杂项篇
一些其他操作
网监调案制作磁盘镜像流程（阿帕云 -云服务器）
网监调案制作磁盘镜像流程（阿帕云 -物理机）

网监调案制作磁盘镜像流程（阿

帕云 -云服务器）

操作之前请务必先确认是否为我司业务机器（包括但不限于：归属在罗仁逸，纪天 “
宇，陈亮，小鸟云等内部系统名下，需要追溯最终客户）

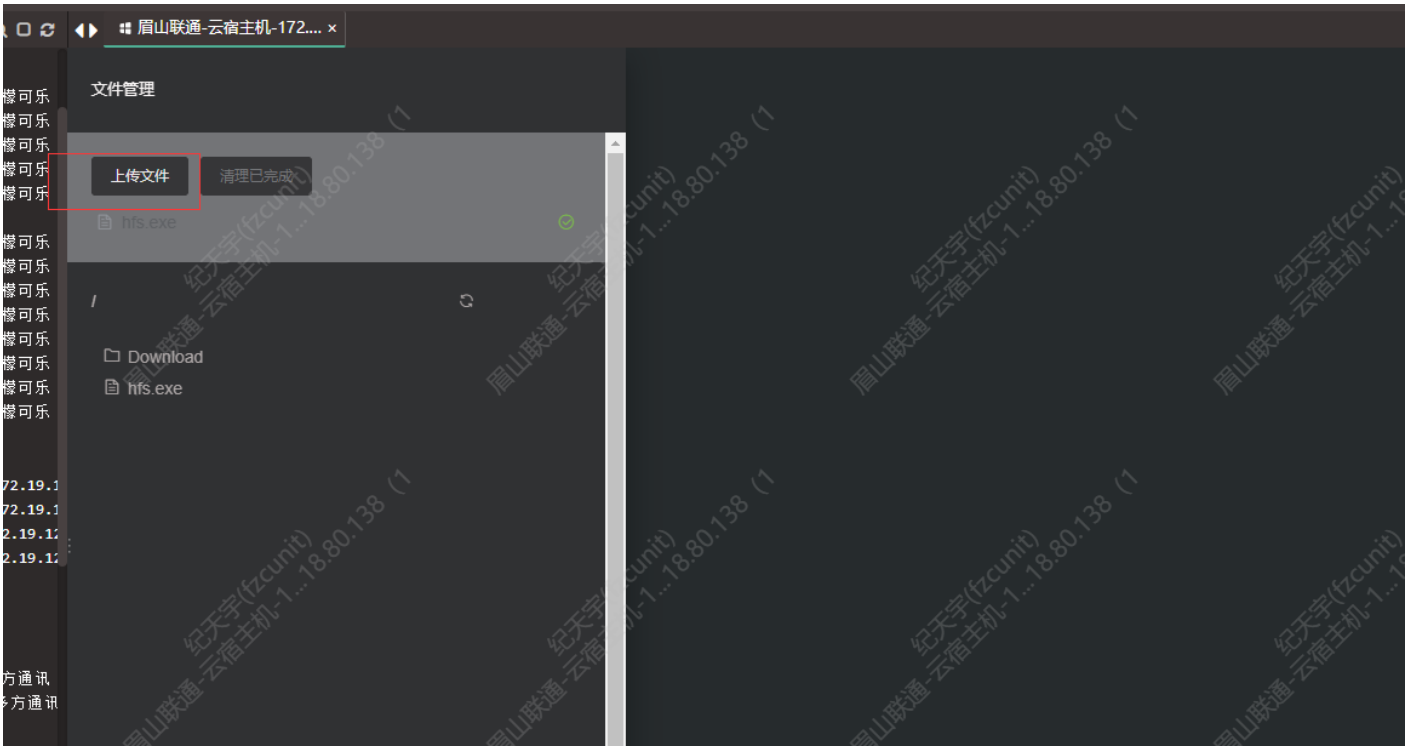
1.进入阿帕云管理后台，搜索相应业务，找到服务器列表，搜索服务器，找到服务器详情，记录业务 ID(如图: 9785）

2.下拉，找到宿主机信息，查看虚拟化类型是否为 Hyper-V，本教程只适用于 Hyper-V，确认后记录宿主机 IP

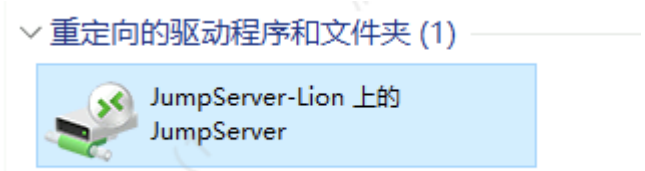
4.□□□□□□□□□ HFS□□□□□□□□□□□□□□□□□□□□

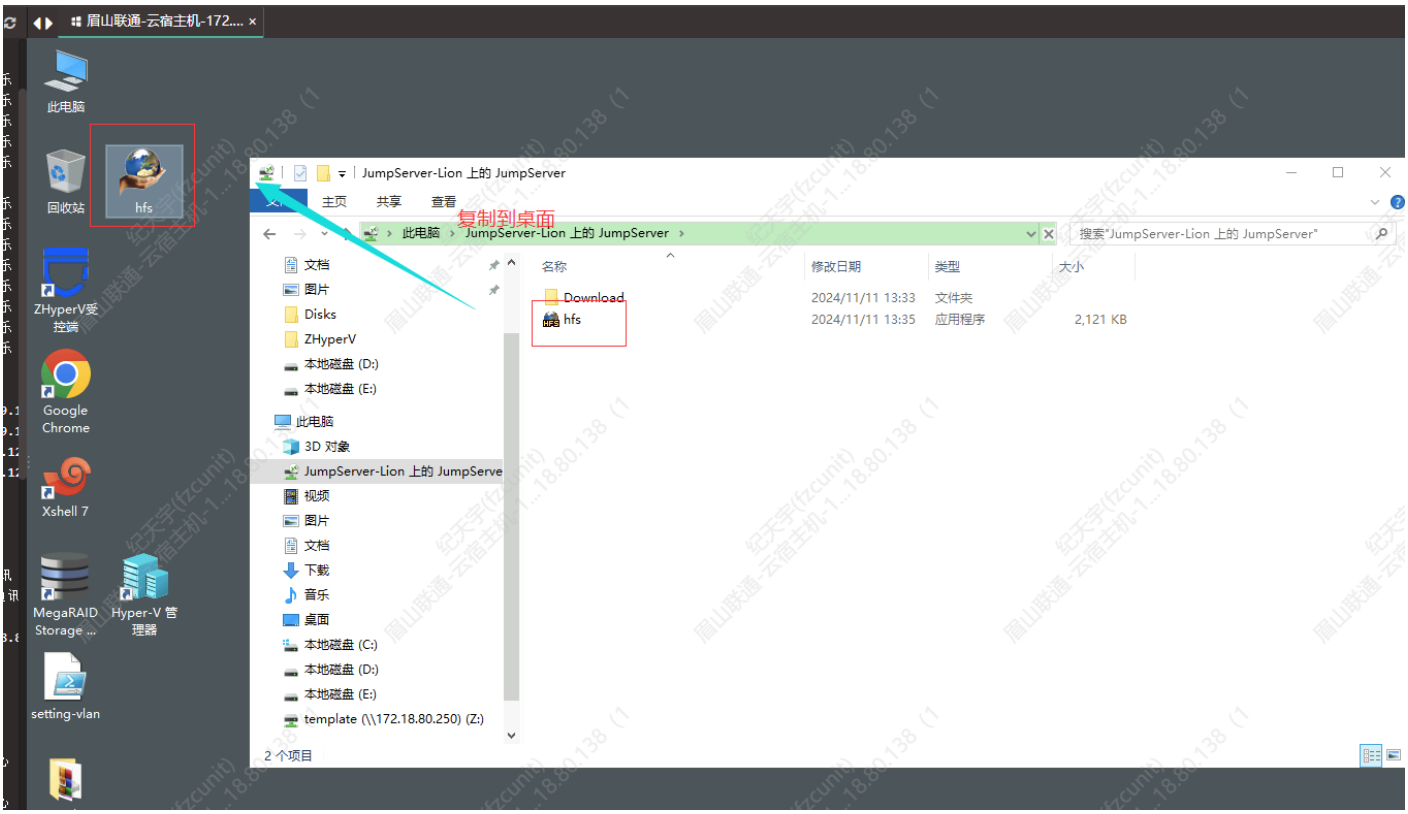

此电脑
回收站
ZHyperV受控端
Google Chrome
Xshell 7
MegaRAID Storage ...
Hyper-V Manager
setting-vlan
Tools


设置
剪贴板
文件管理
快捷键 10
Esc
F11
Ctrl+Alt+Delete
Ctrl+Alt+Backspace
Windows+D
Windows+E
Windows+R
Windows+X
Windows
Alt+Tab
显示
100%
自动适应

