Computer Security Symposium 2016
11 - 13 October 2016

アンチフォレンジック機能に対するメモリフォレンジックツールの有効性検証

田中 郁夫† 橋本 正樹†

概要：近年、情報技術を用いた犯罪が増加しており、これに対処する捜査機関ではデジタルフォレンジック技術の重要性が高まっている。特に、フォレンジックの対象としては、従来のディスクに加えて、メモリから正確に情報を抽出する技術の重要性が高まっている。一方で、昨今では、これを妨害する機能を有するマルウェアが多数知られており、今現在、フォレンジックを実施する現場では、実際に使用している様々なメモリフォレンジックツールについて、その有効性に疑念がもたれている。本研究では、その疑念を払拭するために、様々なメモリフォレンジックツールについて、フォレンジック妨害機能動作時であっても正確にメモリから情報を抽出できるか否かを検証し、確認する。

キーワード：メモリフォレンジックツール，アンチフォレンジック、

Evaluation of the effectiveness of memory forensics tools under the influence of anti-forensic malwares

Ikuo Tanaka† Masaki Hashimoto†

Abstract: In recent years, there is a growing importance of digital forensic technologies to deal with cyber crimes in the criminal investigation agencies, after cyber crimes using information technologies have become more popular in the world. In particular, as the forensic targets, technologies to extract information accurately from volatile memories have become more critical in addition to the hard disk drives. Meanwhile, it is assumed by the criminal investigation agencies that most forensic tools are uncertain of effectiveness after recent malwares have anti-forensic capabilities popularly. In this paper, we report the results of evaluating popular memory forensic tools to clarify the uncertainness, by confirming the accuracy of extracting information from memories infected by anti-forensic malwares.

Keywords: memory forensics tools, anti-forensics

1. はじめに

我々の生活は、益々ICT に依存するようになっており、それに伴いサイバー犯罪の種類や発生件数が増加している。

発生したサイバー犯罪について、被害にあったコンピュータに残されている犯罪の痕跡に対し、適切に証拠保全を実施して原因を調査する作業がデジタルフォレンジックである。デジタルフォレンジックによる調査結果に基づいて、捜査機関が犯人検挙のための証拠として使用したり、同様な犯罪への予防策を検討する事ができるため、その役割は非常に重要である。

デジタルフォレンジックを実施するにあたり、調査対象のコンピュータを解析する上で、従来のディスクフォレンジックだけでなくメモリ上に存在するデータを取得する事を目的とするメモリフォレンジックの技術も欠かす事ができない状況である。とりわけ、調査対象のコンピュータ上でマルウェアの感染が疑われる場合、ディスク上に痕跡を残さないマルウェアが一般化している状況を鑑みてメモリ上のデータを取得する必要がある場合が多い。

メモリ上のデータを取得する場合には、様々なツールを使用する事になるが、一方で、近年、高機能化しているマルウェアの中には、予めフォレンジックが実行される事を想定し、メモリ上のデータ取得を妨害するといったアンチフォレンジック機能を有するマルウェアも存在する。そのため、捜査機関等の実際にデジタルフォレンジックを実施する現場では、利用しているフォレンジックツールのアンチフォレンジックマルウェアに対する有効性に疑念が生じている。

そこで、本研究では、現状一般的によく利用されているものと想定するいくつかのメモリフォレンジックツールについて、アンチフォレンジック技術への対策状況を検証する。具体的には、様々なアンチフォレンジックマルウェアの影響下にあるコンピュータで、それらのフォレンジック

† 情報セキュリティ大学院大学、IISEC

ツールが正しくメモリから情報を抽出できるか否かを検証する。これにより、前述した疑念を払拭するのが本研究の目的である。

以降、第 2 章から第 3 章では本研究の背景とデジタルフォレンジックに関する現状について述べる。その後、第 4 章でアンチフォレンジックへの対策状況に関する先行研究について述べ、第 5 章において今後の研究内容について述べ、本稿をまとめる。

