Fundação Educacional do Município de Assis
Instituto Municipal de Ensino Superior de Assis
Campus "José Santilli Sobrinho"

FERNANDO MORATO LIMA SILVA

DESAFIOS DA PERÍCIA FORENSE COMPUTACIONAL NA INVESTIGAÇÃO EM NUVEM

Assis/SP
2020

Fundação Educacional do Município de Assis
Instituto Municipal de Ensino Superior de Assis
Campus "José Santilli Sobrinho"

FERNANDO MORATO LIMA SILVA

DESAFIOS DA PERÍCIA FORENSE COMPUTACIONAL NA INVESTIGAÇÃO EM NUVEM

Projeto de pesquisa apresentado ao Curso de Ciência da Computação do Instituto Municipal de Ensino Superior de Assis – IMESA e a Fundação Educacional do Município de Assis – FEMA, como requisito parcial à obtenção do Certificado de Conclusão.

Orientando(a): Fernando Morato Lima Silva
Orientador(a): Prof. Me. Fábio Eder Cardoso

Assis/SP
2020

FICHA CATALOGRÁFICA

S586d SILVA, Fernando Morato Lima
Desafios da perícia forense computacional na investigação em nuvem / Fernando Morato Lima Silva. – Assis, 2020.

49p.

Trabalho de conclusão do curso (Ciência da Computação). – Fundação Educacional do Município de Assis-FEMA

Orientador: Me. Fábio Éder Cardoso

1.Computação forense 2.Computação-nuvem

CDD004.65

DESAFIOS DA PERÍCIA FORENSE COMPUTACIONAL NA INVESTIGAÇÃO EM NUVEM

FERNANDO MORATO LIMA SILVA

Trabalho de Conclusão de Curso apresentado ao Instituto Municipal de Ensino Superior de Assis, como requisito do Curso de Graduação, avaliado pela seguinte comissão examinadora:

Orientador: _____
Prof. Me. Fábio Eder Cardoso

Examinador: _____
Prof. Dr. Alex Sandro Romeo de Souza Poletto

Assis/SP
2020

RESUMO

Em consequência do aumento da utilização de métodos de armazenamentos *online*, também conhecidos como nuvem ou *cloud*, os crimes cometidos no mundo digital estão cada vez deixando menos evidencias, tendo em vista que o número de arquivos guardados em um disco rígido convencional estão cada vez menores. A perícia forense computacional busca solucionar esses crimes por meio de várias etapas de investigação e ferramentas usadas pelos profissionais, porém, com o a popularização da *cloud*, o rastreamento de evidencias sido cada vez mais difícil, já que não há evidencias físicas, apenas as armazenadas em serviços *online*. Este trabalho apresenta técnicas, conceitos, ferramentas e etapas da investigação utilizadas por peritos forenses na análise de evidencias, abordando também o tema de computação em nuvem, seus conceitos fundamentais e quais são os desafios do grande aumento da utilização desses serviços na solução de crimes digitais pela perícia forense computacional. Após isso será realizado um estudo de caso, utilizando a técnica de esteganografia e esteganálise em arquivos hospedados em servidores nuvem.

Palavras-chave: Computação Forense, Cloud Computing, Investigação de Crimes Virtuais

ABSTRACT

As a result of the increased use of online storage methods, also known as cloud, crimes committed in the digital world are increasing, leaving less evidence, given that the number of files stored on a conventional hard drive is decreasing. Computer forensic expertise seeks to solve these crimes, through various stages of investigation and tools used by professionals, however, with the popularization of the cloud, the tracking of evidence has become increasingly difficult, since there is no physical evidence, only those stored in online services. This paper presents techniques, concepts, tools and steps of the investigation used by forensic experts in the analysis of evidence, also addressing the topic of cloud computing, it's fundamental concepts and what are the challenges of the great increase in the use of these services in the solution of digital crimes computer forensic expertise. After that, a case study will be carried out, using a technique of steganography and reverse steganography on files hosted on cloud servers.

Keywords: Computer Forensics, Cloud Computing, Investigation of Virtual Crimes.

LISTA DE ILUSTRAÇÕES

SUMÁRIO

1. INTRODUÇÃO

A Internet vem ao longo dos anos ficando cada vez mais acessível para todos, fazendo com que o número de usuários aumente muito rapidamente. Juntamente com essa evolução e maior alcance da *web*, pode-se observar um crescente aumento na quantidade de crimes cometidos no mundo virtual, fazendo com que uma nova área tenha que surgir para investigar e solucionar esses delitos virtuais.

Lopes (2018) define a perícia forense computacional como uma ciência multidisciplinar, a qual se aplica metodologias investigativas para determinar a análise de evidências, sendo diferente dos outros tipos de perícias forenses, já que produz resultados diretos e não interpretativos, sendo decisivos em cada caso e com a finalidade de auxiliar na solução de situações onde há infrações cometidas utilizando algum dispositivo conectado à Internet.

> A evolução tecnológica faz com que a Computação Forense permeie áreas nunca antes imagináveis como: a balística, ao tratar da fabricação caseira de armas de fogo por meio de impressoras 3D; a medicina, em função da análise de dispositivos médicos, como marca passos; e a perícia em acidentes de trânsito, que pode contar com o auxílio da eletrônica embarcada (FRANCO; GUILAR; GUSMÃO; GROCHOCKI, 2016, p. 2).

> A computação em nuvem pode ser definida, de forma simplificada, como um paradigma de infraestrutura que permite o estabelecimento do SaaS (software como serviço), sendo um grande conjunto de serviços baseados na web com o objetivo de fornecer funcionalidades, que até então, necessitavam de grandes investimentos em hardware e software, e que funciona através de um modelo de pagamento pelo uso (BORGES; SOUZA; SCHULZE; MURY, 2011, p. 9).

Pode-se dizer que a computação em nuvem é um serviço onde o usuário paga para ter um "disco rígido *online*", com tamanho de acordo com o plano de armazenamento selecionado, o qual ele pode acessar de qualquer lugar, desde que tenha acesso a Internet.

> Antes os peritos buscavam informações em discos rígidos de máquinas, tinha-se o domínio de toda a infraestrutura e também o controle sobre aquela rede que era objeto de investigação. Hoje, com essa nova tecnologia, busca-se identificar de onde partiram as informações, se elas não foram

> adulteradas no transcurso dos envios, e como se fazer para rastrear alguém nesse sistema. Esbarrando-se, inevitavelmente na ausência de leis específicas para o caso de uma perícia em ambiente de computação em nuvem (DAMACENA, 2014, p.14).

1.1 OBJETIVOS

Esse trabalho tem como objetivo conceituar a perícia forense computacional, descrevendo os processos de coleta e análise de evidências, relatar as dificuldades em analisar e resolver crimes em ambiente de nuvem. Conceitualizar a computação em nuvem, detalhando como funciona esse ambiente. Por fim, realizar um estudo de caso, afim de mostrar na prática a dificuldade da perícia forense em arquivos armazenados em nuvem.

De forma geral, pretende-se conceituar a perícia forense computacional e a computação em nuvem, realizando um estudo de caso que unifica os dois tópicos.

1.2 JUSTIFICATIVA

A perícia forense computacional é uma das áreas mais novas da perícia, portanto a maior parte das informações de artigos, livros, trabalhos e documentos são escassos. Esse trabalho almeja preencher a lacuna, provendo conhecimento a respeito da investigação da perícia forense nos ambientes em nuvem, tal como um estudo de caso do respectivo tema. A seguinte pesquisa é de extrema importância para a área da perícia forense computacional, retratando um dos assuntos que, em um futuro próximo, é algo que será muito estudado e utilizado por profissionais forenses, já que cada vez mais o uso de meios físicos para armazenar informações está diminuindo e os ambientes em nuvem crescendo mais a cada dia.

1.3 MOTIVAÇÃO

A motivação para a elaboração desse trabalho foi o interesse de seguir na área da perícia forense computacional após o termino da faculdade e de auxiliar trabalhos futuros com assuntos parecidos, tendo em vista que a computação forense em nuvem é uma área mais recente da perícia digital, a qual vem ganhando cada vez mais espaço, já que a tendência é de que em um futuro próximo a maioria dos nossos dados fiquem armazenados em ambiente de nuvem, tal como o Google Drive ou Dropbox.

1.4 PERSPECTIVAS DE CONTRIBUIÇÃO

Este trabalho poderá contribuir com futuros estudos envolvendo a computação forense em nuvem, já que a tendência é que cada vez mais crimes virtuais utilizando ambientes em *cloud* surjam, podendo assim, auxiliar outras pessoas que tenham interesse em realizar estudos na área. Percebe-se, cada vez mais, que o desafiador cenário globalizado é uma das consequências do fluxo de informações. Desta maneira, o fenômeno da Internet estende o alcance e a importância das diretrizes de desenvolvimento para o futuro.

1.5 METODOLOGIA DE PESQUISA

Esse trabalho terá como metodologia estudos e análise de projetos retirados de artigos científicos, teses, TCC, revistas, tendo como conceito parte da pesquisa descritiva onde, serão levantados informações e dados sobre o tema, visando uma análise no ambiente natural, para que exista uma maior concretização das informações identificadas.

Após o levantamento dos dados e análises, o trabalho terá como característica a pesquisa exploratória, onde haverá a exploração um problema, de modo a fornecer informações para uma investigação mais precisa. Por fim, a metodologia se encerrará com um estudo de caso no ambiente retratado.

1.6 ESTRUTURA DO TRABALHO

A estrutura deste trabalho será composta das seguintes partes:

- **Capítulo 1 – Introdução:** Neste capítulo é contextualizada a área de estudo e apresentará os objetivos, justificativas, motivação, perspectivas de contribuição e metodologia de pesquisa para o desenvolvimento deste trabalho.
- **Capítulo 2 – Perícia Forense Computacional:** Neste capítulo, introduz-se os conceitos fundamentais sobre a perícia forense computacional, seus desafios com a computação em nuvem, assim como a coleta e análise de técnicas utilizadas pelos profissionais.
- **Capítulo 3 – Computação em Nuvem:** Neste capítulo, é apresentada a computação em nuvem, analisando seus conceitos e aplicações, juntamente com softwares para a coleta e análise de evidências em nuvem.
- **Capítulo 4 - Proposta de trabalho:** Neste capítulo, é realizado um estudo de caso, envolvendo a computação forense e a computação em nuvem.
- **Capítulo 5 – Conclusão:** Neste capítulo, apresentam-se as conclusões obtidas no trabalho.
- **Referências**

2. PERÍCIA FORENSE COMPUTACIONAL

Esta sessão tem como objetivo, apresentar conceitos, técnicas de extração e investigação de evidências utilizadas pela polícia forense computacional.

2.1 CONCEITO

> A Computação Forense é a ciência que, através de técnicas e habilidades especializadas, trata da coleta, preservação e análise de dados eletrônicos em um incidente computacional ou que envolvam a computação como meio de praticá-lo. (ELEUTÉRIO E MACHADO, 2011, p. 31).

Com o exponencial aumento de dispositivos conectados surgindo pelo mundo, a perícia forense se torna cada vez mais necessária, já que a medida com que mais pessoas se conectam, mais crimes surgem no mundo virtual.

