

**Instituto Politécnico de Beja**

**Escola Superior de Tecnologia e Gestão de Beja**

**Mestrado em Engenharia de Segurança Informática**

**Ataques Fulminantes em Sistemas Operativos**

**Microsoft Windows**

**Mário Jorge Costa Candeias**

**Beja**

**2015**



**Instituto Politécnico de Beja**  
**Escola Superior de Tecnologia e Gestão de Beja**  
**Mestrado em Engenharia de Segurança Informática**

**Ataques Fulminantes em Sistemas Operativos Microsoft  
Windows**

**Dissertação de Mestrado a apresentada na Escola Superior de Tecnologia e  
Gestão do Instituto Politécnico de Beja**

**Elaborado por:**  
**Mário Jorge Costa Candeias**

**Orientado por:**  
**Professor Doutor Rui Miguel Soares Silva**

**BEJA**  
**2015**



---

## **Resumo**

### *Ataques Fulminantes em Sistemas Operativos Microsoft Windows*

A segurança informática tem hoje em dia um foco mediático bastante acentuado, sendo recorrente a divulgação de notícias relativas a intrusões e fraudes informáticas, furtos de informação, bem como o surgimento de séries televisivas sobre o tema. Esta crescente importância da segurança informática deve-se, em grande parte, à divulgação de um número crescente de ataques informáticos de enorme relevância, quer pelos prejuízos financeiros causados quer pelo acesso, modificação ou destruição de informações privilegiadas.

Nos ataques a sistemas informáticos é comumente envolvida a pesquisa por vulnerabilidades conhecidas, sendo necessário obter informações sobre o sistema vítima o que, geralmente, é efetuado através da *Internet* ou da rede informática. Este é um dos motivos que leva os ataques a sistemas informáticos serem caracterizados pela sua duração, possibilitando aos equipamentos de monitorização do tráfego de redes a identificação do ataque. A recolha de informações que estes ataques efetuam dota o atacante de conhecimentos que possibilitam a exploração de alguma vulnerabilidade. Assim torna-se relevante a recolha, inclusivamente, de informações voláteis, ou seja, se o atacante tiver necessidade de reiniciar o computador alvo, estas informações poderão ser perdidas.

Com esta dissertação pretende-se contribuir para uma maior segurança da informação dos utilizadores e das organizações, através do desenvolvimento de estratégias e técnicas de ataques de curta duração a sistemas informáticos com o sistema operativo *Microsoft Windows*, sistema operativo utilizado por cerca de 91% dos utilizadores em computadores de tipo *Desktop*, e alvo recente de melhorias significativas na sua segurança.

## **Palavras-Chave**

Ataque informático, Recolha de Informações, Segurança Informática, Análise Forense, Análise de Registo, Windows Forensics, Ataques USB.

---

## **Abstract**

### *Fulminating attacks on Microsoft Windows Operating Systems*

The computer security, also known as cybersecurity or IT security is nowadays a hot topic by media coverage, being common news related to intrusions and computer fraud, information theft and the emergence of television series on the subject. This growing importance of computer security is largely due to the growing number of relevant cyber-attacks causing financial losses or access, modification or destruction of privileged information.

On attacks against Computer Systems are commonly involved search for known vulnerabilities, requiring information on the victim system and is usually made by the Internet or a computer network. This is one of the reasons why that specific software attacks are characterized by their length, enabling the monitoring equipment of network traffic to identify the attack. The collection of information that these attacks perform endows the attacker knowledge that enable the exploitation of a vulnerability. So it is relevant to the collection, including, volatile information, that is, if the attacker has restarting the target computer, this information may be lost.

This dissertation aims to contribute to increased information security of users and organizations by developing short attacks strategies and techniques on computer systems running operating system Microsoft Windows, operating system used for about 91% of users in Desktop computers [1], and recent target of significant improvements in their safety.

## **Key Words**

Hacking, Information Gathering, Computer Security, Forensics Analysis, Registry Analysis, Windows Forensics, USB attacks.

---

## Agradecimentos

Mais uma fase cumprida na minha vida académica, que contou com importantes apoios e incentivos aos quais estarei eternamente grato.

Ao amigo e Professor Rui Silva pelo seu positivismo, orientação e visão concedida ao longo do desenvolvimento desta Dissertação de Mestrado.

Um agradecimento sempre especial à minha família pela compreensão, o sempre presente apoio, incessante incentivo, e por tudo...

À Direção do Agrupamento de Escolas de Ferreira do Alentejo, por todo o apoio, compreensão e disponibilidade, nomeadamente à Diretora Antónia Figueiredo, Madalena Salgado, António Lota e em especial à Ana Paula Patriarca.

A todos os docentes do Mestrado em Engenharia de Segurança Informática, que em muito contribuíram para uma maior valorização pessoal.

Aos amigos e colegas de Mestrado que também eles permitiram a partilha de valores e conhecimentos que em muito ajudaram na conclusão desta etapa, em especial ao Paulo Monteiro, parceiro na primeira fase do Mestrado, e ao Vitor Farropas, parceiro de lides no Laboratório UbiNET.

De um modo geral, gostaria de deixar um sincero agradecimento a todos os que ao longo deste percurso contribuíram para a sua conclusão.

---

*“A vida é curta demais para se acordar com arrependimentos.  
Ama as pessoas que te tratam bem. Esquece aquelas que não...  
Ninguém disse que a vida seria fácil, só prometeu que iria valar  
a pena. Vive, deixa viver e sê feliz!”*  
*António Feio*



---

# Índice

RESUMO .....	I
PALAVRAS-CHAVE.....	I
ABSTRACT.....	II
KEY WORDS.....	II
AGRADECIMENTOS .....	III
ÍNDICE.....	V
ÍNDICE DE FIGURAS.....	IX
ÍNDICE DE TABELAS .....	X
ÍNDICE DE GRÁFICOS .....	XI
ABREVIATURAS E SIGLAS.....	XII
<b>1. INTRODUÇÃO .....</b>	<b>1</b>
<b>2. ESTADO DA ARTE E HIPÓTESE DE INVESTIGAÇÃO.....</b>	<b>7</b>
2.1. FERRAMENTAS FORENSES E A ALTERNATIVA FORENSE .....	7
2.1.1. E-FENSE LIVE RESPONSE E APERIO.....	9
2.1.2. ENCASE PORTABLE .....	11
2.1.3. COMPUTER ONLINE FORENSIC EVIDENCE EXTRACTOR .....	11
2.1.4. THE VOLATILITY FRAMEWORK .....	12
2.1.5. WIN-UFO.....	12
2.1.6. MANDIANT REDLINE .....	14
2.2. FERRAMENTAS DE RECOLHA DE INFORMAÇÃO NÃO FORENSE .....	14
2.2.1. SYSINTERNALS .....	14
2.2.2. NIRSOFT .....	15
2.2.3. INFOHACK.....	16
2.2.4. SCRIPTS .....	18
2.3. HIPÓTESE DE INVESTIGAÇÃO .....	19
<b>3. CARACTERIZAÇÃO DOS SISTEMAS OPERATIVOS WINDOWS.....</b>	<b>22</b>
3.1. EVOLUÇÃO HISTÓRICA.....	22
3.2. REGISTO.....	23
3.2.1. ESTRUTURA LÓGICA DO REGISTO DO WINDOWS .....	24

---

3.2.2.	ESTRUTURA INTERNA DO REGISTO DO WINDOWS.....	27
3.2.3.	ACESSO AOS FICHEIROS DO REGISTO .....	28
3.2.4.	ANÁLISE DO REGISTO .....	28
3.3.	DISPOSITIVOS USB .....	29
3.4.	SEGURANÇA NOS SISTEMAS OPERATIVOS WINDOWS .....	32
3.4.1.	WINDOWS VISTA .....	32
3.4.2.	WINDOWS 7 .....	34
3.4.3.	WINDOWS 8 E 8.1 .....	36
3.4.4.	WINDOWS 10 .....	39
3.4.5.	ANÁLISE CRÍTICA DAS EVOLUÇÕES DE SEGURANÇA DOS SISTEMAS OPERATIVOS WINDOWS .....	40
3.5.	CONDICIONANTES DE SEGURANÇA .....	40
3.5.1.	SISTEMAS DE SEGURANÇA GENÉRICOS .....	41
3.5.2.	USER ACCOUNT CONTROL (UAC) .....	41
3.5.3.	EXECUÇÃO AUTOMÁTICA NOS DISPOSITIVOS USB .....	41
<b>4.</b>	<b>DESENVOLVIMENTO DO SISTEMA .....</b>	<b>46</b>
4.1.	CENÁRIOS DE UTILIZAÇÃO.....	47
4.1.1.	ATAQUE OU <i>HACKING</i> .....	48
4.1.2.	INVESTIGAÇÃO FORENSE.....	49
4.1.3.	RESPOSTA A INCIDENTES .....	50
4.2.	OPÇÕES DE DESENVOLVIMENTO .....	51
4.3.	ARQUITETURA DE <i>HARDWARE</i> .....	52
4.4.	ARQUITETURA DE <i>SOFTWARE</i> .....	53
4.4.1.	SCRIPT <i>AUTORUN</i> .....	53
4.4.2.	<i>SCRIPT</i> DE RECOLHA .....	55
4.4.3.	INTERFACE GRÁFICA .....	58
<b>5.</b>	<b>AVALIAÇÃO .....</b>	<b>65</b>
5.1.	AVALIAÇÃO DO FUNCIONAMENTO.....	65
5.2.	AVALIAÇÃO DA EFICIÊNCIA .....	66
<b>6.</b>	<b>CONCLUSÕES E TRABALHOS FUTUROS .....</b>	<b>81</b>
	<b>REFERÊNCIAS BIBLIOGRÁFICAS .....</b>	<b>87</b>
	<b>APÊNDICE I - INFORMAÇÕES ÚTEIS EM SISTEMAS WINDOWS .....</b>	<b>101</b>
<b>1.</b>	<b>INFORMAÇÕES ÚTEIS EM SISTEMAS WINDOWS.....</b>	<b>103</b>
1.1.	INFORMAÇÕES DE SISTEMA.....	103
1.1.1.	DATA E HORA .....	105

1.1.2.	VARIÁVEIS DE AMBIENTE .....	105
1.1.3.	NÚMERO DE SÉRIE DA PARTIÇÃO DE SISTEMA.....	105
1.1.4.	UTILIZADORES NO SISTEMA .....	106
1.1.5.	INFORMAÇÕES DE REDE .....	107
1.1.6.	PROCESSOS E APLICAÇÕES .....	109
1.1.7.	ATUALIZAÇÕES DE SEGURANÇA .....	110
1.1.8.	REGISTO .....	110
1.1.9.	SERVIÇOS .....	111
1.1.10.	TAREFAS AGENDADAS .....	112
1.1.11.	EVENTOS .....	112
1.1.12.	MEMÓRIA RAM .....	113
1.1.13.	ÁREA DE TRANSFERÊNCIA .....	113
1.1.14.	HARDWARE .....	113
1.1.15.	BITLOCKER .....	114
1.1.16.	DOCUMENTOS IMPRESSOS .....	115
1.1.17.	SERVIÇO DE INDEXAÇÃO .....	115
1.1.18.	FICHEIROS PREFETCH .....	115
1.2.	INFORMAÇÕES DE UTILIZADORES.....	115
1.2.1.	DOCUMENTOS E FICHEIROS DO UTILIZADOR .....	116
1.2.2.	ATIVIDADE DO UTILIZADOR.....	116
1.2.3.	IMAGEM DO AMBIENTE DE TRABALHO.....	117
1.2.4.	CONTACTOS.....	117
1.2.5.	PASSWORDS.....	118
1.2.6.	ITENS ENCRIPADOS .....	119
1.2.7.	ITENS OCULTOS .....	120
1.2.8.	ITENS ELIMINADOS .....	121
1.2.9.	PERFIL NO <i>BROWSER</i> .....	121
1.2.10.	FAVORITOS .....	121
1.2.11.	TRANSFERÊNCIAS .....	122
1.2.12.	E-MAILS .....	122
1.2.13.	HISTÓRICO DE ENDEREÇOS DIGITADOS .....	123
1.2.14.	HISTÓRICO DE SITES VISUALIZADOS .....	123
1.2.15.	FICHEIROS TEMPORÁRIOS DA <i>INTERNET</i> (CACHE) .....	124
1.2.16.	COOKIES .....	124
1.2.17.	LOG'S DE APLICAÇÕES.....	125
<b>APÊNDICE II – PÁGINA DE AJUDA NA APLICAÇÃO .....</b>		<b>127</b>
<b>CRIME SCENE FORENSIC INFORMATION GATHERING .....</b>		<b>128</b>



---

## Índice de figuras

FIGURA 1 - E-FENSE LIVE RESPONSE.....	10
FIGURA 2 - WIN-UFO.....	13
FIGURA 3 - NIRLAUNCHER.....	16
FIGURA 4 - INFOHACK UAC WARNING.....	17
FIGURA 5 - INFOHACK TERMINADO.....	18
FIGURA 6 - <i>SCRIPT</i> DE RECOLHA DE INFORMAÇÃO DE SISTEMA.....	19
FIGURA 7 - CRONOLOGIA DO LANÇAMENTO E DURAÇÃO DE SISTEMAS OPERATIVOS MICROSOFT WINDOWS PARA COMPUTADORES E SERVIDORES.....	22
FIGURA 8 - LOCALIZAÇÃO DO EDITOR DE REGISTO.....	24
FIGURA 9 - RAMIFICAÇÕES DO REGISTO (WIN 8.1).....	25
FIGURA 10 - CHAVES E SUBCHAVES DO REGISTO.....	26
FIGURA 11 - ESTRUTURA INTERNA DO HIVE.....	27
FIGURA 12 - OFFSET E DIMENSÃO DOS CAMPOS NO BLOCO BASE.....	28
FIGURA 13 - LISTA DOS FICHEIROS MODIFICADOS RECENTEMENTE.....	32
FIGURA 14 - RUBBERDUCKY.....	43
FIGURA 15 - PROCEDIMENTO DE ATAQUE.....	46
FIGURA 16 - PROCEDIMENTO DE ATAQUE EM DUAS FASES.....	49
FIGURA 17 - PROCEDIMENTO DE ATAQUE EM FASE ÚNICA.....	49
FIGURA 18 - FLUXOGRAMA DO DISPOSITIVO DE <i>AUTORUN</i> .....	54
FIGURA 19 - EXCERTO DO CÓDIGO DO <i>SCRIPT AUTORUN</i> .....	55
FIGURA 20- EXCERTO DO <i>SCRIPT</i> DE RECOLHA.....	56
FIGURA 21 - APLICAÇÃO “CRIME SCENE FORENSIC INFORMATION GATHERING”.....	58
FIGURA 22 - OPÇÕES DE RECOLHA.....	59
FIGURA 23 - SELEÇÃO DA RAIZ DA PESQUISA DE FICHEIROS.....	59
FIGURA 24 - SELEÇÃO DAS EXTENSÕES.....	60
FIGURA 25 - MENU FILE E HELP.....	60
FIGURA 26 - ABOUT.....	61
FIGURA 27 - VERSÃO DO SISTEMA OPERATIVO ATRAVÉS DO REG.EXE.....	103
FIGURA 28 - VERSÃO DO SISTEMA OPERATIVO ATRAVÉS DO WMIC.....	104
FIGURA 29 - VERSÃO DO SISTEMA OPERATIVO ATRAVÉS DO PSINFO.....	104
FIGURA 30 - RESULTADO DA FERRAMENTA USERPROFILESVIEW.EXE.....	106
FIGURA 31 - NIRSOFT TURNEDONTIMESVIEW.....	107
FIGURA 32 - ENCRYPTED DISK DETECTOR.....	120

---

## Índice de tabelas

TABELA 1 - LOCALIZAÇÃO DOS FICHEIROS DOS <i>HIVES</i> PRINCIPAIS .....	25
TABELA 2 - EFICIÊNCIA DO BLOCO "VARIÁVEIS COMUNS" .....	69
TABELA 3 - EFICIÊNCIA DO BLOCO "INFORMAÇÃO DE SISTEMA" .....	69
TABELA 4 - EFICIÊNCIA DO BLOCO "INFORMAÇÃO DE SISTEMA" .....	70
TABELA 5 - EFICIÊNCIA DO BLOCO "INFORMAÇÕES DE UTILIZADORES" .....	70
TABELA 6 - EFICIÊNCIA DO BLOCO "FICHEIROS DE REGISTO" .....	71
TABELA 7 - EFICIÊNCIA DO BLOCO "EVENTOS" .....	71
TABELA 8 - EFICIÊNCIA DO BLOCO "HISTÓRICO DE NAVEGAÇÃO" .....	72
TABELA 9 - EFICIÊNCIA DO BLOCO "COOKIES" .....	72
TABELA 10 - EFICIÊNCIA DO BLOCO "FICHEIROS" .....	73
TABELA 11 - EFICIÊNCIA DO BLOCO "UNIDADES E FICHEIROS ENCRIPADOS" .....	73
TABELA 12 - EFICIÊNCIA DO BLOCO "PASSWORDS" .....	74
TABELA 13 - EFICIÊNCIA EM DIFERENTES COMPUTADORES .....	75
TABELA 14 - EFICIÊNCIA COM DIFERENTES DISCOS RÍGIDOS .....	75
TABELA 15 - EFICIÊNCIA EM DIFERENTES SISTEMAS OPERATIVOS .....	77

---

## Índice de gráficos

GRÁFICO 1 - TAXAS DE TRANSFERÊNCIA POR TIPO DE LIGAÇÃO .....	29
--	----

---

## **Abreviaturas e siglas**

BIOS – Basic Input Ouput System  
Caine – Computer Aided INvestigative Environment  
COFEE – Computer Online Forensic Evidence Extractor  
DEFT – Digital Evidence & Forensic Toolkit  
DFF – Digital Forensics Framework  
DNS – Domain Name System  
IDS – Intrusion Detecting System  
IDS - Intrusion Detection System  
IoT – Internet of Things  
NSA – National Security Agency  
NW3C – National White Collar Crime Center  
POI – Points Of Interest  
RAM – Random Access Memory  
SO – Sistema Operativo  
SSD – Solid State Disk  
UAC – User Account Control  
USB – Universal Serial Bus



## INTRODUÇÃO

---

Neste Capítulo é efetuado um enquadramento da dissertação, dando ênfase à dimensão que a *Internet* assumiu na relação com o grau de dependência que os indivíduos têm para com as tecnologias. Esta interligação leva a uma maior quantidade de dispositivos interligados e, por conseguinte, assume-se como essencial a segurança informática a par do crescimento da *Internet* nas sociedades digitais de hoje.



## 1. Introdução

Com o acentuado aumento da dependência da tecnologia e da *Internet*, o aumento dos utilizadores ligados à *Internet*, que aumentaram 753% de 2000 a 2015, correspondendo a 3 mil milhões de atuais utilizadores [1], conjuntamente com a espectável explosão proporcionada pela “*Internet of Things*” (IoT), onde se prevê que em 2020 cada pessoa utilize uma média de 25 dispositivos ligados à *Internet* [2], também a cibercriminalidade tem tido um aumento significativo. Toda a informação a circular nesta rede mundial é extremamente atrativa às organizações criminosas, proporcionando o desenvolvimento de atividades ilegais à escala mundial, com um grau superior de sofisticação e anonimização, maximizando lucros, em períodos de tempo cada vez menores.

Apesar de ainda continuar válida a expressão “quem detém a informação, detém o poder”, a crescente importância das Tecnologias de Informação na sociedade facilita a espionagem industrial e de Estado através da interligação das suas redes com a *Internet*.

A aposta na segurança dos sistemas e das informações tem um papel cada vez mais fulcral, devido ao crescente número pessoas com a motivação, a oportunidade e a tecnologia necessárias para atacar sistemas informáticos, recolhendo informações para benefício próprio ou de terceiros.

*“The new source of power is not money in the hands of a few, but information in the hands of many.”*

*John Naisbitt*

Deste modo, estamos a presenciar uma revolução na segurança da informática e da informação, uma crescente consciencialização sem precedentes para a segurança informática, muito por “culpa” de Edward Snowden e as suas delações sobre as atividades da Agência de Segurança Nacional (NSA) dos Estados Unidos da América. A eficácia dos processos e equipamentos de defesa das informações e sistemas estão continuamente a ser postos em causa pela quantidade de ameaças que têm de suportar através dos seus mais diversos vetores de ataque.

Um dos vetores de ataque abordados neste trabalho de dissertação é o “ataque fulminante”, o qual se caracteriza numa perspetiva de segurança ofensiva, pelo curto tempo de duração com elevada capacidade de recolha de informações da máquina alvo. Tipicamente, as primeiras fases de um ataque informático caracterizam-se por “*information gathering*”, aliada à engenharia social e sempre com o objetivo de obter

informações que possibilitem o acesso ao sistema alvo através da exploração de uma determinada vulnerabilidade.

Os ataques fulminantes a sistemas operativos Windows, tema objeto da investigação, é desafiante não só pela importância que representa no seio das organizações as quais, de um modo global, não se encontram devidamente preparadas para combater ataques internos, mas também por ter como alvo máquinas com o sistema operativo Microsoft Windows, o sistema mais utilizado a nível global, com uma taxa de utilização de cerca de 91% dos utilizadores em computadores fixos e portáteis [3].

Com o objetivo de estudar a possibilidade da rápida recolha de informações nos sistemas Microsoft Windows, um dos desafios será a compreensão do funcionamento dos mesmos, principalmente a nível dos locais de armazenamento das informações pretendidas. Deste modo, o fator de oportunidade será a principal restrição do ataque, já que este poderá ter um espaço temporal limitado, por exemplo, a pausa de almoço de um utilizador, ou mesmo enquanto o utilizador se desloca à impressora central na organização. É deste modo imperativo que a recolha das informações seja efetuada de modo simples, mas parametrizável, mediante o tempo disponível para a quantidade de informação pretendida.

Para a concretização do objetivo proposto, é necessária a utilização de um método de investigação baseado no estudo abrangente de literatura diversa e participação em *workshops*. Posteriormente, o desenvolvimento de uma aplicação necessita de uma abordagem de investigação de cariz mais exploratória devido, principalmente, à identificação dos fatores condicionantes ao desenvolvimento da aplicação.

O presente documento foi repartido em nove capítulos, de modo conseguir descrever-se o processo de investigação, identificando as questões principais decorrentes das condicionantes ao objetivo proposto, testar, verificar e validar os resultados, avaliando o grau de confiança da aplicação.

Deste documento constam o capítulo 2 como “Estado da arte e hipótese de investigação”, onde é efetuada a descrição de informações e ferramentas semelhantes existentes até ao momento, na tentativa de encontrar novas e inspiradoras ideias para o desenvolvimento do trabalho e para a formulação da hipótese de investigação.

No capítulo 3, “Caracterização dos sistemas operativos Windows”, é descrita a evolução histórica dos sistemas operativos da *Microsoft*, e é efetuado o estudo do seu funcionamento ao nível do registo e do seu comportamento com os dispositivos USB, e por fim é efetuado um estudo sobre a segurança dos sistemas operativos Windows e condicionantes de segurança para o presente projeto.

O capítulo 4 “Desenvolvimento do sistema” descreve todo o processo de desenvolvimento dos *scripts* e também da aplicação.

Por fim, são descritos os testes realizados e as conclusões decorrentes dos mesmos no capítulo 5, Avaliação.

Existe ainda o Apêndice 1, “Informações úteis em sistemas Windows” como o nome indica são descritas as informações relevantes passíveis de recolher na máquina alvo.



## **ESTADO DA ARTE E HIPÓTESE DE INVESTIGAÇÃO**

---

Neste capítulo é efetuada a descrição de informações e ferramentas existentes relacionadas com o projeto até ao momento, na tentativa de encontrar novas e inspiradoras ideias para o desenvolvimento do trabalho e para a formulação da hipótese de investigação.





## 2. Estado da arte e hipótese de investigação

Este capítulo caracteriza-se, na sua essência, pela descrição do que mais recente e inovador existe sobre o tema em estudo. Deste modo, foram efetuadas pesquisas exaustivas na mais diversa literatura com a intenção de determinar os avanços aplicados ao tema em estudo. No entanto, no decorrer das primeiras pesquisas, ficou patente a dificuldade na obtenção de informações relativas ao tema, definida a utilização deste tipo de aplicações por duas principais e opostas áreas. Por um lado, temos o atacante, que desenvolve a sua atividade por motivos de espionagem, políticos, financeiros, ou benefício próprio e, pelo outro lado, trabalham as forças policiais na análise de computadores na tentativa de provar a existência de crime através da extração de evidências sobre os factos em investigação, capazes de responder às típicas questões de investigação forense de um qualquer incidente:

*“o quê?, onde?, quando?, como?, quem?, porquê? e quanto?”*  
*Inspetor Chefe Rogério Bravo*

Foram vários os *scripts*, *software* e dispositivos alvos de pesquisas e análises com objetivos semelhantes aos propostos. No entanto, no decorrer das análises efetuadas, podemos categorizá-los de acordo com o processo de recolha da informação, isto porque a maioria dos *scripts* e *software* de recolha da informação utiliza a rede interna na qual a máquina alvo se encontra ligada e que, por sua vez, se encontra ligada à *Internet*. São dispositivos que utilizam as portas de transferência da informação da máquina alvo para ligar algum tipo de dispositivo de armazenamento como destino da informação. Existem ainda ferramentas que permitem a cópia e/ou imagem forense do disco, para posterior análise, ferramentas que são aqui consideradas principalmente pelos procedimentos e técnicas de recolha de informações e também pelas metodologias já definidas no processo de recolha.

### 2.1. Ferramentas forenses e a alternativa forense

Apesar dos objetivos propostos serem num campo de ação de ataque, as ferramentas de âmbito forense são realçadas devido sobretudo à sua capacidade de proceder à recolha de informações numa máquina alvo, para posterior análise.

É necessário desde já realçar que numa investigação forense e principalmente numa investigação “*Live Forensics*”, é necessário que as ferramentas utilizadas se encontrem certificadas, para que não a sua validade não seja posta em causa. Nestas situações o

investigador deverá editar o *script* para utilizar ferramentas próprias. No entanto, existem situações que todas estas ferramentas podem ser utilizadas, como é o caso de uma análise em ambientes virtualizados, em que é possível efetuar alterações aos sistemas sem preocupações, uma vez que o sistema original continua intacto.

As ferramentas forenses caracterizam-se também de acordo com a sua forma de abordagem, podendo ser ferramentas de “análise *Post Mortem*” ou ferramentas “*Live Forensics*”. As primeiras não serão desenvolvidas neste trabalho, uma vez que, de acordo com os objetivos propostos, existe interesse na captura de informações voláteis, que não são obtidas na análise *Post Mortem*, isto é com o computador desligado. No entanto, é de realçar as várias distribuições Linux existentes [4] com *software* de recolha e análise *Post Mortem*, tais como, entre outros:

- Caine (Computer Aided INvestigative Environment - [www.caine-live.net](http://www.caine-live.net))
- DFF Linux Live (Digital Forensics Framework - [www.digital-forensic.org/live](http://www.digital-forensic.org/live))
- DEFT Linux (Digital Evidence & Forensic Toolkit - [www.deftlinux.net](http://www.deftlinux.net))
- Helix ([www.e-fense.com/helix](http://www.e-fense.com/helix)).

Existem ainda muitas outras distribuições Linux que contêm *software* específico forense, mas que são distribuições desenvolvidas para testes de penetração, tais como o Kali Linux, BackBox Linux, entre outros. É de referir ainda que a maioria destas distribuições é de utilização gratuita e podem ser gravadas num *livecd* ou mesmo numa *pendrive* para serem iniciadas no arranque do computador.

Em várias dessas distribuições existem aplicações de testes de penetração em sistemas informáticos, tal como a *Metasploit framework*, que permitem aos atacantes recolher informações num sistema alvo, em modo silencioso. Em [5] foi apresentado um modo de recolha de informação forense à distância, sendo o acesso à máquina alvo efetuado através do *Metasploit framework*, possibilitando a execução de ferramentas forenses.

A análise *Live Forensics* consiste num conjunto de procedimentos de recolha de informações sem que o computador seja desligado, priorizando as mais voláteis por conceito, das quais constam as seguintes, entre outras:

- memória principal ou RAM;
- ligações de rede;

- processos ativos;
- serviços ativos;
- sessões ativas.

Deste modo, a informação recolhida em modo *Live Forensics* torna-se indispensável para uma correta análise forense, possibilitando o cruzamento de dados e contextualizando o sistema aquando do incidente ocorrido. Assim, são destacadas as seguintes ferramentas:

### 2.1.1. e-fense Live Response e Aperio

Apesar de ser um dispositivo comercializado como a primeira resposta após um incidente num computador, e não de ataque, podendo facilmente ser utilizado como tal, tem como principal objetivo permitir aos investigadores ou responsáveis de segurança informática a recolha prioritária dos dados voláteis, uma vez que estes facilmente serão perdidos, não apenas quando o computador seja desligado ou reiniciado, mas também com a realocação das áreas de memória, apesar de se ter comprovado que é possível extrair das memórias pequenas frações de informação mesmo após a interrupção de energia. Desenvolvido pela e-fense [6], empresa na área de investigação forense e de desenvolvimento de *software* de âmbito forense, o e-fense *Live Response* destaca-se por ser uma vulgar *pendrive* com 16GB de capacidade.

Desde 2009 que existe uma parceria entre a e-fense e a Access Data [7], uma das empresas de referência no que diz respeito ao desenvolvimento de *software* forense, muito devido ao sucesso do FTK Imager. No âmbito desta parceria, a Access Data optou por descontinuar o seu dispositivo de características semelhantes ao e-fense *Live Response*, apoiando o desenvolvimento do dispositivo da e-fense, com o objetivo de o comercializar.

A aplicação que esta *pendrive* contém permite a configuração do procedimento de recolha de informação. O investigador necessita de executar a aplicação na máquina pretendida e selecionar quais as informações que pretende recolher para que esta seja executada, ilustrada na Figura 1.



Figura 1 - e-fense Live Response

A empresa e-fense tem ainda um dispositivo em muito semelhante ao Live Reponse, mas comercializado apenas para organizações policiais ou agências governamentais, dispositivo designado por “Aperio”.

Ambos os dispositivos têm objetivos semelhantes no que diz respeito à recolha de informações, sendo publicitada a possibilidade da recolha e armazenamento de informações, incluindo ficheiros ocultos ou eliminados, bem como a análise dos resultados, sendo que as informações recolhidas são as seguintes:

- memória RAM;
- conexões de rede, portas abertas TCP ou UDP, NetBIOS;
- utilizador com a sessão ativa e contas de utilizadores;
- processos e serviços em execução;
- tarefas agendadas;
- registo do Windows;
- dados de preenchimento automático dos *browsers* e *passwords*;
- captura de ecrã;
- *logs* de programas de conversação online (*chats*);
- ficheiros SAM e NTUser.dat;
- logs de sistema;
- aplicações instaladas e *drives*;
- variáveis de ambiente;
- histórico da *Internet*.

### 2.1.2. EnCase Portable

Detido pela Guidance Software Inc. [8], uma das empresas com maior reconhecimento na comercialização e desenvolvimento de *software* e *hardware* forense, o EnCase Portable [9] é uma ferramenta desenvolvida especificamente para abranger o máximo número de pessoas, desde utilizadores com experiência limitada (normalmente na ótica do utilizador) a utilizadores com conhecimentos forenses suficientes para efetuar uma correta recolha de informação aos investigadores forenses de agências policiais.

