

メディア(媒体)解析キット(MEK:Media Exploitation Kit)

使用方法は簡単

ターゲットのハードドライブはPCに入ったままで、取り出し不要。

特別なトレーニングは不要。

標準的な X86PC からハードドライブ・イメージを作成します。

データの保存

キャプチャ操作による、ハードドライブの内容改変の心配は無用です。

キャプチャされたイメージには、データのハッシュ値、ハードドライブのシリアル番号、キャプチャをおこなった時間の記録などのフォレンジック・メタデータが含まれます。

PCのハードドライブからフォレンジックデータを収集

犯罪に PC が関与する例が増えてきています。デジタル捜査は、デジタルデータに残る証拠を確認し、アクセス権限を持つユーザおよび持たないユーザが取った行動についての情報を収集します。

デジタル捜査の手順は、通常、PC からハードディスクをとりはずし、その内容を他のストレージにコピーし、そのハードディスクをまた元の PC に戻して分析します。これは非常に困難で時間のかかる作業なうえ、重要なデータを消去してしまう可能性があり、また十分なトレーニングを必要とします。しかし、Basis Technology のメディア解析キット(MEK)は、トレーニングが不要で簡単に利用できます。

作業の自動化

Basis Technology の MEK は、PC からのデータ入手プロセスを迅速に、かつ簡略化しておこない、ドライブ・イメージを作成します。MEK は PC のハードドライブを外さずに内容をすべてキャプチャすることができる簡便なフォレンジック・ツールです。

ステップ 1: 外付けの MEK キャプチャ・ドライブを USB もしくは FireWire ケーブルを使って PC に接続します。

ステップ 2: MEK の起動用 CD-ROM を PC に挿入します。

ステップ 3: PC を起動します。

この後のプロセスはすべて自動です。特別なトレーニングや、ハードドライブに損傷を与えたりデータを消去する恐れのある操作は一切不要です。

MEK は、各ハードドライブのコピーをまるごとキャプチャ・ドライブに保存します。また、ドライブのシリアル番号、キャプチャをおこなった時間の記録などのフォレンジック・メタデータも保存します。ハッシュ値によってデータが同じものであることが確認できます。MEK は、当該データのデジタルシグネチャや、ユーザーによって指定されたほかのメタデータも保存できるよう設計されています。

MEKの使用環境

MEK は x86CPU(Pentium、AMD Athlon 等の i386MPU)使用のいかなる PC、ブート可能なオプティカル・ドライブ、USB あるいは FireWire インターフェースからのデータのキャプチャが可能です。MEK は当該 PC の IDE, ATA, SATA, SCSI, USB, FireWire ドライブへの対応も予定しています。

AFF: Advanced Forensics Format

AFF は、ハードドライブ・イメージを表示するための、公開、オープンソース・フォーマットです。AFF ファイルは、ロスレス（可逆）でフォレンジック・メタデータとデジタルシグネチャが含まれます（開発予定）。

ベシス・テクノロジー株式会社

Tel: 03-3511-2947

Fax: 03-3511-2948

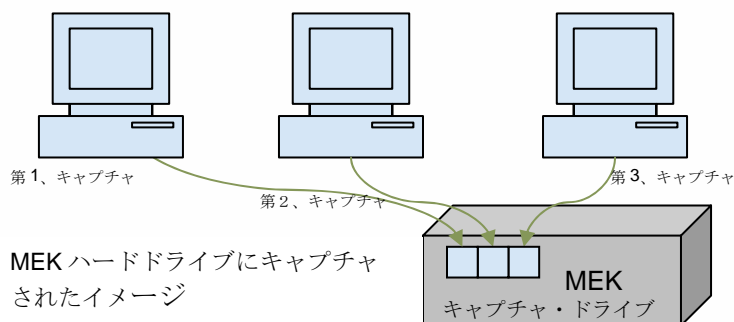
Tokyo.Marketing@basistech.com

パッケージ内容

- PC のハードドライブのコンテンツをキャプチャするソフトウェアを搭載した起動用 CD-ROM
- 外付けハードドライブと電源、USB インターフェース、FireWire インターフェース。オプションとして、安心して持ち運べる丈夫なドライブも用意。

外付けのキャプチャ・ドライブ

MEK キャプチャ・ドライブへの取り付けが可能な限り、多数のハードドライブからイメージをキャプチャすることができます。



イメージファイルをキャプチャ・ドライブからレポジトリへと移した後は、ふたたび新たなイメージをドライブにキャプチャすることが可能となります。

ハードドライブ・イメージ

MEK は、AFF(Advanced Forensics Format) の 3 種類のフォーマットのうち 1 種類のドライブ・イメージをキャプチャすることができます。1 つ目のフォーマットはデータを単一のファイルに保存、2 つ目は複数のファイルに保存、3 つ目はディスクデータをそのままファイルに保存し、メタデータを別のファイルに保存します。

AFF は圧縮したドライブ・イメージを含むオープンストレージ・フォーマットで、通常の 2 倍以上(ハードドライブに空き容量があればそれ以上)のイメージをキャプチャ・ドライブに保存することが可能です。AFF のメタデータには、空きセクタ数、読み取り不可のこわれたブロック数、フォレンジック・メタデータ、ハッシュ値が含まれます。

この製品についての詳細は、下記までメールにてお問い合わせください。Tokyo.Marketing@basistech.co.jp