

Álvaro Vilobaldo Rios da Silva

Antiforense com uso de rootkits

São Paulo

2013

Álvaro Vilobaldo Rios da Silva

Antiforense com uso de rootkits

Monografia de Conclusão de Curso apresentada à Universidade Presbiteriana Mackenzie de São Paulo como requisito parcial à obtenção do título de Especialista em Computação Forense do Curso Lato Sensu em Computação Forense

Orientador:
Ivete Irene dos Santos

UNIVERSIDADE PRESBITERIANA MACKENZIE

São Paulo

2013

Monografia sob o título Antiforense com uso de rootkits, desenvolvida por Álvaro Vilo-
baldo Rios da Silva, e aprovada em 6 de abril de 2013, São Paulo capital, pela banca constituída
por:

Ivete Irene dos Santos
Orientadora

Ana Cristina Azevedo
Orientadora

Epígrafe

“Se você conhecer o inimigo e a si mesmo, não precisa temer o resultado de uma centena batalhas. Se você se conhecer a si mesmo, mas não o inimigo, para cada vitória você também sofrerá uma derrota. Se você não conhecer nem o inimigo, nem a si mesmo, você sucumbirá em todas as batalhas.” (TZU, IV a.C)

Resumo

Esta monografia é um estudo sobre antforense com utilização de rootkits visando mostrar como funciona um rootkit e como ele pode ser usado na antforense. Definições de antforense e rootkits com suas práticas comuns e respectivos históricos junto com algumas técnicas de subversão demonstrarão que o uso combinado de técnicas antforenses incorporadas a rootkits cria mecanismos de destruição de provas de forma sistemática e eficiente.

Palavras-chave: antforense, rootkit, forense, provas, evidências.

Abstract

Write here the English version of your 'Resumo'...

keywords:

Lista de Figuras

4.1	Hexadecimal da Microsoft Calculator v. 5.1 visto no WinHex 16.3 SR-2 . . .	p. 24
4.2	Arquivo com MAC time original (ACKERMAN, 2007a)	p. 25
4.3	Utilização do timestomp (ACKERMAN, 2007b)	p. 26

Lista de Tabelas

Sumário

Introdução	p. 10
0.1 Tema	p. 10
0.2 Hipótese(s)	p. 10
0.3 Metodologia	p. 11
0.4 Justificativa	p. 11
0.5 O Problema de Pesquisa	p. 12
0.6 Objetivos	p. 12
0.6.1 Objetivo Geral	p. 12
0.6.2 Objetivo Específico	p. 13
0.7 Delimitações do Estudo	p. 13
0.8 descricao dos capitulos	p. 13
 1 Forense Computacional	 p. 14
 2 Antiforense Computacional	 p. 16
 3 Rootkits	 p. 17
 4 Antiforense com Rootkits	 p. 20
4.1 Cópia forense do HDD	p. 21
4.2 Recuperar arquivos	p. 23
4.3 Coletar metadados dos arquivos	p. 24
4.4 Retirar arquivos conhecidos	p. 25

4.5	Análise estática dos executáveis suspeitos desconhecidos	p. 26
4.6	Análise dinâmica dos executáveis suspeitos	p. 27
4.7	outro	p. 27

Referências Bibliográficas	p. 28
-----------------------------------	-------

Introdução

A monografia apresenta uma incursão na antforense focada na utilização de rootkits em ambientes Microsoft principalmente Windows, visando mostrar seu funcionamento, as práticas mais comuns e como o rootkit pode ser usado na antforense.

O rootkit é em geral utilizado por atacantes avançados com fins maliciosos e oferece grande obstáculo para ser detectado, pois seu uso força o perito a ter um conhecimento amplo além de usar técnicas sofisticadas. Entender o seu funcionamento é determinante para uma perícia bem sucedida. Para desenvolver esse tema foi utilizada vasta bibliografia, exemplos práticos e aplicações de rootkits comuns.

Ao longo dos capítulos são desenvolvidos os conhecimentos para o entendimento do tema proposto, onde cada um foi dividido em um assunto específico. No primeiro capítulo será mostrado uma visão ampla do que é a ciência forense e como ela é aplicada na computação. No segundo capítulo são apresentados conceitos de antforense e os tipos de antforense. Por fim no terceiro capítulo conduz a uma visão do funcionamento de um rootkit e algumas técnicas para subverter os sistema.

0.1 Tema

Antforense em Windows 7 com uso de rootkits.

0.2 Hipótese(s)

Técnicas podem ser usadas para ocultar processos ou ações? Rootkits e bombas lógicas são exemplos de como um usuário avançado pode disfarçar, dificultar ou impossibilitar a ação de um perito forense na obtenção de provas.

0.3 Metodologia

0.4 Justificativa

Por que invadir um país armado arriscando vidas de centenas se você pode destruir centrífugas de enriquecimento de urânio de forma sigilosa do outro lado do planeta? Conforme o mundo se digitalizou se digitalizaram-se também as suas ameaças, onde antes se podia ver mesmo que por instantes mísseis ou bombas sendo lançada hoje temos inúmeras ameaças invisíveis que podem causar tanto estrago quanto, contudo pelo princípio de Locard o problema dessas ameaças invisíveis é que elas podem não ser tão invisíveis assim, levando a procura de métodos antifo-forenses mais eficazes.

O perito deve estar preparado para a ação de um usuário avançado que conheça bem o sistema operacional atacado, comprometido ou usado. Mesmo que não seja algo corriqueiro na rotina da grande maioria dos profissionais, encontrar um atacante de alto nível trará novos desafios e obstáculos tão poucos corriqueiros. Saber como dificultar ou impossibilitar o trabalho do perito é como ele poderá evitar a armadilha de achar que no corpo (corpo de delito) investigado não existe nada.

