UNIVERSIDADE DO EXTREMO SUL CATARINENSE – UNESC
CURSO DE CIÊNCIA DA COMPUTAÇÃO

CÉLIO FABRICIO DA CONCEIÇÃO FILIPE

FORENSE COMPUTACIONAL: MÉTODO PROCEDIMENTO E FERRAMENTAS PARA PERÍCIA FORENSE EM CLOUD COMPUTING

CRICIÚMA
2014

CÉLIO FABRICIO DA CONCEIÇÃO FILIPE

FORENSE COMPUTACIONAL: MÉTODO PROCEDIMENTO E FERRAMENTAS PARA PERÍCIA FORENSE EM CLOUD COMPUTING

Trabalho de Conclusão de Curso, apresentado para a obtenção do grau de Bacharel no curso de Ciência da Computação da Universidade do Extremo Sul Catarinense, UNESC.

Orientador: Prof. MSc. Paulo João Martins
Co-orientador: Prof. MSc. Luciano Antunes

CRICIÚMA

2014

CÉLIO FABRICIO DA CONCEIÇÃO FILIPE

FORENSE COMPUTACIONAL: MÉTODO PROCEDIMENTO E FERRAMENTAS PARA PERÍCIA FORENSE EM CLOUD COMPUTING

Trabalho de Conclusão de Curso aprovado pela Banca Examinadora para obtenção do Grau de Bacharel, no Curso de Ciência da Computação da Universidade do Extremo Sul Catarinense, UNESC, com Linha de Pesquisa em Perícia Forense Computacional.

Criciúma, 24 de Novembro de 2014

BANCA EXAMINADORA

Prof. MSc. Paulo João Martins - (Unesc) - Orientador

Prof. MSc. Luciano Antunes - (Unesc) – Co-orientador

Prof. MSc. Rogério Antônio Casagrande - (Unesc) – Membro Banca

Prof. Esp. Sérgio Coral - (Unesc) – Membro Banca

À Deus pelas bênçãos, à minha mãe por estar sempre do meu lado, me motivando e amparando nos bons e maus momentos, e a todos os meus parentes e amigos.

AGRADECIMENTOS

À DEUS primeiramente por estar sempre presente em minha vida, e aos meus pais Gonçalves José Filipe e Francisca Vanda e Silva da Conceição Filipe, por me conceberem e terem dado a oportunidade de nascer e crescer segundo a palavra de DEUS, em especial a minha Mãe por ser uma supermulher e por acreditar sempre no potencial dos seus filhos.

Aos meus amados irmãos Edileia e Laércio Filipe que sempre me apoiaram, as minhas avós Cecília Domingos e Fernanda Ribeiro, aos meus tios Catarino Fontes Pereira, Isabel Fontes Pereira, Alfredo e Hélder da Conceição, por serem os precursores da minha não desistência do curso de ciência da computação dando todo apoio, agradeço também aos tios e primos, Paulo, Raquel, Sílvia, Ricardo Bessa, Décio, Osmar, Alice, Shalon da Conceição, Arnaldo Soares, Felizarda Gonçalves e Fernanda Filipe, obrigado pelo apoio.

Sem esquecer as pessoas que mesmo não tendo uma relação cósanguínea, mas são como uma família, especialmente a minha namorada Sandra Borges, e os amigos Edivaldo Neto, Walter Francisco, Odin Peso, Harilton Dias, Vunda Xavier, Antônio Pinto, Wilma Cristiano, Nádia e Yasmine Pessoa, Ester Sangunja, Suelen Pereira, Neuma Delgado, Bruna Voss, Sílvia Campos, Maria Isabel, Dona Anita, ao meu mano Aguinaldo Cristiano e aos seus irmãos Weza e Áurio Cristiano obrigado pela amizade e irmandade criada desde o começo, aos meus colegas de turma que desde o começo foram bons companheiros.

À Sociedade Nacional de Petróleos de Angola (SONANGOL), pela oportunidade concedida, a Universidade Do Extremo Sul Catarinense (UNESC) e seu quadro docente, pelo apoio, carinho, suporte e profissionalismo mostrados durante a árdua jornada, e ao meu orientador e co-orientador, professores Paulo João Martins e Luciano Antunes pelas ideias, ajuda e apoio.

Por último agradeço a todos os que contribuíram direta ou indiretamente para que eu me tornasse no homem que sou hoje.

O meu muito obrigado a todos!

“O sucesso nasce do querer, da determinação e persistência em se chegar a um objetivo. Mesmo não atingindo o alvo, quem busca e vence obstáculos, no mínimo fará coisas admiráveis."

José Alencar

RESUMO

A *Cloud Computing* tem sido atualmente uma das tendências no mercado de tecnologia, proporcionando aos seus usuários outra visão sobre como armazenar e gerenciar os seus dados e alterar a sua maneira de trabalhar. Por mais que surjam novos mecanismos para o uso da *Cloud Computing,* ainda existem desafios, tais como: obtenção ou recuperação de dados forenses, bem como realizar a perícia forense computacional. Esta pesquisa visou fornecer uma abordagem geral em torno da perícia forense em *Cloud Computing*, aplicando um estudo de caso para descrever um método para recuperar e analisar os dados existentes em um ambiente *Google Drive*. Para a realização do trabalho, seguiu-se a seguinte metodologia: pesquisa bibliográfica, elaboração de um estudo de caso fictício que foi solucionado aplicando a metodologia *Standard Operating Procedures* (*SOP)* em sete (7) etapas que são: autorização, preparação do equipamento, coleta e preservação, imagem forense, exame e análise, documentação, relatório e revisão. Conseguiu-se estudar e aplicar os conceitos de perícia forense computacional envolvendo ambientes Cloud Computing, onde foi possível analisar com sucesso os arquivos existentes, foi então usado o ambiente *Deft 7.2*, as ferramentas *AccessData FTK Imager*, *Autopsy* e a pasta de sincronização do *Google Drive*, tendo sido encontradas provas em alguns dos arquivos examinados.

Palavras-chave*:* *Cloud Computing*. Perícia Forense. Segurança. Crimes Digitais. *Cloud Forensics*.

ABSTRACT

The *Cloud Computing* is nowadays one of the trends in the technology market, providing its users a different view on how to store and manage your data and change your way of working. As there are new mechanisms for the use of *Cloud Computing*, there are still challenges, such as obtaining or recovery of forensic data and perform computer forensics. This research aimed to provide a general approach around the forensic expertise in *Cloud Computing*, applying a case study to describe a method to retrieve and analyze the data in a *Google Drive* environment. To carry out the work, followed the following methodology: bibliographic research, preparation of a fictional case study that was solved by applying the *Standard Operating Procedures methodology* (*SOP*) in seven (7) steps that are: authorization, equipment preparation, collection and preservation, forensic image, examination and analysis, documentation, reporting and review. It was possible to study and apply the concepts of computer forensics involving *Cloud Computing* environments, where it was possible to successfully analyze existing files, was then used *Deft 7.2* environment, the tools *AccessData FTK Imager*, *Autopsy* and synchronization folder of *Google Drive* , evidence has been found in some of the examined files.

Keywords: Cloud Computing. Digital Crimes. Cloud Forensics.

LISTA DE ILUSTRAÇÕES

LISTA DE ABREVIATURAS E SIGLAS

API	Application Programming Interface
AWS	Amazon Web Service
CAPEX	Capital Expenditure
CC	Cluster controller
CEO	Chief Executive Officer
CERT.br	Centro de Estudos, Respostas e Tratamento de Incidentes de Segurança do Brasil
CIO	Chief Information Officer
CIRC	Computer Incident Response Capability
CLC	Cloud Controller
CIRT	Computer Incident Response Team
CRM	Customer Relationship Management
CSA	Cloud Security Alliance
CSIRT	Computer Security Incident Response Team
CSP	Cloud Service Provider
DFRWS	Digital Forenics Research Workshop
EC2	Elastic Compute Cloud
GB	Gigabyte
FOSS	Free and Open Source Software
IAAS	Infrastructure-as-a-Service
ICS	Infrastructure-as-a-Service
IDC	International Data Corporation
IDS	Sistema de Detecção de Intrusão
IP	Internet Protocol
JPG/JPEG	Joint Photographic Experts Group
Log	Registro de Eventos de um Sistema Computacional
MB	Megabyte
MISD	Multiple Instruction, Single Data
NIST	National Institute of Standards and Technology
OPEX	Operational Expenditure
PAAS	Platform-as-a-Service
PDF	Portable Document Format

SAAS	Software-as-a-Service
SOP	Standard Operating Procedures
SIMD	Single Instruction, Multiple Data
SISD	Single Instruction, Single Data
SLA	Service Level Agreement
TI	Tecnologia de Investigação
TB	Terabyte
VM	Virtual Machine
WFT	Windows Forensics Toolchest

SUMÁRIO

1 INTRODUÇÃO

Nos dias de hoje as tecnologias de informação tem evoluído com uma velocidade incontrolável, esta rápida evolução tem trazido inúmeros benefícios a todos, e com ela, também algumas consequências. O computador não é o único meio tecnológico e digital que faz parte do nosso cotidiano, existem hoje outros aparelhos como telefones celulares, tablets entre outros, desempenhando um papel fundamental na organização e difusão de informações, compartilhamento de dados, pesquisas por meio da Internet e no entretenimento. Têm-se muitos benefícios, porém surge um problema no que se refere à falta de segurança.

Com o uso crescente desses meios tecnológicos, bem como a difusão e massificação da Internet, surge a *Cloud Computing* ou computação em nuvem. Nesse modelo é possível armazenar e acessar dados, prover recursos, entre outros serviços. Este recurso tem sido muito difundido e com ele a insegurança por parte dos usuários, por não saberem o lugar físico onde seus dados estão armazenados, até que ponto eles estão seguros e como recuperá-los se forem apagados em um ambiente na nuvem.

Segundo Marins (2009), a *Cloud Computing* é uma expansão genérica que descreve a evolução de tecnologias e processos, compostos de serviços, aplicações, informações e infraestrutura distribuída, de modo que estes possam ser organizados dinamicamente, elástica e rapidamente na medida em que forem consumidos.

Existem hoje pessoas que se dedicam a estudar vulnerabilidades e técnicas de invasão em computadores, e usam tais técnicas, como um meio para facilitar a execução de atividades criminosas. Assim, tem-se o inicio a era de crimes digitais. Os crimes digitais são toda conduta ilegal, que fere a ética, que envolva o processamento e ou transmissão de dados (CRISTIANO, 2011).

Desta forma, o presente trabalho realizou o estudo de algumas plataformas de ambiente em nuvem, que foram definidas no decorrer da pesquisa, bem como o processo de perícia forense usado em um desses ambientes, focando-se na metodologia de coleta e análise de evidências em ambientes *Cloud Computing.*

1.1 OBJETIVOS

1.1.1 Objetivo geral

Pesquisa de procedimento e ferramentas para a perícia forense computacional em ambiente *Cloud Computing*.

1.1.2 Objetivos específicos

Os objetivos específicos desta pesquisa foram:

a) aplicar os conceitos sobre perícia forense computacional;

b) compreender como ocorrem os crimes digitais e como manter a segurança da informação;

c) compreender e aplicar os conceitos de *Cloud Computing*;

d) descrever e relatar acerca das ferramentas de código aberto e software livre usadas na busca e análise de evidências;

e) relatar e documentar um estudo de caso, de forma a elucidar a referida pesquisa, com as evidências obtidas.

1.2 JUSTIFICATIVA

A rápida mutação e evolução das tecnologias de informação têm influenciado no desenvolvimento de sistemas e no comportamento de usuários, com este fenômeno vem surgindo a necessidade de se encontrar mecanismos científicos e tecnológicos para acompanhar esta rápida evolução. Atualmente no século XXI os desafios tecnológicos vão além do imaginável no século XX, os crimes são planejados e executados com a ajuda da tecnologia e, é essa mesma tecnologia que tem ajudado a desvendar e solucionar tais crimes (SCHWEITZER, 2003).

Em 2012 um caso chamou a atenção do Brasil, a atriz Carolina Dieckmann teve fotos intimas publicada na Internet, durante a investigação foram levantadas inúmeras hipóteses antes de chegarem à conclusão de que ela teria sido vitima de malfeitores (*Hackers*), a polícia chegou a tal conclusão graças a um trabalho de perícia nas contas de *e-mail* da atriz usando *softwares* apropriados que levaram aos Protocolos de Internet, do inglês *Internet Protocol* (IP), dos suspeitos.

No ano seguinte foi aprovada a lei 12.737/2012 popularmente conhecida como Lei Carolina Dieckmann que, entre outros, torna crime a invasão de aparelhos eletrônicos para obtenção de dados particulares (BRASIL, 2012). Este caso ilustra a realidade atual, que as novas tecnologias fomentam novos crimes e que não existem crimes não solucionáveis, pois se pode observar o aumento da relevância da evidência digital em processos jurídicos (WEBBA, 2010).

A perícia forense computacional vem se mostrando uma arma eficaz no combate à impunidade que há no mundo cibernético, porém, ainda existe uma carência de estudos sobre o tema, abordando soluções práticas e mais aprofundadas em ambientes *Cloud Computing*.

O conceito de *Cloud Computing* tem sido o protagonista de uma mudança na maneira como as pessoas e corporações armazenam, processam e acessam os seus dados, tirando delas a responsabilidade de gerenciar os equipamentos e as informações, deixando este trabalho para plataformas especializadas em armazenar e gerenciar grandes volumes de informações e disponibilizá-las na nuvem. Nela o usuário pode acessar as suas informações de qualquer lugar sem a necessidade de possuir uma unidade de armazenamento local, ou de instalar qualquer programa, bastando apenas ter uma conexão de Internet.