2. 研究の背景

2.1 研究の必要性

デジタルフォレンジックにおいては、調査に際して、まず証拠保全が基本的な作業となる。

メモリフォレンジックにおいては、調査対象のコンピュータのメモリ上に存在するデータについて証拠保全を実施するには、ツールを調査対象のコンピュータ上で実行し、ツールが出力したメモリ上のデータが書き込まれているイメージファイルやダンプファイルを取得する事で可能になるため、正確な情報を保全する事ができるかどうかは、ツールの性能に関わっている。

メモリフォレンジックの実施にあたりどのツールが正確な情報を保全できるかどうかに関する具体的な資料が乏しく、また研究もほとんどなされていない状況から、現在、デジタルフォレンジックの現場において活用されているツールの有用性について検証する必要がある。

2.2 研究の目的

メモリフォレンジックを実施するにあたり、ツールの基本的な機能については保証されていると考えられるが、アンチフォレンジック技術への対応に関する機能については、スクリプトにアンチフォレンジック機能を擬似的に実装する事で、現在活用されているツールについてアンチフォレンジック技術への対応状況を検証している研究が一部存在するが、実際にマルウェアが感染し、動作している環境でツールを検証している研究や資料は、現在のところほぼ存在しない。

よって、実際にマルウェアが動作している環境で現在使用されているツールがどの程度、アンチフォレンジック技術に対応しているか可能な限り網羅的に検証する。

3. デジタルフォレンジック

3.1 デジタルフォレンジックにおける証拠保全の重要性

ICT に深く依存している現在の社会において、コンピュータを利用している際に発生した事故や犯罪が増加している状況があり、発生した事故や犯罪に関する証拠保全、調査、分析を実施するためにデジタルフォレンジックの必要性・有用性が益々高まっていると言える。

デジタルフォレンジックのプロセスの中で基本となるのは電磁的証拠の保全の手続きである。事故や犯罪といったインシデントに関わる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、確実にそのまま収集、取得、保存する事が重要である[3]。

証拠保全の手続きに不備があり、原本との同一性について疑義があると、分析結果の信頼性そのものがなくなってしまう事から、デジタルフォレンジックにおいて、証拠保全は最も基本的で重要な事項である。

3.2 デジタルフォレンジックの現状

デジタルフォレンジックにおいて、これまでは、証拠となる情報がハードディスク内に残されている事を前提として、調査対象のコンピュータについて電源が落ちている或いは電源を落とした状態にして、物理コピー等を実施する事によりディスクイメージを作成して証拠を保全し、従来のディスクフォレンジックによる不揮発性データを中心とした調査を実施する事が主流だった。現在でも事案内容によっては、有効な手法である。

しかし、年々、攻撃手法が高度化し、ハードディスク内に攻撃の痕跡を残していない事から、証拠保全として単にディスクイメージを作成し、ディスクイメージを調査するだけでは、インシデントの原因が判明しない事が多くなっている。

マルウェアの中には、メモリ上にしか痕跡を残さないものや、自身の存在を隠蔽する機能を持っているものがあり、揮発性データについても証拠保全を実施し、調査する事が求められている。

3.3 揮発性データの重要性

揮発性データには、調査対象のコンピュータにおける最新のシステム情報が存在しており、ディスクイメージからは取得できない。

調査対象に関する最新のシステム情報として、実行されているマルウェアの情報、暗号に使用する鍵情報、パスワード等の認証情報、ネットワーク情報、未だハードディスクに書き出されていないが書き込み予定の情報、実行されているプロセスの情報等を有しており、手順や方法を誤ってしまった場合、取得する事ができなくなるケースもある。

また、揮発性データには、揮発性の高さという情報の失われ易さを考慮し、証拠保全を実施しなければ適切に揮発性データを取得する事はできない。

揮発性の高さの順序は、RFC3277 の証拠保全とガイドライン[13]に揮発性の高さに関する目安が示されており、表 1 のとおりである。

揮発性 高	レジスタ、キャッシュ
	ルーティングテーブル、arp キャッシュ、プロセステーブル
	カーネル統計、メモリ
	テンポラリファイルシステム
	ディスク
	当該システムと関連する遠隔ロギング と監視データ
	物理的設定、ネットワークトポロジ
低	アーカイブ用メディア