Sendo assim, esse trabalho poderá ajudar a traçar um processo bem elaborado de trabalho que seja rápida e eficiente sem deixar brechas que permitam ou ajudem ações antifo-forenses. Com um processo bem definido o perito tende a diminuir o tempo de análise e um melhor aproveitamento das mesmas. Provendo mais qualidade com mais precisão.

Durante a perícia o perito pode se deparar com um atacante avançado que utiliza técnicas bem sofisticadas para esconder ou destruir evidências impossibilitando ou dificultando a obtenção de provas e comprometendo a qualidade das mesmas quando são obtidas. Para tal feito o atacante pode se valer de rootkits.

Ao estudar o comportamento dos rootkits e entender como ele pode ser usado na antifo-forense, permite ao perito lidar corretamente com rootkits, como por exemplo, desenvolvendo rotinas.

O perito deve estar preparado para a ação de um usuário avançado que conheça bem o sistema operacional atacado, comprometido ou usado. Mesmo que não seja algo corriqueiro na rotina da grande maioria dos profissionais, encontrar um atacante de alto nível trará novos desafios e obstáculos tão poucos corriqueiros. Saber como dificultar ou impossibilitar o trabalho do perito é como ele poderá evitar a armadilha de achar que no corpo (corpo de delito) investigado não existe nada.

Por que invadir um país armado botando vidas de centenas em risco se você pode destruir centrífugas de enriquecimento de urânio de forma sigilosa do outro lado do planeta? Conforme o mundo se digitalizou se digitalizaram-se também as suas ameaças, onde antes se podia ver mesmo que por instantes mísseis ou bombas sendo lançada hoje temos inúmeras ameaças invisíveis que podem causar tanto estrago quanto, contudo pelo princípio de Locard o problema dessas ameaças invisíveis é que elas podem não ser tão invisíveis assim, levando a procura de métodos antifofoense mais eficazes.

Sun Tzu (544 a.C. - 456 a.C.) há mais ou menos 500 anos de cristo já dizia que se conhecer a si mesmo e ao adversário não temerá o resultado de mil batalhas.

Conhecendo como essas técnicas podem ser usadas o perito pode se precaver e saber agir no momento de detectar o uso dos mesmos. O perito deve tomar alguns cuidados na análise de computadores, pois o mesmo pode ter sido usado por um usuário avançado o que muda razoavelmente a sua abordagem.

0.5 O Problema de Pesquisa

Técnicas podem ser usadas para ocultar processos ou ações. Como um rootkit funciona e como ele pode ser usado para antifofoense?

Pode ajudar a traçar um processo bem elaborado de trabalho que seja rápida e eficiente sem deixar brechas que permitam ou ajudem ações antifofoenses. Com um processo bem definido o perito tende a diminuir o tempo de análise e um melhor aproveitamento das mesmas. Provendo mais qualidade e mais precisam nas futuras análises.

0.6 Objetivos

Pode esclarecer diversos tópicos obscuros a respeito do que pode ser encontrado em investigações forenses quando o perito se ve de frente com ameaças persistentes e elaboradas, ou seja, ajuda a resolver casos onde existiu antifofoense.

0.6.1 Objetivo Geral

Apresentar o funcionamento de rootkits voltados para antifofoense.

0.6.2 Objetivo Específico

Apresentar o que é ciência forense, para que serve a ciência forense, o que é computação forense e citar a legislação que garante a existência do perito no Brasil; Mostrar o que é antifo-
rense computacional, categorizar os tipos de antifo-
rense computacional e descrever os tipos de
computação forense; e Expor o que é um rootkit, como ele funciona e como ele pode impedir a
formação de provas.

0.7 Delimitações do Estudo

Análise de rootkits em ambientes Windows 7 voltados para restringir ou destruir provas.

0.8 descricao dos capitulos

1 *Forense Computacional*

A humanidade sempre teve assuntos divergentes, onde em outrora esses assuntos eram resolvidos com o mais forte ou hauto sobrepujando a vontade doutro, com o advento da civilização se convencionou o uso de um mediador que em teoria deve ser alguém neutro.

Quando trata-se de assuntos de disputa de interesse, espera-se que o mediador busque e chegue o mais próximo possível da verdade antes de tomar uma decisão. Hoje é dado esse poder de mediação ao juiz, contudo em diversos conflitos se faz necessário conhecimentos técnicos específicos. Nesses casos ele é auxiliado por um especialista ou perito no assunto técnico em discussão. Para tal, esse especialista utiliza-se da ciência forense para trazer luz os fatos respaldando a decisão do juiz sobre o assunto.

Segundo Houaiss e Villar (2009) ciência é um “corpo de conhecimentos sistematizados adquiridos via observação, identificação, pesquisa e explicação de determinadas categorias de fenômenos e fatos, e formulados metódica e racionalmente.” e forense é “relativo aos tribunais e à justiça”. Logo as ciências forenses é a utilização da ciência “à análise de vestígios, no intuito de responder às demandas judiciais” (VELHO; GEISER; ESPINDURA, 2012, p. -3).

De certo a área médica foi a primeira a ser requisitada em tribunais construindo técnicas que levaram ao desenvolvimento ao longo dos anos da medicina legal. No Império Romano médicos eram chamados para lucidar mortes diz França (2008), outro exemplo histórico da importância do parecer técnico pode ser visto no *Código Criminal Carolino* feito em 1532 por Carlos Magno que definia a análise médica em determinados crimes.

