FUNDAMENTOS DA FORENSE DIGITAL

Co-funded by the Erasmus+ Programme of the European Union

Financiado pela União Europeia. Os pontos de vista e as opiniões expressas são as do(s) autor(es) e não refletem necessariamente a posição da União Europeia ou da Agência de Execução Europeia da Educação e da Cultura (EACEA). Nem a União Europeia nem a EACEA podem ser tidos como responsáveis por essas opiniões.

Índice

1. Introdução à Informática Forense

A informática forense está relacionada diretamente com a resposta a incidentes, sendo mesmo um dos seus componentes mais importantes, sendo necessária para obter a informação sobre eventos e ações realizadas no sistema em análise. A informática forense é também determinante a nível criminal, investigando as ações passadas nos dispositivos na tentativa de identificar e recolher indícios de crime, que poderá ajudar a decisão em tribunal. Será que nos dias de hoje existem crimes não ciberinstrumentados?

"it is impossible for a criminal to act, especially considering the intensity of a crime, without leaving traces of this presence" (Doctor Edmond Locard, s.d.)[1]

Informática Forense *(Digital forensics)* é entendida como um ramo da ciência forense que estuda e aplica o processo de adquirir, analisar e preservar indícios digitais de modo a estas serem legalmente admissíveis e tecnicamente irrefutáveis em tribunal.

Prova digital é qualquer dado ou informação digital, legalmente admissível (obtenção) e tecnicamente irrefutável (origem, integridade e não repúdio).

Informação digital são todos os dados armazenados ou transmitidos de modo digital, como logs, documentos, emails, base de dados, tráfego de rede, entre muitos outros.

O objetivo da forense digital e resposta a incidentes é:

- Identificar, recolher e preservar as evidências de um cibercrime;
- Interpretar, documentar e apresentar as provas de modo a serem admissíveis em tribunal;
- Compreender as técnicas e métodos usados pelos criminosos;
- Realizar resposta a incidentes para evitar perdas de propriedade intelectual, financeiras e de reputação durante um ataque;
- Conhecer a legislação de diversas regiões;
- Conhecer os processos de manipulação de plataformas digitais, tipos de dados e sistemas operativos;
- Identificar as ferramentas apropriadas para a investigação forense;
- Recuperar ficheiros excluídos, ficheiros ocultos e dados temporários que podem ser utilizados como evidência;
- Apoiar a acusação na investigação de cibercrime;
- Proteger a organização de incidentes semelhantes no futuro.

---

[1] https://www.crimemuseum.org/crime-library/forensic-investigation/edmond-locard

1.1. Responsabilidades do Perito

Um analista forense, bem como o perito informático é o responsável legal por analisar o conteúdo digital dos equipamentos que lhe serão confiados, entregando um relatório designado por Relatório de perícia forense digital. Após ter conhecimento das sanções em que incorre na sua recusa ou incumprimento, ler a seguinte frase perante a autoridade judiciária ou o magistrado, "comprometo-me, por minha honra, a desempenhar fielmente as funções que me são confiadas" e assinar o auto de compromisso. Deste modo, o perito toma compromisso em efetuar a análise e o relatório de perícia forense digital, dispensando o termo de compromisso os peritos que forem funcionários públicos e intervierem no exercício das suas funções. Será informado sobre o processo e sobre os quesitos a dar resposta. As sanções que incorre por recusa ou incumprimento estão presentes no Código de Processo Penal Português no Artigo 91.º, n.º4. No que diz respeito à entrega do relatório pericial, o Art. 157.º do mesmo Código de Processo Penal, indica que o relatório deve conter as respostas e conclusões devidamente fundamentadas, devendo ser apresentado num prazo não superior a 60 dias.

É imperativo que o relatório apresente apenas informações verdadeiras, já que informações incorretas são puníveis com pena de prisão de seis meses a três anos ou com multa não inferior a 60 dias, conforme indicado no Art. 360.º.

1.2. Aplicação da forense digital

As áreas de atuação da forense digital são cada vez mais abrangentes, onde antes seriam apenas analisados os discos rígidos e outros suportes de armazenamento de informação, atualmente poderá ser necessária a recolha e análise de dados em memórias voláteis (atuação em live-data forensics) ou mesmo dados de tráfego de rede (network forensics), dados armazenados em dispositivos móveis (mobile forensics), dados armazenados em sistemas distribuídos em Clouds na Internet, entre muitos outros.

Edmond Locard (Figura 1), afirmou que:

“it is impossible for a criminal to act, especially considering the intensity of a crime, without leaving traces of this presence”

Nos crimes que de algum modo envolvem uma componente digital, crime ciberinstrumental e ciberdependente (R.Bravo) e de acordo com a afirmação de Edmond Locard, existe uma maior possibilidade de serem deixados indícios digitais, relacionando o crime com a utilização de meios digitais.

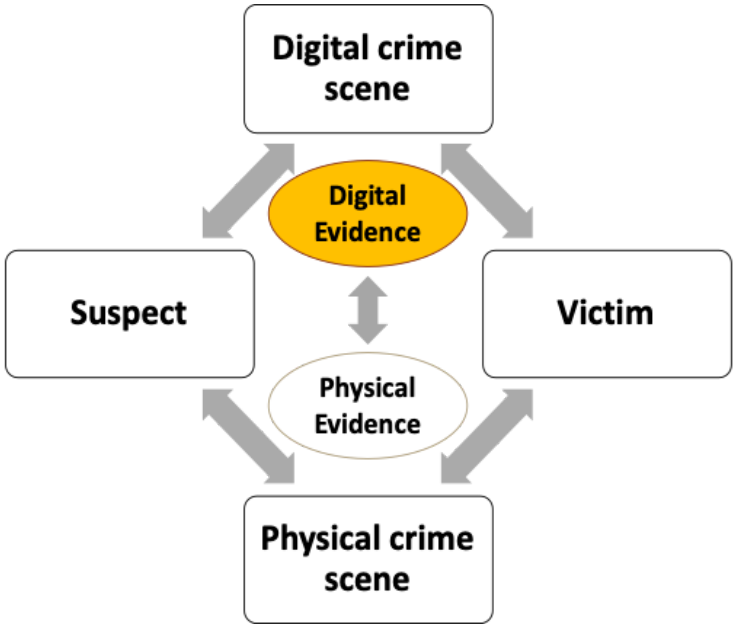


Figura 1 - Esquema Edmond Locard

Fonte: https://www.crimemuseum.org/crime-library/forensic-investigation/edmond-locard

A forense digital não é considerada uma ciência exata, sendo possível que o mesmo relatório de forense digital analisado por diferentes pessoas, tenha diferentes entendimentos, daí que seja essencial a preocupação em assegurar os princípios básicos da segurança da informação (Figura 2), confidencialidade, integridade e não repúdio. Deste modo a forense digital terá de ser necessariamente:

LEGALMENTE ADMISSÍVEL e TECNICAMENTE IRREFUTÁVEL

A utilização de técnicas de universalmente aceites, cumprindo com o disposto nas leis nacionais na tentativa de por cada questão em investigação uma resposta o mais completa possível, sendo a regra dos 7 porquês a forma mais completa de resposta:

“O quê? Onde?, Quando?, Como?, Quem?, Porquê? e Quanto?”

Inspetor-coordenador Rogério Bravo – Polícia Judiciária

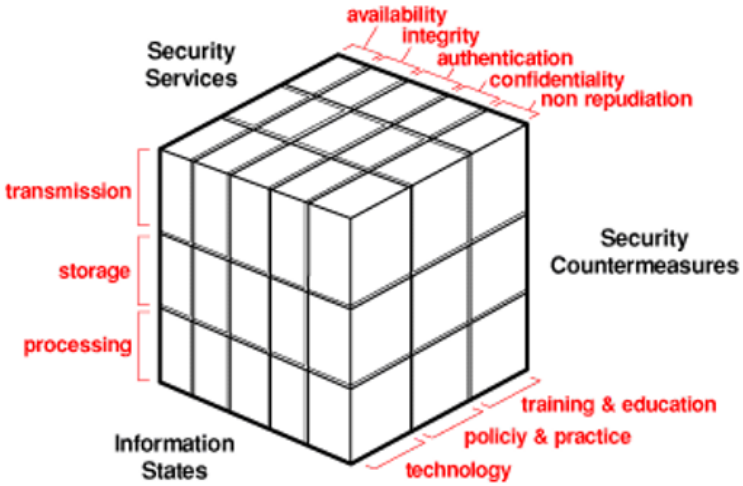


Figura 2 - Segurança da informação

Fonte: John McCumber

Confidencialidade

Até decisão do tribunal, as pessoas envolvidas são e devem continuar como inocentes, sendo o acesso a dados das mesmas totalmente restrito ao próprio perito, não podendo este disponibilizá-los a terceiros.

Autenticidade

A evidência deve ser autêntica. Produzida pelas pessoas que podem responder acerca da mesma. Caso contrário as evidencias são consideradas irrelevantes em tribunal.

Integridade

A informação constante nos dispositivos, devem a todo o custo ser mantida nos seus estados originais. O perito é responsável pelo uso de técnicas que altere a integridade da informação.

Não Repúdio

No que diz respeito ao exercício das funções de perito, o "não repúdio" adequa-se à utilização de técnicas universalmente aceites, possibilitando o recurso a contra perícias para a obtenção dos mesmos resultados.

1.3. Desafios da Informática Forense

Os métodos e técnicas forenses digitais enfrentam grandes desafios no presente, forçando o investigador forense a uma necessidade contínua de pesquisa e melhoria. Tradicionalmente, os investigadores forenses digitais procuram sistematicamente um olhar muito mais atento aos artefactos em busca de uma possível pista que pode ser uma evidência de crime. Mas, com a evolução das tecnologias, os procedimentos e as abordagens para encontrar esta evidência de crime precisam de ser melhorados e adaptados. Há imensos novos pequenos desafios para os forenses digitais para superar, no entanto apresentamos um pequeno resumo em 3 categorias:

Técnicos:

- Diferentes tipos de armazenamento;
- Encriptação;
- Stegnografia;
- Técnicas Antiforense;
- Aquisição e Análise em Live Data Forensics;
- Ocultação e Eliminação de dados
- Volatilidade dos dados;
- Partilhas de rede;
- ...

Legais:

- Privacidade;
- Proteção de dados;
- Demora na adaptação das leis à realidade tecnológica;
- Atuação em local do crime;
- Análise e manuseamento de dados;
- ...

Recursos:

- O aumento do volume de dados;
- Complexidade dos sistemas distribuídos de armazenamento de dados;
- ...

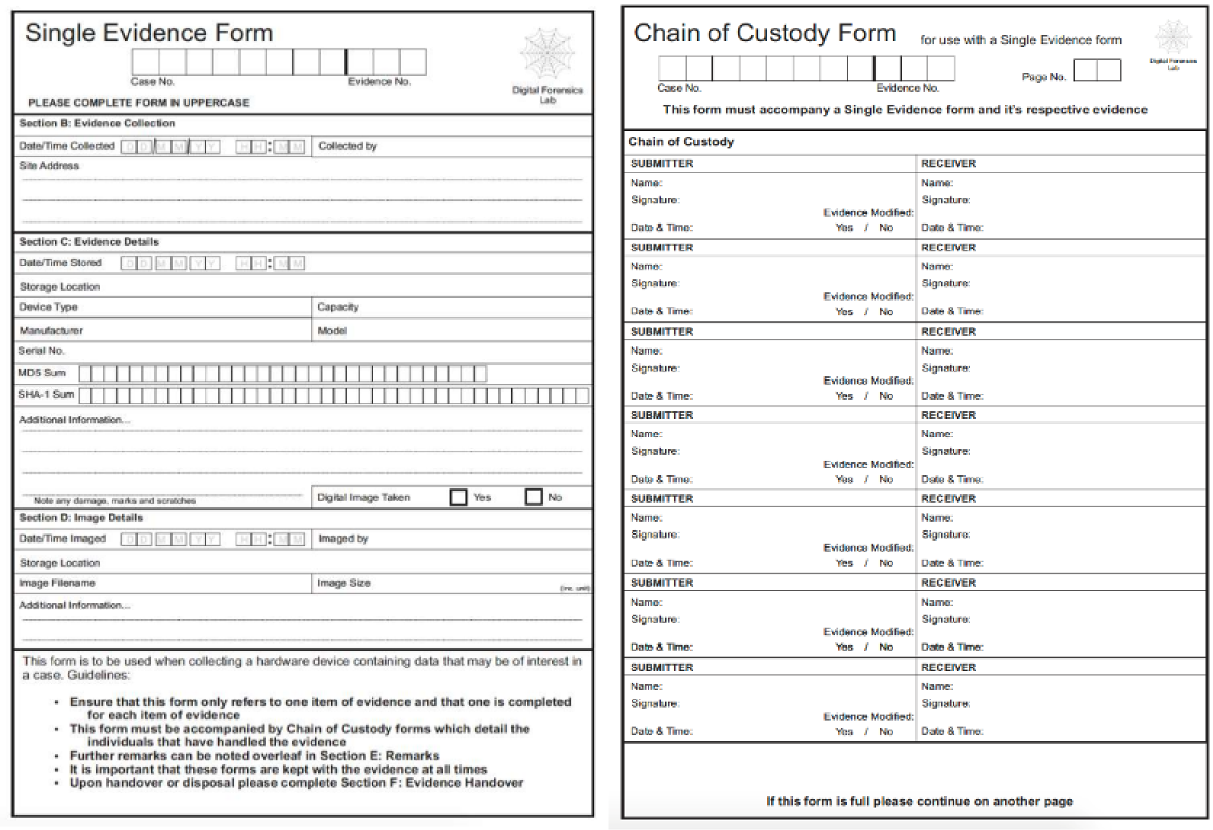
1.4. Standards Internacionais

As entidades que procuram desenvolver guias de boas práticas na área da forense digital, são inúmeras, no entanto as nossas referências são o ISO/IEC, o NIST, a ENISA, a SANS e outras pessoas que procuram divulgar e desenvolver o conhecimento na área. Deste modo, existem alguns documentos importantes no desenvolvimento das funções do perito em forense digital, a saber:

- **RFC 3227:2002** Guia para a aquisição e preservação de evidências digitais
- **NIST 800-86** Guia da integração de técnicas forenses em resposta a incidentes
- **NIST 800-144** Guia para a segurança e privacidade na Cloud
- **NIST 800-101** Guia relativo a forense em dispositivos móveis
- **ISO/IEC 20000-1:2018** Information technology - Service management
- **ISO/IEC 27001:2013** Definição de um ISMS (Information Security Management System)
- **ISO/IEC 27002:2013** Guia de boas práticas na segurança da informação
- **ISO/IEC 27005:2018** Information security risk management
- **ISO/IEC 27032:2012** Guia para a cibersegurança
- **ISO/IEC 27037:2012** Guia para identificação, recolha, aquisição e preservação das evidências digitais

1.5. Cadeia de custódia

A cadeia de custódia é um documento/formulário que deve ser preenchido pela pessoa que realiza a apreensão do equipamento. Este documento deve acompanhar sempre o próprio equipamento, mantendo o registo datado de todas as pessoas que tiveram a custódia do equipamento. Apresenta-se um exemplo da cadeia de custódia (Figura 3 - Digital Forensics Lab).



Single Evidence Form

Case No. Evidence No.

Digital Forensics Lab

PLEASE COMPLETE FORM IN UPPERCASE

Section B: Evidence Collection

Date/Time Collected D D M M Y Y H H : M M — Collected by

Site Address

Section C: Evidence Details

Date/Time Stored D D M M Y Y H H : M M

Storage Location

Device Type — Capacity

Manufacturer — Model

Serial No.

MD5 Sum

SHA-1 Sum

Additional Information...

Note any damage, marks and scratches — Digital Image Taken ☐ Yes ☐ No

Section D: Image Details

Date/Time Imaged D D M M Y Y H H : M M — Imaged by

Storage Location

Image Filename — Image Size (inc. unit)

Additional Information...

