# メモリフォレンジック

～ メモリ情報からプロセスや通信履歴を迅速解析 ～【２日間】

揮発性データであるメモリ情報を保全し、解析することで、実行プロセスや通信履歴を迅速に把握することが可能です。また、近年、HDDに痕跡を残さないファイルレスマルウェアなどの増加やファストフォレンジックの必要性から、メモリフォレンジックの技術が注目されています。メモリ情報の保全から解析まで、実践的な演習を通して、メモリフォレンジックについて学習します。

## 研修のゴール

・メモリ情報の保全方法及び手順を理解し、適切にメモリ保全ができるようになる
・メモリ情報の解析ツールの使い方を理解し、適切に使用できるようになる
・メモリ情報から確認できた痕跡情報から、適切に情報の解析ができるようになる

## 受講対象者

・デジタルフォレンジック担当者
・セキュリティ担当者、CSIRT/SOC担当者
・システム管理者

## 前提知識/望ましいスキルなど

・ネットワークに関する基礎知識
・OS（Windows/Linux）に関する基礎知識
・デジタルフォレンジックの基礎知識

## 実施アジェンダ

【1日目】

１．デジタルフォレンジック基礎
２．システムの全体像
　１）コンピュータシステム概要
　２）メモリの基礎、データ構造
３．メモリ保全
　１）メモリ保全の考え方
　２）メモリダンプ/保全基礎
　３）メモリイメージの変換
４．メモリ解析ツール
　１）Volatility Framework
　２）その他ソフトウェア、ツール群
５．メモリ解析基礎
　１）アーティファクト解析
　２）メモリ上のデータ解析/データカービング

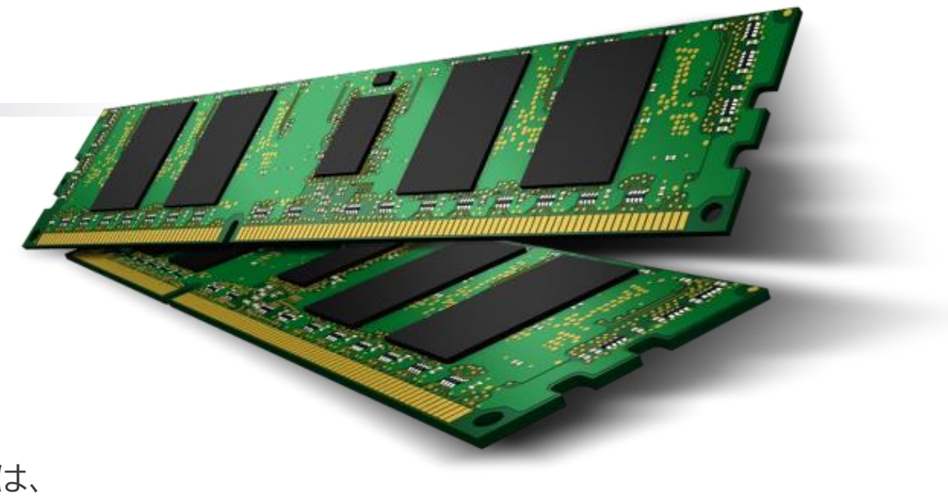
【２日目】

６．Windowsシステムのメモリ解析
　１）ネットワーク
　２）Windows オブジェクト
　３）プロセス、ハンドル、トークン
　４）プロセスメモリ
　５）Windowsマルウェア解析
　６）イベントログ
　７）レジストリ情報
　８）Windows サービス
７．パスワード解析 / 暗号化解析
８．イベントの再構成
９．タイムライン作成
１０．総合演習

## 開催要項

・コース名：メモリフォレンジック
・開催日数：２日間（ 9:30-17:30 ）
・実施方法：オンライン、または、集合研修
・研修形式：座学、実機を使った演習
・研修費用：200,000円（税別）／人 （最少催行人数：4名）

当社の定期開催は1名様からお申込みいただけます。定期開催の実施スケジュールは、
弊社営業へお問い合わせください。また、個別開催も可能です。随時お問い合わせ下さい。



## お問い合わせ・お申込み

・ストーンビートセキュリティ株式会社
・TEL 03-6869-9567　メール：training@stonebeat.co.jp
・https://www.stonebeat.co.jp#training

Stonebeat Security
Your Trusted Security Advisor

# 研修テキスト

（サンプル）

## Volatility Framework

- Pythonで実装されたメモリフォレンジックツール
- コマンドライン（CUI）で利用
- 解析のための豊富なプラグインあり
- オープンソース
- Windows/Linux/Mac に対応