Com o avanço da tecnologia e o valor da perspectiva especializada, foi natural que outras áreas também fossem utilizadas no foro. A computação forense, apesar da tecnologia e inovação inatas, conceitualmente ainda se propõe a grosso modo a usar a ciência para mostrar fatos demandados judicialmente, como podemos ver em Machado e Eleutério (2011), “[...] computação forense tem como objetivo principal determinar a dinâmica, a materialidade e autoria de ilícitos ligados à área da informática, tendo como questão principal a identificação e o processamento de evidências digitais em provas materiais [...], por métodos técnicos-científicos, conferindo-

lhes validade probatória em juízo.”.

2 *Antiforeense Computacional*

Harris (2006) define antiforeense como método para prevenir ou agir contra a ciência usada a favor das leis civis e criminais que são aplicadas por órgãos como a polícia. Berinato (2007), amplia essa ideia mostrando que é mais que uma técnica usada, é uma abordagem crimosa. Assim todas as tentativas de afetar negativamente a existência, quantidade e / ou qualidade da evidência de uma cena de crime, ou fazer a análise e exame das provas difíceis ou impossíveis de realizar, para Rogers (2005) será considerada antiforeense. Dessa forma concluímos resumidamente que a antiforeense computacional pode ser definida como qualquer ação praticada para obstruir, dificultar ou destruir evidências ou provas no âmbito computacional.

Dentre as modalidades de antiforeense computacional, Blunden (2009a) as categoriza em cinco grandes grupos, sendo eles: destruição de dados, ocultação de dados, corrupção de dados, fabricação de dados e eliminação da fonte de dados.

3 *Rootkits*

Malware é a junção das palavras em inglês *malicious* e *software*, termos em inglês que pode ser traduzido livremente como aplicativo malicioso. Dessa forma podemos considerar como malware os vírus, worms, trojans, botnets kit dentro outros, contudo o inverso não é valido, ou seja, todo vírus é um malware, mas nem todo malware é um vírus.

Os vírus e worms são feitos para se espalha a diferença está em como eles se espalham. O vírus precisa ser ativado ou executado pelo usuário e em geral fica atrelado a algum executavel que pode ser ou não um programa legitimo subvertido (LUDWIG, 1995), ao contrário do worm que não precisam da ação direta do usuário para se espalhar e permanece apenas na memória (MCAFEE, 2013).

Uma *botnet* é uma rede de computadores controlados por cybercriminosos(KASPERSKY, 2013). Basicamente quando um computador é infectado pelo agente da *botnet* o mesmo se torna parte da rede e é controlado pelo dono da botnet.

No universo *UNIX*¹ ou *UNIX-like*² a conta de usuário com menor restrição de segurança é referênciada como conta *root* sendo que em alguns sistemas o nome de usuário é literalmente root, mas isso é apenas uma convenção histórica do que uma imposição (BLUNDEN, 2009b). Enquanto *kit* significa conjunto de peças (SANTOS, 2000).

Rootkit pode ser visto como um “kit” composto de pequenos programas úteis por exemplo, binários, scripts, arquivos de configuração que permitem a um atacante manter o acesso “root”. Em outras palavras, um rootkit é um conjunto de programas e de código, que permite a presença permanente ou consistente, não detectável em um computador (HOGLUND; BUTLER, 2005).

Essa coleção de ferramentas que permitem aos invasores ocultarem suas atividades em um computador, de modo que eles podem secretamente monitorar e controlar o sistema por um período prolongado, ou seja, existem três serviços que o são inerentes dos rootkits, ocultação,

¹Um sistema operacional multiusuário amplamente utilizado.

²Sistemas Operacionais baseados no Unix, como o GNU/Linux

comando e controle (C2) e vigilância (BLUNDEN, 2009b). Ocultação, o rootkit deve passar despercebido, sem que o usuário e/ou antivírus o detecte; vigilância ou monitoramento basicamente consiste em acompanhar as ações do usuário, o rootkit tem que ser capaz de saber o que o usuário está fazendo; e comando e controle, permite ao dono do rootkit o controle remoto sobre o mesmo, definindo suas ações e direcionando. Desses três serviços o mais importante para o rootkit é a furtividade, pois um rootkit detectável vai durar muito pouco.

Como pode ser visto cada um desses agentes subversivos tem definições e características próprias diferentes e uma em comum todos eles subvertem o sistema de alguma forma, contudo é bom resaltar que nem todo rootkit é um malware, pois existem aplicações legítimas para o mesmo, como de computadores corporativos e inclusive aplicações investigativas.

Os primeiros rootkits apareceram em de 20 anos atrás no fim dos anos 80 e início dos 90, quando alguns foram percebidos comportamentos anormais em computadores como espaço em disco utilizado sem identificação, conexões de rede não-listadas e uso anormal do CPU (ROSANES, 2011).

Basicamente o processador pode receber dois tipos de exceções, uma gerada por hardware chamada de externa e interrupções geradas por programas (INTEL, 2011, p. 6-2 Vol. 3A). A grosso modo, quando uma interrupção ou exceção ocorre o processador usa o endereço de memória armazenado no índice correspondente a interrupção lançada que por definição aponta para uma *procedure* que trata a interrupção (INTEL, 1986), ou seja, esse endereço na memória vai direcionar o processamento a *procedure* específica para a interrupção ou exceção que ocorreu. O rootkit pode interceptar uma chamada a tabela estrutura de dados com índices dessas tratativas como *Interrupt Vector (IVT)* em modo real ou a *Interrupt Descriptor Table (IDT)* em modo protegido, ambas as estruturas possuem funções similares, apesar da forma como trabalham ser muito distinta.

tipos de rootkit <http://www.terena.org/activities/tf-csirt/meeting27/oesterberg-rootkits.pdf>

falando assim parece uma tarefa fácil realizar qualquer um desses metodos...