O cenário atual aponta que cerca de 77 mil brasileiros sofrem ataques cibernéticos por dia e, provavelmente por falta de educação tecnológica ou conhecimentos de Computação Forense, apenas 21% deles denunciam o ataque (FRANCO; VILAR; GUSMÃO; GROCHOCKI, 2016, p. 3).

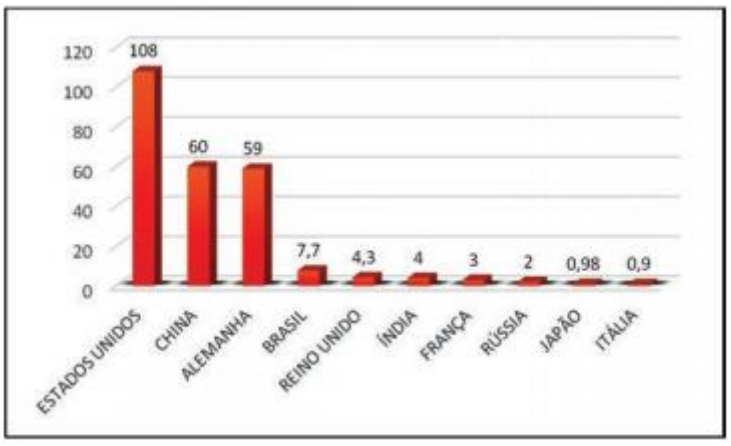

Figura 1: Custo dos crimes virtuais no mundo em 2016, em bilhões de dólares.
Fonte: FRANCO; VILAR; GUSMÃO; GROCHOCKI (2016, p. 3).

> A forense computacional surge como um elemento facilitador na limitação da perpetração desses crimes, podendo ser definida como uma ciência

> multidisciplinar que visa à preservação, identificação, análise e apresentação de evidências digitais de maneira científica e legalmente válida, permitindo a reconstrução de eventos passados e colaborando na investigação de crimes, comportamentos ilegais ou inapropriados cometidos em meio virtual, principalmente na internet (PALMER, 2001 apud DIDONÉ, 2011 p. 21).

2.2 ETAPAS DE UMA INVESTIGAÇÃO FORENSE

A perícia forense computacional possui quatro procedimentos básicos para realizar uma investigação: as evidências devem ser coletadas, examinadas, analisadas e seus resultados devem ser apresentados.

Essas etapas são a base para uma investigação em um crime cibernético, que muitas vezes não são evidências físicas, mas virtuais (hospedadas em algum serviço em nuvem).

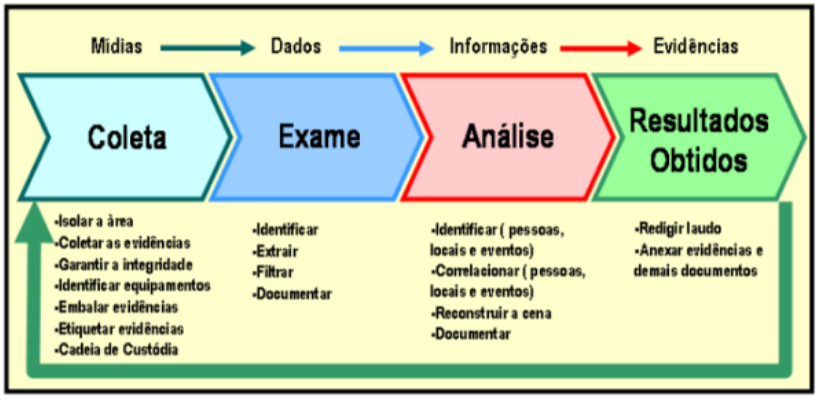

Figura 2: Ciclo da Investigação Computacional Forense

Fonte: MARTINS (2016).

2.2.1 COLETA

Nessa etapa o perito deve realizar a coleta das evidências, tomando cuidados para não comprometer a integridade da mesma, ou seja, nenhuma informação jamais poderá sofrer qualquer alteração ou modificação, permanecendo da mesma maneira como se encontrava no local em que foi retirada. A coleta da evidência deve ser realizada de forma extremamente cuidadosa, para não a comprometer, tendo em vista que, caso ela seja

alterada, isso pode influenciar com o resto da investigação, tal como na decisão das autoridades judiciais.

> O processo de identificação, processamento e documentação de possíveis provas, ocorre no primeiro passo de uma investigação criminal, ou seja, durante o processo de coleta de evidências, sendo esta, considerada a mais vital das etapas da investigação. Ao extrair o material de análise é necessário que se tome todos os cuidados possíveis para que não haja perda ou alteração de dados, pois isso trará prejuízos para todos os outros passos do processo, especialmente investigações que tiverem fins judiciais (NEUKAMP, 2007, p. 26).

2.2.2 EXAME

A fase de exame é a mais trabalhosa, já que a examinação da evidência deve ser cautelosa, sendo uma boa prática realizar uma cópia dos vestígios para caso algo não saia como planejado, fazendo assim com que nada seja comprometido.

Esta etapa é de extrema importância para o resto da investigação, pois os resultados serão todos provenientes do exame, a incúria ao realizar essa etapa pode comprometer toda a investigação, levando a uma decisão judicial diferente do que seria se o exame tivesse sido realizado da maneira correta.

> O ato de extrair, localizar e filtrar somente as informações que possam contribuir, de forma positiva, em uma investigação ocorre na segunda etapa, denominada “exame de evidências”. Considera-se esta, a etapa mais trabalhosa do processo de investigação criminal, principalmente pela quantidade de diferentes tipos de arquivos existentes (áudio, vídeo, imagem, arquivos criptografados, compactados, etc.) que facilitam o uso de esteganografia, o que exige que o perito esteja ainda mais atento e apto a identificar e recuperar esses dados (FARMER; VENEMA, 2007, p.41).

Segundo Eleutério e Machado (2010, p. 62-63) pode-se dividir os dados de um disco rígido em camadas, fazendo com que a exploração se torne mais difícil, à medida que se conhece as partes mais profundas. A parte mais conhecida pelos usuários é aquela em que os arquivos podem ser visualizados através do Windows Explorer, por exemplo. A camada mais profunda é aquela sem que se encontram os arquivos temporários, ocultos, excluídos e que necessitam de um complexo processo para serem acessados, como arquivos criptografados.

2.2.3 ANÁLISE

De acordo com Damacena (2014, p. 29 apud Queiroz e Vargas, 2010) a análise tem como objetivo examinar as informações coletadas em busca de evidências, para que no final do processo possa ser formulada a conclusão referente ao crime que originou a investigação. Na análise deve ser investigado todas as fontes de informação, para que seja possível identificar práticas criminosas por parte do suspeito ou suspeitos.

Essa é uma das fases mais demoradas, onde o perito utilizada técnicas e ferramentas para analisar as evidências coletadas, que nem sempre são explicitas, já que podem ser arquivos criptografados.

Nessa etapa deve ser feita uma reconstrução da cena, a fim de responder algumas perguntas que podem levar a solução do caso: como foi feito, quando foi feto, onde foi feito e o que foi feito.

A análise pode ser dividida em duas fases: física e lógica. A física consiste na análise dos dados brutos.

> Segundo Freitas (2003, p. 8), os dados podem ser analisados por três processos principais: uma pesquisa de sequência, um processo de busca e extração e uma extração de espaço subaproveitado e livre de arquivos. Na análise lógica, é analisado os arquivos das partições, utilizando um sistema operacional que consiga entender o sistema de arquivos da partição que está sendo investigada.

2.2.4 RESULTADOS

Nessa última etapa é apresentado o laudo pericial, que é uma documentação de como foi realizada a investigação, ele deve conter tudo sobre as outras etapas, de uma maneira que seja de fácil entendimento. Não existe um modelo padrão de laudo, o perito é livre para confeccionar o documento da maneira como quiser.

> O laudo pericial é o relato do perito após análise e correlação das evidências, resultado de um processo de avaliação. Consiste na tradução das informações captadas pelo perito por meio de conhecimentos especializados e deve estar pautado em aspectos éticos e legais,

> apresentando os resultados obtidos pela investigação de forma clara, organizada, concisa, imparcial e conclusiva (DAMACENA, 2014, p. 29).

2.3 TÉCNICAS ANTI-FORENSE

Existem algumas técnicas utilizadas para não deixar qualquer tipo de rastro ou evidência em mídias físicas, fazendo assim com que uma busca fique mais complicada ou até mesmo impossível. Essas técnicas podem ser utilizadas para esconder dados ou até para apagar dados de uma maneira com que não seja possível recuperar.

2.3.1 ROOTKITS

> Um rootkit é um conjunto de programas utilizados para impedir a detecção de atividades maliciosas no sistema, como a presença de usuários não autorizados. Costumam ser usados por invasores de sistemas para manterem acesso após um ataque bem sucedido, sem que precisem subverter o sistema novamente. (ROSANES, 2011, p. 2).

Esse é um dos *softwares* mais utilizados para não ser detectado ao invadir uma máquina, a palavra *"root*" é utilizada para denominar o acesso de super usuário em um sistema operacional, juntando com a palavra *"kit"*, temos o *kit* do super usuário.

> O rootkit intercepta os dados que são requisitados e faz uma filtragem dessa informação quando algum sistema operacional efetua um pedido de leitura de um arquivo, deixando o sistema ler apenas os arquivos que não estão infectados. Por isso, o antivírus instalado na máquina ou outra ferramenta de segurança do computador não consegue detectar alguma ameaça ou arquivo malicioso (CANALTECH, [2017?]).

2.3.2 MÉTODO GUTMANN

Ao apagar um arquivo do computador, ele não é completamente excluído, fazendo assim com que alguém com maior conhecimento consiga recuperá-lo com certa facilidade. Para isso foi desenvolvida uma técnica por Peter Gutmann, em 1996, que deleta completamente o arquivo da memória de um disco magnético. A técnica consiste em um algoritmo de 35 passos de sobrescrita de disco para a exclusão de dados permanentemente.

O apagador de disco básico pode ser aprimorado um pouco adicionando passes aleatórios antes e depois do processo de apagamento e executando os passes determinísticos em ordem aleatória para tornar mais difícil adivinhar quais dos passes de dados conhecidos foram feitos naquele momento. Para lidar com tudo isso no processo de substituição, usamos a sequência de 35 gravações consecutivas (GUTMANN, 1996).