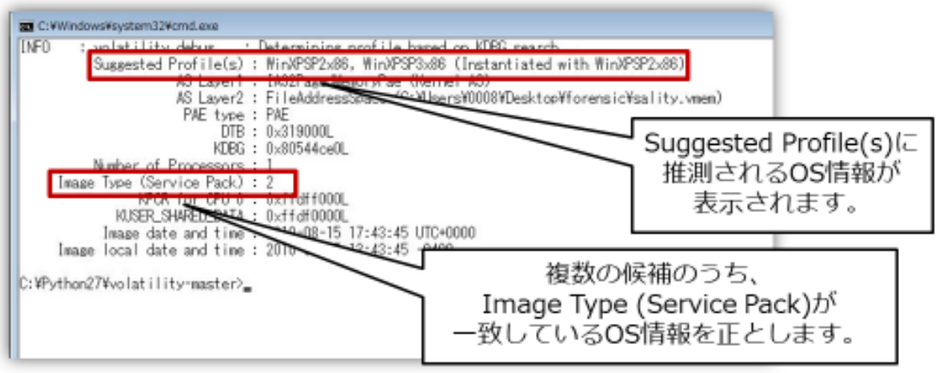

http://www.volatilityfoundation.org/



## 解析対象の識別

■ 識別コマンド　**imageinfo**

# volatility -f [メモリパス] imageinfo




- 以降の調査ではimageinfoコマンドの結果で確認したOS情報をもとに調査を行います。



## 演習：特権の状態の確認

A) カーネルドライバをロードできる特権はなんですか？

B) sample004.bin において、privsプラグインを実行し、
カーネルドライバをロードできるプロセスを列挙してください。

C) sample005.bin において、 privsプラグインを実行し、
dfssvc プロセス (PID 1608) が SeRestorePrivilege と
SeBackupPrivilege を有効にしています。
この点について、何か注意すべきことはありますか？

dfssvc.exe:
the Distributed File System Service
(分散ファイルシステムサービス)のプロセス



## volshellプラグインの利用

【volshell の実行例(対話的処理)】

```
In [1]: modules()
Offset     Base       Name
0x823fc3a0 0x804d7000 ¥WINDOWS¥system32¥ntoskrnl.exe
0x823fc338 0x806ee000 ¥WINDOWS¥system32¥hal.dll
0x823fc2d0 0xf8a50000 ¥WINDOWS¥system32¥KDCOM.DLL
0x823fc260 0xf8960000 ¥WINDOWS¥system32¥BOOTVID.dll
[snip]

In [2]: db(0x804d7000)
0x804d7000  4d 5a 90 00 03 00 00 00 04 00 00 00 ff ff 00 00   MZ..............
0x804d7010  b8 00 00 00 00 00 00 00 40 00 00 00 00 00 00 00   ........@.......
0x804d7020  00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00   ................
0x804d7030  00 00 00 00 00 00 00 00 00 00 00 00 d8 00 00 00   ................
0x804d7040  0e 1f ba 0e 00 b4 09 cd 21 b8 01 4c cd 21 54 68   ........!..L.!Th
0x804d7050  69 73 20 70 72 6f 67 72 61 6d 20 63 61 6e 6e 6f   is.program.canno
0x804d7060  74 20 62 65 20 72 75 6e 20 69 6e 20 44 4f 53 20   t.be.run.in.DOS.
0x804d7070  6d 6f 64 65 2e 0d 0d 0a 24 00 00 00 00 00 00 00   mode....$.......
```



## レジストリ情報
### ～ Registry in Memory

- レジストリには、Windows OS、アプリケーション、ユーザ情報など様々な設定と構成に関する情報が含まれているため、フォレンジックにおいては、非常に重要な調査対象となります。
  - 最近実行されたプログラムの特定
  - パスワードハッシュの抽出
  - 悪意のあるコードがシステムに導入したキーや値の調査
    など
- レジストリは、Windowsのコアコンポーネントとして、OS実行時に常にアクセスされます。

- この章では、メモリ内のレジストリの収集や調査方法を学習します。



## メモリダンプから文字列を抽出
### ～ Extracting Strings

- メモリダンプから文字列を解析する最初のステップは、文字列を抽出することです。文字列の抽出には stringsコマンド が利用できます。
- stringsコマンドでは、ASCII文字列 と Unicode文字列 の両方を抽出することが重要です。
- また、Volatilityで解析可能な形式で出力が可能です。Volatilityで対応できる形式は下記の通りです。

```
<decimal_offset>:<string>
<decimal_offset> <string>
```

※ Volatilityにはオフセットが必要で、その後にコロンやスペース、その後に抽出された文字列が続きます。
※ オフセットと文字列のペアは、プレーンテキストファイル内の改行で区切らなければなりません。



Stonebeat Security
Your Trusted Security Advisor