Sendo considerada pela empresa como uma primeira resposta a um incidente permite, efetuar uma cópia exata do disco rígido e da memória da máquina alvo, além de permitir efetuar pesquisas por expressões, identificando e recolhendo todos os dados relevantes sobre as mesmas. Possibilita ainda a visualização de imagens, do correio eletrónico, do histórico da *Internet*, entre outras informações [10].

O conceito desta ferramenta é bastante interessante já que permite a configuração de um conjunto de tarefas por especialistas forenses, que automatizam o processo de recolha de evidências logo após um incidente, através da utilização de uma *pendrive* USB. Mais fácil e rapidamente, os especialistas forenses poderão analisar os resultados obtidos em laboratório, sem terem de se deslocar ou de recolher o próprio computador.

### 2.1.3. Computer Online Forensic Evidence Extractor

Em Abril de 2009 [11], e após o acordo entre a Microsoft e o National White Collar Crime Center (NW3C), foi desenvolvida uma ferramenta designada por “Computer Online Forensic Evidence Extractor” (COFEE), com o intuito de auxiliar, em conjunto com os seus privilegiados conhecimentos, as organizações policiais na recolha de evidências de computadores através da abordagem *live forensics*, também através de uma *pendrive* USB.

Esta ferramenta foi distribuída pelas agências policiais dos 187 países pertencentes, em Outubro de 2009, à organização policial Interpol. No entanto, no mês seguinte (Novembro de 2009), foi disponibilizada pela Wikileaks [12]. Esta ferramenta foi desenvolvida pensando na recolha de informação nos sistemas operativos Windows, implicando a prévia configuração da aplicação de modo a gerar o *script* para executar na máquina alvo as ferramentas necessárias à recolha da informação pretendida. Após a recolha da informação na máquina alvo, é necessário carregar essa informação na aplicação para gerar o respetivo relatório.

#### 2.1.4. The Volatility Framework

*Volatility Framework* [13] é um *software Open Source* desenvolvido em Python pela *Volatility Foundation*, com suporte para Windows, MacOS, Linux e Android, e projetado principalmente para executar o *dump* da memória e respetiva análise através da pesquisa de assinaturas e estruturas de dados da informação contida no *dump* de memória efetuado. Esta ferramenta está especialmente desenvolvida para ser utilizada no contexto de uma investigação forense, na resposta a incidentes ou mesmo na investigação de *malware*.

É uma ferramenta que contém um conjunto de *scripts* desenvolvidos para extraírem de um *dump* de memória informações tais como, entre outras [14]:

- processos em execução;
- ficheiros abertos para cada processo;
- ligações de rede estabelecidas;
- portos de rede abertos;
- lista de DLLs referenciadas para cada processo;
- sockets abertos.

#### 2.1.5. Win-UFO

O Windows Ultimate Forensic Outflow (Win-UFO) [15], é um programa de licença livre e foi concebido como resultado de uma parceria entre Scott White e Emory Casey Mullis, programador informático e um investigador forense reformado, respetivamente. Este *software* aglutina um conjunto de *scripts* e outros pequenos programas existentes, produzindo um relatório final aproveitando os resultados de cada um. Para isso, conta com diversas pequenas ferramentas de extração de informação, tal como demonstrado na Figura 2, onde se incluem as ferramentas da SysInternals e da Nirsoft, descritas nos pontos 2.2.1. “Sysinternals” e 2.2.2. “Nirsoft”.

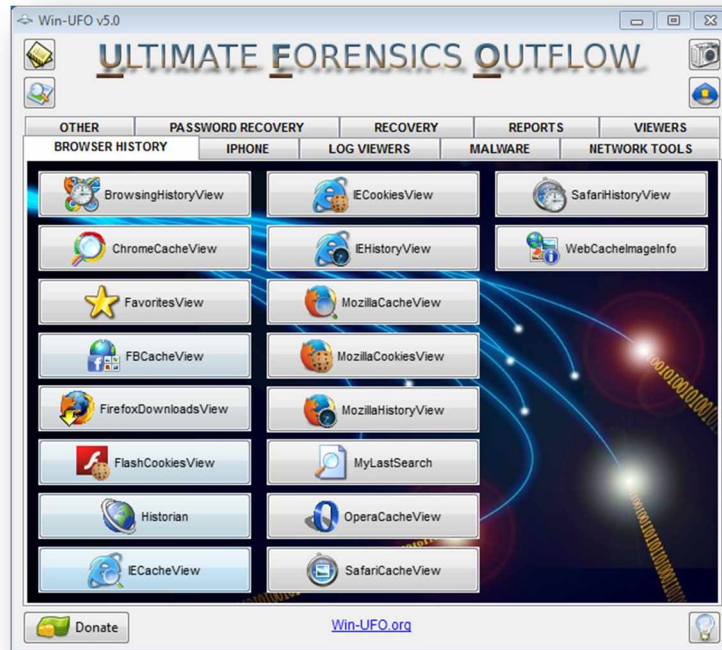


Figura 2 - Win-UFO

Esta é uma ferramenta com um executável que inclui todas as pequenas ferramentas necessárias para a sua execução, onde o utilizador poderá copiar toda a pasta de instalação para uma *pendrive* ou mesmo um CD ou DVD, executando a aplicação na máquina alvo. A aplicação no seu conjunto tem a capacidade de execução das seguintes tarefas, entre outras:

- listar as contas de utilizadores;
- conhecer as pesquisas realizadas na *Internet*;
- listar o histórico da *Internet* por utilizador;
- conhecer a localização de *drives* e partições encriptadas;
- recuperar dados eliminados;
- recuperar *passwords*;
- saber quais as contas de *Internet* que o utilizador está ligado;
- recuperar os *thumbnail* das imagens através do “thumbs.db”;
- verificação de virus e malware;
- pesquisa de dispositivos USB que já estiveram ligados ao computador;
- criação de relatório com os resultados da análise;
- visualização da cache dos *browsers* da *Internet*.

Esta aplicação tem um conceito bastante interessante, apesar de conter algumas limitações, como a deteção pelos antivírus das ferramentas relacionadas com as *passwords*, bem como a falta de automatização no seu principal objetivo aquando da sua utilização por investigadores forenses no âmbito de uma análise *Live Forensics*.

### 2.1.6. Mandiant Redline

Redline [16] é um *software* desenvolvido pela Mandiant, pertencente à empresa FireEye, e é uma ferramenta forense concebida para investigar sinais de atividade maliciosa, recolhendo e analisando diversas informações da máquina alvo, como processos, informações de registo, informações contidas na memória, entre outras. Apesar de ser uma ferramenta gratuita, conta com importantes características, como a possibilidade de visualizar as informações recolhidas através de uma *timeline*, que ajuda a dar resposta a como o *malware* entrou no computador.

A alusão desta ferramenta tem por base a sua capacidade de seleção das informações a recolher, sendo esta realizada através da aplicação Redline instalada na máquina do investigador, de modo a gerar o *script* de recolha das informações com as opções selecionadas. Posteriormente, é necessário que o investigador copie o conteúdo da pasta para uma *pendrive* ou disco externo e execute o *script* em *Batch* na máquina suspeita. Ainda como uma das principais características desta aplicação é a possibilidade de uma priorização na investigação através da análise da pontuação aos processos suspeitos, tendo em conta os designados “indicadores de compromisso” [17], que não são mais do que pequenos dados forenses que indicam uma intrusão.

## 2.2. Ferramentas de recolha de informação não forense

As ferramentas, consideradas mais significativas, de recolha de informação em sistemas operativos Windows, num âmbito de ataque, *hacking*, testes de penetração, ou mesmo *backup*, são descritas abaixo.

### 2.2.1. Sysinternals

As ferramentas SysInternals foram inicialmente conhecidas por *ntinternals*, desenvolvidas em 1996 por Mark Russinovich e Bryce Cogswell e divulgadas no *site* [www.sysinternals.com](http://www.sysinternals.com) [18], pertencente à sua empresa Winternals Software LP. Devido ao enorme sucesso, principalmente no mundo empresarial por administradores de sistemas, a Microsoft adquiriu a empresa e contratou Mark Russinovich, que continuou a



divulgar, através do agora Windows Sysinternals Suite [19], e a desenvolver as ferramentas, integrando-as nos sistemas operativos da Microsoft.

O objetivo no desenvolvimento destas ferramentas passou por compreender e resolver os problemas que o sistema operativo causava, sendo que o conceito destas ferramentas está necessariamente abrangido pelos seguintes fatores:

- não existir a necessidade de instalação;
- criar uma pegada digital (*footprint*) mínima no sistema operativo;
- ser um único ficheiro executável por ferramenta;
- suportar as várias versões do sistema operativo Microsoft Windows;
- não necessitar de reiniciar o computador.

Estas características tornaram estas ferramentas aliciantes aos administradores de sistemas e de redes, a investigadores forenses, mas também são eficazmente utilizadas em *hacking*.

A *SysInternals Suite* contém mais de 70 ferramentas com capacidade de recolher as mais variadas informações, dos utilizadores, processos, serviços, sistema, software instalado, memória e rede, entre muitas outras.

O objetivo deste documento não passa pela descrição de todas estas ferramentas, apesar de muitas delas terem objetivos semelhantes ao que é necessário atingir com o presente projeto. No entanto, as ferramentas diretamente relacionadas com este projeto serão descritas no Apêndice I.

### 2.2.2. Nirsoft

A par da SysInternals, também Nir Sofer, proprietário do *site* [www.nirsoft.net](http://www.nirsoft.net), desenvolveu um conjunto de pequenas ferramentas [20] que permitem a recolha de dados do sistema operativo da *Microsoft*. Das mais de 180 ferramentas disponibilizadas, todas foram desenvolvidas com um conceito semelhante ao da SysInternals, sendo ferramentas portáteis, sem necessidade de instalação, de licença *freeware* e com um único ficheiro executável.

Existe ainda a ferramenta NirLauncher [21], apresentada na Figura 3, que reúne mais de 180 das mais recentes ferramentas disponibilizadas, muitas são as de recolha de dados do computador. No entanto, e como a mesma figura revela, são quatro as ferramentas detetadas pelo antivírus, neste caso o Avira Free Antivírus 2015.

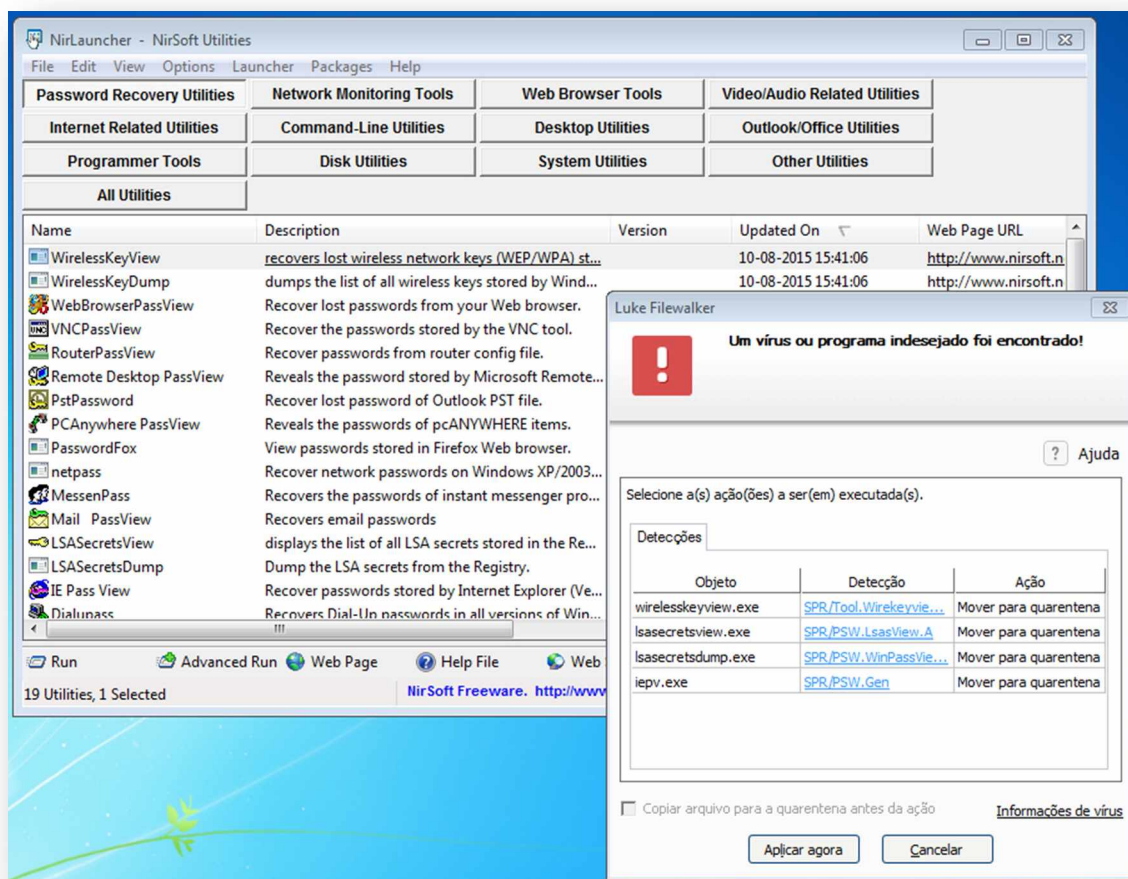


Figura 3 - NirLauncher

À semelhança do referido no ponto anterior, também as ferramentas da Nirsoft diretamente relacionadas com este projeto serão descritas no Apêndice I.

### 2.2.3. InfoHack

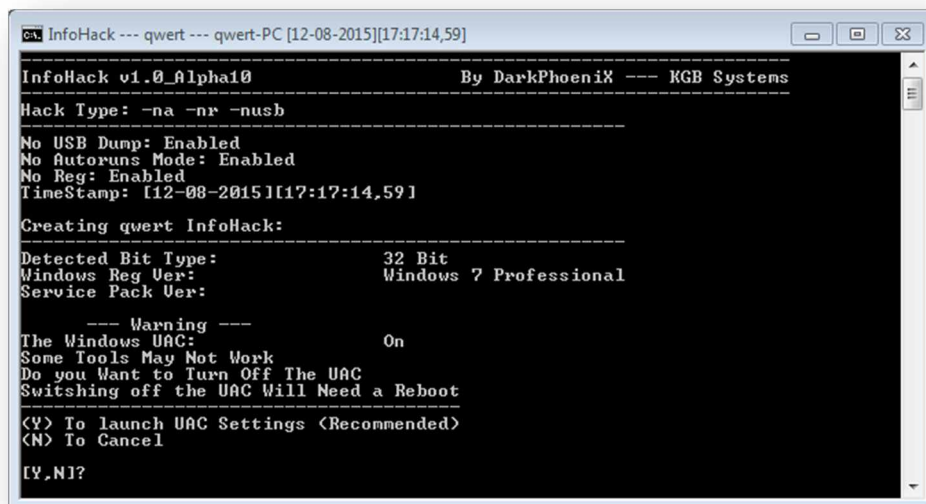
Em [22], *site* respeitante à distribuição de *software*, encontra-se divulgada uma ferramenta intitulada InfoHack. Esta foi disponibilizada pelo intitulado DarkPhoeniX, um membro de topo deste fórum.

Esta ferramenta tem especificamente como objetivo capturar informações de sistemas operativos Windows. Apesar de não existirem atualizações desde 2012, esta contém um conjunto de *scripts* e pequenas ferramentas de entre as quais se destaca a SysInternals e a Nirsoft.

Com a possibilidade de serem iniciados dois *scripts* na linguagem *batch*, um designado de "FastHack.bat", com uma duração aproximada a 15 segundos, e um outro designado de "InfoHack.bat" com uma duração de aproximadamente 2 minutos, esta ferramenta consegue recolher as seguintes informações, entre outras:

- ficheiros do registo NTUSER.DAT, SAM, SECURITY, SOFTWARE e SYSTEM;
- BIOS;
- informações de sistema;
- informações de utilizadores;
- histórico das pesquisas na *Internet*;
- ficheiros recentemente modificados;
- histórico dos dispositivos USB.

Esta ferramenta encontra-se desenvolvida de modo a permitir que os utilizadores executem um dos dois ficheiros *batch* disponibilizados, podendo estes encontrar-se numa *pendrive* USB. Seguidamente, o *script* será inicializado com a identificação do sistema operativo e criação da pasta onde todos os resultados serão guardados. Caso o *User Account Control* (UAC) se encontre ativo, será exibido um aviso, tal como ilustrado na Figura 4, alertando para este ser desligado de modo a permitir a execução de todas as pequenas ferramentas incorporadas no InfoHack. Assim, se o utilizador pretender a desativação do UAC, seleciona “Y” para que apareça a janela de opção do UAC permitindo a sua desativação e posterior execução de todas as ferramentas, sendo necessário reiniciar o computador para que o mesmo tenha efeito.

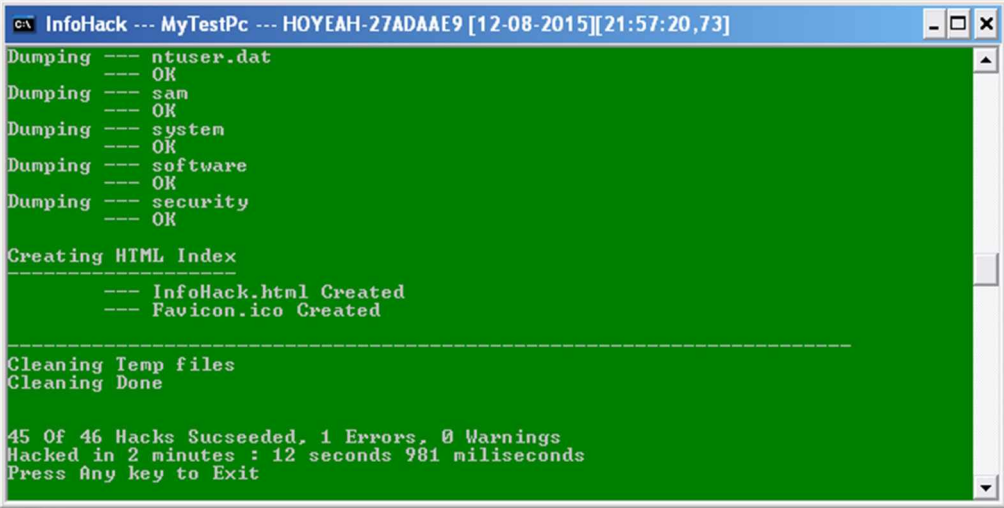


```
InfoHack --- qwert --- qwert-PC [12-08-2015][17:17:14,59]
-----
InfoHack v1.0_Alpha10                               By DarkPhoenix --- RGB Systems
-----
Hack Type: -na -nr -nusb
-----
No USB Dump: Enabled
No Autoruns Mode: Enabled
No Reg: Enabled
TimeStamp: [12-08-2015][17:17:14,59]
-----
Creating qwert InfoHack:
-----
Detected Bit Type:                               32 Bit
Windows Reg Ver:                               Windows 7 Professional
Service Pack Ver:
-----
--- Warning ---
The Windows UAC:                               On
Some Tools May Not Work
Do you Want to Turn Off The UAC
Switching off the UAC Will Need a Reboot
-----
<Y> To launch UAC Settings <Recommended>
<N> To Cancel
[Y,N]?
```

Figura 4 - InfoHack UAC Warning

É a própria aplicação que alerta o utilizador para este reinício, bastando ao utilizador premir uma qualquer tecla para o computador reiniciar.

Já com o UAC desativado é necessário executar novamente o *script* InfoHack, passando o fundo de preto para verde, assim que o mesmo termina. Mesmo com o UAC desativado, o *script* não consegue executar todas as ferramentas, devido principalmente à proteção ativa do antivírus. No entanto, foi necessário correr esta ferramenta no Windows XP, já que o mesmo não tem UAC, sem antivírus, para o *script* conseguir correr com sucesso 45 das 46 ferramentas, tal como exemplificado na Figura 5.



```
ca InfoHack --- MyTestPc --- HOYEAH-27ADAAE9 [12-08-2015][21:57:20,73]
Dumping --- ntuser.dat
      --- OK
Dumping --- sam
      --- OK
Dumping --- system
      --- OK
Dumping --- software
      --- OK
Dumping --- security
      --- OK

Creating HTML Index
-----
      --- InfoHack.html Created
      --- Favicon.ico Created
-----

Cleaning Temp files
Cleaning Done

45 Of 46 Hacks Succeeded, 1 Errors, 0 Warnings
Hacked in 2 minutes : 12 seconds 981 milliseconds
Press Any key to Exit
```

Figura 5 - InfoHack terminado

Como já referido, esta ferramenta gera uma pasta com o nome do utilizador ativo e o respetivo nome de domínio, onde são guardados todos os ficheiros com os resultados.

De acordo com o objetivo desta dissertação, esta ferramenta é interessante por efetuar a distinção entre sistemas operativos de 32 e de 64bits, adequando, desse modo, as ferramentas a executar, por ter o atributo “-np”, que permite a execução do *script* sem paragens, e também por proporcionar a visualização dos resultados através de um *browser*, sem ser necessário qualquer *software* extra.

### 2.2.4. Scripts

Em [23, 24, 25, 26], e em inúmeros outros exemplos de *scripts* de recolha de informações de sistemas operativos Windows, são frequentemente utilizadas as linguagens de *scripting* nativas da Microsoft (*Batch*, *JScript*, *VBScript*, *Windows Script Host* e desde o lançamento do Windows 7 o *PowerShell*) [27], por não necessitarem da instalação de interpretadores.

Muitos são os *scripts* desenvolvidos por administradores de sistema, ou responsáveis de segurança informática com objetivos de salvaguarda de informações (*backup*), ou gestão dos computadores nas organizações. Apesar destes objetivos não serem coincidentes com os pretendidos, estes *scripts* são facilmente customizáveis, adaptando-os aos nossos objetivos, podendo mesmo proceder-se à recolha das instruções pretendidas na construção de um *script* com os nossos objetivos.

Atualmente os administradores de sistema recorrem a *scripts* em PowerShell para atingir os seus objetivos de gestão [28]. No entanto, para a recolha de informação de computadores, a ferramenta *Windows Management Instrumentation Command-line* (WMIC) [29], apesar de ter mais de uma década e ter passado inicialmente despercebida, tornou-se bastante importante por permitir o rápido e fácil acesso a informações de sistema, permitindo também a sua integração em *scripts*. Exemplo disso é um pequeno *Batch script* [23] que possibilita a recolha de informação de sistema de computadores locais e remotos através da ferramenta *wmic*, como ilustrado na Figura 6.

```
94 REM Get Computer OS
95 FOR /F "tokens=2 delims='=' " %%A in ('wmic %cstring% %ustring% %pstring%
    os get Name /value') do SET osname=%%A
96 FOR /F "tokens=1 delims='|' " %%A in ("%osname%") do SET osname=%%A
97
98 REM Get Computer OS SP
99 FOR /F "tokens=2 delims='=' " %%A in ('wmic %cstring% %ustring% %pstring%
    os get ServicePackMajorVersion /value') do SET sp=%%A
100
101 echo done!
102
103 echo -----
104 echo System Name: %system%
105 echo Manufacturer: %manufacturer%
106 echo Model: %model%
107 echo Serial Number: %serialnumber%
108 echo Operating System: %osname%
109 echo Service Pack: %sp%
110 echo -----
```

Figura 6 - *Script* de recolha de informação de sistema

### 2.3. Hipótese de investigação

De acordo com o objetivo desta dissertação e tendo em conta a possibilidade de transferir dados da máquina alvo, optou-se então pela utilização da transferência local através de portas USB. Esta escolha teve por base a ponderação entre vários fatores, entre

os quais a deteção e monitorização de rede por parte dos mecanismos de defesa através da rede, como os IDS e *firewall*, a universalidade dos dispositivos com portas USB, e também a taxa de transferência de dados através da rede ou através das portas USB.

No que diz respeito às ferramentas a utilizar no projeto, esta opção recaiu em ferramentas com licenças de valor gratuito (*Open Source*, GNU, *freeware*, entre outras).

Formulou-se então a seguinte hipótese de investigação:

**“É possível desenvolver um sistema simples de utilizar, eficiente, com capacidade de superar mecanismos de defesa, para recolha de informações de sistema e qualquer tipo de ficheiros armazenados de forma parametrizável, em sistemas operativos Windows?”**

# CARACTERIZAÇÃO DOS SISTEMAS OPERATIVOS WINDOWS

---

Neste capítulo, são descritas as características do sistema operativo Windows Vista e seguintes, de acordo com a hipótese de investigação formulada. É descrita inicialmente uma evolução histórica dos sistemas operativos em análise, o funcionamento do registo, o comportamento dos sistemas operativos perante as portas USB e também as linguagens de *script* suportadas.

### 3. Caracterização dos sistemas operativos Windows

Para o desenvolvimento dos objetivos propostos nesta dissertação, é relevante conhecer o funcionamento interno dos sistemas operativos Microsoft Windows, quer pelo acesso às informações e suas localizações, quer pela possibilidade da utilização de comandos direcionados com o intuito de retirar apenas a informação necessária. Deste modo, será abordada a evolução dos sistemas operativos em questão, bem como a sua estrutura e funcionamento.

#### 3.1. Evolução histórica

Desde os primórdios da Microsoft, inicialmente uma parceria entre Bill Gates e Paul Allen [30], que são constantes os lançamentos de novos sistemas operativos, como podemos observar na Figura 7, fazendo desta empresa uma das mais valiosas do mundo.

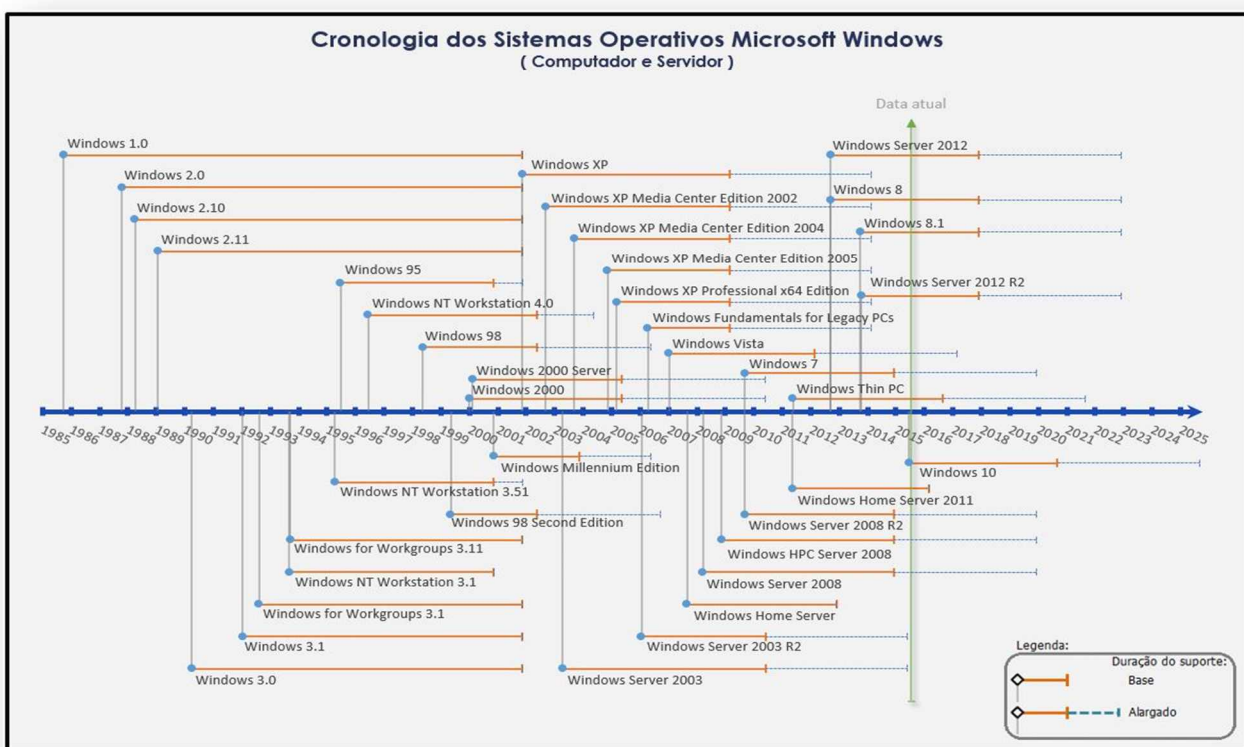


Figura 7 - Cronologia do lançamento e duração de Sistemas Operativos Microsoft Windows para Computadores e Servidores

Nesta Figura é possível observar um resumo de todos os sistemas operativos já lançados pela Microsoft, para computadores e servidores, bem como a respetiva duração do suporte base e alargado, sendo que atualmente estes têm definidas durações não inferiores a 5 anos [31].



Dominante no mercado com os seus sistemas operativos Windows, a Microsoft também fabrica *hardware* através da produção de periféricos, telemóveis e *tablets*.

O sucesso e explosão de vendas dos primeiros computadores com o sistema operativo Windows fez com que a Microsoft só mais tarde definisse a data de 31 de Dezembro de 2001, como data limite do suporte à maioria dos sistemas operativos Windows iniciais, desde o Windows 1.0 ao Windows 95. Deste modo, a política da empresa no que diz respeito ao desenvolvimento e à correção de problemas, poderia focar-se nos sistemas operativos mais recentes. Com o Windows NT Workstation 3.51, principalmente pelo seu alvo serem as empresas, surgiu a necessidade de prolongar o suporte, sendo definido um período de suporte alargado pela primeira vez. Este suporte alargado foi definido para serem efetuadas as correções a nível de segurança e o suporte a incidentes [31].

### 3.2. Registo

O registo do Windows é considerado pela própria Microsoft, como uma base de dados hierárquica centralizada, onde são armazenadas informações necessárias à configuração do sistema, e o seu desenvolvimento acompanha a evolução das diferentes versões dos sistemas operativos Microsoft Windows.

Muitas das informações contidas no registo são bastante relevantes por conterem informações dos utilizadores e da utilização destes sistemas.

*“A central hierarchical database in Windows ... used to store information necessary to configure the system for one or more users, applications, and hardware devices. The Registry contains information that Windows continually references during operation, such as profiles for each user, the applications installed on the computer and the types of documents each can create, property sheet settings for folders and application icons, what hardware exists on the system, and which ports are being used.”*

*Microsoft Computer Dictionary [32]*

Assim, é bastante pertinente a análise do registo do Windows, sendo esta prática corrente em análises forenses. Estas são informações que os sistemas operativos Microsoft continuamente referenciam no decorrer do seu funcionamento (e.g.: o registo é consultado quando é modificado um ficheiro, executando a aplicação correspondente ao mesmo com as configurações definidas).

As informações armazenadas no registo podem ser acedidas através de diversas aplicações. Apesar disso, os sistemas operativos Windows têm pré-instaladas várias

ferramentas de acesso ao registo por linha de comandos, como o “reg.exe” e o “regini.exe”, ou então através de uma aplicação específica, o Editor de Registo ou “regedit.exe”, localizado em “c:/Windows/regedit.exe”<sup>1</sup>, tal como ilustrado na Figura 8.

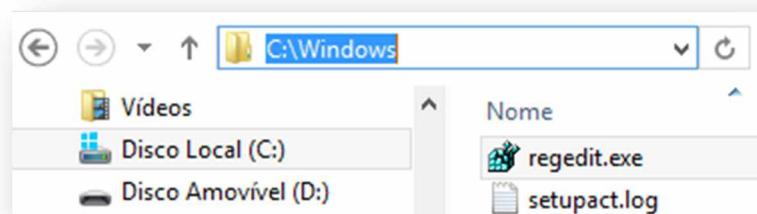


Figura 8 - Localização do Editor de Registo

No entanto, existem também outras ferramentas, externas ao sistema operativo com capacidade de acesso ao registo, como várias das ferramentas da SysInternals [19].

