

## Digital Media Exploitation Kit

### Collecting forensic data from PC hard drives

An ever increasing number of PCs are being used to commit or plan crimes. Digital investigations identify digital evidence and collect intelligence about the actions of authorized and unauthorized computer users.

The typical digital investigation process includes removing the hard drive from a PC, copying the drive contents to another storage location, reinstalling the hard drive in the PC, and finally analyzing the contents. These are difficult and time-consuming steps that risk the loss of critical data and require substantial training.

### The automated alternative

Basis Technology's Media Exploitation Kit (MEK) speeds up and simplifies the process of acquiring data from PCs to make a drive image. MEK is an easy-to-use forensics tool for capturing the entire contents of a PC hard drive without removing it from the PC.

**Step 1:** Connect the external MEK capture drive to the PC with the USB or FireWire cable

**Step 2:** Insert the bootable MEK CD-ROM in the PC

**Step 3:** Boot the PC

The remainder of the process is automatic. No specialized training is required, and the user is not required to perform any operation that risks damaging the hard drive or losing data.

MEK stores a perfect copy of each PC hard drive on its own *capture drive*. It also stores forensic metadata, such as the serial number of the drive, and the time the data is captured. MEK also produces a cryptographic hash to allow the integrity of the data to be verified. The user may also store a cryptographic signature of the data and other user-specified metadata.

### Where can I use MEK?

MEK can capture data from any PC with an x86 CPU (i386 through Pentium, AMD Athlon, etc.), a bootable optical drive, and a USB or FireWire interface. MEK will capture from IDE, ATA, SATA, SCSI, USB, and Firewire drives on the target computer.

### Easy to Use

The target hard drive remains in the PC

No specialized training required

Creates a hard drive image from any x86 standard PC

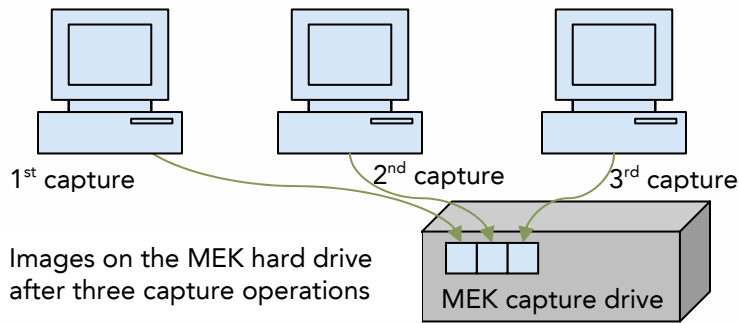
### Noninvasive

The capture operation does not modify, in any way, the contents of the hard drive.

The captured image includes forensic metadata such as a cryptographic hash of the data, the hard drive serial number, and the time the capture was performed.

### What's included in the package?

- A bootable software CD-ROM with software for capturing the content of PC hard drives
- An external hard drive with power supply, USB interface, and FireWire interfaces. Rugged drive options are also available.



### Advanced Forensics Format

AFF is a non-proprietary, open-source format for representing hard drive images. An AFF file is lossless and includes forensic metadata and a digital signature.

### The external capture drive

The user can capture images from as many PC hard drives as fit on the MEK capture drive.

The user can later off-load the image files from the capture drive to a repository and reuse the drive to capture additional images.

### The hard-drive image

MEK can capture the drive image in one of three formats of the Advanced Forensics Format (AFF). One format stores the data in a single file, the second stores the data in multiple files, and the third stores the disk data in a raw file and the metadata in a separate file.

AFF is an open format for storing a compressed drive image. Typically AFF can store twice as many images as the raw format on a capture drive – more if the hard drives were not fully used. AFF metadata includes the number of empty sectors, the number of unreadable (corrupted) blocks, forensic metadata, and the cryptographic hash.

### MEK Pricing

The Media Exploitation Kit is available on the Basis Technology's GSA schedule.

For more information on pricing or details, please call 617.386.2090 or email [info@basistech.com](mailto:info@basistech.com)

Basis Technology Corporation

T 1.617.386.2000  
1.800.697.2062 (toll-free)

F 617.386.2020

E [info@basistech.com](mailto:info@basistech.com)