Jamie Butler, the creator of the FU rootkit

O uso de rootkits é limitado a usuários avançados sendo que seu desenvolvimento exige conhecimentos profundos tanto de arquitetura de computadores quanto do funcionamento do Sistema Operacional que o mesmo vai corromper.

Rootkits proporcionam uma grande variedades de opções e pode ser utilizado para quase tudo,

vem sendo utilizado historicamente para subverter sistemas dando permissão

O fato de alguns eventos e rootkits terem ficados famosos, como é o caso do stuxnet(), torna esse assunto muito interessante de ser abordado, porque

A grosso modo rootkits sempre tentarão esconder sua presença e seus rastros, logo a anti-forense desde o início já é parte ...

não são novidades e sua aplicação já não é

e durante o avanço do trabalho, poderão ser notadas diversas formas de detecção de rootkits além de indícios de seu uso em análises.

4 *Antiforeense com Rootkits*

Quando o perito vai realizar a coleta do material para a análise, ele pode encontrar dois cenários o corpo de delito que na ciência forense computacional quase sempre consiste em computadores, pode estar ligado ou desligado. Quando o mesmo está ligado é possível realizar a análise viva, entretando a análise *live* de um ambiente com rootkit pode gerar dados falsos ou imprecisos.

Análise *live* ou análise viva, consiste em uma análise focada em extrair e examinar dados volatéis (MCDOUGAL, 2006), esses dados volatéis são perdidos ao desligar o computador, como por exemplo, o conteúdo de registradores do processador, dados na *cache*, dados na memória etc. Essa abordagem possui diversas vantagens entre elas estão extração de dados voláteis como já citado, triagem de equipamentos, triagem de dados, preservação de dados criptografado e a possibilidade de estabelecer flagrante (MESQUITA; HOELS; RALHA, 2011).

É importante ressaltar que toda ferramenta ou *hardware* utilizado para a coleta de dados em equipamentos que ainda estão em execução, vai depender de dados fornecidos pelo equipamento periciado, ou seja, em algum momento essas ferramentas forenses vão requisitar dados de um sistema comprometido e passível de alguma interceptação mesmo quando a solução utilizada para coleta é um hardware (RUTKOWSKA, 2007). Logo em um ambiente dominado por um rootkit não é um ambiente confiável, pois ele pode interceptar e alterar chamadas das ferramentas de análise, impossibilitando uma coleta real e fiel.

A metodologia empregada na análise de um ambiente supostamente com um rootkit varia muito, mas em termos gerais a análise *Post mortem* é menos arriscada e indicada para casos de rootkits. As medidas antiforeense que podem ser tomadas pelo rootkit dependem do ambiente de execução e engloba também a equipe que o administra. No melhor dos cenários para o atacante é quando o sistema é administrado por leigos, não capacitados, sobrecarregados e/ou os sistemas não são atualizados com frequência tornando mais fácil para o rootkit esconder-se exigindo menos do atacante. No pior dos cenários o administradores são altamente qualificados, realizam rotinas frequentes, esta sempre atualizado e é auditorado (BLUNDEN, 2009a). Entender isso

pode indicar ao perito o quão complexo o rootkit é, pois quanto mais próximo do pior cenário mais avançado tem que ser o rootkit o que pode caracterizar um *Advanced persistent threat* (APT) ou ameaça avançada e persistente, ou seja, o ataque utilizando o rootkit foi orquestrado e planejado apenas para esse alvo específico.

Não existe técnica 100% antioforense, então o objetivo do atacante é tornar a análise cansativa para induzir ao erro podendo adicionar inclusive falsos rootkits ou malwares para despistar, iludir ou levar a conclusões precipitadas. Em (BLUNDEN, 2009a) são mostrados passos para a análise *Post mortem* onde se suspeita de rootkit:

- Clone do *hard disk drive* (HDD);
- Recuperar arquivos;
- Coletar metadados dos arquivos;
- Retirar arquivos conhecidos;
- Análise estática dos executáveis suspeitos desconhecidos; e
- Análise dinâmica dos executáveis suspeitos.

Esses passos pode ser vistos como filtros, onde cada passo retira cada vez mais ruído, eliminando em cada etapa arquivos superfúos. A seguir serão descritos cada um dos passos e alguns dos problemas que o mesmo pode gerar.

4.1 Cópia forense do HDD

A primeira fase e mais importante é a coleta, que nesse caso é clone do HDD. O clone do HDD, pode ser feito com software, como o dd¹ ou por hardware específico para clonagem de HDDs. Por via de regra essas ferramentas são homologados por órgãos como *National Institute of Standards and Technology* (NIST) que atestam a qualidade e eficácia dessas ferramentas em produzir cópias fidedignas que podem ser usadas em disputas legais como evidências. Basicamente todas essas ferramentas fazem cópias de setor por setor de todo o disco, para que o perito possa trabalhar nessa cópia preservando o HDD original. Essas cópias já foram exaustivamente usadas em tribunais e são muito úteis e indispensáveis para a análise do perito. Hoje sua eficácia não é questionada, pois essa cópia ou clone tem os dados idênticos ao do HDD objeto de análise

¹<http://pubs.opengroup.org/onlinepubs/9699919799/utilities/dd.html>

e essa igualdade pode ser atestada com *checksums* como os algoritmo de *hash MD5* ou *SHA1* (MULVEY, 2007). Essa abordagem pode ter alguns empecilhos e o rootkit pode não vir a ser clonado junto com os dados do HDD.