Seguidamente é descrita a estrutura do registo do Windows, bem como o acesso aos seus ficheiros e respetiva análise.

### 3.2.1. Estrutura lógica do registo do Windows

O registo do Windows é composto fisicamente no disco por um conjunto fechado de ficheiros, designados por *hives* (ramificações) [33].

<i>Registry Hive</i>	<i>Localização dos ficheiros dos hives principais</i>
HKLM\SAM	%SystemRoot%\System32\Config\sam
HKLM\SECURITY	%SystemRoot%\System32\Config\security
HKLM\SOFTWARE	%SystemRoot%\System32\Config\software
HKLM\SYSTEM	%SystemRoot%\System32\Config\system
HKLM\HARDWARE	volatile hive
HKU\Default	%SystemRoot%\System32\Config\Default
HKU\ <sid account&gt;<="" local="" of="" service="" td=""> <td>%SystemRoot%\ServiceProfiles\LocalService\Ntuser.dat</td> </sid>	%SystemRoot%\ServiceProfiles\LocalService\Ntuser.dat
HKU\ <sid account&gt;<="" network="" of="" service="" td=""> <td>%SystemRoot%\ServiceProfiles\NetworkService\Ntuser.dat</td> </sid>	%SystemRoot%\ServiceProfiles\NetworkService\Ntuser.dat
HKU\ <sid of="" td="" username&gt;<=""> <td>\Users\%UserProfile%\Ntuser.dat</td> </sid>	\Users\%UserProfile%\Ntuser.dat
HKU\ <sid of="" td="" username&gt;_classes<=""> <td>\Users\%UserProfile%\AppData\Local\Microsoft\Windows\UsrClass.dat</td> </sid>	\Users\%UserProfile%\AppData\Local\Microsoft\Windows\UsrClass.dat

<sup>1</sup> Para os sistemas operativos que não se encontram instalados na unidade C, deve utilizar-se a unidade onde o sistema operativo está instalado.

Tabela 1 - Localização dos ficheiros dos *hives* principais

Cada *hive* está organizado numa estrutura lógica hierárquica “em árvore” armazenando as informações em chaves e subchaves, descritas de seguida.

**Hives do registo** (*Root Keys*) são caracterizados pelo prefixo “HKEY\_”, abreviatura de “Handle to a Key”. São 5 os *hives* principais, tal como apresentado na Figura 9, armazenadas nos diversos ficheiros que compõem o registo, apesar de apenas o HKEY\_USERS e o HKEY\_LOCAL\_MACHINE serem considerados como os verdadeiros *hives*, sendo os restantes atalhos ou *aliases* para ramificações dentro destes [34].

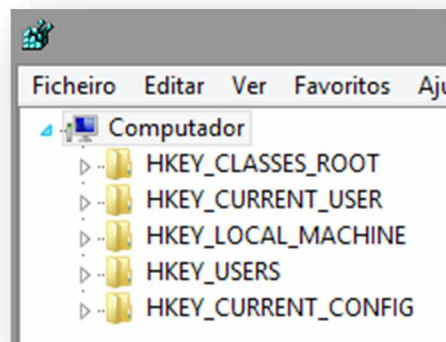


Figura 9 - Ramificações do registo (Win 8.1)

Para uma melhor contextualização cada um dos *hives* é seguidamente descrito:

- HKEY\_CLASSES\_ROOT contém configurações essenciais do sistema operativo Windows, bem como as necessárias associações de ficheiros e outros elementos;
- HKEY\_CURRENT\_USER inclui o perfil, bem como as configurações personalizadas do utilizador autenticado no sistema no momento da sua utilização. Este inclui variáveis de ambiente, grupos de programas pessoais, definições do ambiente de trabalho, ligações de rede, impressoras e preferências específicas de *software*. Como este ramo é específico do utilizador autenticado no momento, é necessariamente criado sempre que um utilizador se autentica, caso seja a primeira vez que esse utilizador se autentica, e é recolhido o perfil do utilizador por defeito armazenado no ficheiro “C:\Users\Default\Ntuser.dat”;

- HKEY\_LOCAL\_MACHINE contém informações referentes ao computador em análise, tais como, informações do *Hardware*, Sistema Operativo, tipos de barramento, memória do sistema, *drivers* dos dispositivos ou mesmo parâmetros de controlo de arranque;
- HKEY\_USERS armazena os perfis de todos os utilizadores já autenticados no sistema;
- HKEY\_CURRENT\_CONFIG contém informações sobre o perfil de *Hardware* utilizado pelo computador em análise durante o arranque do Sistema Operativo.

**Chaves do registo** são o nível abaixo dos ramos no registo, tal como exemplificado na imagem Figura 10 com as chaves de nome “Software” e “System”, pertencentes à ramificação “HKEY\_CURRENT\_CONFIG”.

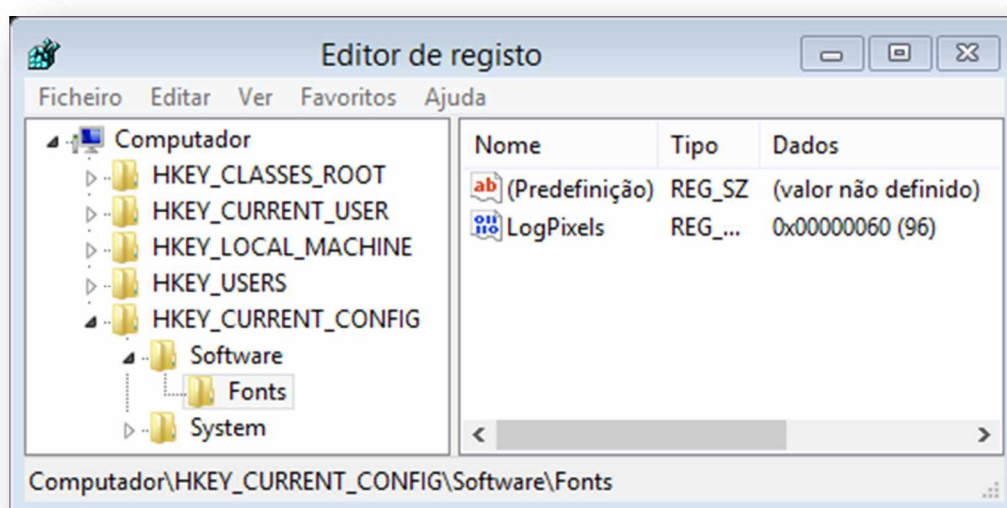


Figura 10 - Chaves e Subchaves do registo

**Subchaves do registo.** Esta é a pasta no nível mais baixo da estrutura do registo, onde são armazenadas as informações do registo, como exemplificado na Figura 10 com a subchave “Fonts”.

**Valores do registo** são as informações visíveis do lado direito da janela do editor de registo, tal como se visualiza na Figura 10, podendo ver-se ainda 3 colunas com o nome do valor, o tipo de dados e os dados.

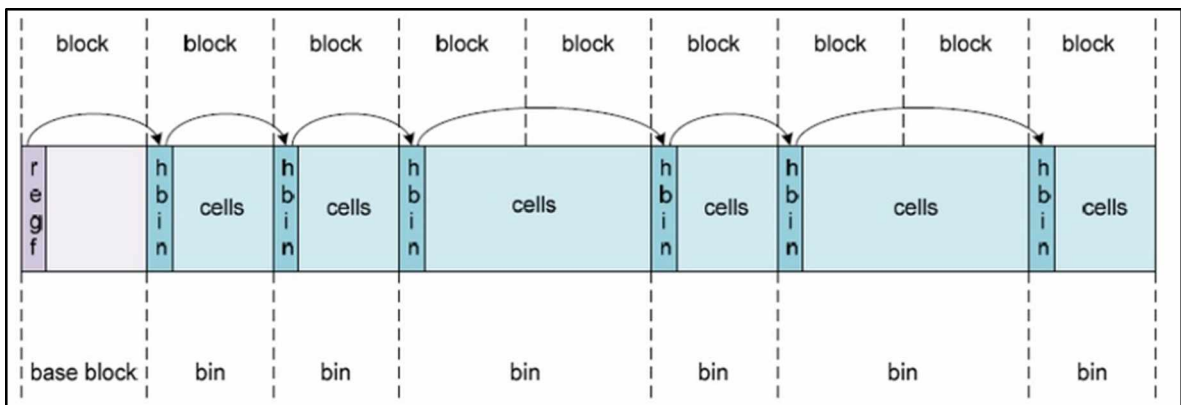
É ainda de referir que as versões dos sistemas operativos Windows de 64-bit possibilitam a instalação de aplicações de 32-bit. No caso de serem instaladas aplicações

de 32-bit num sistema operativo de 64-bit, estas são instaladas especificamente na pasta %SystemRoot%\Programs(x86), sendo também criadas chaves no registo equivalentes às aplicações de 64-bit (e.g.: o “HKE\_LOCAL\_MACHINE\Software” tem como seu equivalente de 32-bit o “HKE\_LOCAL\_MACHINE\Software\Wow6432Node”), existindo também uma versão de 64-bit específica do editor de registo, no seguinte comando:

```
"%systemroot%\syswow64\regedit.exe"
```

### 3.2.2. Estrutura interna do registo do Windows

Cada *hive* de registo encontra-se constituído internamente por *clusters* de blocos [35], iniciado por um *header* designado por “*Base Block*”, e com a dimensão de 4096 bytes, que inclui a informação global do *hive*, incluindo a sua assinatura como apresentado na Figura 11.



fonte: "Registry forensics" [36]

Figura 11 - Estrutura interna do hive

Cada bloco (*bin*) contém um *header*, designado por *hbin*, contendo a sua assinatura. No caso de o bloco ser de uma célula de informação, esta assinatura poderá ser de 6 tipos diferentes: *key cell* (nk), *value cell* (vk), *security descriptor cell* (lf, lh, ri, li), *sub-key list cell*, *value-list cell* e *data cell*. Estes dois últimos não contêm *header* mas sim apenas informações.

Os pontos no bloco base para a primeira estrutura *hbin* integram o *offset* para a *root key* do *hive* do registo.

No que diz respeito ao *offset* e dimensão de cada um destes campos no bloco base é possível identificar os mesmos na Figura 12.

Offset	0	1	2	3	4	5	6	7	8	9	A	B	C	D	E	F	
00000000	72	65	67	66	F7	05	00	00	F7	05	00	00	12	DB	EF	1E	regf+
00000010	E5	A5	CC	01	01	00	00	00	03	00	00	00	00	00	00	00	÷
00000020	01	00	00	00	20	00	00	00	00	50	00	00	01	00	00	00	Ûi
00000030	5C	00	53	00	79	00	73	00	74	00	65	00	6D	00	52	00	P
00000040	6F	00	6F	00	74	00	5C	00	53	00	79	00	73	00	74	00	\ S y s t e m R
00000050	65	00	6D	00	33	00	32	00	5C	00	43	00	6F	00	6E	00	o o t \ S y s t
00000060	66	00	69	00	67	00	5C	00	53	00	41	00	4D	00	00	00	e m 3 2 \ C o n
																	f i g \ S A M

Fonte: Registry forensics [36]

Figura 12 - Offset e dimensão dos campos no bloco base

O Sistema Operativo Windows organiza a informação no registo, nos chamados “contentores de informação”, também designados por células, como observável na Figura 11. Cada célula poderá conter “uma chave de registo, uma lista de subchaves, um valor, um descritor de segurança ou mesmo uma lista de valores chave”, sendo que cada célula é definida pelo seu tipo.

### 3.2.3. Acesso aos ficheiros do registo

O acesso ao registo pode ser efetuado através da aplicação “regedit.exe” integrada por defeito no sistema operativo. No entanto, por razões de segurança o sistema operativo Windows não permite o acesso a todos os ficheiros do registo. Deste modo, o acesso aos mesmos deverá ocorrer sem o sistema iniciado, acedendo ao disco do nosso sistema alvo através de um segundo sistema operativo (e.g.: através de um *livecd* Linux). Este método não consegue recolher os *hives* voláteis como o “HKLM\HARDWARE”, uma vez que o sistema não está iniciado. Já a ferramenta Erunt [37] possibilita a obtenção de todos os ficheiros do registo, incluindo os ficheiros referentes a *hives* voláteis, dado que permite a cópia dos ficheiros do registo com o sistema iniciado.

### 3.2.4. Análise do registo

Existem dois modos de análise dos ficheiros do registo, através da análise manual utilizando ferramentas como o WinHex<sup>2</sup>, ou utilizando ferramentas de análise automática *offline*. Estas efetuam a seleção e tratamento da informação contida nos ficheiros do

<sup>2</sup> WinHex – Editor hexadecimal universal (<http://x-ways.net/winhex/>)

registo, sendo um desses exemplos a aplicação “Windows Registry Recovery” [38], ou mesmo a aplicação “Accessdata Registry Viewer” [39]. Estas aplicações permitem que sejam carregados os ficheiros de uma cópia de segurança do registo previamente efetuada, permitindo a análise de toda a informação que o registo continha no momento da cópia de segurança.

### 3.3. Dispositivos USB

A interface USB é utilizada para a comunicação entre todo o tipo de dispositivos. Sofrendo várias evoluções desde 1996, ano em que surgiu com a sua versão 1.0. [40]. Atualmente a versão mais generalizada é a 2.0, atingindo taxas de transferência teóricas na ordem dos 480Mb/s. Os dispositivos mais recentes já contêm ligações USB versão 3.0, atingindo o seu limite máximo de transferência teórica de 5Gbp/s, que é superior às várias versões do IEEE 1394 (FireWire), e eSata, ambas com cerca de 3,2Gb/s. Apesar de já existir o USB versão 3.1, com taxas de transferência teórica de 10Gb/s, estas são em muito inferiores à tecnologia ThunderBolt, atingindo estas valores de 40Gb/s, como podemos observar n Gráfico 1 - Taxas de transferência por tipo de ligação. **Erro! A origem da referência não foi encontrada..**

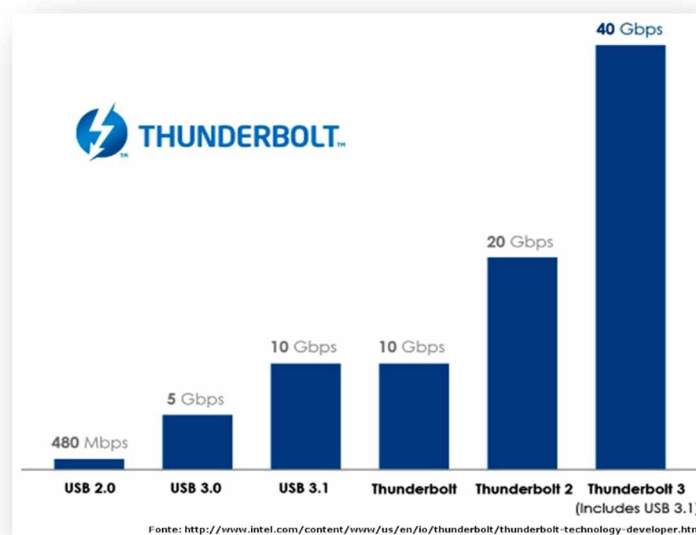


Gráfico 1 - Taxas de transferência por tipo de ligação

Tendo por base o estudo realizado no estado da arte, a seleção do dispositivo para o desenvolvimento desta dissertação, no que diz respeito à conectividade com a máquina alvo, recaiu sobre dispositivos com a interface USB, por se encontrar disponível em todos os computadores, tendo sido ponderadas também as taxas de transferência que este tipo

de conectividade oferece. Outro fator a salientar pela importância neste trabalho de dissertação, é facto deste interface conter alimentação incorporada, não requerendo de alimentação externa para alimentar os seus dispositivos. Estes são configurados pelo sistema operativo na primeira utilização, armazenando no registo informações sobre o dispositivo, para não ser efetuada nova configuração numa segunda ligação. Em [41], artigo publicado em 2012 por A. J. Tanushree Roy, as informações armazenadas pelos sistemas operativos são o foco principal, sendo de seguida descritas algumas destas informações.

A maioria dos dispositivos utilizados hoje em dia são detentores da tecnologia “*plug-and-play*”, dispoindo assim do *firmware* necessário ao seu funcionamento no sistema operativo. Na primeira vez que o dispositivo é ligado ao computador, o sistema irá obter nesse *firmware* informações como a identificação, descrição e fabricante do dispositivo, criando deste modo as seguintes chaves de registo [41]:

- HKEY\_LOCAL\_MACHINE\SYSTEM\ControlSet00x\Enum\USBSTOR\<Device\_class>\<device\_unique\_id>\
- HKEY\_LOCAL\_MACHINE\SYSTEM\ControlSet00x\Control\DeviceClasses\{<disk\_devices\_GUID>\
- <device\_class#device\_unique\_id#{disk\_devicesGUID}>\
- HKEY\_LOCAL\_MACHINE\SYSTEM\ControlSet00x\Control\DeviceClasses\{<volume\_devices\_GUID>\
- <STORAGE\_RemovableMedia#ParentId\_Prefix#{volume\_devices\_GUID}>\
- HKEY\_LOCAL\_MACHINE\SYSTEM\ControlSet00x\Enum\Storage\RemovableMedia\<ParentID\_Prefix>\

Os sistemas operativos Microsoft Windows armazenam informações dos dispositivos USB que se ligam ao sistema pela primeira vez. Estas são armazenadas no ficheiro “%WINDIR%\setupapi.log”, para sistemas operativos Windows XP/2000/2003, ou nos ficheiros “%WINDIR%\inf\setupAPI.dev.log” e “%WINDIR%\inf\setupapi.app.log”, para os *logs* de eventos relacionados com dispositivos e instalações de *drivers*, e instalações de aplicações, respetivamente, nos sistemas operativos Windows Vista/7/8 [42]. Através do ficheiro



“**setupAPI.dev.log**” é-nos também possível verificar a hora a que o dispositivo esteve pela última vez ligado ao sistema.

Já a letra atribuída pelo sistema ao dispositivo é armazenada na chave:

**HKEY\_LOCAL\_MACHINE\SYSTEM\MountedDevices**

É por esta chave de registo que se torna possível a um investigador forense relacionar a letra atribuída pelo sistema ao dispositivo USB, ou mesmo o perfil do utilizador pelo qual o dispositivo foi ligado ao sistema. A verificação da hora corrente do sistema pode ser verificada pela seguinte chave de registo:

**HKEY\_LOCAL\_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Time**

Já a chave de registo:

**HKEY\_LOCAL\_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Explorer\RecentDocs\**

permite as verificações mais importantes para um investigador forense, uma vez que possibilita a verificação da utilização do dispositivo para copiar ou mover ficheiros de ou para o dispositivo através do explorador do Windows, ou verificar se algum ficheiro foi executado através de duplo clique do rato.

Já que existe a possibilidade de terem sido copiados ou movidos ficheiros para ou do dispositivo por outros métodos que não os regulares do Windows, é possível verificar se um determinado ficheiro foi modificado, acedido ou criado (MAC) através do seu tempo MAC, que não é mais que o registo da última data/hora de modificação, acesso e criação. No entanto, este registo poderá ser desativado através da alteração para 0 da seguinte chave de registo:

**HKEY\_LOCAL\_MACHINE\SYSTEM\CurrentControlSet\Control\FileSystem\NtfsDisableLastAccessUpdate**

O registo permite investigar os nomes dos ficheiros utilizados recentemente, já que surgem quando um determinado utilizador escreve nas caixas de diálogo Abrir, Guardar ou outras do mesmo estilo do explorador do Windows. Estas caixas de diálogo apresentam uma lista dos ficheiros modificados recentemente “*Most Recent Used*” (MRU) e podemos obter esta informação através da chave de registo **OpenSaveMRU**, no

### 3.4. Segurança nos sistemas operativos Windows

Windows XP/2000/2003 ou através do **OpenSavePidLMRU**, para o Windows Vista ou superior [43], tal como apresentado na Figura 13.

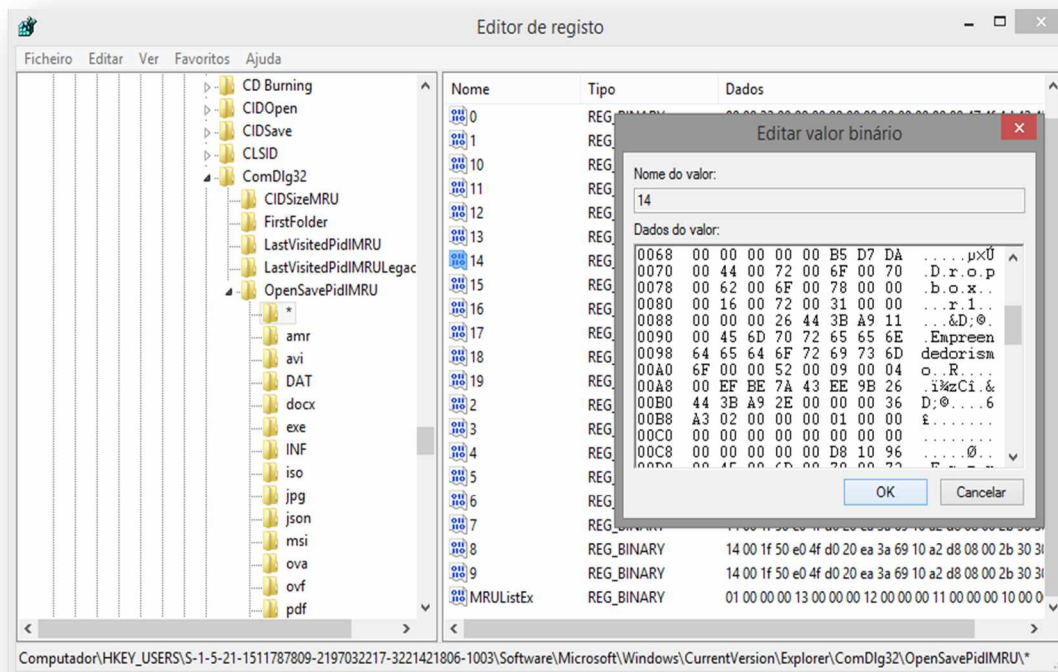


Figura 13 - Lista dos ficheiros modificados recentemente

É ainda importante referir que o sistema armazena as chaves referentes a esta lista de ficheiros individualmente por utilizador e por extensão de ficheiro, pertencendo desse modo ao *hive* de registo correspondente ao perfil do utilizador, tal como apresentado na Figura 13.

### 3.4. Segurança nos sistemas operativos Windows

Os sistemas operativos Microsoft têm sofrido uma enorme evolução a nível da segurança dos sistemas e dados do utilizador. Esta tem sido uma preocupação da Microsoft, bem patente nos tópicos seguintes:

#### 3.4.1. Windows Vista

O Windows Vista surgiu no início de 2007 com várias melhorias de segurança em relação aos antecessores, sendo mesmo apelidado [44] do mais seguro e confiável sistema operativo Microsoft até então. O Windows Vista sofreu desenvolvimentos de segurança com vista à proteção dos computadores e de ameaças como *malware*, sendo as principais medidas de segurança as seguintes:

- *User Account Control (UAC)* — Esta foi a principal medida de segurança implementada e na qual o sistema operativo ficou conhecido ao nível de segurança. O UAC permite que um utilizador com privilégios limitados preencha as credenciais de administrador e efetue alterações ao sistema, ou para executar determinados programas com privilégios de administrador enquanto os restantes continuam com privilégios restritos;
- *Internet Explorer* — O *browser* nativo foi alvo de melhorias nos filtros de proteção contra *malware* e ataques por *phishing* e *spoofing*. Outra melhoria foi permitir ao utilizador facilmente verificar na barra de estado se o certificado do *site* se encontra válido;
- *Windows Defender* — Através da sua proteção em tempo real, o Windows Defender consegue eliminar muitos tipos de *malware*, ajudando a manter a integridade do sistema;
- *Firewall* — Apesar do Windows já trazer uma *firewall* nativa desde o Windows XP SP2, esta trouxe melhorias ao nível do filtro de aplicações permitindo aos administradores o bloqueio da comunicação por rede e também por permitir a configuração através das políticas de grupo;
- *Windows Service Hardening* — Esta foi uma característica de segurança implementada para combater as modificações ao nível dos serviços, restringindo as alterações aos serviços considerados críticos ao sistema, como os do sistema de ficheiros, do registo ou de rede. Assim são mitigados os possíveis ataques na tentativa de instalação de *malware*;
- *Network Access Protection Infrastructure* — Considerado um agente que consegue proteger o computador de ataques por acesso remoto. Este agente assegura que as últimas atualizações de segurança se encontram instaladas e define apenas um número limitado de acessos por rede;
- *BitLocker* — É um sistema de encriptação permitindo aos utilizadores a encriptação de toda a unidade do disco rígido. Encontra-se descrito com maior detalhe no ponto 1.1.15. “BitLocker”;
- *New authentication architecture* — O objetivo da Microsoft foi de disponibilizar uma *Application Programming Interface (API)* para permitir o desenvolvimento de novos métodos de autenticação, como por via de dados biométricos ou por *tokens*. Esta nova arquitetura permite também a

autenticação por um Número de Identificação Pessoal (PIN) e melhoramentos à autenticação por Kerberos e *smart card*.

- *autorun* — A execução automática de *software* (*autorun*) acontece quando um CD, DVD ou dispositivo amovível é ligado ao sistema e sempre que o ficheiro “*autorun.inf*” é encontrado na raiz do disco, executando automaticamente as instruções nele contidas. Devido aos problemas de segurança inerentes a esta funcionalidade, no Windows Vista, esta funcionalidade vem desativada por defeito, integrada no “AutoPlay”.

#### 3.4.2. Windows 7

O **Windows 7** surgiu em 2009 com algumas novidades de segurança [45], onde várias foram as melhorias às tecnologias de segurança existentes, principalmente ao nível do reforço das competências das políticas de grupo. Das melhorias a tecnologias já existentes, seguem-se as mais relevantes:

- *ActiveX* — Utilizado como um suplemento ao Internet Explorer para permitir a melhoria da experiência de navegação, é requisito de alguns *sites*. A Microsoft ativou o serviço de ActiveX, por defeito, no Windows 7, e permitiu que este controlo fosse instalado através das políticas de grupo, já que utilizadores restritos não o poderiam efetuar por falta de permissões;
- *BitLocker Drive Encryption* — A Microsoft desenvolveu o BitLocker para abranger discos fixos e poder ser utilizado em unidades amovíveis, como os discos externos e as *pendrives* USB, designando-o de “BitLocker To Go”;
- *Encryption File System* (EFS) — Esta é uma tecnologia utilizada para armazenar ficheiros encriptados em unidades com o sistema de ficheiros NTFS. O EFS foi desenvolvido para, no Windows 7, suportar também algoritmos de criptografia *elliptic curve cryptography* (ECC) e *Rivest-Shamir-Adleman* (RSA), além dos algoritmos já anteriormente suportados como o *Advanced Encryption Standard* (AES) e o *Secure Hash Algorithm* (SHA);
- *Kerberos Authentication* — O sistema de autenticação kerberos passou a utilizar por defeito cifras AES e RC4, descontinuando as cifras DES;
- *NTLM Authentication* — Nas políticas de segurança foi definida uma encriptação mínima de 128bit nos sistemas baseados em NTLM;

- *Security Auditing* — Passou a ser possível a configuração de políticas de auditoria de segurança centralizada através das políticas de grupo;
- *TPM Management* — Foram efetuadas melhorias que possibilitam o reinício do bloqueio do valor do *Trusted Platform Module* (TPM). Este é um módulo que permite a segurança de *hardware* através da introdução de chaves criptográficas nos dispositivos, tendo a capacidade de se bloquear para impedir a manipulação ilícita ou um ataque;
- *User Account Control* — As melhorias no UAC passaram pelo aumento do número de tarefas que o utilizador restrito pode efetuar, pela configuração do UAC no painel de controlo com permissões de administrador, e também por novas configurações através das políticas de segurança.

A nível das funcionalidades de segurança seguem-se as mais relevantes implementadas com o lançamento:

- *AppLocker* — Basicamente é uma nova versão do “*Software Restriction Policies*” introduzido com o Windows XP, permitindo agora o bloqueio de aplicações não só pelo nome, mas também pelo nome da empresa que a desenvolve, pelo nome do ficheiro, pelo tipo de ficheiro ou mesmo pela versão;
- *Suite B Cryptography* — Adoção do grupo de algoritmos criptográficos “*Suite B*” aprovados pela Agência Nacional de Segurança dos Estados Unidos da América (NSA), por estes constituírem o *standard* em *software* de encriptação;
- *Enhanced Storage Access* — O acesso a dispositivos de armazenamento foi melhorado para permitir o suporte a certificados e autenticação com *password*;
- *Negotiate Authentication Protocol* — Este é um protocolo utilizado na autenticação e encriptação, tendo sido desenvolvida uma extensão a este protocolo para permitir os novos algoritmos criptográficos;
- *Internet Explorer 8.0* — A segurança do *browser* Internet Explorer contemplou novas funções de defesa, prevenindo ataques de *exploits* por *browser*, vulnerabilidades referentes ao servidor *web* e ataques de engenharia social. A utilização do SmartScreen no Internet Explorer 8 permite alertar os utilizadores para *sites* não confiáveis;
- *Managed Service Accounts* — Esta é também uma nova característica desenhada para adequar o tipo de conta à aplicação ou serviço que a necessita,

permitindo a execução isolada de serviços com privilégios diferentes dos restantes;

- *Online Identity* — Esta característica permite a autenticação dos utilizadores em redes locais através de uma identidade *online*;
- PKU2U — Significando “*Public Key Cryptography Based User-to-User*”, permite a autenticação ponto-a-ponto, principalmente entre partilhas de rede;
- *Smart Card Plug and Play* — Esta é uma característica desenvolvida para suportar o “Plug and Play” dos “smart card” com o *standard* do “*National Institute of Standards and Technology*” (NIST), o “*Personal Identity Verification*” (PIV). É assim garantida a compatibilidade em situações como o desbloqueio do BitLocker, ou início de sessão com “Smart card”, ou ainda na assinatura digital de documentos;
- *NTLM Authentication Restriction* — A “*NT LAN Manager*” (NTLM) é um conjunto de protocolos utilizados pela Microsoft para providenciar autenticação, integridade e confidencialidade dos dados. Foram introduzidas novas políticas de segurança para ajudar a analisar e restringir a utilização da autenticação via NTLM em ambientes empresariais, melhorando a gestão do protocolo NTLM;
- Windows Biometric Service — Foi introduzido no início de sessão por via biométrica, contemplando a respetiva elevação de privilégios através do UAC, bem como a possibilidade de gestão através das políticas de grupo;
- TLS v1.2 — Foi implementado o protocolo “*Transport Layer Security*” (TLS) versão 1.2 na segurança das comunicações por rede.

#### 3.4.3. Windows 8 e 8.1

O Windows 8 surgiu no final de 2012. A segurança no Windows 8 foi desenvolvida com base na segurança existente no Windows 7 e teve uma forte aposta na proteção dos utilizadores do acesso não autorizado e de resistir a ameaças de *exploits* e *malware* [46].