Overwrite Data				
Pass No.	**Data Written**	**Encoding Scheme Targeted**		
1	Random			
2	Random			
3	Random			
4	Random			
5	01010101 01010101 01010101 0x55	(1,7) RLL		MFM
6	10101010 10101010 10101010 0xAA	(1,7) RLL		MFM
7	10010010 01001001 00100100 0x92 0x49 0x24		(2,7) RLL	MFM
8	01001001 00100100 10010010 0x49 0x24 0x92		(2,7) RLL	MFM
9	00100100 10010010 01001001 0x24 0x92 0x49		(2,7) RLL	MFM
10	00000000 00000000 00000000 0x00	(1,7) RLL	(2,7) RLL	
11	00010001 00010001 00010001 0x11	(1,7) RLL		
12	00100010 00100010 00100010 0x22	(1,7) RLL		
13	00110011 00110011 00110011 0x33	(1,7) RLL	(2,7) RLL	
14	01000100 01000100 01000100 0x44	(1,7) RLL		
15	01010101 01010101 01010101 0x55	(1,7) RLL		MFM
16	01100110 01100110 01100110 0x66	(1,7) RLL	(2,7) RLL	
17	01110111 01110111 01110111 0x77	(1,7) RLL		
18	10001000 10001000 10001000 0x88	(1,7) RLL		
19	10011001 10011001 10011001 0x99	(1,7) RLL	(2,7) RLL	
20	10101010 10101010 10101010 0xAA	(1,7) RLL		MFM
21	10111011 10111011 10111011 0xBB	(1,7) RLL		
22	11001100 11001100 11001100 0xCC	(1,7) RLL	(2,7) RLL	
23	11011101 11011101 11011101 0xDD	(1,7) RLL		
24	11101110 11101110 11101110 0xEE	(1,7) RLL		
25	11111111 11111111 11111111 0xFF	(1,7) RLL	(2,7) RLL	
26	10010010 01001001 00100100 0x92 0x49 0x24		(2,7) RLL	MFM
27	01001001 00100100 10010010 0x49 0x24 0x92		(2,7) RLL	MFM
28	00100100 10010010 01001001 0x24 0x92 0x49		(2,7) RLL	MFM
29	01101101 10110110 11011011 0x6D 0xB6 0xDB		(2,7) RLL	
30	10110110 11011011 01101101 0xB6 0xDB 0x6D		(2,7) RLL	
31	11011011 01101101 10110110 0xDB 0x6D 0xB6		(2,7) RLL	
32	Random			
33	Random			
34	Random			
35	Random			

Figura 3: Os 35 passos do algoritmo de Gutmann

Fonte: GUTMANN (1996).

2.3.3 ESTEGANOGRAFIA

“Esteganografia é uma técnica que consiste em esconder um arquivo dentro do outro, de forma criptografada” (FIZMAN, 2015).

Através desse método anti-forense é possível esconder informações e arquivos dentro de imagens, de maneira com que a imagem permaneça igual a original, sendo necessária a utilização de um *software* para visualizar o conteúdo oculto.

As mensagens escondidas pela esteganografia possuem um tamanho limitado, determinado pelo meio que é utilizado. Existem diversos aplicativos que realizam essa técnica, tal como o JP Hide and Seek.

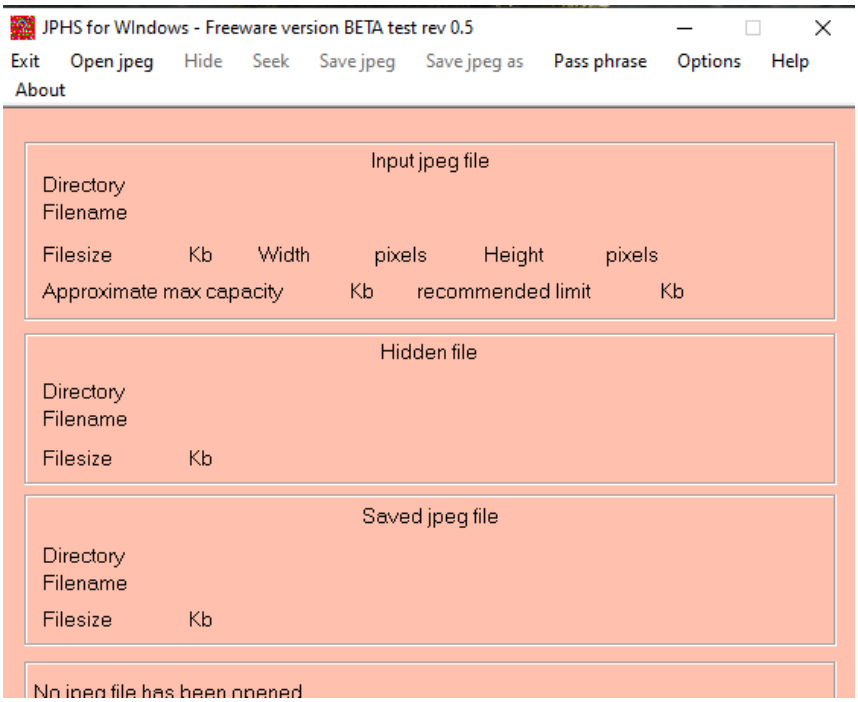

Figura 4: Interface do programa JP Hide and Seek

Fonte: O autor.

A técnica de esteganografia mais utilizada é a LSB (*Least Significant Bit*) que consiste em obter a representação binária da imagem e sobrescrever os bits menos significativos de cada *byte* da imagem escolhida. O programa retratado na figura 4 utiliza essa técnica.

2.4 FERRAMENTAS FORENSES

Para auxiliar nas investigações, os peritos possuem ferramentas, que na maioria das vezes são *softwares*. Existem também sistemas operacionais, como o Kali Linux, que possuem ferramentas específicas para a perícia forense computacional.

De acordo com Eleutério e Machado (2011) há várias ferramentas criadas para Perícia Computacional, que são específicas de acordo com a fase em que a investigação se encontra.

2.4.1 FORENSIC TOOLKIT (FTK)

Criado pela empresa AcessData, o FTK é uma das ferramentas mais usadas no mundo na perícia forense. O *software* escaneia o HD, localizando uma série de informações, como e-mails e arquivos apagados, podendo também tentar adivinhar senhas com base no conteúdo encontrado no disco rígido.

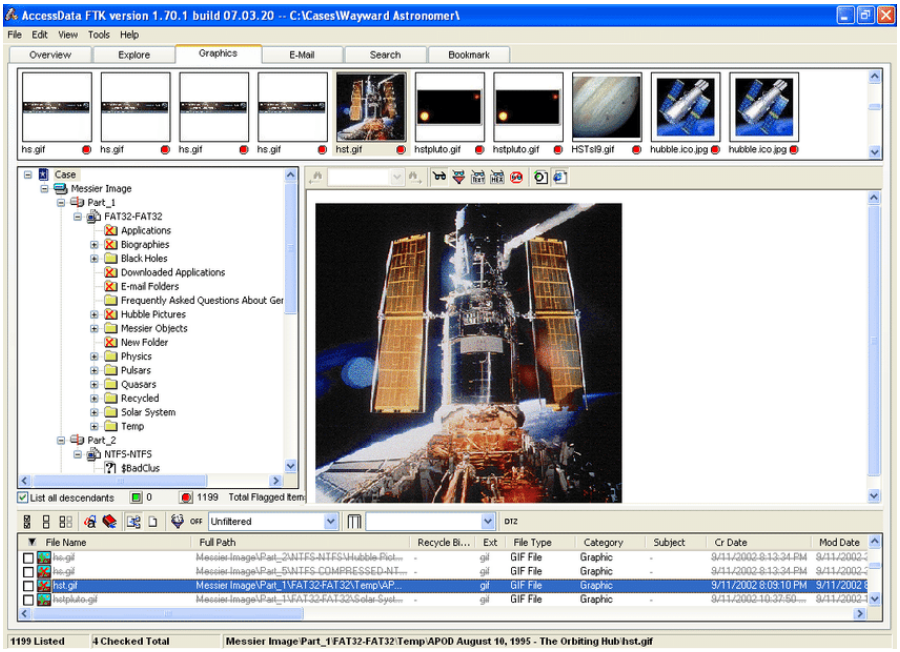

Figura 5: Interface do programa Forensic Toolkit

Fonte: SCANLON (2009, p. 22).

2.4.2 ENCASE

O software foi desenvolvido pela empresa Opentext e funciona de maneira semelhante ao Forensic Toolkit, analisando o disco rígido e procurando por arquivos deletados, sejam eles de qualquer formato ou tamanho.

> O EnCase Forensic produz uma cópia binária exata da unidade de disco ou da mídia original, depois a verifica gerando valores de hash MD5 para os arquivos de imagem relacionados e atribuindo valores de CRC aos dados. Essas verificações e balanços revelam quando provas foram falsificadas ou alteradas, mantendo todas as provas digitais legalmente válidas para os processos judiciais (ONDATA, 2009, p. 1).

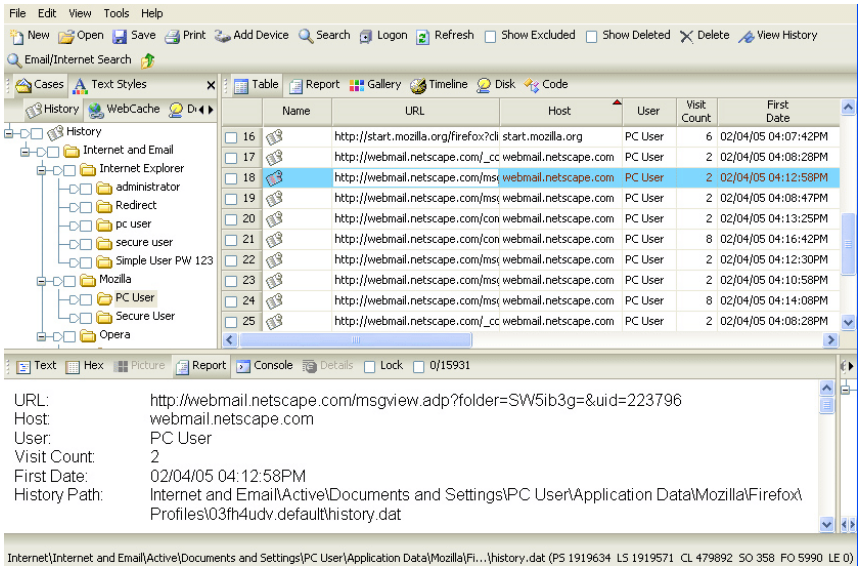

Figura 6: Interface do programa EnCase

Fonte: SCANLON (2009, p. 20).

2.4.3 THE CORONER'S TOOLKIT

Desenvolvido por Wietse Venema e Dan Farmer em 2000, o *software* consiste em vários utilitários para a perícia forense, tal como: *grave-robber*, *mactime* e *lazarus*.

O comando *grave-robber* automatiza a coleta de evidências, gera assinaturas criptográficas, lista de arquivos apagados que ainda estão em uso e históricos de *shell*, tudo de acordo com a ordem e volatilidade.

O *mactime* cria um histórico de arquivos acessados e apagados, de acordo com os dados fornecidos pelo *grave-robber*.

Por fim, o *lazarus* consegue recuperar arquivos que foram apagados, assim como o FTK e o EnCase.

2.5 INVESTIGAÇÕES EM AMBIENTES NUVEM

Com o crescimento da utilização de meios online para armazenamento de arquivos crescendo cada dia mais, chegou-se ao mais recente desafio da polícia forense computacional, a investigação em ambientes nuvem.

> “A computação em nuvem contribui para tornar mais complexa a análise usando a metodologia tradicional de informática forense, pois introduz variáveis inerentes as suas características, modelos e arquitetura”. (MARINS, 2009, p. 3).

No capítulo 3, será retratado o processo de coleta e análise de evidências localizadas em servidores na nuvem.

3. COMPUTAÇÃO EM NUVEM

Nesse capítulo é apresentado o conceito de computação em nuvem, seus modelos de serviços e provedores mais utilizados atualmente.