Primeiro e mais óbvio é que o rootkit pode nem estar no disco clonado, como estar somente na memória ou ser alocado em um outro dispositivo. O rootkit poder ser projetado para ficar somente na memória, entretando isso pode impedir que o mesmo persista já que é apagado sempre que o computador desliga (MEDINA, 2009). Contudo o mesmo esteja num parque de máquinas que permita infectar o computador toda vez que este for iniciada, como em grandes *data centers* em geral nunca tem todas as máquinas desligadas o rootkit pode ficar vivo na rede e persistir infectando novamente as máquinas assim que elas iniciarem.

Num *Personal Computer (PC)* durante o *boot* ele inicia o *Basic Input/Output System (BIOS)* fornece suporte básico para os principais periféricos como teclado e vídeo em modo texto e inicia o *Power-On Self-Test (POST)* que além de realizar alguns testes inicia, com base das configurações do *SETUP* salvas na memória CMOS, todos os circuitos periféricos, vídeo, Sistema Operacional e passa o controle para o sistema operacional (TORRES, 2001). Durante todo esse processo o computador é executado em *Real Mode*, e como já foi descrito anteriormente, em modo real os programas não são isolados uns dos outros como no *Protected Mode*, logo qualquer programa em execução pode acessar todo conteúdo na memória. O rootkit pode persistir no *firmware*² de algum periférico, como a placa de vídeo (ECONOMOU; JUAREZ, 2012) ou placa de rede (BLANCO; EISSLER, 2012), dessa forma que tornariam o clone do HDD inútil além de ter acesso em *Real Mode* na inicialização do computador.

O perito deve ter em mente ainda que o rootkit pode estar em áreas reservadas do disco como *host protected area (HPA)* ou *Device configuration overlay (DCO)*, essas areas são desenvolvidas para não serem modificadas ou mesmo acessadas por usuários, BIOS ou Sistema Operacional (GUPTA et al., 2006). Dessa forma dependendo da ferramenta utilizada para clone do HDD pode ser que essas áreas não sejam clonadas ((NIST, 2008a) ou (NIST, 2008b)), inutilizando o clone do HDD.

Com o disco clonado o perito deve se ater a outros fatores, como criptografia, arquivos salvos em estruturas não convencionais etc. O disco clonado pode ter *full disk encryption* o que significa que todos os dados no disco estão criptografados (RUBENS, 2012) e que ao clonar o clone, como é uma cópia fidedigna do original, também tem todos os dados criptografados. Logo o disco deverá ser decriptado antes da análise. É improvável que um rootkit criptografe todo o disco da vítima, pois chamaria muita atenção e iria de encontro a uma de suas premissas

²Todo programa salvo numa *Read-only memory (ROM)* é chamado de firmware

que é se ocultar no sistema. Então quando disco está encriptado, ele provavelmente foi feito pela vítima e conseqüentemente a maior interessada no trabalho do perito facilitando a deciptação do disco. O mais comum nesses casos quando envolve criptografia é do rootkit encriptar somente o seu binário, mas isso vai ser discutido adiante na análise estática.

4.2 Recuperar arquivos

O próximo passo a ser tomado deve ser recuperar todos os arquivos do disco, isso inclui todos os arquivos *Master Table File (MFT)* deletados ou não, seguido por *data carving* com especial preocupação com:

- Assinaturas de executáveis;
- Fragmentos de arquivos;
- Data streams alternativos; e
- Slack space;

Todos os arquivos tem um especificação que define o formato que o arquivo deve ter para ser corretamente interpretado, essas especificação define um padrão de como o *bits* são organizados internamente e é chamado de *file format* (ROUSE, 2005). Esse formato também é usado por ferramentas de *data carving* para encontrar arquivos. Por exemplo a especificação do *Portable Executable (PE) File Format* (MICROSOFT, 2013) determina que todos os programas comecem com um pequeno executável *MS-DOS*. Esse pequeno executável inicia com o *Magic Number* 0x5A4D ou MZ em *ASCII*, as iniciais de Mark Zbikowski um dos arquitetos originais do MS-DOS (PIETREK, 2002), e uma mensagem como pode ser vista na figura 4.1. A função desse pequeno programa é apresentar a mensagem “This program cannot be run in DOS mode”.

Programas que fazem *data carving* buscam essas estruturas definidas, para encontrar executáveis. Contudo o rootkit pode usar programas como o *Transmogrify* do *Metasploit Anti-Forensics Project (MAFIA)* que é capaz de mascarar um arquivo em qualquer assinatura (MAYNOR; MOOKHEY, 2007), de forma a deixar um executável no formato de um arquivo texto por exemplo.