This form is to be used when collecting a hardware device containing data that may be of interest in a case. Guidelines:

- **Ensure that this form only refers to one item of evidence and that one is completed for each item of evidence**
- **This form must be accompanied by Chain of Custody forms which detail the individuals that have handled the evidence**
- **Further remarks can be noted overleaf in Section E: Remarks**
- **It is important that these forms are kept with the evidence at all times**
- **Upon handover or disposal please complete Section F: Evidence Handover**

Chain of Custody Form for use with a Single Evidence form

Case No. Evidence No. Page No.

Digital Forensics Lab

This form must accompany a Single Evidence form and it's respective evidence

Chain of Custody

SUBMITTER		RECEIVER
Name:		Name:
Signature:	Evidence Modified:	Signature:
Date & Time:	Yes / No	Date & Time:
SUBMITTER		RECEIVER
Name:		Name:
Signature:	Evidence Modified:	Signature:
Date & Time:	Yes / No	Date & Time:
SUBMITTER		RECEIVER
Name:		Name:
Signature:	Evidence Modified:	Signature:
Date & Time:	Yes / No	Date & Time:
SUBMITTER		RECEIVER
Name:		Name:
Signature:	Evidence Modified:	Signature:
Date & Time:	Yes / No	Date & Time:
SUBMITTER		RECEIVER
Name:		Name:
Signature:	Evidence Modified:	Signature:
Date & Time:	Yes / No	Date & Time:
SUBMITTER		RECEIVER
Name:		Name:
Signature:	Evidence Modified:	Signature:
Date & Time:	Yes / No	Date & Time:
SUBMITTER		RECEIVER
Name:		Name:
Signature:	Evidence Modified:	Signature:
Date & Time:	Yes / No	Date & Time:

If this form is full please continue on another page

Figura 3 - Formulário de Cadeia de custódia

Fonte: https://www.dfir.training/index.php?option=com_jreviews&format=ajax&url=media/download&m=wx99T&1661384494937

1.6. Modelos de processo na análise forense

Cada investigador forense tem o seu método e metodologia de trabalho no decorrer de uma análise forense, não existindo um modelo standard de atuação em cada tipo de investigação, sendo habitualmente orientada pela experiência passada de cada investigador.

Ao longo do tempo, têm surgido diversas metodologias que definem a necessidade de uma sequência de etapas genéricas numa investigação forense, sendo habitualmente definidas por "evidence collection, preservation or examination, analysis".

Têm sido propostos diversos modelos de investigação, também designados por "Digital Forensics Investigation Frameworks"(Figura 4), sendo estes alguns dos mais populares:

- DFRWS model - Digital Forensic Research Workshop (Palmer et al. 2001)
- ADFM - Abstract digital forensics model (Reith et al. 2002)
- IDIP - Integrated Digital Investigation Process (Carrier et al. 2003)
- EIDIP - Enhanced Integrated Digital Investigation Process (Baryamureeba & Tushabe 2004)
- CFFTPM - Computer Forensics Field Triage Process Model (Rogers et al. 2006)
- SRDFIM - Systematic Digital Forensic Investigation Model (Agarwal et al. 2011)
- IDFPM - Integrated Digital Forensic Process Model (Kohn et al. 2013)
- EDRM - Electronic Discovery Reference Model (https://edrm.net, 2014)

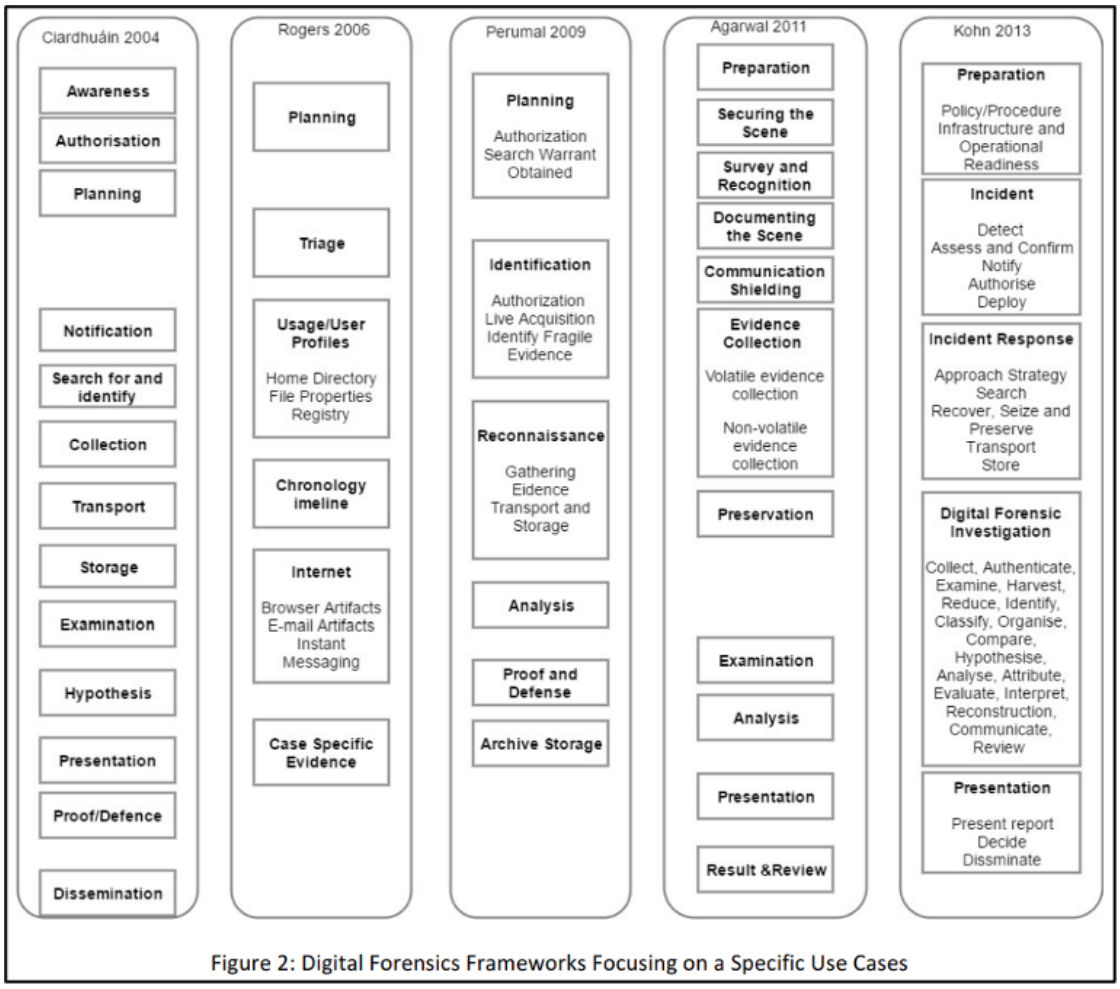


Figura 4 - Digital Forensics Investigation Frameworks

Fonte: Figura 2 do artigo https://arxiv.org/ftp/arxiv/papers/1708/1708.01730.pdf

Em 2001, a investigação decorrente do Digital Research Workshops propôs uma framework composta por 6 etapas, como apresentado na Figura 5.

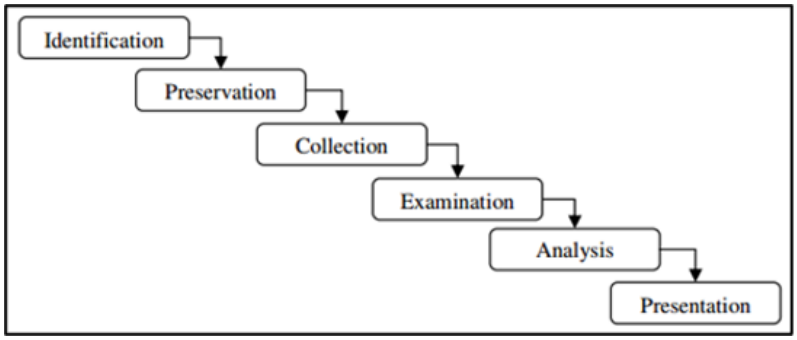


Figura 5 - DFRWS Framework

Esta é ainda hoje uma das principais metodologias de investigação forense digital, sendo a que iremos seguir. Descreve-se em seguida, cada uma das etapas:

Identification – Quando o investigador necessita de identificar todas as informações relevantes e definir a estratégia para adquirir essa informação. O investigador pode estar a lidar com um dispositivo de armazenamento típico, como um disco rígido, um cartão de memória, ou então pode ser necessário recolher dados digitais a partir de dados de tráfego de rede, dados voláteis como dados de memória, dispositivos móveis ou IoT, ou qualquer outro dispositivo de armazenamento de dados digitais. Nesta fase, a preparação prévia à utilização de técnicas e ferramentas, é extremamente importante para garantir a autenticidade, integridade e não-repúdio de todos os indícios em tribunal.

Preservation – Esta é a etapa que procura envolver tarefas como a criação de uma gestão adequada dos casos e a garantia de uma cadeia de custódia aceitável em tribunal. Esta fase é crucial para garantir que os dados são recolhidos sem qualquer contaminação externa e analisados de forma correta.

Collection – Este passo refere-se à aquisição de provas digitais, e tradicionalmente isso pode ser feito através da clonagem ou imagem forense do dispositivo de armazenamento. É necessário recolher e preservar dados através de técnicas e ferramentas previamente testadas, garantindo a Cadeia de Custódia. A aquisição de dados voláteis ou outros dados relevantes e voláteis, poderia ser decisivo para a fase de investigação, principalmente quando os dados relativos ao armazenamento adquirido são encriptados. Os dados recolhidos nesta fase são os dados de entrada ou a fonte de dados para fase de análise.

Examination – Esta é a fase de pesquisa dos dados pretendidos, envolvendo técnicas de pesquisa, recuperação de dados eliminados, decifra de dados, quebra de palavras-passe, análise de malware, análise de padrões, entre outras. Esta fase está interligada com a fase de análise, já que, por exemplo, após a identificação de documentos será necessário a sua análise, tendo em conta a resposta aos quesitos solicitados.

Analysis – Análise de todos os dados recolhidos. Esta é a fase mais demorada, devido à necessidade de fazer uma pesquisa minuciosa e identificar todos os artefactos relevantes. É comum, na maioria dos casos, que os dados recolhidos provenham sob a forma de dados não estruturados, requerendo ferramentas específicas e análises mais morosas para identificar potenciais dados de evidência digital, onde estão incluídos os dados estruturados, tais como registos, bases de dados, ficheiros de dados, ficheiros de sistema, páginas web e outros.

Presentation – Esta é a última fase do processo de análise forense digital, onde um relatório final com todos os dados relevantes a submeter ao juiz. Este relatório deve ser apresentado em cópia impressa, com todos os artefactos considerados importantes. Em caso de dúvidas sobre as informações presentes no relatório apresentado, é necessário o testemunho do perito no tribunal prestar os respetivos esclarecimentos.

2. Preservação e recolha de evidências digitais no local do crime/incidente

Para que a análise seja realizada na melhor condição, será necessário que a preservação e recolha seja ela também realizada corretamente. Nesta secção iremos abordar a atuação em local do incidente de igual modo como a atuação em local do crime, já que existem semelhanças evidentes em ambos, sendo que cada um destes terá necessariamente as suas especificidades e características específicas que não iremos aqui retratar.

INCIDENTE

"Incidente informático é uma interrupção ou quebra de qualidade num serviço de Tecnologia de Informação" Fonte: Manual "ITIL V3 – Service Operation" (OGC, 2007)

Para que exista um incidente, terá necessariamente de existir um comprometimento da disponibilidade, autenticidade, integridade e/ou confidencialidade dos dados.

São as redes Computer Security Incident Response Team (CSIRT) que possibilitam a recolha de dados relativos a incidentes informáticos, para isso desenvolveram uma taxonomia comum (Fonte: https://www.redecsirt.pt/files/RNCSIRT_Taxonomia_v3.0.pdf) de classificação de incidentes, classificando-os através de 2 vetores, por tipo de incidente e por tipo de evento.

Já a ENISA tem também desenvolvido e promovido o conhecimento relativo às boas práticas na identificação e gestão dos incidentes, publicando regularmente sobre o tema (Ler: https://www.enisa.europa.eu/publications/using-taxonomies-in-incident-prevention-detection).

A ENISA em 2010, publicou um documento (https://www.enisa.europa.eu/publications/good-practice-guide-for-incident-management) onde classifica os incidentes em categorias de acordo com o seu grau de severidade, tal como apresentado na Figura 6.

Group	Severity	Examples
RED	Very High	DDoS, phishing site
YELLOW	High	Trojan distribution, unauthorised modification of information
ORANGE	Normal	Spam, copyright issue

Figura 6 - Classificação de incidentes

Fonte: Incident Management Guide (ENISA 2010)

2.1. Standards Internacionais de resposta a incidentes

As entidades que procuram desenvolver guias de boas práticas na área de resposta a incidentes, são inúmeras, no entanto as nossas referências são o ISO/IEC, o NIST e a ENISA. Deste modo, existem alguns documentos importantes no desenvolvimento das funções do perito em forense digital, a saber:

- **Incident Management Guide** (ENISA 2010)
- **ISO/IEC 27035:2016** Guia para gestão de incidentes de segurança da informação para organizações de média e grande dimensão
- **ISO/IEC 27037:2012** Guia para identificação, recolha, aquisição e preservação das evidências digitais
- **NIST 800-86** Guia da integração de técnicas forenses em resposta a incidentes
- **NIST IR 8796** Análise de Segurança do First Responder a dispositivos móveis e wearables
- **ISO/IEC 27001:2013** Definição de um ISMS (Information Security Management System)
- **ISO/IEC 27002:2013** Guia de boas práticas na segurança da informação
- **ISO/IEC 27005:2018** Information security risk management
- **ISO/IEC 27032:2012** Guia para a cibersegurança

A **ISO/IEC 27002** - Gestão de incidentes de segurança da informação define a diferença entre **Evento** e **Incidente**, sendo que um evento poderá nem sempre dar origem a um incidente, mas um incidente tem sempre origem num evento.

2.2. Gestão e mitigação de incidentes

A **ISO/IEC 27035** define 5 etapas na gestão e mitigação de incidentes, a saber:

1. Preparação e Planeamento
2. Deteção e registo
3. Avaliação e decisão
4. Resposta
5. Lições Aprendidas

1.Preparação e Planeamento é a fase de identificação de todos os ativos críticos da instituição, processos internos de acessos à informação, criação de sistemas de monitorização que permitam a identificação de incidentes, bem como de todas as responsabilidades e procedimentos em caso de incidente.

Preparação

- Preparação do laboratório digital
- Definir o responsável de equipa
- Definir os membros da equipa e responsabilidades
- Preparar o briefing / estratégia de intervenção

Briefing

- Estratégia de intervenção?
- Equipamento necessário para levar ao local do incidente?
- Qual o tipo de recolha/métodos de aquisição (ferramentas)?
- Qual a atividade de rede?
- Volatilidade dos dados recolhidos?
- O equipamento pode ter sido configurado para destruir evidências?
- Como vamos armazenar/ transportar as evidências digitais?
- Equipamentos relacionados, manuais, etc?
- Identificar possíveis conflitos de interesse?
- Avaliação de Riscos

2. Deteção e registo é necessariamente a fase de identificação de eventos e distinção entre evento ou consecutivos eventos e possível incidente.

Semelhante a qualquer outro local de crime, já que o incidente poderá ter sido intencionalmente provocado por um colaborador interno da organização. Deste modo devemos ter em consideração a prévia preparação para atuar de acordo com os seguintes pontos:

- Proteger a cena do crime
- Recolher informação preliminar
- Documentar o local do crime
- Recolher a preservar as evidências
- Embalar e transportar
- Cadeia de custódia

Deve ser efetuada a máxima **recolha de informação** possível, adequada ao tipo de possível incidente, de modo a possibilitar uma tomada de decisão eficiente. Deste modo devemos ter em consideração todos os tipos de informação possíveis de serem adquiridos, tais como:

- Tipo de conexão (Wi-Fi/Ethernet)

- Os computadores que são utlizados para ligação a internet?
- Localização dos sistemas e identificar que são as pessoas com acesso
- Detalhes sobre dispositivos removíveis e propriedades do utilizador
- Obter detalhes sobre a topologia de rede
- Obter detalhes sobre outros periféricos ligados ao computador
- Existem outras perguntas sobre o assunto que não foram respondidas?