A *Cloud Computing* pretende melhorar e suprir algumas lacunas, porém existe a necessidade de se aprofundar nos cuidados e nos conhecimentos ao lidar com ela. Primeiramente, por não se ter os arquivos em um local físico, onde possa ser recuperado, no caso deles serem apagados ou ocultados e também por não existirem ainda muitas aplicações específicas para fazer uma perícia em nuvem (ESES; RAMOS, 2010).

Assim sendo, a presente pesquisa descreve o processo de perícia forense computacional em ambientes *Cloud Computing*, baseando-se na coleta e análise de evidências obtidas por softwares.

1.3 TÓPICOS DO TRABALHO

A presente pesquisa teve como objetivo descrever um método e procedimento para perícia forense em *Cloud Computing*. O trabalho esta dividido em duas etapas e conta com cinco capítulos. A primeira etapa é a fundamentação

teórica sobre o tema e a segunda abordou o estudo de caso onde forem usadas ferramentas e aplicadas técnicas na busca de evidências.

O primeiro capítulo é a introdução, nela é encontrada a definição do problema, objetivo geral, objetivos específicos e a justificativa do trabalho. O segundo capítulo aborda sobre a perícia forense computacional, crimes digitais, metodologias para solucionar um crime digital bem como as leis existentes no Brasil e em Angola. O terceiro capítulo aborda *Cloud Computing,* conceitos de computação distribuída, descrição da taxonomia de *Flynn*, tipos de *Cloud Computing* e como ela funciona como computação distribuída. O quarto capítulo aborda a perícia forense em ambientes *Cloud Computing* (*Cloud Forensic*) sua dimensão, seu uso e desafios. Os trabalhos correlatos usados para o desenvolvimento da pesquisa são abordados no quinto capítulo. O sexto capítulo discorre a temática da pesquisa, metodologia utilizada para a pesquisa, ambientes utilizados para desenvolvimento da pesquisa, procedimento para a realização da perícia utilizando uma metodologia e por fim os resultados e discussão. A conclusão é o último capítulo desta pesquisa.

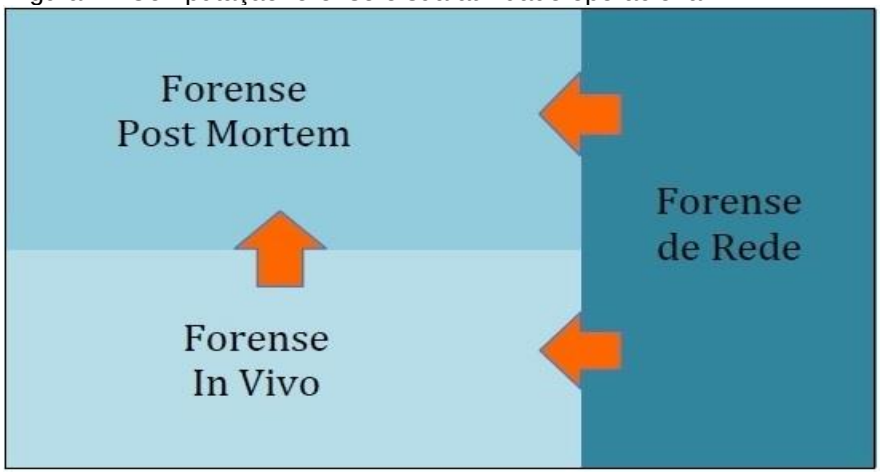
2 PERÍCIA FORENSE COMPUTACIONAL

A computação forense é considerada uma ciência multidisciplinar relativamente nova, e quando associada a técnicas de investigação ajuda a determinar e analisar evidências seguindo métodos e procedimentos definidos pelas suas etapas de perícia (DIDONÉ; QUEIRÓZ, 2011).

Segundo Steve Haileys, CEO e professor do Instituto de Segurança Cibernética (*Institute Cyber Security* ICS), a Perícia Forense Computacional é a preservação, identificação, coleta, interpretação e documentação de evidências computacionais, incluindo as regras de processo legal, integridade da evidência, provisão da opinião de especialista em uma corte judicial e relatório do factual da evidência, ou algum outro processo legal com relação ao que foi encontrado (HAILEYS, 2002).

A Computação Forense é uma área de especialização relativamente nova no mundo e tem se desenvolvido muito rápido, principalmente pela necessidade que as instituições legais têm ao atuarem no combate aos crimes eletrônicos. Este processo tem gerado ao longo dos anos, resultados positivos e confiáveis decorrentes de procedimentos e protocolos detalhados com documentações e revisões aceitas pela comunidade cientifica. O uso de metodologia e de protocolos deve ser considerado na prática de investigação, como garantia de aceitação em uma corte judicial. As atividades desenvolvidas pelos especialistas em perícia forense podem ser entendidas do ponto de vista macro em três fases ilustradas na figura 1 (CRISTIANO, 2011; MELO, 2009).

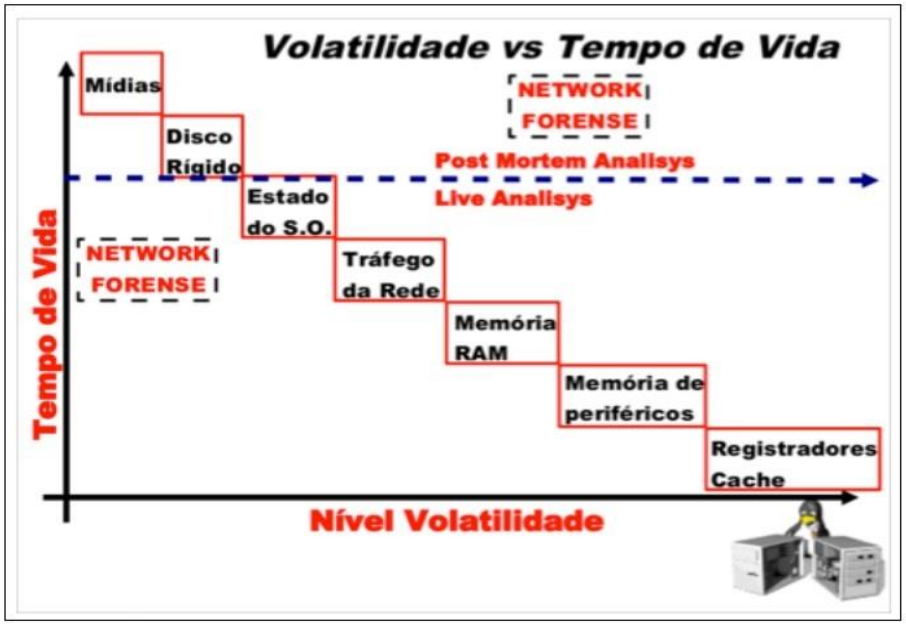
Figura 1 - Computação forense e sua atividade operacional.



Fonte: Melo (2009).

A forense *Post Mortem* é a etapa que visa coletar e analisar todos os dados logo após o encerramento do sistema, nela apenas serão coletados dados não voláteis que entre outros, incluem discos rígidos, *pendrives*. Esta é por muitos especialistas considerada a etapa mais difícil pelo elevado volume de dados encontrados nas memórias, sendo de extrema importância que a análise seja feita em outra máquina para que as provas de perícia não sejam comprometidas (CRISTIANO, 2011; MELO, 2009).

Figura 2 - Grau de volatilidade versus tempo de vida.



Fonte: Melo (2009).

A forense *In Vivo*, é a etapa que ocorre no momento em que o perito entra em contato com o incidente, onde ele não precisa encerrar o sistema para fazer a coleta dos dados. Os dados são coletados mediante os níveis de prioridade, dos mais voláteis aos menos voláteis, porque na maioria das vezes após o sistema ser encerrado os dados mais voláteis são perdidos (CRISTIANO, 2011; SACRAMENTO, 2012).

Melo (2009) também definiu a Forense *In Vivo* como a etapa que consiste na coleta de evidência antes que o sistema seja desligado da fonte elétrica, onde tem por objetivo registrar o estado do sistema. Buscar evidências em um sistema operacional é fazer uma varredura nas informações que nele residem, tanto dados em arquivos de memória apagados ou não.

A forense em Rede é a etapa em que são capturados e analisados os dados da comunicação entre a máquina atacada e a do atacante, os dados uma vez capturados por intermédio de *sniffers*, irão servir posteriormente para cruzar as informações dos dados obtidos durante o *Post Mortem* e na forense *In vivo* (CRISTIANO, 2011; MELO, 2009).

Para Melo (2009) Forense de Rede ou *Network Forensic*, consiste em coletar informações da rede, tanto no servidor e nos ativos de rede que têm informações pertinentes. Pode-se dizer que a Forense de Rede pode ser dividida em dois momentos, o primeiro é quando o perito forense analisa e coleta informações de comunicações de rede do servidor e o segundo é a análise e coleta das informações de comunicações de redes em outros ativos como servidor de *logs*, *firewall*, roteadores e entre outros.

Para que seja recorrido ao uso da ciência forense e da perícia forense computacional, é necessário que haja um incidente e, no século XXI os maiores incidentes são os crimes digitais que ocorrem pelo uso ilegal das tecnologias de informação.

2.1 CRIMES DIGITAIS

No mundo atual, a sociedade tem sentido a mudança de certos hábitos e costumes, tem se notado uma mudança no jeito de se comunicar, trabalhar, lecionar, aprender, entre outros. A proliferação de meios tecnológicos como computadores pessoais, acesso fácil à Internet, e um mercado em expansão relacionado com novos dispositivos de comunicação, mudaram a forma como se gasta o tempo e como se fazem negócios.

Crime do latim *crimen*, é qualquer violação grave da lei moral, civil, religiosa ou ato ilícito cometido em uma sociedade passível de uma sansão penal (WEBBA, 2010).

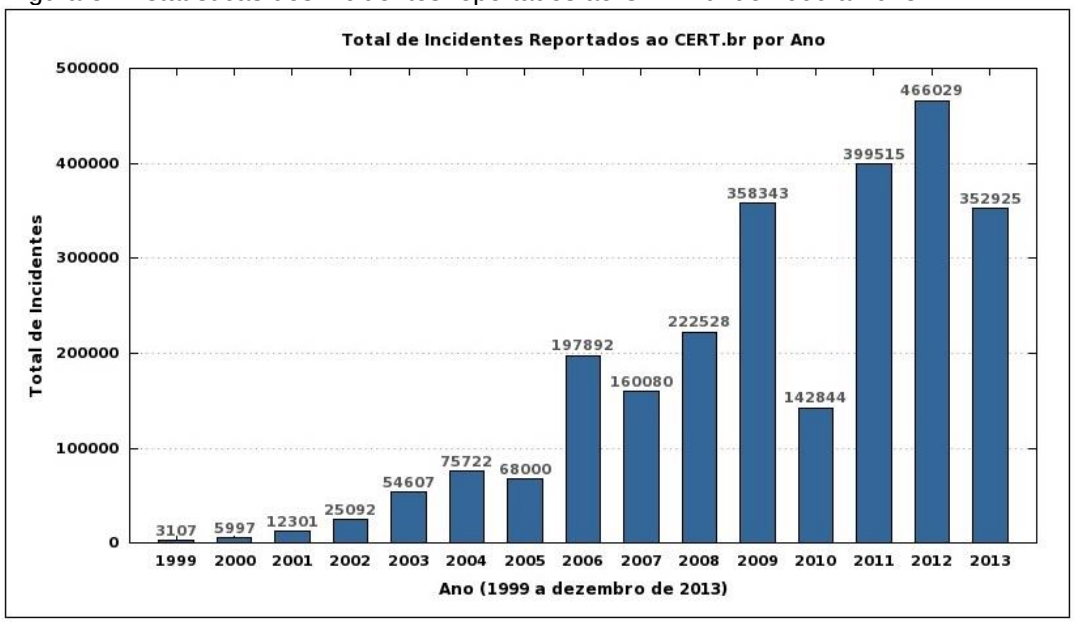
Crimes digitais são violações graves a lei moral, civil ou ato ilícito cometido por meio de um computador, celular ou qualquer meio digital (tecnológico). Eles podem assemelhar-se a alguns crimes comuns, a única diferença é que no crime comum não é obrigatório o uso de computadores ou alguma tecnologia digital.

Alguns conceituados escritores brasileiros como Pinheiro (2001) em suas obras literárias classificam os crimes em três subgrupos descritos a seguir:

a) **crimes digitais ou virtuais puros** – é toda conduta ilícita que visa lesar o hardware ou o software de um computador ou sistema informatizado;
b) **crimes digitais ou virtuais mistos** – eles utilizam a Internet ou redes de computadores para cometer delitos, não visam sistemas informáticos e são normalmente usados em transações ilegais de valores de contas correntes;
c) **crimes digitais ou virtuais comuns** – utilizam a Internet ou as redes públicas de computadores para realização de qualquer delito, ele consta no código penal.

Dados obtidos no Comitê Gestor da Internet no Brasil CERT.br, apontam o crescimento dos incidentes de segurança em computadores que envolvam redes conectadas à Internet brasileira ilustrada na figura 3.

Figura 3 - Estatísticas dos incidentes reportados ao CERT.br de 1999 a 2013.



Fonte: CERT.br (2014).