Outra forma do rootkit esconde-se de um *data carving* é utilizando-se de uma organização de arquivo não convencional, como usar fragmentos de diversos arquivos que só fazem sentido quando organizados de determinada forma, salvar seus arquivos em slack space buscando e

Offset	0	1	2	3	4	5	6	7	8	9	A	B	C	D	E	F	ASCII
00000000	4D	5A	90	00	03	00	00	00	04	00	00	00	FF	FF	00	00	MZ
00000010	B8	00	00	00	00	00	00	00	40	00	00	00	00	00	00	00	,
00000020	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	
00000030	00	00	00	00	00	00	00	00	00	00	00	00	F0	00	00	00	
00000040	0E	1F	BA	0E	00	B4	09	CD	21	B8	01	4C	CD	21	54	68	is
00000050	69	73	20	70	72	6F	67	72	61	6D	20	63	61	6E	6E	6F	program
00000060	74	20	62	65	20	72	75	6E	20	69	6E	20	44	4F	53	20	cannot
00000070	6D	6F	64	65	2E	0D	0D	0A	24	00	00	00	00	00	00	00	be
00000080	87	45	16	64	C3	24	78	37	C3	24	78	37	C3	24	78	37	run
00000090	39	07	38	37	C6	24	78	37	19	07	64	37	C8	24	78	37	in
000000A0	C3	24	78	37	C2	24	78	37	C3	24	79	37	44	24	78	37	DOS
000000B0	39	07	61	37	CE	24	78	37	54	07	3D	37	C2	24	78	37	mode
000000C0	19	07	65	37	DF	24	78	37	39	07	45	37	C2	24	78	37	.
000000D0	52	69	63	68	C3	24	78	37	00	00	00	00	00	00	00	00	\$
000000E0	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	
000000F0	50	45	00	00	4C	01	03	00	10	84	7D	3B	00	00	00	00	
00000100	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	

Figura 4.1: Hexadecimal da Microsoft Calculator v. 5.1 visto no WinHex 16.3 SR-2

indexando-os em um *file system* próprio (EASTTOM, 2007), ou ainda usando *features* de um sistema de arquivos como as *streams* do NTFS (THOMPSON; MOROE, 2006). Entretanto por mais eficiente que seja o método utilizado, o rootkit em algum momento tem que executar, logo em algum ponto o rootkit tem que trabalhar com estruturas convencionais para que o sistema operacional o interprete, mesmo que seja apenas um *stub* (ver análise estática).

4.3 Coletar metadados dos arquivos

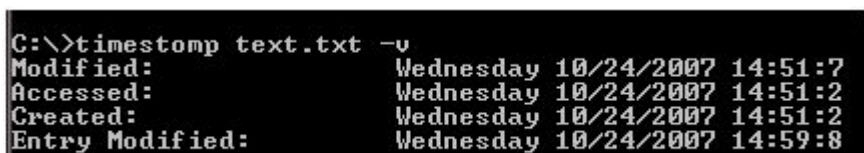
Nessa etapa é feita a coleta dos metadados de todos os arquivos, segue os principais:

- Hash;
- MAC time;
- Localização completa do arquivo em disco (*Path*); e
- Nome;
- Tamanho;

É importante que se tenha ao menos esses metadados dos arquivos recuperados. Os próximos passos podem depender de um desses elementos. O *hash* é fundamental para o próximo passo, o tamanho vai ser abordado na análise estática, o nome e *path* são obviamente para sua identificação

e para localização, e o *MAC (Modify, Access, Create) time* pode vir a ser utilizado para desenvolver uma *timeline*, ferramenta útil e poderosa para favor do perito.

A análise da *timeline* é um importante passo para todo processo tradicional de investigação, com base nela um perito forense computacional pode extrair informações cruciais para o caso (GUJÓNSSON, 2010). Criar uma *timeline* de eventos com base nos *MAC time* dos arquivos ajuda a entender o ciclo de contaminação, além de levantar suspeitas sobre varios dados inconsistentes, como por exemplo, porque o papel de parede do Windows tem a data de modificação ou criação recente? Além de ajudar a entender como o rootkit pode ter se mantido no ambiente analisado. Dessa forma é possível recriar a cadeia de eventos gerando ao mesmo tempo contexto.



```
C:\>timestomp text.txt -v
Modified:      Wednesday 10/24/2007 14:51:7
Accessed:      Wednesday 10/24/2007 14:51:2
Created:       Wednesday 10/24/2007 14:51:2
Entry Modified: Wednesday 10/24/2007 14:59:8
```

Figura 4.2: Arquivo com MAC time original (ACKERMAN, 2007a)

Para (HALLMAN, 2011) um dos principais desafios na análise de *timeline* envolve a fácil manipulação. Para não levantar suspeitas, ou dificultar o processo de análise da *timeline*, o rootkit pode ser programado a alterar o *MAC time* quando necessário. O programa *Timestomp* também do *MAFIA* e hoje integrado ao *Meterpreter* é capaz de alterar esses metadados como é mostrado na figura 4.3.

4.4 Retirar arquivos conhecidos

No passo anterior foram retirados *hashes* dos arquivos encontrados e eles podem ser comparados com bases de hashes conhecidos, como os fornecidos pelo *National Software Reference Library (NSRL)* ³ fornecidos pelo NIST. Comparando os hashes dos arquivos com essas bases é possível retirar todos os arquivos conhecidos maliciosos ou não diminuindo o escopo que o perito deve trabalhar

base de hash de arquivos conhecidos bons e ruins (assinatura de malwares conhecidos);

³<http://www.nsrll.nist.gov/Downloads.htm>

```

C:\>timestamp text.txt -m "Monday 1/01/2001 01:01:1 AM"

C:\>dir
Volume in drive C has no label.
Volume Serial Number is 3036-18D7

Directory of C:\

05/26/2007  06:01 PM                0 AUTOEXEC.BAT
05/26/2007  06:01 PM                0 CONFIG.SYS
10/24/2007  02:58 PM                <DIR>      Documents and Settings
05/29/2007  01:15 PM                <DIR>      Program Files
01/01/2001  01:01 AM                0 text.txt
10/24/2007  02:50 PM            57,344 timestamp.exe
06/18/2007  05:31 PM                <DIR>      WINDOWS
               4 File(s)            57,344 bytes
               3 Dir(s)   11,767,320,576 bytes free

C:\>timestamp text.txt -v
Modified:                Monday 1/1/2001 1:1:1
Accessed:                Wednesday 10/24/2007 14:51:2
Created:                 Wednesday 10/24/2007 14:51:2
Entry Modified:          Wednesday 10/24/2007 14:59:8

C:\>