Destas informações, devemos ter em consideração a informação envolvente, tais como:

- Quais os serviços oferecidos pela organização?
- Quem são os afetados pelos incidentes? Foram informados?
- Existem medidas de proteção lógica (antivírus, firewall, IDS, IPS)? Alarmes?
- Quais as medidas de segurança física que estão em vigor?
- Existem registos de CCTV
- Identificar o número de computadores e computadores ligados a internet
- Verificar as últimas substituições de hardware
- Nível de acesso dos funcionários? Despedimentos recentes?
- Níveis de acesso Administrativo / Administrador?
- Políticas de segurança da organização?
- Procedimentos dados para conter o incidente?
- Lista de suspeitos? Porque são suspeitos?
- Logs de sistema? Rede? Algo suspeito?
- Utilização do sistema após o incidente? Comandos CMD/Shell? Scripts? Tarefas? Processos?
- Procedimentos de análise pós-incidente?

A equipa de resposta a incidentes deverá ter em consideração a recolha de dados voláteis, sendo estes possivelmente críticos para a rápida tomada de decisão referente a todos os eventos passados. Assim, é importante atuar de modos diferentes de acordo com o estado do computador, se ligado ou desligado (Figura 7).

Como encontra o computador?

Figura 7 - Primeira atuação

The first responder must have proper authority and expertise to act

O U.S. Department of Homeland Security dos Estados Unidos da América, publicou um pequeno guia para os *First Responders*, com o título "Best Practices for seizing Electronic Evidence", o qual conta com o que designaram de regras de ouro, que se apresentam na Figura 8.

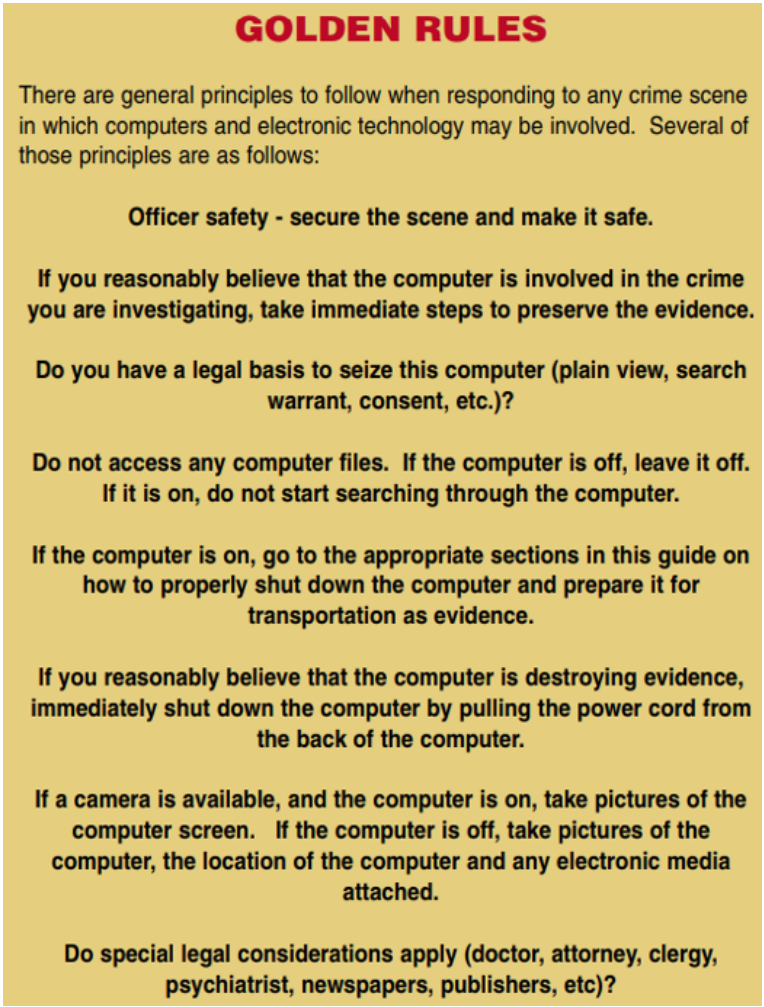


Figura 8 - Best Practices for seizing Electronic Evidence

Fonte: https://www.crime-scene-investigator.net/SeizingElectronicEvidence.pdf

Estas regras estão atualmente em vigor e devem ser seguidas na resposta a incidentes de segurança.

Já o U.S. Department of Justice - National Institute of Justice, publicou um fluxograma resumindo o processo de abordagem aos dispositivos, denominado de "Collecting Digital Evidence Flow Chart" (Figura 9).

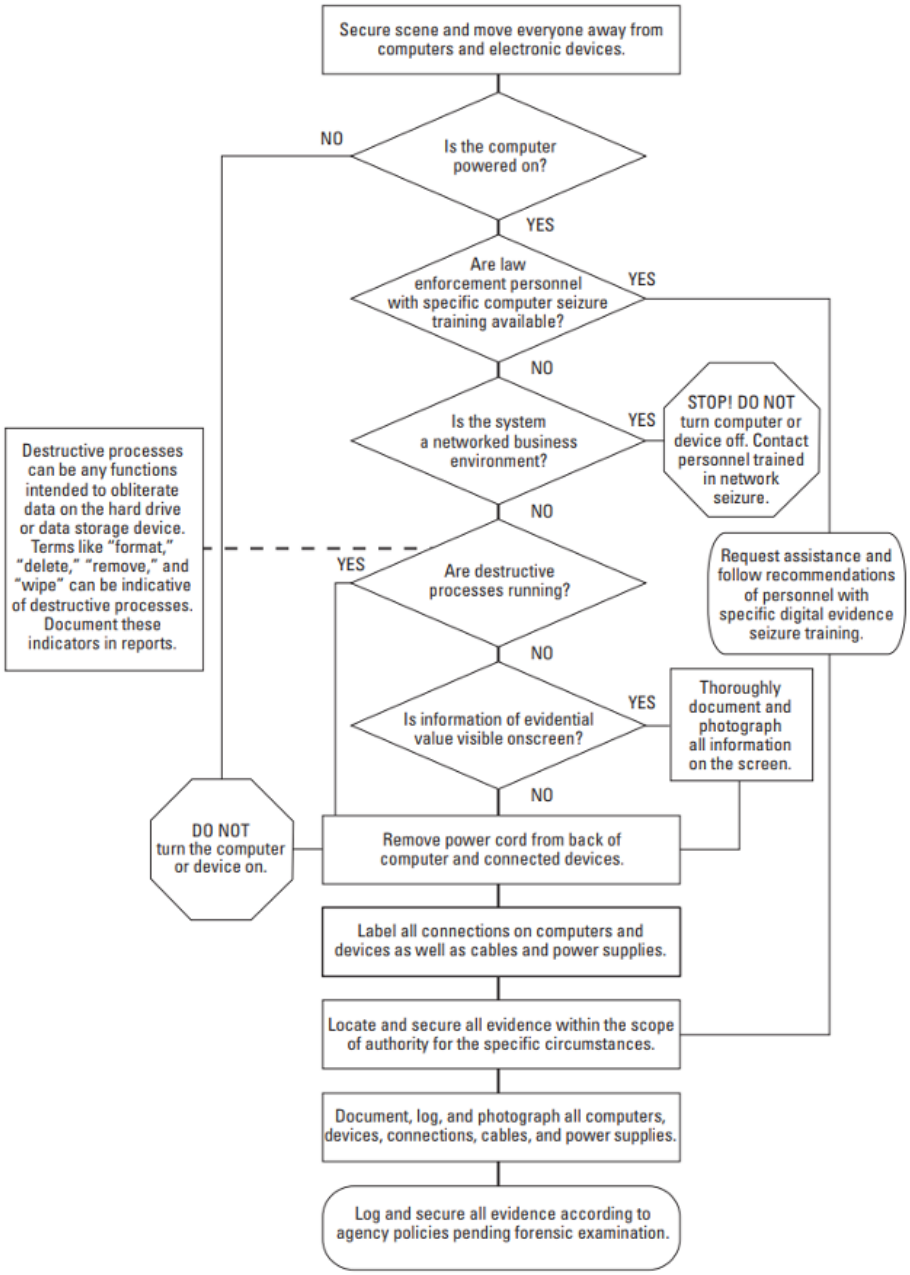


Figura 9 - Collecting Digital Evidence Flow Chart

Fonte: Collecting Digital Evidence Flow Chart. US Department of Justice - National Institute of Justice (2010).

Neste sentido, podemos determinar os seguintes procedimentos:

1. Garantir a segurança física e eletrónica.
2. Caso o computador esteja desligado:

· Garantir que este não liga (Desligar o cabo da energia/Remover bateria, caso exista)

· Fazer a etiquetagem/fotos de todos os componentes e periféricos

· Identificar os dispositivos de armazenamento

· Verificar a data/hora da BIOS (Sem o disco rígido)

3. Caso o computador esteja ligado:

· Desligar as comunicações (desligar cabo de Rede/ retirar Cartão SIM)

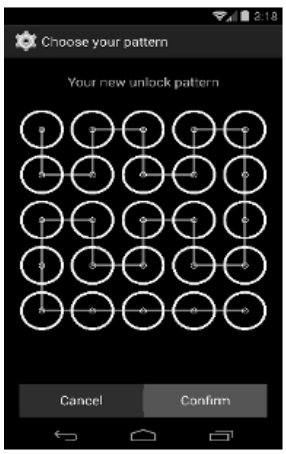
· Fotografar o ecrã e todo o seu conteúdo (descrever o conteúdo visível)

- Se existir a necessidade de recolher dados voláteis e não voláteis:
- Realizar a aquisição em Live dos dados (de acordo com a ordem de volatilidade)
- Verificar se os dispositivos de armazenamento se encontram encriptados
- Desligar o computador da fonte de energia
- Fazer a etiquetagem/fotos de todos os componentes e periféricos
- Identificar os dispositivos de armazenamento
- Verificar a data/hora da BIOS (Sem o disco rígido)

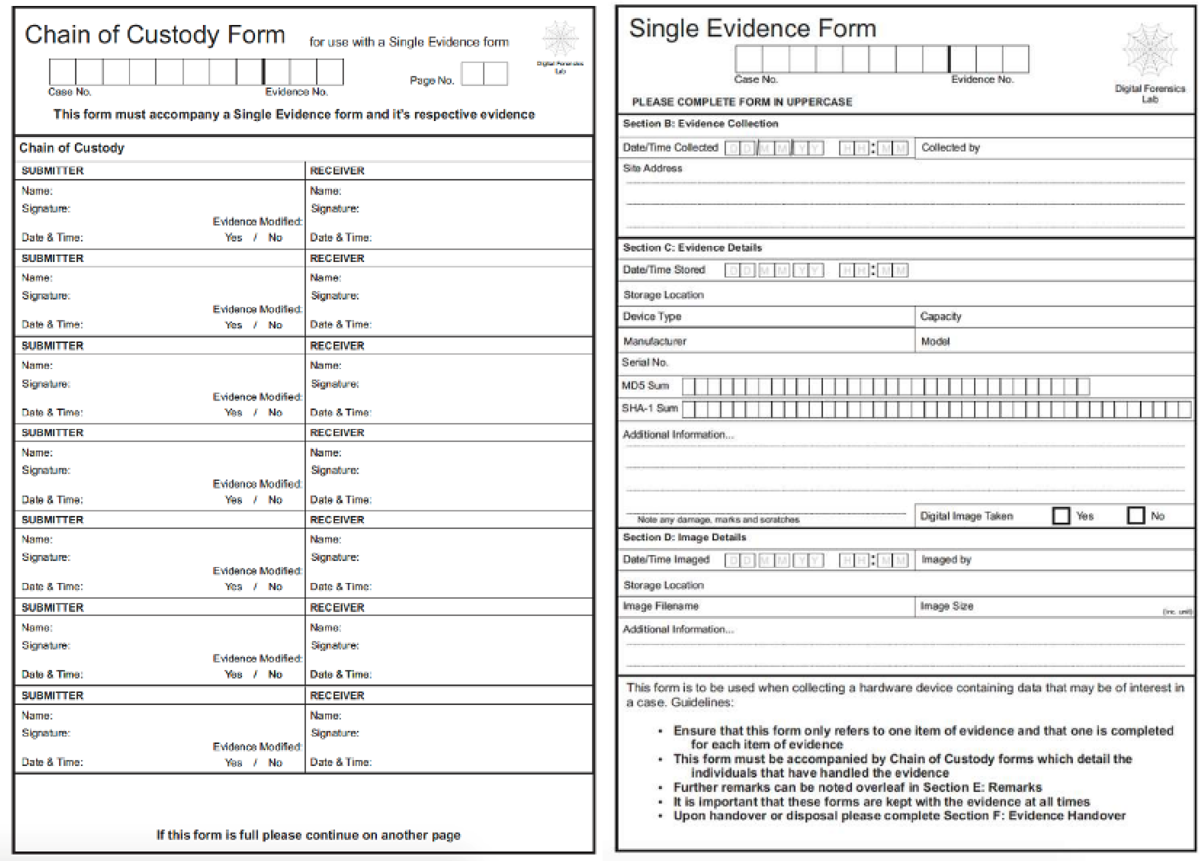
3. Uma imagem com texto Descrição gerada automaticamente Caso esteja envolvido um dispositivo móvel (smartphone/Tablet):

- Se o dispositivo estiver desligado, não ligar
- Se o dispositivo estiver ligado:
- Fotografar o visor (se disponível)
- Colocar em modo de voo
- Certifique-se sempre de que o dispositivo conectado à bateria tem fonte de alimentação suficiente para o manter ativo até análise
- Utilizar uma bolsa/saco de Faraday (Figura 10)

- Etiquetar/fotografar todos os componentes
- Recolher todos os dispositivos de armazenamento adicionais (cartões de memória, cartões de SIM, etc.)
- Documentar todas as etapas envolvidas na apreensão de dispositivos móveis
- Questionar por códigos de acesso (PIN/Padrão), códigos PIN e PUK do cartão SIM (verificar as bolsas de transporte dos dispositivos – Figura 11)
- Como armazenar e transportar?
- Utilizar luvas
- Figura 11 - Código Padrão



- Não cubra informações de identificação
- Provas digitais com aberturas e componentes móveis devem ser seladas com selos ou fitas de anti-adulteração ou de sinalização de abertura
- Os dispositivos devem ser armazenados em saco de dissipação estática e de faraday
- Documentar
- Documentar em relatório próprio e assinado por todos os envolvidos
- Preencher a Cadeia de Custódia dos equipamentos (Figura 12)



Chain of Custody Form for use with a Single Evidence form

Case No. Evidence No. Page No.

This form must accompany a Single Evidence form and it's respective evidence

Chain of Custody

SUBMITTER	RECEIVER
Name: Signature: Date & Time: Evidence Modified: Yes / No	Name: Signature: Date & Time:
Name: Signature: Date & Time: Evidence Modified: Yes / No	Name: Signature: Date & Time:
Name: Signature: Date & Time: Evidence Modified: Yes / No	Name: Signature: Date & Time:
Name: Signature: Date & Time: Evidence Modified: Yes / No	Name: Signature: Date & Time:
Name: Signature: Date & Time: Evidence Modified: Yes / No	Name: Signature: Date & Time:
Name: Signature: Date & Time: Evidence Modified: Yes / No	Name: Signature: Date & Time:
Name: Signature: Date & Time: Evidence Modified: Yes / No	Name: Signature: Date & Time:

If this form is full please continue on another page

Single Evidence Form

Case No. Evidence No.

Digital Forensics Lab

PLEASE COMPLETE FORM IN UPPERCASE

Section B: Evidence Collection

Date/Time Collected DD/MM/YY HH:MM Collected by

Site Address

Section C: Evidence Details

Date/Time Stored DD/MM/YY HH:MM

Storage Location

Device Type | Capacity

Manufacturer | Model

Serial No.

MD5 Sum

SHA-1 Sum

Additional Information...