Figura 7: Dispositivos conectados a nuvem

Fonte: https://www.estudopratico.com.br/wp-content/uploads/2015/10/o-que-e-computacao-em-nuvem-1200x675.jpg

3.1 CONCEITO

> A computação na nuvem ou *Cloud Computing* é um novo modelo de computação que permite ao usuário final acessar uma grande quantidade de aplicações e serviços em qualquer lugar e independente da plataforma, bastando para isso ter um terminal conectado à “nuvem” (PEDROSA e NOGUEIRA, p. 1).

Podemos definir a nuvem como um disco rígido virtual, onde o usuário pode armazenar a informação que quiser e acessar de qualquer lugar, desde que possua acesso à internet.

> A palavra nuvem sugere uma ideia de ambiente desconhecido, o qual podemos ver somente seu início e fim. Por este motivo esta foi muito bem empregada na nomenclatura deste novo modelo, onde toda a infraestrutura e recursos computacionais ficam “escondidos”, tendo o usuário o acesso apenas a uma interface padrão através da qual é disponibilizado todo o conjunto de variadas aplicações e serviços (PEDROSA e NOGUEIRA, p. 1).

3.2 CARACTERÍSTICAS

3.2.1 ELASTICIDADE

Uma das características da nuvem é a elasticidade, já que mais recursos podem ser adicionados a nuvem a qualquer momento, como mais capacidade de armazenamento, tornando a nuvem algo elástico, que pode ser estendido quando for necessário. Através dessa elasticidade, os usuários tem a impressão de que a nuvem é algo infinito, com recursos ilimitados.

Recursos podem ser adquiridos de forma rápida e elástica, em alguns casos automaticamente, caso haja a necessidade de escalar com o aumento da demanda, e liberados, na retração dessa demanda. (RUSCHEL; ZANOTTO; MOTA, 2008, p. 6).

3.2.2 AUTO-ATENDIMENTO

O usuário pode adquirir unilateralmente recurso computacional, como tempo de processamento no servidor ou armazenamento na rede na medida em que necessite e sem precisar de interação humana com os provedores de cada serviço (RUSCHEL; ZANOTTO; MOTA, 2008, p. 5).

> A computação em nuvem é um sistema autônomo gerenciado de forma transparente para os usuários. Hardware e software dentro de nuvens podem ser automaticamente reconfigurados, orquestrados e estas modificações são apresentadas ao usuário como uma imagem única. Essa autonomia é importante, pois reduz o custo de equipe de monitoramento do sistema tanto no âmbito centralizado quanto distribuído (BIRMAN ET al. 2009 apud DAMACENA, 2014, p. 50).

3.2.3 ACESSIBILIDADE

Todas as informações estão disponíveis em diversas plataformas para o usuário acessar a qualquer momento, dando a nuvem um amplo acesso à rede.

> A interface de acesso a nuvem não obriga os usuários a mudarem suas condições e ambientes de trabalho, como por exemplo, linguagens de programação e sistema operacional. Já os softwares clientes instalados localmente para o acesso à nuvem são leves, como um navegador de Internet (RUSCHEL; ZANOTTO; MOTA, 2008, p.5).

3.3 MODELOS DE SERVIÇO

A computação em nuvem é dividida em serviços. Existem três tipos de serviços: Infraestrutura como serviço (IaaS), Plataforma como serviço (PaaS) e *Software* como serviço (SaaS).

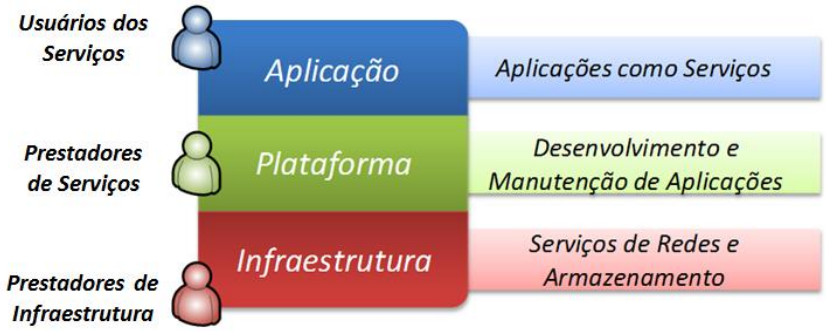

Figura 8: Divisão de serviços da nuvem

Fonte: CHIRIGATI (2009).

3.3.1 INFRAESTRUTURA COMO SERVIÇO (IAAS)

A infraestrutura como serviço (*Infrastructure as a Service*) é referente a camada em nuvem responsável pelos servidores, *data centers* e *hardware*, garantindo o funcionamento das duas outras camadas. Basicamente, a IaaS é responsável por providenciar toda a infraestrutura para as outras duas camadas.

O IaaS é baseado em técnicas de virtualização de recursos de computação. Observando do lado da economia, não será necessário a aquisição de novos servidores e equipamento de rede para a ampliação de serviços (RUSCHEL; ZANOTTO; MOTA, 2008, p. 8).

3.3.2 PLATAFORMA COMO SERVIÇO (PAAS)

A plataforma como serviço (*Platform as a Service*) é a camada de *software*, onde as aplicações podem ser desenvolvidas. O intuito dessa camada é facilitar o desenvolvimento de aplicações para usuários finais.

> Esse modelo fornece a seus clientes um ambiente completo composto por todos os recursos necessários para o desenvolvimento de software em uma ou mais linguagens de programação tais como compiladores, depuradores, bibliotecas e um sistema operacional (CARISSIMI, 2015, p. 8).

Alguns exemplos da camada IaaS, como o Microsoft Azure e Amazon EC2.

3.3.3 *SOFTWARE* COMO SERVIÇO (SAAS)

O *software* como serviço (*Software as a Service*) consiste na aplicação já operacional para o usuário final. Não é necessário configuração nem manutenção, ela já está pronta para o uso. Pode-se considerar que essa é a camada de mais alto nível da nuvem. Já que representa as aplicações em sua versão final.

Segundo Chirigati (2009) o SaaS é disponibilizado por prestadores de serviços na camada de aplicação. Ele roda inteiramente na nuvem e pode ser considerado uma alternativa a rodar um programa em uma máquina local.

Alguns exemplos dessa camada são: Google Drive, MEGA, Gmail e Hotmail.

3.4 MODELOS DE IMPLEMENTAÇÃO

Pode-se separar a nuvem em modelos de implementação, além de seus modelos de serviço. Uma nuvem pode ser classificada como pública, privada, híbrida e comunitária.

Figura 9: Divisão de implementação da nuvem

Fonte: BARDI (2017, p. 5)

3.4.1 PÚBLICA

Segundo o site da RedHat a nuvem pública foi desenvolvida com base em *hardware* e gerenciada por uma empresa terceirizada, a nuvem pública é um *pool* de recursos virtuais que é provisionado e alocado automaticamente entre vários clientes por meio de uma interface de autosserviço. Pode-se definir as nuvens públicas como serviços executados por terceiros, onde os dados de usuários ficam juntos no servidor de armazenamento. A nuvem pública é disponibilizada para todo público, podendo ser acessada por qualquer um que conheça a localização do serviço.

> As nuvens públicas tentam fornecer aos consumidores elementos de TI sem problemas. Seja software, infraestrutura de aplicativo ou infraestrutura física, o provedor de nuvem assume as responsabilidades de instalação, gerenciamento, fornecimento e manutenção (AMRHEIN, 2009 apud DAMACENA, 2014, p. 64).

3.4.2 PRIVADA

Segundo o site da Microsoft Azure uma nuvem privada consiste em recursos de computação usados exclusivamente por uma única empresa ou organização. A nuvem privada pode estar localizada fisicamente no data center local da sua organização ou pode ser hospedada por um provedor de serviços terceirizado. Podemos dizer que as nuvens privadas são um tipo de armazenamento online usado exclusivamente para uma pessoa ou empresa, onde esse usuário possui total controle das aplicações implementadas nela. Normalmente, fica localizada em um data center privado.

> Para esse modelo de implantação são empregados políticas de acesso aos serviços. Gerenciamento de redes, configurações dos provedores de serviços e a utilização de tecnologias de autenticação e autorização são as

> principais características deste modelo (RUSCHEL; ZANOTTO; MOTA, 2008, p. 9).

3.4.3 HÍBRIDA

As nuvens híbridas podem ser caracterizadas como uma combinação das nuvens privadas com as nuvens públicas, combinando o melhor de dois mundos. Nesse tipo de implementação, os dados podem ser movidos entre a nuvem pública e privada, de acordo com a necessidade do momento, garantindo uma maior flexibilidade.

> Essa característica possui a vantagem de manter os níveis de serviço mesmo que haja flutuações rápidas na necessidade dos recursos. A conexão entre as nuvens pública e privada pode ser usada até mesmo em tarefas periódicas que são mais facilmente implementadas nas nuvens públicas, por exemplo (CHIRIGATI, 2009).

3.4.4 COMUNITÁRIA

As nuvens comunitárias são compartilhadas por várias organizações, como ministérios e autarquias.

> No modelo de implantação de nuvem comunidade ocorre o compartilhamento por diversas empresas de uma nuvem, sendo esta suportada por uma comunidade específica que partilha interesses, tais como a missão, os requisitos de segurança, política e considerações sobre flexibilidade. Este tipo de modelo de implantação pode existir localmente ou remotamente e geralmente é administrado por alguma empresa da comunidade ou por terceiros (SOUSA, 2011 apud DAMACENA, 2014, p. 68).

3.5 COMPUTAÇÃO FORENSE EM NUVEM

Aqui será estudado como é feita a coleta e análise de evidência em ambientes nuvem, apontando os principais desafios da investigação nesse mundo virtual.

3.5.1 INTRODUÇÃO

> Nos casos de investigações criminais em ambientes tradicionais, é prática comum que a perícia computacional desligue o equipamento e realize uma cópia dos discos que será analisada posteriormente em laboratório. Isso é inviável num ambiente de computação em nuvem, tendo em vista a grande capacidade de armazenamento, questões jurídicas, distribuição geográfica e controle dos dados, que podem variar conforme o modelo de serviço contratado. Além disso, a falta de acesso físico para a coleta dos dados e a falta de controle sobre o sistema tornam a aquisição das informações uma tarefa desafiadora para a perícia em nuvem (SOUZA, 2018).

Com o crescente aumento da utilização de serviços em nuvem, a computação forense passa a ter um novo desafio: como coletar e analisar evidências onde não há meios físicos acessíveis? Para responder tal pergunta, vamos analisar softwares tais como UFED Cloud Analyser e Forensics Openstacks Tools.

3.5.2 ACESSO AOS DADOS

Quando o acesso aos dados não é obtido de forma voluntária, os peritos precisam realizar um processo de liberação aos mesmos, através de uma comunicação com o provedor, que muitas vezes pode demorar de três semanas a três meses, no caso dos Estados Unidos. Em alguns casos a liberação pode até não ocorrer, fazendo com que o andamento da investigação pare de vez (TECHBIZ, 2015).