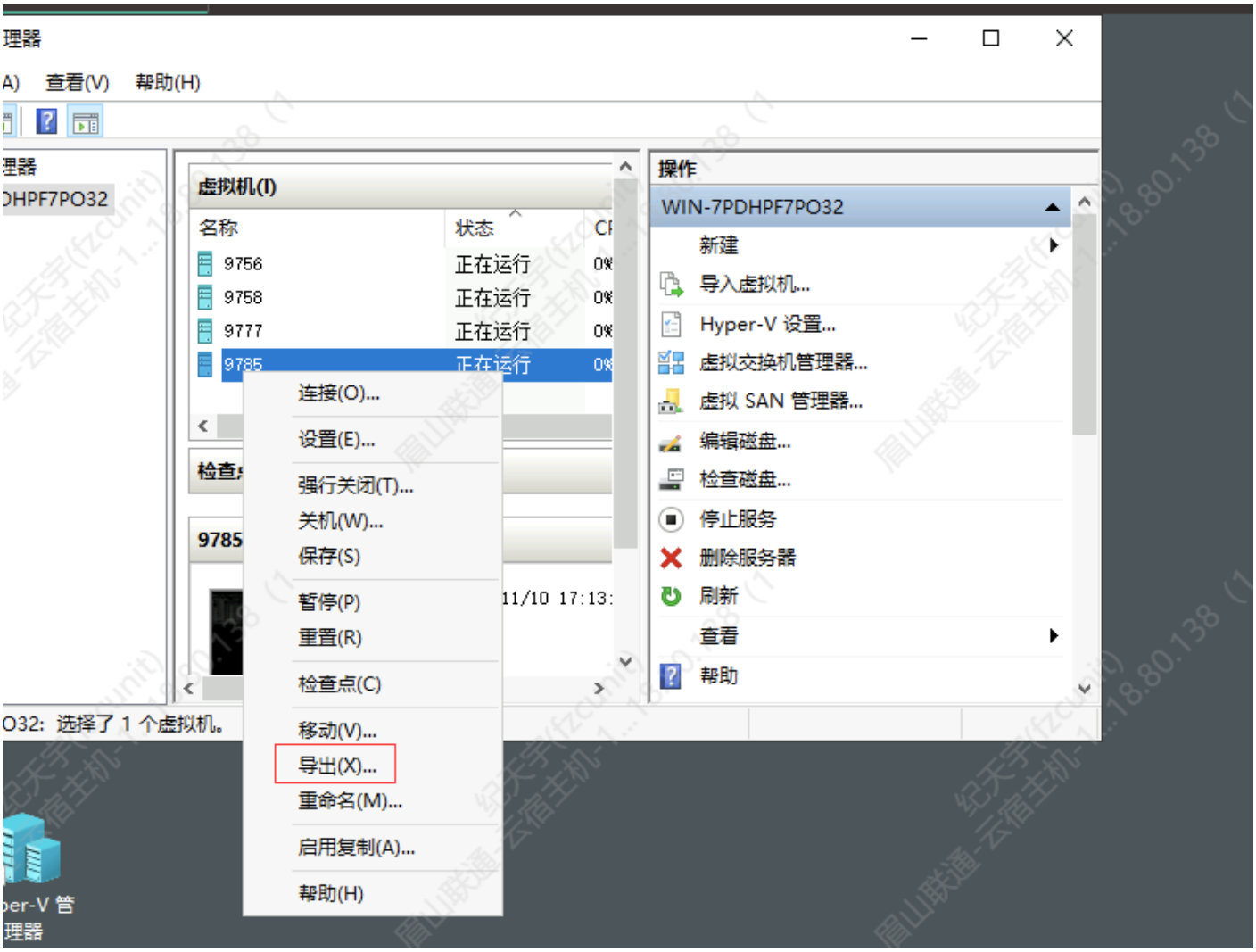

眉山联通-云宿主机-172....
文件管理
上传文件
清理已完成
hfs.exe
/
Download
hfs.exe

□□□□□□□□□□□□□ "□□□ "□□□ JumpServer□□□□□□□□□□□□□□□ HFS□□□□□



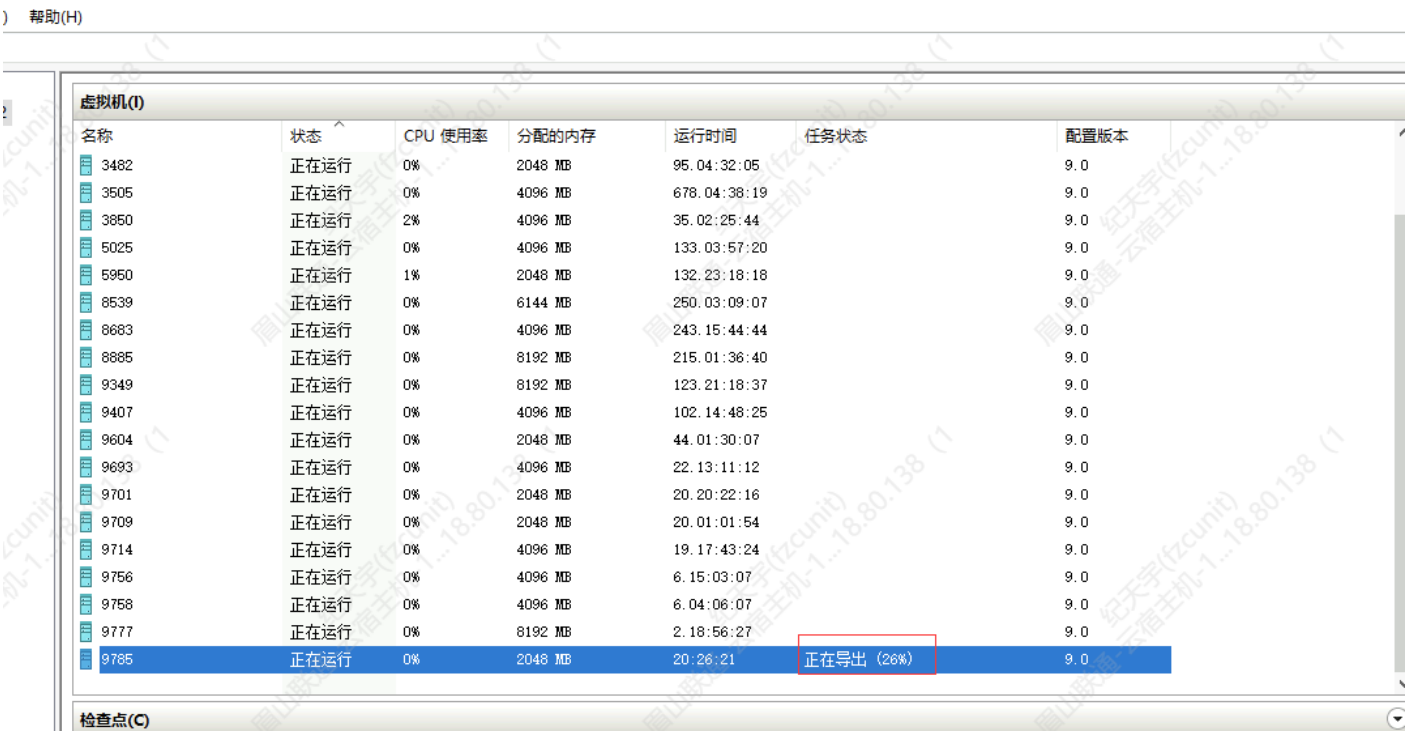


5.□□ Hyper-V□□□□□□□□□□□□ ID□□□□□□□□□□□□□□□□□□□□ C
□□□□□□□□□□□□□□□□□□□□□□□□□□□□□□□□ D□□□□□□ "9785□□ "□□□□


理器
A) 查看(V) 帮助(H)
虚拟机(I)
名称
状态
9756 正在运行
9758 正在运行
9777 正在运行
9785 正在运行
连接(O)...
设置(E)...
强行关闭(T)...
关机(W)...
保存(S)
暂停(P)
重置(R)
检查点(C)
移动(V)...
导出(X)...
重命名(M)...
启用复制(A)...
帮助(H)
操作
WIN-7PDHPF7PO32
新建
导入虚拟机...
Hyper-V 设置...
虚拟交换机管理器...
虚拟 SAN 管理器...
编辑磁盘...
检查磁盘...
停止服务
删除服务器
刷新
查看
帮助
O32: 选择了 1 个虚拟机。

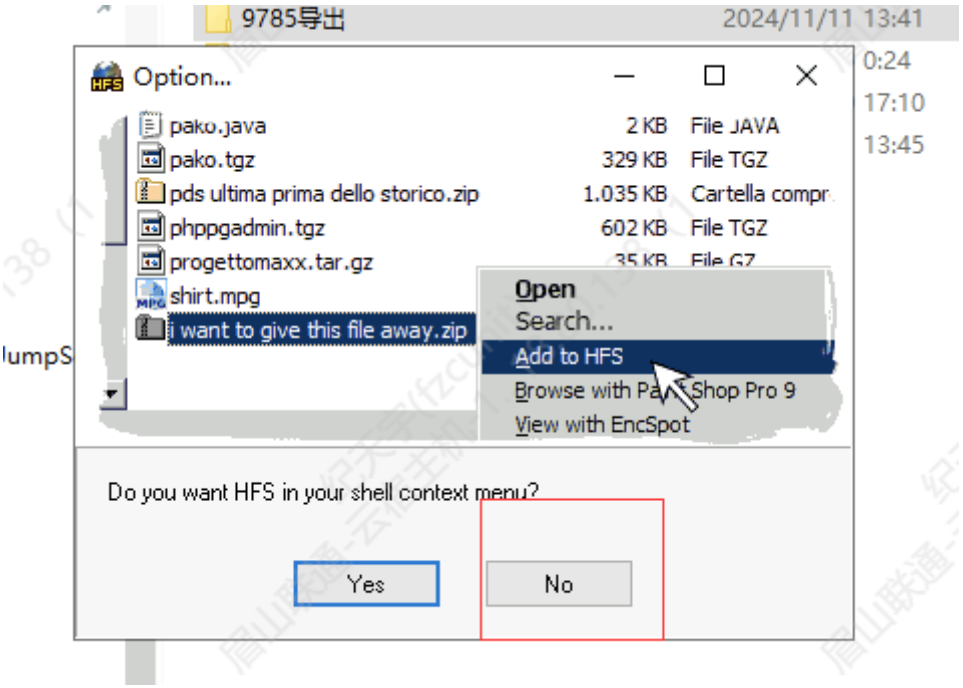

虚拟机(I)
名称
状态
导出虚拟机
指定你要保存文件的位置。
位置(L):
D:\9785导出\
浏览(B)...
导出(X)
取消(C)
9785
创建时间: 2024/11/10 17:13:
配置版本: 9.0
操作
WIN-7PDHPF7PO32
新建
停止服务
删除服务器
刷新
查看