Note any damage, marks and scratches | Digital Image Taken Yes No

Section D: Image Details

Date/Time Imaged DD/MM/YY HH:MM Imaged by

Storage Location

Image Filename | Image Size

Additional Information...

This form is to be used when collecting a hardware device containing data that may be of interest in a case. Guidelines:

- Ensure that this form only refers to one item of evidence and that one is completed for each item of evidence
- This form must be accompanied by Chain of Custody forms which detail the individuals that have handled the evidence
- Further remarks can be noted overleaf in Section E: Remarks
- It is important that these forms are kept with the evidence at all times
- Upon handover or disposal please complete Section F: Evidence Handover

Figura 12 - Cadeia de custódia

Fonte: https://www.dfir.training/index.php?option=com_jreviews&format=ajax&url=media/download&m=wx99T&1661384494937

3.Avaliação e decisão é a fase após o conhecimento da existência de um possível incidente, recolhendo todas as informações úteis sobre o sucedido, levando a uma tomada de decisão sobre a confirmação de um incidente de segurança informática. Com esta confirmação, deve ser realizada uma rápida resposta de modo a mitigar e resolver o mesmo.

4.Resposta é a fase onde é classificado o incidente, de acordo com o definido na fase 1, categorizando o incidente e classificando a sua severidade, realizando os procedimentos necessários à sua mitigação e resolução, utilizando mecanismos de gestão de crises e reporte de incidentes às autoridades competentes, no caso português são a Polícia Judiciária (PJ), o Centro Nacional de Ciber Segurança (CNCS) e a Comissão Nacional de Proteção de Dados (CNPD).

5.Lições Aprendidas é uma das mais necessárias fases, já que permite implementar medidas para que não volte a suceder um incidente igual, bem como, aproveitar o conhecimento gerado para melhorar o sistema de segurança da organização.

Ver: https://www.cncs.gov.pt/certpt/coordenacao-da-resposta-a-incidentes/

2.3. Relação entre o processo de resolução de incidentes e a informática forense

Estes procedimentos relacionam-se com a forense digital (Figura 13) sempre que é detetado um incidente e se pretende saber mais sobre o mesmo, na tentativa de levar a tribunal o autor do mesmo. Assim, no processo de gestão do incidente, temos o mesmo processo de investigação indicado no ponto 1.6, no que diz respeito às 6 etapas da framework de análise.

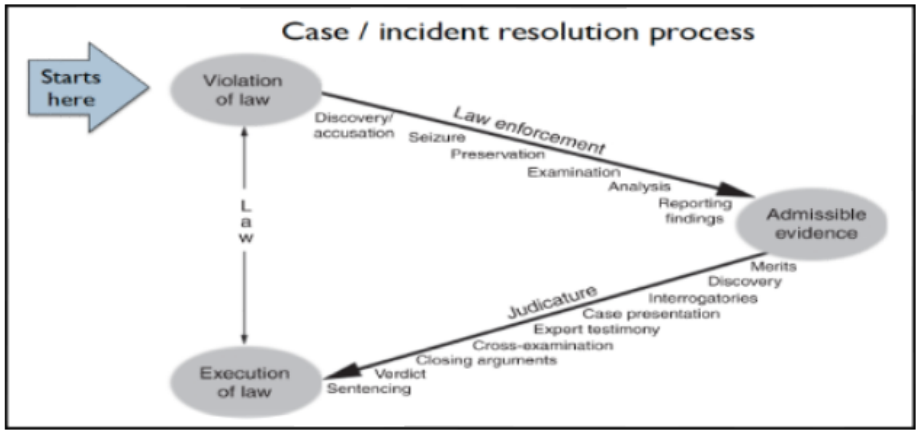


Figura 13 - Processo de resolução de incidentes

Fonte: http://www.c-jump.com/bcc/t155t/Week03a/W24_0030_overview_of_caseinci.htm

3. Procedimentos de aquisição de evidências digitais

A informática forense é o processo de adquirir, analisar e preservar evidências digitais, recorrendo a procedimentos normalizados que permitem a integridade da imagem de prova.

É assim necessário garantir que a aquisição forense dos dispositivos de armazenamento seja realizada de acordo com as melhores práticas internacionalmente aceites, sendo uma delas a prévia esterilização do disco rígido que irá receber a cópia dos dados, como descrito no ponto seguinte.

3.1. Procedimento de esterilização

O procedimento de esterilização destina-se a garantir que o nosso dispositivo de destino está preparado para receber a informação original. A esterilização tem como objetivo escrever todos os bits do nosso disco de recolha com o valor 0 (zero), garantido assim que nenhuma informação anterior está presente no mesmo.

Após a esterilização é sempre necessário validar, verificando que a esterilização ocorreu do modo correto. Após essa validação podemos proceder com a formatação do disco para um sistema de ficheiros apropriado.

Existe diverso software que permite efetuar este procedimento de esterilização de um disco, e respetiva formatação para o sistema de ficheiros desejado. Vamos aqui demonstrar o processo utilizando as ferramentas presentes na grande maioria de distribuições Linux, o lsblk, fdisk e o dc3dd.

O primeiro passo será o de identificar o disco a esterilizar. É muito importante que essa identificação seja unívoca e confirmada as vezes que foram necessárias. Um disco esterilizado não é recuperável.

3.1.1. Identificação do dispositivo

A identificação do dispositivo realiza-se através de uma séria de comandos. Em primeiro lugar é necessário determinar quais os volumes instalados no computador a ser utilizados. Uma boa prática, é utilizar um computador que tenha ligado apenas o disco a esterilizar, iniciando o sistema operativo a partir de um liveCD ou de uma pen USB. Esta prática reduz a possibilidade de erro na identificação do disco:

$ lsblk | grep sd*

Este comando irá listar todos os dispositivos de armazenamento reconhecidos pelo sistema operativo. Serão apresentados todos os discos bem como o seu tamanho e partições. Este comando apenas nos ajuda a saber qual o nome do nosso disco no computador.

Em caso de dúvida ainda podemos utilizar o comando (Figura 14)

*fdisk -l /dev/sd**

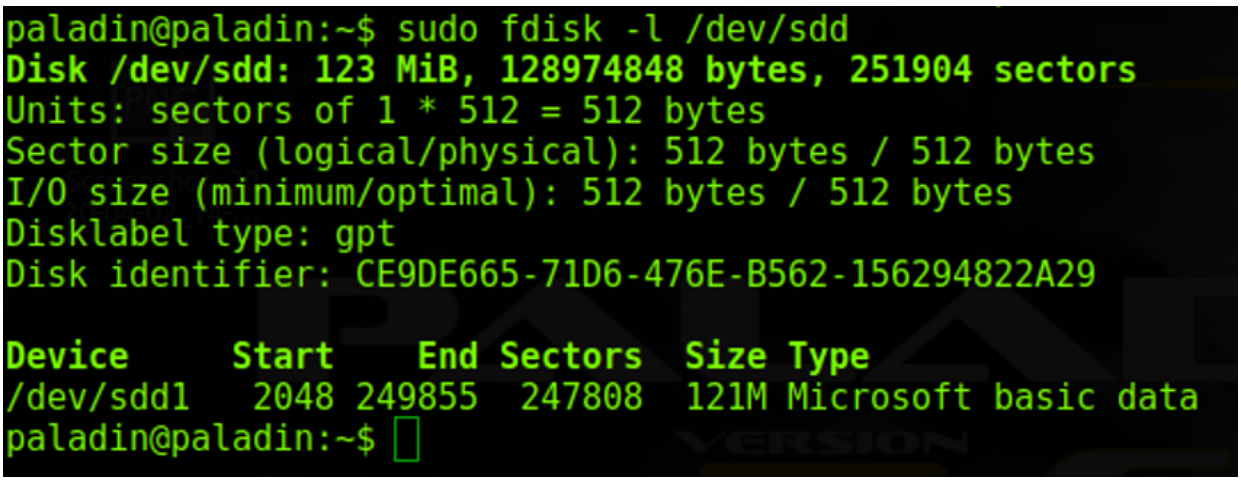


Figura 14 - Identificação do dispositivo

Este comando fornece-nos mais informações sobre o disco pretendido.

3.1.2. Esterilização do disco de destino

O processo de esterilização não é mais do que escrever todo o disco com o valor 0 (zero), ou seja, forçar todos os bits do disco rígido a adquirirem o valor zero.

Para esta tarefa poderão ser utilizadas ferramentas como o Live-CD DBAN (www.dban.org) ou em Windows o Eraser (eraser.heidi.ie).

Em Linux podemos utilizar os comandos (Figura 15)

dc3dd wipe=/dev/sdd verb=on corruptoutput=on

ou

dcfldd if=/dev/zero of=/dev/sdb bs=8k conv=noerror,sync

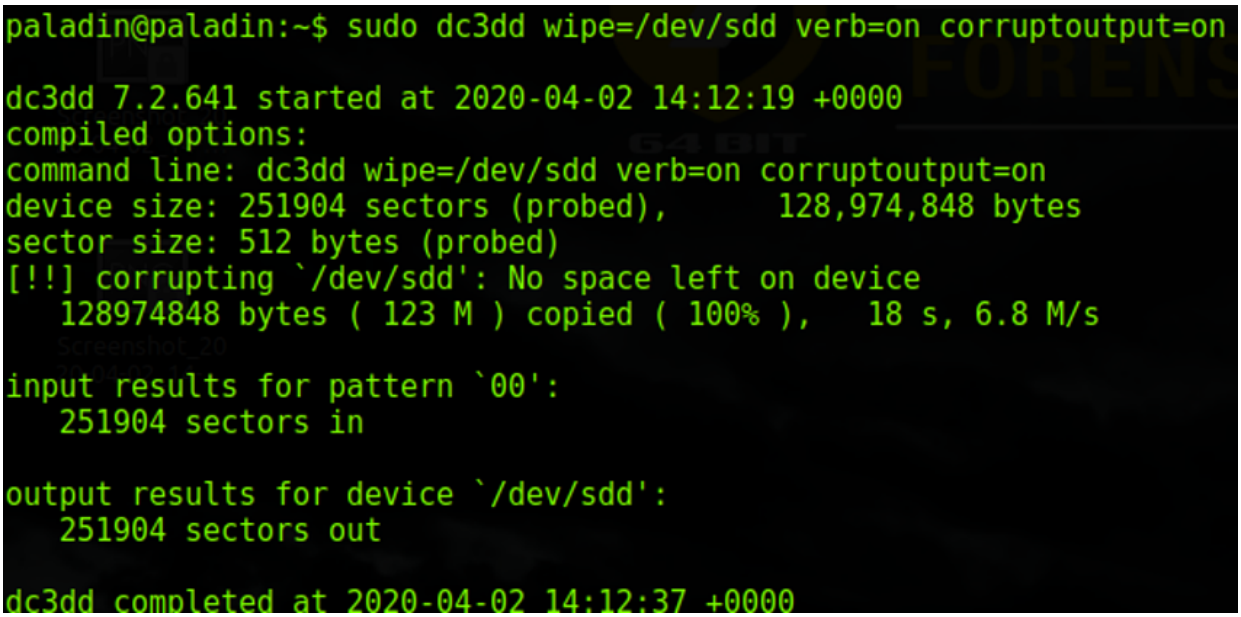


Figura 15 - Esterilização do disco de destino

Este comando efetua uma escrita de todos os bits de um disco rígido, pelo que será tão mais demorado quanto maior for o disco rígido. No nosso exemplo um dispositivo de apenas 123 Mb demorou 18 segundos a ser escrito, no entanto um disco rígido de 1 Tb, poderá demorar mais de 8 horas. É ainda importante referir que dependendo da tecnologia do disco rígido, este tempo poderá ser superior ou inferior, dependendo da sua velocidade de escrita.

Em Microsoft Windows, a esterilização do disco de destino, poderá ser realizada através do comando diskpart.

Realizando a identificação do disco de destino através de:

LIST DISK (identificação do dispositivo)

LIST VOLUME (identificação do volume)

SELECT DISK 1 (selecionar o disco a esterilizar)

Realização da esterilização (Figura 16)

CLEAN ALL

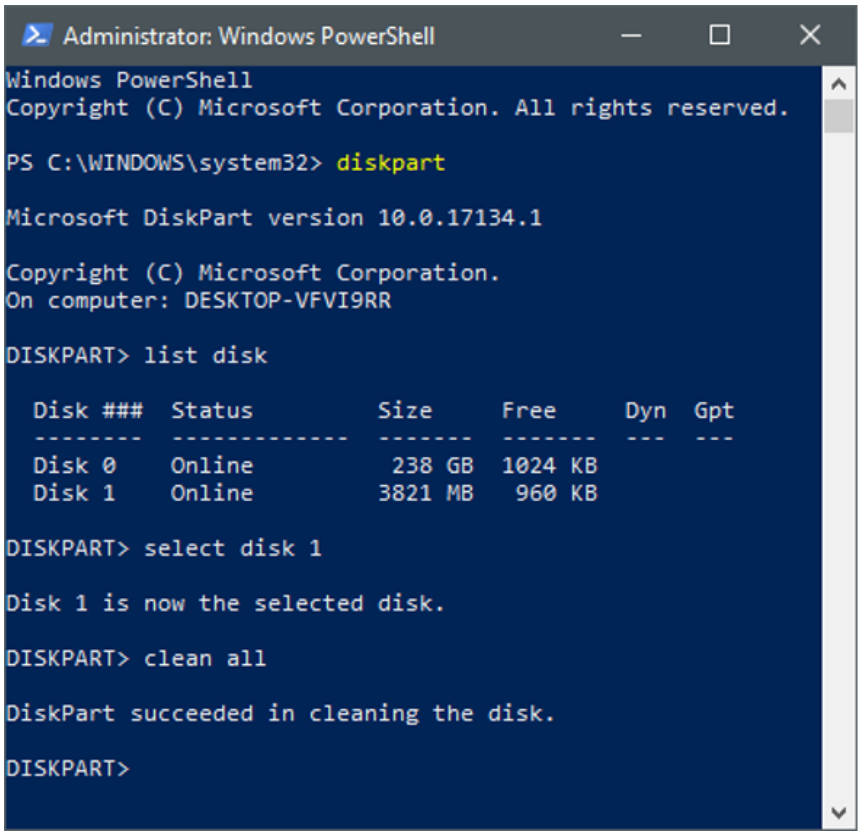


Figura 16 - Esterilização do disco de destino em Windows

3.1.3. Verificação da esterilização

Finalmente, é importante verificar que a escrita do disco rígido foi eficaz, para tal executamos o comando:

cat /dev/sdb |od

Se a escrita foi bem-sucedida, o output do comando será 0000000, que indicam que o disco rígido está escrito apenas com zeros (Figura 17).

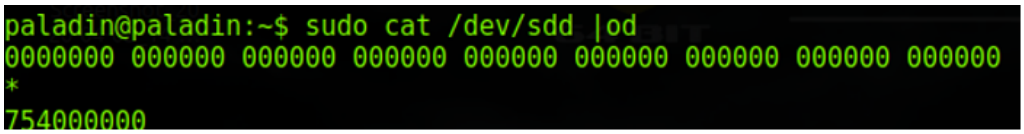


Figura 17 - Verificação da esterilização

O comando “cat” irá apresentar o conteúdo do dispositivo, enquanto que o argumento “|od”, irá converter este conteúdo para base octal, daí que seja apresentado apenas zeros quando a esterilização foi bem sucedida.

Para além dos procedimentos apresentados, existem outros métodos e diferentes comandos que se podem utilizar, como o recurso à visualização em formato hexadecimal, ou outros.

3.1.4. Formatação

Após a esterilização, é necessário formatar o disco, capacitando-o para receber dados.

Esta formatação poderá continuar a ser realizada através do Diskpart, do seguinte modo:

Criação da partição primária (Figura 18)

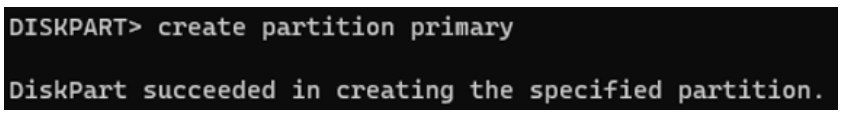


Figura 18 - Criação da partição primária

Formatação em NTFS (Figura 19)

```
DISKPART> select partition 1

Partition 1 is now the selected partition.

DISKPART> format fs=ntfs quick

  100 percent completed

DiskPart successfully formatted the volume.
```

Figura 19 - Formatação

Já através do ambiente gráfico, pode ser utilizada a aplicação Disk Management através do comando DISKMGMT.MSC (Figura 20).

