# Virtualbox

## Raw disk access to partition

```
# @Elevated command prompt
.\VBoxManage internalcommands listpartitions -rawdisk "\\.\PhysicalDrive0"
.\VBoxManage internalcommands createrawvmdk -filename
D:\Virtualbox\raw_disk.vmdk -rawdisk "\\.\PhysicalDrive0" -partitions 7
```

## VirtualKD

```
.\VBoxManage.exe setextradata "win7_x64_2"
VBoxInternal/Devices/VirtualKD/0/Config/Path
"D:\Titannet\Projekte\Windows\Kernel\Software\VirtualKD-3.0\kdclient64.dll"
```

## Paravirtualized debugging

```
# https://www.virtualbox.org/manual/ch09.html#gimdebughyperv
# https://download.virtualbox.org/virtualbox/6.0.0_RC1/UserManual.pdf

 .\vboxmanage showvminfo "VM name" | select-string paravirt
kdvm.dll

VBoxManage modifyvm "VM name" --paravirtdebug "enabled=1"


VBoxManage modifyvm "VM name" --paravirtdebug
"enabled=1,address=10.22.6.40,port=50001"

netsh int ip set address "local area connection" static 10.22.6.41
255.255.255.0

bcdedit /set loadoptions
host_ip=5.5.5.5,host_port=50000,encryption_key=5.6.7.8
bcdedit /set dbgtransport kdvm.dll

bcdedit /set debug on
# bcdedit /set bootdebug on ##win8+
# bcdedit /set {bootmgr} bootdebug on

C:\Windows\system32>bcdedit /set loadoptions
host_ip="1.2.3.4",host_port=50001,e
ncryption_key="5.6.7.8"
```

```
netsh interface ipv4 set address name="Local Area Connection" static 10.22.6.41 255.255.255.0
bcdedit /set loadoptions host_ip=5.5.5.5,host_port=50001,encryption_key=5.6.7.8
bcdedit /set dbgtransport kdvm.dll
bcdedit /set debug on

netsh interface ipv4 set address name="Local Area Connection" static 10.22.6.42 255.255.255.0
bcdedit /set loadoptions host_ip=5.5.5.5,host_port=50002,encryption_key=5.6.7.8
bcdedit /set dbgtransport kdvm.dll
bcdedit /set debug on
VBoxManage modifyvm "win7_x86_sp1" --paravirtdebug "enabled=1,address=10.22.6.40,port=50002"

netsh interface ipv4 set address name="Local Area Connection" static 10.22.6.43 255.255.255.0
bcdedit /set loadoptions host_ip=5.5.5.5,host_port=50003,encryption_key=5.6.7.8
bcdedit /set dbgtransport kdvm.dll
VBoxManage modifyvm "win7_x64_sp1" --paravirtdebug "enabled=1,address=10.22.6.40,port=50003"
bcdedit /set debug on
```

## Toolz

```
Set-ExecutionPolicy Bypass -Scope Process -Force; iex ((New-Object System.Net.WebClient).DownloadString('https://chocolatey.org/install.ps1'))
choco feature enable -n allowGlobalConfirmation
choco install visualcpp-build-tools --params "'/IncludeOptional'"
choco install visualcpp-build-tools --version 14.0.25420.1
choco install notepadplusplus.install nasm hxd totalcommander windbg ida-free
```