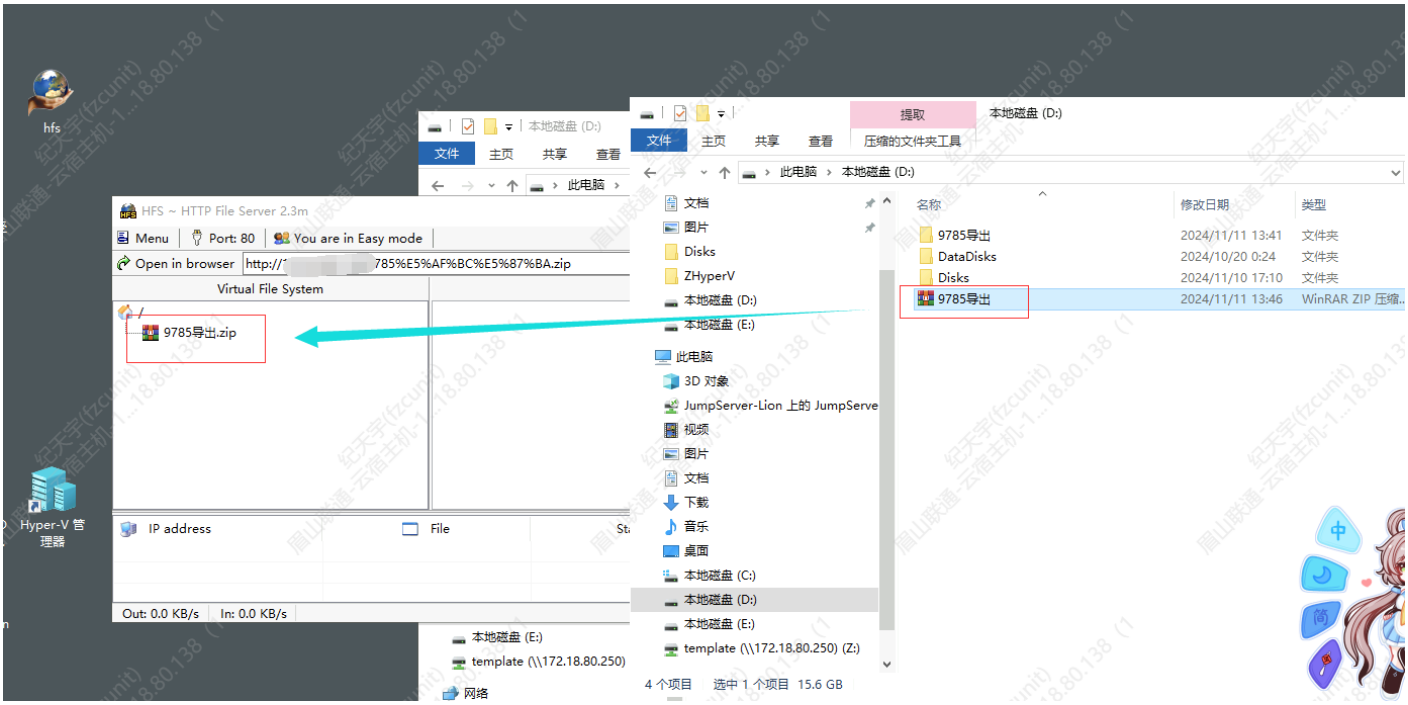
□□□□□□□□□□□□□□□□□□□□□□□ Hyper-V□□□□□□



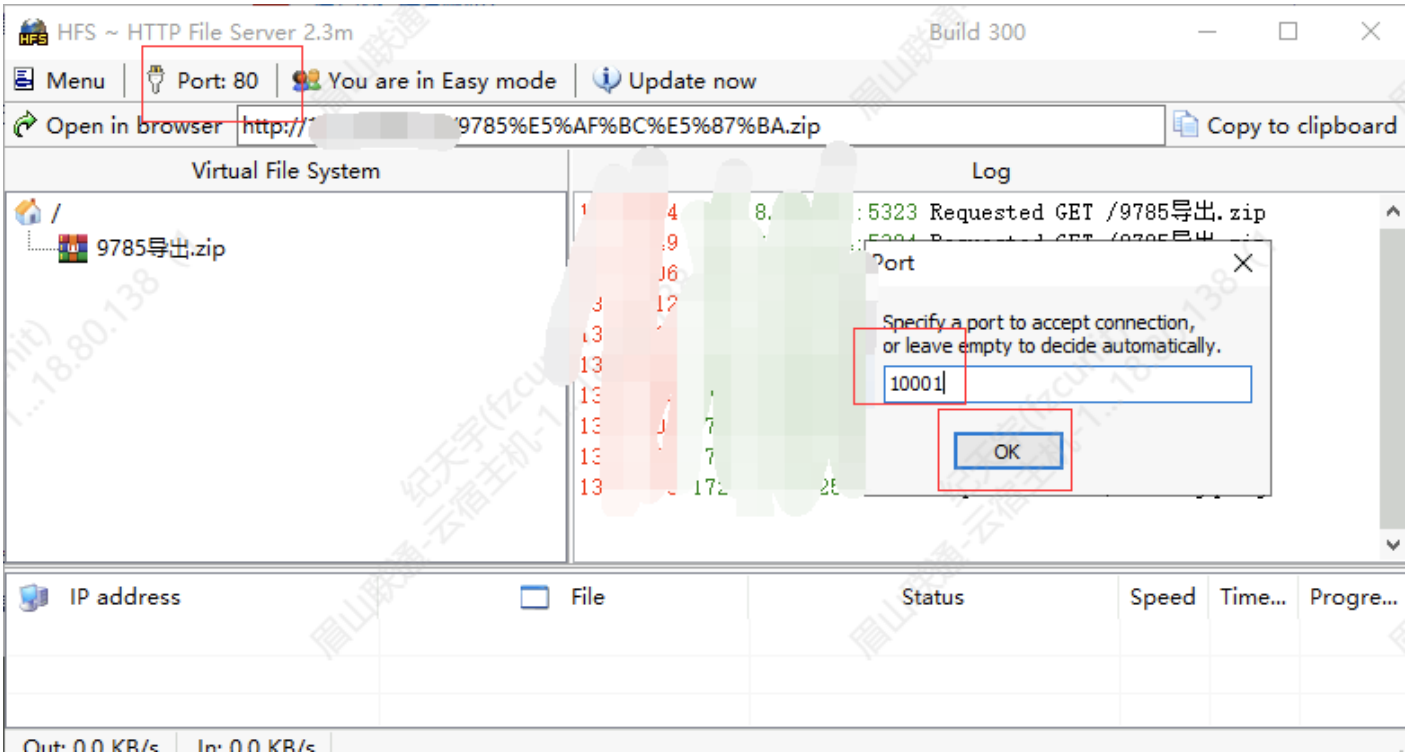
6.导出完成后，进入刚刚导出的目录，压缩为压缩包（压缩软件如果没有可以自行安装）