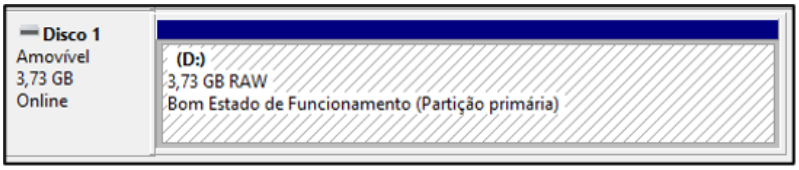


Figura 20 - Disk Management

Clicando com o botão direito do rato sobre o disco pretendido e selecionando "Formatar", indicando de seguida o nome e o sistema de ficheiros pretendido. Poderá ser selecionada a formatação rápida, já que o disco foi esterilizado anteriormente (Figura 21).

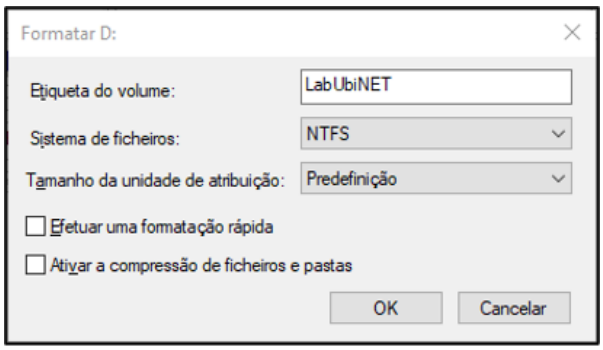


Figura 21 - Formatação através do Disk Management

3.2. Identificação de dispositivos de armazenamento de dados

Os dispositivos de armazenamento têm sofrido nos últimos anos uma rápida evolução, necessitando que o analista forense esteja atento e pesquise sobre cada equipamento em análise, procurando saber sobre todos os dispositivos de armazenamento de dados que o equipamento suporta. Deste modo, o analista poderá procurar identificar todos esses equipamentos (Figura 22).

Figura 22 - Identificação de dispositivos de armazenamento

3.3. Reportagem fotográfica

Após a identificação dos equipamentos e dos respetivos dispositivos de armazenamento de dados, é importante registar o atual estado dos mesmos, devendo para isso, atribuir uma designação interna a cada equipamento e fotografar os dispositivos nos seus diversos ângulos (Figura 23), com recurso ao uma escala métrica e tendo em especial atenção os danos que os mesmos poderão ter. Esta é uma informação que poderá ser importante em tribunal.

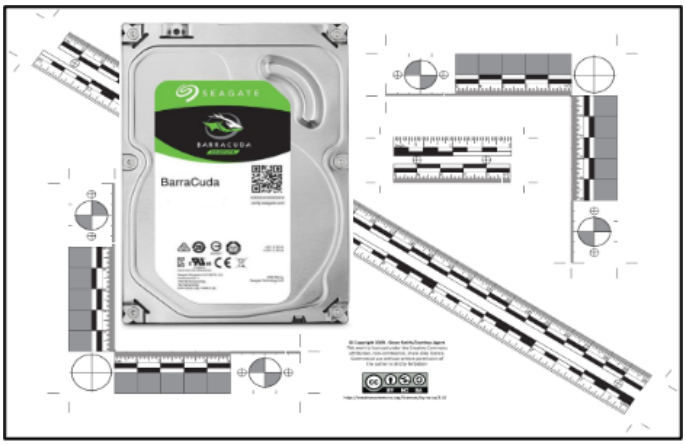


Figura 23 - Reportagem fotográfica

3.4. Distribuições de âmbito Forenses

Tendo em conta as técnicas e procedimentos de aquisição e análise de dispositivos de armazenamento de dados, é relevante ter conhecimento de distribuições Linux de âmbito forense. Estas têm um conjunto de ferramentas que permitem a aquisição e análise de informação, tendo em conta as melhores práticas. São geralmente distribuições Live, não necessitando de ser instaladas no computador, mas que permitem ligar os discos sem a preocupação do bloqueio de escrita, por virem configurados nativamente sem os montarem automaticamente no sistema.

As distribuições que indicamos são as seguintes:

- **CAINE (Computer Aided INvestigative Environment Live CD/DVD)**
- **DFF (Digital Forensics Framework)**
- **SANS SIFT (Sans Investigative Forensics Toolkit)**
- **Paladin Edge (Sumuri)**

3.5. Técnicas de aquisição

O procedimento de aquisição é determinante para garantir a integridade da evidência digital e facilitar o processo de análise da mesma, sendo uma das técnicas utilizadas no âmbito das boas práticas em forense digital, que garante a admissibilidade dos indícios extraídos em tribunal.

Designamos por aquisição, a cópia binária bit a bit dos dispositivos de armazenamento de dados, existindo também a designada de cópia ou duplicação forense (Figura 24).

Figura 24 - Duplicador de dispositivos de armazenamento

Fonte: https://security.opentext.com/tableau/hardware/details/td2u

Em qualquer dos tipos de recolha forense utilizado, é importante ter em conta que o disco de destino deverá ter maior capacidade do que o de origem.

3.5.1. Bloqueador de escrita (Write Blocker)

No procedimento de aquisição, deve ser utilizado um dispositivo de hardware (Figura 25) com o objetivo de bloquear a escrita no disco de origem. Deste modo é garantida toda a integridade dos dados nesse disco, protegendo o disco contra alterações inadvertidas, como do sistema operativo ou do antivírus, bem como a validação dos dados copiados para o disco de destino.

Figura 25 - Bloqueador de escrita

Fonte: www2.guidancesoftware.com

Em caso de não ter acesso a um bloqueador de escrita por hardware, é possível utilizar bloqueadores de escrita por software. Estes requerem um maior cuidado na validação do seu bom funcionamento, já que dependem do sistema operativo que estamos a utilizar. Alguns exemplos são apresentados na Figura 26.

Figura 26 - Software forense com bloqueio de escrita

O bloqueio de escrita no sistema operativo Microsoft Windows, poderá ser realizado através da criação da chave de registo

"HKLM\SYSTEM\ControlSet001\Control\StorageDevicePolicies\WriteProtect", como descrito de seguida:

- "regedit" em modo administrador e aceda ao seguinte caminho:
"HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Control"
- Crie uma nova chave em "Control" com o nome: **"StorageDevicePolicies"**
- Adicione um novo valor do tipo "DWORD (32-bit)", com o nome: **"WriteProtect"**
- Altere a informação deste de "**0**" para **"1"**
- Teste o bloqueio com diversos dispositivos de armazenamento

3.5.2. Comparativo das aplicações de aquisição

É possível realizar o procedimento de aquisição forense em diversos sistemas operativos, já que existem múltiplas aplicações com capacidade de executar essa tarefa, a exemplo disso é a Figura 27 comparativa dessas mesmas aplicações.

Tool	Platform			Input Sources				Encoding		Output Formats			
	❖	🐧		Physical Disk	Logical Volume	Files	Folders	Compression	Encryption	Raw	E01	Ex01	Split
FTK Imager 3.2	✓			✓	✓		✓	✓	✓	✓	✓		✓
FTK Imager CLI 3.1.1	✓	✓	✓	✓	✓		✓	✓	✓	✓	✓		✓
EnCase Forensic Imager 7.0	✓			✓	✓	✓	✓	✓	✓	✓	✓	✓	✓
dd		✓	✓	✓	✓	✓	✓			✓			
dcfldd		✓		✓	✓	✓	✓			✓			✓
dd_rescue		✓		✓	✓	✓	✓			✓			
dd.exe	✓			✓	✓	✓	✓	✓	✓	✓			
dc3dd	✓	✓		✓	✓	✓	✓			✓			✓
ewfacquire		✓	✓	✓	✓					✓	✓	✓	✓

Figura 27 - Comparativo das aplicações de aquisição

Fonte: Vandeven, Sally, The SANS Institute, 2014

Ler: https://www.raedts.biz/forensics/forensic-imaging-tools-compared-tested/

3.5.3. Aquisição em Linux

A aquisição através do sistema operativo Linux, entre outras aplicações, poderá ser realizada através do dcfldd ou do dc3dd, aplicações derivadas do conhecido dd.

Deve-se proceder à identificação do dispositivo e da respetiva tabela de partições

mmls /dev/sdb

Aquisição através do dclfdd:

dcfldd if=/dev/sdb hash=md5,sha256 hashwindow=10G md5log=md5.txt sha256log=sha256.txt hashconv=after bs=512 conv=noerror,sync split=10G of=diskimage.dd

Ou aquisição através do dc3dd:

dc3dd if=/dev/sdb hash=md5,sha256 hlog=hash_log.log log= diskimage.log rec=off of=diskimage.dd

Deverá verificar-se os ficheiros de log, identificando a correspondência das hash do conteúdo do disco de origem com o conteúdo da imagem forense criada neste procedimento. É ainda importante a verificação do conteúdo ilegível, ou bad sectors, que em ambos os procedimentos irão permanecer sem qualquer valor escrito, ficando esse espaço com o valor 0 (zero).

3.5.4. Aquisição em Windows

A aquisição através do sistema operativo MS Windows, entre outras aplicações, poderá ser realizada através da conhecida aplicação de utilização gratuita FTK Imager da empresa Access Data.

Deverá selecionar a opção Create Disk Image / Physical Drive no FTK Imager, tal como apresentado na Figura 28.

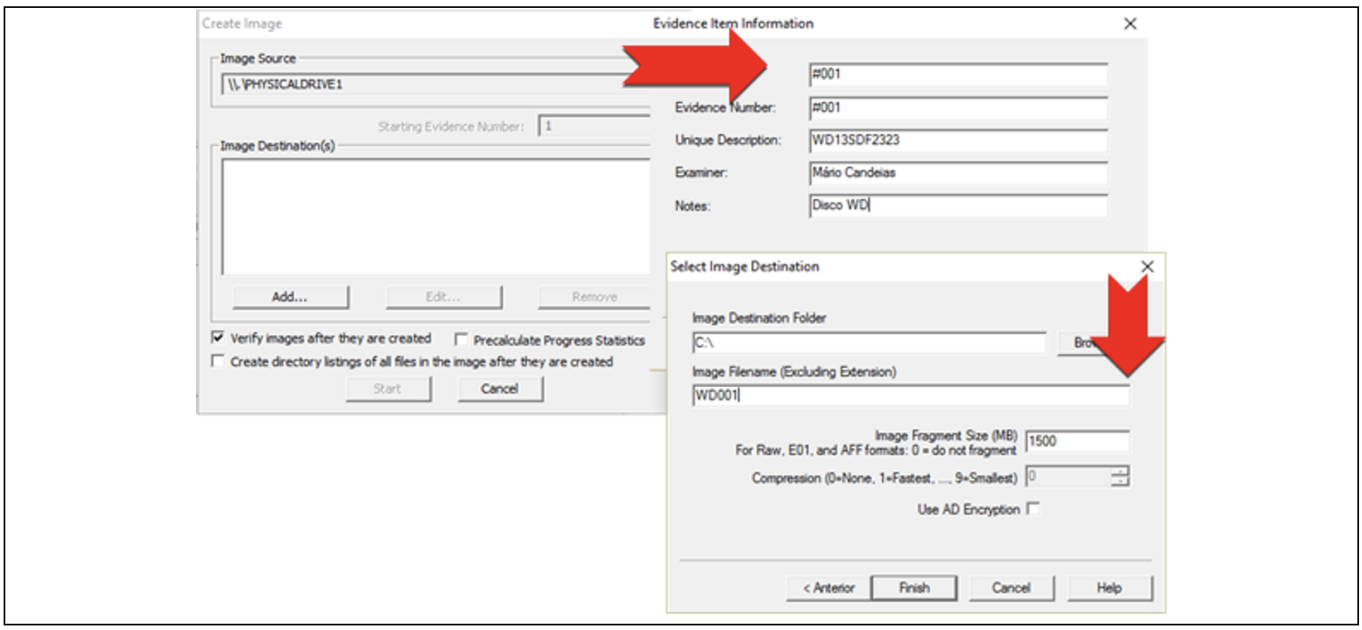


Figura 28 - Procedimento de aquisição com o AccessData FTK Imager

Antes do início do procedimento de aquisição, é possível selecionar a opção de criar uma lista de todos os ficheiros, que será criada posteriormente à aquisição e será guardada no formato ".csv".

Após o início da aquisição, será apresentada uma janela de validação, com a validação da correspondência das hash, bem como a informação dos setores não lidos, também designados por *bad sectors* (Figura 29).

Figura 29 - Resultado da aquisição com o AccessData FTK Imager

Teremos também essa mesma informação num ficheiro de texto, armazenado na mesma localização do ficheiro de imagem forense (Figura 30). O ficheiro ".csv", irá também constar na mesma localização, caso tenhamos selecionado para ser criada a lista de ficheiros.

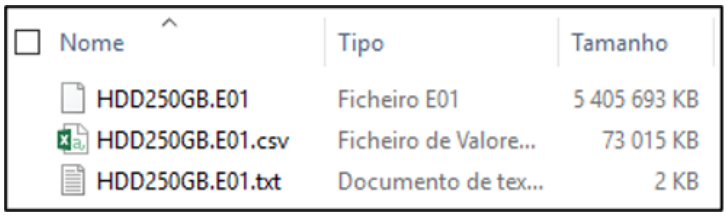


Figura 30 - Ficheiros resultantes da aquisição com o AccessData FTKImager

4. Aquisição e análise de informação volátil

A informação volátil é informação que se perde quando um sistema é desligado ou perde energia. A informação volátil existe geralmente na memória física, ou RAM, e consiste em informação sobre processos, ligações de rede, ficheiros abertos, área de transferência (clipboard), e semelhantes. Esta informação descreve o estado do sistema num determinado momento.

Ao executar uma análise em *live-data forensics*, uma das primeiras coisas que os investigadores devem recolher é o conteúdo da memória RAM. Ao recolher esta informação em primeiro lugar, é minimizado o impacto da sua recolha de dados sobre o conteúdo da RAM, no entanto esta captura poderá causar instabilidade no sistema ou levar mesmo a um Blue Screen of Death (BSoD), levando diversos autores a indicarem que este procedimento seja realizado posteriormente à recolha de outras informações voláteis, sendo priorizada consoante a cada situação.

Alguns dos tipos específicos de informação volátil que deve se recolhida:

- Memória RAM
- Data e hora do sistema
- Informação de rede
- Utilizadores logados
- Arquivos abertos
- Ligações de rede
- Informações sobre processos em execução
- Mapeamento entre processos e portos
- Estado da rede
- Conteúdo da Área de Transferência (clipboard)
- Informações sobre serviços e drivers
- Histórico de comandos executados
- Unidades mapeadas
- Partilhas
- Senhas e chaves criptográficas

Destes, é necessário identificar para cada caso em concreto, quais as informações mais voláteis e que serão mais importantes obter em primeiro lugar. Apresenta-se uma possível sequência de informações mediante a sua ordem de volatilidade (Figura 31).

