公判対応を前提とした メモリ・フォレンジック有用性の考察

Usefulness of memory forensics for the examination of evidence

野上 紘・ネットワーク分科会・情報セキュリティ大学院大学

Abstract In this study, focusing on the memory forensic techniques, we showed the usefulness of memory forensics through the examination of acquired information details and clarification of expected fact items of the designated crime. Furthermore, we discuss the reliability of tools used to clarify the evidence at law enforcement agencies from the view point of freedom impression principle.

目的

メモリ・フォレンジックについて
- どのような情報が判明するか
- どのように活用できるのか
- 得られた情報に証拠能力はあるのか

を明らかにして有用性を示し、普及へとつなげる

本研究の貢献

①判明する情報とその取得方法を明らかにし、想定に対する検証結果を公開することで、有用性を示した
②今まで曖昧であった証拠能力について考察を行い、解析の正確性を確保するための手法を提案した

① 判明する情報の一覧（一部抜粋）

カテゴリ	コマンド	cmd	GUI	判明する情報	備考
プロセスメモリ	memmap	○	×	メモリマップを表示	GUI：アプリケーションエラーが発生
	memdump	○	○	メモリデータ内に存在するプロセスの全メモリページをダンプして出力	
	procdump	○	○	メモリデータ内に存在するプロセス実行形式ファイル（EXE）をダンプして出力	
	evtlogs	×	×	メモリデータ内に存在するイベントログ情報を出力	XP/2003のみ対応
	iehistory	○	○	メモリデータ内に存在するブラウザ履歴を表示	
ネットワーク	connections	×	×	アクティブなネットワーク接続を表示	XP/2003のみ対応
	connscan	×	×	過去に発生したものを含めたネットワーク接続を表示	XP/2003のみ対応
	sockets	×	×	オープンしているTCPやUDPのソケット情報を一覧表示	XP/2003のみ対応
	sockscan	×	×	過去に発生したものを含めたソケット情報を一覧表示	XP/2003のみ対応
	netscan	○	○	TCPやUDPの接続状況を一覧表示	

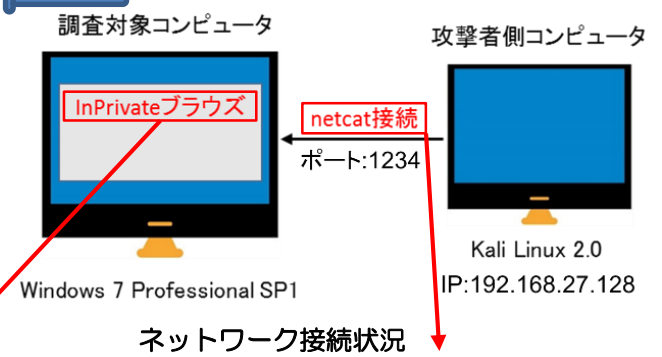
② 証拠能力確保の重点

■証拠の一貫性
■手続きの正当性
■解析の正確性
- コンピュータ内の情報を正しく取得できるか
- 取得した情報を正しく解析できるか

提案

解析ツールの正確性保証が、解析の正確性につながるのではないか⇒想定に対する出力結果を評価することで正確性の保証を図る

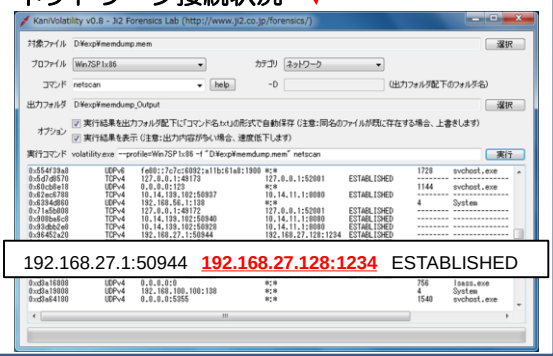
想定



Web閲覧履歴

```
**************************************************
Process: 5752 iexplore.exe
Cache type "URL " at 0x52bc280
Record length: 0x180
Location: https://www.iisec.ac.jp/
Last modified: 2016-01-08 03:38:28 UTC+0000
Last accessed: 2016-01-08 10:55:36 UTC+0000
File Offset: 0x180, Data Offset: 0x84, Data Length: 0x98
File: iisec_ac_jp[1].htm
Data: HTTP/1.0 200 OK
```

ネットワーク接続状況



課題

■技術面
活用事例の増加
- マルウェア検体の解析検証
- BitLockerの復号

■法律面
証拠の同一性確保
- 従来の手法は、ツールの動作や操作する人間の行為が正しいという前提の元で成立⇒実社会での利用を通じて客観性を高める検討が必要
- 意図的な改ざんの防止