7.压缩完成后打开桌面的 HFS工具，将压缩包拖入即可（如果有提示一概选择 NO）





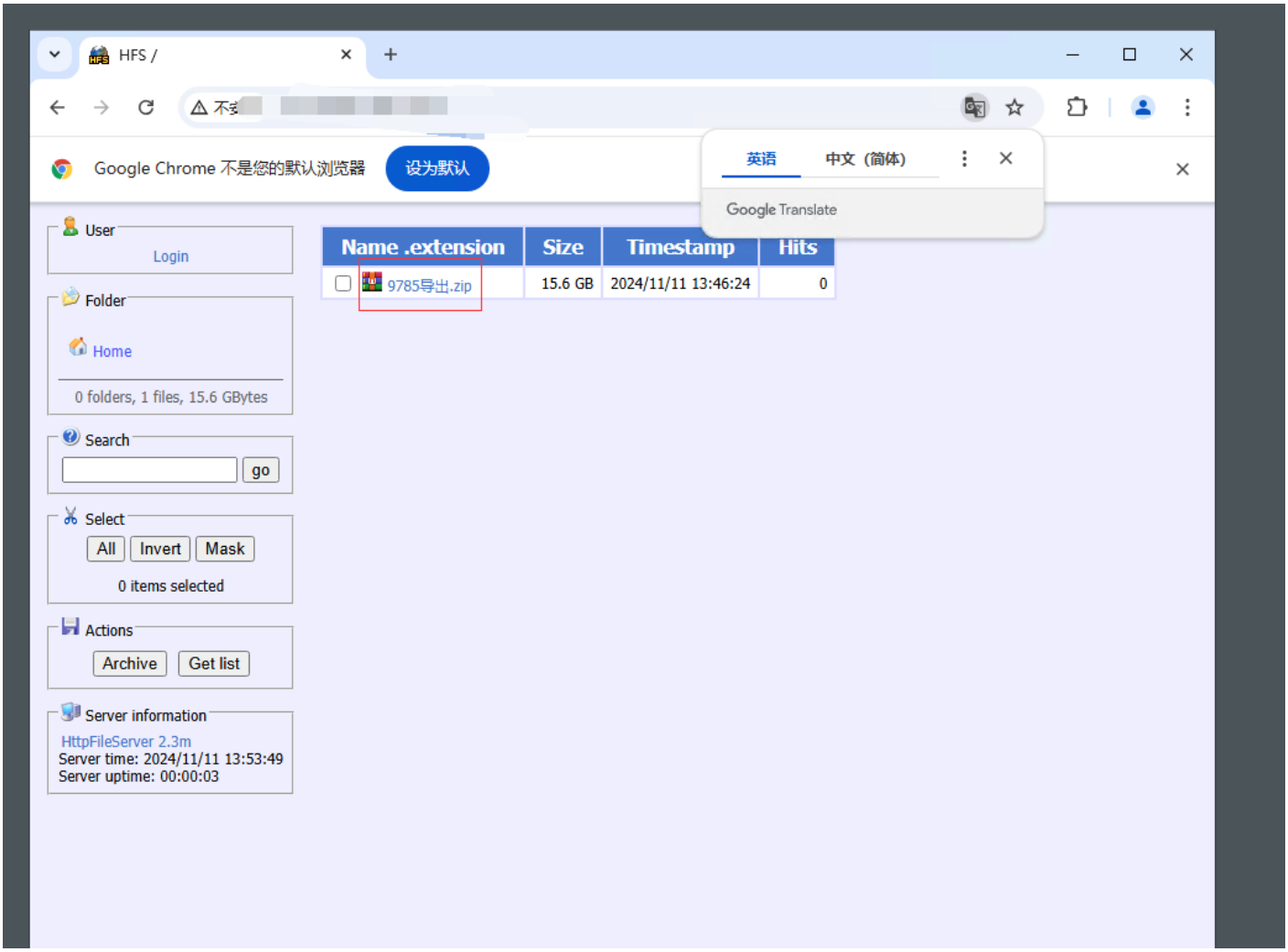
8.□□□□□ Port:80 □□□ 10001



9.□□□□□□□□□□□□□□□□ http://<□□□□ IP>:10001

□□□□□□□□□□□□□□□□□□□□□□□□□□□□□□□□

□□□□□□□□□□□□□



10.下载完成后，将宿主机复原（关闭 HFS 工具，如果刚刚有关闭防火墙请打开），将文件上传到网盘分享并交付即可。

网监调案制作磁盘镜像流程（阿帕云 -物理机）

操作之前请务必先确认是否为我司业务机器（包括但不限于：归属在罗仁逸，纪天 “
宇，陈亮，小鸟云等内部系统名下，需要追溯最终客户）
注意:该操作会导致服务器被重启，并在操作期间无法连接，请确认可以操作后进行操作。
1.打开阿帕云后台，找到需要做镜像的物理机，并确认 IPMI地址



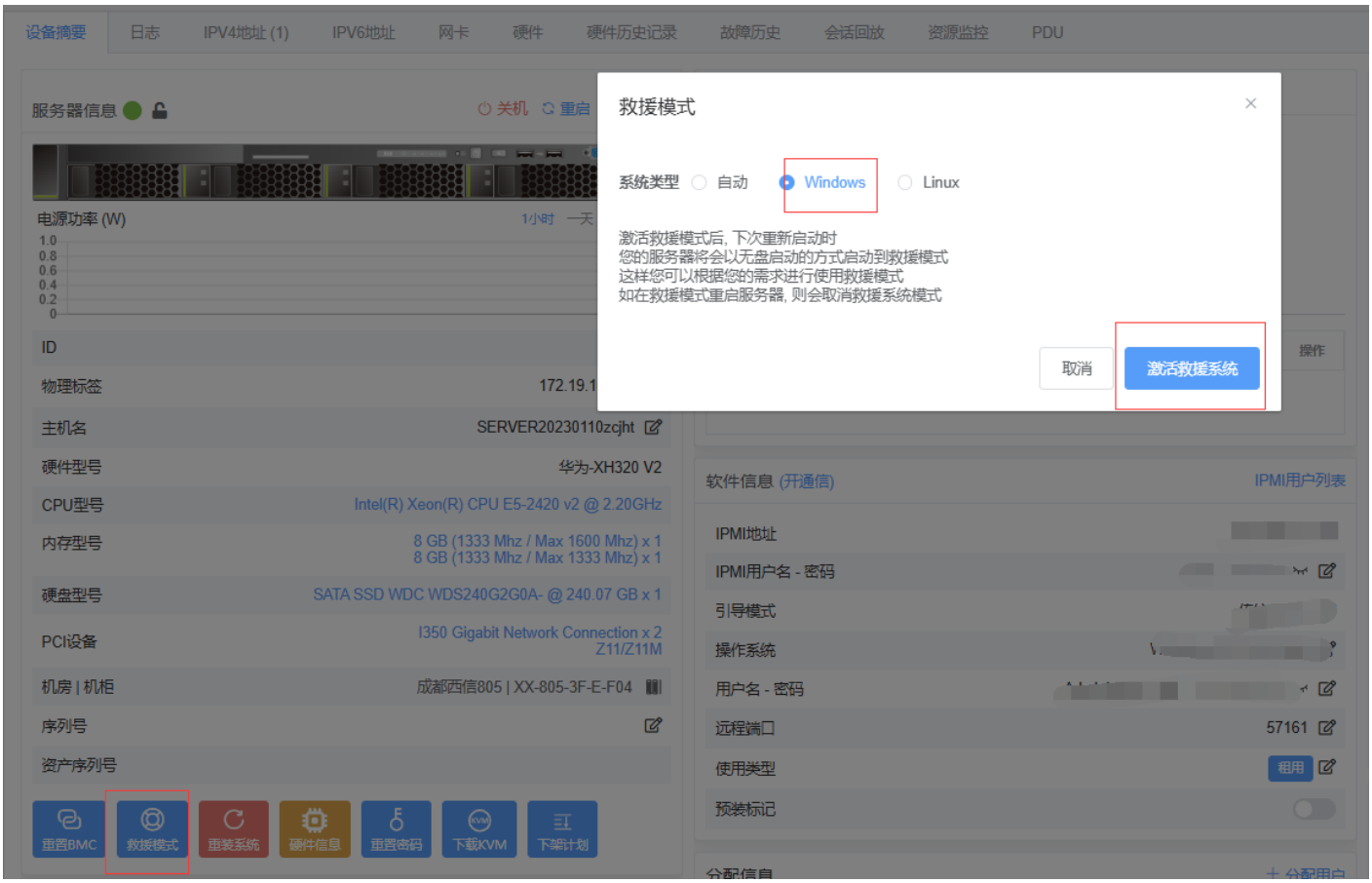
2.喊机房现场添加一个用于镜像拷贝的盘。硬盘容量需大于等于机器自带硬盘，如果机器有 RAID 卡请将该磁盘制作单盘 RAID0

3.DCIM内搜索 IPMI地址，找到对应机器，并将该机器的公网地址绑定到 DCIM对应机器（如果 IP 之前绑定了用户，请记录绑定的用户，操作完成后需要复原）





4.点击援救系统，选择 Windows，并记录远程信息，打开 VNC
观察，等待援救模式进入完成后，远程该地址（如果无法进入请参考 DCIM常见排障流程自行排查）


设备摘要
日志
IPV4地址 (1)
IPV6地址
网卡
硬件
硬件历史记录
故障历史
会话回放
资源监控
PDU
服务器信息
关机
重启
电源功率 (W)
1小时
一天
ID
物理标签
主机名
SERVER20230110zcjht
硬件型号
华为-XH320 V2
CPU型号
Intel(R) Xeon(R) CPU E5-2420 v2 @ 2.20GHz
内存型号
8 GB (1333 Mhz / Max 1600 Mhz) x 1
8 GB (1333 Mhz / Max 1333 Mhz) x 1
硬盘型号
SATA SSD WDC WDS240G2G0A- @ 240.07 GB x 1
PCI设备
I350 Gigabit Network Connection x 2
Z11/Z11M
机房 | 机柜
成都西信805 | XX-805-3F-E-F04
序列号
资产序列号
重置BMC
救援模式
重装系统
硬件信息
重置密码
下载KVM
下架计划
救援模式
系统类型
自动
Windows
Linux
激活救援模式后, 下次重新启动时
您的服务器将会以无盘启动的方式启动到救援模式
这样您可以根据您的需求进行使用救援模式
如在救援模式重启服务器, 则会取消救援系统模式
取消
激活救援系统
操作
软件信息 (开通信)
IPMI用户列表
IPMI地址
IPMI用户名 - 密码
引导模式
操作系统
用户名 - 密码
远程端口
57161
使用类型
租用
预装标记

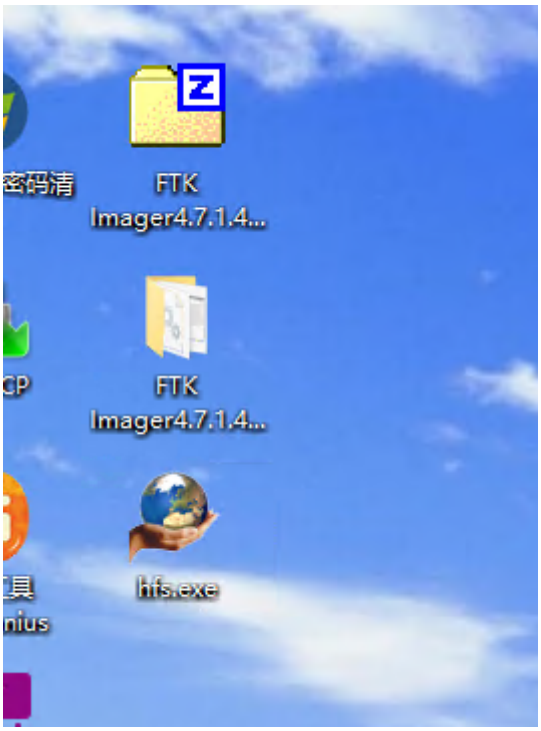

成功
Windows PE 已成功激活
您的服务器应将进入救援模式
然后, 您可以使用
用户名: Administrator
密码:
远程端口: 3389
以救援模式访问服务器
关闭


uration, Please Wait...