O Windows 8.1 teve o seu lançamento um ano após o lançamento do Windows 8, ficando conhecido como uma atualização ao Windows 8, apesar de a Microsoft o considerar um novo sistema operativo para o utilizador final. Contou com melhorias na experiência de utilização e personalização, e também com novas aplicações incorporadas no gestor de aplicações “Metro”. Contou também com várias melhorias de segurança a medidas já implementadas no Windows 8, das quais se destacam as melhorias nos

controles de acesso, e na aleatoriedade dos endereços de memória, mitigando os *exploits* que introduzem *software* malicioso por este modo.

São descritas de seguida as principais medidas de segurança implementadas e/ou melhoradas em ambos os sistemas:

Melhorias a tecnologias já existentes:

- AppLocker — Esta função foi atualizada para abranger as aplicações provenientes da “*Windows Store*”.
- SmartScreen — No Windows 8, o SmartScreen foi atualizado para abranger as aplicações, verificando a “reputação” da aplicação na sua primeira execução, prevenindo o utilizador de instalar aplicações com *malware*;
- Windows Defender — A ferramenta de *antispyware* nativa do Windows foi atualizada sendo agora equiparada a um antivírus, conseguindo detetar e eliminar uma vasta gama de *software* malicioso;
- Kernel — Na tentativa de anular os ataques com *exploits* e instalação de *malware*, a Microsoft efetuou melhorias de baixo nível no “*Address Space Layout Randomization*” (ASLR), restringindo também o acesso à memória;
- ACL Editor — O editor do *Access Control List* (ACL) foi atualizado para contemplar o novo *Dynamic Access Control*;
- Windows Firewall — A Firewall foi alvo de vários desenvolvimentos, entre os quais o bloqueio não só do tráfego de rede não autorizado na sua entrada mas também na saída do sistema;
- *Credential Locker* — Conhecido em português como gestor de credenciais, foi atualizado para abranger as aplicações da “*Windows Store*” e para permitir a sincronização entre dispositivos;
- *Kerberos protocol* — Várias foram as atualizações ao protocolo *Kerberos*, principalmente atualizações na redução de falhas e também na configuração e manutenção do centro de distribuição de chaves (KDC);
- Security audits — A ferramenta de auditorias de segurança e deteção de comportamentos anómalos foi alvo de melhorias de modo a proporcionar um relatório mais completo.

Novidades implementadas:

- *Secure Boot* — O “*Secure Boot*” é um sistema de prevenção do arranque do sistema, com *Unified Extensible Firmware Interface* (UEFI), quando um *bootkit* é detetado. Este é um dos tipos de *malware* mais perigosos, por se iniciar antes do sistema operativo e com isso ficar com acesso a todos os recursos do sistema, uma vez que os mecanismos de defesa ainda não se encontram ativos;
- *Trusted Boot* — Este é um sistema de verificação da integridade dos ficheiros de arranque, através do “*early launch antimalware*” (ELAM), sistema de verificação de *malware* de todos os ficheiros de arranque não certificados pela Microsoft;
- *Windows 8 Apps* — As aplicações do Windows 8 provenientes da “*Windows Store*” são executadas com privilégios muito limitados não tendo acesso a nível do sistema. São assim aplicações com um menor risco de conterem vulnerabilidades que possam ser exploradas por *malware* ou *exploits*;
- BitLocker — Na tecnologia de encriptação BitLocker foi desenvolvido o designado “*Encrypted Hard Drive*”. Este novo método de encriptação transpõe o processo de criptografia para o processador, melhorando o tempo do processo de encriptação e o desempenho do sistema. O BitLocker passou a poder ser ativado no momento da instalação, por se encontrar presente no *Windows Preinstallation Environment* (WinPE). Foi fornecida a possibilidade dos utilizadores alterarem o PIN e a *password* do BitLocker;
- *Trusted Platform Module* (TPM) — A tecnologia de proteção do arranque do sistema obteve novas funcionalidades ao nível da sua proteção e proteção *antimalware*. Foi ainda desenvolvido o “*key storage provider*” (KSP) facilitando a utilização do *Trusted Platform Module* (TPM);
- *Access Control* — Foram desenvolvidos novos recursos de controlo de acesso tais como a utilização de *Virtual Smart Cards* com certificados guardados no Windows 8 e a possibilidade da autenticação a dois fatores. Outra das novidades de controlo de acesso foi a possibilidade da substituição da autenticação através de *password* para o toque em diversos pontos numa imagem, facilitando a entrada principalmente em dispositivos com ecrã tátil. Foi implementado o *DirectAccess* que permite uma ligação segura através da



*Internet*. Foi também implementado o *Dynamic Access Control* para permitir o acesso a recursos partilhados com base em regras dinâmicas.

- *Security Policy Settings* — Foi desenvolvido um novo grupo de políticas de segurança como parte do *Group Policy Object* (GPO) e com novas medidas de segurança.

#### 3.4.4. Windows 10

O Windows 10 foi lançado em Julho de 2015, com novas melhorias na segurança dos dados e dos utilizadores, e com a atualização de tecnologias de segurança já existentes e algumas novidades [47]. No entanto, é de salientar que este sistema operativo contempla vários dispositivos além do computador de secretária:

- BitLocker — Este sistema de encriptação continua a sofrer constantes melhorias, tais como a incorporação de novas funcionalidades de encriptação e recuperação da chave do dispositivo através do *Azure Active Directory*. Outra nova funcionalidade foi o bloqueio da possibilidade de comunicação utilizada pelo *Direct Memory Access* quando o dispositivo é iniciado. Foi criada uma nova política de grupo para a configuração de recuperação antes do arranque;
- Microsoft Edge — Lançado juntamente com o Windows 10, este *browser* foi desenvolvido tendo em conta todo o historial de vulnerabilidades do Internet Explorer. A Microsoft resolveu não adotar módulos com mais vulnerabilidades e isso poderá trazer alguma segurança ao Edge. No entanto, este *browser* continua a necessitar de muita atenção para conseguir substituir o Internet Explorer;
- *Credential Guard* — Esta é uma inovadora funcionalidade com o objetivo de armazenar as credenciais do utilizador através de um sistema de virtualização que permite o acesso apenas a *software* de sistema privilegiado;
- Device Guard — Esta é a resposta da Microsoft às ameaças de *bootkit*, uma nova funcionalidade que utiliza o novo sistema de segurança baseado em virtualização para proteger o *hardware* quando o utilizador tenta executar uma aplicação não confiável;
- *Microsoft Passport* — Este é o novo sistema de autenticação do Windows 10. Consiste na utilização dum dispositivo e do *Hello*, um sistema de autenticação biométrico, ou um número PIN, efetivando assim a autenticação a dois passos.

No entanto, Este PIN numérico poderá facilitar a entrada no sistema a terceiros, caso sejam utilizados números como os de identificação pessoal.

- *Security auditing* — Com o Windows 10 também o *Security Audit* foi atualizado, contando agora com duas novas subcategorias e vários novos eventos.

#### **3.4.5. Análise crítica das evoluções de segurança dos sistemas operativos Windows**

Com base nos pontos anteriores é possível atestar a importância do Windows Vista para a atual segurança dos sistemas operativos Windows. Apesar das expectativas falhadas enquanto Sistema Operativo, foi sem dúvida um marco na implementação de novas tecnologias de segurança, nas suas mais variadas vertentes, desde a proteção *antimalware*, o escalonamento de privilégios, as tecnologias de encriptação, a execução automática de *software*, a proteção de rede e *Internet*, entre várias outras.

Os sistemas operativos sucessores ao Windows Vista desempenharam um papel importante na consolidação e aperfeiçoamento das tecnologias implementadas, conseguindo ao mesmo tempo o desenvolvimento de novas tecnologias relacionadas com as configurações de políticas de segurança e com a segurança das aplicações provenientes da “Windows Store”.

O Windows 10 não só enfrentou uma preocupação efetiva na melhoria de medidas de segurança já antes implementadas, mas também na implementação de medidas como um novo sistema de controlo de acesso, novos sistemas de proteção *antimalware*, entre vários outros.

Os sistemas operativos Microsoft Windows continuam a ser dominantes no seu segmento, por isso são também o alvo da maior. Com todo o investimento em segurança realizado ao longo das várias versões dos sistemas operativos Windows é possível afirmar que o Windows 10 é certamente o mais seguro.

### **3.5. Condicionantes de segurança**

A aposta na segurança é bem notada no ponto anterior, transpondo estes desafios para este trabalho, demarcados como aspetos que condicionam o desenvolvimento dum projeto, mas não o seu objetivo final. Deste modo, como condicionantes ao desenvolvimento do projeto são enunciadas as seguintes:

### 3.5.1. Sistemas de segurança genéricos

Pretende-se nesta secção referir brevemente os sistemas de segurança *antimalware*, nos sistemas Windows. Assim, podem-se definir duas principais classes de proteção no *software* de segurança de sistemas operativos Windows. A classe de proteção do sistema, onde o principal mecanismo de proteção é o antivírus, e a classe de proteção das comunicações de rede, onde a *firewall* é o seu principal mecanismo de proteção.

Atualmente detetando muitos dos tipos de *malware* existentes, os *antivírus* são classificados pelo tipo de deteção de possíveis ameaças, que pode ser por assinatura, heurístico, comportamental, por *data-mining* [48] ou baseada na *cloud* [49].

Na prevenção de possíveis intrusões através das redes informáticas, a *firewall* desempenha uma importante barreira limitando o acesso, não permitindo intrusões já identificadas. Neste âmbito existem ainda os *Intrusion Detection System* (IDS), que identificam as possíveis intrusões através da análise das comunicações da rede permitindo a análise dessa possível intrusão e o seu bloqueio.

No que diz respeito à segurança em torno dos dispositivos USB também a sua evolução foi alvo de grandes progressos, onde atualmente é comum, nas soluções de segurança, efetuar a pesquisa automática por *malware* sempre que um dispositivo de armazenamento USB é ligado ao sistema.

### 3.5.2. User Account Control (UAC)

A distinção dos privilégios entre os utilizadores tem sido um dos principais focos de desenvolvimento de segurança ao longo das várias versões do sistema operativo. Apesar da elevação de privilégios existir no Windows XP com a necessidade de colocar as credências de administrador, foi desde o lançamento do *User Account Control* (UAC) com o Windows Vista, descrito no ponto 3.4.1, que a elevação de privilégios restringe eficazmente a execução de aplicações aos utilizadores sem credenciais de administração.

É imprescindível obter privilégios elevados para aceder a toda a informação do utilizador e do sistema. Ao longo do tempo foram divulgados novos outros modos de contornar esta condicionante, quer através de *exploits*, quer por novas vulnerabilidades, que a Microsoft foi corrigindo nas suas atualizações de segurança.

### 3.5.3. Execução automática nos dispositivos USB

Desde o Windows 95 que esta funcionalidade sempre foi importante para os sistemas operativos Microsoft. No entanto, contém um enorme problema de segurança, já que permite que seja o sistema a executar e instalar *software* malicioso automaticamente.

Com o Windows XP foi lançada a funcionalidade “AutoPlay” que efetua uma pesquisa nos conteúdos das *pendrives* para aconselhar o programa adequado a executar, sendo necessário a intervenção do utilizador para que fosse executado o *autorun*. O *autorun* em CD e DVD continuava sem esta restrição, levando a SanDisk e a M-Systems a desenvolver a “*pendrive U3*” [50] que emula uma *drive* de CD ao mesmo tempo que monta a unidade de armazenamento, possibilitando assim a execução automática de *software*.

Como descrito no ponto 3.4.1. “Windows Vista”, esta funcionalidade foi integrada no “AutoPlay”, necessitando da intervenção do utilizador para ser executada. Deixou assim de ser possível a execução automática de *software* em qualquer dispositivo amovível, e sem a prévia alteração do registou ou permissão do utilizador. Esta passou a ser a principal condicionante ao desenvolvimento desta dissertação.

Em [51], foi divulgado o então designado “badUSB”, que aproveita uma vulnerabilidade crítica de concessão do USB, permitindo contornar o problema do bloqueio do *autorun*. Consiste na reprogramação do *firmware* do *chip* do dispositivo, neste caso uma *pendrive* USB, para que esta, quando ligada ao sistema, seja detetada como um normal teclado USB, conseguindo inclusivamente escrever como se fosse um indivíduo a escrever no teclado.

*“It can do whatever you can do with a keyboard, which is basically  
everything a computer does,”  
Karsten Nohl (SRLabs) [52]*

O BadUSB é assim um novo género de *autorun*, desta vez sem o consentimento do sistema, uma vez que o atacante prepara o dispositivo para ser o próprio sistema a executar o *malware* com as instruções que bem entender.

Como no próprio nome “USB”, está garantida a universalidade da conexão pelos mais diversos dispositivos, e como a vulnerabilidade encontra-se na possibilidade de reprogramar o *chip* controlador USB, é possível transformar qualquer dispositivo com conexão USB num dispositivo de ataque informático. A SRLabs, laboratório que publicou esta vulnerabilidade, apresentou um conjunto de dispositivos que testou, dos

quais indicou os que têm e os que não têm esta vulnerabilidade [53]. Dos dispositivos testados apresentando a vulnerabilidade encontram-se: *hubs* USB; adaptadores de cartões; adaptadores SATA; ratos; teclados; *webcams*; discos externos e *pendrives*.

Um conceito diferente mas com objetivos semelhantes, surgiu em 2010, foi o desenvolvido pela comunidade do fórum hak5.org [54] e designado de “RubberDucky”. Com as suas origens no arduino<sup>3</sup>, modificaram o Teensy<sup>4</sup>, um dispositivo que emula os teclados permitindo a inserção de comandos, de forma a simplificar o seu funcionamento e também a sua aparência, fazendo com se apresente como uma simples *pendrive* USB, como se pode constatar através da Figura 14.

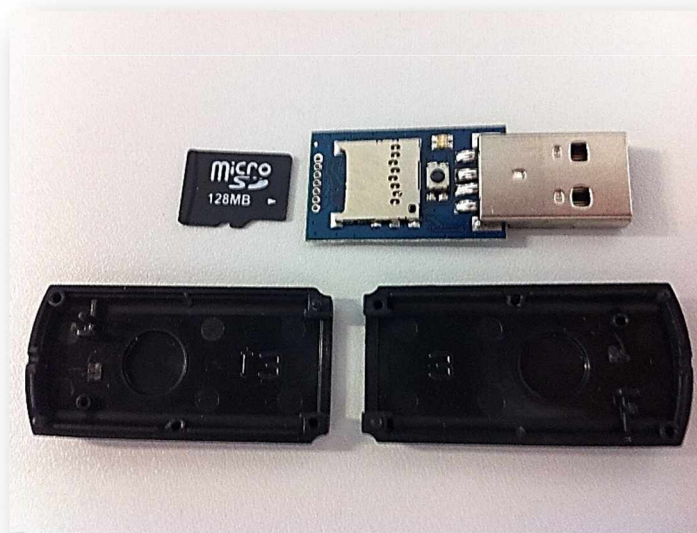


Figura 14 - RubberDucky

De facto, apenas com o teclado é possível controlar todo o sistema, quer pelas teclas de atalho que o sistema operativo proporciona, quer pela linha de comandos. Foi esta a principal motivação que levou à compra deste dispositivo, realizada através do seu *site* oficial<sup>5</sup>.

Os membros da comunidade que criaram a RubberDucky desenvolveram também plataformas de suporte, criando *scripts*, aplicações ou melhorando o próprio *firmware*.

<sup>3</sup> <https://www.arduino.cc/>

<sup>4</sup> <https://www.pjrc.com/teensy/>

<sup>5</sup> <http://hakshop.myshopify.com/products/usb-rubber-ducky-deluxe>



## **DESENVOLVIMENTO DO SISTEMA**

---

São descritas neste capítulo as opções de desenvolvimento tomadas com base nas condicionantes encontradas e nos objetivos propostos.

## 4. Desenvolvimento do sistema

Com esta dissertação, e de acordo com a hipótese de investigação formulada no ponto 2.3, foi desenvolvido um método de ataque recorrendo a dois *scripts*, um para ultrapassar a principal condicionante de segurança dos sistemas Windows, o UAC, e um outro para a efetivação da recolha de informação. Foi ainda desenvolvida uma aplicação recorrendo à linguagem de programação *Python*, com o objetivo de integrar ambos os *scripts* numa só aplicação, e de os parametrizar de acordo com os objetivos de cada recolha a realizar.

O método de ataque foi desenvolvido para ser executado em duas fases, devido à necessidade de parametrização dos referidos *scripts*, a fase preparatória e a de execução do ataque, como exemplificado na Figura 15.

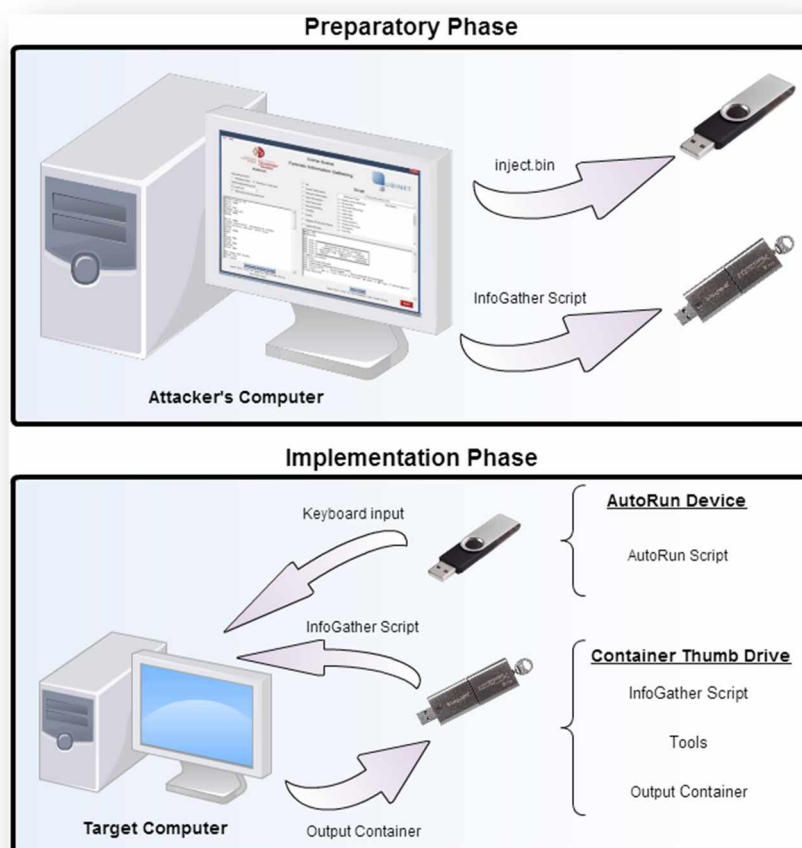


Figura 15 - Procedimento de ataque



É apresentado o procedimento do ataque informático a um computador alvo, este necessariamente em duas fases, a fase preparatória e a fase de execução.

Na fase preparatória, no *script autorun*, o atacante confirma os vários comandos e respetivos tempos de atraso, selecionando de seguida as informações que pretende recolher no *script* de recolha de informação. Após estes passos, o atacante clica no botão gerar o *script* de *autorun*, guardando o ficheiro “inject.bin” no cartão de memória que insere no dispositivo de *autorun*. De seguida, clica no botão para guardar o *script* de recolha e guarda-o na *pendrive* de armazenamento, dando por concluída a fase preparatória.

Na fase de execução, o atacante insere ambos os dispositivos no computador alvo e aguarda até que o *script* esteja concluído, quando o *led* referente à tecla “Caps Lock” piscar por duas vezes, retirando o dispositivo de *autorun*. Agora, poderá aguardar pela conclusão do *script* de recolha da *pendrive* de armazenamento, no qual o *script* de *autorun* irá executar de modo oculto. O atacante aguarda até o *led* referente à tecla “Caps Lock” piscar novamente duas vezes, retirando, por último, o dispositivo de armazenamento.

Seguidamente, serão descritas as opções tomadas no decorrer do desenvolvimento dos *scripts* e da aplicação, as estruturas de *hardware* e *software* na qual este projeto se baseia e, por último, os cenários possíveis para a utilização prática desta ferramenta.

#### **4.1. Cenários de utilização**

Tendo como base ideias já descritas anteriormente, como as já referidas no ponto 2.1. “Ferramentas forenses e a alternativa forense”, em que existe a necessidade de uma parametrização prévia ao processo de recolha da informação, foi também desenvolvido neste projeto um procedimento idêntico, já que se pretende abranger vários cenários de utilização. Cada um desses cenários irá certamente conter diferentes necessidades na recolha de informação. Assim, independentemente do cenário de utilização pretendido, o sistema desenvolvido requer a configuração de dois *scripts*, um para a fase preparatória e outro para a fase de execução.

Como descrito no ponto 2.2. “Ferramentas de recolha de informação não forense”, é possível utilizar este método em três cenários diferentes, devido principalmente ao conjunto de ferramentas utilizadas na recolha de informação: o cenário de ataque ou

*hacking*, o cenário de investigação forense e também numa primeira iniciativa de resposta a incidentes.

#### 4.1.1. Ataque ou *hacking*

O primeiro é um cenário de ataque, no qual o atacante pretende obter informações contidas na máquina alvo. Neste caso, existem várias condicionantes à obtenção de informação com este dispositivo: o estado do computador, os privilégios do utilizador, *hardware* antiquado e o tempo disponível para a recolha.

- O estado do computador, porque este dispositivo necessita que o computador se encontre ligado e que o utilizador tenha uma sessão ativa, para conseguir correr os *scripts*;
- Os privilégios do utilizador, porque se o utilizador tiver privilégios restritos, será também limitada a quantidade de informação recolhida, já que várias serão as ferramentas que não irão conseguir recolher qualquer informação;
- *Hardware* antiquado é de facto uma limitação para este dispositivo, já que este dispositivo abrange todo o *hardware* que suporte sistemas operativos com Windows Vista ou mais recentes, bastando para isso conter uma porta USB ativa. Caso o *hardware* seja muito antiquado apenas é afetado o tempo de toda a operação;
- Por último, o tempo disponível para o ataque é certamente um condicionamento. Apesar deste dispositivo se encontrar configurado para uma rápida recolha, existem algumas informações que terão necessariamente uma recolha mais lenta, como o *dump* da memória RAM.

Num cenário de *hacking*, o acesso físico ao computador poderá ser usado apenas enquanto o utilizador se ausenta momentaneamente. Por isso, o tempo disponível poderá variar, e o atacante poderá retirar o dispositivo em caso de necessidade, sem que a recolha esteja totalmente terminada.

Neste cenário, numa primeira fase, é utilizado o dispositivo de *autorun*, realizando a preparação do computador para a segunda fase, com a ligação do dispositivo de armazenamento com os *scripts* e *software* necessário para a recolha da informação. Será nesta última que será armazenada toda a informação recolhida, procedimentos apresentados na Figura 16:

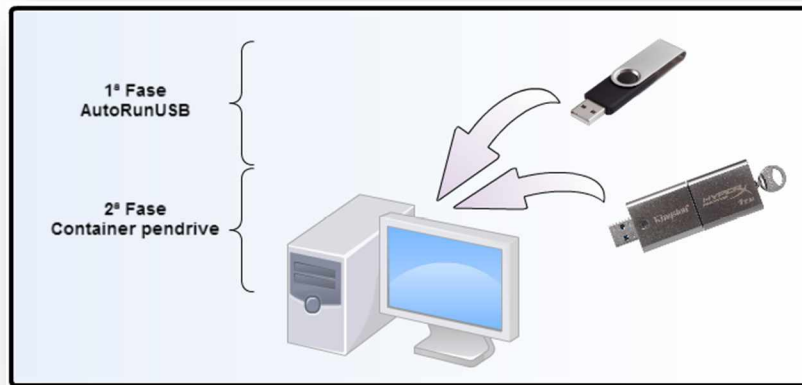


Figura 16 - Procedimento de ataque em duas fases

Nesta Figura é apresentado um ataque em duas fases, uma vez que o dispositivo de *autorun* escreve um *script* que só desencadeia o processo quando é inserida a *pendrive* de armazenamento. É assim possível efetuar o ataque em dois momentos diferentes, desde que não seja reiniciado o computador entre os mesmos. Deste modo, o atacante poderá iniciar a fase preparatória ao ataque, após o utilizador entrar no sistema, inserindo o dispositivo de *autorun*, por poucos segundos, e voltar mais tarde para efetuar o ataque.

É possível efetuar o ataque numa única fase, através da inserção de ambos os dispositivos ao mesmo tempo, desde que existam portas USB disponíveis na máquina alvo, ou então com recurso a um *Hub* USB, como demonstrado na Figura 17.

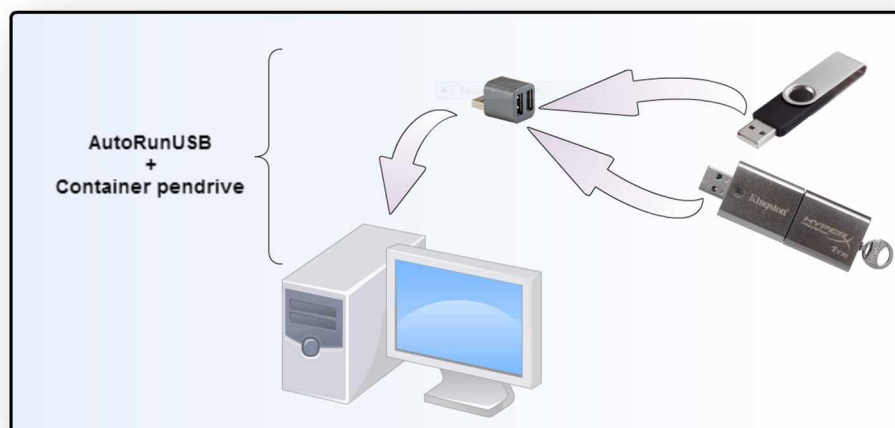


Figura 17 - Procedimento de ataque em fase única

#### 4.1.2. Investigação forense

Este dispositivo poderá ter um papel interessante para um investigador forense, já que poderá automatizar um conjunto de processos, reduzindo o tempo de investigação. Como

descrito no ponto 2.1. “Ferramentas forenses e a alternativa forense”, é possível utilizar deste dispositivo com ferramentas devidamente certificadas, bastando para isso efetuar a integração das mesmas nos *scripts*.

Um outro cenário de utilização no campo forense é a análise da imagem de um disco através da virtualização da mesma, algo que já é efetuado nas investigações forenses. Deste modo, é possível utilizar todas as ferramentas enunciadas nesta dissertação, já que não existem problemas em efetuar alterações ao sistema operativo virtualizado, uma vez que o original é preservado, permitindo uma automatização de todo o processo de recolha de informações da máquina alvo, libertando o investigador de tarefas repetitivas e morosas.

Por fim, neste cenário, ainda é possível com o sistema desenvolvido, realizar a parametrização das informações relevantes ou para as quais se tem autorização de recolha por parte de pessoal técnico, e posteriormente a recolha no local do crime, ou a recolha no computador alvo ser efetuada por pessoal com menos conhecimentos técnicos. Deste modo, o pessoal com maior conhecimento técnico seria aproveitado para a análise da informação ou mesmo para investigações mais complexas.

#### **4.1.3. Resposta a Incidentes**

Para um Administrador de sistemas a investigar um incidente é essencial obter e analisar a informação o mais rapidamente possível, de modo a atuar rápida e proporcionalmente. É este um possível cenário de aplicação prática deste dispositivo no meio empresarial, ou até mesmo na administração pública.

Os administradores de sistemas têm normalmente a seu cargo um conjunto variado de computadores, cada um com as suas características e especificidades, sendo normalmente morosa a sua reposição quando assim é necessário. Um *malware* que se consiga instalar num dos computadores pode-se propagar rapidamente através da rede informática, podendo levar à necessidade de reposição dos computadores infetados, levando a quebras de produtividade e mesmo de segurança se o *malware* recolher as informações, como é o exemplo do “Ramsonware” [55].

Outra utilização neste cenário e com um objetivo totalmente diferente seria a utilização deste dispositivo e da aplicação para a aplicação de um *script* de instalação e configuração de sistemas de modo totalmente automático, libertando o administrador de sistemas de tarefas repetitivas num conjunto de computadores ou ainda para a automatização aa

realização de backups para um dispositivo de armazenamento ou mesmo para um servidor centralizado, enviando apenas os ficheiros ou pastas definidos para o caso.

## 4.2. Opções de desenvolvimento

O desenvolvimento deste projeto requereu algumas decisões de desenvolvimento que condicionaram de algum modo o objetivo final desta dissertação, tendo as principais sido as seguintes:

- As ferramentas utilizadas na aplicação foram seleccionadas com base nos princípios de: utilização gratuita; execução através da linha de comandos, podendo assim serem integradas nos *scripts*; de não apresentarem janelas no ecrã, enviando os resultados para ficheiros; e também por terem uma reduzida *footprint*;
- As linguagens de programação utilizadas para o desenvolvimento do *script* foram seleccionadas tendo em conta as linguagens de *scripting* nativas dos sistemas operativos em análise, como já referido no ponto 2.2.4. “*Scripts*”. Assim, a escolha recaiu para o *Batch Script* como linguagem principal do *script* de recolha, já que o Windows Vista não traz o *PowerShell* como linguagem nativa. No entanto, no *script* foi colocado um pequeno comando em *PowerShell* e na aplicação foi dada a possibilidade de seleccionar o sistema operativo, precisamente para poder distinguir os comandos em *PowerShell*, “*A posteriori*”. Foi ainda necessária a utilização de um pequeno *script* em *VBScript*. A aplicação foi inteiramente desenvolvida em *Python*, por esta ser uma linguagem verdadeiramente versátil e pelo conjunto de bibliotecas disponíveis, permitindo uma enorme escalabilidade no seu posterior desenvolvimento;
- No desenvolvimento da aplicação, chegou-se à conclusão de que a quantidade de opções na utilização de ferramentas e a quantidade de extensões de ficheiros eram incomportáveis com uma só janela, existindo a necessidade de dividir as opções em separadores ou em menus distintos. No entanto, foi tomada a decisão de manter um aspeto simples em janela única, apresentando apenas o essencial ao utilizador;
- Por último, foi tomada a opção de recolher a informação possível com os privilégios do utilizador com a sessão ativa no momento da recolha da

informação, assumindo a consequência de não se obter toda a informação desejada, mas cumprindo o objetivo de não modificar o sistema, o que um possível escalonamento de privilégios poderia provocar. Esta poderá ser opção para trabalho futuro.

### 4.3. Arquitetura de *hardware*

A arquitetura de *hardware* define-se em 3 domínios principais: na fase preparatória, por um computador com a aplicação de configuração do processo de recolha; numa segunda fase, um conjunto do dispositivo de *autorun* com uma *pendrive* de armazenamento, sendo este conjunto utilizado junto do computador com a aplicação de configuração e depois junto do computador alvo da recolha de informação; e por último, um computador que será o alvo da recolha de informação, que será o computador da vítima no caso de um ataque ou de recolha de evidência forense ou então um computador de onde se pretende recolher informação para análise de situações no âmbito da administração de sistemas, tal como apresentado nos três cenários no ponto 4.1.

O computador que irá executar esta aplicação referida para a primeira fase deverá ter os requisitos mínimos de *hardware* para executar o sistema operativo Windows Vista *32bits* ou superior.

É ainda possível a utilização de um *Hub* USB, sendo conveniente que o mesmo tenha características de conexão com velocidade de transferência iguais ou superiores à do dispositivo de recolha, uma vez que é possível utilizar diferentes dispositivos de recolha além da já mencionada *pendrive*, como o caso de discos externos, cartões de memória, ou qualquer outro dispositivo de armazenamento.