3.5.3 UFED CLOUD ANALYSER

O *software* desenvolvido pela empresa israelense Cellebrite permite a extração de informações em nuvem, analisando e-mails, mensagens do Facebook, Twitter, Google Drive, calendário da Google, histórico de localização, senhas e fotos. O aplicativo coleta todos os dados de uma determinada conta, independente de onde ela esteja conectada, seja em um dispositivo móvel ou *desktop*.

> Segundo pesquisa realizada nos últimos quatro anos pelo o IACP (*International Associationof Chiefs of Police*), em 2010 os dados coletados

nas nuvens contribuíram com menos de 50% dos casos (45,3%) investigados no mundo. Já em 2014 quase 80% (78,8%) dos crimes foram solucionados de alguma maneira com informações obtidas na nuvem. Um claro reflexo do crescente uso das mídias sociais pela população, que os acessa, em sua maioria, através de celulares. Dos 2,1 bilhões de usuários ativos de mídias sociais em todo o mundo, 80% acessam esses dados via dispositivos móveis, segundo dados de janeiro de 2015 da Wearesocial. E os criminosos também fazem parte dessas estatísticas (TECHBIZ, 2015).

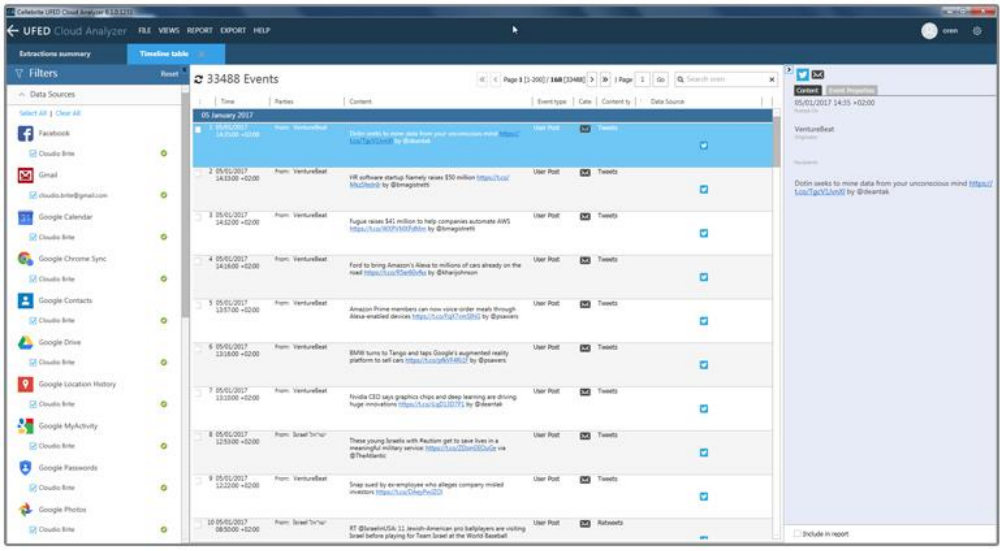

Figura 10: Interface do programa UFED Cloud Analyser
Fonte: https://cf-media.cellebrite.com/wp-content/uploads/2017/06/4.2.2_CloudAnalyzer_screen02.jpg

Ao conectar uma conta no aplicativo, o mesmo coleta os dados disponíveis em nuvem, resultando em uma listagem, onde é possível visualizar mensagens, e-mails, localizações, fotos e postagens em redes sociais de forma clara e bem organizada, fazendo assim com que o perito não precise ter o trabalho de organizar as evidências coletadas.

3.5.4 FORENSIC OPENSTACK TOOLS (FROST)

A OpenStack é uma plataforma de computação em nuvem de código aberto, que foi desenvolvida pela NASA juntamente com a empresa Rackspace em 2010 e projetada como

ambiente IaaS. Essa plataforma possui mais de 600000 linhas de código e 415 desenvolvedores ativos e é muito utilizada como uma nuvem privada por grandes empresas, como Intel, Argonne National Laboratory, AT&T, Rackspace e Deutsche Telekom (DYKSTRA, 2013).

De acordo com Dykstra (2013) o FROST fornece os primeiros recursos forenses integrados ao OpenStack, os quais são os primeiros a serem incorporados a qualquer plataforma em nuvem de Infraestrutura como Serviço (IaaS).

Ele pode ser utilizado para recuperar logs do *firewall* e recuperação de discos virtuais.

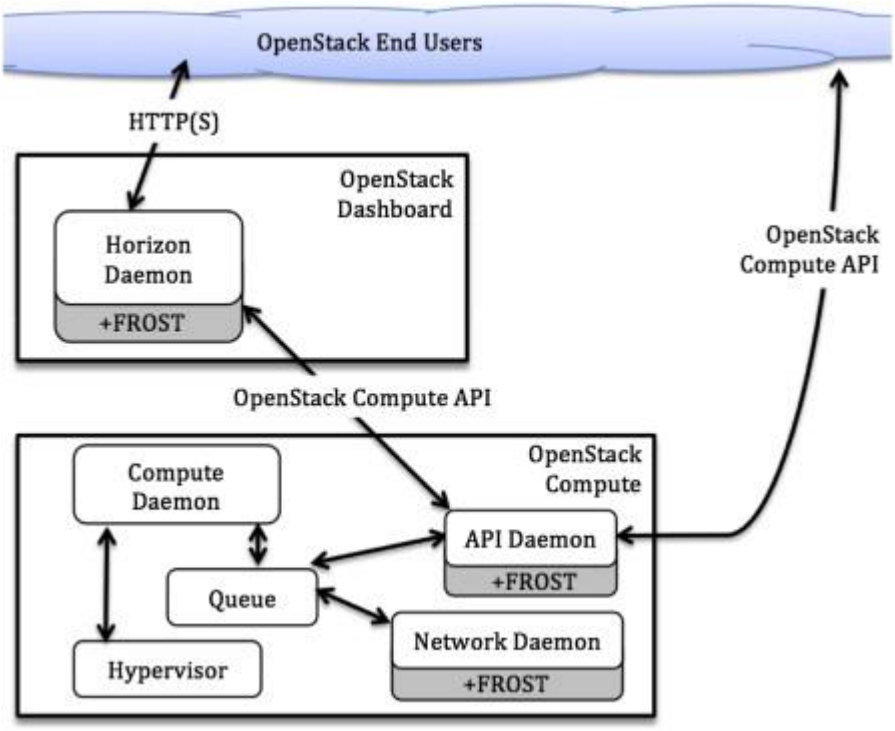

Figura 11: Design e implementação do FROST

Fonte: https://ars.els-cdn.com/content/image/1-s2.0-S174228761300056X-gr1.jpg

4. PROPOSTA DE TRABALHO

Esse estudo de caso explora a esteganálise em imagens que estão armazenados em ambientes nuvem (Google Drive, Dropbox e OneDrive) e estão esteganografadas, assim, revelando as mensagens escondidas nesses arquivos. Esse processo é algo muito comum no dia-a-dia de um perito forense computacional. Para realizar essa técnica será utilizado o programa JP Hide and Seek.

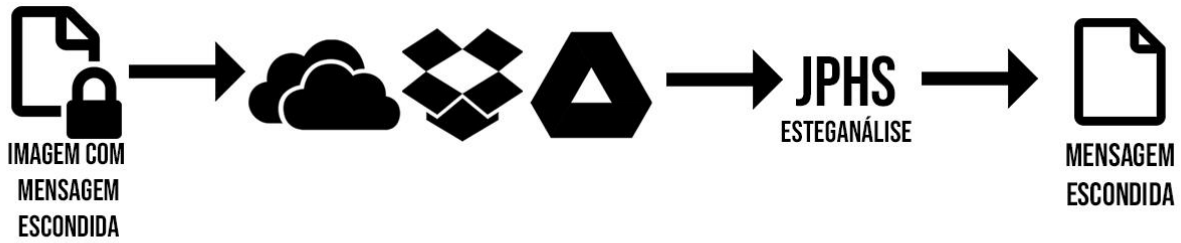

Figura 12: Cenário no qual será realizado o estudo de caso

Fonte: O autor.

4.1 FERRAMENTAS UTILIZADAS NO ESTUDO DE CASO

4.1.1 DROPBOX

O Dropbox é um serviço de hospedagem e compartilhamento de arquivos em nuvem, podendo ser utilizado em sua forma gratuita, onde é disponibilizado 2 GB de armazenamento para o usuário, ou em sua forma paga, podendo variar de US$ 9,99 a US$ 16,58 por mês para pessoas físicas, com armazenamento de 2TB até 3TB. Para esse estudo, será utilizada uma conta em sua versão gratuita.

4.1.2 ONE DRIVE

O OneDrive, assim como o Dropbox, é um serviço de armazenamento e compartilhamento de arquivos que funciona em nuvem, criado pela Microsoft em 1 de agosto de 2007, com o nome de Windows Live SkyDrive, que em 27 de janeiro de 2014 passou a ser chamado de OneDrive. O serviço disponibiliza, de forma gratuita, 5 GB para o usuário, possuindo planos pagos, que variam de R$ 9,00 a R$ 299,00 por mês, com armazenamento de 100 GB até 6 TB (SCRIPTBRASIL, 2014). Nesse estudo será utilizado um conta em sua versão gratuita.

4.1.3 GOOGLE DRIVE

O Google Drive, assim como o Dropbox e OneDrive, é um serviço de armazenamento e compartilhamento de arquivos em nuvem, sendo um dos mais populares por ser da gigante empresa Google. O serviço foi lançado em 24 de abril de 2012 e oferece, de forma gratuita, 15 GB para o usuário. A nuvem da Google também possui planos pagos, variando de R$ 6,99 a R$ 34,99 por mês, com armazenamento de 100 GB até 2TB. Para esse caso será utilizada um conta em sua versão gratuita.

4.1.4 JP HIDE AND SEEK

JP Hide and Seek é um software utilizado para realizar esteganografia e esteganálise em imagens comuns, no formato JPEG. O programa é de código aberto e possui versões para Windows e Linux.

> JPHIDE e JPSEEK distribuem o arquivo oculto na imagem jpeg para que os efeitos visuais e estatísticos sejam minimizados. O JPHS usa a substituição de bits menos significativos dos coeficientes discretos de transformação de cosseno usados pelo algoritmo jpeg. Programas simples que armazenam os dados ocultos em bits de baixa ordem podem resultar na imagem jpeg ser tão estatisticamente diferente do arquivo jpeg normal que o arquivo oculto pode ser recuperado facilmente (ATHABASCA UNIVERSITY, 2004, tradução do autor).

4.2 TÉCNICAS UTILIZADAS NO ESTUDO DE CASO

4.2.1 ESTEGANOGRAFIA

A esteganografia, como já abordado no capítulo 2.3.3 é uma técnica utilizada para esconder arquivos e mensagens em imagens JPEG, de maneira com que não altere o arquivo original. Para realização dessa técnica foi utilizado o software JP Hide and Seek.

4.2.2 ESTAGANÁLISE

A esteganálise é uma técnica para quebrar uma mensagem esteganografada, podendo exibir, alterar ou destruir a mensagem. Existem dois tipos de esteganálise: ativa e passiva. A primeira tem por objetivo extrair a mensagem escondida, sendo necessário conhecer o software utilizado para esteganografar a imagem, tal como descobrir a sua senha. A passiva tem como principal objetivo detectar a presença de uma mensagem oculta na imagem desejada. Para esse estudo foi utilizado o método ativo, através do software JP Hide and Seek e sem a utilização de senhas.