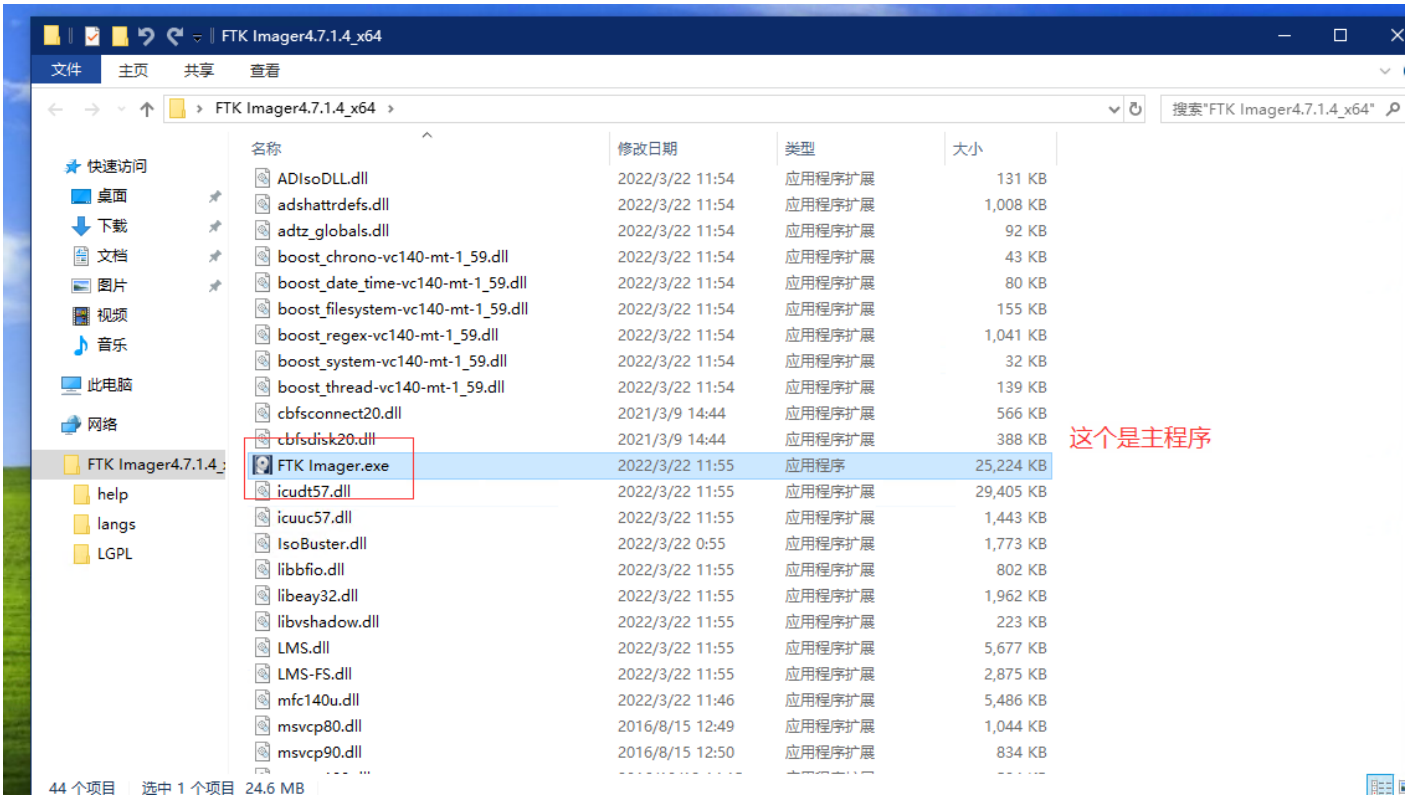

此电脑
Everything
镜像还原恢复
回收站
HDTune
浏览器
屏幕键盘
PuTTY
内存检测
AIDA64
Windows 安装器
数据恢复 (支持网络传输)
到这个界面才是启动完成
AnyDesk
Windows密码清除
无损分区
CPU-Z
WinSCP
虚拟光驱
DISM++
分区工具 DiskGenius
远程接入 USB
英
6:20
2024/11/11


222.211.75.71 - 远程桌面连接
回收站
Windows密码清除
屏幕键盘
WinSCP
AIDA64
分区工具 DiskGenius
使用远程桌面连接
AnyDesk
镜像还原恢复
CPU-Z
浏览器

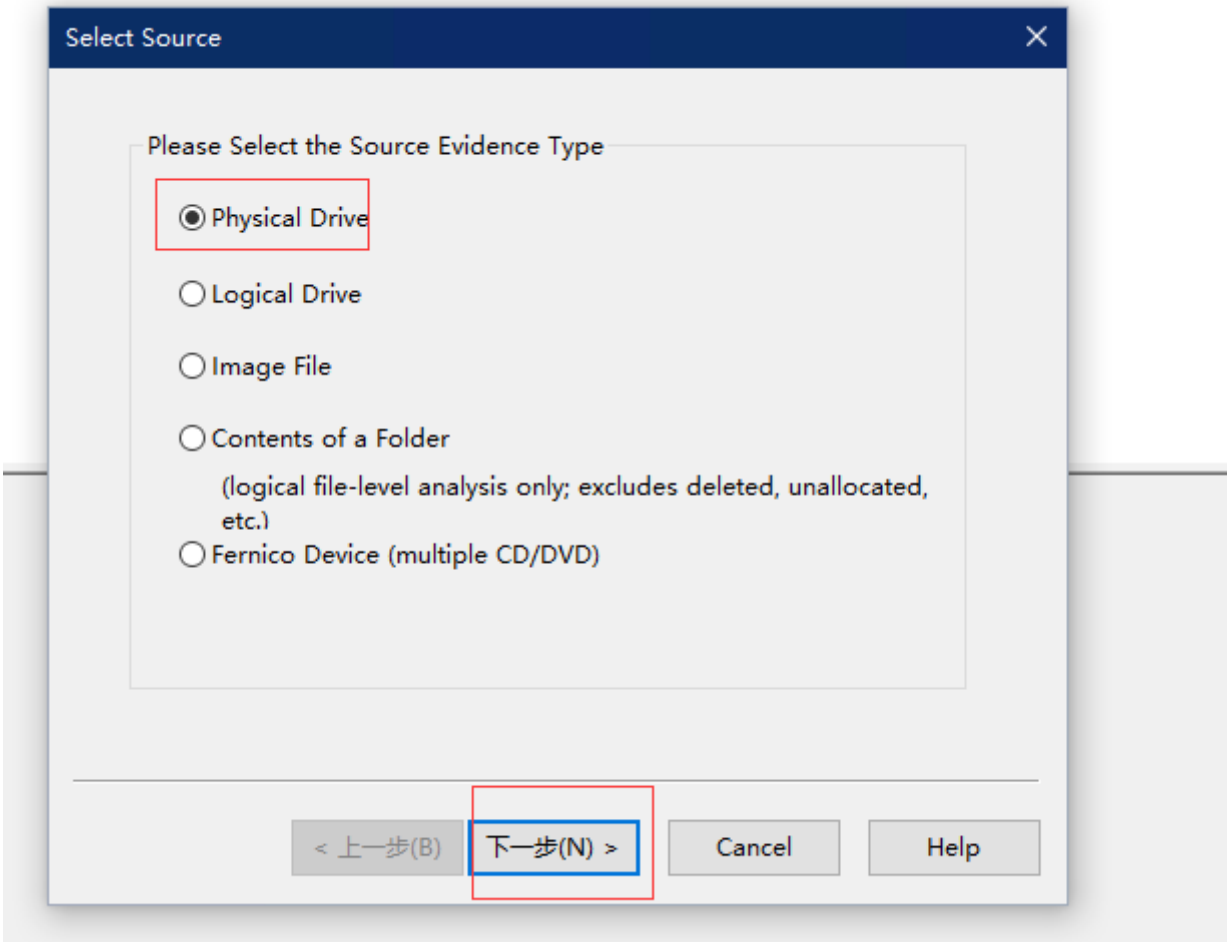
5.□□□□□□□□□□□□□□□□ FTK□□□ HFS□□□□□ FTK□□□□



6.□□ FTK□□□



□□□□□ File-Create Disk Image□□ Physical Drive□□□□□


Select Source
Please Select the Source Evidence Type
Physical Drive
Logical Drive
Image File
Contents of a Folder
(logical file-level analysis only; excludes deleted, unallocated, etc.)
Fernico Device (multiple CD/DVD)
< 上一步(B)
下一步(N) >
Cancel
Help