Como anteriormente referido, ponto 3.3. "Dispositivos USB", os principais motivos de utilização da *pendrive* com conexão USB são a sua dimensão e portabilidade, o que poderá ser relevante num cenário de ataque, a universalidade da sua conexão, por ser compatível entre as suas diversas versões, e também a sua velocidade de comunicação, que poderá chegar, em teoria, aos 10Gb/s na sua versão 3.1.

Como o dispositivo de armazenamento é reconhecido através do seu nome, não importa o tipo de ligação, desde que o nome corresponda ao configurado no *script* de *autorun*. É possível utilizar dispositivos de armazenamento com conexões mais rápidas,

como dispositivos que utilizem tecnologia ThunderBolt, descrita no ponto 4.4. “Arquitetura de *software*”.

#### 4.4. **Arquitetura de *software***

Como referido no início deste capítulo, foram desenvolvidos dois *scripts* além da aplicação de configuração, a saber:

##### 4.4.1. **Script *autorun***

Este é um *script* necessário para ultrapassar a proteção dos sistemas operativos em relação à execução automática de *software* nos dispositivos USB, como descrito no ponto 3.5.3. “Execução automática nos dispositivos USB”. O dispositivo utilizado, USB RubberDucky, vem configurado para as instruções contidas no ficheiro binário que é armazenado na raiz do cartão de memória inserido no dispositivo.

O ficheiro é gerado através de um codificador java, convertendo o *script* para hexadecimal através do seguinte comando:

```
“java -jar encoder.jar -i inputFile.txt -l pt.language -o  
inject.bin”
```

Como anteriormente referido, é necessária a instalação do java no computador, uma vez que o codificador utilizado se encontra em java, como revela o atributo utilizado: “-jar encoder.jar”. O atributo “-i inputFile.txt” serve apenas para indicar o ficheiro de origem, este no formato de texto. O atributo “-l pt.language” determina a configuração do teclado que irá ser utilizado, uma vez que a disposição das teclas num teclado português é diferente da de outros países. Por fim, o atributo “-o inject.bin” é apenas para determinar qual o ficheiro de *output*, colocado na raiz do cartão de memória do dispositivo.

A linguagem utilizada [56] é designada de “*Ducky Script*” e pode ser utilizado qualquer editor de texto para a programar, já que o *script* será um ficheiro de texto onde cada linha é considerada um comando. Nesta linguagem, foram definidos os comandos necessários para efetuar praticamente tudo o que é possível fazer com um teclado.

Os comandos são introduzidos em maiúsculas, simulando o pressionar de apenas uma tecla, combinações de teclas ou então funções como a definição de tempos de espera entre comandos, como o comando “DEFAULT\_DELAY” que deve ser colocado no início do

*script*, para definir um determinado tempo, em milissegundos entre os comandos, não necessitando do especificar para cada um dos comandos.

Aproveitando as teclas de atalho do Sistema Operativo e também a possibilidade que esta linguagem proporciona, é possível escrever um *script* com as instruções necessárias para que seja o sistema a procurar e executar um possível *malware* introduzido através de uma *pendrive*.

No seu fórum [54] e repositório [57] oficiais, encontram-se diversos *scripts* desenvolvidos pelos membros da comunidade que desenvolveu o dispositivo. Alguns destes *scripts* [58, 59, 60, 61] vão de encontro às necessidades deste projeto e poderão ser adequados para adaptar o *script* para novas realidades e cenários.

O desenvolvimento deste *script* teve em conta fatores como o tempo necessário para o dispositivo ser identificado e instalado pelo sistema, proporcionando um atraso inicial antes do primeiro comando, ou as janelas no ecrã.

Este *script* foi desenvolvido de acordo com o apresentado na Figura 18.

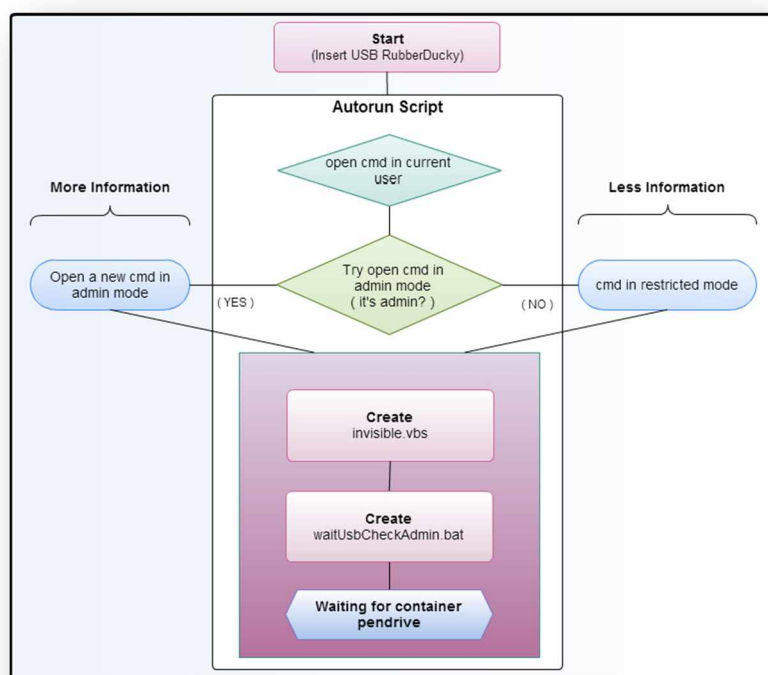


Figura 18 - Fluxograma do dispositivo de *autorun*

Após o dispositivo de *autorun* ser reconhecido pelo sistema, o *script* é iniciado com a abertura de uma consola de linha de comandos, que é escondida de seguida. É aberta a janela de execução de comandos na tentativa de abrir uma consola com privilégios de



administrador. Se o utilizador tiver esses privilégios, o sistema operativo não irá pedir as credenciais, bastando clicar no botão “Sim” na janela do UAC, ou então através da tecla para baixo seguida da tecla para cima, como apresentado na Figura 19.

```
18 DELAY 1000
19 STRING powershell -WindowStyle Hidden
    Start-process cmd.exe -Verb runAs
20 ENTER
21 DELAY 1000
22 DOWN
23 UP
```

Figura 19 - Excerto do código do *script autorun*

Independentemente de ser administrador ou não, através da linha de comandos é criado o “invisible.vbs”, um *script* em Visual Basic com o objetivo de ocultar a janela do *script* principal quando este for executado. É também criado o “waitUSBCheckAdmin.bat”, um *Batch Script*, com o objetivo de encontrar o dispositivo de armazenamento, procurando continuamente pelo nome dos volumes montados no sistema. De seguida, são iniciados os *scripts* através do seguinte comando:

```
“STRING wscript.exe invisible.vbs waitUsbCheckAdmin.bat &
    exit”
```

Com este comando é executado o *script* “invisible.vbs” que possibilita a execução oculta do “waitUsbCheckAdmin.bat”. Por fim, é dada a informação de término deste *script*, possibilitando assim a visualização do término através da luz indicadora do “CAPS LOCK” no teclado do computador.

#### 4.4.2. *Script de recolha*

Este é o *script* principal desta dissertação, já que é o que realiza a própria pesquisa e recolha de informação. Foi desenvolvido em *Batch Script* pela compatibilidade da linguagem com todos os sistemas operativos após Windows XP.

Foi desenvolvido com intenção de ser parametrizável através da aplicação CSIFIG, agrupando ferramentas e comandos por tipo de recolha ou blocos, possibilitando que, na aplicação, seja retirado todo o bloco caso o atacante / investigador não queira recolher essa informação. Existe ainda a possibilidade de edição do bloco, caso se pretenda a utilização da maioria das suas ferramentas retirando as que não pretende, sendo que todas as ferramentas utilizadas ocupam cerca de 13MegaBytes.

Esta estrutura permite a escalabilidade da aplicação, integrando facilmente novas ferramentas ao *script* ou retirando outras e, uma vez que a aplicação permite a criação de perfis, não são perdidas as alterações efetuadas.

Foram utilizadas as ferramentas e os comandos descritos no Apêndice I – Informações úteis em sistemas operativos Windows, tal como ilustrado na Figura 20.

```

210 :cipherFiles
211 %softDir%\EDD.exe /accepteula /Batch > edd.txt 2>>"%LogFile%"
212 cipher.exe /u /n %systemdrive% > %outputDir%\cipher.txt | xcopy/y %a %outputFiles%
    \cipherFiles\ 2>>"%LogFile%"
213 for %A in (%drives%) do ( @%softDir%\TCHunt.exe -d %A >> %outputFiles%
    \cipherFiles\cipherFiles.txt | xcopy/y %a %outputFiles%\cipherFiles\ 2>>"%LogFile%" )
214 ::End
215 :registrySecurity
216 MD %outputDir%\registry
217 %softDir%\regdmp.exe > %outputDir%\registry\registry.txt 2>>"%LogFile%"
218 %softDir%\dumpsec.exe /rpt=users /outfile=%outputDir%\registry\security.txt /saveas=csv 2>>"
    %LogFile%"
219 if %itsAdmin%==yes (%softDir%\shadowspawn "%systemroot%\system32\config" R: robocopy R:\ "
    %outputDir%\registry\config" /b /mir /r:1 /w:1 2>>"%LogFile%") else (@robocopy
    %systemroot%\system32\config %outputDir%\registry\config /r:1 /w:1 2>>"%LogFile%")
220 ::End
221 :Files
222 SET extensions="*.png"
223 REM Direct Copy Points of Interest
224 if %itsAdmin%==yes ( if %sh%==yes (MD "%outputDir%\POI\Prefetch" & @%softDir%\shadowspawn "
    %SystemRoot%\Prefetch\" S: robocopy S: "%outputDir%\POI\Prefetch" /b /mir /r:1 /w:1 2>>"
    %LogFile%") else (@MD "%outputDir%\POI\Prefetch" & @robocopy "%SystemRoot%\Prefetch" "
    %outputDir%\POI\Prefetch" /r:1 /w:1 2>>"%LogFile%")
225 if %itsAdmin%==yes ( if %sh%==yes (MD "%outputDir%\POI\Indexing" & @%softDir%\shadowspawn "
    %ProgramData%\Microsoft\Search\Data\Applications\Windows\" S: robocopy S: "%outputDir%
    \POI\Indexing" /b /mir /r:1 /w:1 Windows.edb 2>>"%LogFile%") else (MD "%outputDir%

```

Figura 20- Excerto do *script* de recolha

Os blocos desenvolvidos são identificados pela aplicação através do símbolo “:” no início de cada bloco e da expressão “::End” no final, como se pode observar na Figura 20 (linhas 220 e 221), o fim de um bloco e o início de outro. As ferramentas e comandos foram repartidos por onze blocos que se apresentam de seguida:

- “:Common Variables” — Este bloco é utilizado para executar todos os parâmetros de variáveis utilizadas por mais de um módulo. É também utilizado para efetuar o registo da data/hora em que é iniciado o *script*, para executar a identificação do dispositivo de armazenamento, a identificação da arquitetura do processador, permitindo a correta utilização das ferramentas e, por último, é neste bloco que é capturada a memória, por esta ser útil em todos os cenários. É de referir que este é o único bloco que não terá opção de remoção na aplicação;
- “:systemInfo” — É utilizado para recolher todas as informações de sistema, na consulta de processos, dispositivos de *hardware*, *software*

instalados, entre outros. Contém um grande número de consultas ao registo, bem como ferramentas que automatizam as consultas (consultar Apêndice 1, ponto 1.1. “Informações de sistema”);

- “:networkInfo” — Neste bloco são recolhidas informações sobre a rede e os dispositivos de rede. Na sua maioria, são utilizados comandos do próprio sistema operativo, recolhendo assim a informação necessária sobre a rede do computador alvo (consultar Apêndice 1, ponto 1.1.5. “Informações de rede”);
- “:userInfo” — Este bloco contém as ferramentas e comandos necessários para recolher a informação do próprio utilizador (consultar Apêndice 1, ponto 1.2. “Informações de utilizadores”). São recolhidas informações como nomes, data/hora de início de sessões recentes, a atividade recente, os contactos, registos de conversações, entre outros;
- “:browsersHistory” — Neste bloco são recolhidas informações sobre a navegação do utilizador, através de consultas ao registo e recolha de ficheiros específicos que armazenam informação deste tipo. São também utilizadas ferramentas que possibilitam a consulta desta informação em diversos *browsers* (consultar Apêndice 1, do ponto 1.2.9. “Perfil no *browser*” ao 1.2.15. “Ficheiros temporários da *Internet* (Cache)”);
- “:cookies” — Este é um bloco específico para a recolha de *cookies* através da cópia de ficheiros a partir de localizações conhecidas (consultar Apêndice 1, ponto 1.2.16. “Cookies”);
- “:events” — A cópia de eventos é efetuada neste bloco, através da cópia da pasta específica de eventos do sistema, e também através de ferramentas de recolha de eventos (consultar Apêndice 1, ponto 1.1.11. “Eventos”);
- “:cipherFiles” — Os ficheiros encriptados são pesquisados e copiados neste bloco, sendo utilizadas três ferramentas específicas para este tipo de ficheiros (consultar Apêndice 1, pontos 1.1.15. “BitLocker” e 1.2.6. “Itens encriptados”);
- “:registrySecurity” — Neste bloco é efetuado o *dump* da memória e da segurança do sistema, efetuando também a cópia dos ficheiros mais relevantes do registo (consultar Apêndice 1, ponto 1.1.8. “Registo”);
- “:Files” — Este é um dos blocos mais morosos por efetuar a cópia de ficheiros e pastas específicas de interesse e também os ficheiros com as

extensões que forem definidas na aplicação. É também recolhida informação de indexação, ficheiros armazenados em *drives online* (OneDrive, GoogleDrive ou iCloudDrive), entre outros ficheiros (consultar Apêndice 1);

- “:userPasswords” — São aqui utilizadas as ferramentas relacionadas com a recolha de *passwords*, incluindo a ferramenta Mimikatz. Também estas ferramentas se encontram descritas no Apêndice 1 no ponto 1.2.5.

#### 4.4.3. Interface gráfica

Foi desenvolvida uma aplicação gráfica para permitir a configuração de forma integrada dos *scripts* necessários ao sistema, que se descreve nesta secção. A aplicação apresenta como título “*Crime Scene Forensic Information Gathering*”, nome atribuído ao sistema desenvolvido tendo em conta o cenário descrito no ponto 4.1.2.

A interface gráfica desta aplicação foi desenvolvida de modo a ter uma aparência simples e fácil de utilizar, apresentando, do lado esquerdo, as opções referentes ao *script* de *autorun* e, do lado direito, as várias opções de recolha, tendo em conta os vários blocos do *script* de recolha, como apresentado mais em detalhe na Figura 21.

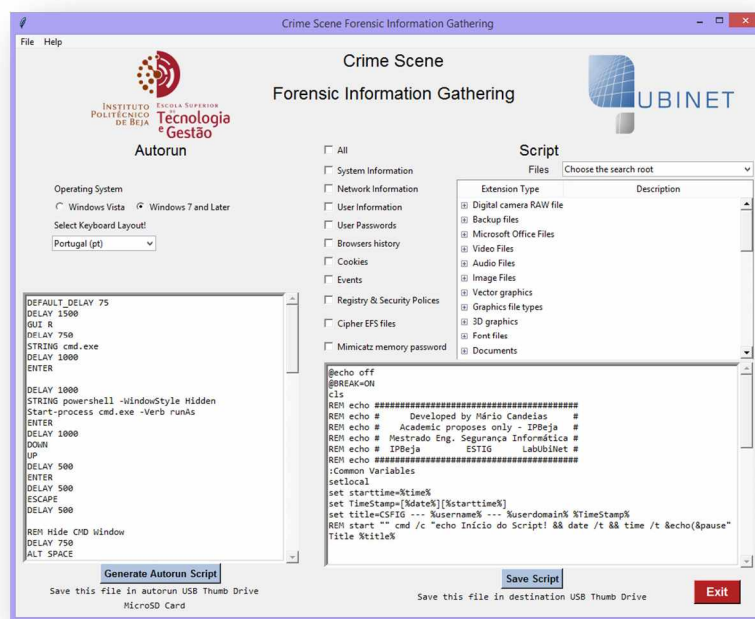


Figura 21 - Aplicação “Crime Scene Forensic Information Gathering”

No que diz respeito às opções no *script* de *autorun*, existe a possibilidade de escolha entre o Windows Vista e o Windows 7 ou posterior, devido principalmente à utilização da linguagem de *Script PowerShell*, suportada a partir do Windows 7. Se o atacante não tiver qualquer conhecimento sobre o sistema operativo da máquina alvo, torna-se mais

seguro utilizar apenas linguagens suportadas pelo Windows Vista, já que estas também o são nos seus subseqüentes. Aqui é também realizada a escolha do esquema do teclado, já que existem diferenças entre os diferentes esquemas, sendo esta uma importante definição para o sucesso da execução do *script* de *autorun*. É apresentado o próprio *script* de *autorun*, permitindo uma adequação dos tempos de espera entre os comandos, ou mesmo a integração de novos comandos, mais personalizados ao ataque ou investigação. Por fim, é apresentado o botão “Generate *Autorun Script*”, cuja função é gerar o ficheiro binário com as opções atrás definidas, possibilitando guardar o próprio ficheiro diretamente no dispositivo de *autorun*.

Já as opções contempladas para o *script* de recolha são necessariamente mais diversificadas, como apresentadas na Figura 22.



Figura 22 - Opções de recolha

Estas são as opções principais que permitem parametrizar o *script* de recolha. Cada opção selecionada irá preencher o *script* de recolha com o código respetivo.

Para a pesquisa e cópia dos ficheiros, é necessário selecionar a raiz na qual se irá basear essa seleção, escolhendo uma opção na lista pendente com o texto “Choose the search root”. As possibilidades de escolha são a pasta do utilizador atual, a pasta do sistema operativo, a raiz do sistema, ou então todas as unidades de disco montadas no sistema, como é possível verificar através da Figura 23.

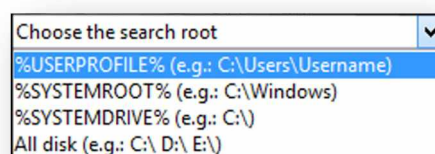


Figura 23 - Seleção da raiz da pesquisa de ficheiros

Ainda no âmbito do *script* de recolha de informações, a pesquisa e cópia de ficheiros está dependente das extensões dos mesmos, podendo esta ser selecionada na área apresentada pela Figura 24.

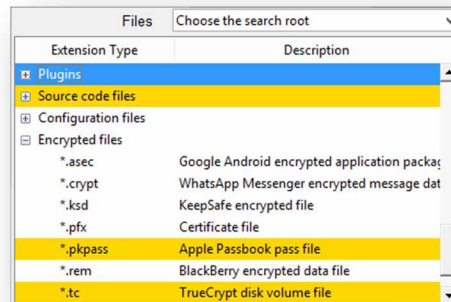


Figura 24 - Seleção das extensões

Na área de seleção de extensões a pesquisar, é apresentada uma lista com os mais diversos tipos de extensões, bastando um duplo clique com o botão esquerdo do rato, para selecionar uma extensão ou grupo de extensões, permanecendo a amarelo todas as extensões selecionadas. Ao mesmo tempo que são selecionadas e desde que a raiz da pesquisa esteja também selecionada, são também integradas no *script* de recolha.

Após a seleção das opções necessárias à recolha pretendida, é possível alterar o *script*, adequando o código à recolha pretendida, seja através da alteração ou adição de novos comandos ou ferramentas, seja retirando algumas das ferramentas que não serão necessárias. Por último, basta clicar no botão com o texto “*Save Script*” para gravar este *script* no dispositivo de armazenamento.

A aplicação dispõe ainda de uma barra de menus, com o menu “File” e o “Help”, como apresentado na Figura 25.



Figura 25 - Menu File e Help

No menu “*File*”, existem as opções “*Load Profile*” e “*Save Profile*”, que permitem carregar um ficheiro com um perfil e guardar todas as opções e alterações num único ficheiro e com o nome que se pretender. É deste modo possível armazenar opções para aplicar posteriormente, ou mesmo enviar remotamente para ser aplicado por outra pessoa.

Já o menu “*Help*” contém a habitual ajuda sobre as funcionalidades da aplicação (Consultar Apêndice II) e também o “*About*” que contém a versão e âmbito da aplicação, como ilustrado na Figura 26.

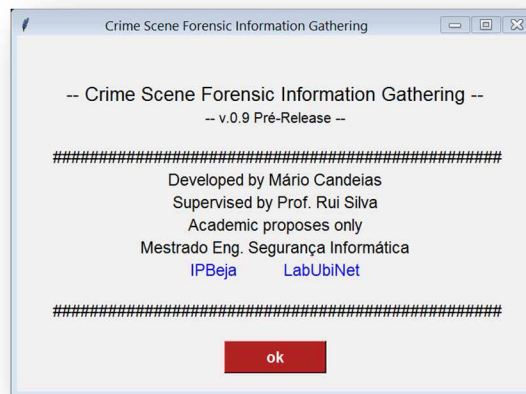


Figura 26 - About





## **AVALIAÇÃO**

---

Este capítulo tem como principal objetivo a avaliação da execução do dispositivo na recolha da informação indicada na aplicação nos sistemas operativos em análise.



## 5. Avaliação

A avaliação desta ferramenta passa necessariamente por testar o seu funcionamento e a sua eficiência, tendo sempre em conta o seu objetivo principal. Assim, não se pretende a avaliação de cada comando e ferramenta, mas sim a avaliação do funcionamento do dispositivo de um modo geral, num cenário real, e também a sua eficácia na recolha da informação pretendida.

### 5.1. Avaliação do funcionamento

Para a realização dos testes de avaliação foram utilizados computadores afetos ao laboratório UbiNET [62] do Instituto Politécnico de Beja, cujos dados foram gerados para este efeito, e um computador pessoal devido às suas características de *hardware*.

Com o objetivo de envolver diferentes características de *hardware* para cada um dos sistemas operativos, não descurando os computadores mais antigos, foram utilizados dois computadores *desktop*, um com o sistema operativo Windows Vista, um com o Windows 7 e dois computadores portáteis, um com o Windows 8.1 e outro com o Windows 10. Deste modo, foi possível relacionar as características de *hardware* com o respetivo sistema operativo à data do seu lançamento.

O computador com melhores características serviu de base para a avaliação do funcionamento e da eficiência entre os diferentes sistemas operativos. Este é um computador portátil de marca Dell e que apresenta as seguintes características físicas:

- Processador intel I7 2201Mhz;
- 4GB de memória RAM;
- Disco rígido Kingston 240GB SSD com 191MB/s de leitura e 142MB/s de escrita;
- Duas portas USB2.0 e outras duas USB3.0.

De acordo com o estudo realizado no ponto 3.3, na primeira vez que um dispositivo USB é ligado ao computador, o sistema irá recolher informações do mesmo criando as respetivas chaves de registo, motivo pelo qual o sistema leva mais tempo a disponibilizar a utilização do dispositivo. Deste modo, para testes realizados na mesma máquina, iríamos sempre obter piores tempos para a primeira vez que o dispositivo é ligado ao sistema. Para ultrapassar esta condicionante, nos sistemas em que são realizados mais de um teste, foi instalado o *software* “*Shadow Defender*” [63], que manterá o sistema

operativo totalmente funcional, retrocedendo todas as modificações ao momento em que foi bloqueado, sempre que o sistema for reiniciado. Assim, quando inserimos os dispositivos de *autorun* e de armazenamento, o sistema irá sempre reconhecê-los como se fosse a primeira vez que são ligados.

Para a avaliação do funcionamento do dispositivo, foram definidos dois testes com intuito de testar o funcionamento do dispositivo com diferentes privilégios nos utilizadores. Assim, em ambos os testes, será utilizado o mesmo computador com o sistema operativo Windows 7, uma vez que é, no momento, o mais utilizado com 57,7% [64]. Pretende-se com este teste, avaliar se o dispositivo de *autorun* conclui os seus objetivos, nomeadamente os seguintes:

1. Autoexecução;
2. Abertura de uma consola em linha de comandos;
3. Criação do *script* “invisible.vbs”;
4. Criação do *script* “waitUsbCheckAdmin.bat”;
5. Execução do *script* de recolha de informação no dispositivo de armazenamento.

Neste teste, cada um dos objetivos referidos encontra-se dependente do sucesso do objetivo anterior, deixando de ser importante determinar os tempos de cada objetivo, mas sim efetuar apenas uma validação do mesmo. O registo dos tempos para a execução desta fase serão registados para se determinar os tempos totais conjuntamente com o procedimento de recolha.

A avaliação de funcionamento verificou-se com sucesso, quer ao longo do processo de desenvolvimento, quer após a sua conclusão. No entanto, no ponto seguinte relativo à avaliação da eficiência, apresenta-se um conjunto de tabelas com os tempos obtidos e onde se verificou novamente a conformidade entre as informações expectáveis de obter e as informações obtidas.

## 5.2. Avaliação da Eficiência

A avaliação da eficiência do dispositivo poderá efetuar-se através do tempo decorrido desde o início do *script* de recolha até à sua conclusão, podendo estar dependente de um conjunto de condicionantes, nomeadamente:

- a) Informação a recolher;

- b) Sistema Operativo;
- c) Características do disco rígido;
- d) Características de *hardware*.

Cada uma destas alíneas poderá afetar os resultados de eficiência, sendo necessário efetuar testes comparativos a cada uma das possíveis condicionantes com vista a determinar a sua influência na avaliação global do dispositivo.

No que diz respeito à alínea a), a quantidade de informação a recolher é um fator importante na eficiência dos resultados finais, nomeadamente quando são recolhidas grandes quantidades de informações, como a obtenção da memória RAM, ou a pesquisa e cópia de ficheiros. Por este motivo, foram especificados os blocos de informações a obter em todos os testes realizados com base nos blocos referidos no ponto 4.4.2. Destes, selecionou-se o bloco de informação dos utilizadores, o bloco do histórico de navegação na *Internet* e o bloco de recolha de ficheiros.

Para a validação da informação recolhida, verificou-se se cada um dos blocos de recolha obteve toda a informação estipulada para o efeito.

No bloco do histórico de navegação, foram visitados *sites* específicos para serem validados em cada um dos três *browsers* mais populares:

No Mozilla Firefox:

- [www.ipbeja.pt](http://www.ipbeja.pt)
- [ubinet.ipbeja.pt](http://ubinet.ipbeja.pt)

No Google Chrome:

- [www.museuregionaldebeja.net](http://www.museuregionaldebeja.net)
- [www.diariodoalentejo.pt](http://www.diariodoalentejo.pt)
- [www.facebook.com/bibliotecamunicipaldebeja](http://www.facebook.com/bibliotecamunicipaldebeja)

No Internet Explorer:

- [www.roteirodoalqueva.com](http://www.roteirodoalqueva.com)
- [www.visitalentejo.pt](http://www.visitalentejo.pt)
- [www.vinhosdoalentejo.pt](http://www.vinhosdoalentejo.pt)
- [www.ovibeja.pt](http://www.ovibeja.pt)

No bloco de informações de utilizadores foi configurado um utilizador com privilégios restritos e um administrador.

A validação necessária para o bloco de recolha de ficheiros será realizada não só com a recolha das pastas classificadas como “*Points Of Interest*” (POI - expressão utilizada para identificar ficheiros ou pastas específicas com informações úteis a recolher do sistema), mas também com a validação da cópia da imagem “logo-ubinet.png”, armazenada na pasta “%userprofile%\images”, aquando da visita ao *site* “ubinet.ipbeja.pt”.

Para avaliar o impacto do sistema, foi necessário efetuar o teste aos sistemas operativos em análise, nomeadamente o Windows Vista, 7, 8 e 10, analisando sobretudo a eficiência do dispositivo. Deste modo, foram implementados os testes necessários à avaliação deste método de ataque, sendo de destacar a importância da obtenção dos tempos de recolha efetuada pelos comandos e ferramentas utilizadas, recorrendo ao computador de marca Dell, descrito no ponto 5.1. Neste computador, foram instalados e configurados os sistemas operativos em análise, com as mesmas configurações e, com o antivírus “Microsoft Security Essentials” instalado e atualizado, e com a *firewall* do Windows ativa.

Seguidamente, são descritas as várias tabelas com os tempos que cada bloco de comandos e ferramentas demora nas suas operações, bem como a necessidade de privilégios de administrador para a execução da cada ferramenta. Cada uma das tabelas apresentadas refere-se ao anteriormente descrito no ponto 4.4.2. “*Script* de recolha”.

Na tabela 2, é possível observar que, no bloco “Variáveis Comuns”, todos os comandos e ferramentas de sistema podem ser executados sem privilégios de administração, apesar da necessidade de privilégios de administrador para a recolha da memória RAM. É também possível observar que, sem a recolha da memória, este bloco leva apenas 2 segundos a ser executado, em contraste com os 61 segundos com a recolha da memória RAM, tendo em conta que o computador de teste contém 4GB de memória RAM.

Necessidade de Privilégios de Administrador		
Bloco “Variáveis Comuns”	Utilizador Restrito	Admin.
Comandos e definições comuns	✓	✓
<i>Dump.</i> da memória RAM	✗	✓
Tempos (seg.)	<b>2</b>	<b>61</b>

Tabela 2 - Eficiência do bloco "Variáveis Comuns"

É de referir que, na avaliação da eficiência dos restantes blocos, optou-se por não se efetuar o *Dump.* da memória RAM, uma vez que o objetivo principal é a avaliação de cada bloco. Apesar dos cerca de 59 segundos necessários para a recolha da memória não serem contabilizados, é necessário para todos os restantes blocos contabilizar os 2 segundos da execução dos comandos e definições comuns, já que estes são necessários para a execução dos comandos e ferramentas dos restantes blocos, tal como referido no ponto 4.4.2. “*Script* de recolha”.

Na tabela 3, referente à avaliação da eficiência do bloco “Informações de sistema”, é possível observar que, de todos os comandos e ferramentas utilizados, apenas o “CPU-Z” necessitam de privilégios de administração para executar o *script*, influenciando bastante a eficiência, uma vez que os tempos passam de 27 segundos para 63 segundos apenas pela execução do “CPU-Z”.

Necessidade de Privilégios de Administrador		
Bloco “Informações de sistema”	Utilizador Restrito	Admin.
Comandos e ferramentas de sistema	✓	✓
USBDeview	✓	✓
Inside Clipboard	✓	✓
ProduKey	✓	✓
<i>Autorunsc</i>	✓	✓
Listdlls	✓	✓
CPU-Z	✗	✓
Tempos (seg.)	<b>27</b>	<b>63</b>

Tabela 3 - Eficiência do bloco " Informação de sistema "

Na tabela 4, referente a informações de rede, os tempos de execução são de apenas 7 e 8 segundos, respetivamente. Como só são utilizadas ferramentas inerentes ao sistema operativo, os tempos de execução são pequenos e não apresentam uma diferença significativa entre os utilizadores.

<b>Necessidade de Privilégios de Administrador</b>		
<b>Bloco “Informação de rede”</b>	Utilizador Restrito	Admin.
Comandos e ferramentas de sistema	✓	✓
Tempos (seg.)	<b>7</b>	<b>8</b>

Tabela 4 - Eficiência do bloco " Informação de sistema "

A eficiência do bloco de informações de utilizadores, apresentada na tabela 6, contém algumas ferramentas que necessitam de privilégios de administração para serem executadas, apesar de não se refletir em diferenças de eficiência no final. As ferramentas que necessitam de privilégios elevados são as que necessitam de acesso a localizações protegidas pelo sistema operativo, como o exemplo da atividade recente do utilizador no sistema operativo.

