A-3-2
標的型攻撃の痕跡調査

金城学院大学
西松　高史

このセッションの目的

われわれで、できる証拠保全の方法を実習にて確認する

（1） スナップショットを実際に行い、動きを理解する
（2） スナップショットを利用し簡単な解析を体験する

メニュー

1. 証拠保全について
    1. 証拠保全の重要性
    2. デジタル・フォレンジックについて
2. スナップショットの取得について
    1. スナップショットの取得と種類
    2. スナップショットの注意点
3. 実習
4. メモリダンプの解析例
5. まとめ

証拠保全について

証拠保全について

■ 証拠保全の重要性

稼働中のシステムで調査を行えば、不正なプロセスやネットワーク情報を検出することができる可能性が高い。

しかし、闇雲に調査を行うことで「日時情報」「一時ファイル」「揮発性データ」「ログ」など様々な情報が変化してしまう。最悪の場合、不正なプログラムが自己消去してしまう可能性も想定される。これでは、調査では無く、妨害になってしまう。

これを防ぐためにも、可能な限り被害当時のままの状態を複製する必要がある。この作業のことをデジタル・フォレンジックの世界では「証拠保全」と呼んでいる。解析するかどうかの判断の前に「証拠保全」は必要である。

証拠保全について

■ デジタル・フォレンジック

基本となるのは電磁的証拠の保全(Digital Evidence Preservation)の手続き。

インシデントに関わるデジタル機器に残されたデータの中から、電磁的証拠となり得るものを、収集・取得・保全する手続き。

この手続きに不備があると、後の分析結果の信頼性を失ってしまう。非常に神経を使う作業である。

詳しく書かれている資料
「証拠保全ガイドライン　第2版」 2012年7月13日
特定非営利活動法人　デジタル・フォレンジック研究会
「技術」分科会ワーキンググループ

ちなみに、業者に依頼すると…
解析費用は1台、約60万円(定価)
フォレンジックのためのセミナーもある。約16万円～約50万円

スナップショットの取得について

スナップショットの取得について

- スナップショットの取得と種類

フォレンジックとまではいかないが、われわれで比較的簡単に調査ができれば、あたりをつけることができるのではないか？ということで、今回は、怪しいと思ったときのコンピュータの状況の物理コピーしたものを「スナップショット」と表現する。

スナップショットは大きく分けて、メモリとファイルシステムに分かれる。今回は、この2つのスナップショットの取得について実習をする。

スナップショットの取得について

■ スナップショットの注意点

スナップショットは稼働中に行う必要があり、ネットワークケーブルなども抜かずに作業を行う必要がある。実行環境が変わると、必要(不正)なプロセスが起動しない可能性があるため、よいスナップショットにならない。

スナップショットの取得について

■ ツールの準備

Windowsベースで動作するもの

フリーツール

- ・FTK Image Lite(メモリ、HDD)　→今回はこれを利用
- ・Moonsol Dumplt(メモリ)
- ・MANDIANT Memoryze Memory(メモリ)