□□□□□□□□□□□□□□□□□□□□□□□□ Finish(□□□□□□□□□□□□□□□□□□□□□□

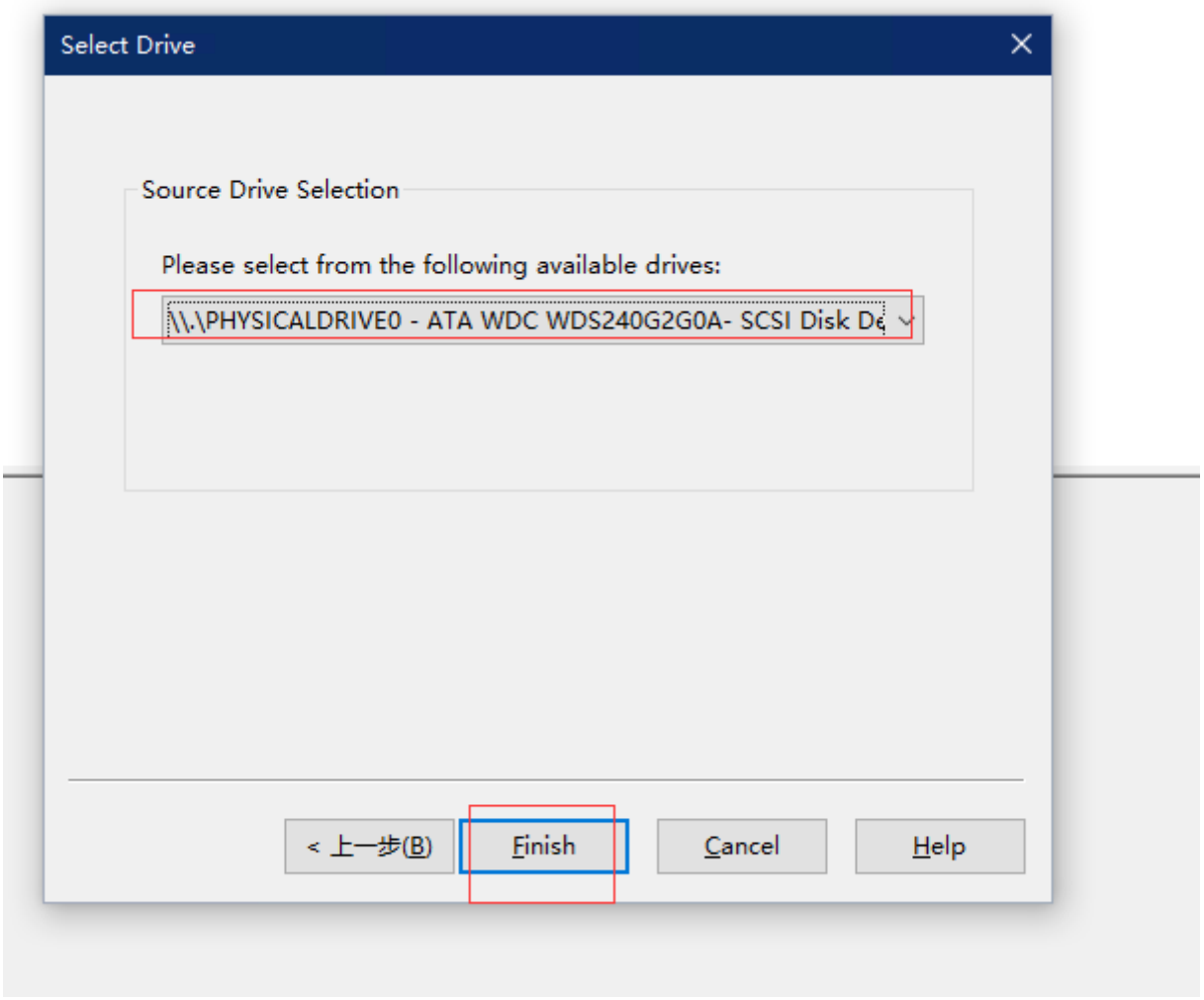
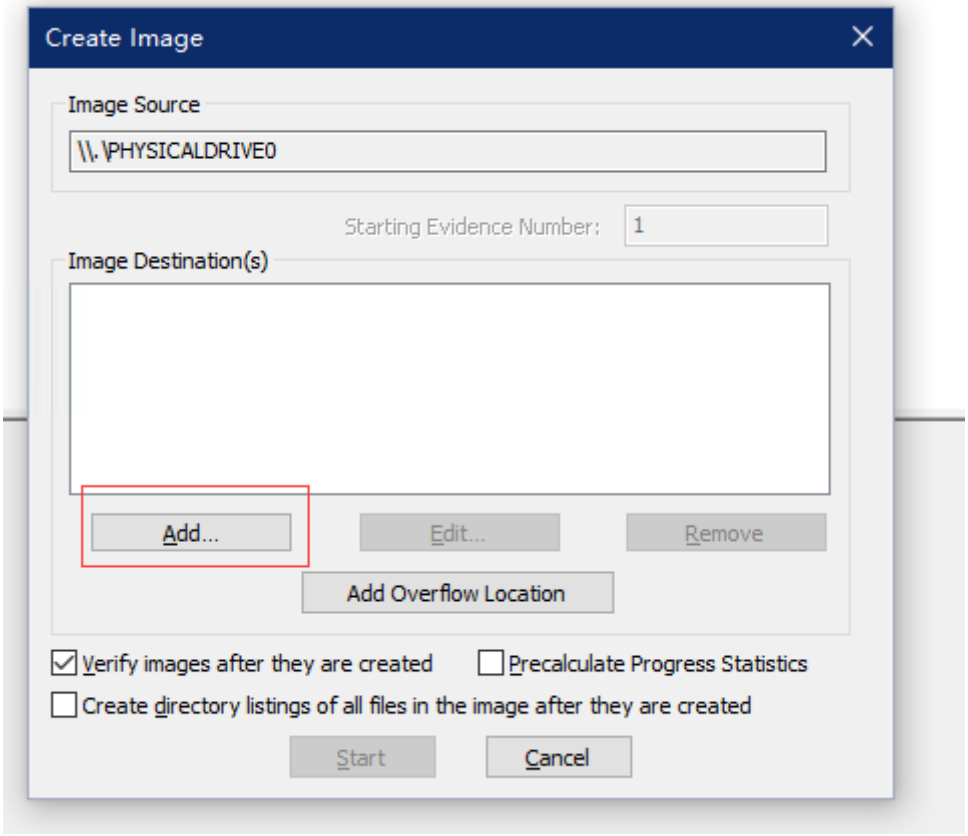
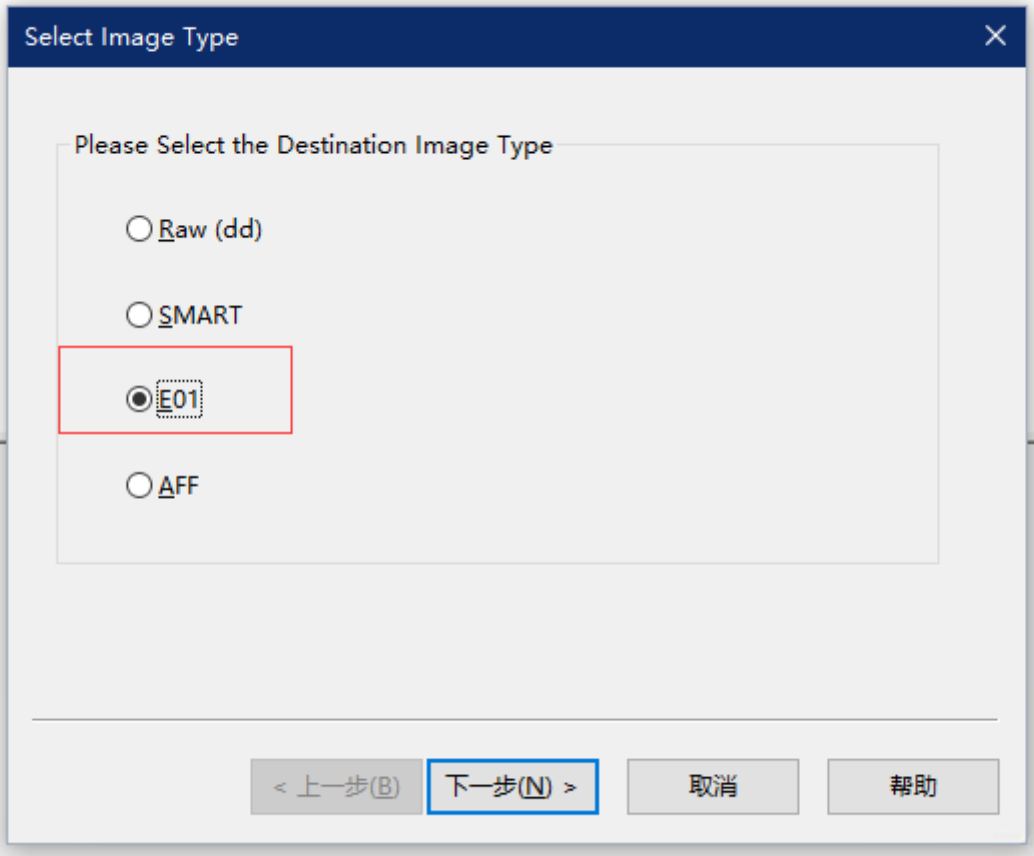


Image Destination□□□　ADD□□□　E01


Create Image
Image Source
\\.\PHYSICALDRIVE0
Starting Evidence Number:
1
Image Destination(s)
Add...
Edit...
Remove
Add Overflow Location
Verify images after they are created
Precalculate Progress Statistics
Create directory listings of all files in the image after they are created
Start
Cancel


Select Image Type
Please Select the Destination Image Type
Raw (dd)
SMART
E01
AFF
< 上一步(B)
下一步(N) >
取消
帮助