```

Figura 4.3: Utilização do timestamp (ACKERMAN, 2007b)

4.5 Análise estática dos executáveis suspeitos desconhecidos

suspeita do tamanho do arquivo jpg com 2GB, estegnografia

cryptors e packers. colocar o binário numa forma encriptado e comprimido que as tools nao interpretam, o stub (esbolço) decodifica o payload e munda o controle do executável para o entry point do binario original. usado pelo skype (<http://www.blackhat.com/presentations/bh-europe-06/bh-eu-06-biondi/bh-eu-06-biondi-up.pdf>)

UPX _ merge secxtions (.text, .data, .idata, etc) em um unico sector upx1, onde tem uma stub que unpack o original.

funcionamento do upx

com a tooool dumpbin da para ver as sections do upx

upx0 é espaço vazio upx1 onde esta o stub e o executavel compactado, ao descompactar o executavel ele move para os endereços do upox (na low memory), assim o mesmo é decompoi-lado e executado e com o tempo ele sobrescreve tbm os endereços onde atnes estavam o upx1 (<http://upx.sourceforge.net/>)

embeded virtual machine, o rootkit esta em bytecode que sao interpretados pela vm em runtime, a tool nem mesmo o processador tem como saber como interpretar o bytecode sem a vm

combinação de ambos o stub decodifica a vm que interpreta o bytecode

basicamente o stub tem a chave para decodificar o binario, mas isso pode ser mais difícil quando crypter e packer privado, pode dividir o código em diversos setores e cada setor ter uma chave criptografada diferente SALT + HWID + TIME + PCI ROM para criar a chave

4.6 Análise dinâmica dos executáveis suspeitos

antidebugger FS flag determina o debug na arquitetura IA32, explicar que assim e processador faz uma instrução por vez

Windows SDK duas rotinas, WINAPI isDEBUggerPresent(void) user-mode ou KdRefreshDebuggerNotPresent() Kernel-mode (being debugged PEB <http://www.symantec.com/connect/articles/windows-anti-debug-reference>)

antivirtualização, para testar qualquer código malicioso deve-se

<http://www.chmag.in/article/sep2011/rootkits-are-back-boot-infection>

4.7 outro

nao existe tecnica antiforense 100% nem metodologia para analise infalivel, nem 100% segura e confiavel

Referências Bibliográficas

- ACKERMAN, D. *Timestomp mace*. 2007. Disponível em: <http://www.forensicswiki.org/wiki/File:Timestomp_mace.jpg>.
- ACKERMAN, D. *Timestomp mace change*. 2007. Disponível em: <http://www.forensicswiki.org/wiki/File:Timestomp_mace_change.jpg>.
- BERINATO, S. *The Rise of Anti-Forensics*. 2007. Disponível em: <<http://www.csoonline.com/article/221208/the-rise-of-anti-forensics>>.
- BLANCO, A.; EISSLER, M. One firmware to monitor é m all. Eko Party 2012, 2012. Disponível em: <http://www.ekoparty.org/archive/2012/BlancoEissler_2012-paper.pdf>.
- BLUNDEN, B. Anti-forensics: The rootkit connection. Black Hat USA 2009, 2009. Disponível em: <<http://www.blackhat.com/presentations/bh-usa-09/BLUNDEN/BHUSA09-Blunden-AntiForensics-PAPER.pdf>>.
- BLUNDEN, B. *The rootkit arsenal*. 1ª. ed. Plano, Texas: Wordware Publishing, 2009. ISBN 978-1-59822-061-2.
- EASTTOM, C. Utilizing slack space for hidden partitions. 2007. Disponível em: <<http://chuckeasttom.com/ghostdrive.pdf>>.
- ECONOMOU, N. A.; JUAREZ, D. Vga persistent rootkit. Eko Party 2012, 2012. Disponível em: <http://www.ekoparty.org/archive/2012/VGA_Persistent_Rootkit.pdf>.
- FRANÇA, G. V. *Medicina Legal*. 8ª. ed. Rio de Janeiro - RJ: Guanabara-kooga, 2008. ISBN 978-85-7302-9635.
- GUPTA, M. R. et al. Hidden disk areas: Hpa and dco. *International Journal of Digital Evidence*, 2006. Disponível em: <<http://www.utica.edu/academic/institutes/ecii/publications/articles/EFE36584-D13F-2962-67BEB146864A2671.pdf>>.
- GUJÓNSSON, K. Mastering the super timeline with log2timeline. SANS Institute Reading Room, 2010. Disponível em: <<http://www.sans.org/readingroom/whitepapers/logging/mastering-super-timeline-log2timeline3438>>.
- HALLMAN, M. *Timeline Creation and Analysis*. 2011. Disponível em: <<http://www.basistech.com/pdf/events/open-source-forensics-conference/osdf-2011-hallman-log2timeline.pdf>>.
- HARRIS, R. Arriving at an anti-forensics consensus: Examining how to define and control the anti-forensics problem. *Digital investigation 3S (2006) s4-s49*, 2006. Disponível em: <<http://www.dfrws.org/2006/proceedings/6-Harris.pdf>>.