表 1 揮発性の高さの順序

NIST SP800-86 インシデント対応へのフォレンジック技法の統合に関するガイド[9]において、揮発性データを収集する順番が表 2 のとおり示されている。

取得順序	揮発性データの内容
1	ネットワーク接続
2	ログインセッション
3	メモリの内容
4	実行中のプロセス
5	開かれているファイル
6	ネットワーク構成
7	オペレーティングシステム時間

表 2 揮発性データの収集順序

3.4 ライブフォレンジック

揮発性データについて証拠保全を実施する手法として、ライブフォレンジックがある。

これまで、インシデントレスポンスの中で、稼働中のシステムから必要な情報について証拠保全を実施するため、揮発性データと不揮発性データ共に取得するライブフォレンジックが使用されてきた。

ライブフォレンジックでは、ライブレスポンスとメモリフォレンジックという 2 つの手法に分ける事ができる。

3.5 ライブレスポンス

ライブレスポンスは、稼働中のコンピュータに対してコンソールにアクセスしてコマンドやツールを実行する事により、稼働中のシステム上で証拠保全を実施する手法であり、主にメモリ上に展開されているカーネル、プロセス、ファイル、レジストリ、ネットワーク接続情報等の稼働中システムの最新情報を対象する。

また、暗号化されているハードディスクに対して、稼働中にディスクイメージの作成を行うといった不揮発性データの証拠保全も実施する。

3.6 メモリフォレンジック

メモリフォレンジックでも、ライブフォレンジックと同様に稼働中のコンピュータから証拠保全を実施するが、稼働中のコンピュータのメモリ上のデータに対してツールを実行する事でイメージファイルやダンプファイルを出力し、証拠保全を実施する。不揮発性データの取得は行わない。

3.7 ラブレスポンスとメモリフォレンジックの関係

揮発性データを取得する際のライブレスポンスとメモリフォレンジックの特徴と相違点は、表 3、4 に示す内容が挙げられる。

取得、解析方法	情報収集、解析に OS 標準のコマンドが利用できる。 緊急対応等で柔軟に対応できる。
難易度	臨機応変な対応が必要になり、高度な知識が必要
対象端末から 受ける影響	調査対象となるコンピュータがマルウェア等に感染していた場合、調査の際、プロセスの隠蔽といった影響を受け易い
取得範囲	既に解放されているメモリ領域の調査は不可能
再現性	調査において、後日の再現は困難

表 3 ライブレスポンスの特徴

取得、解析方法	ダンプファイルの取得、解析には専用のツールを使用する
難易度	ツールの使用手順を決めておけば、ダンプファイルの取得は、高度な知識を有しない者でも可能。
対象端末から 受ける影響	ダンプファイルの取得時に、マルウェアや rootkit によりプロセスの隠蔽等の影響を受ける可能性はあるが、解析は解析用の他のコンピュータで実施するため、解析時の影響は受けない。
取得範囲	ダンプファイルを解析する事で、解放済みのメモリ領域を調査する事ができる
再現性	一度、ダンプファイルを取得しているので、解析は繰り返し実施できる。

表 4 メモリフォレンジックの特徴

ライブフォレンジックを実施する中で、従来、ライブレスポンスが実施されてきた。ライブレスポンスは、調査対象のコンピュータ上で多数のコマンドを直接実行するため、調査対象のコンピュータへ影響を与えてしまうという事や調査を実施する上で再現性が低いというデメリットがあったが、解析技術の向上によりメモリフォレンジックがライブレスポンスを補完する形で発展し、双方を併用する事で適切な証拠保全を実施する事ができる。

しかし、メモリフォレンジックについても適切な機能を

有しているツールでなければ、適切な証拠保全を実施する事はできない。

4. アンチフォレンジック

デジタルフォレンジックの作業を妨害する技術は、以前から存在している。

デジタルフォレンジックの作業を妨害するアンチフォレンジックと呼ばれる技術は、フォレンジックの作業プロセスにおける証拠の可用性や有益性を損なうための試みである。

アンチフォレンジックに関する技術は、暗号化に関する技術、ステガノグラフィに関する技術、ネットワーク通信に関する技術、データ隠蔽に関するする技術、データの痕跡を消去する技術等、いくつかの種類別に分類する事ができツールとして配布されている[14]。