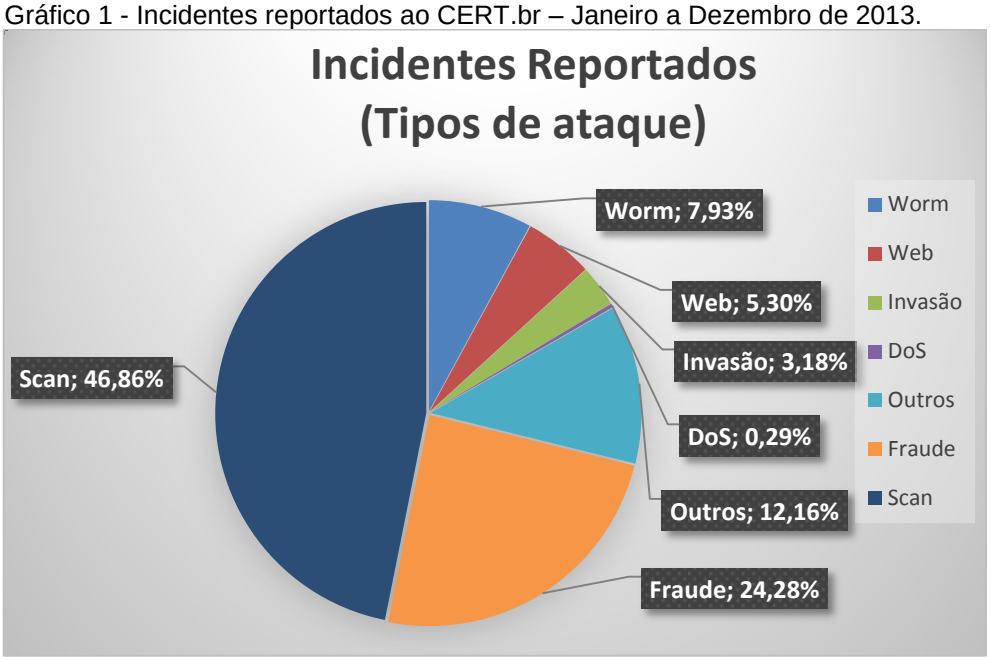
Em 2013 foram reportados 352.925 incidentes como ilustra a figura 3, este número foi 24% menor que do ano anterior que foram de 466.029, os incidentes foram de diferentes tipologias (CERT.br, 2014).

2.1.1 Tipos de crimes digitais mais comuns no Brasil

De acordo com a CERT.br (2014) os crimes digitais mais comuns são classificados pelos seguintes tipos como ilustra o gráfico 1:

a) ***worm*** – são programas maliciosos (malware), automatizados para propagação de códigos maliciosos na rede;
b) ***web*** – são os ataques que visam o comprometimento de servidores Web ou desfigurações de páginas na Internet;
c) ***denial of service (Dos)*** – são ataques de negação de serviços, nela o criminoso utiliza um computador ou um conjunto de computadores (Cluster) para retirar um determinado serviço do ar;
d) **invasão** – são ataques bem sucedidos que resultam no acesso não autorizado a um computador ou rede;
e) ***scan*** – são buscas ou varreduras em redes de computadores, com a finalidade de identificar quais computadores estão ativos e quais serviços são disponibilizados por eles. É muito usado por criminosos para identificar alvos em potencial, pois ele permite associar possíveis vulnerabilidades aos serviços habilitados em um computador;
f) **fraude** – É toda ou qualquer ação ardilosa, enganosa, de má-fé, com intuito de lesar ou ludibriar outrem, ou de não cumprir determinado dever. Esta categoria engloba as notificações de tentativas de fraudes, ou seja, de incidentes em que ocorre uma tentativa de obter vantagem;
g) **outros** – são os incidentes que não se enquadram nas categorias anteriores.

Gráfico 1 - Incidentes reportados ao CERT.br – Janeiro a Dezembro de 2013.



Fonte: Adaptado de CERT.br (2014).

Analisando os dados fornecidos pelo CERT.br, constatou-se que os crimes digitais são uma ameaça real, e todos usuários são passíveis de tal ameaça, para se evitar tais incidentes existe um mecanismo que é a segurança da informação.

2.2 METODOLOGIAS PARA SOLUCIONAR UM CRIME DIGITAL

Apesar da indústria cibernética desenvolver inúmeros mecanismos para conter os crimes digitais, a segurança de informação continua a ser primordial para se evitar a ocorrência de tais incidentes. Existem hoje alguns processos para investigar e solucionar crimes digitais, estes processos investigativos têm como objetivo desvendar e apresentar as evidência do crime ou a solução do mesmo com as informações de onde aconteceu, o que aconteceu, quando e como, quais os envolvidos (CASEY, 2004).

2.2.1 Metodologia DFRWS

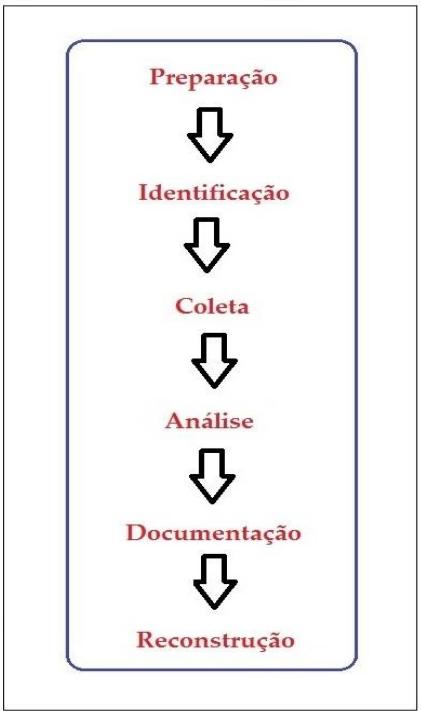
Esta metodologia é composta por sete etapas e foi criada e apresentada por Gary Palmer na primeira edição do *Digital Forensics Research WorkShop* (DFRWS) (BERTOGLIO, 2008):

a) **identificação –** ocorre a notificação do incidente ao perito;
b) **preservação –** deve ser assegurada a integridade e estado das evidências;
c) **coleta –** é feita a coleta de itens por meio de ferramentas e métodos específicos;
d) **exame –** é feita uma análise minuciosa dos itens encontrados, tendo como principal foco extrair as informações das evidências encontradas;
e) **análise –** são analisadas todas as evidências encontradas, para posteriormente criar as conclusões;
f) **apresentação –** o perito deve relatar os fatos de maneira clara, objetiva, concisa e organizada, de modos a não deixar margens para contestações;
g) **decisão –** é feita a apresentação ao tribunal os laudos onde o perito relata as suas conclusões sobre o caso.

2.2.2 Metodologia SOP

A metodologia *Standard Operating Procedures* (SOP), foi criada pela *Scientific Working Goup on Digital Evidence (SWGDE) e* exposta pela primeira vez no ano de 1999 em Londres durante a *Internacional Hi-Tech Crime and Forensis Conference*, a tecnologia é constituída por seis etapas (figura 4) e agrega procedimentos e conceitos da ciência forense (WEBBA, 2010).

Figura 4 - Metodologia SOP para resposta a incidentes.



Fonte: Schultz (2008).

2.2.2.1 Preparação

Esta é uma das etapas cruciais, nela o perito deve estar atento aos seus procedimentos para não infringir as regras de perícia e a lei, caso contrário ele coloca em causa o seu trabalho. Nesse caso é obrigatória a autorização do juiz ou de um conselho administrativo, e deve ser feita exclusivamente aquilo que foi solicitado pelos mesmos (WEBBA, 2010).

2.2.2.2 Identificação

Devem-se coletar as informações relevantes referentes ao crime e identificação completa do objeto a ser examinado (WEBBA, 2010). Só serão obtidas as informações necessárias para a tipologia de crime cometido, e a habilidade de procurar nos locais certos depende da prática do perito forense.

2.2.2.3 Coleta

Esta etapa só deve ser executada após a identificação das fontes de evidências, estas fontes devem ser coletadas para mais tarde serem autenticadas. É fundamental que as evidências não sejam alteradas durante o processo de

investigação, também é recomendável fazer o cálculo do valor *hash* da unidade de armazenamento original antes das evidências serem copiadas e ao final deve ser feita uma verificação para saber se a cópia é igual a original. Alguns peritos recomendam que sejam feitas mais de uma cópia dos dados em unidades de armazenamento vazias e com ferramentas diferentes (BERNARDO, 2006; CASEY, 2004).

2.2.2.4 Análise

É a fase posterior a coleta das evidências, onde estas serão examinadas e analisadas pelo perito na busca de provas.

2.2.2.5 Documentação

A etapa de documentação é elementar em uma perícia forense, se porventura outro perito entrar no caso ele terá acesso a tudo o que já foi feito, e também o trabalho de perícia terá mais crédito se tiver uma documentação completa com a identificação do perito e de todos os que participaram do processo com a respectiva data e hora (BERNARDO, 2006).

2.2.2.6 Reconstrução

A etapa de reconstrução da cena do crime tenta responder as perguntas chaves: Quando aconteceu? O que aconteceu? Quem executou? Onde aconteceu? Por que aconteceu? E Como aconteceu?

2.3 CRIMES DIGITAIS E SUAS LEIS

As pessoas ao redor do mundo têm conhecido uma maneira relativamente nova de verem os seus pertences usurpados ou furtados sem qualquer ação violenta, esta nova e argilosa maneira é denominada de crimes digitais do inglês cyber crimes ou digital crime. Este crime tem recebido não só a atenção dos desenvolvedores de novas tecnologias, mas também dos juristas e pessoas ligadas as leis, não só pela sua gravidade ou intensidade, mas pela sua rápida proliferação.

No Brasil existem hoje leis de combate a crimes informáticos, a mais atual é a LEI Nº 12.737 de 30 de Novembro de 2012, que tipifica os crimes da seguinte maneira.

2.3.1 Invasão de dispositivo informático

A lei no seu artigo 154-A dispõe que invadir dispositivo informático alheio, conectado ou não à rede de computadores, mediante violação indevida de mecanismo de segurança e com o fim de obter, adulterar ou destruir dados ou informações sem autorização expressa ou tácita do titular do dispositivo ou instalar vulnerabilidades para obter vantagem ilícita da pena de detenção de três meses a um ano, e multa (BRASIL, 2012):

a) na mesma pena incorre quem produz, oferece, distribui, vende ou difunde dispositivo ou programa de computador com o intuito de permitir a prática da conduta definida;
b) aumenta-se a pena de um sexto a um terço se da invasão resulta prejuízo econômico;
c) se da invasão resultar a obtenção de conteúdo de comunicações eletrônicas privadas, segredos comerciais ou industriais, informações sigilosas, assim definidas em lei, ou o controle remoto não autorizado do dispositivo invadido a Pena será reclusão, de seis meses a dois anos, e multa, se a conduta não constitui crime mais grave;
d) na hipótese do terceiro, aumenta-se a pena de um a dois terços se houver divulgação, comercialização ou transmissão à terceiro, a qualquer título, dos dados ou informações obtidos;
e) aumenta-se a pena de um terço à metade se o crime for praticado contra presidente da república, governadores e prefeitos, presidente do supremo tribunal federal, presidente da câmara dos deputados, do senado federal, de assembleia legislativa de estado, da câmara legislativa do distrito federal ou de câmara municipal, dirigente máximo da administração federal, estadual, municipal ou do distrito federal.

2.3.2 Ação penal

O artigo 154-B Frisa que nos crimes definidos no artigo 154-A, somente se procede mediante representação, salvo se o crime é cometido contra a administração pública direta ou indireta de qualquer dos Poderes da União, Estados, Distrito Federal, Municípios ou contra empresas concessionárias de serviços públicos como, por exemplo (BRASIL, 2012):

a) interrupção ou perturbação de serviço telegráfico, telefônico, informático, telemático ou de informação de utilidade pública;
b) incorre na mesma pena quem interrompe serviço telemático ou de informação de utilidade pública, ou impede ou dificulta-lhe o restabelecimento;
c) aplicam-se as penas em dobro se o crime é cometido por ocasião de calamidade pública.

Em Angola existe desde 24 de Maio de 2011 uma lei que protege dados pessoais e regulam comunicações eletrônicas e serviços da sociedade de informação, inspirada na lei Norte Americana e na Portuguesa, ela dá poderes às forças de segurança para procurar e confiscar os dados sem uma ordem judicial e cria penas de até 12 anos de prisão para qualquer crime cometido usando um computador (COMPUTERWORLD, 2011). Porém, ainda está em aprovação o código penal para tipificação destes crimes.

O subcapítulo a seguir é um extrato da Lei Ordinária 12.965 que aborda sobre o Marco civíl da Internet no Brasil aprovado em 2014.

2.4 MARCO CIVÍL DA INTERNET NO BRASIL

O Marco Civil é um processo legislativo que teve o seu começo em 2009, tendo como base dez princípios que seguem a Constituição da República, ele foi proposto para regulamentar o uso da Internet no Brasil, visando os princípios, garantias, direitos e deveres de quem usa a rede mundial de computadores, abordando alguns assuntos como responsabilidade civil de usuários e provedores de Internet, função social da rede, neutralidade da rede, e retenção de dados (BRASIL, 2014).

O Marco Civill da Internet está composto por cinco capítulos e eles abordam os seguintes temas (BRASIL, 2014):

a) no primeiro capítulo encontram-se as Disposições Preliminares composta por seis artigos que entre outros abordam sobre os princípios, direitos, garantias, deveres, disciplina, no uso da Internet, e determina regras para a atuação das autoridades;
b) o segundo capítulo discorre sobre os Direitos e Garantias do Usuário e, estando composto por dois artigos que nas suas entrelinhas asseguram o acesso à Internet pelo usuário, defendendo a inviolabilidade da intimidade privada, proteção, indenização, garantia dos direitos à privacidade, liberdade de expressão e entre outros;
c) a provisão de Conexão e de Aplicações da Internet é referente ao terceiro capitulo,que está composta por doze artigos que discorrem sobre a neutralidade da rede, proteção aos registros, aos dados pessoais e comunicação privada, guarda de registros de conexão, acesso a aplicação, Responsabilidade por danos decorrentes de conteúdo gerado por terceiros e requisição judicial de registros;
d) o quarto capítulo aborda sobre a atuação do poder público, estando composto em quatro artigos que discorrem sobre as diretrizes que constituem a atuação da União, dos Estados, do Distrito Federal, dos Municípios no desenvolvimento da Internet no Brasil, o cumprimento dos deveres constitucionais do estado, bem como as iniciativas públicas de fomento à cultura digital e de promoção da Internet como ferramenta social;
e) o quinto e último capítulo aborda sobre as disposições finais, composto por quatro artigos que discorrem sobre a liberdade que o usuário terá na escolha de programas no seu terminal desde que sejam respeitados os princípios da lei do estatuto da criança e adolescente (Lei n ^{o} 8.069 de 13 de Julho de 1990).