□□□□□□□□

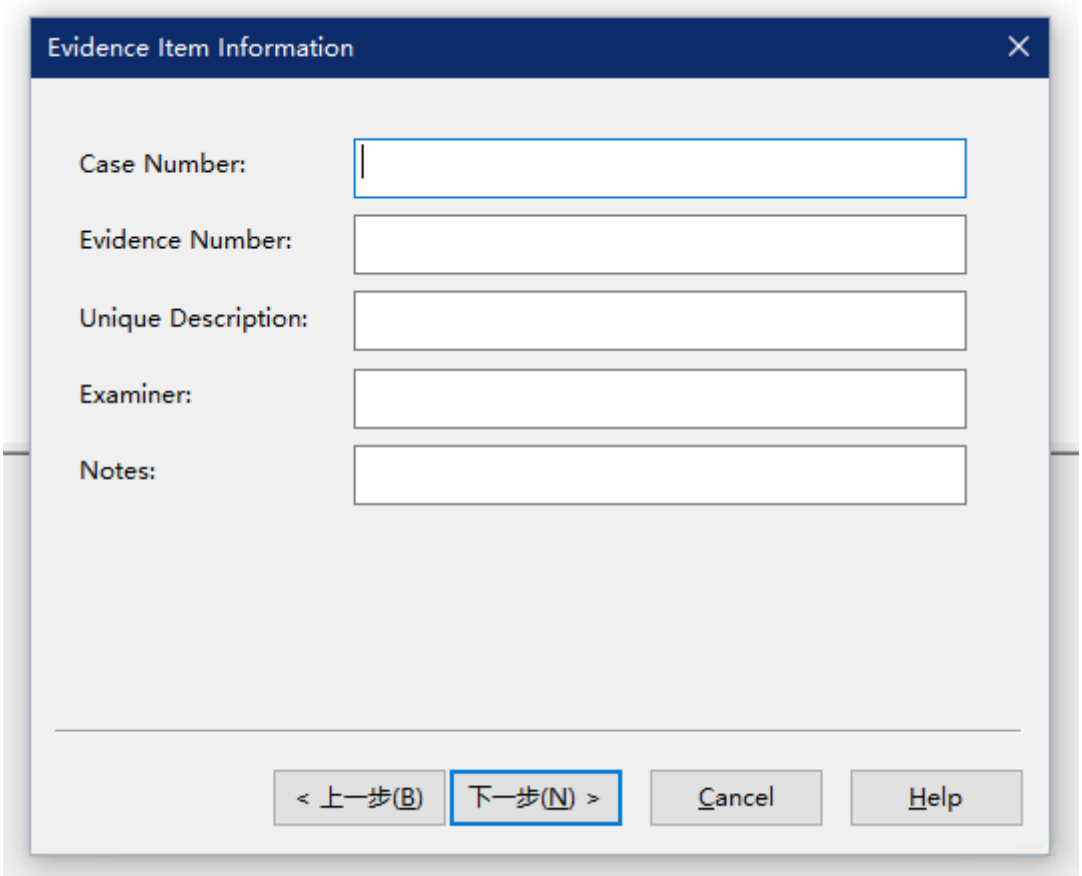
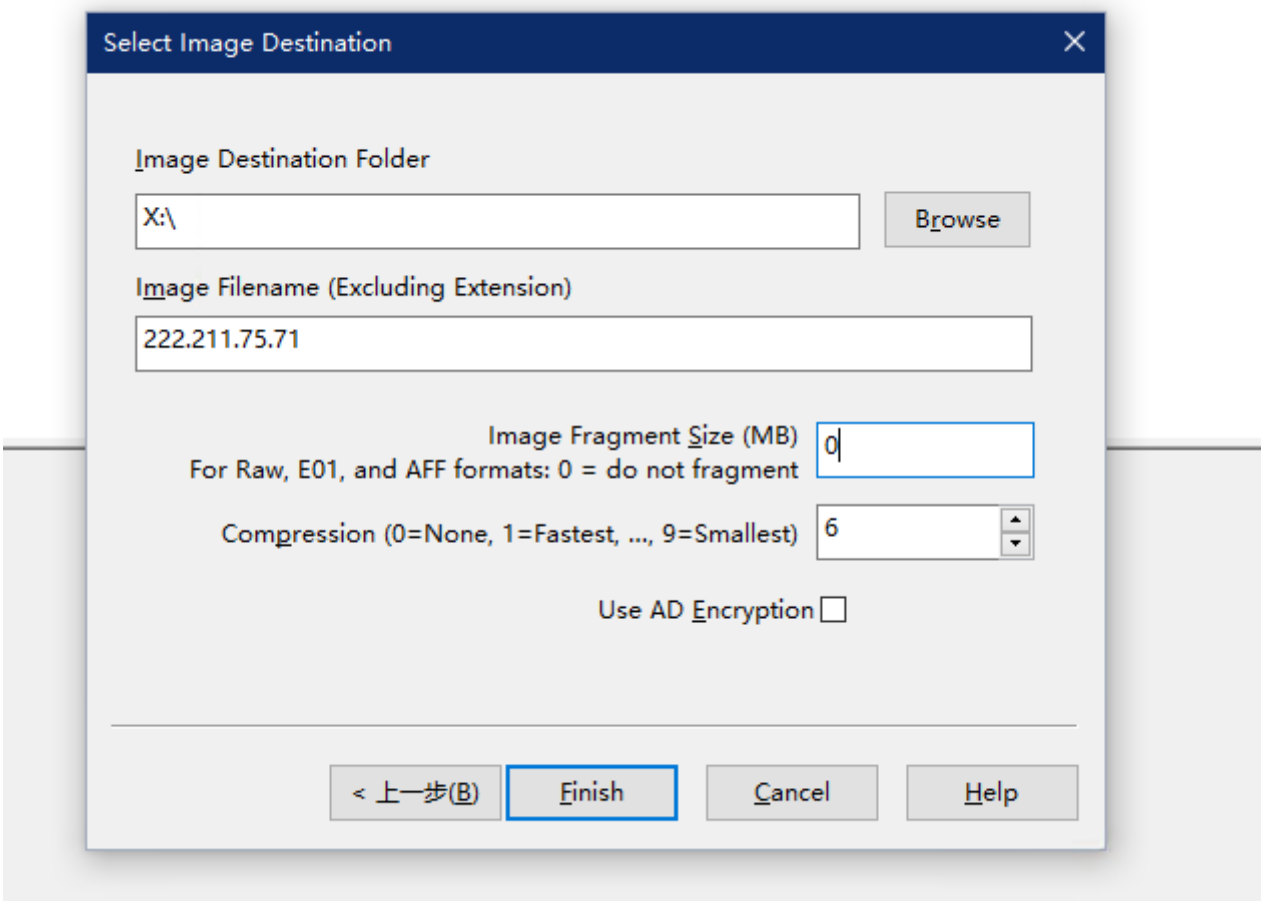