HOGLUND, G.; BUTLER, J. *Rootkits: Subverting the Windows Kernel*. 1ª. ed. [S.l.]: Addison Wesley Professional, 2005. ISBN 0-321-29431-9.

HOUAISS, A.; VILLAR, M. de S. *Dicionário Houaiss da língua portuguesa*. 1ª. ed. Rio de Janeiro - RJ: Objetiva, 2009. ISBN 978-85-7302-9635.

INTEL. Intel 80386 programmer's reference manual 1986. Intel, 1986. Disponível em: <<http://css.csail.mit.edu/6.858/2011/readings/i386.pdf>>.

INTEL. Intel 64 and ia-32 architectures software developer's manual, volume 3a: System programming guide, part 1. Intel, 2011. Disponível em: <<http://download.intel.com/design/processor/manuals/253668.pdf>>.

KASPERSKY. *Computer Security FAQ*. 2013. Disponível em: <http://www.kaspersky.com/threats_faq>.

LUDWIG, M. A. *The rootkit arsenal*. 1ª. ed. Show Low, Arizona: American Eagle Publications, Inc., 1995.

MACHADO, M. P.; ELEUTÉRIO, P. M. da S. *Desvendando a Computação Forense*. 1ª. ed. [S.l.]: Novatec, 2011. ISBN 978-85-7522-260-7.

MAYNOR, D.; MOOKHEY, K. K. *Metasploit Toolkit for Penetration Testing, Exploit Development, and Vulnerability Research*. 1ª. ed. Rio de Janeiro - RJ: Syngress Publishing, Inc, 2007. ISBN 978-1-59749-074-0.

MCAFEE. *Glossary*. 2013. Disponível em: <<http://home.mcafee.com/virusinfo/glossary>>.

MCDUGAL, M. Live forensics on a windows system: Using windows forensic toolchest(wft). Fool Moon - Software Security, 2006. Disponível em: <http://www.foolmoon.net/downloads/Live_Forensics_Using_WFT.pdf>.

MEDINA, P. Österberg. Detecting rootkits in memory dumps. *PTS*, Associação Brasileira De Especialistas Em Alta Tecnologia (ABEAT), 2009. Disponível em: <<http://www.terena.org/activities/tf-csirt/meeting27/oesterberg-rootkits.pdf>>.

MESQUITA, F. I.; HOELS, B. W. P.; RALHA, C. G. Raciocínio baseado em casos aplicado em análise live. Associação Brasileira De Especialistas Em Alta Tecnologia (ABEAT), 2011. Disponível em: <<http://www.icofcs.org/2011/papers-published-007.html>>.

MICROSOFT. *Microsoft PE and COFF Specification*. 2013. Disponível em: <<http://msdn.microsoft.com/en-us/windows/hardware/gg463119.aspx>>.

MULVEY, B. *Hash Functions*. 2007. Disponível em: <<http://home.comcast.net/bretm/hash/>>.

NIST. Test results for digital data acquisition tool: Encase linen 6.01. National Institute of Justice, 2008. Disponível em: <<https://www.ncjrs.gov/pdffiles1/nij/224147.pdf>>.

NIST. Test results for digital data acquisition tool: Ftk imager 2.5.3.14. National Institute of Justice, 2008. Disponível em: <<https://www.ncjrs.gov/pdffiles1/nij/222982.pdf>>.

PIETREK, M. *An In-Depth Look into the Win32 Portable Executable File Format*. 2002. Disponível em: <<http://msdn.microsoft.com/en-us/magazine/cc301805.aspx>>.

ROGERS, D. M. Anti-forensic presentation given to lockheed martin. San Diego, 2005.

ROSANES, P. Rootkits. *GRIS - Grupo de Resposta a Incidentes de Segurança. Universidade Federal do Rio de Janeiro*, 2011. Disponível em: <<http://www.gris.dcc.ufrj.br/documentos/artigos/rootkits-survey>>.

ROUSE, M. *DEFINITION: File format*. 2005. Disponível em: <<http://searchcio-midmarket.techtarget.com/definition/file-format>>.

RUBENS, P. *Buyer's Guide to Full Disk Encryption*. 2012. Disponível em: <<http://www.esecurityplanet.com/mobile-security/buyers-guide-to-full-disk-encryption.html>>.

RUTKOWSKA, J. Beyond the cpu: Defeating hardware based ram acquisition (part i: Amd case). Black Hat DC 2007, 2007. Disponível em: <<http://www.blackhat.com/presentations/bh-dc-07/Rutkowska/Presentation/bh-dc-07-Rutkowska-up.pdf>>.

SANTOS, C. M. *Dicionário Inglês-Português*. 2ª. ed. Santa Terezinha, São Paulo: Rideel, 2000.

THOMPSON, I.; MOROE, M. Fragfs: An advanced data hiding technique. Black Hat, 2006. Disponível em: <<http://www.blackhat.com/presentations/bh-federal-06/BH-Fed-06-Thompson/BH-Fed-06-Thompson-up.pdf>>.

TORRES, G. *Hardware Curso Completo*. 4ª. ed. Rio de Janeiro - RJ: Axcel Books do Brasil Editora, 2001. ISBN 85-7323-165-3.

TZU, S. *A Arte da Guerra*. Tradução de Candida de Sampaio Bastos. 1ª. ed. [S.l.]: Golden Books, IV a.C. 47 p. ISBN 978-85-7501-272-7.

VELHO, J. A.; GEISER, G. C.; ESPINDURA, A. *Ciências Forenses*. 1ª. ed. Campinas - SP: Millennium, 2012. ISBN 978-85-7625-249-8.