Para melhor entendimento, esclarecimento e visualização na integra vide anexo A.

2.5 SISTEMAS OPERACIONAIS E FERRAMENTAS UTILIZADOS PARA RESPOSTA A INCIDENTES

Para a coleta, duplicação, recuperação e análise de dados, existem diversos sistemas operacionais e ferramentas, as quais formam um conjunto, que deve ser composto por softwares de backup, descriptografia, coleta, monitoramento de protocolos de Internet, recuperação e analise de arquivos (PLADNA, 2009). O uso destas ferramentas no meio judicial ajudam a não afetar a veracidade das provas recolhidas.

2.5.1 DEFT

O *DEFT* (Figura 5) é um software livre GNU / LINUX que tem como base o *S.O Ubuntu, f*oi desenvolvido pelo Italiano *Stefano Fratepietro* para satisfazer as necessidades relacionadas a computação forense e a segurança da informação. Teve o lançamento da sua primeira versão pública baseada em Linux Kubunto em Janeiro de 2007 que posteriormente foram aperfeiçoadas em outras versões no mesmo ano (V2, V3), atualmente está na versão 8.2 (DEFT, 2014).

Figura 5 - Sistema Operacional Deft.

Fonte: DEFT (2014).

Desenvolvido exclusivamente para realização de perícia forense digital, tem como qualidades garantir que a estrutura dos arquivos analisados mantenham-

se coesos, reduzir o risco de alteração da cena do crime, não utiliza partições Swap na inicialização do sistema, não constrói partições de maneira automática e não faz a automação de processos no decorrer da execução de alguma análise.

2.5.2 HELIX

O *HELIX* é um *software* livre, desenvolvido a partir da base do *Ubuntu* por *Klaus Knopper* e distribuída pela E-fense, comporta um leque de mais de 100 ferramentas forenses, que têm como objetivos auxiliar o perito em diversas ações como obtenção de imagem, análise de imagens ou mídias, emissão de relatórios. A sistema Helix é multiplataforma, tendo versões para os três principais sistemas operacionais, eles são: *Windows, Linux e Mac OS (E-FENSE, 2014).*

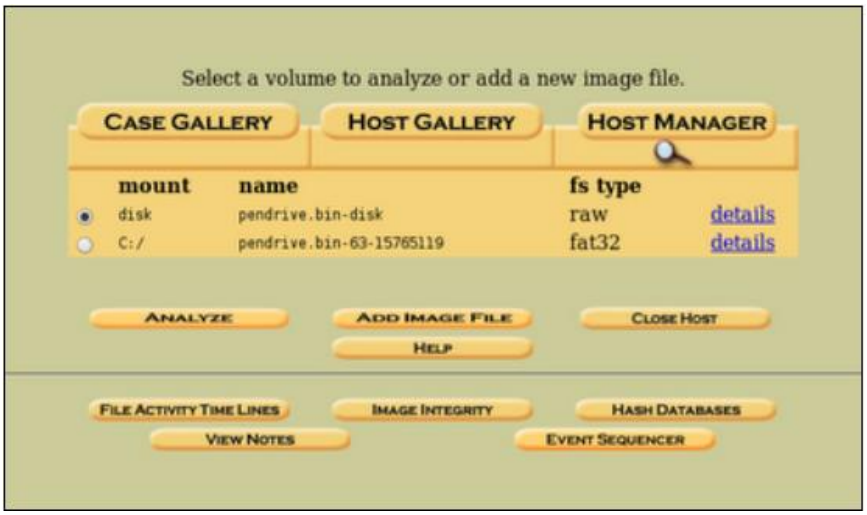
2.5.3 Algumas ferramentas de perícia forense computacional

Na investigação forense existem metodologias para resposta a estes incidentes, tais metodologias para que sejam seguidas efetivamente precisam de apoio de ferramentas, de modo a que se possa, por exemplo: manter a cena do crime deixando as evidências intactas, fazer a aquisição, a reconstrução do auto, e a sua posterior análise (CARRIER, 2003). Serão descritas algumas destas ferramentas, sobretudo aquelas que se encontram no ambiente a ser estudado.

2.5.3.1 The Sleuth Kit (TSK)

Inclui um conjunto de ferramentas de perícia forense computacional baseadas em UNIX, usadas em linha de comandos, e tais ferramentas facilitam o perito na realização de um estudo não invasivo do sistema de arquivos de um computador suspeito, com estas ferramentas é possível ter acesso aos dados apagados ou escondidos. E as mesmas são maioritariamente suportadas por uma interface gráfica conhecida por *Autopsy Forensic Browser* (DOWLING, 2006).

Figura 6 - Autopsy apos ser adicionada a imagem.



Fonte: Sleuth Kit (2011).

2.5.3.2 The Coroner's Toolkit (TCT)

É um conjunto de ferramentas reunidas por *Wietese Venema* e *Dan Farmer*, peritos forenses reconhecidos, e elaborados segundo a combinação de duas linguagens de programação, *C e Perl*. Têm como objetivo ajudar o perito forense na análise de copias proveniente de sistemas possivelmente comprometidos. Estas ferramentas fazem uma análise profunda de modo a reconstruir ocorrências. De acordo com *Farmer e Venema* (2009) no *The Coroner's Toolkit*, existem as seguintes ferramentas:

a) ***GRAVE robber*** - colhe dados relevantes e guarda-os para uma posterior análise, executando diversos comandos;
b) ***mactime*** - cria uma linha de tempo que contém as últimas atividades realizadas em ASCII no sistema suspeito;
c) ***icat*** (Inode-cat) - através do Inode, ajuda na visualização do conteúdo de um arquivo ou diretório;
d) ***ils*** - faz a listagem dos vestígios removidos ou apagados;
e) ***md5*** – analisa a integridade de um aquivo gerado em *hash md5*;
f) ***pcat*** – captura processos na memória;
g) ***unrm*** – faz o Dump de espaços não alocados em um disco;
h) ***lazarus*** – recolhe os dados produzidos pela ferramenta Unrm, tentando criar alguma estrutura a partir de dados não estruturados;
i) ***timeout*** – realiza comandos com restrição de tempo.

Figura 7 - Comando Mactime em funcionamento.

```
Time         Size MAC Permission Owner Group File name
19:47:04    49152 .a. -rwsr-xr-x root  staff /usr/bin/login
            32768 .a. -rwxr-xr-x root  staff /usr/etc/in.telnetd
19:47:08      272 .a. -rw-r--r-- root  staff /etc/group
              108 .a. -r--r--r-- root  staff /etc/motd
             8234 .a. -rw-r--r-- root  staff /etc/ttytab
             3636 m.c -rw-rw-rw- root  staff /etc/utmp
            28056 m.c -rw-r--r-- root  staff /var/adm/lastlog
          1250496 m.c -rw-r--r-- root  staff /var/adm/wtmp
19:47:09     1041 .a. -rw-r--r-- root  staff /etc/passwd
19:47:10   147456 .a. -rwxr-xr-x root  staff /bin/csh
```

Fonte: Sleuth kit (2011).

2.5.3.3 Coleta de dados em dispositivos de memória

Os peritos forenses são auxiliados por ferramentas que recolhem evidências em computadores suspeitos, deste modo, estes softwares necessitam ser adquiridos e levados para o local da ocorrência. Na coleta de dados, para evitar problemas que possam vir a acontecer por incompatibilidade com os sistemas operacionais, ou inconvenientes que possam resultar em perda de tempo no processo de investigação, uma ótima opção preventiva neste caso é a otimização, utilizando ferramentas de *Live CD* Linux, que podem ser utilizadas sem que as precisar instalar (IEONG, 2006). Citando algumas destas ferramentas (RAMOS; SATURNINO et al., 2009):

a) ***dc3dd*** – cria imagens bit-a-bit de uma mídia;

b) **automated Image & Restore (*Air*)** - captura imagens com dd e dcfldd, determina o algoritmo hash e envia a imagem capturada via netcat ou cryptcat;

c) ***guymager*** – ferramenta que serve para a obtenção de imagens forenses, sendo possível destacar o seguinte:

   a) interface interativa, possuindo diversos idiomas,

   b) permite que se utilize mais núcleos de processamento,

   c) permite que novas unidades possam ser adicionadas a qualquer instante,

   d) funciona com o sistema operacional Linux;

e) ***Dc3ddgui*** – versão com interface gráfica do dc3dd, usado para a criação de imagem;

f) ***Memdump*** - efetua Dump de memória em sistemas UNIX;

g) ***Aimage*** – usa o padrão aff para a geração de imagens forenses;

h) ***Dd*** – gera imagem de dados;

i) ***Dcfldd*** – é uma versão do dd aprimorada pelo departamento de defesa dos Estados Unidos.

2.5.3.4 Análise de tráfego de rede

A perícia forense em rede é um mecanismo para busca e resposta de incidentes, como já definido, e existem algumas ferramentas para análise e coleta de dados:

a) ***ntop*** – ferramenta que possibilita a visualização em tempo real do trafego na rede;

b) ***xplico*** – distríbuido sob a licença *GNU* (*General Public License*), extrai os dados contidos em pacotes capturados na rede, como por exemplo os arquivos em formato *PCAP*, assim como a extração de conteúdos *HTTP,* informações de e-mails, *VOIP*, *TFTP*, *FTP*, entre outros;

c) ***xtraceroute*** – tem como função traçar rotas, é uma versão do *TRACEROUTE* em modo gráfico;

d) ***nmap*** – ferramenta de código livre para exploração e auditoria de segurança em rede, possibilita no escaneamento de redes de grande e pequeno porte, executado pela maioria dos sistemas operacionais como o *LINUX, Mac OS X* e o *Windows* (NMAP, 2009).

2.5.3.5 Identificação e Análise de arquivos

Abaixo estão descritas algumas das metodologias para a identificação e a análise de arquivos:

a) ***grisson analizer*** – por intermédio desta ferramenta pode-se executar comandos que fazem parte do Sleuth Kit para análise forense como fsstat, imgstat, Mml;

b) ***orange e cabextract*** – ambos acessam os conteúdos de arquivos com extensão .cab;

c) ***stegdetect*** – é uma ferramenta automatizada e tem como função detectar imagens que contenham pornografia;

d) ***rkhunter e Chkrootkit*** – tem como objetivo detectar a presença de rootkits no computador;
e) ***rifiuti*** – analisa arquivos *INF2*
f) ***grocevt e fccu*** – Evtreader – ajudam na visualização de arquivos de eventos provenientes do sistema Windows;
g) ***eindeutig*** – faz a análise de arquivos com extensão. *Dbx*;
h) ***regripper*** – esta ferramenta extrai e analisa dados do registro;
i) ***pyflag*** – é uma ferramenta para análise de grandes volumes de arquivos.

2.5.3.6 Recuperação de dados em disco rígido (HD)

Para a recuperação de dados em discos rígidos existentes no Helix modo LINUX (RAMOS; SATURNINO, 2009), destacamos algumas ferramentas:

a) ***recover*** – tem como função principal recuperar informações apagadas de inodes;
b) ***photorec*** – tem como objetivo recuperar arquivos de vários tipos, mas seu foco principal é recuperar arquivos de imagem e vídeo;
c) ***ddrescu*** – recupera os dados de uma partição para outra, efetuando uma cópia.
d) ***fatback, ntfsundelete, e2undel, scrounge-ntfs*** – recupera arquivos apagados em partições ext3, Ntfs;
e) ***testdisk*** – recupera partições geralmente quando ocorre algum tipo de erro específico ou problemas com vírus;
f) ***mondorestore*** – a sua função é restaurar informações de fitas, *CD's* ou *HD's*;
g) ***magicrescue*** – tem como função recuperar imagens raw;
h) ***jpgforemost, recoverjpg*** – recuperam, imagens no formato *jpg*.

2.5.3.7 Análise de arquivos temporários em navegadores

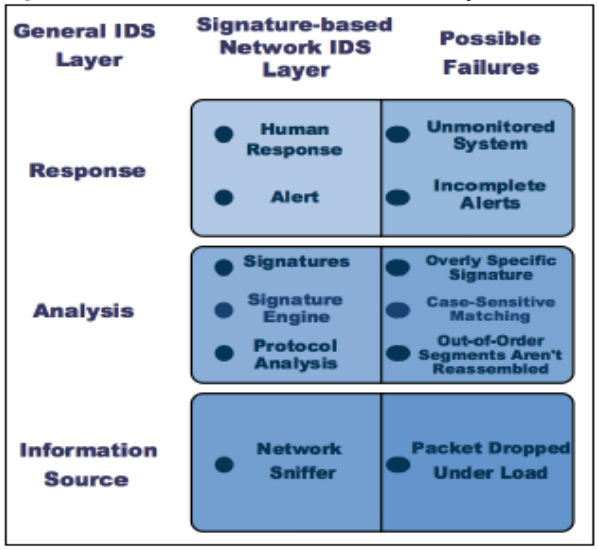
Para a análise de arquivos que provém de navegadores, são descritas abaixo algumas ferramentas:

a) ***pasco*** – é uma ferramenta que tem como função analisar a cache do Internet Explorer;
b) ***coockie_cruncher*** – realiza a análise de cookies de diversos navegadores;
c) ***mork*** – tem como função visualizar os arquivos history.dat do Firefox;
d) ***galleta*** – analisa cookies do Windows.

2.5.3.8 Sistema de detecção de intrusão (IDS)

Quando existem riscos de ocorrência de um provável incidente, que correspondem a violações ou ameaças iminentes de políticas de segurança de informação de uso aceitável ou de práticas de segurança comuns entram os *IDS*, que são sistemas que analisam e fazem o monitoramento de eventos realizados no computador ou na rede, para assim detectar possíveis intrusões (SCARFONE, 2007). Sendo a detecção uma das etapas mais importantes, é curiosamente a fase de menor controle para os profissionais experientes (MANDIA; PROSISE, 2003).