<b>Necessidade de Privilégios de Administrador</b>		
<b>Bloco “Informação de utilizadores”</b>	Utilizador Restrito	Admin.
Ferramentas de sistema	✓	✓
POI: Recentes	✗	✓
POI: Contactos	✓	✓
POI: App. People	✓	✓
POI: Skype	✓	✓
userprofilesview	✓	✓
logonsessions	✗	✓
psloggedon	✗	✓
savescreenshot	✓	✓
turnedontimesview	✓	✓
LiveContactsView	✓	✓
SkypeLogView	✓	✓
SkypeContactsView	✓	✓
RecentFilesView	✓	✓
LastActivityView	✗	✓
OutlookAddressBookView	✓	✓
OutlookAttachView	✓	✓
Tempos (seg.)	<b>5</b>	<b>5</b>

Legenda: POI - Pontos de Interesse

Tabela 5 - Eficiência do bloco "Informações de Utilizadores"

No bloco “Ficheiros de registo”, a tabela 6 apresenta a eficiência no acesso a ficheiros de registo em que existe uma diferença significativa entre a execução do *script* com



privilégios elevados, já que estes permitem a cópia dos ficheiros de registo, o que faz aumentar o tempo de recolha. Quando a conta utilizada não tem privilégios elevados, não permitindo a cópia dos ficheiros de registo, é efetuado o *dump*. de todo o registo através da consulta às suas chaves guardando-as num ficheiro de texto.

Necessidade de Privilégios de Administrador		
Bloco "Ficheiros de registo"	Utilizador Restrito	Admin.
Dump do registo para texto	✓	✓
Dump da segurança para texto	✓	✓
Cópia dos ficheiros de registo	✗	✓
<i>Tempos (seg.)</i>	<b>8</b>	<b>28</b>

Tabela 6 - Eficiência do bloco "Ficheiros de registo"

A tabela 7, apresenta a eficiência na recolha de informações de eventos de sistema. Estes são normalmente protegidos pelo sistema, requerendo privilégios elevados para acesso e cópia. No entanto, é realizada uma pesquisa de ficheiros, através das extensões utilizadas por ficheiros de eventos, e respetiva cópia.

Os tempos apresentados são reduzidos para cerca de metade quando se utiliza uma conta com privilégios elevados, apesar de serem recolhidos um maior número de ficheiros. Este facto justifica-se através do tempo despendido pelo sistema no controlo de acesso aos ficheiros.

Necessidade de Privilégios de Administrador		
Bloco "Eventos"	Utilizador Restrito	Admin.
Ficheiros de eventos	✓	✓
MyEventViewer	✗	✓
POI: Pasta de sistema - Eventos	✗	✓
<i>Tempos (seg.)</i>	<b>46</b>	<b>28</b>

Tabela 7 - Eficiência do bloco "eventos"

Na tabela 8, observa-se a possibilidade de recolher informação de navegação na *Internet* mesmo com um utilizador restrito. No entanto, a quantidade de informação recolhida como administrador é superior, facto que justifica a diferença de tempos entre ambos os utilizadores.

<b>Necessidade de Privilégios de Administrador</b>		
<b>Bloco “Histórico da Navegação”</b>	Utilizador Restrito	Admin.
POI: Firefox	✓	✓
POI: Chrome	✓	✓
POI: Edge	✓	✓
POI: Favorites	✓	✓
POI: Downloads	✓	✓
POI: Outlook	✓	✓
POI: EmailsVista_7	✓	✓
POI: Emails8_10	✓	✓
POI: Thunderbird	✓	✓
POI: BrowserHistory	✓	✓
POI: TempInternetFiles	✓	✓
Registo: TypedUrls	✓	✓
browsinghistoryview	✓	✓
Ficheiro: history.ie5	✓	✓
Ficheiros: index.dat	✓	✓
MyLastSearch	✓	✓
Tempos (seg.)	<b>23</b>	<b>138</b>

Tabela 8- Eficiência do bloco "Histórico de navegação"

A eficiência na recolha de *cookies* de navegação é apresentada na tabela 9, não existindo uma diferença entre os mesmos, já que os ficheiros com os *cookies* de navegação são guardados em pastas específicas acessíveis aos utilizadores.

<b>Necessidade de Privilégios de Administrador</b>		
<b>Bloco “Cookies”</b>	Utilizador Restrito	Admin.
Ferramentas de sistema	✓	✓
POI: Cookies	✓	✓
POI: INetCookies	✓	✓
Tempos (seg.)	<b>19</b>	<b>19</b>

Tabela 9 - Eficiência do bloco "Cookies"

O bloco de recolha de ficheiros poderá ser um dos mais demorados, uma vez que é efetuada a pesquisa e cópia de ficheiros pelo sistema operativo, processo que normalmente é demorado. Para esta avaliação, foi guardado o ficheiro “logo-ubinet.png” na pasta “%userprofile%\images\” para validar a cópia de ficheiros através da respetiva extensão.

Na tabela 10, podemos observar que o acesso a pastas de sistema do “Prefetch” e “Indexing” só é possível com privilégios elevados, o que influencia os tempos de recolha deste bloco.

Necessidade de Privilégios de Administrador		
Bloco “Ficheiros”	Utilizador Restrito	Admin.
POI: Prefetch	✘	✓
POI: Indexing	✘	✓
POI: Documents	✓	✓
POI: OneDrive	✓	✓
POI: GoogleDrive	✓	✓
POI: iCloudDrive	✓	✓
POI: RecycleBin	✓	✓
POI: PrintedFiles	✓	✓
POI: Desktop	✓	✓
Ficheiros Ocultos	✓	✓
Ficheiros *.png	✓	✓
Tempos (seg.)	<b>61</b>	<b>155</b>

Tabela 10 - Eficiência do bloco "Ficheiros"

Para a pesquisa e cópia de ficheiros encriptados, apenas a ferramenta “EDD” necessita de privilégios elevados na identificação de volumes encriptados. Como apresentado na tabela 11, é possível utilizar sem privilégios de administração a ferramenta “TCHunt” e a ferramenta de sistema “Cipher” para pesquisar e copiar ficheiros cifrados com ferramentas semelhantes ao “TrueCrypt”. A eficiência destas ferramentas depende do tamanho e quantidade de ficheiros encontrados.

Necessidade de Privilégios de Administrador		
Unidades e ficheiros encriptados	Utilizador Restrito	Admin.
EDD	✘	✓
Cipher	✓	✓
TCHunt	✓	✓
Tempos (seg.)	<b>48</b>	<b>50</b>

Tabela 11 - Eficiência do bloco "Unidades e ficheiros encriptados"

Na tabela 12, é apresentada uma eficiência nula para utilizadores restritos, já que as ferramentas utilizadas neste bloco necessitam de privilégios elevados para a sua

execução. Já como administrador o *script* demora cerca de 6 segundos a recolher as *passwords* do utilizador. É de referir que os antivírus detetam algumas das ferramentas utilizadas, pelo que será necessário desativar o antivírus previamente, caso contrário, não será recolhida a informação espectável da ferramenta detetada pelo antivírus. Como podemos observar na coluna Antivírus da Tabela 12 - Eficiência do bloco "Passwords" Tabela 12, são indicadas as ferramentas que não são, ao momento, detetadas pelo antivírus.

Necessidade de Privilégios de Administrador			
Bloco "Passwords"	Utilizador Restrito	Admin.	Antivírus
Mimicatz	✗	✓	✗
BitLocker Key recovery	✗	✓	✓
Mspass	✗	✓	✓
Mailpv	✗	✓	✗
Dialupass2	✗	✓	✗
BulletsPassView	✗	✓	✓
iepv	✗	✓	✗
pspv	✗	✓	✗
ChromePass	✗	✓	✗
OperaPassView	✗	✓	✓
WirelessKeyView	✗	✓	✗
VncPassView	✗	✓	✓
LSASecretsDump	✗	✓	✓
Tempos (seg.)	<b>4</b>	<b>6</b>	

Tabela 12 - Eficiência do bloco "Passwords"

No que diz respeito à avaliação da eficiência em diferentes tipos de *hardware*, esta foi avaliada tendo em conta as espectáveis limitações de transferência de dados nas interfaces de ligação utilizadas, e também nos diferentes discos rígidos.

A Tabela 13 compara os tempos de recolha entre diferentes tipos de USB e diferentes computadores. Para esta avaliação, foi utilizada a mesma configuração de *software* em todos os testes realizados, inclusivamente utilizado o computador Dell, descrito no ponto 4.3, com ligação USB 3.0. entre os dispositivos. Como o referido computador também contém portas USB 2.0, foi possível apurar a diferença entre ambas as portas de ligação, mantendo todos os restantes parâmetros. Assim, a diferença de tempos apenas pela

alteração da interface revela-se significativa, já que a cópia de ficheiros de grandes dimensões requer a melhor velocidade de ligação disponível.

Ainda na Tabela 13 é apresentado o tempo decorrido pela mesma configuração e parametrização, num computador com características de *hardware* inferiores, levando cerca do dobro do tempo do primeiro.

Eficiência com diferente <i>hardware</i> de suporte	
Computador	Total
Recente c/USB 3.0	291s (4m:45s)
Recente c/USB 2.0	357s (5m:38s)
Antigo	536s (8m:56s)

Tabela 13 - Eficiência em diferentes computadores

Foi também avaliada a eficiência com diferentes discos rígidos, já que as suas características, podem influenciar a eficiência global da recolha.

Foram utilizados nesta avaliação três discos rígidos com diferentes características de capacidade e de leitura/escrita.

Na Tabela 14, é possível observar que a diferença entre os discos de pratos rotativos é aceitável, dada a diferença entre ambas as velocidades de rotação mas, em comparação com os tempos obtidos com o disco SSD, esta diferença passa para aproximadamente o dobro do tempo do disco de 7200rpm, revelando ser esta uma diferença significativa.

Eficiência com diferentes discos rígidos						
Características do disco rígido		Características da recolha			Total	
Capacidade	Rotação	Duração	Tamanho	Quantidades		
500Gb	5400rpm	14m:03s	4,97GB	1507 Ficheiros	564 Pastas	<b>843s</b> (14m:03s)
2Tb	7200rpm	12m:54s	4,97GB	1507 Ficheiros	564 Pastas	<b>774s</b> (12m:54s)
240Gb	SSD 191MB/s Read 142MB/s Write	4m:54s	4,97GB	1507 Ficheiros	564 Pastas	<b>291s</b> (4m:85s)

Tabela 14 - Eficiência com diferentes discos rígidos

Por último, foi avaliada a eficiência em diferentes sistemas operativos. Esta avaliação teve em conta os objetivos descritos no início deste ponto, mantendo sempre as configurações e parametrizações nos diferentes sistemas operativos. Foi avaliada a eficiência da configuração de *script* definida, nos diferentes sistemas operativos, tendo sido escolhidos os sistemas operativos com arquitetura de *32bits*, Windows Vista e 7,

apenas devido a esta ser a mais utilizada no momento do lançamento do referido sistema operativo. Atualmente, e como anteriormente referido, o Windows 7, na sua versão de *64bits*, ainda continua como o sistema operativo mais utilizado, razão pela qual também este sistema operativo foi incluído nestes testes.

A Tabela 15 apresenta a avaliação da eficiência dos dispositivos de *autorun* e de recolha nos diferentes sistemas operativos, com recurso a utilizadores com privilégios elevados, permitindo avaliar a recolha de informação protegida pelo sistema operativo. Na avaliação da eficiência do dispositivo de *autorun* (Total 1), foi cronometrado manualmente o tempo desde o reconhecimento do dispositivo pelo sistema operativo até ao momento em que o *script* de recolha é iniciado. Como se pode observar na tabela (Total 1), o tempo de execução do dispositivo de *autorun* manteve-se idêntico nos diferentes sistemas operativos, podendo ser parametrizado na aplicação, modificando-se os tempos de espera entre os comandos, de modo a serem adequados à velocidade do sistema. Os tempos de espera utilizados nesta avaliação foram os mesmos para possibilitar a utilização do mesmo *script* em todos os sistemas operativos.

No dispositivo de recolha, é possível observar que o tempo de recolha varia entre os sistemas operativos em análise (Total 2) e, embora o Windows Vista seja o mais rápido, é também onde menos ficheiros são recolhidos, facto que se justifica pela presença de um menor número de ficheiros de sistema contemplados na pesquisa e um reduzido número de informações classificadas como pontos de interesse. No entanto, apesar de não serem obtidas tantas informações, os ficheiros de validação foram recolhidos. Existe ainda uma diferença significativa entre os tempos de recolha entre ambas as versões do Windows 7, sendo de notar a maior eficiência na versão de *64bits*. Já o Windows 8.1 revela-se bastante eficiente no processo de recolha, o segundo mais rápido e o segundo com um maior número de informação e, em comparação com o Windows 10, leva menos de metade do tempo, apesar do Windows 10 recolher um maior número de informação. A quantidade destacada de ficheiros recolhidos no Windows 8.1 e no Windows 10 está relacionada com a localização do armazenamento de ficheiros das aplicações e com o sistema de segurança inerente a estas aplicações, já que o sistema atribui caracteres aleatórios a parte do nome da pasta onde algumas das aplicações armazenam os seus dados, recorrendo à necessidade de armazenar toda a pasta anterior.

<b>Eficiência em diferentes sistemas operativos</b>					
<b>Sistema Operativo</b>	<b>Windows Vista 32bit</b>	<b>Windows 7 32bit</b>	<b>Windows 7 64bit</b>	<b>Windows 8.1 64bit</b>	<b>Windows 10 64bit</b>
<b>Privilégios</b>	Admin.	Admin.	Admin.	Admin.	Admin.
<b>Dispositivo de Autorun</b>					
<b>Total 1</b> (segundos)	48	48	48	48	48
<b>Dispositivo de Recolha</b>					
<b>Total 2</b> (segundos)	103	536	243	171	386
<b>Quantidade de ficheiros copiados</b>	584 Ficheiros 57 pastas	1176 Ficheiros 503 pastas	1507 Ficheiros 564 pastas	2148 Ficheiros 225 pastas	2565 Ficheiros 420 pastas
<b>Tamanho da recolha</b>	3,35GB	5,16GB	4,97GB	4,99GB	5,12GB
<b>Total</b> (1+2)	<b>151s</b> (2min:31s)	<b>584s</b> (9min:44s)	<b>291s</b> (4min:51s)	<b>219s</b> (3min:39s)	<b>434s</b> (7min:14s)

Tabela 15 - Eficiência em diferentes sistemas operativos

Num contexto exterior ao laboratório UbiNET, e apenas a título de interesse, com um computador com cerca de 10 anos, com o sistema operativo Windows 8.1, sem ser formatado há cerca de 3 anos, com um utilizador com privilégios de administração, o mesmo *script* levou cerca de 26 minutos a ser concluído, recolhendo 5,78GB de informação das quais 1836 ficheiros em 293 pastas. Também desta análise podemos depreender que o *hardware* e o estado atual do sistema são relevantes para a eficiência da recolha.





## **CONCLUSÕES E TRABALHOS FUTUROS**

---

De acordo com o estudo realizado, com o desenvolvimento do método de ataque e da aplicação, neste capítulo é realizada uma reflexão final sobre o projeto tendo em conta a hipótese de investigação, contemplando ainda trabalhos futuros para a melhoria deste método de ataque.



## 6. Conclusões e trabalhos futuros

Nesta dissertação, formulou-se como hipótese a concretização de um sistema parametrizável de ataque a informações contidas em sistemas operativos Windows de modo rápido e eficiente.

Foram apresentados alguns exemplos de ferramentas de recolha de informação de sistemas informáticos, destacando-se os dispositivos de âmbito forense devido às características de interesse para este projeto.

Através do estudo da caracterização dos sistemas operativos Windows, foi possível conhecer o seu funcionamento interno, nomeadamente o funcionamento a nível do registo, compreendendo as informações armazenadas por este e, o seu comportamento perante os dispositivos USB. Foi ainda possível analisar o modo como são armazenadas as informações dos utilizadores e aplicações por si utilizadas, determinando a localização das mesmas para os programas mais populares e relevantes para a recolha de informações dos seus utilizadores.

Tendo em conta a recolha de informações de sistemas operativos Windows, foi necessária a análise dos seus sistemas de segurança, sendo notória a preocupação de anular as vulnerabilidades existentes e combater os métodos utilizados por *malware* para se instalar nos sistemas operativos.

Explorar um método de recolha de informações de sistemas operativos, já de si bastante protegidos, foi um desafio aliciante, conquistado através de um dispositivo que explora uma vulnerabilidade da interface USB. Foi possível através dum dispositivo USB, reconhecido pelos sistemas operativos como um teclado genérico, introduzir comandos ou realizando as operações pretendidas de modo parametrizável.

Foi criado um método de ataque para recolha de informações, de modo totalmente parametrizável, permitindo automatizar um conjunto de tarefas. Este sistema de ataque foi desenvolvido para a simulação de um utilizador a executar um script armazenado numa *pendrive* USB, e que de modo automático realiza a cópia da informação pretendida. Com este dispositivo e com a possibilidade de obtenção de uma consola com privilégios de administrador é obter um grande conjunto de informações sobre o sistema alvo e os seus utilizadores.

Como parte integrante do sistema desenvolveu-se uma aplicação que permite a parametrização de todo o processo de recolha de informação permitindo a utilização deste método num vasto leque de cenários possíveis de atuação, como cenários de ataque ou *hacking*, de investigação forense ou de resposta a incidentes.

### *“Como nos podemos proteger deste tipo de ataques?”*

O dispositivo USB utilizado no sistema desenvolvido é, neste momento, válido para todos os sistemas operativos Microsoft Windows, e para os restantes sistemas operativos como o MacOS ou mesmo Linux, posto que o dispositivo é reconhecido através de um driver de teclado genérico, deixando os produtores dos Sistemas Operativos de “mãos atadas” pelas implicações da desativação dos *drivers* genéricos. Assim, cabe aos administradores de sistemas, no caso das organizações, e aos indivíduos, de um modo geral, ponderarem sobre a possível quebra de segurança que esta característica proporciona, tomando a decisão de desativar as portas USB, ou de recorrerem a pequenos utilitários que limitam a sua utilização.

Assim, são várias as conclusões possíveis decorrentes da realização deste trabalho, principalmente, a não utilização de contas com privilégios de administração para uma utilização regular, uma vez que é possível recolher as informações pretendidas ou mesmo efetuar as alterações nos sistemas para um acesso continuado.

Para a obtenção de mais segurança no armazenamento de ficheiros, guardados numa pasta de sistema, deve ser o próprio sistema operativo a oferecer uma camada extra de proteção no acesso aos ficheiros, por requerer privilégios elevados, apesar de ser necessário algum cuidado para não se eliminar nenhum ficheiro de sistema.

Apesar de todo o esforço na deteção de *malware* em dispositivos USB, este ainda requer uma especial atenção, totalmente aconselhada na utilização de utilitários limitadores.

É notória a dificuldade em dar como terminado um aliciente projeto como foi este, sendo várias as ideias de possível desenvolvimento no futuro, das quais se sugerem as seguintes: a incorporação de novas ferramentas como o “TestDisk” [65], que possibilita a recuperação de ficheiros eliminados da reciclagem; desenvolver a utilização deste sistema de ataque para permitir o acesso via redes sem fios, permitindo a utilização apenas da *pendrive* de *autorun* por segundos, enquanto as informações são copiadas para um

dispositivo de armazenamento com recurso à rede sem fios, tal como o dispositivo apresentado em [66]; incorporar na aplicação mecanismos que permitam o armazenamento cifrado da informação sem perder velocidade de recolha; desenvolvimento da aplicação para a incorporação de *exploits* no escalonamento de privilégios, caso o cenário de utilização o permita; desenvolvimento e adequação do sistema de ataque para a inclusão do ataque em novos sistemas operativos; o desenvolvimento de um conjunto de perfis adequados a cada tipo de cenário e máquinas alvo, permitindo ao utilizador a seleção de perfis previamente parametrizados, sendo mais rápida a sua adequação ao pretendido.



## **REFERÊNCIAS BIBLIOGRÁFICAS**

---

Ao longo do processo de investigação e de desenvolvimento deste trabalho de dissertação, muitos foram os livros, *sites*, trabalhos e artigos consultados, sendo objetivo deste capítulo listar estas referências, que de algum modo, influenciaram o desenvolvimento do mesmo.





---

## Referências bibliográficas

- [1] Miniwatts Marketing Group, “World Internet Users and 2015 Population Stats,” Miniwatts Marketing Group, Junho 2015. [Online]. Available: <http://www.internetworldstats.com/stats.htm>. [Acedido em 22 Julho 2015].
- [2] intel, “A Guide to the Internet of Things Infographic,” intel, 2015. [Online]. Available: <http://www.intel.com/content/dam/www/public/us/en/images/iot/guide-to-iot-infographic.png>. [Acedido em 22 Julho 2015].
- [3] netmarketshare.com, “Desktop Operating System Market Share,” Net Applications.com, Junho 2015. [Online]. Available: <http://www.netmarketshare.com/operating-system-market-share.aspx?qprid=8&qpcustomd=0>. [Acedido em 22 Julho 2015].
- [4] DistroWatch, “DistroWatch,” DistroWatch, 07 Agosto 2015. [Online]. Available: <http://distrowatch.com/search.php?ostype=All&category=Forensics&origin=All&basedon=All&notbasedon=None&desktop=All&architecture=All&package=All&status=Active>. [Acedido em 07 Agosto 2015].
- [5] R. W. McGrew, “Covert Post-Exploitation Forensics With Metasploit,” em *BLACK HAT USA 2011*, LAS VEGAS, 2011.
- [6] e-fense, “e-fense,” e-fense, [Online]. Available: <https://www.e-fense.com/>. [Acedido em 18 Fevereiro 2014].
- [7] AaccessData, “E-Discovery & Computer Forensics | AccessData,” AaccessData, [Online]. Available: <http://accessdata.com/>. [Acedido em 18 Fevereiro 2014].
- [8] Guidance Software, “Guidance Software - Endpoint Data Security, eDiscovery, Forensics,” Guidance Software, [Online]. Available: <https://www.guidancesoftware.com/>. [Acedido em 18 Fevereiro 2014].

- [9] “Computer Forensic Triage and Collection - Encase Portable,” [Online]. Available: EnCase® Portable is a powerful solution, delivered on a USB device, that allows forensic professionals and non-experts alike to quickly and easily triage and collect vital data in a forensically sound and court-proven manner. You’ll close cases faster and. [Acedido em 2015].
- [10] Guidance Software, “EnCase Portable v4,” Guidance Software, [Online]. Available:  
<https://www.guidancesoftware.com/resources/Pages/doclib/Document-Library/EnCase-Portable-v4.aspx>. [Acedido em 10 Agosto 2015].
- [11] W. REDMOND, “Microsoft and National White Collar Crime Center Make Digital Forensics Tool Available to U.S. Law Enforcement Agencies,” Microsoft Corp., 18 Outubro 2009. [Online]. Available: <http://news.microsoft.com/2009/10/13/microsoft-and-national-white-collar-crime-center-make-digital-forensics-tool-available-to-u-s-law-enforcement-agencies/>. [Acedido em 25 Abril 2015].
- [12] Microsoft, “Microsoft COFEE (Computer Online Forensics Evidence Extractor) tool and documentation, Sep 2009,” Microsoft, 30 Novembro 2009. [Online]. Available: [https://wikileaks.org/wiki/Microsoft\\_COFEE\\_\(Computer\\_Online\\_Forensics\\_Evidence\\_Extractor\)\\_tool\\_and\\_documentation,\\_Sep\\_2009](https://wikileaks.org/wiki/Microsoft_COFEE_(Computer_Online_Forensics_Evidence_Extractor)_tool_and_documentation,_Sep_2009). [Acedido em 15 Abril 2015].
- [13] Volatility Foundation, “The Volatility Foundation - Open Source Memory Forensics,” Volatility Foundation, 11 Agosto 2015. [Online]. Available: <http://www.volatilityfoundation.org/>. [Acedido em 13 Fevereiro 2014].
- [14] F. I. M. e. P. A. Bruno Werneck Pinto Hoelz, XI Simpósio Brasileiro de Segurança da Informação e de Sistemas Computacionais – SBSeg 2011, Brasília: Sociedade Brasileira de Computação - SBC, 2011.
- [15] E. Mullis e S. White, “Win-UFO,” Win-UFO, 2015. [Online]. Available: <http://win-ufo.org>. [Acedido em 13 Fevereiro 2014].

- 
- [16] Mandiant - A FireEye Company, "Mandiant - Security Consulting Services," Mandiant, 06 Fevereiro 2015. [Online]. Available: <https://www.mandiant.com/resources/download/redline>. [Acedido em 06 Fevereiro 2015].
- [17] Mandiant, "Redline User Guide," 2015. [Online]. Available: [https://dl.mandiant.com/EE/library/Redline1.14\\_UserGuide.pdf](https://dl.mandiant.com/EE/library/Redline1.14_UserGuide.pdf). [Acedido em 09 Agosto 2015].
- [18] M. R. e. B. Cogswell, "Sysinternals Freeware," web.archive.org, 22 Setembro 2006. [Online]. Available: <http://web.archive.org/web/20060922223419/http://www.sysinternals.com/>. [Acedido em 19 Agosto 2015].
- [19] M. Russinovich, "Windows Sysinternals," Microsoft, 2015. [Online]. Available: <https://technet.microsoft.com/en-us/sysinternals/bb842062>. [Acedido em 09 Julho 2014].
- [20] Nirsoft, "Nirsoft Tools," Nirsoft, 2015. [Online]. Available: <http://www.nirsoft.net/utils/index.html>. [Acedido em 09 Julho 2014].
- [21] N. Sofer, "NirLauncher - Collection of more than 170 portable utilities from NirSoft," 03 Agosto 2015. [Online]. Available: <http://launcher.nirsoft.net/>. [Acedido em 09 Julho 2015].
- [22] DarkPhoeniX, "InfoHack - reboot.pro," reboot.pro, 19 Junho 2012. [Online]. Available: <http://reboot.pro/files/file/118-infohack/>. [Acedido em 11 Junho 2015].
- [23] COMPUTERONIX, "Gather Computer Information (Remotely)," COMPUTERONIX, 20 Abril 2011. [Online]. Available: <http://community.spiceworks.com/scripts/show/855-gather-computer-information-remotely>. [Acedido em 24 Abril 2015].
- [24] K. G. (Simac), "Copy Userdata to external Drive," Koen Gijsbers (Simac), Setembro 2014. [Online]. Available:

- <http://community.spiceworks.com/scripts/show/2839-copy-userdata-to-external-drive>. [Acedido em 24 Abril 2015].
- [25] IT\_Frank, “Batch tool Great for fun and administration,” IT\_Frank, 06 Junho 2013. [Online]. Available: <http://community.spiceworks.com/scripts/show/1991-batch-tool-great-for-fun-and-administration>. [Acedido em 19 Maio 2014].
- [26] Chris Campbell - obscuresec, “PowerSploit - A PowerShell Post-Exploitation Framework,” obscuresec, 07 Maio 2014. [Online]. Available: <https://github.com/mattifestation/PowerSploit>. [Acedido em 14 Agosto 2015].
- [27] Microsoft, “Types of Script Files,” Microsoft, 2015. [Online]. Available: [https://msdn.microsoft.com/en-us/library/67w03h17\(v=vs.84\).aspx](https://msdn.microsoft.com/en-us/library/67w03h17(v=vs.84).aspx). [Acedido em 08 Agosto 2015].
- [28] B. Wilhite, “Get-ComputerInfo - Query Computer Info From Local/Remote Computers - (WMI),” Microsoft, 06 Março 2013. [Online]. Available: <https://gallery.technet.microsoft.com/scriptcenter/Get-ComputerInfo-Query-23dd6042#content>. [Acedido em 26 Julho 2015].
- [29] Microsoft, “Windows Management Instrumentation Command-line,” Microsoft, 2005. [Online]. Available: [https://technet.microsoft.com/en-us/library/Cc784189\(v=WS.10\).aspx](https://technet.microsoft.com/en-us/library/Cc784189(v=WS.10).aspx). [Acedido em 08 Maio 2015].
- [30] Microsoft, “A história do Windows,” Microsoft, Novembro 2013. [Online]. Available: <http://windows.microsoft.com/pt-pt/windows/history?woldogcb=0#T1=era0>. [Acedido em 16 Agosto 2015].
- [31] Microsoft, “Windows lifecycle fact sheet,” Microsoft, Julho 2015. [Online]. Available: <http://windows.microsoft.com/en-us/windows/lifecycle>. [Acedido em 16 Agosto 2015].
- [32] Microsoft Corporation, “Microsoft Computer Dictionary.--5th ed.,” em *Microsoft Computer Dictionary.--5th ed.*, Redmond, Washington, Microsoft Press, 2002, p. 445.

- [33] M. Russinovich, "Inside the Registry," Windows NT Magazine, [Online]. Available: <http://technet.microsoft.com/en-us/library/cc750583.aspx>. [Acedido em 29 Dez 2013].
- [34] S. Khadsare, "Windows forensics," 04 Jan 2013. [Online]. Available: <http://www.slideshare.net/santoshkhadsare/windowsforensics>. [Acedido em 29 Dez 2013].
- [35] P. P. K. Pragati Pawar, "Security for Windows Registry Using Carving," *International Journal of Scientific and Research Publications*, vol. Volume 3, Abril 2013.
- [36] P. K. Boonlia, "Registry forensics," 21 Novembro 2011. [Online]. Available: <http://www.slideshare.net/boonlia/registry-forensics-10249175>. [Acedido em 03 Janeiro 2014].
- [37] L. Shederer, "ERUNT - The Emergency Recovery Utility NT," 20 10 2005. [Online]. Available: <http://www.larshederer.homepage.t-online.de/erunt/>. [Acedido em 05 01 2014].
- [38] "Windows Registry Recovery," MiTeC, [Online]. Available: <http://www.mitec.cz/wrr.html>. [Acedido em 16 Agosto 2015].
- [39] AccessData Group, Inc., "Registry Viewer," AccessData Group, Inc., 23 Setembro 2014. [Online]. Available: <http://accessdata.com/product-download/digital-forensics/registry-viewer-1-8-0-5>. [Acedido em 16 Agosto 2015].
- [40] B. Anderson, A. Rabie e B. Anderson, *Seven Deadliest USB Attacks*, Oxford: Elsevier, Inc., 2010.
- [41] A. J. Tanushree Roy, "Windows Registry Forensics: An Imperative Step in Tracking Data Theft via USB Devices," em *(IJCSIT) International Journal of Computer Science and Information Technologies*, 2012.
- [42] D. Cowen, "Hacking Exposed - Computer Forensics Blog," 28 Agosto 2013. [Online]. Available:

- <http://hackingexposedcomputerforensicsblog.blogspot.pt/2013/08/daily-blog-66-understanding-artifacts.html>. [Acedido em 18 01 2014].
- [43] Microsoft, “Nomes de ficheiros abertos e guardados anteriormente apresentada na típica caixas de diálogo estilo do Explorador de Windows no Windows XP,” Microsoft, 24 08 2007. [Online]. Available: <http://smallbusiness.support.microsoft.com/pt-pt/kb/322948>. [Acedido em 18 01 2014].
- [44] T. Northrup, “Windows Vista Security and Data Protection Improvements,” Microsoft, 01 Junho 2005. [Online]. Available: <https://technet.microsoft.com/en-us/library/cc507844.aspx>. [Acedido em 15 Agosto 2015].
- [45] Microsoft, “What's New in Client Security,” Microsoft, 04 Junho 2009. [Online]. Available: <https://technet.microsoft.com/en-us/library/dd571087%28v=ws.10%29.aspx>. [Acedido em 15 Agosto 2015].
- [46] Microsoft, “What's Changed in Security Technologies in Windows 8,” Microsoft, 12 Abril 2013. [Online]. Available: <https://technet.microsoft.com/library/dn169048.aspx>. [Acedido em 28 Agosto 2015].
- [47] Microsoft, “What's new in Windows 10,” Microsoft, 01 Maio 2015. [Online]. Available: <https://technet.microsoft.com/en-us/library/dn986867%28v=vs.85%29.aspx>. [Acedido em 28 Agosto 2015].
- [48] C. L. A. E. A. N. Ivan Firdausi, “Analysis of Machine Learning Techniques Used in Behavior-Based Malware Detection,” *Second International Conference on Advances in Computing, Control, and Telecommunication Technologies*, n° MALWARE DETECTION, pp. 201 - 203, 2010.
- [49] L. Zeltser, “How antivirus software works: Virus detection techniques,” TechTarget, Outubro 2011. [Online]. Available: <http://searchsecurity.techtarget.com/tip/How-antivirus-software-works-Virus-detection-techniques>. [Acedido em 30 Agosto 2015].

