce5120 fffff800`0184d900 nt!KiDebugTrapOrFault+0x131
[…]
fffff980`00cea400 fffff800`0184d900 nt!KiDebugTrapOrFault+0x131
fffff980`00cea598 fffff800`0184b871 nt!KiExceptionDispatch
fffff980`00cea5a0 fffff800`0184d900 nt!KiDebugTrapOrFault+0x131
fffff980`00cea738 fffff800`0184b871 nt!KiExceptionDispatch
fffff980`00cea740 fffff800`0184d900 nt!KiDebugTrapOrFault+0x131
fffff980`00cea8d8 fffff800`0184b871 nt!KiExceptionDispatch
fffff980`00cea8e0 fffff800`0184d900 nt!KiDebugTrapOrFault+0x131
fffff980`00ceaa78 fffff800`0184bec3 nt!KiExceptionDispatch
fffff980`00ceaa80 fffff980`13ac910b nt!KiInvalidOpcodeFault+0xc3
fffff980`00ceac10 fffff980`13ac9415 spsys!SPVersion+0x237db
fffff980`00ceac50 fffff980`13ad4e6c spsys!SPVersion+0x23ae5
fffff980`00ceac90 fffff800`01859ca3 spsys!SPVersion+0x2f53c
fffff980`00ceace0 fffff800`01ae1bbb nt!ExpWorkerThread+0x12a
fffff980`00cead50 fffff800`018344f6 nt!PspSystemThreadStartup+0x5b
fffff980`00cead80 00000000`00000000 nt!KxStartSystemThread+0x16
```

!Ad Hardcore Software Diagnostics Training

May, 13, 2013	Philosophy of Software Diagnostics (FREE)
June 17, 2013	Pattern-Oriented Network Trace Analysis (FREE)
July, 19-22, 2013	Accelerated Windows Debugging^3
July 24-29, 2013	Accelerated Windows Memory Dump Analysis
2013	The New Old Debugging

Debugging^3

Now Available for Booking

Debugging.TV

Now on YouTube!

http://www.youtube.com/DebuggingTV