Figura 8 - Modelo de Sistema de Detecção de Intrusão e casos de falha.



Fonte: Skaion (2009).

Normalmente os incidentes são detectados quando algum responsável do grupo de segurança desconfia que um determinado evento ilegal, não autorizado ou inaceitável ocorreu ou está ocorrendo, envolvendo computadores, algum outro

equipamento de processamento ou a rede da organização (MANDIA; PROSISE, 2003).

2.5.3.8.1 Tipos de sistemas de detecção de intrusão (IDS)

De acordo com a *RED HAT*, muitos *IDS* baseiam-se em informações, usando um banco de dados que contenha informações dos ataques mais frequentes, para assim alertar antecipadamente os administradores de segurança. Os IDS também baseiam-se em comportamentos, e dos mesmos são realizadas buscas de anomalias que normalmente são sinais que comprovam a ocorrência de algum tipo de atividade perigosa, sendo que as *IDS* atuam de modo autônomo, majoritariamente em segundo plano e monitorando todas as atividades de maneira passiva, realizando um registro de todos os pacotes que são suspeitos na parte de fora do sistema. Os tipos de *IDS* mais conhecidos, são as que se baseiam em Redes e em Hosts, sendo os em Hosts tidos como o mais completo, e os em Rede são considerados como menos abrangentes. Detalhando cada um dos *IDS* segundo a *RED HAT* temos:

a) **IDS baseado em rede** – a maioria destes *IDS* tem como condição a definição do dispositivo de rede para modo indistinto, e a IDS baseada em rede examina detalhadamente pacotes da rede ao nível do Host ou roteador, o dado do pacote audita e registra todos os pacotes suspeitos nos arquivos especiais com dados extras, capturando os pacotes suspeitos e estes, por conseguinte serão comparados com os dados existentes em um banco de dados que contenha assinatura com os mais frequentes ataques, atribuindo um grau de inflexibilidade a cada um dos pacotes, e no caso se estes atinjam graus não frequentes será enviado um e-mail ao administrador para de modos a que seja feita uma investigação da essência da suposta anomalia;
b) **IDS baseado em host** – tem a possibilidade de consultar diversos tipos de *Logs*, como Servidor, *Firewall*, Rede, *Kernel* do sistema, entre outros tantos, facilita na análise de vários segmentos ajudando na determinação do indevido uso da rede, atividades suspeitas ou intrusões, são verificados também os arquivos executáveis, e os seus dados a fim de saber a sua veracidade, sendo estes arquivos

importantes em um banco de dados confidencial cria um *Checksum* para cada arquivo *MD5SUM* (Algoritmo de 128 bits), ou o *SHALSUM* (Algoritmo de 160 bits), seguidamente são armazenados valores em um arquivo de texto que será comparado periodicamente, e no caso de algum *CHECKSUM* não ser igual será enviado um alerta para o administrador por meio de um e-mail.

2.5.3.8.2 Ferramentas para detecção de intrusão

As ferramentas de *IDS* detectam atividades não autorizadas pelo administrador do sistema, também são usadas para análise de todos os pacotes que trafegam pela rede, principalmente aqueles suspeitos que são de imediato comparado com as assinaturas existentes (RAIMUNDO, 2006). Podendo citar algumas dessas ferramentas:

a) ***intruder alert*** – sistema de detecção de Intrusão baseado em Host, que detecta e monitora as violações de segurança em tempo real isso de modo automático. Após ser detectada uma ameaça o sistema ativa um alarme tendo em conta políticas de segurança determinadas, e no painel principal, podem ser implantadas diretrizes seguras para coleta e arquivamento de logs que seguidamente um auditor fará a análise, deixando o sistema sempre ativo e preservando a integridade dos seus dados (SYMANTEC, 2012).

b) ***realsecure*** – é um sistema de filtro contra intrusão, que protege a rede e sistemas, que estão conectados ou em missões críticas, e também protege a capacidade de processamento de pacotes, para garantir uma velocidade alta dos Links de rede, o tráfego quando circula na rede ou sistemas é analisado ao mesmo tempo procurando dados que põem em evidência possíveis ataques ou o mau uso. Os dados serão encapsulados num bloco que os manterá em quarentena, para que não passe para outra interface, isso no caso de serem identificadas anomalias (B2NET, 2011).

c) ***snort*** – é um moderno software de segurança, atuando como um Sniffer de pacotes, sistema de detecção de intrusão (*IDS*), ou como Packet Logger. Associado ao programa foi desenvolvido módulos

adicionais que adaptam diferentes modos para a manutenção de um conjunto de regras gerenciamento de logs arquivados, formas de gravação, alertando e permitindo deste modo que os seus administradores tenham conhecimento da sua presença de algum dado suspeito no tráfego (BAKER; CASWELL, 2004). Como Packet Lonngger o Snort, atua fazendo o registro de todos os pacotes no disco, como Sniffer, ele atua elaborando a leitura de todos aqueles pacotes que se encontram em tráfego na rede, e a parte aonde o Snort é mais completo e consequentemente tem uma configuração mais complexa, é como Detector de Intrusão, o qual efetua a análise do tráfego de rede, a partir de determinadas regras que são definidas pelo administrador de rede, e assim procurando por possíveis tentativas de invasão (SILVA, 2003).

d) ***asgaard*** – com métodos próprios para IDS, é um sistema com arquitetura baseada em formas modulares, que são distribuídas em vários computadores da rede e que têm conceitos diferentes, desde funções básicas como, análise de informações tidas como atividades finais até a autenticidade (CAMPELLO; WEBER, 2001).

O capítulo a seguir abordará sobre *Cloud Computing* seus tipos, vantagens, benefícios, os seus provedores, sua segurança e os problemas decorrentes da sua utilização.

3 CLOUD COMPUTING

Nas últimas décadas o mundo tem convivido com novas tendências tecnológicas, as empresas ao seu redor também têm sido impulsionadas pelas tecnologias de informação. A Internet tem sido o percursor de uma boa parte dessa mudança socioeconómica, e tem levado a mudanças em variados extratos, seja na forma como se comunicam, trabalham, estudam e até como se divertem, nesse segmento surge a *Cloud Cumputing* (LIMA, 2009).

A *Cloud Computing* ou computação em nuvens (tradução literal para o português), segundo o *National Institute of Standards and Technology* (NIST) é um modelo que possibilita acesso de modo conveniente e sob demanda a um conjunto de recursos computacionais configuráveis (por exemplo, redes, servidores, armazenamento, aplicações e serviços) que podem ser rapidamente adquiridos e disponibilizados com mínimo esforço gerencial ou interação com provedor de serviços (NIST, 2009).

Segundo Miller (2008), a *Cloud Computing* anuncia uma mudança importante na maneira como são armazenadas informações e executadas aplicações. Em vez de executarmos os programas e as informações em computadores individuais, tudo será armazenado em nuvem.

Algumas empresas têm feito da *Cloud Computing* um negócio válido e significativamente lucrativo na terceirização de serviços como uma solução aplicada aos seguintes fatores (IBM, 2012):

a) redução de custos – podem ser reduzidas as despesas de capital (CAPEX) e despesas operacionais (OPEX) porque os recursos somente serão adquiridos quando necessário e só são pagos quando usado;
b) uso refinado de pessoal – o uso da *Cloud Cumputing* permite reduzir o pessoal de manutenção de hardware e software, possibilitando o reenquadramento dos mesmos em outras áreas que agreguem outros valores a empresa;
c) escalabilidade robusta – ela permite o escalonamento imediato, para cima ou para baixo, a qualquer momento, sem compromisso de longo prazo.

A *Cloud Computing* é constituída em camadas e cada uma oferece níveis distintos de funcionalidades. Esta estratificação dos componentes da nuvem garante um meio para que as camadas tornem-se um bem como energia elétrica, serviço de telefone entre outros. A mercadoria que ela vende é o poder de computação a um custo menor e com isso, poucas despesas para o usuário. Ela está pronta para se tornar o próximo serviço de mega utilidade (IBM, 2012).

Michael J. Flynn classificou a arquitetura computacional de acordo com o processamento do fluxo de instrução e de dados e chamou-lhe de taxonomia de Flynn, e fazem parte dela (FERRÃO; PLOTZE, 2012):

a) ***single instruction single data (sisd) –*** em português é o fluxo único de instruções sobre um único conjunto de dados, é um modelo tradicional simples de uniprocessamento ou monoprocessamento, no qual são executada uma por vez as instruções de um programa. Ele pode ser aplicado por computadores pessoais com um único processador convencional;

b) ***single instruction multiple data (simd) –*** em português fluxo único de instruções em múltiplos conjuntos de dados, é uma arquitetura de multiprocessamento que executa o processamento da instrução em diferentes itens de dados. Este modelo é muito usado para tratamento de conjuntos regulares de dados como as matrizes e os vetores;

c) ***multiple instructions single data (misd) –*** em português fluxo múltiplo de instruções em um único conjunto de dados, é uma arquitetura de multiprocessamento cujo processamento de dados é efetuado em múltiplas unidades de processamento e cada uma delas executa de maneira independente as instruções. Este modelo é usado em computadores que executam algoritmos de criptografia para tentar quebrar uma mensagem codificada ou arquiteturas de processamento distribuído.

Nas novas arquiteturas são usadas à taxonomia de *Flynn*, e a *Cloud Computing* não é diferente, pois ela funciona como uma arquitetura de computação distribuída.

3.1 COMPUTAÇÃO DISTRIBUÍDA

Computação distribuída ou sistemas distribuídos são um conjunto de computadores independentes que se apresentam ao usuário como um sistema único e consistente (STEEN; TANENBAUM, 2007).

Os sistemas distribuídos têm como uma de suas características importantes, as diferenças entre os diversos computadores e o modo como eles se comunicam, estes estão, em grande parte oculto ao usuário e do mesmo modo acontece com a organização interna do sistema distribuído. Outra característica é que os usuários e as aplicações podem interagir com o sistema distribuído de maneira uniforme e consistente, independentemente de onde a interação partir ou ocorrer (TANEMBAUM, 2007).

O sistema distribuído tem como meta principal facilitar os usuários e as aplicações, ao acesso a recursos remotos e seu compartilhamento de maneira eficiente e controlada. Existem hoje varias razões para se compartilhar recursos, e uma delas é a economia (TANEMBAUM, 2007).

3.2 MODELOS DE IMPLANTAÇÃO DE CLOUD COMPUTING

Segundo o princípio de computação em grade (*Grid*) a *Cloud Computing* ou computação em nuvem é a utilização da memória e das capacidades de armazenamento e cálculo de computadores, softwares compartilhados e conectados por meio de uma rede (SISNEMA, 2009).

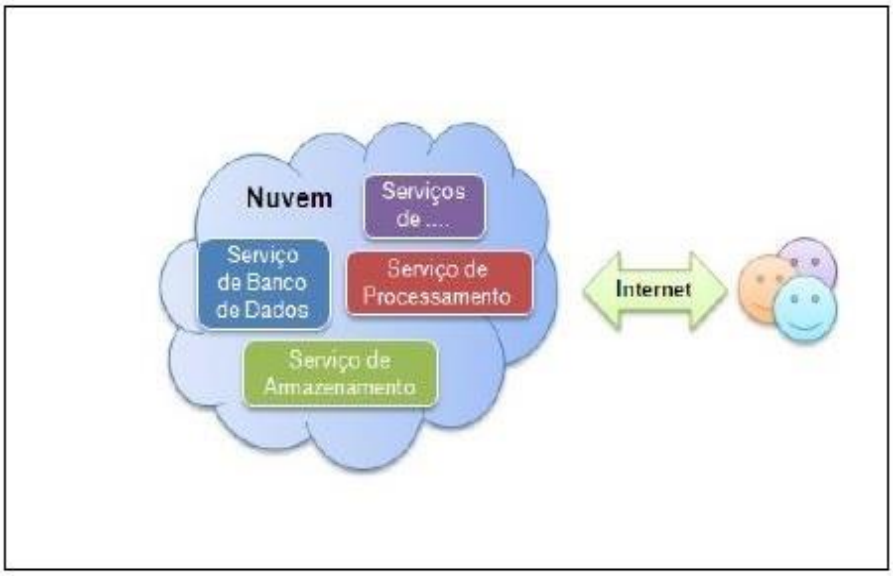
Na *Cloud* os dados são armazenados em serviços que podem ser acessados de qualquer parte do mundo, a qualquer hora e sem haver a necessidade de instalar um banco de dados ou qualquer software, o seu acesso é feito por meio de uma rede privada ou pela Internet (de onde surge a denominação nuvem do inglês *Cloud*) viabilizando o seu uso comparado com o uso de servidores como unidade principal (NUBLING, 2011).

Existem disponíveis quatro modelos para se implantar uma *Cloud Computing*, eles estão classificados como *Cloud* Híbrida, *Cloud* Pública, *Cloud* Privada e *Cloud* Comunitária.

3.2.1 Cloud pública

A *Cloud* Pública (Figura 9) é um conjunto de hardware, redes, armazenamento, serviços, aplicações e interfaces, operados por terceiros para uso de pessoas ou empresas. Nela não podem ser aplicadas restrições de acesso no que concerne ao gerenciamento de redes, também não podem ser utilizadas técnicas para autenticação e autorização (NUBLING, 2011; SOUSA, 2011).

Figura 9 - Cloud pública.



Fonte: Borges et al (2010).