商用ツール

- ・FTK Image
- ・EnCase Forensic など…

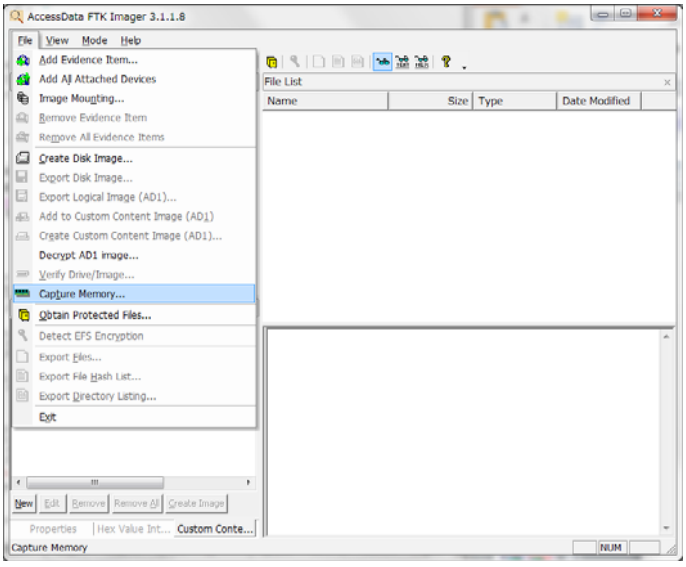
今回は「FTK Image Lite 3.1.1」を利用する

http://www.accessdata.com/support/product-downloads

実習

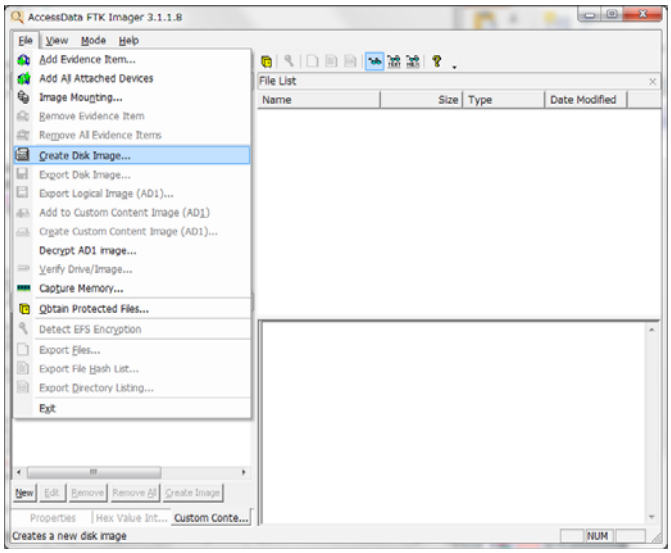
スナップショットの取得

- メモリダンプの取得（演習3-4）
  - 「FTK Image Lite」を起動し、「Capture Memory」でメモリダンプを取得



スナップショットの取得

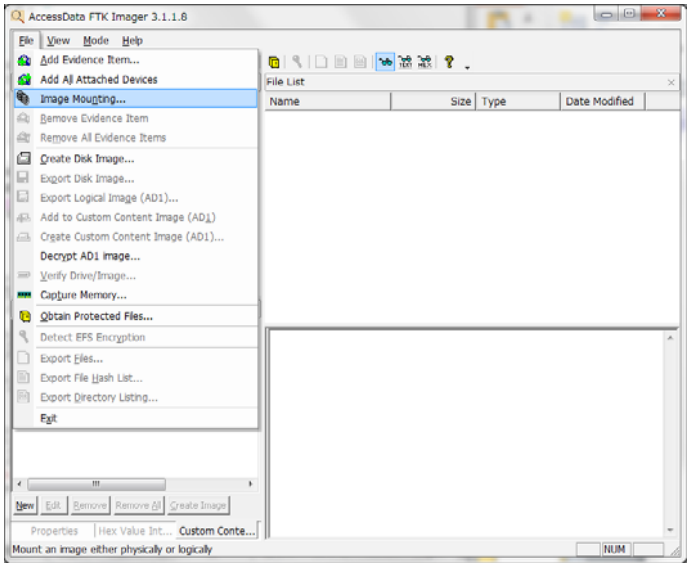
- HDDスナップショットの取得（演習3-5）
  - 「FTK Image Lite」を起動し、「Create Disk Image」でHDDスナップショットを取得



スナップショットの解析

- HDDスナップショットのマウント（演習3-6）
  - 「FTK Image Lite」を起動し、「Create Disk Image」でHDDスナップショットをマウント

本来ならば、この前にイメージのコピーが必要



スナップショットの解析

- メモリダンプの解析
  - 「volatility」を利用
  - Pythonで開発されており、比較的容易にプラグインを取り込むことができる。
  - 現在の2.2でサポートされているバージョン
    - Windows XP SP 2,3
    - Windows 2003 Server SP 0,1,2
    - Windows Vista SP 0,1,2
    - Windows 2008 Server SP 1,2
    - Windows 7 SP 0,1

https://code.google.com/p/volatility/downloads/list

今回は「volatility-2.2.standalone.exe」を使用する

メモリダンプの解析例

- メモリダンプの解析（演習3-7）
  - 「volatility」を利用
    - pslist
    - sockscan
  - 別紙

まとめ

- 証拠保全の必要性
  - フォレンジックかスナップショットか
  - 調査の妨害をしないように
- スナップショットについて
  - スナップショットの取得方法
  - スナップショットからわかること（メモリダンプ、HDDイメージ）
  - 簡易的な解析方法

高度な技術、ツールが必要