Image Destination Folder选择刚刚现场临时加的盘，如果不显示硬盘请打开 DiskGenius 工具对刚现场临时加的盘进行分区

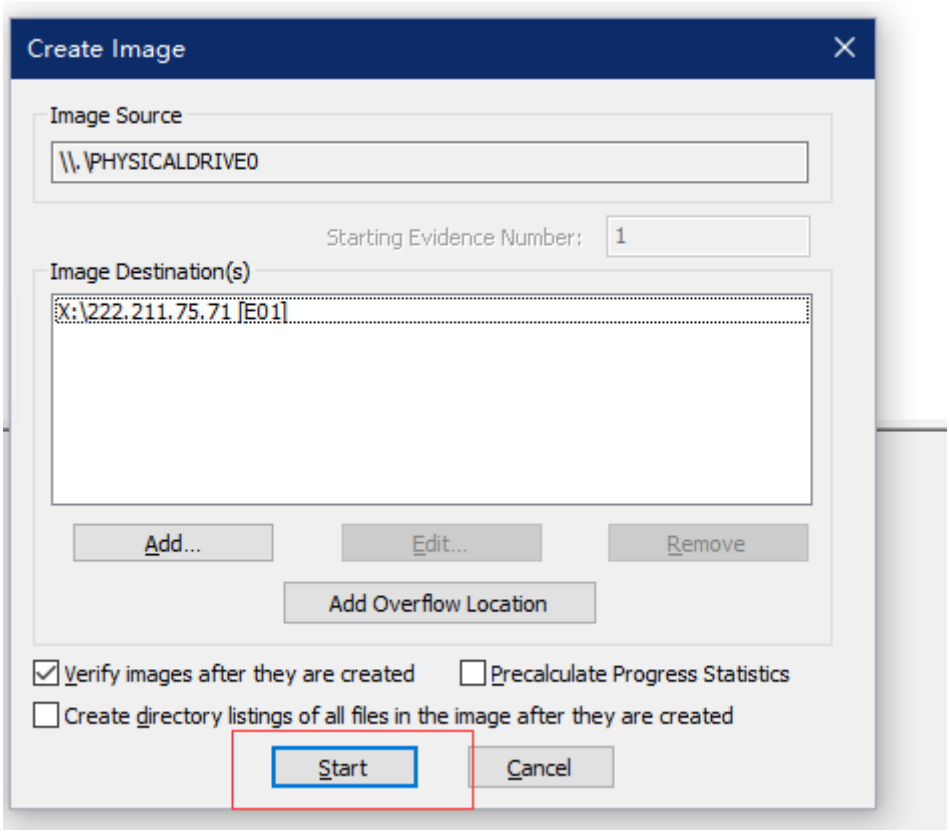
Image Fileame请填写服务器 IP

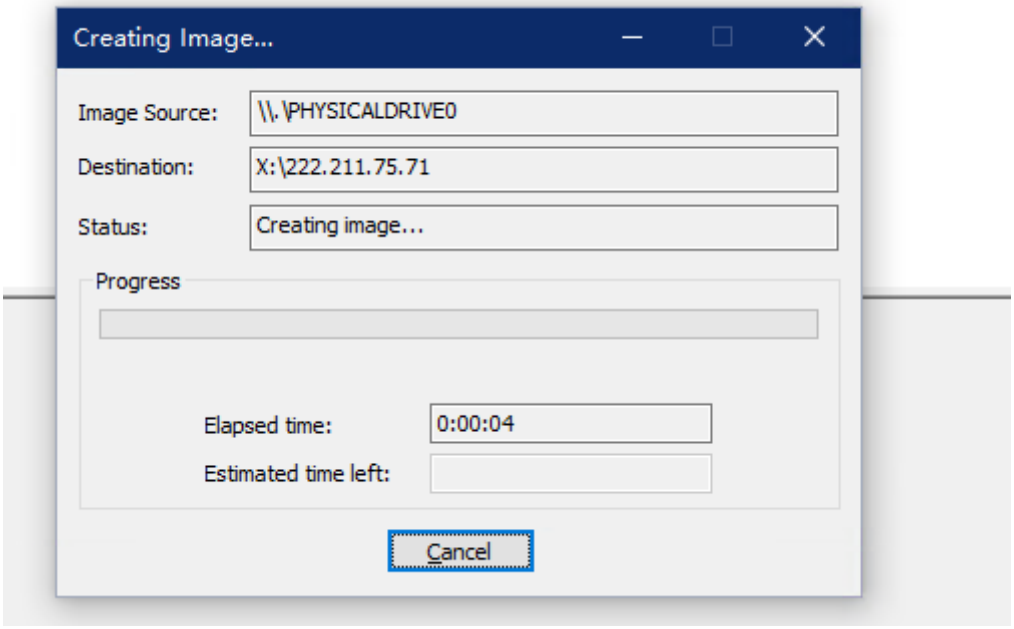
Image Fragment Size填写 0

并点击 Finish

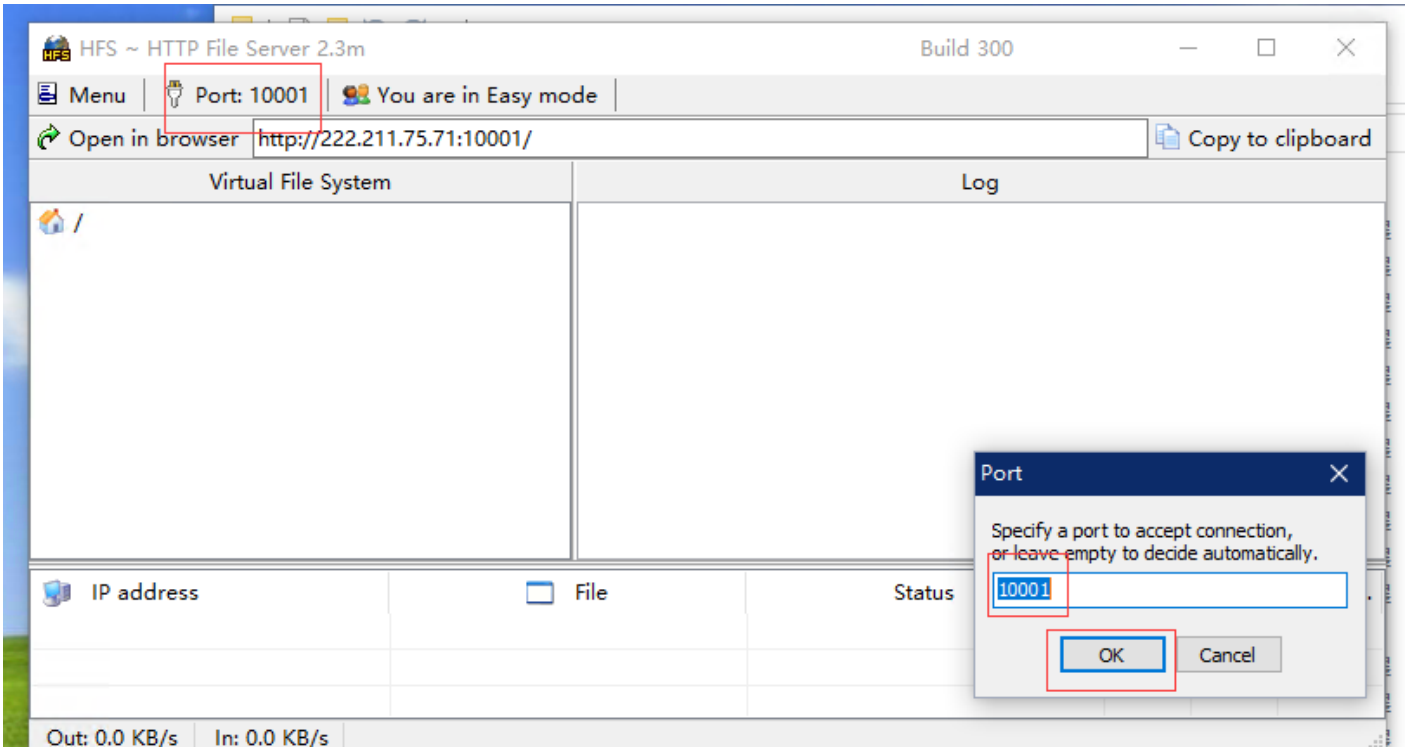

Select Image Destination
Image Destination Folder
X:\
Browse
Image Filename (Excluding Extension)
222.211.75.71
Image Fragment Size (MB)
For Raw, E01, and AFF formats: 0 = do not fragment
0
Compression (0=None, 1=Fastest, ..., 9=Smallest)
6
Use AD Encryption
< 上一步(B)
Finish
Cancel
Help

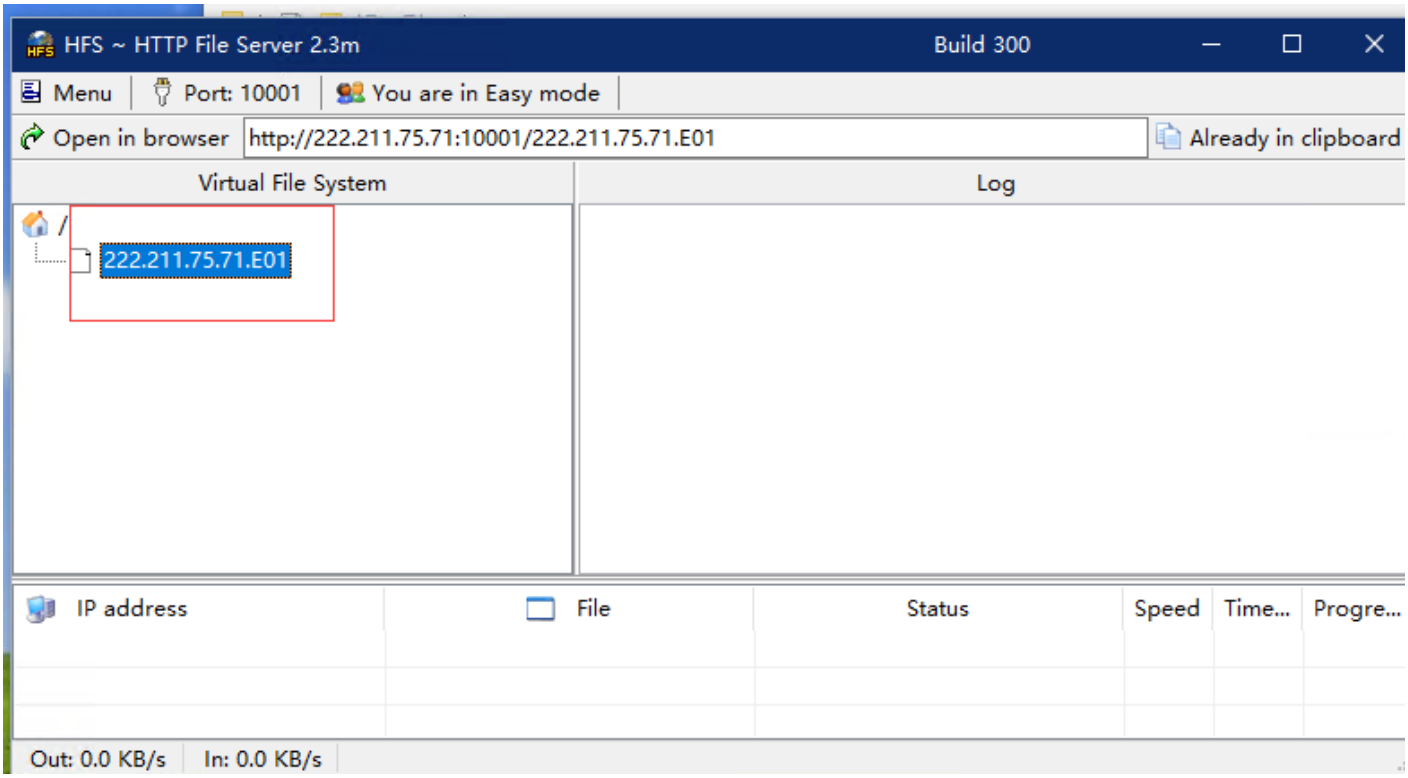
□□ Start□□□□□


Create Image
Image Source
\\.\PHYSICALDRIVE0
Starting Evidence Number:
1
Image Destination(s)
X:\222.211.75.71 [E01]
Add...
Edit...
Remove
Add Overflow Location
Verify images after they are created
Precalculate Progress Statistics
Create directory listings of all files in the image after they are created
Start
Cancel



7.□□□□□□□□□□ HFS□□□□ HFS□□□□□ 10001□□□□□□□□□□□□□





8.□□□□□□□ http://<□□□ IP>:10001□□□□□□□□□

9.□□□□□□□□□□□□□□□□□□□□□□□□□□

10.□□□□□□□□□□