- [50] Sandisk, “Sandisk Support,” Sandisk, 2009. [Online]. Available: <http://u3.sandisk.com/>. [Acedido em 28 Novembro 2014].
- [51] SRLabs, “BadUSB,” SRLabs, 2-7 Agosto 2014. [Online]. Available: <https://srlabs.de/badusb/>. [Acedido em 16 Agosto 2014].
- [52] A. Greenberg, “Why the Security of USB Is Fundamentally Broken,” Wired, 31 Julho 2014. [Online]. Available: <http://www.wired.com/2014/07/usb-security/>. [Acedido em 16 Agosto 2014].
- [53] SRLabs, “BadUSB Exposure,” SRLabs, [Online]. Available: <https://opensource.srlabs.de/projects/badusb>. [Acedido em 28 Agosto 2015].
- [54] Hak5, “USB Rubber Ducky,” Hak5, [Online]. Available: <https://forums.hak5.org/index.php?/forum/56-usb-rubber-ducky/>. [Acedido em 14 Maio 2015].
- [55] “Nova campanha de distribuição de CTB-Locker Ramsonware,” CERT.PT, 2015. [Online]. Available: <http://fe02.cert.pt/index.php/alertas/1740-nova-campanha-de-distribuicao-de-ctb-locker-ramsonware>. [Acedido em 30 Agosto 2015].
- [56] T. Mattison, “Duckyscript - hak5darren/USB-Rubber-Ducky Wiki - GitHub,” Hack5darren, 29 Julho 2014. [Online]. Available: <https://github.com/hak5darren/USB-Rubber-Ducky/wiki/Duckyscript>. [Acedido em 08 Maio 2015].
- [57] hak5darren/USB-Rubber-Ducky, “Payloads - hak5darren/USB-Rubber-Ducky,” GitHub, 08 Maio 2015. [Online]. Available: <https://github.com/hak5darren/USB-Rubber-Ducky/wiki/Payloads>. [Acedido em 08 Maio 2015].
- [58] overwraith, “Payload runexe from sd,” 20 Abril 2015. [Online]. Available: <https://github.com/hak5darren/USB-Rubber-Ducky/wiki/Payload---runexe-from-sd>. [Acedido em 08 Maio 2015].
- [59] T. Mattison, “Payload retrieve sam and system from a live file system,” hak5darren/USB-Rubber-Ducky, 29 Julho 2014. [Online]. Available:

- <https://github.com/hak5darren/USB-Rubber-Ducky/wiki/Payload---retrieve-sam-and-system-from-a-live-file-system>. [Acedido em 08 Maio 2015].
- [60] overwraith, “Payload mimikatz payload,” hak5darren/USB-Rubber-Ducky, 30 Junho 2013. [Online]. Available: <https://github.com/hak5darren/USB-Rubber-Ducky/wiki/Payload---mimikatz-payload>. [Acedido em 08 Maio 2015].
- [61] T. Mattison, “Payload hide cmd window,” hak5darren/USB-Rubber-Ducky, 23 Julho 2014. [Online]. Available: <https://github.com/hak5darren/USB-Rubber-Ducky/wiki/Payload---hide-cmd-window>. [Acedido em 08 Maio 2015].
- [62] Lab UbiNET, “Lab UbiNET - Segurança Informática e Cibercrime,” Lab UbiNET, 2015. [Online]. Available: <http://ubinet.ipbeja.pt/>. [Acedido em 25 Agosto 2015].
- [63] SHADOWDEFENDER.COM, “Shadow Defender,” SHADOWDEFENDER.COM, 20 Julho 2015. [Online]. Available: <http://www.shadowdefender.com/>. [Acedido em 31 Agosto 2015].
- [64] Net Market Share, “Desktop Operating System Market Share,” Net Market Share, 30 Agosto 2015. [Online]. Available: <https://www.netmarketshare.com/operating-system-market-share.aspx?qprid=10&qpcustomd=0>. [Acedido em 31 Agosto 2015].
- [65] CGsecurity.org, “TestDisk Download,” <http://www.cgsecurity.org/>, 18 Abril 2015. [Online]. Available: [http://www.cgsecurity.org/wiki/TestDisk\\_Download](http://www.cgsecurity.org/wiki/TestDisk_Download). [Acedido em 28 Agosto 2015].
- [66] SanDisk, “SanDisk Connect Wireless Stick,” SanDisk, Julho 2015. [Online]. Available: <https://www.sandisk.com/home/mobile-device-storage/connect-wireless-stick>. [Acedido em 26 Agosto 2015].
- [67] M. Russinovich, “TN PsInfo,” Microsoft, 28 Abril 2010. [Online]. Available: <https://technet.microsoft.com/en-us/sysinternals/bb897550>. [Acedido em 20 Agosto 2015].



- [68] Microsoft, “Volume Shadow Copy Service Overview,” Microsoft, [Online]. Available: [https://msdn.microsoft.com/en-us/library/aa384649\(v=vs.85\).aspx](https://msdn.microsoft.com/en-us/library/aa384649(v=vs.85).aspx). [Acedido em 04 Agosto 2015].
- [69] Proneer - Digital Forensics Tools, “Proneer - GitHub,” Proneer - Digital Forensics Tools, Agosto 2013. [Online]. Available: <https://code.google.com/p/proneer/>. [Acedido em 04 Agosto 2015].
- [70] candera - GitHub, “candera,” GitHub, 29 Abril 2015. [Online]. Available: <https://github.com/candera>. [Acedido em 04 Agosto 2015].
- [71] Microsoft, “Event Logs,” Microsoft, 02 Fevereiro 2014. [Online]. Available: <https://technet.microsoft.com/en-us/library/cc722404.aspx>. [Acedido em 04 Agosto 2015].
- [72] AccessData, “Forensic Toolkit (FTK),” AccessData, [Online]. Available: <http://accessdata.com/solutions/digital-forensics/forensic-toolkit-ftk>. [Acedido em 02 Outubro 2014].
- [73] ntsecurity.nu, “PMDump - ntsecurity.nu,” Arne Vidstrom, [Online]. Available: <http://ntsecurity.nu/toolbox/pmdump/>. [Acedido em 02 Outubro 2014].
- [74] Belkasoft Live RAM Capturer, “Belkasoft Live RAM Capturer,” Belkasoft , [Online]. Available: <http://forensic.belkasoft.com/en/ram-capturer>. [Acedido em 02 Outubro 2014].
- [75] Mandiant , “Mandiant Memoryze,” Mandiant , 23 Julho 2013. [Online]. Available: <https://www.mandiant.com/resources/download/memoryze>. [Acedido em 02 Outubro 2014].
- [76] Michael Cohen, “rekall - WinPMEM,” Rekall Memory Forensic Framework, 27 Agosto 2014. [Online]. Available: <https://github.com/google/rekall/tree/master/tools/windows/winpmem>. [Acedido em 02 Outubro 2014].
- [77] MoonSols , “MoonSols Windows Memory Toolkit,” MoonSols , 2011. [Online]. Available: <http://www.moonsols.com/windows-memory-toolkit/>. [Acedido em 02 Outubro 2014].

- [78] 100dof, “Save Clipboard Here,” 100dof, 27 Novembro 2013. [Online]. Available: <http://100dof.com/windows/save-clipboard-here>. [Acedido em 14 Agosto 2015].
- [79] CPUID, “CPU-Z,” CPUID, 12 Agosto 2015. [Online]. Available: <http://www.cpubid.com/software/cpu-z.html>. [Acedido em 24 Agosto 2015].
- [80] É. Pinto, “Windows 10 - Forensics Facts,” High54security, 31 Julho 2015. [Online]. Available: <http://high54security.blogspot.co.uk/2015/07/windows-10-forensics-facts.html>. [Acedido em 26 Agosto 2015].
- [81] OFcom, “UK adults taking online password security risks,” OFcom, 23 Abril 2013. [Online]. Available: <http://media.ofcom.org.uk/news/2013/uk-adults-taking-online-password-security-risks/>. [Acedido em 04 Julho 2015].
- [82] B. DELPY, “mimikatz | Blog de Gentil Kiwi,” Benjamin DELPY, 25 Agosto 2015. [Online]. Available: <http://blog.gentilkiwi.com/mimikatz>. [Acedido em 30 Agosto 2015].
- [83] Microsoft TechNet, “Cipher,” Microsoft, 2015. [Online]. Available: <https://technet.microsoft.com/en-us/library/bb490878.aspx>. [Acedido em 21 Abril 2015].
- [84] Stephenjudge, “stephenjudge/TCHunt,” Stephenjudge, 28 Agosto 2011. [Online]. Available: <https://github.com/stephenjudge/TCHunt>. [Acedido em 28 Maio 2015].
- [85] Magnet Forensics, “Encrypted Disk Detector,” Magnet Forensics, 22 Abril 2013. [Online]. Available: <https://www.magnetforensics.com/free-tool-encrypted-disk-detector/>. [Acedido em 14 Março 2015].
- [86] Punch Security, “Skype sneak,” Punch Security, [Online]. Available: <http://www.punchsecurity.com/#!/skypesneak/ca0l>. [Acedido em 02 Outubro 2014].
- [87] t. f. e. Wikipedia, “Windows 7 - Wikipedia, the free encyclopedi,” Wikipedia, the free encyclopedi, [Online]. Available: [http://en.wikipedia.org/wiki/Windows\\_7](http://en.wikipedia.org/wiki/Windows_7). [Acedido em 21 01 2014].

- [88] M. E. a. A. R. A. Neil, “Fuzzy Crime Investigation Framework for Tracking Data Theft based on USB Storage,” em *International Journal of Computer Applications*, 2013.
- [89] “how to add a vertical line to an excel xy chart,” The Closet Entrepreneur, 08 Junho 2007. [Online]. Available: <http://theclosetentrepreneur.com/how-to-add-a-vertical-line-to-an-excel-xy-chart>. [Acedido em 27 05 2014].
- [90] J. Wittwer, “Timeline Template - How to Create a Timeline,” Vertex42 LLC, 09 Fevereiro 2005. [Online]. Available: <http://www.vertex42.com/ExcelArticles/create-a-timeline.html>. [Acedido em 27 Maio 2014].



## **APÊNDICES**

---



## **Apêndice I - Informações úteis em sistemas Windows**

---

# **INFORMAÇÕES ÚTEIS EM SISTEMAS WINDOWS**

---

Este capítulo descreve as informações úteis a recolher nos sistemas operativos em análise, bem como uma breve descrição de como proceder a essa recolha.



# 1. INFORMAÇÕES ÚTEIS EM SISTEMAS WINDOWS

Com base no estudo do estado da arte, verificou-se que existe um padrão no que são consideradas informações relevantes a obter numa rápida análise ao sistema operativo Microsoft Windows. Sabendo que, neste tipo de ataque, não é possível efetuar a clonagem completa do disco, torna-se fundamental uma abordagem direcionada, na tentativa do que o processo de identificação e recolha da informação seja o mais efetivo possível.

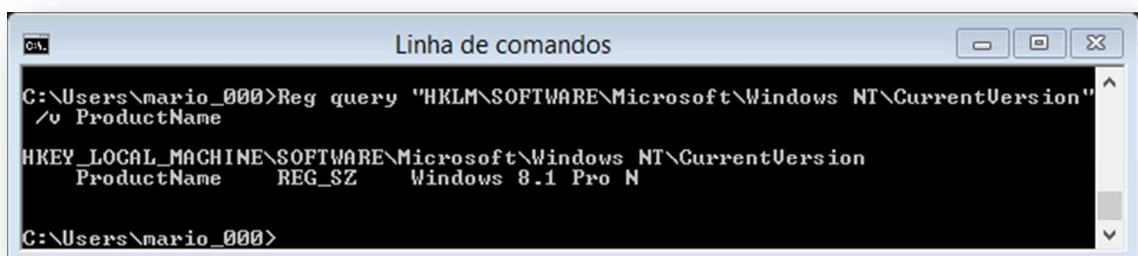
Foram também descritas várias ferramentas que realizam um correto acesso e recolha de informações relevantes no sistema. Assim, a utilização destas ferramentas será uma mais-valia para o objetivo deste projeto.

De seguida são descritas as informações mais relevantes de serem recolhidas nos vários sistemas operativos em análise, bem como o modo como as mesmas serão recolhidas.

## 1.1. Informações de sistema

A recolha das informações de Sistema pode ser efetuada pela consulta direta ao registo (e.g.: `reg.exe query HKEY`), através de ferramentas disponibilizadas pelo próprio sistema operativo (e.g.: `wmic`), ou então através de ferramentas externas como as descritas no ponto 2. “Estado da arte e hipótese de investigação”. Assim, torna-se importante testar as várias soluções e seleccionar a mais adequada para os objetivos propostos, como por exemplo, será necessário saber a versão do sistema operativo.

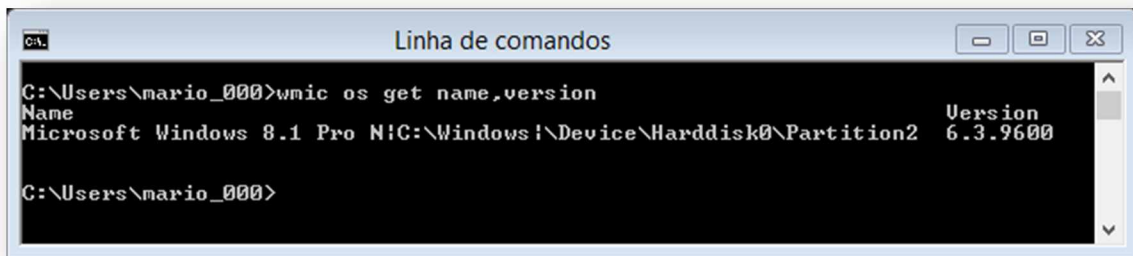
Na consulta direta do registo, poderá ser utilizado o comando apresentado na Figura 27.



```
C:\Users\mario_000>reg query "HKLM\SOFTWARE\Microsoft\Windows NT\CurrentVersion"
/v ProductName
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows NT\CurrentVersion
  ProductName    REG_SZ    Windows 8.1 Pro N
C:\Users\mario_000>
```

Figura 27 - Versão do sistema operativo através do reg.exe

Na consulta, utilizando apenas o comando “wmic” é possível obter o nome, a localização e a versão do sistema operativo, como apresentado na Figura 28.



```
C:\Users\mario_000>wmic os get name,version
Name                               Version
Microsoft Windows 8.1 Pro N       6.3.9600
C:\Users\mario_000>
```

Figura 28 - Versão do sistema operativo através do wmic

Existem aplicações externas ao sistema operativo que permitem o acesso ao nome e à versão do sistema, além de muitas outras informações. O exemplo de uma dessas aplicações é o SysInternals PSInfo.exe [67], como apresentado na Figura 29.



```
C:\Users\mario_000>Psinfo.exe
PsInfo v1.77 - Local and remote system information viewer
Copyright (C) 2001-2009 Mark Russinovich
Sysinternals - www.sysinternals.com

System information for \\DREAMSUAI:
Uptime:                               Error reading uptime
Kernel version:                        Windows 8.1 Pro N, Multiprocessor Free
Product type:                           Professional
Product version:                         6.3
Service pack:                            0
Kernel build number:                     9600
Registered organization:                  DreamSparky
Registered owner:                         9.0000
IE version:                               C:\Windows
Processors:                               4
Processor speed:                          2.6 GHz
Processor type:                           Intel(R) Core(TM) i7-2620M CPU @
Physical memory:                          2 MB
Video driver:                             Intel(R) HD Graphics 3000
C:\Users\mario_000>
```

Figura 29 - Versão do sistema operativo através do PSInfo

No entanto, para os sistemas operativos Microsoft Windows existem outros comandos que permitem saber a versão do sistema, tal como o comando “ver”, que apresenta apenas a versão, ou então o comando “systeminfo /fo list”, este sim apresenta, em formato de lista (/fo list), um completo conjunto de informações sobre o sistema operativo que pode ser complementado pelo resultado do comando “PSInfo.exe -h -s -d /accepteula”, apesar das diferenças não serem significativas. Com os

atributos “-h” este comando revela as correções (*hotfixes*) instaladas no sistema operativo, com o “-s” revela as aplicações instaladas, com o “-d”, a informação dos volumes de armazenamento montados no sistema e, por fim, o atributo “/accepteula” para que não apareça a janela da licença na primeira vez que é executada esta ferramenta.

Vários são os ficheiros que contêm configurações e / ou informações consideradas úteis num contexto de correlação de informações. Destes enunciam-se os seguintes:

- %SystemRoot%\win.ini;
- %SystemRoot%\system.ini.

#### 1.1.1. Data e Hora

A data e a hora de Sistema são dados importantes a analisar em todos os processos de investigação e análise. Numa análise *Live Forensics*, a data e a hora são informações de maior relevância, principalmente devido à possibilidade de determinar o momento em que os eventos de sistema resultantes da investigação sejam delimitados temporalmente. Caso a data e hora de sistema não se encontrem corretos ou se encontrem definidos para um fuso horário diferente do nosso, poderão também induzir em erro os resultados das ferramentas de análise utilizadas.

Estes podem ser recolhidos com os comandos:

- date /t;
- time /t.

#### 1.1.2. Variáveis de ambiente

As variáveis de ambiente podem ser modificadas por processos e aplicações, possibilitando a recolha de alguma informação relevante.

É possível verificar as variáveis de ambiente através do comando:

- set.

#### 1.1.3. Número de série da partição de sistema

Quando um determinado disco rígido é formatado ou modificado, é gerado um número de série para o respetivo volume. Este pode ser entendido como uma assinatura única que poderá ser utilizada como forma de identificação do disco em análise e garantia de que o

mesmo não foi modificado. Para encontrar o número de série do volume de sistema nos vários sistemas operativos, é possível utilizar o seguinte comando:

- `Dir %SystemDrive% /a | find "olume"`

#### 1.1.4. Utilizadores no sistema

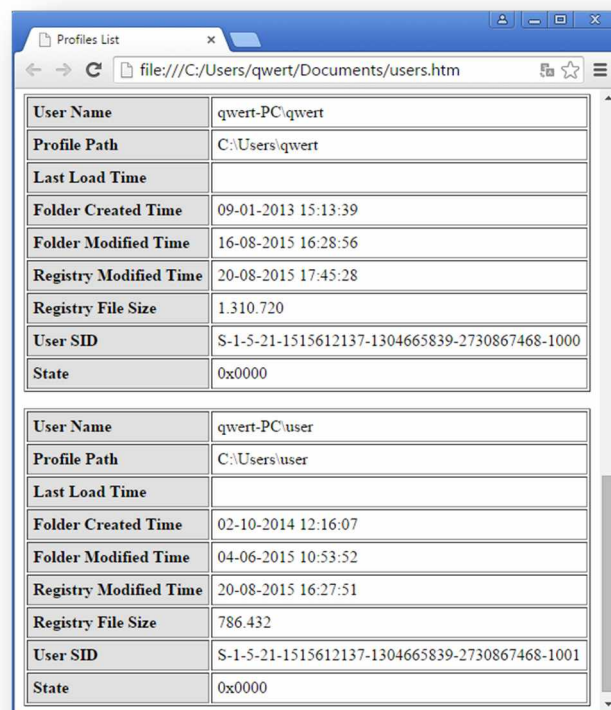
No que diz respeito a informações de utilizadores no sistema, são várias as que poderão ser obtidas, desde um simples comando “whoami”, ou outras como a listagem dos utilizadores através do comando:

- “Net User”

Para mais informação sobre o utilizador em utilização, como a data e hora do último acesso ao sistema, ou o grupo de utilizadores locais a que o mesmo se encontra associado:

- “Net User %USERNAME%”

Com a utilização da ferramenta da Nirsoft, “usersprofilesview.exe”, é possível recolher informações sobre todos os utilizadores ao mesmo tempo, com possibilidade de se visualizar o resultado num *browser*, tal como ilustrado na Figura 30.



User Name	qwert-PC\qwert
Profile Path	C:\Users\qwert
Last Load Time	
Folder Created Time	09-01-2013 15:13:39
Folder Modified Time	16-08-2015 16:28:56
Registry Modified Time	20-08-2015 17:45:28
Registry File Size	1.310.720
User SID	S-1-5-21-1515612137-1304665839-2730867468-1000
State	0x0000

User Name	qwert-PC\user
Profile Path	C:\Users\user
Last Load Time	
Folder Created Time	02-10-2014 12:16:07
Folder Modified Time	04-06-2015 10:53:52
Registry Modified Time	20-08-2015 16:27:51
Registry File Size	786.432
User SID	S-1-5-21-1515612137-1304665839-2730867468-1001
State	0x0000

Figura 30 - Resultado da ferramenta userprofilesview.exe

Já a aplicação da SysInternals LogonSessions permite recolher a informação de todos os inícios de sessão e respetivos processos associados, necessitando para isso de privilégios de administrador.

Também a ferramenta da SysInternals PsLoggedOn permite, sem privilégios de administrador, aceder à data e hora a que os utilizadores registados acederam ao sistema, e não apenas o utilizador atual, como é indicado através da ferramenta systeminfo, descrita atrás.

Como é no Ambiente de Trabalho que os utilizadores com frequência guardam informações recentes ou importantes, é possível guardar uma imagem do ambiente de trabalho, através da ferramenta da Nirsoft nircmd, com o comando:

- `"nircmd.exe savescreenshot"`

Como já referido no ponto 3.2. "Registo", o registo do Windows armazena todo o tipo de eventos de sistema, existindo ferramentas com a capacidade de visualizar as datas e horas a que o sistema é iniciado e desligado. Uma dessas ferramentas é a TurnedOnTimesView, cujo exemplo é apresentado na Figura 31.

The screenshot shows the Nirsoft TurnedOnTimesView application window. The title bar reads "Startup and Shutdown Times". Below the title bar, it says "Created by using TurnedOnTimesView". The main content is a table with the following columns: Startup Time, Shutdown Time, Duration, Shutdown Reason, Shutdown Type, Shutdown Process, and Shutdown Code. The table contains 15 rows of data, including entries for planned disk issues, installation issues, and normal shutdowns.

Startup Time	Shutdown Time	Duration	Shutdown Reason	Shutdown Type	Shutdown Process	Shutdown Code
11/02/2015 19:43:03	11/02/2015 19:43:24	00:00:21				0x00000000
11/02/2015 19:45:02	11/02/2015 19:53:35	00:08:33				0x00000000
11/02/2015 19:54:04	11/02/2015 19:59:58	00:05:54				0x00000000
11/02/2015 20:00:41	11/02/2015 20:02:29	00:01:48	Operating system issue Disk (Planned)	Reiniciar	C:\Windows\System32\FveNotify.exe (DREAMSVAD)	0x80020007
11/02/2015 20:02:42	11/02/2015 20:26:30	00:23:48		Reiniciar	C:\Windows\Explorer.EXE (DREAMSVAD)	0x00000000
11/02/2015 20:26:44	11/02/2015 21:27:51	01:01:07	Operating system issue Installation (Planned)	Reiniciar	Explorer.EXE	0x80020002
11/02/2015 21:28:17	11/02/2015 22:17:02	00:48:45	Operating system issue Installation (Planned)	Reiniciar	Explorer.EXE	0x80020002
11/02/2015 22:17:29	11/02/2015 23:44:02	01:26:33		Desligado	C:\Windows\Explorer.EXE (DREAMSVAD)	0x00000000
12/02/2015 10:37:21	12/02/2015 10:50:51	00:13:30	Operating system issue Installation (Planned)	Reiniciar	Explorer.EXE	0x80020002
12/02/2015 10:51:22	12/02/2015 11:09:28	00:18:06	Operating system issue Installation (Planned)	Reiniciar	Explorer.EXE	0x80020002
12/02/2015 11:09:57	12/02/2015 16:59:16	05:49:19		Reiniciar	C:\Windows\Explorer.EXE (DREAMSVAD)	0x00000000
12/02/2015 16:59:33	12/02/2015 20:00:37	03:01:04				0x00000000

Figura 31 - Nirsoft TurnedOnTimesView

### 1.1.5. Informações de rede

No que diz respeito à recolha de informações de rede existe a condicionante de não efetuar qualquer recolha que implique o possível despoletar de alarmes de rede. Assim,

---

as informações a obter devem conter apenas informações da rede da própria máquina, para existir um tráfego de rede mínimo.

Com o resultado da ferramenta “SystemInfo”, descrita no ponto 1.1. “Informações de sistema”, já são obtidas as informações das placas de rede. No entanto, é possível recolher um conjunto de outras informações que poderão ser relevantes, tais como:

- “`ipconfig /all`” permite visualizar todos os parâmetros de configuração de todos os adaptadores de rede, como as placas de rede *ethernet* ou *wireless*, até às placas de banda larga ou mesmo as *interfaces* lógicas como as *interfaces* do *software* de virtualização;
- “`ipconfig /displaydns`” permite a visualização do conteúdo da cache de resolução DNS. Revela, além dos pedidos recentes de resolução de nomes, o endereço IP do servidor que resolveu o pedido, sendo também possível verificar o endereço IP de um possível servidor DNS local;
- “`netstat -ano`” é uma importante ferramenta de redes, a qual permite visualizar as conexões de rede atuais e o estado dos respetivos portos. Os atributos “-ano” são para revelar todas as conexões incluindo os portos que se encontram à escuta, para mostrar os endereços e portos no formato numérico e para mostrar qual o identificador do processo associado a cada conexão, respetivamente;
- “`arp -a`” permite a visualização da tabela do protocolo de resolução de endereços IPv4, tabela ARP;
- “`netsh int ipv6 show neigh`” permite a visualização da tabela ARP para endereços IPv6;
- “`netsh wlan show all`” permite visualizar o designado de *Wireless System Information Summary*, que revela toda a informação disponível sobre as placas de rede sem fios e respetivas ligações.
- “`route print`” permite a visualização da tabela de encaminhamento IPv4 e IPv6;
- Ficheiro “`hosts`” é um ficheiro de sistema que permite a resolução de nomes do computador, relacionando o endereço IP com o respetivo nome.

- “nbtstat -n” permite a visualização dos nomes de NetBIOS registados localmente, significando que o mapeamento de um nome de NetBIOS para um endereço IP teve êxito;
- “nbtstat -c” permite a visualização do conteúdo da cache com os nomes NetBIOS já mapeados;
- “nbtstat -s” lista o estado das atuais sessões NetBIOS;
- “net accounts” revela as configurações atuais de início de sessão, *password* e domínio;
- “net localgroup” revela o nome dos grupos de utilizador locais;
- “net share” permite a visualização de todos os recursos partilhados no computador;
- “net view” lista os computadores pertencentes ao próprio domínio;
- “nslookup -d” permite a visualização dos registos de DNS e respetivas configurações;
- “rasdial” exhibe o estado das ligações VPN ou mesmo as ligações de banda larga;
- “netsh wlan show profiles” este comando exhibe a rede sem fios à qual o computador se encontra ligado.

Como ferramentas externas ao sistema operativo e com interesse na recolha de informações de rede, temos:

- Nirsoft WifiInfoView, que revela um conjunto importante de informações sobre as redes sem fios captadas pela placa de rede sem fios, se o computador a tiver.

#### 1.1.6. Processos e aplicações

Os processos iniciados facilmente poderão ser visualizados através de ferramentas como a Nirsoft PsList ou o CurrProcess. Este último revela um conjunto alargado de informações. No entanto, se for objetivo apenas as informações base sobre os processos, basta utilizar o seguinte comando:

```
“tasklist /v”
```

Ou então através do comando wmic:

---

```
“wmic process get
name,processid,priority,threadcount,privatepagecount”
```

Tem sido dada uma maior importância ao que corre no início do sistema, e com muita razão já que as chaves de registo começam a ser acedidas antes mesmo do NT *kernel*, as designadas “aplicações persistentes” estão configuradas no registo para serem iniciadas automaticamente, sendo acedidas através de chaves de registo como os seguintes exemplos:

- “HKLM\Software\Microsoft\Windows\CurrentVersion\Run”
- “HKLM\System\CurrentControlSet\Services”
- “HKLM\SOFTWARE\Microsoft\Windows\CurrentVersion\ShellServiceObjectDelayLoad”

São chaves como estas que são acedidas por aplicações como a SysInternals *Autoruns*, que tem vindo a atualizar a aplicação. É possível visualizar, através desta aplicação, todas as entradas de registo correspondentes a aplicações configuradas para serem iniciadas com o sistema, mesmo a funcionar em linha de comandos.

Também é útil visualizar os programas instalados no sistema, o que é possível através da seguinte consulta:

```
“reg.exe query
HKLM\Software\Microsoft\Windows\CurrentVersion\Uninstall /S”
```

Aplicações instaladas através do Windows Store podem ser visualizadas através da seguinte consulta:

```
“Reg query
HKEY_LOCAL_MACHINE\Software\Microsoft\Windows\CurrentVersion\
Appx\AppxAllUserStore\Applications\”
```

### 1.1.7. Atualizações de segurança

Com um simples comando “`wmic qfe`”, é possível verificar se o sistema se encontra atualizado ou ainda não contém a correção de segurança para uma determinada vulnerabilidade.

### 1.1.8. Registo



Muitas serão as chaves de registo que poderão conter informações válidas e que não serão recolhidas por serem mais específicas do utilizador ou do sistema. Deste modo é importante a recolha do registo como um todo (*registry dump*) para possibilitar uma análise posterior. Por motivos de segurança, os sistemas operativos Microsoft Windows não permitem a cópia dos ficheiros que constituem o registo sendo necessário proceder à recolha por outros métodos. Um dos métodos é a utilização da ferramenta da Microsoft “RegDmp”, que efetua a leitura de todo o registo, incluindo toda a sua estrutura, gravando-a num ficheiro de texto, por exemplo:

```
“regdmp.exe > registryDump.txt”
```

Posteriormente, este ficheiro de texto poderá ser consultado com uma simples pesquisa, onde, no exemplo seguinte, é pesquisado o termo URL, obtendo todas as referências a páginas de *Internet*:

```
“find/i "URL" registryDump.txt”
```

Um outro modo de obter os ficheiros que constituem o registo, é através de aplicações que criam um clone desses ficheiros através do *Volume Shadow Copy Service* (VSS) [68], serviço nativo nos sistemas operativos Microsoft Windows. Ferramentas como o ForeCopy [69], o HoboCopy e o ShadowSpawn [70] copiam ficheiros bloqueados pelo sistema ou mesmo ficheiros em utilização, apesar de necessitarem de privilégios de administrador para ser executados. Qualquer destas ferramentas já foram descontinuadas pelos seus autores, não se encontrando a ser desenvolvidas neste momento, apesar de ainda continuarem a ser utilizadas.