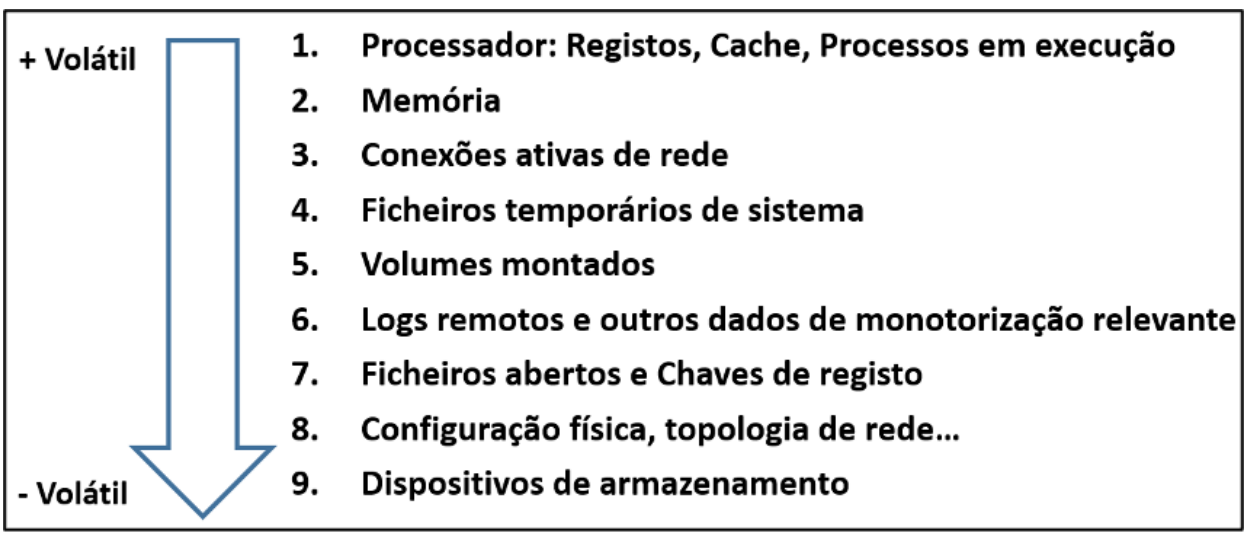


Figura 31 - Possível sequência de informações por ordem de volatilidade

4.1. Processo de captura da informação volátil

Em primeiro lugar é necessário garantir a estabilidade da nossa máquina de trabalho. Um dos problemas que podem ser sentidos é o reinício automático da máquina, causado por atualizações automáticas do sistema operativo. Aconselha-se assim a desativação, não das atualizações do sistema operativo, mas a capacidade das mesmas de forçarem o reinício da máquina. Este reinício poderá por exemplo interromper uma aquisição de um disco ou uma análise de uma imagem.

Outra boa prática é negar o acesso de escrita a discos amovíveis, impedindo assim que os discos de origem sejam alterados.

Um **dado volátil** é qualquer dado que pode ser perdido quando o sistema é desligado, como por exemplo um registo de uma ligação a um site na Internet, que ainda esteja presente na memória RAM ou o conteúdo do clipboard do sistema. A recolha destes dados deve de ocorrer com o sistema em funcionamento.

Live-Data Forensics, é a técnica utilizada na recolha de dados voláteis e que podem ser perdidos caso o dispositivo deixe de ter energia.

DUMP da memória é o procedimento de armazenar num ficheiro, todos os dados presentes num determinado momento na memória física do computador.

Na recolha deste tipo de dados é necessário ter em conta a ordem de volatilidade dos dados, adaptando a recolha à categoria de dados que mais interessam. Caso o nosso objetivo seja identificar o envio de um e-mail para determinado endereço, não fará muito sentido dar prioridade à identificação de processos em vez da recolha de senhas, ou a credencias de acesso, que permitam acesso ao endereço de e-mail.

É muito importante que a recolha de dados em live data seja devidamente documentada, preferencialmente criando uma equipa de recolha de pelo menos dois elementos, de modo a garantir os procedimentos de recolha seja efetuado por um elemento enquanto o outro documenta o processo de recolha utilizado.

É também importante garantir a mínima alteração ao sistema a ser analisado e caso seja necessário efetuar alguma alteração que a mesma seja registada em relatório, para memória futura.

Recomendações na utilização de scripts:

· Utilização de variáveis de ambiente
(ex.: cmd: %COMPUTERNAME% / PS: $env:Computername)

· Execução em modo Administrador

4.1.1. Ferramentas Nativas de Sistema

Tendo em consideração a mínima pegada digital no dispositivo, devemos sempre que possível utilizar ferramentas de âmbito forense para a recolha de informações úteis que permitam uma análise mais eficiente. A exemplo disso temos informações relativas a *full-disk encryption*. No entanto o sistema operativo MS Windows permite a execução de comandos e scripts com ferramentas nativas, sendo uma excelente possibilidade de obter as informações necessárias com uma mínima pegada digital.

Linha de Comandos	A linha de comandos do sistema MS Windows é nativamente uma das mais utilizadas na recolha de informação de sistema, possibilitando a execução de inúmeros programas para este fim.	
Windows Management Instrumentation (WMI)	Windows Management Instrumentation permite o acesso ao sistema operativo através do Windows Management Instrumentation Command-line, sendo uma excelente forma de obter informações do mesmo.	
Windows Batch File	É um ficheiro de script que permite agrupar um conjunto de comandos, linha a linha. Permite a utilização de estruturas de repetição, estruturas condicionais, a utilização de variáveis, típicas de uma linguagem de script.	

Powershell	PowerShell é atualmente a linguagem de script, inicialmente desenvolvida para os sistemas MS Windows, sendo disponibilizado o seu código-fonte aberto e com suporte multiplataforma, em 2016. Com uma Shell própria, o PowerShell foi desenvolvido para permitir a execução de cmdlets, permitindo também a execução de outras shells.	

4.1.2. Ferramentas Externas

Como recurso a ferramentas externas, deve existir o cuidado de testar exaustivamente cada uma destas ferramentas, de modo a saber exatamente o que as mesmas fazem no sistema. Quaisquer ferramentas externas utilizadas, deve ser anotado a data/hora de utilização, bem como descrever a intenção de utilização.

Windows Sysinternals	Windows Sysinternals representa um conjunto de ferramentas originalmente criadas por Mark Russinovich, com intenções de ajudar os administradores de sistemas a gerir e monitorizar os sistemas Windows. https://docs.microsoft.com/en-us/sysinternals/	
Nirsoft	NirSoft representa um conjunto de ferramentas criadas por Nir Sofer, das quais destacamos as que o mesmo categorizou de âmbito forense. http://www.nirsoft.net/	
Mitec	Mitec é também um site que disponibiliza um conjunto de ferramentas interessantes para recolha e análise de informação, a exemplo é o seu MiTeC System Information X e o Windows Registry Recovery https://www.mitec.cz/	
Zimmerman	Eric Zimmerman desenvolveu um conjunto de ferramentas de utilização gratuita, com a intenção de ajudar na resposta a incidentes e na análise forense.	**Eric Zimmerman Tools**

4.1.3. Data, Hora e outras informações do Sistema

Este elemento deve ser o primeiro a ser recolhido quando se executa uma investigação. A data do sistema permite contextualizar a informação recolhida mais tarde e permite ao investigador construir uma timeline de eventos ocorridos, não só no sistema em análise, mas através da correlação entre as informações de outros sistemas. Outro dado importante é o tempo decorrido desde o último boot (uptime).

Algumas ferramentas podem ajudar os investigadores nestas tarefas, como por exemplo MiTeC - System Information X[1] e WinAudit[2].

Recolha da data/hora do sistema que está a ser intervencionado (Figura 32).

Figura 32 - Obtenção da data e hora do sistema.

Recolha da data/hora do último arranque do sistema (Figura 33).

Figura 33 - Obtenção da data e hora do último boot do sistema

Comandos úteis para obtenção de dados do sistema:

- Versão do Windows: **ver**
- Variáveis de ambiente: **set**
- Informações de Sistema: **systeminfo /fo list >> C:\tmp\info.txt**
- Consulta ao registo: **reg query "HKLM\SOFTWARE\Microsoft\Windows NT\CurrentVersion" /v ProductName**
- Consulta através do WMI: **wmic os get name, version**
- Início e encerramento do sistema: **TurnedOnTimesView.exe** (Fonte: Nirsoft.net)

Comandos úteis para obtenção de dados sobre Utilizadores de Sistema

- Utilizadores:

o **Net User** [username]

o **Userprofilesview.exe /shtml "f:\temp\profiles.html" /sort "User Name"** (Fonte: Nirsoft.net)

- Utilizadores Logados:

o **PSLoggedOn.exe** (Fonte: SysInternals)

o **LogonSessions.exe** (Fonte: SysInternals)

4.1.4. Processos e Aplicações

É fulcral a enumeração dos processos em execução num Sistema potencialmente comprometido. Um processo é uma seção ou instância de uma aplicação que está a ser executado. A observação dos processos em execução no Task Manager dá algumas informações, no entanto pode ser obtida muito mais informação do que a aí observada.

Alguns dos tipos de informações sobre os processos em execução, possíveis de serem obtidos:

- O caminho absoluto do ficheiro executável
- O comando utilizado para lançar o processo
- A quantidade de tempo em que o processo está em execução
- Qual o utilizador que iniciou o processo e o seu nível de permissões no sistema
- Módulos que o processo tenha carregado
- Conteúdo da memória alocada ao processo

Exemplos de programas e comandos para aquisição de informações sobre os **processos em execução** no sistema:

- **Psinfo.exe -h -s -d /accepteula** (Fonte: SysInternals)
- ***PsList.exe*** (Fonte: sysinternals)
- ***CurrProcess.exe*** (Fonte: Nirsoft.net)
- ***tasklist /v***
- ***Wmic process get name, processid, priority, threadcount, privatepagecount***

Exemplos de programas e comandos para aquisição de informações sobre os **serviços, tarefas agendadas e eventos** do sistema:

- [serviços] **PsService.exe** (SysInternals)

- [serviços] **net start**
- [tarefas agendadas] **schtasks**
- [eventos] **PsLogList.exe** (SysInternals)
- [eventos] **EventLogSourcesView.exe** (Nirsoft)
- [eventos] **wevtutil**

4.1.5. Memória

Clipboard é uma área na memória onde podem ser armazenados dados para uso futuro. A maior parte das aplicações em Windows providenciam esta funcionalidade através do menu Edit e as escolhas Copiar, Colar ou Cortar. Esta funcionalidade é útil para mover dados entre aplicações ou documentos. Muitas vezes dados ficam na Área de Transferência durante dias, sem que o utilizador se aperceba.

Para recolher os dados persentes nesta zona da memória pode ser utilizada a aplicação **InsideClipboard.exe** (Nirsoft.net).

Analistas de malware pesquisam na memória quando lidam com malware ofuscado, pois quando este é executado é decifrado para a mesma memória. Além disso os Rootkits escondem processos, ficheiros, chaves de registo e até ligações de rede. É possível verificar o que está escondido da vista do utilizador através da análise da memória RAM. Estes dados são bastante úteis para contextualizar dados identificados em análises futuras.

4.1.6. Aquisição da Memória

O processo de Dump da Mémória (Figura 34) é também muito utilizado para diagnosticar bugs em programas, pois normalmente são criados esses dumps quando existe um erro e os programas deixam de inesperadamente de funcionar.

Estes dumps da memória são feitos em formato binário, octal ou hexadecimal. Pode ser feita uma investigação utilizando programas, como por exemplo:

- DumpIT (moonsols)
- AccessData FTK Imager
- Belkasoft Live RAM Capturer

Figura 34 - Exemplo do funcionamento do DumpIT

Existem outros ficheiros[3], de suporte à memória principal, que devem ser recolhidos, como por exemplo **pagefile.sys**, utilizado pelo Windows como "memória virtual". Sempre que o sistema necessita de utilizar mais memória do que a disponível na RAM. Ou **hiberfil.sys** é utilizado para armazenar os dados da memória quando o computador hiberna.

Para recolha da memória em ambiente Linux podem ser utilizados os programas *dcfldd* ou *insmod*.

- dcfldd if=/dev/fmem of=memory.dump
- insmod lime-XX.ko "path="memory.dump" format=raw"

4.1.7. Informação de Rede

Recolha de informações voláteis sobre o estado da rede do computador: conexões ativas, portos abertos, informações e configuração de encaminhamento, cache, ARP....

Assim que um incidente é reportado, o investigador deve recolher informações sobre o estado das ligações de rede com o sistema afetado.

Estas ligações podem expirar e a informação desaparecer com o passar do tempo. A observação destes dados pode ajudar a determinar se um atacante ainda está logado no sistema, se existe ligações relacionadas com malware, se existe algum processo a tentar encontrar outras máquinas na rede para propagação desse malware ou enviar informações de log para um servidor malicioso.

A recolha destas informações pode providenciar pistas importantes e acrescentar contexto a outras informações recolhidas.

Exemplos de comandos para recolha de informações de rede:

- Informação sobre placa de rede: **ipconfig /all**
- Cache do DNS: **ipconfig /displaydns**
- Ligações de Rede ativas: **Netstat -a**
- Cache do ARP: **Arp -a**
- **Netsh int ipv6 show neigh**
- Eventos wifi: **Netsh wlan show all**
- Redes Wireless: **WifiInfoView.exe** (Fonte: Nirsoft.net)
- Tabela de Routing: **Route print**
- Cache conexões: **Netstat -c**
- Lista as sessões de Cache: **Netstat -s**
- **Net accounts**
- Partilha de recursos: **Net share**
- Questiona o Servidor sobre DNS: **Nslookup -d**
- Lista as conexões atuais: **Rasdial**
- Lista os perfis: **Netsh wlan show profiles**

---

[1] www.mitec.cz/msi.html

[2] www.parmavex.co.uk

[3] https://www.hackingarticles.in/forensics-analysis-of-pagefile-and-hibersys-file-in-physical-memory/

4.2. Análise da Aquisição da Memória

Existem algumas ferramentas para análise do dump da memória que se baseiam apenas nos conteúdos da RAM. Estes conteúdos poderão estar incompletos, já que partes da memória são armazenadas em disco quando esta não é suficiente para o armazenamento de todos os dados. Para ultrapassar este problema, Nicholas Paul Maclean publicou na sua tese, "Acquisition and Analysis of Windows Memory", o funcionamento da gestão da memória em sistemas Windows e providenciou uma ferramenta, open-source, com o nome de vtop para reconstruir na íntegra o espaço virtual da memória de um processo.

Para a análise do Dump de Memória podemos utilizar o programa Volatility[1], onde é possível realizar tarefas como a obtenção de informações de alto nível sobre a imagem, onde é deduzida a identificação do sistema operativo (Figura 35), service pack, arquitetura de hardware, endereço de memória e a hora do Dump.

Figura 35 - Obter informação acerca de um dump de memória

Comandos úteis para efetuar o dump do registo:

Exportação para texto:

C:\Regdmp.exe > e:\registryDump.txt

Localizar Expressões no ficheiro exportado:

C:\Find/i "URL" registryDump.txt

Cópia dos ficheiros de registo em utilização:

C:\RawCopy.exe C:\WINDOWS\system32\config\SYSTEM E:\output -AllAttr

Outros comandos úteis:

Obter um screenshot do ambiente de trabalho:

C:\nircmd.exe savescreenshot screen1.png (Nirsoft.net)

Verificação se o disco está protegido com Encriptação (Figura 36)

C:\EDD.exe /accepteula /Batch > e:\EncryptedDiskDetector.txt

C:\Manage-bde –protectors c: -get

Figura 36 - Identificação de um disco encriptado

4.2.1. Sintaxe do programa Volatility

A primeira versão do The Volatility Framework foi lançada numa conferência Black Hat. O software está baseado em anos de investigação académica em análise avançada de memória e forense. O Volatility passou a permitir aos investigadores analisar o estado em que a máquina estava, na altura em que a aquisição foi feita, com base em dados recolhidos da memória volátil.

O The Volatility Framework é baseada na linguagem de programação Python, sendo desenvolvida em Python 2 a sua versão mais maturada, sendo esta que iremos abordar neste tópico. Com o aparecimento do Python 3, surgiu também a necessidade de atualizar a versão do Volatility, aproveitando as vantagens da utilização da nova versão do Python e dotando-o de uma maior automatização. Na versão 2 do The Volatility Framework, o primeiro passo para proceder à análise da memória é a identificação do tipo de Sistema Operativo. Para tal podemos utilizar o comando imageinfo do programa Volatility (Figura 37). Este comando é útil para obtenção de informações de alto nível sobre a imagem, indica a provável identificação do sistema operativo (perfil), service pack, arquitetura de hardware, endereço de memória e a hora do Dump.