4.3 METODOLOGIA

Para realizar esse estudo de caso, foi utilizado como metodologia os padrões da SWGDE (*Scientific Working Group on Digital Evidence*) que é o grupo de trabalho científico em evidência digital e consistem, basicamente, em que todas as organizações que trabalham com investigações forenses devem manter um nível de qualidade alto a fim de não comprometer a qualidade, confiabilidade e precisão das evidências através dos processos de coleta, exame, análise e resultados, como já abordado no capítulo 2.2. Utilizando essa metodologia, após as imagens serem esteganografadas através do software JP Hide and Seek e salvas nos serviços de armazenamento em nuvem escolhidos através de seus respectivos aplicativos na versão desktop, foi realizada a coleta das contas, através da identificação dos provedores, usuários e senhas utilizados. Para o processo de exame, foi realizado o download das evidências através do aplicativo na versão desktop dos provedores e criado um backup de todos os arquivos baixados. A análise foi realizada através da opção seek, do software JP Hide and Seek, a qual possibilita realizar a estaganálise das evidências coletadas. Após as etapas anteriores foi realizada a apresentação dos resultados obtidos nesse estudo de caso.

4.4 APLICAÇÃO DA METODOLOGIA

4.4.1 ESTEGANOGRAFIA DAS IMAGENS

Após selecionar 6 diferentes imagens, foi realizada a esteganografia, através do *software* JP Hide and Seek.

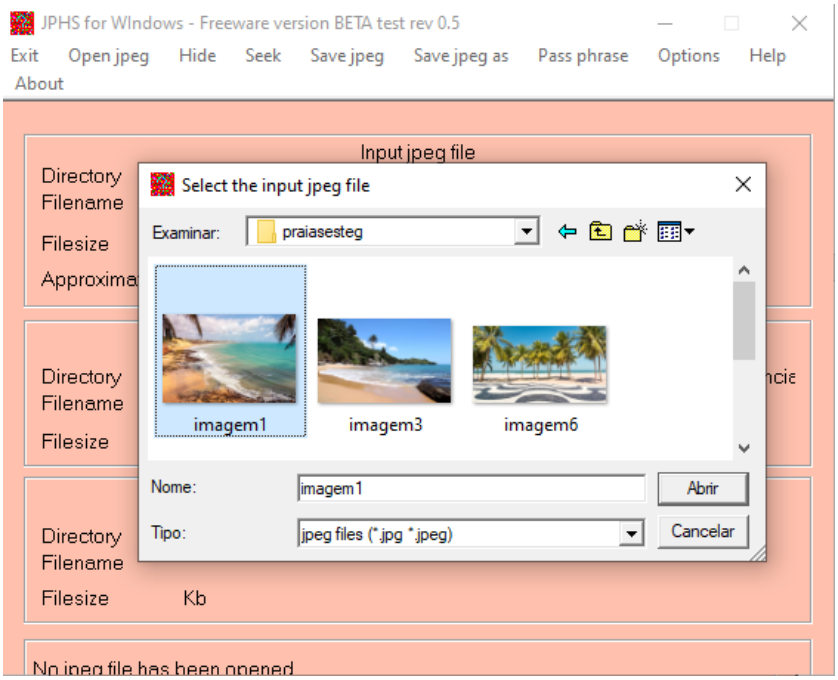

Figura 13: Escondendo um arquivo com o software JP Hide and Seek

Fonte: O autor.

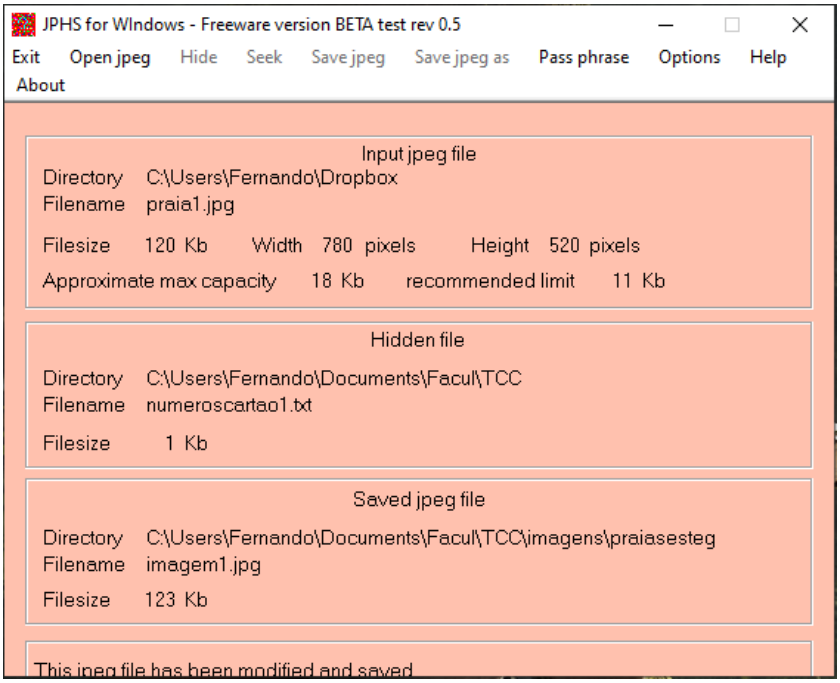

Figura 14: Imagem esteganografada e renomeada para imagem1.jpg

Fonte: O autor.

O mesmo procedimento foi realizado em outras imagens selecionadas para o estudo.

Figura 15: Imagem antes e depois do processo de esteganografia

Fonte: O autor.

Foi realizado o upload nas nuvens selecionadas para o estudo (Google Drive, Dropbox e OneDrive).

4.4.2 INVESTIGAÇÃO

4.4.2.1 COLETA

Após obter acesso as contas, foi constatado que haviam 6 imagens disponíveis em todos serviços em nuvem (OneDrive, Dropbox e Google Drive).

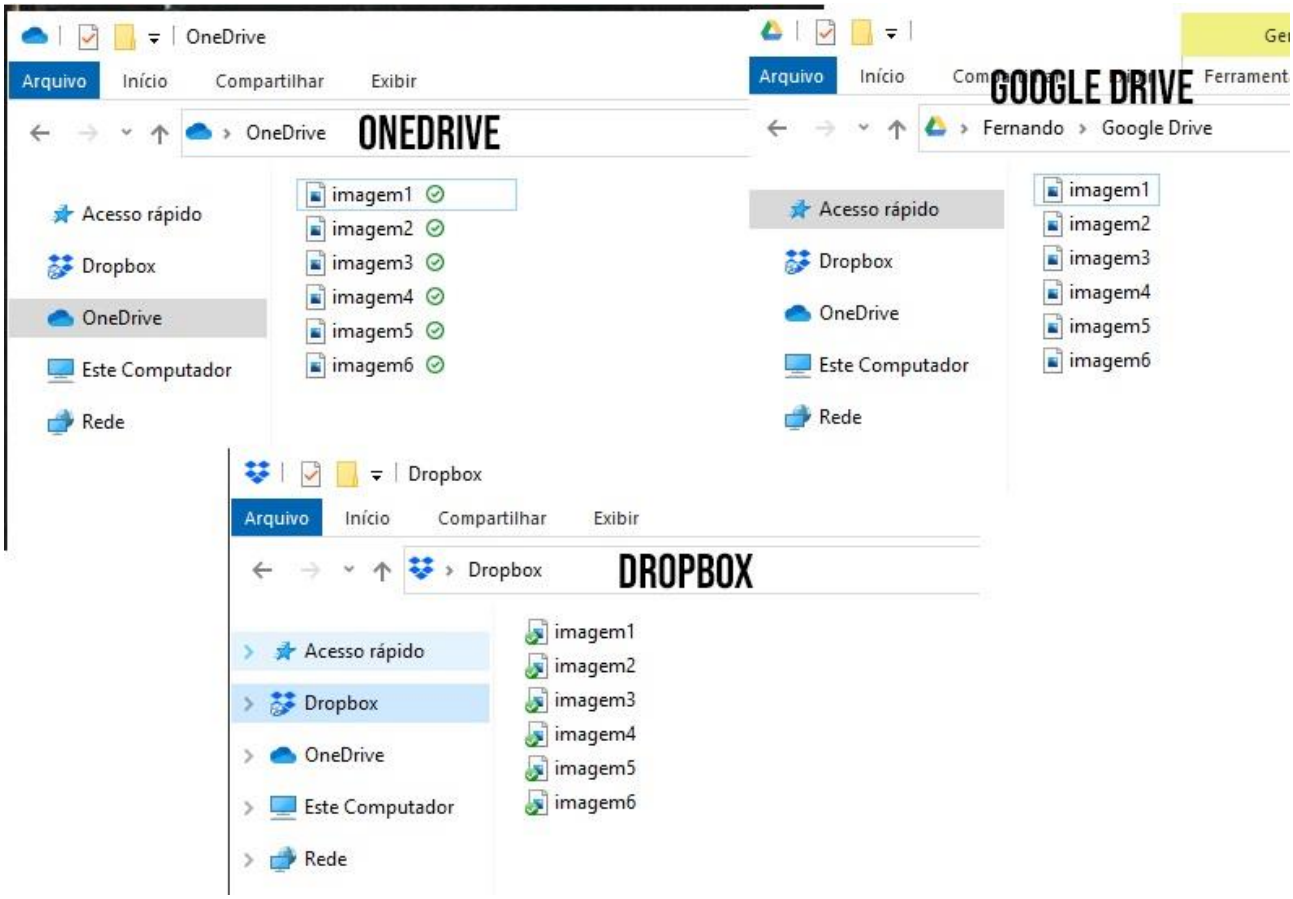

Figura 16: Imagens encontradas nas contas nuvem

Fonte: O autor.

4.4.2.2 EXAME

Ao iniciar o processo de exame foi realizado um *backup* das evidências coletadas, afim de manter a integridade dos arquivos caso algo não esperado ocorra durante o processo de

examinação. Utilizando o *software* JP Hide and Seek foi realizada a esteganálise de todas as imagens coletadas.

