Commands to run Virtual iPhone for Penetration Testing

Download iPhone.zip from the URL Below:

https://drive.google.com/file/d/19YBI9vgVNDlyeZ0DtG7dA2cBmpOVQAjS/view?usp=sharing

Unzip iPhone.zip

Navigate to iPhone directory
cd iPhone

Execute Qemu with iOS for 6S Plus Phone =
./xnu-qemu-arm64/aarch64-softmmu/qemu-system-aarch64 -M iPhone6splus-n66-s8000,kernel-filename=kernelcache.release.n66.out,dtb-filename=Firmware/all_flash/DeviceTree.n66ap.im4p.out.mod,secmon-filename=securemonitor.out,ramdisk-filename=048-32651-104.dmg.out,tc-filename=static_tc,kern-cmd-args="debug=0x8 kextlog=0xff cpus=1 rd=md0 serial=2" -cpu max -m 6G -serial mon:stdio

In the bash Shell - Export the path on bash so as to access all the commands =

export PATH=$PATH:/iosbinpack64/usr/bin:/iosbinpack64/bin:/iosbinpack64/usr/sbin:/iosbinpack64/sbin