また、アンチフォレンジック技術を有しているルートキットをマルウェアの一部として動作させる事により、感染したコンピュータ上でマルウェアの存在を隠蔽する事にも使用されている。

マルウェアの一部として動作するルートキットは、0S の機能を使用してマルウェアの存在を隠蔽したり、調査のためのデータ取得そのものを妨害するため、マルウェアの感染が疑われるコンピュータに対してデジタルフォレンジックを実施する際、証拠保全が正しくできないため、調査自体を実施する事が困難になる。

4.1 アンチフォレンジック対策の先行研究

アンチフォレンジック対策に関する先行研究として、Stüttgen.J、Cohen.M らの”Anti-forensic resilient memory acquisition”[6]がある。

この研究は、メモリフォレンジックを実施する際、ルートキットが動作しているコンピュータ上では、ルートキットは OS が管理している仮想アドレス空間の情報をフックする事から、OS が提供する機能を通じて仮想アドレス空間の情報を得るのではなく、独自に作成したドライバを使用する事で独自のカーネル空間を確保し、この領域内に独自のページテーブルエントリを作って、物理メモリの情報を取得し、ルートキットの影響を回避する手法について提案している。

この研究を実施するにあたり、既存の主要メモリフォレンジックツールがアンチフォレンジック機能にどの程度影響を受けるのかという事について検証している。

4.2 メモリフォレンジックツールの検証実験

Stüttgen.J らの論文中で述べられている既存のメモリフォレンジックの検証実験は、Windows 環境において実際にマルウェアを使用するのではなく、アンチフォレンジック機能を有する Python で実装されたスクリプトを使用する事で、擬似的に実施している。

擬似的に使用しているアンチフォレンジック機能は、メモリ上にある Windows のカーネル構造体である KDBG 構造体に不正な値を上書きし、ほとんどのメモリフォレンジックツールがメモリ情報を取得する際に利用する API から不正な値を返すようにする事で、ツールによるメモリ情報の取得を妨害するという機能である。

表 5 の示したものが、メモリフォレンジックツールで使用される事が多い Windows の API である。

API	機能
ZwMapViewOfSection	プロセスに関して仮想アドレス空間においてマップされたものを返す
MmMapIOSpace	デバイスの仮想アドレスを提供し、カーネルアドレス空間の中の物理アドレス範囲をマップする
MmMapMemoryDumpMdl	ドキュメント化されていない API で、MmMapIOSpace と同様の機能を持つと思われ、クラッシュダンプをハンドリングするのにも使用されている
MmGetPhysicalMemoryRanges	有効な物理アドレスの範囲のリストを返すメモリフォレンジックツールで使用される事が多い

表 5 メモリフォレンジックツールで利用される事が多い Windows API

表 5 の API のうち、ZwMapViewOfSection、MmMapIOSpace の２つの API は Windows において、他の複数のドライバで使用されおり、呼び出しの際にフックすると Windows 自体が不安定になってハングアップしたり、リブートしてしまうため、Stüttgen.J らの検証では、MmMapMemoryDumpMdl と MmGetPhysicalMemoryRanges の呼び出しのみをフックし、加えて、KDBG を上書きして不正な値を設定する様に実装し、メモリフォレンジックツールの検証を実施した。

4.3 メモリフォレンジックツールの検証結果

擬似的なアンチフォレンジック機能が実装された環境で実施したメモリフォレンジックツールの検証について、使用したツールの種類と結果は表 6、7 の通りである。

Acquisition tool	Version	Format	KDBG	API (1)	API (2)
Memoryze	2.0	raw	PASS	FAIL	PASS
FTK Imager	3.1.2	raw	PASS	FAIL	PASS
Win64dd	1.4.0	raw	FAIL	FAIL	FAIL
Win64dd	1.4.0	dmp	FAIL	FAIL	FAIL
DumpIt	1.4.0	raw	PASS	FAIL	FAIL
WinPmem	1.3.1	raw	FAIL	FAIL	PASS
WinPmem	1.3.1	dmp	FAIL	FAIL	PASS
WindowsMemoryReader	1.0	raw	PASS	FAIL	PASS
WindowsMemoryReader	1.0	dmp	PASS	FAIL	PASS