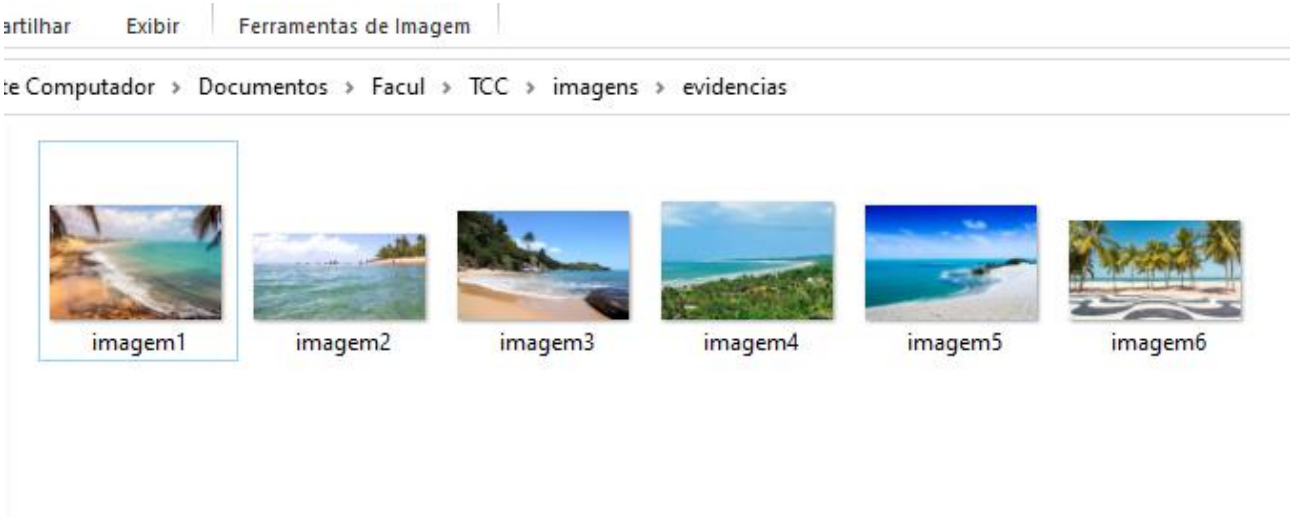

Figura 17: Backup das imagens encontradas em nuvem.

Fonte: O autor.

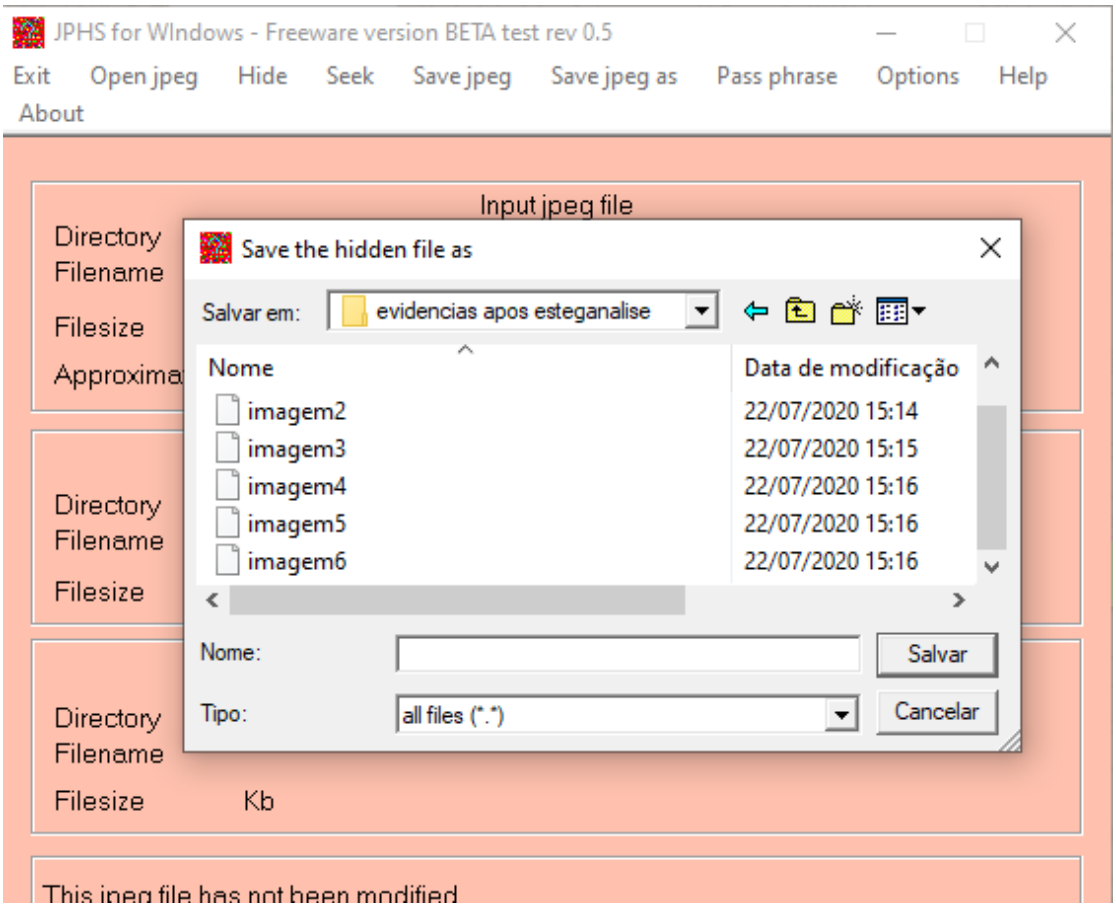

Figura 18: Processo de esteganálise

Fonte: O autor.

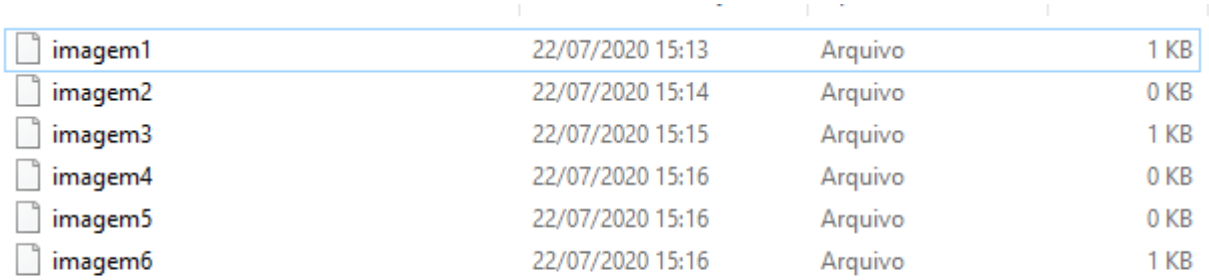

imagem1	22/07/2020 15:13	Arquivo	1 KB
imagem2	22/07/2020 15:14	Arquivo	0 KB
imagem3	22/07/2020 15:15	Arquivo	1 KB
imagem4	22/07/2020 15:16	Arquivo	0 KB
imagem5	22/07/2020 15:16	Arquivo	0 KB
imagem6	22/07/2020 15:16	Arquivo	1 KB

Figura 19: Arquivos criados pelo JP Hide and Seek após a esteganálise

Fonte: O autor.

4.4.2.3 ANÁLISE

Ao realizar a análise dos arquivos encontrados após a esteganálise foi possível constatar que 3 arquivos (imagem1, imagem3 e imagem6) possuíam o tamanho de 1 KB, levando a conclusão de que poderiam conter alguma mensagem extraída. Ao abrir esses arquivos usando um editor de texto, é possível visualizar que realmente existem mensagens que antes estavam escondidas, como pode ser visto na figura 20.

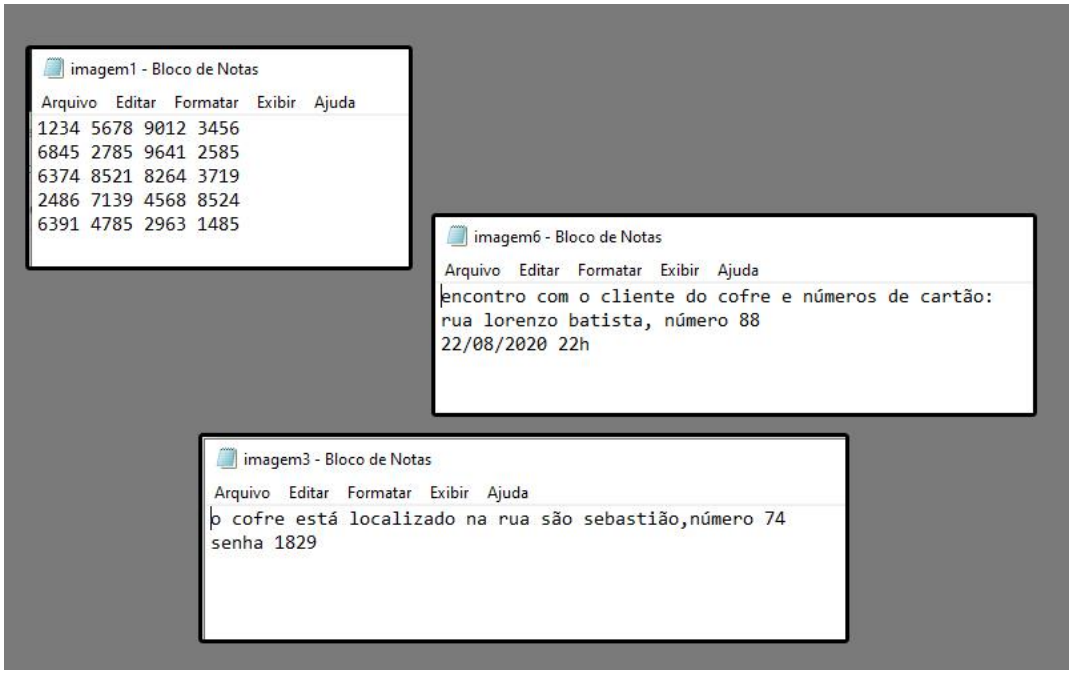

Figura 20: Evidências abertas com editor de texto

Fonte: O autor.

4.4.2.4 RESULTADOS OBTIDOS

Após realizar todas as etapas necessárias para a investigação foi possível constatar que as imagens encontradas no OneDrive, Google Drive e Dropbox estavam esteganografadas. Ao realizar a esteganálise foi possível verificar que apenas 3 das 6 imagens possuíam algum tipo de mensagem escondida. Ao abrir os arquivos utilizando um editor de texto foi possível visualizar que haviam números de cartão de crédito, um endereço que possivelmente irá levar a um cofre, juntamente com sua senha e um endereço com horário para um encontro com um cliente em potencial.

4.5 CONSIDERAÇÕES

Neste capítulo foi explicado o que pretendia ser realizado no estudo de caso, todas as técnicas e ferramentas utilizadas e aplicadas, e a utilização da metodologia, bem como os resultados obtidos.

Utilizando a metodologia estabelecida pela SWGDE o estudo foi realizado de forma com que todas as etapas fossem respeitadas, simulando uma perícia em ambiente de trabalho real de um profissional forense, utilizando técnicas e tecnologias semelhantes as usadas pelos mesmos.

Obter dados em um ambiente nuvem nem sempre é uma tarefa fácil, já que em muitos casos os provedores são localizados em outros países, fazendo com que exista um maior tempo de espera e que uma ordem judicial seja emitida, para poder ocorrer a quebra de sigilo de dados pelo provedor do serviço.

5. CONCLUSÃO

Tendo em vista o tema abordado no presente trabalho, a computação forense em nuvem tem tido aumento significativo nos últimos anos, sabendo que a utilização de serviços de armazenamento em nuvem vem crescendo cada vez mais.

A área de perícia forense ainda é muito pequena no Brasil e está em constante desenvolvimento, fazendo com que exista uma certa dificuldade em encontrar trabalhos relacionados a esse tema, isso aumenta ainda mais quando o assunto é perícia forense computacional. A perícia em nuvem é uma, se não a, área da perícia forense computacional mais nova, fazendo com que pesquisas relacionadas a esse tema em português sejam muito escassas. Existe uma facilidade muito maior em encontrar estudos e pesquisas em línguas estrangeiras, principalmente em inglês, idioma o qual possui o maior repositório.