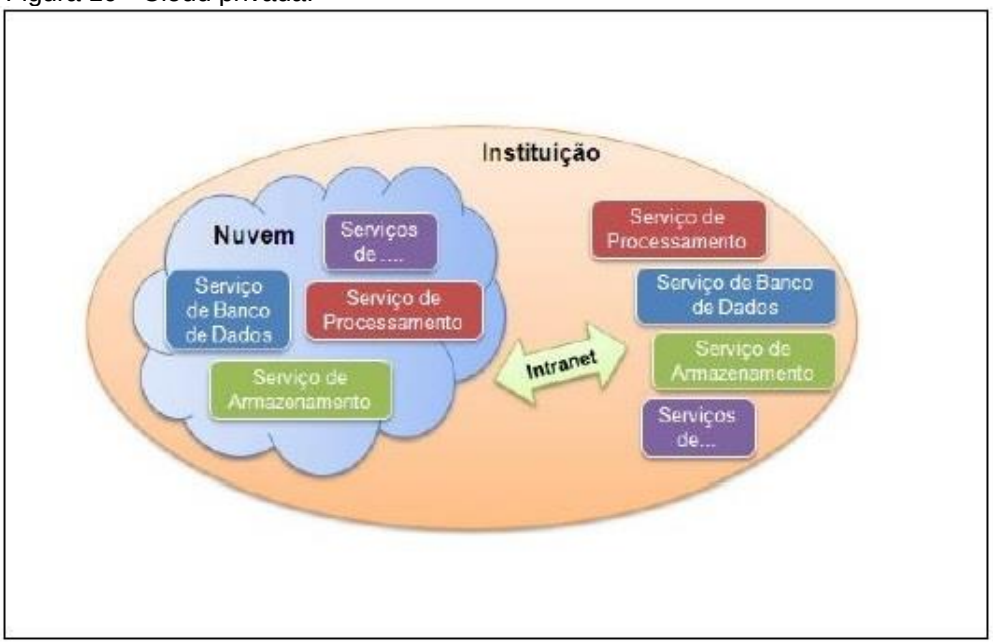
Este tipo de serviço tem sido muito utilizado desde 2010 por ser mais econômico em termos de custos e também porque os únicos custos são baseados na capacidade em que é usada. A *Cloud* pública tem algumas limitações, porém devem-se saber quais as reais necessidades e se são atendidas por esta estrutura.

3.2.2 Cloud privada

O modelo *Cloud* Privada (Figura 10) tem como base arquiteturas de Data Center que são propriedade de uma única empresa que oferece escalabilidade, flexibilidade, provisionamento, monitoramento e automação. O seu objetivo não é a venda de serviços para clientes externos e sim ter os benefícios de uma nuvem sem abrir mão do controle de administrar os seus próprios dados.

Segundo Taurion (2009), algumas características que diferenciam as nuvens privadas são o fato das restrições de acesso, pois ela encontra-se atrás do firewall da empresa, sendo uma forma de aderir à tecnologia e beneficiando-se das suas vantagens, porém mantendo o controle do nível de serviço e aderência às regras de segurança da instituição.

Figura 10 - Cloud privada.



Fonte: Borges et al. (2010).

Neste tipo de modelo empregam-se políticas de acesso aos serviços e para prover os serviços são usadas técnicas em nível de gerenciamento de redes, configurações dos provedores de serviços e utilização de tecnologias de autorização e autenticação (NUBLING, 2011; SOUSA, 2011).

3.2.3 Cloud híbrida

A *Cloud* Híbrida (figura 11) é a combinação de uma *Cloud* Privada com o uso de alguns serviços da *Cloud* Pública, nela podem existir um ou mais pontos de contato entre os ambientes. Tem como objetivo combinar serviços e dados de uma gama de modelos de *Cloud* a fim de se criar um ambiente de computação unificada, automatizada e bem gerenciada (NUBLING, 2011).

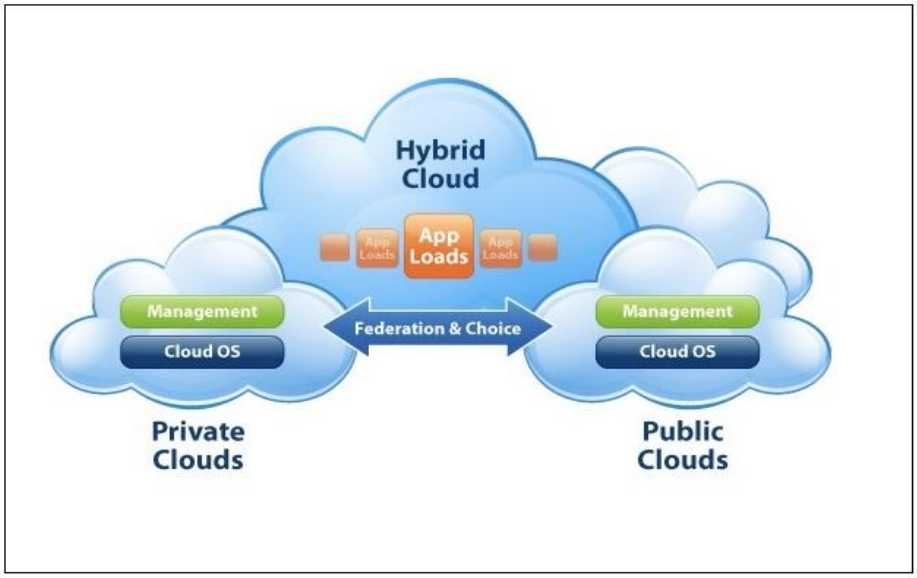
Ela é definida como a nova Computação Corporativa, por combinar os serviços públicos com as nuvens privadas tendo no centro de dados um sistema hibrido. Uma *Cloud* é Hibrida se (SOUSA, 2011):

a) for usada uma plataforma de desenvolvimento pública que envie dados para uma nuvem privada ou uma aplicação baseada no centro de dados;
b) for usada uma série de *SaaS* e aplicativos que movam os dados entre os recursos privados ou de *Data Center*;
c) um processo de concedido como um serviço para que ele possa conectar-se com outro ambiente como se fosse um único ambiente.

Uma *Cloud* não é hibrida se:

a) for usado um serviço de nuvem pública para o protótipo de um novo aplicativo que não está conectado a uma nuvem privada ou a um centro de dados;
a) no uso de um aplicativo *SaaS* para um projeto, não ocorrer nenhum movimento de dados partindo dessa aplicação para um centro de dados.

Figura 11 - Cloud híbrida.



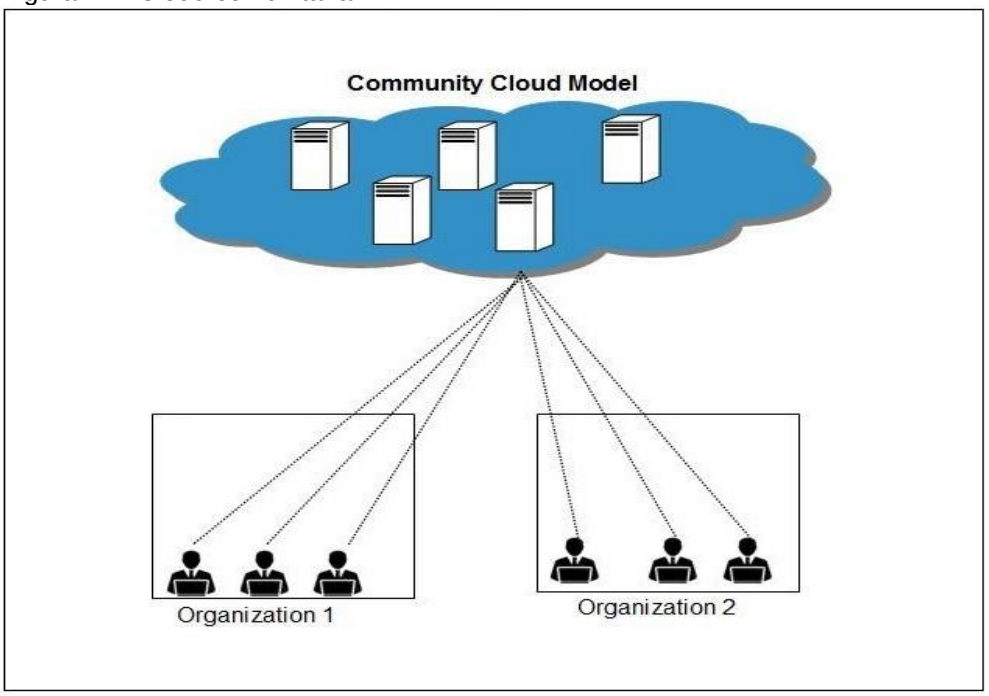
Fonte: Virtualization Practice (2013).

3.2.4 Cloud comunitária

Na *Cloud* Comunitária (Figura 12) a sua infraestrutura é compartilhada com variadas entidades de uma determinada região ou comunidade com

preocupações comuns como jurisdição, segurança, conformidade, entre outros. Este modelo pode ser gerenciado por uma empresa local ou por terceiros e hospedado internamente ou externamente (SOUSA, 2011).

Figura 12 - Cloud comunitária.



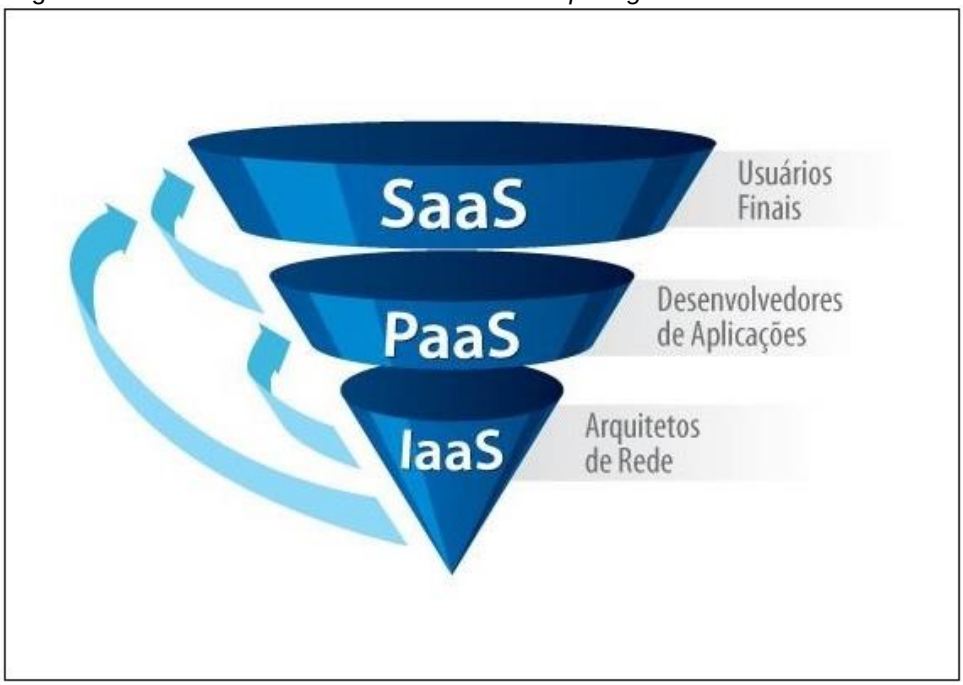
Fonte: Tutorialspoint (2013).

3.3 MODELOS DE SERVIÇO DE CLOUD COMPUTING

Existem hoje diversos modelos de serviço de *Cloud Computing*, tal diversidade é benéfica, pois ela permite que a empresa ou pessoa possa adquirir o serviço que melhor se adequa as suas necessidades (TAURION, 2009).

A arquitetura de *Cloud Computing* segundo algumas literaturas, é dividida em três camadas distintas que são a *IaaS, PaaS, SaaS* (Figura 13). Estas camadas podem ter seu monitoramento ou gerenciamento independentes das demais camadas, garantindo maior escalabilidade, flexibilidade e reutilização no que diz respeito à adição ou substituição de recursos computacionais sem interferir ou afetar as demais camadas (SOUZA, 2009).

Figura 13 - Camadas do modelo de *Cloud Computing*.



Fonte: Added (2014) e Souza (2009).

3.3.1 Infraestrutura como serviço (IaaS)

A *Infrastructure as a Service* (*IaaS*) pertence a camada mais baixa e estrutural que é fundamental para o funcionamento de *Coud Computing*, representando toda arquitetura física como *Data centres*, servidores, hardwares e equipamentos de energia e climatização, que possibilitam e garantam o armazenamento e a transmissão de dados e aplicações de maneira rápida por intermédio da Internet (ADDED, 2013). Ele possibilita o acesso a recursos fundamentais, como armazenamento virtual, máquinas virtuais, máquinas físicas, endereço de IP, pacotes de *softwares*, rede local virtual, armazenamento em disco de máquina virtual, entre outros (TUTORIALSPOINT, 2013).

Existem inúmeras vantagens na utilização de *IaaS,* porém as que mais se destacam são:

a) custo operacional imutável, ele pode ser cobrado pela utilização e possivelmente por mensalidade;
b) o provedor é responsável pela manutenção e suporte;
c) economia de tempo e dinheiro na gestão de TI;
d) aumento da produtividade da equipe de trabalho;

e) baixo número de *downtime* em computadores ou equipamentos de rede;
f) possibilita a evolução tecnológica dos equipamentos e sistemas de rede necessários para o crescimento da empresa;
g) maior previsão de investimentos futuros para o ambiente de TI;
h) custo zero no investimento de infraestrutura, pois o provedor é responsável por isso.

3.3.2 Plataforma como serviço (PaaS)

A *platform as a service* (*PaaS*) é a segunda camada do modelo, ela é muito utilizada pelos desenvolvedores de aplicações, que aproveitando as bases do IaaS são criadas soluções e recursos necessários para suporte de segurança, sistemas operacionais, escalabilidade, organização de banco de dados e armazenamento (ADDED, 2013).

O PaaS tem como suas maiores características oferecer um ambiente de desenvolvimento baseado em navegadores, ferramentas de serviço web, fluxo de trabalho e processos de aprovação, interação com aplicações da mesma plataforma (TUTORIALSPOINT, 2013).