O ShadowSpawn está concebido de modo a montar uma unidade com a cópia exata da pasta indicada no seu comando permitindo a visualização desses ficheiros com outras aplicações, ou então a cópia com programas como o *xcopy* ou o *robocopy*, nativos nas versões dos sistemas operativos em análise. Apesar do ShadowSpawn não ter necessidade de ser instalado, tem também a limitação de necessitar do “Visual C++ runtime” instalado na máquina em que vai ser executado, o que poderá ser uma forte condicionante a ser utilizado neste projeto.

#### 1.1.9. Serviços

No que diz respeito aos serviços, o comando “net start” disponibiliza apenas o nome dos serviços ativos no momento. No entanto, através da ferramenta da SysInternals

---

PsService, é possível obter muito mais informação sobre cada um dos serviços, estando este iniciado ou não. É também possível obter a informação de segurança para cada um dos serviços através do argumento “security”.

#### 1.1.10. Tarefas agendadas

As tarefas agendadas de sistema são também facilmente obtidas através do seguinte comando:

```
“schtasks”
```

#### 1.1.11. Eventos

Os eventos são registos utilizados na monitorização e resolução de problemas nos sistemas operativos. Estes registos ficam armazenados num conjunto de ficheiros no qual o sistema operativo guarda automaticamente informações sobre todo o tipo de acontecimentos no sistema, sejam eles a ligação de um periférico ou mesmo algum erro, ou outro. Os registos de eventos [71] encontram-se separados pelas seguintes categorias:

- **Aplicação** — contém os registos dos eventos causados por aplicações ou programas, definidos pelos programadores dessas mesmas aplicações;
- **Segurança** — contém os registos relacionados com as políticas de segurança, como as tentativas de início de sessão, sejam elas válidas ou não, ou mesmo a eliminação de ficheiros. É necessário privilégios de administração para aceder a esta categoria;
- **Configuração** — contém eventos relacionados com as configurações das aplicações ou programas;
- **Sistema** — contém eventos registados pelo Windows System Components, tais como erros de controladores ou simplesmente o registo de um novo dispositivo;
- **Eventos Reencaminhados** — contém os registos de eventos relacionados com computadores remotos.

Os eventos estão associados a ficheiros com as extensões “.evt” ou “.evtx” e “.etl”, guardados na pasta “%SystemRoot%\system32\winevt\logs”.

Podemos aceder aos eventos registados através da sua aplicação nativa “Visualizador de eventos”, nas Ferramentas administrativas, através da ferramenta para linha de

comandos “wevtutil”, ou através da cópia dos próprios ficheiros com a ferramenta RoboCopy, desde que se tenha acesso com privilégios de administração.

Outra possibilidade é a utilização de ferramentas como a SysInternals PsLogList, X-Ways Forensics, ou a EventLogSourcesView da Nirsoft, direcionando o resultado para um ficheiro de texto. Com esta ferramenta não é possível a recolha dos eventos de segurança sem se conhecer as credenciais de administrador.

#### 1.1.12. Memória RAM

O conteúdo da memória RAM é um dos principais pontos de interesse, devido principalmente a toda a informação recente que poderá ser posteriormente extraída. Assim, é necessária a recolha da sua totalidade e, para isso, podemos contar com inúmeras ferramentas, das quais AccessData FTK Imager [72], PMDump [73], Belkasoft Live RAM Capturer [74], Mandiant’s Memoryze [75], WinPMEM [76] ou a MoonSols DumpIt [77] são das mais populares.

#### 1.1.13. Área de transferência

A área de transferência é utilizada com frequência muito elevada, podendo mesmo o utilizador colocar informações sensíveis nesta área temporária que irão desaparecer caso o sistema seja reiniciado.

Várias são as ferramentas que podem ser utilizadas para obter o conteúdo da área de transferência, como por exemplo a aplicação “Save Clipboard Here” [78], torna-se possível através da linha de comandos, armazenar o conteúdo da área de transferência, sendo a principal mais-valia desta aplicação o facto de suportar formatos de imagens, html e texto. No entanto, tem o inconveniente de apresentar uma mensagem de erro no ecrã, em formatos de ficheiros que não reconhece.

Já a ferramenta da Nirsoft “InsideClipboard” permite guardar o conteúdo da área de transferência para um ficheiro que poderá ser lido posteriormente.

#### 1.1.14. Hardware

Muitas das informações gerais de *hardware* já foram referidas através de ferramentas como “SysInternals PSInfo” e “SystemInfo”. No entanto, é possível obter informações mais específicas através de comandos ou ferramentas para o efeito e sem recorrer à análise posterior dos ficheiros de registo, como é o caso das seguintes:

- 
- A Análise dos registos efetuados por placas de banda larga móvel é possível através da seguinte pesquisa:

```
“Dir/t:c/a/s/o/q c: | find/i ".txt" | find/i "modem"”
```

- A identificação do computador:  
“wmic csproduct get name,vendor,identifyingNumber”
- Para obter informações mais detalhadas dos discos rígidos podemos executar o seguinte comando:

```
“wmic diskdrive get name,size,model”
```

- Ou mesmo para informações das respetivas partições:

```
“wmic partition get bootable,size,type”
```

- Para informação sobre a BIOS do sistema:

```
“wmic bios get name,serialnumber,version”
```

- A Ferramenta “Nirsoft USBDeview” permite obter toda a informação armazenada no sistema sobre dispositivos USB que já tenham sido ligados ao mesmo.
- Também da Nirsoft, a ferramenta “BluetoothCL” permite recolher as informações sobre os dispositivos Bluetooth que o sistema armazena.
- Desenvolvida pela CPUID [79], a ferramenta “CPU-Z” tem a possibilidade de ser executada através da linha de comandos recolhendo assim uma vasta informação sobre o *hardware*.

#### 1.1.15. BitLocker

O BitLocker é um sistema de encriptação de unidades presente desde o sistema operativo Windows Vista. Este sistema de encriptação pode ser utilizado na unidade de disco onde o sistema operativo se encontra instalado, ou em qualquer outra unidade ou disco rígido interno, permitindo o acesso à unidade através de uma *password* definida pelo utilizador aquando da sua configuração inicial. No entanto, também pode ser utilizado em unidades de disco amovíveis através do “BitLocker To Go”.

Quando o BitLocker é configurado, é necessário definir como será efetuada a recuperação do acesso à unidade encriptada. Esta poderá ser realizada através de uma chave de recuperação com 48 dígitos repartidos por 8 grupos, ou através de um ficheiro

chave armazenado numa *pendrive* USB, o qual é lido diretamente pela consola de recuperação do BitLocker.

É possível obter a chave de recuperação da unidade encriptada com um simples comando, desde que seja executado com direitos de administrador:

```
“manage-bde -protectors c: -get”
```

#### 1.1.16. Documentos Impressos

Quando o utilizador imprime um documento, são gerados dois ficheiros na pasta “%SystemRoot%\System32\spool\PRINTERS\”, um designado por “*shadow*”, com a extensão “.SHD” e o “*spool*”, com a extensão “.SPL”. Estes ficheiros são automaticamente eliminados pelo sistema se a impressão for bem-sucedida, permanecendo visíveis e passíveis de serem copiados.

#### 1.1.17. Serviço de indexação

Em [80], o serviço de indexação poderá conter inúmeras informações já que é uma base de dados de ficheiros, *emails*, entre outras informações de grande importância, inclusivamente para a criação de um dicionário de palavras para quebrar *passwords*.

Esta indexação é armazenada no seguinte ficheiro “.EDB”:

```
“%ProgramData%\Microsoft\Search\Data\Applications\Windows  
  \Windows.edb”
```

A análise deste ficheiro pode ser realizada através de ferramentas como a Nirsoft ESEDatabaseView, EseDbViewer, X-Ways Forensics, entre outras.

#### 1.1.18. Ficheiros Prefetch

São ficheiros utilizados pelo sistema para guardar informações sobre o início e o encerramento do computador, de modo a acelerar o processo de início do sistema na próxima vez. Estes estão armazenados na pasta “%SystemRoot%\Prefetch”, com a extensão “.pf”, apesar de existirem outros ficheiros na mesma pasta que também fazem parte do mesmo objetivo. Pelo que toda esta pasta poderá ser recolhida para uma análise posterior.

## 1.2. Informações de utilizadores

---

Muitas são as informações de utilizadores que podem ser obtidas no sistema, como demonstrado no ponto 1.1. “Informações de sistema”.

A grande maioria dos utilizadores de sistemas operativos Microsoft Windows utilizam constantemente as mesmas áreas no seu dia-a-dia. Áreas como o “Ambiente de trabalho” e “Os Meus Documentos” são habitualmente utilizadas para guardar informações. Além destas pastas também devem ser tidas em conta outras partições no disco rígido, já que é também prática corrente a utilização de uma segunda unidade para armazenar documentos de forma estruturada.

Dentro de toda a amplitude de informações relevantes dos utilizadores é efetuado o destaque às seguintes:

### 1.2.1. Documentos e ficheiros do utilizador

Um dos alvos será certamente os documentos do Microsoft Office, imagens ou ficheiros de texto. No entanto, não são de descurar outros ficheiros específicos de aplicações conhecidas, como ficheiros compactados, blocos de notas, ferramentas de desenho, entre muitos outros.

O armazenamento na “*cloud*” é uma das áreas a explorar já que existe a possibilidade de serem encontrados vários documentos com informação relevante sobre o utilizador. Deste modo, devemos obter os ficheiros referentes às pastas de aplicações de armazenamento na *cloud*, como por exemplo:

- Microsoft OneDrive — “%UserName%\OneDrive\”;
- Google Drive — “%UserName%\Google Drive\”;
- Apple iCloud — “%UserName%\iCloudDrive\”;

### 1.2.2. Atividade do utilizador

A atividade recente do utilizador poderá ser determinante para a nossa análise, sendo possível obter esta informação de diversos modos, entre os quais listar os ficheiros ou pastas por ordem de modificação com o simples comando “Dir/t:aw/a/s/oN %systemdrive%”, a correlação de várias chaves de registo e eventos, que é efetuada por diversas ferramentas, sendo uma das ferramentas de referência a Nirsoft “LastActivityView”, apesar de necessitar de permissões de administrador.

Outra ferramenta importante para determinar a atividade do utilizador é a Nirsoft “RecentFilesView” que, para apresentar os ficheiros que foram acedidos recentemente, relaciona os atalhos criados pelo sistema na pasta:

```
“%SystemDrive%\Users\%UserName%\Recent”
```

Com o a seguinte chave de registo:

```
“HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Explorer\ComDlg32\OpenSavePidlMRU”
```

### 1.2.3. Imagem do Ambiente de Trabalho

Uma imagem do “Ambiente de Trabalho” poderá ser importante por vários motivos:

- Se o utilizador definir uma fotografia como fundo do “Ambiente de Trabalho”;
- Os ícones no “Ambiente de Trabalho” revelam normalmente as aplicações que o utilizador mais utiliza;

Para recolher uma imagem do “Ambiente de Trabalho”, poderá ser utilizada a ferramenta da Nirsoft “NirCmd” com o comando:

```
“nircmd.exe savescreenshot screenshot.png”
```

### 1.2.4. Contactos

Nos sistemas operativos Microsoft Windows, existem vários pontos de interesse com informações sobre contactos, desde os contactos do utilizador no sistema operativo às listas de contactos de aplicações.

O registo guarda a localização da pasta “Contacts” que, por defeito, é armazenada em:

```
“%SystemDrive%\Users\%UserName%\Contacts”
```

Esta pasta, apesar de pouco utilizada, é um local onde os utilizadores podem criar os seus contactos e defini-los por grupos, ficando cada contacto em ficheiros individuais e com a extensão “.contact”.

No que diz respeito aos contactos armazenados em aplicações, existem ferramentas que extraem as listas de contactos das aplicações, como por exemplo a ferramenta “Skypecontactsview” que permite a extração da lista de contactos do Skype.

---

O Nirsoft “LiveContactsView” permite a extração de contactos do “Windows Live Messenger”.

O Nirsoft “OutlookAddressBookView” permite a obtenção dos contactos do “Outlook”.

Os contactos encontram-se entre as informações partilhadas entre as aplicações “Mail”, “Calendar” e “People”. Caso corretamente configuradas pelo utilizador, permitem o acesso em *plaintext* a cada um dos contactos partilhados, na pasta:

```
“%LocalAppData%\Packages\microsoft.windowscommunicationsapps_xxxxx\LocalState\Indexed\LiveComm\xxxxx\xxxxx\People\AddressBook\”
```

Já as imagens de cada contacto podem ser encontradas na pasta:

```
“%LocalAppData%\Packages\microsoft.windowscommunicationsapps_xxxx\LocalState\LiveComm\xxxx\xxxx\UserTiles\”
```

Os ficheiros apresentados não contêm extensões. No entanto são ficheiros de imagem, bastando inserir a extensão para os visualizar.

### 1.2.5. Passwords

As *passwords* são sempre o principal foco de atenção nos ataques informáticos. Em [81] está divulgado um estudo sobre a utilização da *password* em abril de 2013. Entre outras conclusões, destaca-se o facto de 55% dos adultos do Reino Unido afirmarem utilizar a mesma *password* para acesso a vários sites. Deste modo, a obtenção de pelo menos uma *password* será sempre um ponto de partida para a tentativa de entrada noutros *sites* ou aplicações com estas credenciais.

No *site* da Nirsoft está disponibilizado um conjunto de ferramentas especificamente para a obtenção de *passwords* de aplicações, a saber:

- MessenPass, para aplicações de conversação instantânea (*chat*), como o Google Talk, e o Windows Live Messenger;
- Mail PassView, para aplicações de *email*, como o Microsoft Outlook e o Mozilla Thunderbird;



- Dialupass, para ligações por *modem (dialup)*, *Remote Access Service (RAS)* e *Virtual Private Network (VPN)*;
- BulletsPassView, para a recolha de *passwords* escondidas atrás de “asteriscos”;
- Network Password Recovery, para obter as *passwords* armazenadas no sistema de partilhas na rede e em servidores remotos;
- WebBrowserPassView, para a recolha de informações e *passwords* nos *browsers* Internet Explorer (Version 4.0 - 11.0), Mozilla Firefox, Google Chrome, Safari, e Opera;
- IE PassView, especificamente para a recolha de informações e *passwords* em versões do Browser Internet Explorer até à sua versão 11:
- PasswordFox, para a recolha de informações e *passwords* especificamente no *browser* Mozilla Firefox;
- ChromePass, para a recolha de informações e *passwords* especificamente no *browser* Google Chrome;
- OperaPassView, para a recolha de informações e *passwords* especificamente no *browser* Opera;
- WirelessKeyView — consegue obter as chaves / *passwords* (WEP / WPA / WPA2) das redes sem fios configuradas no serviço “WLAN AutoConfig”, apesar de necessitar de privilégios de administrador;
- VNCPassView, para a recolha de *passwords* armazenadas no registo especificamente de aplicações VNC, como TightVNC e UltraVNC;
- Mimicatx — esta ferramenta [82] consegue obter a *password* do utilizador em *plaintext*, bastando uma consola com privilégios de administração.

#### 1.2.6. Itens encriptados

Os ficheiros cifrados trazem maior segurança ao utilizador, pelo que também maior será a importância das suas informações.

A Microsoft disponibiliza a ferramenta “Cipher” [83] permitindo visualizar ou modificar o estado da encriptação de ficheiros ou pastas. É deste modo possível utilizar esta ferramenta para pesquisar por ficheiros ou pastas encriptados, através do seguinte comando:

```
“cipher /s:c: /u /n /c /h”
```

Esta ferramenta apenas irá encontrar ficheiros ou pastas que foram cifrados utilizando o sistema de encriptação “Encrypted File System” (EFS), em unidades de armazenamento formatados através de sistemas de ficheiros NTFS.

A ferramenta “TCHunt” [84] é utilizada para pesquisar possíveis ficheiros encriptados por métodos utilizados em ferramentas como “TrueCrypt”.

O “Encrypted Disk Detector” [85] é uma ferramenta que rapidamente verifica se as unidades de armazenamento em utilização pelo sistema são unidades encriptadas através de TrueCrypt, PGP, Safeboot ou Bitlocker. Para ser executada necessita de privilégios de administrador, bastando o seguinte comando:

```
“EDD.exe /accepteula /Batch > edd.txt”
```

Na Figura 32 é apresentada uma consola de administração com o resultado desta ferramenta onde é possível observar que foi encontrada uma partição encriptada com BitLocker e o volume de letra D: com TrueCrypt.

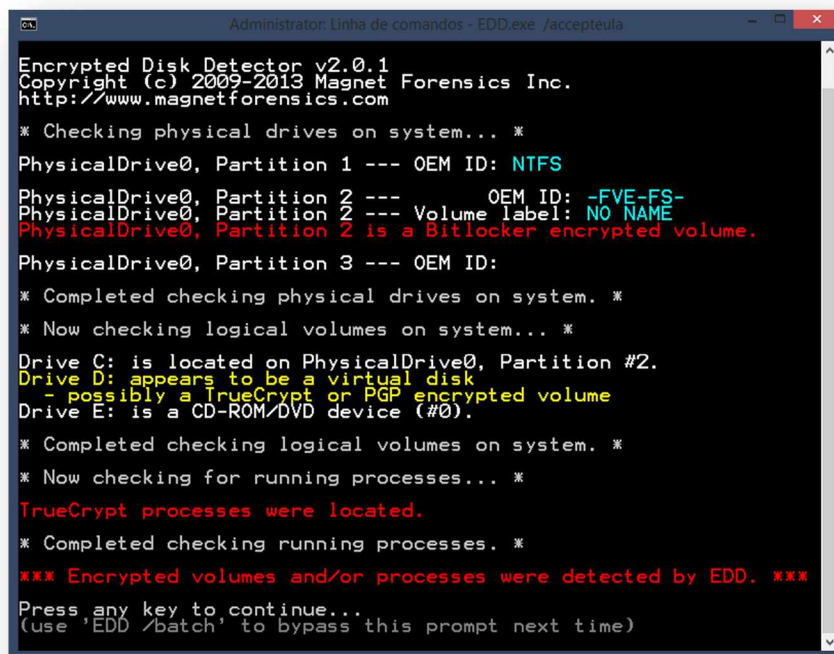


Figura 32 - Encrypted Disk Detector

### 1.2.7. Itens Ocultos

Um dos modos de pesquisar ficheiros e pastas ocultos na unidade de sistema é através do comando:

```
“dir /s /a:dh %SystemDrive%\*”
```

### 1.2.8. Itens eliminados

A “Reciclagem” acolhe os ficheiros eliminados pelo utilizador, podendo muitos deles conter informações relevantes. Na realidade, esses ficheiros não foram eliminados, permanecendo apenas ocultos para que o utilizador consiga recuperá-los. É possível listar o conteúdo da reciclagem na unidade de sistema através do seguinte comando:

```
“dir /a %SystemDrive%\$Recycle.Bin /s”
```

No entanto, o objetivo é obter esses ficheiros, o que poderá ser efetuado através do seguinte comando:

```
“robocopy c:\$Recycle.Bin e:\Destino\ /mir /mt /r:0 /w:0”
```

### 1.2.9. Perfil no browser

O perfil de utilizador num *browser* é de extrema importância por conter as mais diversas informações do utilizador na sua navegação na *Internet*. Os *browsers* mais populares já utilizam sistemas de encriptação de ficheiros na proteção dos perfis e contas dos utilizadores. No entanto, continua a ser possível a análise “*à posteriori*” de alguns dos dados contidos nas pastas destes perfis. A localização do perfil do utilizador varia com o *browser*, sendo de seguida lista a localização dos *browsers* mais populares:

- Mozilla Firefox:

```
“%LOCALAPPDATA%\Mozilla\Firefox\Profiles\”;
```

- Google Chrome:

```
“%LOCALAPPDATA%\Google\Chrome\User Data\  
<Profile name>\”;
```

A pasta “<Profile name>” é utilizada quando o utilizador não tem um perfil guardado, sendo substituído pela pasta “profile 1” a “profile X” conforme o número de perfis definidos.

- Microsoft Edge:

```
“%localappdata%\Packages\Microsoft.Windows.Spartan_x  
xxxxxx\AC\Spartan\User/”
```

### 1.2.10. Favoritos

---

Os favoritos não são mais do que atalhos para endereços de *sites* na *Internet*, cujo objetivo é permitir aos utilizadores armazenar os *sites* de maior interesse sem que tenham de memorizar os seus endereços.

Sabendo que os favoritos são uma fonte importante de informação sobre o utilizador, torna-se necessário proceder à cópia dos mesmos tendo em conta que a localização dos favoritos depende essencialmente do *browser* utilizado. Como referido no ponto 1.2.9 “Perfil no *browser*”, os *browsers* mais populares armazenam na pasta com o perfil do utilizador, entre outras informações, os favoritos do utilizador, com exceção do Internet Explorer que utiliza a pasta “%UserProfile%\Favorites\”.

#### 1.2.11. Transferências

Os ficheiros obtidos através da *Internet* também são importantes e são, por defeito, guardados na seguinte pasta “%UserProfile%\Downloads\”.

#### 1.2.12. E-mails

A utilização de um cliente de *email* local, como o “Microsoft Outlook” ou o “Mozilla Thunderbird”, será também uma importante fonte de informação. É assim necessário contemplar os vários clientes de *email* e as respetivas características, no processo de recolha das suas informações.

O cliente de *email* Microsoft Outlook utiliza um ficheiro com a extensão “.pst” para armazenar toda a informação do utilizador, onde entre outras, estão informações dos emails, calendários, contactos, tarefas e notas. A localização, por defeito, deste ficheiro nos Windows 8 e 10 é na pasta:

“%LocalAppData%\Microsoft\Outlook\”

Para o Windows Vista e 7, é na pasta:

“%AppData%\Local\Microsoft\Outlook\”

Contas de email empresariais que utilizem o Microsoft Exchange ou Outlook.com, é armazenada uma cópia no computador do utilizador e na pasta utilizada para o Microsoft Outlook, mas o ficheiro contém a extensão “.ost”.

No cliente de email Mozilla Thunderbird, os dados do utilizador são guardados na pasta do seu perfil, localizada em:

```
“%AppData%\Roaming\Thunderbird\Profiles\<<Profile name>”
```

As ferramentas da Nirsoft “OutlookAttachView” e “OutlookStatView” conseguem analisar a informação do Microsoft Outlook permitindo a visualização dos atalhos e de estatísticas de utilização, respetivamente.

Com o Lançamento do Windows 8 e respetivas aplicações, apareceu também a aplicação “Mail”. Esta é um cliente de *email* capaz de configurar diversas contas de *email* diferentes para facilitar a usabilidade ao utilizador. No entanto, e como já referido no ponto 1.2.4. “Contactos”, esta partilha as suas informações com as aplicações “Contacts” e “People”.

As informações contidas nos *emails* são armazenadas em locais diferentes, sendo os próprios emails armazenados em ficheiros “.eml”, na pasta:

```
“%LocalAppData%\Packages\microsoft.windowscommunicationsapps_
xxxxxx\LocalState\Indexed\LiveComm\xxxxxx\xxxxxx\Mail”
```

podendo ser lido por qualquer cliente de *email* ou mesmo o bloco de notas. Já os ficheiros anexos aos *emails* encontram-se na seguinte pasta:

```
“%LocalAppData%\Packages\microsoft.windowscommunicationsapps_
xxxxxx\LocalState\LiveComm\xxxxxx\xxxxxx\Att”
```

### 1.2.13. Histórico de endereços digitados

A chave de registo:

```
“HKEY_CURRENT_USER\Software\Microsoft\Internet Explorer\TypedURLs”
```

armazena os últimos endereços digitados no *browser* “Internet Explorer” e poderá ser consultada com uma simples consulta através do “reg query”.

### 1.2.14. Histórico de sites visualizados

No que diz respeito ao novo histórico da navegação na *Internet*, a ferramenta Nirsoft “BrowsingHistoryView” permite a visualização do histórico da navegação de *browsers* como Internet Explorer, Microsoft Edge, Mozilla Firefox, Google Chrome e Apple Safari.

---

No que diz respeito à localização dos dados armazenados, é possível ver o histórico dos *browsers* da Microsoft na seguinte pasta:

“%LocalAppData%\Microsoft\Windows\History”

#### 1.2.15. Ficheiros temporários da *Internet* (Cache)

Os ficheiros temporários da *Internet* podem ser imagens, vídeos, ou algum *malware*. Uma das opções de segurança é precisamente a eliminação destes ficheiros quando o *browser* é fechado. No entanto, é indispensável o seu armazenamento temporário, utilizando a pasta do perfil do utilizador para o efeito, na maioria dos *browsers*, com exceção dos *browsers* da Microsoft, que continuam a utilizar a seguinte pasta por defeito:

“%LocalAppData%\Temp\”

Dependendo do *browser* utilizado, são também utilizadas as seguintes pastas:

- Internet Explorer:

- Até ao Windows 7:

“%LocalAppData%\Microsoft\Windows\Temporary Internet  
Files”

- Do Windows 8 e seguintes:

“%LocalAppData%\Microsoft\Windows\INetCache”

- Microsoft Edge:

“%LocalAppData%\Packages\Microsoft.MicrosoftEdge\_xxxx\AC\  
#!001\MicrosoftEdge\Cache\”

#### 1.2.16. Cookies

Os *cookies* são pequenos ficheiros de texto, encriptados ou não, que vão sendo armazenados no computador enquanto o utilizador vai navegando na *Internet*. São utilizados para fornecer informações aos *sites* visitados, como a identificação do utilizador, do *browser*, entre outras informações, podendo inclusive, permitir o acesso a áreas reservadas de *sites* sem que o utilizador tenha de introduzir as suas credenciais de segurança. São criados com um determinado período de validade, sendo necessário que o utilizador insira novamente as suas credenciais ao visitar o respetivo *site*. Existem ainda

alguns *sites* que fornecem *cookies* de monitorização com o objetivo de relacionar o utilizador com os *sites* que este visita, ficando assim com o histórico de *sites* visitados.

Os *cookies* dos *browsers* Internet Explorer e Edge são armazenados atualmente na seguinte pasta

- Windows 7 e anteriores:  
“%AppData%\Roaming\Microsoft\Windows\Cookies”
- Windows 8 e superior:  
“%LocalAppData%\Microsoft\Windows\INetCookies”

Também acessível através do comando “shell:Cookies” no explorador do Windows.

### 1.2.17. Log's de aplicações

Os registos de Log são normalmente registos de utilização associados às respetivas aplicações. São utilizados pelos programadores das aplicações para correção de erros, estando localizados normalmente na pasta da aplicação dentro do “%AppData%” do respetivo utilizador.

Para se proceder à recolha dos ficheiros de *log* das aplicações, é necessário definir quais as aplicações mais relevantes e qual a localização dos respetivos ficheiros de *log*.

As aplicações de conversação síncrona são sem dúvida de extrema importância, sendo o Skype uma das principais.

O Skype armazena dados como o histórico de conversação, contactos, conversação, dados de perfil, endereços de *email*, chamadas efetuadas e recebidas e respetivos tempos e endereços IP dos utilizadores, ficheiros transferidos, entre outros. Todas estas informações se encontram na pasta:

“%AppData%\Roaming\Skype\”

Existem ferramentas que efetuam a análise destes ficheiros, como é o caso da ferramenta da Nirsoft “Skypelogview” ou o completo programa “Skype Sneak” desenvolvido pelo punchsecurity [86].

Com o Windows 8, apareceu também um novo tipo de aplicações direcionadas para serem integradas na plataforma designada de “Metro”. Estas aplicações armazenam os seus dados na pasta:

---

“%LocalAppData%\Local\Packages\\”

Exemplo deste tipo de aplicações temos o “Twitter App” que é a aplicação da popular rede social. Contudo, armazena, no computador do utilizador, uma base de dados SQLite3, com os seguintes dados, entre outros:

- mensagens;
- pesquisas;
- lista da conta do utilizador;
- lista das contas de que o utilizador é seguidor;
- lista dos últimos “tweets” de contas em que o utilizador é seguidor;
- perfil de utilizador.



## **Apêndice II – Página de ajuda na aplicação**



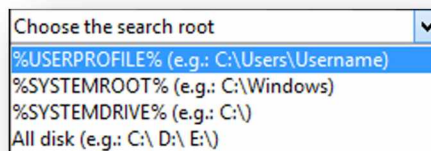
investigation. Finally it is presented the "Generate *Autorun Script*" button whose function is to generate the binary file with the options outlined above, enabling to store directly to file on the *autorun* device.

Since the options contemplated for the collection *script* are necessarily more diverse, as shown in next Figure.

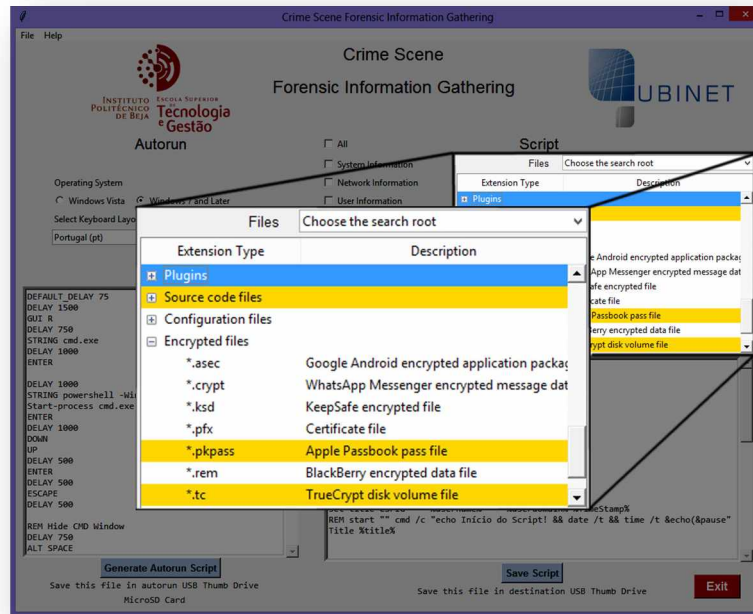


These are the main options that allow to parameterize the gathering *script*. Each selected option will fill the gathering *script* with the respective code.

For research and copy the files you need to select the root in which it will base this selection by choosing an option from the drop-down list with the text "Select the search root". The choices are the folder of the current user, the operating system folder, the root system, or all the disk drives mounted in the system, as shown in next Figure.



Still in the gathering *script* scope, research and file copy is dependent on the extensions thereof, which may be selected from the area shown in next Figure.



In the extensions selection search area is available a list with the most diverse types of extensions, simply double click the left mouse button to select an extension or group of extensions, all selected extensions remain yellow. At the same time they are selected and provided the root of the research is also selected, they are also integrated in the gathering *script*.

After selecting the options you need for the desired gathering you can change the *script*, adapting the code to the desired gathering, either by modifying or adding new commands or tools, either withdrawing some of the not required tools. Finally, just click the button with the text "Save *Script*" to write this *script* on the storage device.

The application also has a menu bar with "File" menu and "Help", as shown in Figure.



In the "File" menu there are the options "Load Profile" and "Save Profile" that let you load a file with a profile and store all the options and changes in a single file and under the number you want. It is therefore possible to store options to apply later, or even send remotely to be applied by someone else.

The "Help" menu contains the usual help related to the application's features and also the "About" that contains the version and scope of application, as illustrated in next Figure.