Com o crescente aumento da utilização de ambientes de armazenamento em nuvem e a constante diminuição da mensalidade desses ambientes, a *cloud* vem se tornando, cada vez mais, o local escolhido por praticantes de crimes cibernéticos para armazenar seus dados, sejam pessoais ou coletados através de forma maliciosa, fazendo com seja mais difícil conduzir uma investigação para solucionar esse roubo de informações, já que não existe um meio físico onde esses dados são armazenados, aumentando o tempo de resolução e a dificuldade em solucionar crimes praticados no mundo virtual. Diversas ferramentas estão sendo desenvolvidas para auxiliar na velocidade da solução desses crimes cibernéticos, tal como o UFED Cloud Analyser e o Forensic OpenStack Tools, que tem a capacidade de extrair dados relevantes para investigações forense, com ou sem consentimento do indivíduo a ser investigado. A tendência é que, em um futuro próximo, existam vários softwares gratuitos para auxiliar na resolução desse tipo de crime, já que a maioria dos programas existentes são pagos, devido a área estar em constante crescimento.

Nesse trabalho foram apresentadas diversas técnicas, procedimentos e ferramentas utilizados pela perícia forense computacional, tal como é realizado um processo investigativo, através da coleta, exame, análise e apresentação de resultados obtidos.

Como estudo de caso foi retratado uma técnica muito utilizada por peritos, a esteganografia, juntamente com esteganálise, com a pretensão de extrair informações de algumas imagens hospedadas nos serviços de armazenamento nuvem da Google (Google Drive), Microsoft

(OneDrive) e Dropbox, utilizando o software JP Hide and Seek, que realiza a esteganografia através da técnica LSB (*Least Significant Bit*) e esteganálise de forma ativa, detalhando todos os passos necessários para realizar essas técnicas.

Como estudo futuro pretende-se aprofundar mais em softwares semelhantes aos da empresa israelense Cellebrite, tal como o UFED Cloud Analyser, que tem o foco em realizar a extração de dados armazenados em nuvem, preservando e acelerando de forma eficiente as investigações em todos os tipos de crimes cibernéticos. *Softwares* como esse anteriormente citado são o futuro da investigação em nuvem, facilitando muito a vida dos peritos, porém uma das maiores dificuldades ainda continuará sendo romper o sigilo de provedores de serviços em nuvem.

REFERÊNCIAS

ATHABASCA UNIVERSITY, 2004. Disponível em: < http://io.acad.athabascau.ca/~grizzlie/Comp607/programs.htm >. Acesso em: 21 jul. 2020.

BARDI, Marcelo A. G.; ZORZI, Lucas. **REAPROVEITAMENTO DE DISPOSITIVOS COMPUTACIONAIS UTILIZANDO COMPUTAÇÃO EM NUVEM COM VISTAS À SUSTENTABILIDADE NA ÁREA DE TECNOLOGIA DA INFORMAÇÃO**. Grupo de Pesquisas em Meio Ambiente e Sustentabilidade (GPMAS), Universidade São Francisco. 2017.

BORGES, Hélder Pereira; SOUZA, José Neuman de; SHULZE, Bruno; MURY, Antonio Roberto. **Computação em nuvem**. p. 48. Disponível em: < https://livroaberto.ibict.br/bitstream/1/861/1/COMPUTA%C3%87%C3%83O%20EM%20NUVEM.pdf >. Acesso em: 9 mar. 2020

BOZZA, Claudia. **Google Drive é lançado oficialmente**. 2012. Disponível em: < https://www.techtudo.com.br/noticias/noticia/2012/04/google-drive-e-lancado-oficialmente.html >. Acesso em: 21 jul. 2020.

CANALTECH**. O que é rootkit?** 2017. Disponível em: < https://canaltech.com.br/seguranca/O-que-e-rootkit/ >. Acesso em: 6 mar. 2020.

CARISSIMI, Alexandre. **Desmistificando a Computação em Nuvem**. Universidade Federal do Rio Grande do Sul. Porto Alegre, RS. 2015. Disponível em: < https://www.researchgate.net/publication/301298378_Desmistificando_a_Computacao_em_Nuvem>. Acesso em: 9 mar. 2020.

CHIRIGATI, Fernando Seabra. **Computação em Nuvem**. Rio de Janeiro, RJ. 2009. Disponível em: < https://www.gta.ufrj.br/ensino/eel879/trabalhos_vf_2009_2/seabra/arquitetura.html >. Acesso em: 9 mar. 2020.

DAMACENA, Barbara Larissa Candido. **DESAFIOS DA PERÍCIA FORENSE EM UM AMBIENTE DE COMPUTAÇÃO NAS NUVENS**. 2014. 130 p. Trabalho de Conclusão de Curso (Bacharelado em sistemas da informação) - Universidade do Planalto Catarinense, Lages (SC), 2014.

DIDONÉ, Dener. **Computação em nuvem: Desafios e Oportunidades para a Forense Computacional**. Dissertação de mestrado. Universidade Federal de Pernambuco, Recife. 2011. P. 114.

DYKSTRA, Josiah. **Design and implementation of FROST: Digital forensic tools for the OpenStack cloud computing platform**. 2013. Disponível em: < https://www.sciencedirect.com/science/article/pii/S174228761300056X#sec3 >. Acesso em: 10 mar. 2020.

ELEUTÉRIO, Pedro Monteiro da Silva; MACHADO, Márcio Pereira; **Desvendando a computação forense**; São Paulo, Novatec Editora, 2011

FARMER, Dan; VENEMA, Wietse. **Perícia Forense Computacional: Teoria e Prática Aplicada**.

São Paulo, Pearson Prentice Hall, 2007, p.171.

FIZMAN, Gabriela. **O que é esteganografia?** Disponível em: < https://www.techtudo.com.br/noticias/noticia/2015/07/o-que-e-esteganografia.html >. Acesso em: 7 mar. 2020.

TECHBIZ. **UFED Cloud Analyser oferece acesso imediato aos dados privados da nuvem**. 2015. Disponível em: < http://forensedigital.com.br/new/ufed-cloud-analyzer-oferece-acesso-imediato-aos-dados-privados-da-nuvem/ >. Acesso em: 10 mar. 2020.

FRANCO, Deivison Pinheiro; VILAR, Gustavo Pinto; GUSMÃO, Luiz Eduardo Marinho; GROCHOCKI, Luiz Rodrigo. **Introdução à Computação Forense**, [S. l.], p. 13. Disponível em:< https://www.editorajuspodivm.com.br/cdn/arquivos/e747cfb156d4939f779db96ffc5ed94b.pdf > Acesso em: 10 mar. 2020.

FREITAS, Andrey Rodrigues de. **Perícia Forense Aplicada à Informática**. 2003. 58 p. Trabalho de Conclusão de Curso (Pós graduação em Internet Security) - IBPI, [*S. l.*], 2003.

GONÇALVES, Márcio; AMADIO, Renato Arnaut; GAVILAN, Júlio César; SANTOS, Herlones Wuilles dos. **PERÍCIA FORENSE COMPUTACIONAL: METODOLOGIAS, TÉCNICAS E FERRAMENTAS.** Revista Científica Eletrônica de Ciências Socias Aplicadas da Eduvale. Vale de São Lourenço - Jaciara/MT, p. 17, 7 nov. 2012. Disponível em:< http://eduvalesl.revista.inf.br/imagens_arquivos/arquivos_destaque/LXkEA5FVHGZF1FB_2015-12-19-2-33-33.pdf> Acesso em: 10 mar. 2020.

GUTMANN, Peter. **Secure Deletion of Data from Magnetic and Solid-State Memory**. 1996. University of Auckland. Disponível em: < https://www.cs.auckland.ac.nz/~pgut001/pubs/secure_del.html >. Acesso em: 7 mar. 2020.

LOPES, Petter Anderson. **Forense Digital**. Disponível em: < https://jus.com.br/artigos/69827/forense-digital >. Acesso em: 5 mar. 2020.

MARINS, Carlos Eduardo. **Desafios da informática forense no cenário de Cloud Computing**. 2009. Disponível em: < http://icofcs.org/2009/ICoFCS2009-PP10.pdf >. Acesso em: 8 mar. 2020.

MARTINS, Rodrigo. **Laudo Técnico Forense Computacional**. Disponível em: < https://atitudereflexiva.wordpress.com/2016/03/01/laudo-tecnico-forense-computacional/ >. Acesso em: 5 ma. 2020.

MICROSOFT AZURE**. O que são nuvens públicas, privadas e híbridas?** Disponível em: < https://azure.microsoft.com/pt-br/overview/what-are-private-public-hybrid-clouds/>. Acesso em: 9 mar. 2020.

NEUKAMP, Paulo A**. Forense Computacional: Fundamentos E Desafios Atuais**. 11 Junho de 2007. Universidade do Vale do Rio dos Sinos (UNISINOS). 06 Nov. 2007.

ONDATA. **Recursos e funcionalidades do EnCase Forensic**. Disponível em: < http://www.ondata-pt.com/recuperacao-dados/EnCase_Forensic_FeatureSheet.pdf >. Acesso em: 7 mar. 2020.

PALMER, Gary. **A Road Map for Digital Forensic Research**; Technical Report DTR – T001-01, DFRWS. Report From the First Digital Forensic Research Workshop (DFRWS), New York, 2001.

PEDROSA, Paulo H. C.; NOGUEIRA, Thiago. **Computação em Nuvem**. Disponível em: < https://www.ic.unicamp.br/~ducatte/mo401/1s2011/T2/Artigos/G04-095352-120531-t2.pdf >. Acesso em: 8 mar. 2020.

REDHAT**. O que é a nuvem pública**. Disponível em: < https://www.redhat.com/pt-br/topics/cloud-computing/what-is-public-cloud >. Acesso em: 9 mar. 2020.

ROSANES, Pedro. **Rootkits**. Universidade Federal do Rio de Janeiro, Rio de Janeiro. Disponível em: < https://atitudereflexiva.wordpress.com/2016/03/01/laudo-tecnico-forense-computacional/ >. Acesso em: 5 mar. 2020.

RUSCHEL, Henrique; ZANOTTO, Mariana Susan; MOTA, Welton Costa da. **Computação em nuvem**. Especialização em Redes e Segurança de Sistemas. Pontifícia Universidade Católica do Paraná. Curtiba – PR. 2010. p 15.

SCANLON, Mark. **Enabling the Remote Acquisition of Digital Forensic Evidence through Secure Data Transmission and Verification**. National University of Ireland, Dublin. 2009.

SCRIPTBRASIL. **OneDrive: o serviço de armazenamento da Microsoft. 2014. Disponível em**: < https://www.scriptbrasil.com.br/informatica/armazenamento/onedrive-servico-armazenamento-microsoft.html >. Acesso em: 21 jul. 2020.

SOUZA, Ieda Maria**. Evidências nas nuvens**. 2018. Disponível em: < https://www.serpro.gov.br/menu/noticias/noticias-2018/evidencias-nas-nuvens >. Acesso em: 9 mar. 2020.