表 6 検証したメモリフォレンジックツールの種類と結果
※出力ファイル形式別に結果を記載

ツール	検証結果
Memoryze	KDBG の影響は受けない。 MmMapIOSpace がフックされる影響はなかった。 MmGetPhysicalMemoryRanges のフックで、カーネルをクラッシュし、リブートした。
FTK Imager	ZwMapViewOfSectionI で情報を取得しているため、KDBG の影響や MmMapMemoryDumpMdl のフッキングは影響なかった。 MmGetPhysicalMemoryRanges がフッキングされる事により、空のイメージファイルが出力された。
Win64dd	KDBG の影響でリブートしてしまった。 不完全なダンプが作成された。 MmGetPhysicalMemoryRanges または、 MmMapMemoryDumpMdl を フックでもリブート等が発生。
DumpIt	KDBG の影響を受けている。 MmGetPhysicalMemoryRanges、MmMapMemoryDumpMdl のフックに よりイメージファイルの作成に失敗した。
WinPmem	KDBG の影響により、ダンプやイメージファイルの作成に失敗した。カーネルをクラッシュは、発生しなかった。 MmGetPhysicalMemoryRanges をフックすると、エラーで終了した。MmMapMemoryDumpMdl のフックは、影響はなかった。
WindowsMemoryReader	KDBG の影響はなかった。 MmMapMemoryDumpMdl のフック事は、 WindowsMemoryReader で使用されていない API なので特に影響はなかった。 MmGetPhysicalMemoryRanges のフックは、イメージファイルとダンプの出力の両方が完全に無効になり、カーネルをクラッシュさせる事でドライバのエラーを起こしてリブートした。 ダンプやイメージファイルが不正な内容で、解析できない。

※API(1)は、MmGetPhysicalMemoryRanges

※API(2)は、MmMapMemoryDumpMdl

表 7 検証結果の詳細

結果のとおり、検証したほぼ全てのツールでは、正常にメモリの情報を取得できていない事がわかる。

擬似的に実装された環境とはいえ、Stüttgen.J らが行った検証で、既存のメモリフォレンジックツールのアンチフォレンジック対策状況について、ある程度は確認する事ができる。

しかし、2013 年に実施された検証であり、検証に使用したメモリフォレンジックツールについて最新のバージョンで検証された資料は、現時点では確認できていない。

5. マルウェアを使用したツールの検証

本稿でこれまで述べてきたとおり、デジタルフォレンジックにおいて最初に実施する証拠保全の作業が非常に重要であり、証拠保全が適切にできなければ、デジタルフォレンジックによる調査自体の価値がなくなってしまう。

近年注目されているメモリフォレンジックにおいては、ツールが適切にメモリの情報を抽出する事を前提としており、ツールの機能がフォレンジックによる調査そのものの価値を決める事になるため、ツールを使用する際の目安となるものが必要である。

よって、既存の最新のメモリフォレンジックツールがどの程度、進歩しているアンチフォレンジック技術に対応しているのか、実際にマルウェアが動作している環境において検証する。

5.1 検証に使用するメモリフォレンジックツール

検証に使用するメモリフォレンジックツールは表 8 に示すツールを検討している。

ツール名	ベンダ
FTKimager	Access Data
Magnetic RAM Capture	Magnet Forensics
WinPmem	Google
HBGary Responder	CounterTack
Moonsols Windows Memory Toolkit DumpIt	MoonSols
EnCase Forensics Imager	Guidance Software

表 8 検証に使用するメモリフォレンジックツール

検証の対象とするメモリフォレンジックツールの選定基準はデジタルフォレンジック研究会の証拠保全ガイドライン第 5 版に示されているツールや、先行研究の論文内で記載されているツール、業務で一般的使用されているツールのうち、実際のデジタルフォレンジックを行う現場を想定し、スタンドアロンで動作するものを選定している。