Existem algumas vantagens para se utilizar o *PaaS* e elas são:

a) maior segurança e disponibilidade;
a) maior agilidade no suporte;
b) as atualizações são disponibilizadas gratuitamente;
c) menor Investimento inicial.

3.3.3 Software como serviço (SaaS)

O *software as a service* (*Saas*) é um modelo que permite fornecer um software como um serviço para os usuários finais, ele é um software que é implantado em um serviço hospedado, acessado via Internet e as atualizações são por conta dos fornecedores (TUTORIALSPOINT, 2013). Existem vários módulos *SaaS,* os mais usuais são os módulos de Finanças e faturamento, Recursos Humanos (RH), *Help Desk* e o *Customer Relationship Management* (CRM). (FREITAS; OLIVEIRA, 2010).

As vantagens de se usar um modelo *SaaS* são:

a) não são necessárias licenças;

b) o gerenciamento é centralizado;

c) as atualizações e novas versões são por conta do provedor;

d) baixo custo de distribuição.

Podem ser encontrados módulos *SaaS* que permitem ao usuário personaliza-los ao seu gosto e estilo, um exemplo é o *Office Suite*, porém o *SaaS* disponibiliza *API´s* que possibilitam ao desenvolvedor criar um aplicativo personalizado.

3.3.4 Plataformas e modelos de serviço

Na figura 14 são ilustradas algumas plataformas implementadas com base nos modelos *IaaS, PaaS e SaaS*, definidos anteriormente.

Figura 14 - Modelos de serviços e suas plataformas.

Modelo	Exemplos
IaaS	Eucalyptus
	Amazon AWS EC2
	OwnCloud
	Windows Azure
PaaS	Aneka
	Windows Azure
	Google App Engine
	Amazon AWS EC2
SaaS	Mail Live Office
	CRM(Customer Relationship Management) da Sales Force
	Google Docs

Fonte: Adaptado de Freitas e Oliveira (2010).

3.4 SEGURANÇA NOS AMBIENTES CLOUD COMPUTING

A segurança é uma das maiores preocupações no novo mundo tecnológico, e a *Cloud Computing* não foge a regra, uma pesquisa feita pela

Associação Brasileira de *E-business* onde 222 empresas de médio e grande porte foram ouvidas, 39% delas apontou a segurança como uma das maiores preocupações (FERNANDES, 2010).

As pessoas e principalmente as grandes corporações são céticas quanto até que ponto suas informações estão seguras, este ceticismo deve-se pelo simples fato de não se saber qual o lugar físico que suas informações estão alojadas e qual a política do país no que concerne ao sigilo da informação (CASTRO, 2010).

A segurança sempre deve ser vista como uma preocupação, independentemente do sistema ou plataforma que o usuário usa, os cuidados devem partir na compra ou contratação do serviço, devem ser feitas pesquisas e estudos sobre as políticas de segurança que o produto e a empresa oferecem para se garantir uma melhor prestação de serviço e para que não haja problemas quanto à evasão de informações confidenciais e entre outros.

Nas camadas dos modelos *Cloud Computing* os problemas com segurança variam mediante o controle sobre o hardware que cada uma tem. Na camada de *IaaS* tem-se um total controle sobre o hardware que lhe é atribuído, porém não é possível acessar diretamente o hardware da máquina. O *PaaS* não é muito diferente da *IaaS* no quesito segurança, ele não tem controle sobre o hardware da máquina, só lhe são atribuídas permissões referentes a configurações de ambiente e instalações de softwares. O *SaaS* é a camada que não tem acesso a qualquer controle sobre a máquina, a única permissão é a de customização em cima de uma aplicação (FREITAS; OLIVEIRA, 2010).

3.4.1 Ameaças e riscos em ambientes Cloud Computing

É prudente que os usuários façam primeiramente a avaliação dos riscos e as opções de segurança e só depois decidam mover seus sistemas e aplicativos para ambientes de *Cloud Computing*. É pertinente que se avalie quais os dados e serviços podem ser transferidos para ambientes externos no caso de uma Cloud pública. Ela suporta aplicações, dados, serviços e processos e são chamados de tipos de ativos, eles podem ou devem ser analisados quando se pretende determinar qual a sua importância para a organização. O processo de análise visa avaliar os impactos causados caso um ou mais requisitos de segurança sejam comprometidos. Os usuários têm a possibilidade de mover os seus dados ou processos para os

ambientes *Cloud Computing* de modo integral ou parcial, podendo ser mantidas em ambiente privado dentro do perímetro da organização parte dessas transações e informações (CSA, 2009; LAUREANO, et al., 2010).

Em sua maioria, os controles de segurança em *Cloud Computing* são iguais aos de outros ambientes de TI. Todavia, os seus modelos de serviço (*IaaS, PaaS e SaaS*), e os modos de operação, administração e tecnologias usadas para prover os seus serviços, podem eventualmente apresentar distintas ameaças para as organizações (LAUREANO, et al., 2010).

Segundo o Cloud Security Alliance 2009 (CSA), um ambiente *Cloud Computing* pode ter dois domínios de segurança, eles podem ser operacionais ou administrativos:

a) domínio operacional: nele os procedimentos são usados visando marter a segurança dentro da arquitetura;
b) domínio administrativo: nele são abordados os aspectos de gestão e proteção de dados sensíveis, ações legais por violação de contrato.

Métodos para detectar incidentes e aprovisionar notificações, podem ser definidos com a abordagem de mecanismos que quando implantados nos níveis do provedor e do cliente, possibilitam a avaliação e o tratamento adequado de incidentes, podendo ser usada a perícia forense digital (LAUREANO, et al., 2010).

As empresas provedoras das *Cloud Computing* têm investido muito no quesito segurança, porém a melhor alternativa para quem tem informações confidenciais ou de valor imensurável, é criar o seu próprio mecanismo de segurança, garantindo que só ele tenha acesso às informações.

3.5 BENEFÍCIOS DA CLOUD COMPUTING

A *Cloud Computing* além dos recursos de tecnologia de informação oferece muitos benefícios aos seus usuários. Vivek Kundra *CIO* do governo dos Estados Unidos de 2009 a 2011 abordou sobre os benefícios que as repartições federais norte americanas teriam com a utilização da *Cloud Computing*, destacando três dos que ele chamou de postos-chave, eles são: inovação, agilidade e eficiência. (KUNDRA, 2011). Esta abordagem serviu e vem servindo para motivar não só as repartições federais norte americanas, mas também para empresas públicas,

privadas e administrações de outros países a aderirem esta tecnologia como um novo modelo de gestão.

Alguns dos benefícios oferecidos pela *Cloud Computing* são (OPEN GROUP, 2011):

a) flexibilidade;
b) melhor manutenção e administração;
c) menor Custo;
d) Menor tempo de provisionamento (implantação de novos serviços mais rápida).

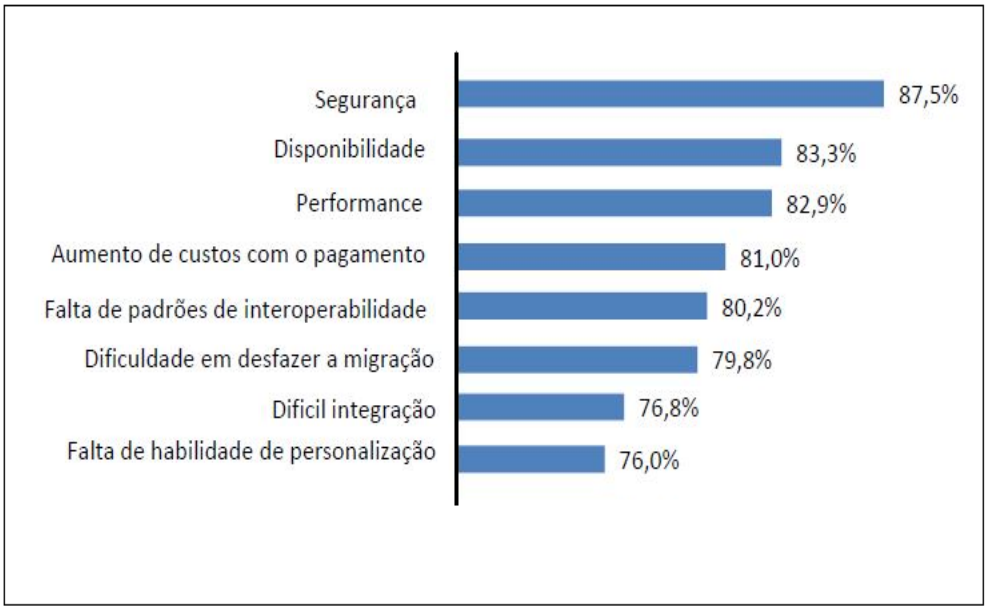
3.6 DESAFIOS E PROBLEMAS DA CLOUD COMPUTING

Toda tecnologia tem os seus desafios o que por muitos são vistos como problemas, muitos deles são criados pelas instituições que escolhem usar esta tecnologia e têm dentro do seu núcleo, pessoas com uma determinada resistência a novas tecnologias e por outro, pelo fato do modelo escolhido não satisfazer todas as suas necessidades. Abaixo são listados alguns desafios segundo o Open Group (2011):

a) integração;
b) acesso aos dados;
c) ausência de definição clara nos componentes das ferramentas;
d) falta de experiência;
e) pouca maturidade da tecnologia.

Uma pesquisa elaborada pela revista *IDC exchange*, permitiu traçar um gráfico dos desafios da *Cloud Computing*. Na pesquisa foram entrevistados 263 executivos de *TI* com a seguinte pergunta: “Quais os pontos fracos ou mais preocupantes da *Cloud Computing?*”, a pesquisa apontou que entre outros a segurança lidera o ranking com 87,5% (DIDONÉ; QUEIRÓZ, 2011; IDC, 2011).

Figura 15 - Imagem do Gráfico sobre os desafios da *Cloud Computing*.



Fonte: Adaptado de Didoné (2011).

3.7 ALGUMAS FERRAMENTAS PARA CRIAÇÃO E GERENCIAMENTO DE CLOUD COMPUTING PRIVADA (IAAS)

Nos últimos anos muitas empresas viram na *Cloud Computing* uma oportunidade real de levar uma filosofia diferente das demais, inovando e investindo em ferramentas para o usuário criar a sua própria nuvem e administrá-la com segurança, desempenho e baixo custo. Elas foram desenvolvidas pensando nos usuários que necessitam de maior independência na gestão e manuseio dos seus dados. Neste capítulo serão abordados quatro provedores de serviço de *Cloud Computing* privada, pois eles destacam-se dos demais pelas suas características e pelo número crescente de usuários que a aderem.

3.7.1 Eucalyptus

Eucalyptus é a sigla que define *Elastic Utility Computing Architecture for Linking Your Programs To Useful Systems, é um projeto que teve o seu começo na universidade da Califórnia* no departamento de Ciência da Computação, hoje ele é comercializado e desenvolvido como um software livre, oferecendo uma infinidade de recursos (SOUZA, 2009).

O *Eucalyptus* dispõe de uma infraestrutura *open source* fornecendo ainda uma interface compatível com algumas interfaces como a *Amazon Elastic Compute Cloud* (*EC2)*, *Simples Storage Service (S3)* e *Elastic Block Storage* (*EBS*), permite também ser compatível com outras interfaces por intermédio de uma infraestrutura que foi desenvolvida para permitir essas mudanças (SOUZA, 2009).

Projetado para ser uma ferramenta de fácil manuseio, ela conta com cinco componentes primordiais para o seu gerenciamento na *cloud*, exercendo cada um deles a sua função. Uma de suas características é de permitir que seus componentes de gerenciamentos sejam separados em vários servidores, o que torna esses processos de administração da *cloud* pouco dispendioso para os seus controladores (LOUREIRO; MACHADO, 2011).

3.7.2 Amazon AWS EC2

A *Amazon Elastic Compute Cloud* (*Amazon EC2*) é uma ferramenta que disponibiliza aos seus usuários uma capacidade escalável na nuvem *Amazon Web Service (AWS),* permitindo o controle total sobre os recursos computacionais, como criação de instâncias de servidores em pouco tempo, configurar a segurança e networking, gerenciar a unidade de armazenamento, e entre outros, suprimindo assim a necessidade do usuário investir em hardware (AMAZON, 2014).

A *amazon aws (EC2)* disponibiliza os seguintes recursos (AMAZON, 2014):

a) ambientes de computação virtual;
b) modelos pré-configurados para suas instâncias, conhecidos como *Amazon Machine Images* (AMIs);
c) inúmeras configurações de CPU, memória, armazenamento e capacidade de rede para suas instâncias;
d) todas as informações de *login* seguro para suas instâncias, utilizando pares de chaves (AWS armazena a chave pública, e você armazenar a chave privada em um local seguro);
e) inúmeros locais físicos para seus recursos, como instâncias e volumes do *Amazon EBS*, conhecidas como regiões e zonas de disponibilidade;

f) um *firewall* que permite que o usuário especifique os protocolos, portas e faixas de *IP* de origem que podem chegar a suas instâncias usando grupos de segurança;
g) endereços *IP* estáticos para a computação em nuvem dinâmica;
h) metadados, conhecida como *Tag*;
i) redes Virtuais.

3.7.3 OwnCloud

O *Owncloud* é uma ferramenta de software livre desenvolvida por *Frank karlitschec* em 2010, que permite ao usuário criar a sua própria *Cloud* com área de armazenamento de dados, visualização, opção de sincronização e compartilhamento de arquivos. Ele destaca-se das outras ferramentas, pois nele o usuário tem o máximo de controle e acesso aos seus dados, sendo possível criar um servidor privativo (Linux ou Windows) garantindo maior segurança, ele também é multiplataforma isso é seu arquivo podem ser acessados ou sincronizados pelas plataformas Windows, Linux, Mac OS, Android, IOS e entre outras (KARLITSCHEC, 2014; OWNCLOUD, 2014).