Figura 37 - Volatility - Exemplo de output do comando imageinfo

Posteriormente devemos passar os conteúdos da memória para ficheiros de texto para que seja possível uma análise aos seus conteúdos. O Volatility disponibiliza uma série de plugins com essa finalidade.

Sintaxe: **volatility -f <nome_da_imagem> -profile=<tipo_de_OS> <plugin> > <output>**

- **-f:** Ficheiro resultante da aquisição do sistema
- **-profile:** instrução para utilizar o perfil de sistema operativo *(previamente identificado)*
- **plugin:** plugin a ser executado
- **output:** ficheiro para exportar os resultados

4.2.2. Plugins Volatility - Extração

Os plugins que o volatility utiliza são específicos para a identificação das respetivas informações no conteúdo do dump da memória RAM. Iremos aqui abordar alguns desses plugins.

Pslist Listar processos em Execução

Pstree Exibir processos, diferenciando-os na sua origem (Figura 38)

Figura 38 - Plugin pstree do volatility

Psxview Comparar processos (Figura 39)

Figura 39 - Plugin psxview do volatility

Netscan Exibir conexões de rede

Cmdline Comparar processos (Figura 40)

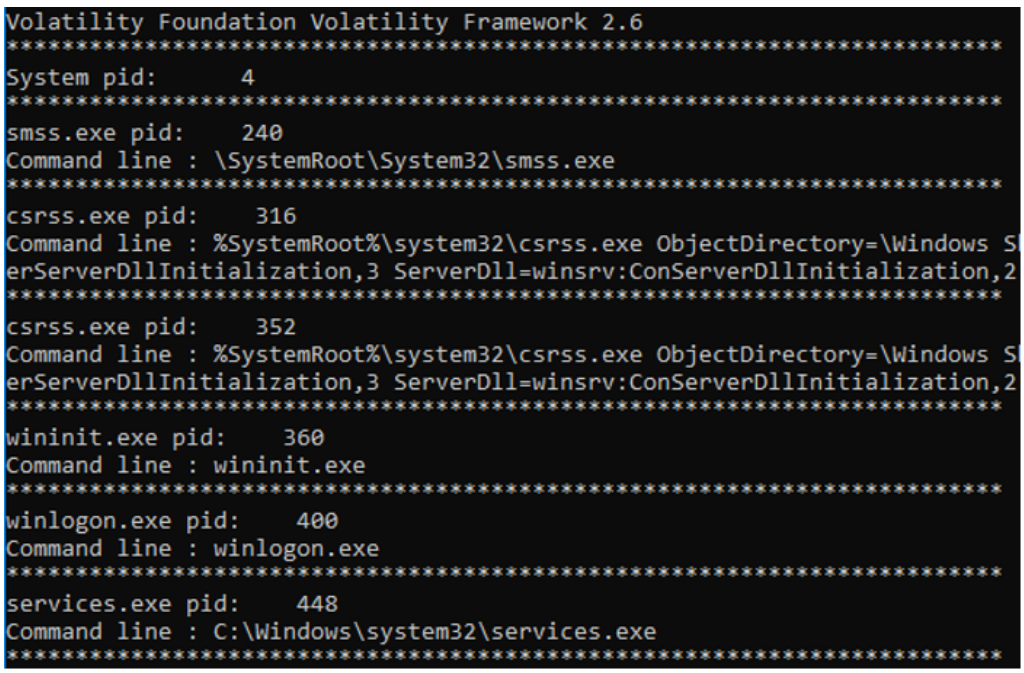


Figura 40 - Plugin cmdline do volatility

Cmdscan Comparar processos (Figura 41)

Figura 41 - Plugin cmdscan do volatility

Consoles. Comparar processos (Figura 42)

Figura 42 - Plugin consoles do volatility

Dumpregistry Extrair arquivos de registo

4.2.3. Plugins Volatility – Análise

Com os ficheiros de registo que foram extraídos da memória, é possível proceder à sua análise com as mesmas ferramentas que os ficheiros de registo extraídos do sistema operativo. A exemplo disso é o RegRipper, o próprio volatility, ou o RegistryReport, cuja imagem se apresenta na Figura 43.

Figura 43 - Análise dos ficheiros com o RegistryReport

Na análise da memória é ainda possível obter ficheiros que tenham sido processados, existindo alguns programas com a possibilidade de identificar e extrair ficheiros da memória, tal como apresentado na figura seguinte com o software Belkasoft, onde é possível verificar que o mesmo identificou endereços de navegação nos Browsers, dados de conversação em chats, ficheiros de email e ficheiros de imagem (Figura 44).

Figura 44 - Análise dos ficheiros com o Belkasoft

A SANS publicou um Poster (Figura 45) alusivo à análise de memória com Volatility, que resume muitos dos plugins úteis neste tipo de análise.

Figura 45 - Poster SANS - Memory Forensics Cheat Sheet v2.0

Criar uma TimeLine de eventos na memória

Com os dados extraídos da memória volátil é útil criar uma **Timeline**, para possibilitar datar e ordenar os indícios no sistema. Sendo este um processo que envolve os procedimentos descritos de seguida:

Timeliner criar uma timeline

C:\> volatility_2.6_win64_standalone.exe -f IE8WIN7.dmp --profile=Win7SP1x86_23418 timeliner -- output=body > timeliner.body

Ler mais: https://volatility-labs.blogspot.com/2013/05/movp-ii-23-creating-timelines-with.html

Mftparser Obter a atividade da MFT (Master File Table).

C:\> volatility_2.6_win64_standalone.exe -f IE8WIN7.dmp --profile=Win7SP1x86_23418 mftparser -- output=body > mftparser.body

Combinar os ficheiros relativos aos plugins **timeliner** e **mftparser.**

cat timeliner.body mftparser.body >> timeline.log

Mactime[2] Gerar a timeline a partir da combinação dos ficheiros

mactime -d -b timeline.log > timeline.csv

Resultado final dos procedimentos de TimeLine (Figura 46)

Figura 46 - Conteúdo do timeline.csv

Com esta tabela é possível identificar facilmente as ações passadas na memória do dispositivo, sendo que estas irão complementar as informações obtidas na análise ao dispositivo em dead-box forensics.

Exemplo de identificação de acessos à rede TOR

A exemplo de análise de dados da memória, temos a utilização do Tor Browser, uma vez que o mesmo não guarda informações de navegação no disco rígido, apesar de ser possível a sua identificação e análise através da memória.

Começamos por confirmar o **perfil do sistema** (Figura 47).

Figura 47 - Plugin imageinfo do volatility

Recorremos ao plugin **pstree** para verificar os processos em execução, filtrando os processos pelo nome “firefox.exe” (Figura 48), já que o Tor Browser utiliza este processo, ou então diretamente pelo nome “tor.exe”. Para obtermos mais informação sobre os processos no dispositivo em análise, ainda temos a possibilidade de utilizar os plugins **pslist**, **psscan**.

Figura 48 - Utilização do volatility na pesquisa de processos

Getsids Informação sobre o início do processo, relacionando o processo com o utilizador (Figura 49).

Figura 49 - Utilização do volatility na identificação de processos

netscan exibir as ligações de rede

Neste caso, o processo “tor.exe” indica uma conexão concluída ao IP de destino "54.37.17.235" no porto 9001 (Figura 50).

```
dfir@LAPTOP:/mnt/c/BoH$ vol.py -f Win10_14393_Tor_Closed.vmem --profile=Win10x64_14393 netscan | egrep "firefox.exe|tor.exe"
Volatility Foundation Volatility Framework 2.6
0x80814c899ab0     TCPv4    127.0.0.1:9150                 127.0.0.1:51014      CLOSED          3552     tor.exe         2018-03-18
11:26:53 UTC+0000
0x80814c8cb8b0     TCPv4    192.168.241.133:50630          54.37.17.235:9001    CLOSED          3552     tor.exe         2018-03-18
11:18:59 UTC+0000
0x80814cafb470     TCPv4    127.0.0.1:51099                127.0.0.1:9150       CLOSED          7960     firefox.exe     2018-03-18
```

Figura 50 - Utilização do volatility na identificação de rede

Firefoxhistory Listar os endereços (URLs) consultados (Figura 51).

Figura 51 - Utilização do volatility na obtenção de URL da memória

Fonte: https://blog.superponible.com/2014/08/31/volatility-plugin-firefox-history/

---

[1] https://github.com/volatilityfoundation/volatility/wiki/Command-Reference

[2] https://wiki.sleuthkit.org/index.php?title=Mactime

5. Identificação e análise de informação nos Sistemas Operativos

De acordo com "https://gs.statcounter.com/os-market-share/desktop/worldwide", o sistema operativo Microsoft Windows detém uma quota de mercado de cerca de 75%, sendo seguido pelo Apple OS X, com 14,5%. Um analista forense, irá encontrar um bastante maior número de dispositivos com sistemas operativos da Microsoft, que quaisquer outros. Justificamos assim a maior atenção dada à análise deste sistema operativo.

A SANS, tem realizado um excelente trabalho de investigação e educação na área da forense digital, sendo um dos fatores de interesse a publicação regular do designado Poster, em: https://www.sans.org/posters/, com os resultados dessa investigação. Estes Posters, são também de importantes fontes de informação relativa à localização de artefactos de interesse forense, já que os sistemas operativos MS Windows, armazenam inúmeros artefactos na ação quotidiana dos seus utilizadores.

5.1. Registo do MS Windows

"*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.*"

Fonte: *Microsoft Computer Dictionary.--5th ed.*, Redmond, Washington, Microsoft Press, 2002, p. 445

É assim possível afirmar que o registo do Windows apesar dos seus ficheiros estruturantes, contém uma estrutura lógica em constante utilização pelo sistema operativo, armazenando um conjunto de informações necessárias ao seu funcionamento.

A estrutura lógica do registo do Windows contém:

1. **Chaves do registo**, chaves de nome "Software" e "System", pertencentes ao *hive* "HKEY_CURRENT_CONFIG".
2. **Subchaves do registo**, onde são armazenadas as informações do registo (e.g.: subchave "Fonts").
3. **Valores do registo,** são estes que contêm as informações especificando o seu tipo na coluna respetiva (e.g.: REG_DWORD - valor binário de 32-bit, REG_QWORD – valor binário de 64-bit).

Os cinco principais Hives na estrutura lógica do sistema operativo MS Windows pode ser observada na Figura 52.

Figura 52 - Root Hive

Hive do registo (Root Keys) são caracterizados pelo prefixo "HKEY_", abreviatura de "Handle to a KEY".

São 5 os hive principais, armazenadas nos diversos ficheiros que compõem o registo, apesar de apenas o HKEY_USERS e o HKEY_LOCAL_MACHINE serem considerados como os verdadeiros hive, sendo os restantes atalhos ou aliases para ramificações dentro destes.

Hive	**Abreviatura**	**Descrição**	***Link***
HKEY_CURRENT_USER	**HKCU**	Points to the user profile of the currently loggedon user	Subkey under HKEY_USERS corresponding to currently loggedon user
HKEY_USERS	**HKU**	Contains subkeys for all loaded user profiles	Not a link
HKEY_CLASSES_ROOT	**HKCR**	Contains file association and COM registration information	Not a direct link; rather, a merged view of HKLM\SOFTWARE\Classes and HKEY_CURRENT_USER\SOFTWARE\Classes
HKEY_LOCAL_MACHINE	**HKLM**	Global settings for the machine.	Not a link
HKEY_CURRENT_CONFIG	**HKCC**	Current hardware profile	HKLM\SYSTEM\CurrentControlSet\Hardware Profiles\Current
HKEY_PERFORMANCE_DATA	**HKPD**	Performance counters	Not a link

Fonte: *Windows Internals.--6th ed., Part 1*,
Redmond, Washington, Microsoft Press, 2012, p. 281

Os ficheiros de registo encontram-se localizados nas seguintes pastas:

Ficheiros do registo referente ao sistema operativo

C:\Windows\System32\Config\

Ficheiros do registo referente a cada utilizador

C:\Users\<username>\ntuser.dat

5.1.1. Editor de registo (RegEdit)

O editor de registo, na sua versão gráfica, permite fazer a exportação de uma, ou mais chaves de registo (Figura 53).

RegEdit, Ficheiro > Exportar

Figura 53 - Exportação do Registo através do RegEdit

Através da linha de comandos:

regedit /e c:\output.reg "HKEY_LOCAL_MACHINE\System\..."

5.1.2. ERUNTgui

A aplicação ERUNTgui (Figura 54), permite realizar o backup, restauro e otimização do registo, sendo de interesse forense a possibilidade de realizar o backup do registo, possibilitando assim a sua posterior análise.

Figura 54 - Exportação do Registo através do ERUNTgui

5.1.3. RAWCopy

A aplicação RAWCopy (Figura 55), permite a cópia dos setores do disco onde os ficheiros em utilização se encontram, ultrapassa-se deste modo a limitação da cópia de ficheiros abertos pelo sistema.

Figura 55 - Exportação do Registo através do RAWCopy

Através do RAWCopy foi possível obter uma cópia do ficheiro SAM e SOFTWARE com o sistema em execução (Figura 56).

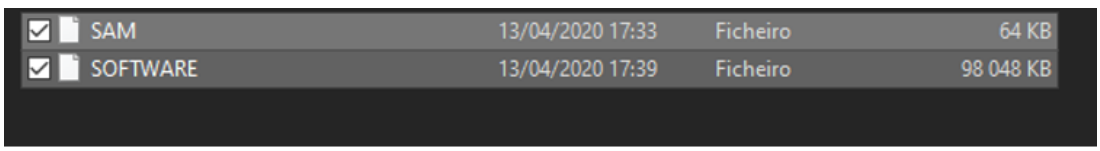


Figura 56 - Ficheiros exportados pelo RAWCopy

Fonte: https://github.com/jschicht/RawCopy

5.2. Análise de Registo do Windows

A análise do registo do Windows poderá ser realizada através de software de âmbito forense, como o AccessData Registry Viewer, ferramentas do Eric Zimmerman, RegRipper, ou mesmo com outro qualquer software com capacidade de realizar a extração de dados destes ficheiros de registo.

Devido à complexidade do registo do Windows, identificar a localização de cada informação relevante, poderá ser uma tarega árdua, no entanto, contamos com a preciosa ajuda da SANS FOR500 (https://digital-forensics.sans.org/docs/DFPS_FOR500_v4.11_0121.pdf), identificando muitas das localizações importantes onde se poderá encontrar informação relevante.

Poderá existir a necessidade de extrair o registo de um computador ligado, sendo o registo uma enorme fonte de informação relevante a nível forense, será imperativo obter toda essa informação. (Ler: https://resources.infosecinstitute.com/windows-registry-analysis-regripper-hands-case-study-2/). Existem diversos modos de realizar o *dump* do registo, vamos aqui focar alguns diferentes modos.

5.2.1. O Fuso horário (TimeZone)

Das primeiras informações a analisar, deve constar o Fuso Horário (Figura 57), já que o mesmo poderá determinar que estejamos induzidos em erro perante ações que apresentam uma data/hora diferente da verdadeira, simplesmente por o sistema estar configurado com um fuso horário diferente do que o analista forense se encontra a utilizar.

Esta informação poderá ser identificada na *hive* SYSTEM, na seguinte localização:

SYSTEM\ControlSet001\Control\TimeZoneInformation

Figura 57 - Visualização do TimeZone no AccessData Registry Viewer

5.2.2. Dispositivos USB

No registo é também possível obter informação de dispositivos USB que se ligaram ao sistema na *hive* SYSTEM:

Para obter: Fabricante / marca / n.º série / data/hora da primeira e última conexão ao sistema

HKLM\SYSTEM\CurrentControlSet\Enum\USBSTOR

HKLM\SYSTEM\CurrentControlSet\Enum\USB

Visualizando esta chave de registo através do Editor de registo, é possível visualizar como são apresentadas estas informações (Figura 58).

