Supported Source Data Formats

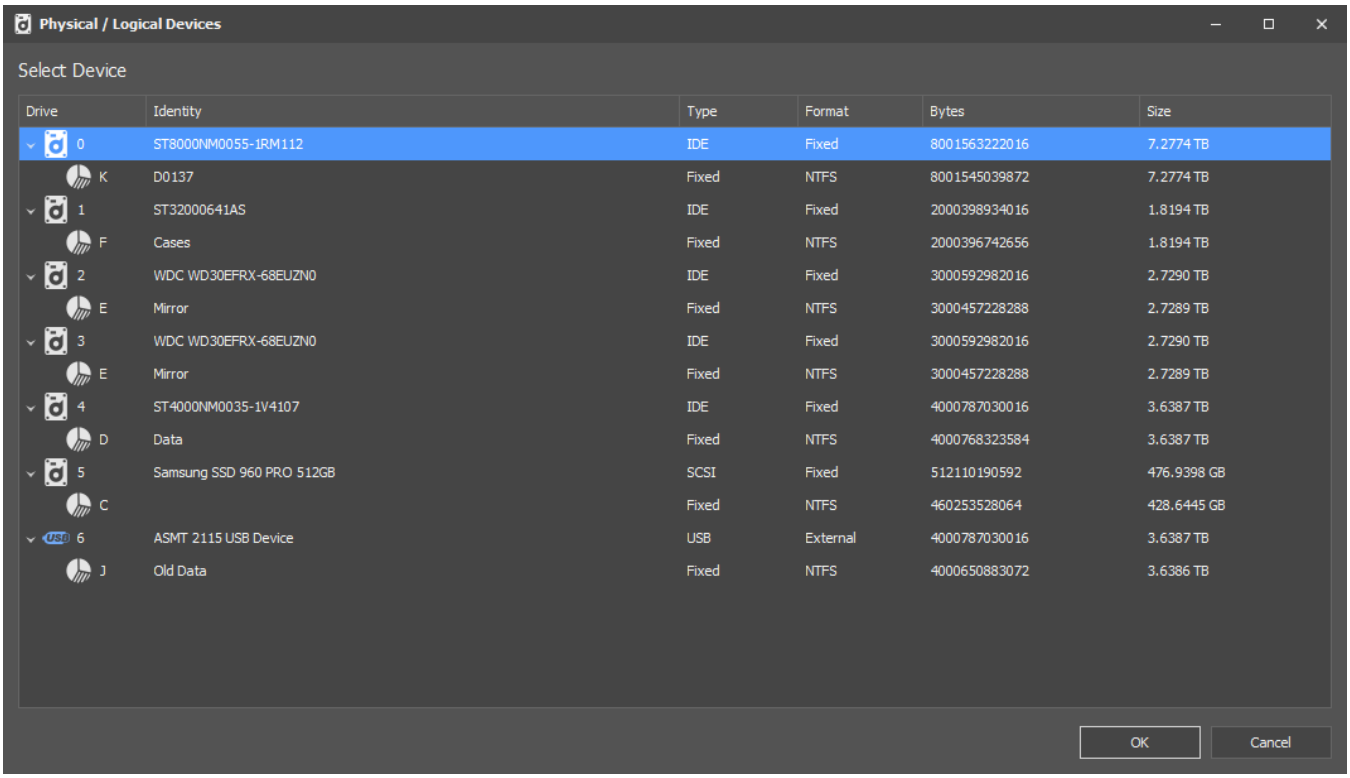
Forensic Image File Formats

Blade® natively supports a number of different image and output file formats. The following table represents a summary of the supported file types.

File Format	File Extensions
EnCase® Image File (EVF / Expert Witness Format)	*.e01
EnCase® Evidence File Format v2	*.ex01
EnCase® Logical Evidence File Format v1	*.L01
EnCase® Logical Evidence File Format v2	*.Lx01
SMART/Expert Witness Image File	*.s01
X-Ways Forensics Image File	*.e01
VMWare Virtual Disk File	*.vmdk
AFF v3	
Virtual Hard Disk	*.vhd
Segmented Image Unix / Linux DD / Raw Image Files	*.000, *.0000, *.00000, *.001, *.0001, *.00001
Single Image Unix / Linux DD / Raw / Monolithic Image Files	*.dd; *.img; *.ima; *.raw
Memory Dumps	*.dmp; *.dump; *.crash; *.mem; *.vmem; *.mdmp
Binary Dumps	*.bin; *.dat; *.unallocated; *.rec; *.data; *.binary
Mobile Phone Raw Binary Memory Dumps	*.bin

Direct Sector Access to Physical and Logical Devices

HstEx® has the ability of directly accessing at the sector level any physical or logical devices attached to the host system. This allows the user to employ write blockers and to recover data directly from a disk or external media.



Warning

Do **NOT** mount supported image types and then process them as if they were physical or logical devices. This makes no sense whatsoever and will result in really slow processing. If the image type is supported, then using HstEx® to natively process the image is by far the fastest and most effective method. If you have an image format that is not supported, please contact support.

A write blocker should be used when accessing physical or logical devices directly. If the hard disk is failing, please use a data recovery imager to capture the data from the device first and run HstEx® against the resulting image.