また、有償のものと無償のもの両方についてツールを選定している。

5.2 検証に使用するマルウェア

検証する際に使用するマルウェアは、カーネルモードで動作する rootkit 機能を有するマルウェアを検討しているが、本研究においては OS がブートされるところまでは信頼できるものとし、MBR を書き換えるブートキットは対象とせず、rootkit 機能を有するマルウェアを使用する。

5.3 検証環境、検証基準

本研究の対象とする検証環境は、Windows7 及び Windows 8 で 32 ビット、64 ビットそれぞれの環境で実施する。

Windows 環境で実施するのは、ルートキット機能を有するマルウェアの数が、現状では Windows 環境のものが多い事や、Windows 環境での被害が多いために研究の対象とした。

検証については、正常時に取得したダンプファイルやイメージファイルの内容に含まれている情報を基準とし、容量、ファイル内に含まれているカーネルモジュール、ドライバー、プロセスの各一覧、プロセスの詳細情報等を正常時に取得したものと、マルウェアが動作している環境で取得したものを比較して差異を確認し、マルウェア自身の情

報が隠蔽されていない内容であればツールが適切に情報を取得できた事がわかると考えている。

6. おわりに

本研究は検討段階であり、これから実施する研究である。

本研究を実施する事により、メモリフォレンジックツールに関するアンチフォレンジック技術の対応状況を公開する事にもなるが、デジタルフォレンジックを実施する現場において作業上の一助となる事を期待する。

参考文献

[1] 羽室英太郎、國浦淳: デジタル・フォレンジック概論～フォレンジックの基礎と活用ガイド～、東京法令出版(2015)

[2] 特定非営利活動法人デジタル・フォレンジック研究会(編): 佐々木良一、舟橋信、安冨潔: 改訂版デジタル・フォレンジック辞典、日科技連出版社(2014)

[3] デジタル・フォレンジック研究会、証拠保全ガイドライン第 5 版、デジタルフォレンジック研究会(オンライン)、入手先〈https://digitalforensic.jp/wp-content/uploads/2016/07/idf-guideline-5-20160421.pdf〉

[4] 今野直樹、田中英彦: ライブフォレンジックにおける有効性の検討及び具体的実施手法の提案、第 14 回情報科学技術フォーラム, No.4, pp.205-212(2015)

[5] 野上紘、田中英彦、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

[6] Stüttgen, J., & Cohen, M.: “Anti-forensic resilient memory acquisition”、Digital Investigation: The International Journal of Digital Forensics & Incident Response, Volume 10, August, 2013

[7] Igor Korkin, Ivan Nesterov “APPLYING MEMORY FORENSICS TO ROOTKIT DETECTION“, Proceedings of the Conference on Digital Forensics, Security and Law (2014)

[8] Florio E, “When malware meets rootkits “, トレンドマイクロ株式会社: 入手〈https://www.symantec.com/avcenter/reference/when.malware.meets.rootkits.pdf〉

[9] NIST: pecial Publication 800-86 Guide to Integrating Forensic Techniques into Incident Response, NIST(onlie), available from〈http://csrc.nist.gov/publications/nistpubs/800-86/SP800-86.pdf〉

[10] NIST: Special Publication 800-60 Revision 1 Guide for Mapping Types of Information and Information Systems to Security Categories, NIST(online),available from〈http://nvlpubs.nist.gov/nistpubs/Legacy/SP/nistspecialpublication800-60v1r1.pdf〉

[11] Mark E. Russinovich, David A. Solomon, Alex Ionescu, 訳者 株式会社クイーブ: インサイド Windows 第 6 版 上 日経 BP 社(2013)

[12] Mark E. Russinovich, David A. Solomon, Alex Ionescu, 訳者 株式会社クイーブ: インサイド Windows 第 6 版 下 日経 BP 社(2013)

[13] 独立行政法人情報処理推進機構, “RFC3227 証拠収集とアーカイビングのためのガイドライン(Guidelines for Evidence Collection and Archiving)” （オンライン）, 入手先〈https://www.ipa.go.jp/security/rfc/RFC3227JA.html〉

[14] 浦野晃、橋本正樹、辻秀典、田中英彦: アンチフォレンジックの痕跡検出手法に関する初期的検討、コンピュータセキュリティシンポジウム 2013 論文集 2013.4（2013）: 163-168