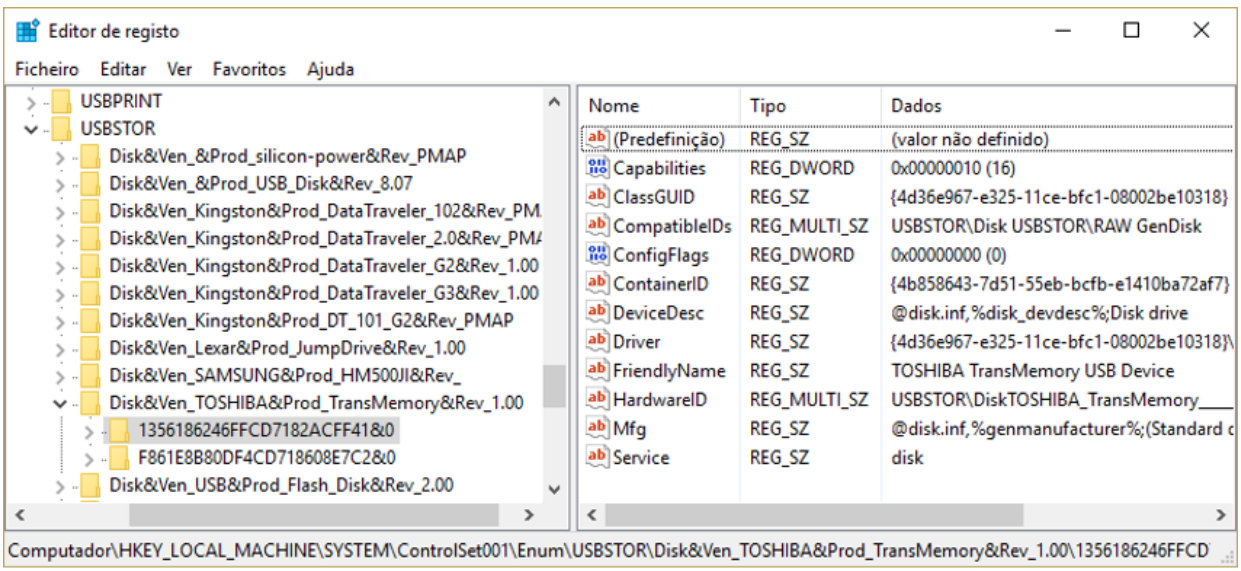


Figura 58 - Visualizando os dispositivos USB no Editor de registo

Para obter a letra atribuída ao dispositivo USB

HKLM\SYSTEM\MountedDevices

Para obter o utilizador que ligou o dispositivo ao sistema

NTUSER.dat\Software\Microsoft\Windows\CurrentVersion\Explorer\MountPoints2

A mesma informação é possível ser obtida com recurso a ferramentas específicas para obter a informação dos dispositivos USB, como é o caso das ferramentas 4Discovery ou USBDeview (Figura 59).

Figura 59 - Visualizando os dispositivos USB no USBDeview

Ler mais: https://www.researchgate.net/publication/318514858_USB_Storage_Device_Forensics_for_Windows_10

5.2.3. Utilizadores

A informação sobre os utilizadores do sistema encontra-se armazenada no registo do Windows na *hive* SAM, no entanto existe ainda o ficheiro de registo NTUSER.DAT por cada utilizador, que armazena dados específicos desse mesmo utilizador:

Lista dos perfis dos utilizadores locais

No registo: HKLM\Software\Microsoft\Windows NT\CurrentVersion\ProfileList

Utilizadores do Sistema

No Ficheiro: SAM\SAM\Domains\Account\Users\

Visualizando esta chave de registo através do Editor de registo, é possível visualizar como são apresentadas estas informações (Figura 60).

Figura 60 - Visualizando os utilizadores no editor de registo

A mesma informação é possível ser obtida com recurso a ferramentas específicas para obter a informação dos utilizadores, como é o caso do AccessData Registry Viewer (Figura 61).

Figura 61 - Visualizando os utilizadores no AccessData Registry Viewer

5.2.4. Rede

O registo contém também diversas informações de rede, como as redes sem fios a que o sistema se ligou:

HKLM\Software\Microsoft\Windows NT\CurrentVersion\NetworkList\

Nesta localização é possível identificar:

- Nome da rede (SSID)
- Nome do domínio / intranet
- Data/Hora da última ligação (através da data/hora que a respetiva chave foi escrita)
- MAC address do Gateway

5.2.5. Análise de Registo do Windows - RegRipper

No que diz respeito à análise do registo do Windows, existem muitas ferramentas de âmbito forense que conseguimos utilizar para facilitar a análise de informações constantes no registo do Windows, focamos aqui algumas ferramentas de utilização gratuita como o RegRipper, o RegistryReport e o Windows Registry Recovery.

RegRipper (http://github.com/keydet89) é uma aplicação Forense Open Source, desenvolvida por Harlan Carvey e escrita em PERL, com o objetivo de extrair de forma legível, informações dos ficheiros de Registo do Windows.

O RegRipper (Figura 62) pode ser utilizado através da linha de comandos e de uma interface gráfica para extrair informações específicas de cada arquivo do Registro. Na utilização em linha de comando é possível selecionar o plugin que se pretende aplicar a cada *hive* de registo, já no caso da linha de comandos são aplicados todos os plugins disponíveis para a *hive* selecionada. O resultado das informações extraídas poderá ser apresentado no ecrã ou gravadas num ficheiro de texto, em caso de utilizarmos a linha de comandos. Através da sua interface gráfica será necessária a indicação da localização de output, designada por Report File, para ser criado o ficheiro de texto com o resultado de todos os plugins aplicados à respetiva *hive* de registo.

Figura 62 - Utilização do RegRipper

Através da linha de comandos é possível verificar os plugins disponíveis para aplicar através do argumento "-l -c".

C:\RegRipper3.0-master>rip -l -c > c:\list.csv

No modo GUI (Figura 63), não nos é possível escolher um único plugin, mas sim a Hive que pretendemos analisar.

Figura 63 - Utilização da GUI do RegRipper

Ficheiro de output (Figura 64)

Figura 64 - Ficheiro de output do RegRipper

Existem outras aplicações de âmbito forense com o mesmo objetivo de interpretarem o conteúdo dos ficheiros de registo, como o Registry Report e o Windows Registry Recovery.

RegistryReport

Tal como o RegRipper, o Gaijin Registry Repport também apresenta as informações do registo de modo facilmente legível e pesquisável. Tendo um funcionamento simples, permitindo selecionar as informações que se pretende obter no registo através de caixas de seleção, taç como apresentado na Figura 65.

Fonte: https://gaijin.at/en/files?dir=old-software registryreport

https://github.com/jschicht?tab=repositories

Figura 65 - Utilização do RegistryReport

Fonte: https://www.gaijin.at/en/files?dir=old-software&sort=N&order=A registryreport

Windows Registry Recovery

O WRR (Figura 66) é uma das aplicações que podemos utilizar para a análise do registo do Windows

Figura 66 - Utilização do MiTeC Windows Registry Recovery

Fonte: http://www.mitec.cz/wrr.html

5.3. Análise de sistemas Linux Based

A digital forense em sistemas operativos MS Windows, estão amplamente divulgados, quer através de cursos e artigos científicos, quer através de novos meios como vídeos. A digital forense em sistemas operativos Linux, não são tão divulgados, principalmente por a análise destes ser também muito menor número.

Sistema de Ficheiros

O sistema de ficheiros padrão atualmente em Linux é o Ext4 apesar de suportar diferentes tipos de sistemas de ficheiros.

Linux File System	Data	
Ext	1992	Significando “Extended file system”, foi o primeiro sistema de ficheiros criados para o linux em 1992
Ext2	1993	Suportava discos com até 2 TB e não suportava journaling. Por não usar journaling pode ser usado em pendrives.
Ext3	1999	Igual ao Ext2, mas com a vantagem de ter journaling.
Ext4	2006	A atual versão dos tipos Ext. possui várias funções vantajosas quando comparada com as suas antecessoras, como redução na fragmentação do sistema, funciona com ficheiros de grande dimensão, entre outras. EXT4 suporta 1EB (1 Exabyte) de tamanho máximo de sistema de ficheiros e 16TB de tamanho máximo de ficheiros. É possível ter um número ilimitado de subdiretórios

Considerações Gerais

1. Não existem ficheiros de registo como no SO Windows
2. A informação deve ser recolhida em localizações dispersas
3. Diferentes estruturas de ficheiros de Sistema em diferentes distribuições

A estrutura de ficheiros e pastas do sistema Linux pode ser resumida como apresentado na Figura 67.

Figura 67 - Estrutura de ficheiros do Sistema Linux

Fonte: The Linux Foundation – https://linuxfoundation.org/blog/classic-sysadmin-the-linux-filesystem-explained/

5.3.1. Points of Interest em Sistemas Linux

A análise da atividade do utilizador em sistemas Linux Ubuntu devem seguir uma sequência de validações e recolhas de informação, tal como a apresentada na Figura 68.

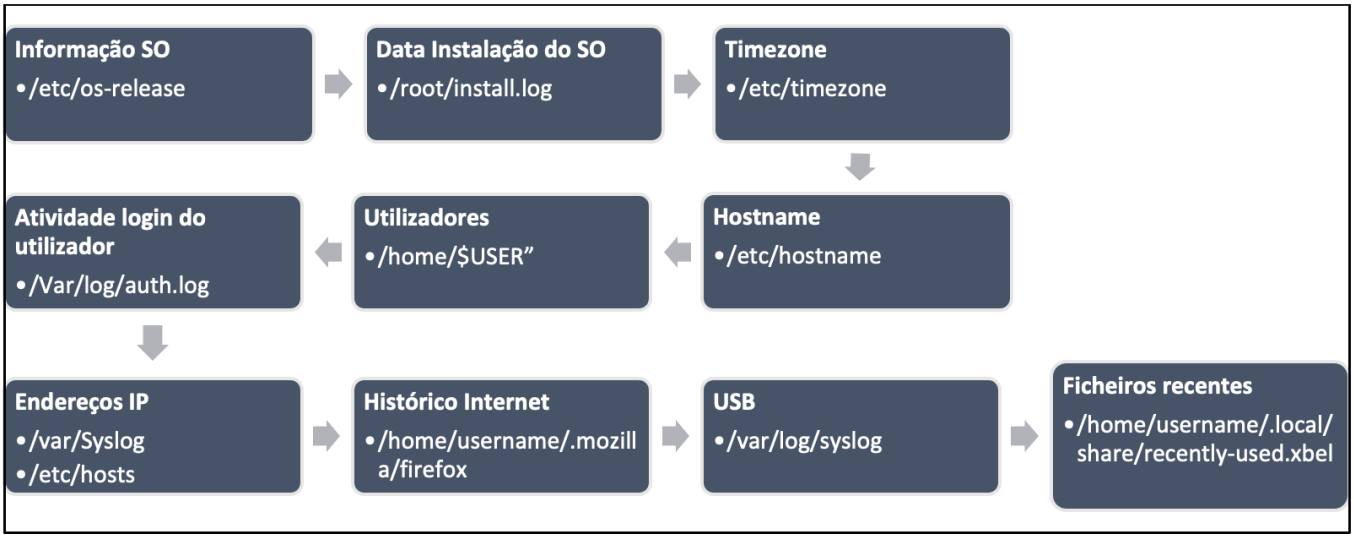


Figura 68 - Proposta de recolha de informação em Linux

Autorun de programas em funcionamento no sistema:

Tendo em conta que muitos programas são configurados para inicializaram automaticamente no arranque do sistema. As informações sobre os programas que devem ser executados no início estão no diretório "**/etc/rc.local**".

Documentos acedidos:

O examinador pode saber quais os documentos a que foram acedidos recentemente. O ficheiro que contém essa informação está em **/home/user/.local/share/recently-used.xbel.** O comando **cat** pode ser utilizado para ver o conteúdo do ficheiro. O ficheiro .xbel fornece informações detalhadas sobre os ficheiros que foram acedidos pelo utilizador, como exemplo, tempo de acesso e de modificação.

Aplicações Instaladas:

As informações sobre as aplicações está na pasta **/usr/bin** as blibiotecas necessárias para as aplicações está na pasta **/usr/lib.** A lista de aplicações pode ser obtida pelo comando **ls –l /usr/bin/.** Sendo possível perceber data de instalação, permissões, dimensão, etc.

Informação de Rede:

O Ubuntu mantém uma lista das redes conectadas ao sistema em: **/etc/NetworkManager/system-connections**

O ficheiro **/var/log/syslog** fornece a data e hora em que uma conexão de rede foi estabelecida.

Equipamentos conectados:

Na diretoria /dev fornece informação sobre o hardware conectado ao sistema.

O ficheiro **/var/log/syslog** tem também informação sobre os dispositivos que foram conectados ao sistema.

Último login e atividade do Utilizador:

A informação sobre o último login pode ser obtida em **/var/log/lastlog**

Atividade de navegação na Internet:

Apresenta-se a localização de pastas com informação de navegação, em dois dos principais browsers utilizados no sistema operativo Linux (Figura 69 e Figura 70). Após a extração destes conteúdos, torna-se possível a sua análise de igual modo que no sistema Windows.

Firefox Browser

Figura 69 - Localização de informações do Browser Firefox

Google Chrome

Figura 70 - Localização de informações do Browser Google Chrome

6. Análise forense com suites utilização gratuita

Uma análise forense requer conhecimento de ferramentas específicas que consigam obter e tratar a informação que pretendemos. Muitas são ferramentas comerciais, como o OpenText EnCase, o AccessData FTK, Magnet Axiom, entre outras. Como ferramentas de utilização gratuita, a situação é bem diferente, uma vez que existem muito poucas suites de análise disponíveis para utilização. Deste modo, iremos focar 2 destas suites, o IPED e o Autopsy The Sleuth Kit.

6.1. IPED

IPED – Indexador e Processador de Evidências Digitais é uma ferramenta open source, desenvolvida em Java pela investigação forense da Polícia Federal Brasileira, ficando conhecida por permitir boas prestações de processamento (Figura 71). Foi desenvolvido para permitir a análise de grande volume de dados por um grande número de pessoas, já que foi intencionalmente desenvolvido para a investigação da operação Lava Jato no Brasil. O elevado desempenho em multithread de até 400GB/h de velocidade de processamento, permite o suporte para grandes casos, com um grande volume de dados a ser processados.

Figura 71 - Processamento com IPED

https://github.com/sepinf-inc/IPED

Este é um software que requer algum conhecimento na sua utilização, apesar de apresentar uma aparência simples e intuitiva, como é possível observar na Figura 72.

Figura 72 - Análise com o IPED

Fontes: https://github.com/sepinf-inc/IPED/wiki/Beginner's-Start-Guide

https://servicos.dpf.gov.br/ferramentas/IPED/

6.2. Autopsy The Sleuth kit

The Sleuth Kit® é uma biblioteca e também um conjunto de ferramentas que permite a análise de sistemas de ficheiros FAT, NTFS, Ext2/3/4 e UFS, onde se incluem os habitualmente utilizados pelo Sistema Operativo Linux, permite ainda a análise de ficheiros e pastas, recuperar ficheiros apagados, criar uma *timeline* de atividades de ficheiros, realizar pesquisas por expressões e usar bases de dados de *hashs*.

https://github.com/sleuthkit/sleuthkit/blob/develop/NEWS.txt

Autopsy - O Autopsy é a interface gráfica (GUI) do The Sleuth Kit. É uma das plataformas de código aberto, desenvolvida para aproveitar as capacidades do The Sleuth Kit para realizar análises forenses a dispositivos como discos rígidos, media cards, smartphones, entre outros. Integra também outras ferramentas forenses, tanto de código aberto e/ou comercial, através de plug-ins ou módulos complementares em Java ou Python.

https://github.com/sleuthkit/autopsy/blob/develop/NEWS.txt

Apresenta-se a interface gráfica simples do Autopsy (Figura 73).

Figura 73 - Análise com o Autopsy

Esta, contém um menu lateral esquerdo, com a informação categorizada, identificando ficheiros, por tipo de extensão e por MIME Type, mas também todas as categorias a que os mesmos pertencem (- Categorização de ficheiros no AutopsyFigura 74).

Figura 74 - Categorização de ficheiros no Autopsy

Versões

https://github.com/sleuthkit/autopsy/releases/

Código Fonte

https://github.com/sleuthkit/autopsy

Tarefas e solicitações

https://github.com/sleuthkit/autopsy/issues