3.7.4 OpenNebula

O *OpenNebula* é uma ferramenta *open source* mantido pela comunidade e por diversas empresas colaboradoras que permite a criação e o gerenciamento de *Cloud Computing,* tendo também a função de gerenciamento e visualização de infraestruturas de servidores (*data centers*) ou *cluster* para *cloud* privada, bem como suporta *cloud* hibrida que funcione com infraestruturas locais ou baseadas *cloud* Pública, proporcionando um melhor ambiente para hospedagem. A ferramenta também possibilita criar e gerenciar *cloud* Pública, por intermédio de recursos que possibilitam a criação de máquinas virtuais (VM), armazenamento e gerenciamento de rede (BONINI; OLIVEIRA JUNIOR, 2011).

3.7.5 Nimbus

O *Nimbus* é uma ferramenta *open source* que possibilita a criação de nuvens privadas, comunitárias e públicas, que foi desenvolvida com o objetivo de suprir as necessidades da comunidade científica, ele conta com serviços para um gerenciamento mais flexível. O Nimbus conta também com *Workspace Service* que da aos usuários um sistema de compartilhamento de recursos computacionais e conta com implementação de *VMs,* que dá a possibilidade do usuário criar uma nuvem de armazenamento, e o gerenciamento de configurações de segurança é prestado pelo *Nimbus broker* (DIDINÉ, 2011).

Após algumas pesquisas é possível fazer uma comparação das ferramentas de criação e gerenciamento de *cloud* Privada (Quadro 1). Para tal, seguimos como base para escolha das ferramentas a maior independência do usuário, abrindo a possibilidade do mesmo ter todos os benefícios de uma *Cloud* privada.

Quadro 1 - Tabela comparativa das ferramentas de gerenciamento de *Cloud Computing*.

Ferramentas	Linguagem de Desenvolvimento	Empresa	Sistema Operacional	Licença	Open Source
Nimbus	*Python, Java*	*Nimbus Comunity*	*Linux*	*Apache license v2*	Sim
OpenNebula	*Java, Shell Script, Lex, Yacc, C++, C*	*OpenNebula Comunity*	*Linux*	*Apache license v2*	Sim
Owncloud	*PHP, JavaScript*	*Owncloud*	*Linux, Windows, OS X*	*AGPLv3*	Sim
Eucalyptus	*Java, C*	*Eucalyptus Systems*	*Linux*	*GPL V3*	Sim

Fonte: Adaptado de Bonini (2011).

Os dados referenciados no quadro 1 fazem uma demonstração clara de que as quatro ferramentas têm ótimos requisitos, entre eles é visível a preocupação das empresas em desenvolver as aplicações com linguagens de programação compiladas por *bytecode* isto é, linguagens interpretadas por uma máquina virtual (VM) possibilitando que os softwares sejam independentes de plataforma ou seja, podem ser criadas máquinas virtuais para cada plataforma garantindo assim que o software seja multiplataforma. A licença de uso livre e a possibilidade de acesso ao

código para melhoria do software pelo usuário, também foi uma preocupação das empresas desenvolvedoras das ferramentas, quebrando assim todos os dogmas e ceticismos muito comuns em ferramentas *SaaS*.

3.8 ALGUNS SERVIÇOS CLOUD COMPUTING PÚBLICA (SAAS)

Existem hoje no mercado diversas empresas que oferecem o serviço de *Cloud Computing* pública Software como Serviço, oferecendo uma gama de recursos aos seus contratantes. Neste subcapítulo serão definidos alguns provedores de *cloud* pública.

3.8.1 DropBox

O *Dropbox* é uma ferramenta SaaS que permite o armazenamento de arquivos na *cloud,* possibilitando compartilhar os mesmos com diversos usuários. Desenvolvido na linguagem *Python* em 2007 por *Drew Houston* e *Arash Ferdowsi* (ambos são ex-alunos do Instituto de Tecnologia de Massachusetts MIT), surgiu da necessidade de manter os dados disponíveis a qualquer hora e em qualquer lugar, dependendo apenas de uma conexão de Internet. O dropbox já conta com mais de 300 milhões de usuários e os seus serviços estão disponíveis para as plataformas *Mac OS X, Linux, Microsoft Windows, IOS, Android, BlackBerry OS, Windows Phone, navegadores, Meego, Symbian*, oferecendo aos seus usuários de 2 a 5 GB grátis e caso o usuário necessite de mais espaço terá de pagar pelo mesmo (DROPBOX, 2014).

3.8.2 OneDrive

O *OneDrive* (anteriormente denominado *SkyDrive*), é uma ferramenta *SaaS* criada pela *Microsoft* em 2008 que permite o armazenamento e hospedagem arquivos na *Cloud* desde que o usuário tenha uma conta Microsoft de e-mail. O *oneDrive* oferece ao usuário 15 Gb de espaço gratuitos e apenas permite que o mesmo faça upload de arquivos que tenham no máximo 50 MB, ele é compatível com as plataformas *Windows, Linux, Mac, iOS, Android*, Navegadores, entre outros, e tem funcionalidades como galeria de fotos que suportem os arquivos com formatos

digitais e *Zip*, *Slide Show*, *Tags* e conta também com o pacote *Office online* integrado (MICROSOFT, 2014).

3.8.3 Google drive

O Google Drive é uma ferramenta *SaaS* desenvolvida pela Google em 2012, que permite armazenar e sincronizar arquivos, oferecendo aos seus usuários 15 Gb grátis e uma diversidade de recursos como o acesso ao *Google Docs*, integração com os serviços do Google, entre outros, ele também é compatível com as plataformas *Windows, Mac, Android, iOS*, navegadores, entre outros, e suporta mais de 30 tipos de arquivos (GOOGLE, 2014).

Mediante aos dados apresentados, é possível fazer uma comparação dos serviços de *Cloud Computing* pública (*SaaS*) (Quadro 2). Para realização deste quadro, foram escolhidos os seguintes quesitos: capacidade de armazenamento gratuito, capacidade máxima de armazenamento, limites de tamanho dos arquivos, aplicativos para plataformas, compartilhamento, integração de outros aplicativos e streaming de mídia.

Quadro 2 - Tabela comparativa de Alguns serviços de e *Cloud Computing* pública (SaaS).

Capacidade de Armazenamento	Capacidade Máxima de Armazenamento	Limite de Tamanho dos Arquivos	Aplicativos para Sistema Operacional	Compartilhamento de Arquivos	Integração de Outros Aplicativos	Streaming de Mídias.
Google Drive	15 GB	10 GB	Android, IOS, Mac OS, Windows.	Sim	Sim	Sim
OneDrive	15 GB	2 GB	IOS, Mac OS, Windows, Windows Phone.	Sim	Sim	Sim
DropBox	2 GB à 18 GB	2 GB	Android, BlackBerry, IOS, Linux, Mac OS, Windows.	Sim	Sim	Não

Fonte: Adaptado de Tecmundo (2014).

O capítulo a seguir abordará mais sobre *Cloud Computing* bem como a perícia forense nesses ambientes e os desafios existentes na sua realização.

4 PERÍCIA FORENSE EM AMBIENTES CLOUD COMPUTING

Quando se fala de *Cloud Computing* logo surge os seus prós e os seus contras. Os seus benefícios são variados entre eles estão flexibilidade, baixo custo de manutenção, administração, implantação e menor tempo na implantação de novos serviços, porém os seus desafios também despertam o ceticismo dos usuários dessa nova ferramenta da computação contemporânea. A despeito da descrença, este ambiente continua a crescer, inovar e conquistar setores importantes da sociedade em todo o planeta.

A *International Data Comporation* (*IDC*) tem levado a frente uma série de estudos em torno da *Cloud Computing*, e um de seus estudos prevê que a fatia de mercado da *cloud* pública em 2015 será de aproximadamente 177 bilhões de dólares, já a privada terá um faturamento de aproximadamente 73 bilhões de dólares, demostrando um crescimento de 331,82% comparados aos 22 bilhões de dólares faturados em 2010. Esses dados demonstram um notório crescimento dessa modalidade de serviço apontando-a como uma clara tendência de mercado (DIDONÉ, 2011; IDC, 2011).

Já não é novidade que indústria de *Cloud Computing está* em alta, porém a novidade está na demanda destes serviços pelas empresas de grande, médio e pequeno porte, tal procura por esses serviços está muito incidente na Europa, e ela dá-se em grande escala nos países mais conservadores como Inglaterra, Alemanha, Espanha, Itália, França, entre outros, que poderão ganhar aproximadamente 763 bilhões de Euros até 2015, com esta inovadora tecnologia (EMC², 2011).

Não obstante aos números que são satisfatórios, esta tecnologia ainda tem inúmeros desafios que precisam de um maior engajamento da indústria tecnológica para ultrapassá-los. A perícia nesses ambientes é vista por muitos especialistas de TI não só, como um dos maiores desafios, pois envolvem questões técnicas, legais e organizacionais, o que faz com que surjam alguns questionamentos quanto ao modelo que será implantado, se estará na própria nuvem (*Cloud Forensics*), ou será desenvolvido outros mecanismos para realizar a perícia (DIDONÉ, 2011; DYKSTRA, 2012).

4.1 CLOUD COMPUTING FORENSIC

A NIST (2014) define a *Cloud Computing Forensic* como a aplicação de princípios científicos, tecnológicos, prática derivada de métodos para reconstruir eventos passados ou informações apagadas de uma nuvem, por meio de identificação, coleta comprovada, preservação, análise, interpretação e elaboração de relatórios de evidências digitais.

Segundo Ruan (2013), a *cloud forensics* é a aplicação da ciência forense digital em modelos de *Cloud Computing*, tratando como se fosse uma abordagem híbrida forense da rede *in* vivo e em grande escala para obter as evidências digitais.

Ruan (2013) propôs a definição da *cloud forensic* como a aplicação da tecnologia digital forense em *Cloud Computing* como um subconjunto da rede forense, mostrando os passos para a localização da *cloud forensic*:

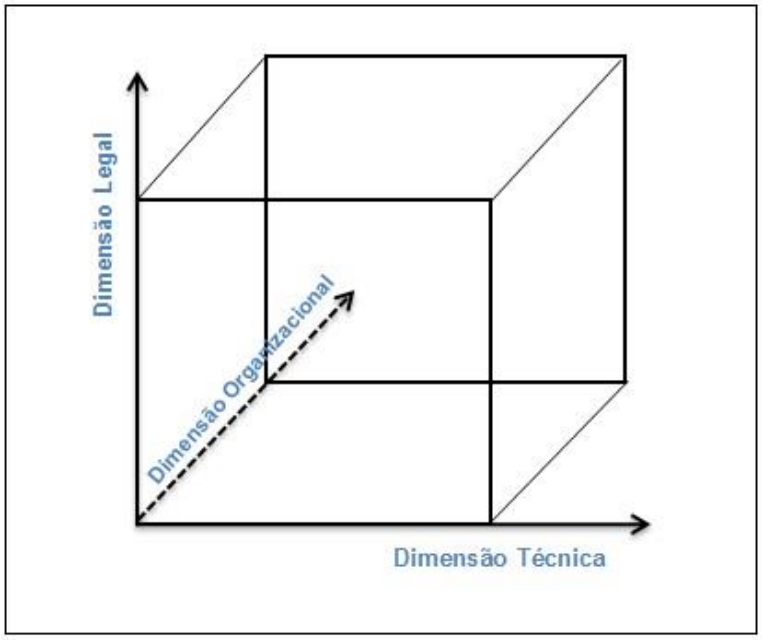
a) a identificação da *cloud forensic* como uma disciplina transversal entre a *Cloud Computing* e forense digital;
b) o reconhecimento da *cloud forensic* como um subconjunto da rede forense (DFRWS, 2001), partindo do princípio de que a rede forense trabalha com investigações forenses em qualquer tipo de redes públicas ou privadas, e a *Cloud Computing* é baseada em acesso a rede ampla. Tecnicamente a *cloud forensic* deve acompanhar as principais fases do processo de rede forense com técnicas avançadas ou inovadoras sob medida para o ambiente *Cloud Computing* em cada uma das fases.

Em modo organizacional, a *Cloud Forensic* envolve interação entre os atores da *cloud* (provedores, consumidores, portador, auditor) com o objetivo de facilitar tanto a nível interno como externo nas investigações (NIST, 2014).

4.2 DIMENSÃO DA CLOUD FORENSIC

A *cloud forensic* segue um modelo tridimensional para sua definição (Figura 16), tal modelo é composto por dimensões legais, organizacionais e técnicas, tornando difícil o convívio entre usuários e provedores de *Cloud Computing* (DIDONÉ, 2011; RUAN, 2013).

Figura 16 - Modelo Tridimensional da Cloud forensic.



Fonte: Adaptado de Ruan (2011).

4.2.1 Dimensão legal

Como foi citado no capítulo 2, para que seja realizada uma perícia forense, deve-se ter em conta alguns aspectos e o aspecto legal é um dos cruciais. Na *cloud forensic* não é diferente, pois ela está subdividida em Multijurisdição e Multiarrendamento e acordo de nível de serviço (RUAN, 2013):

a) multijurisdição e multiarrendamento (multi-tenancy): os especialistas forenses digitais (BROADHURST, 2006; LILES, 2009), mostraram-se preocupados e apontam a jurisdição e o arrendamemnto múltiplo, como os elementos mais desafiadores na *cloud forensic*. É necessário que sejam criados acordos e regulamentos na dimensão jurídica da *cloud forensic* de modo a garantir que as atividades forenses não violem leis ou regulamentos de qualquer jurisdição onde os dados se encontram armazenados, e a confidencialidade para que os dados de outros usuários que partilham da mesma infraestrutura não sejam comprometidos no decorrer da investigação (RUAN, 2011).

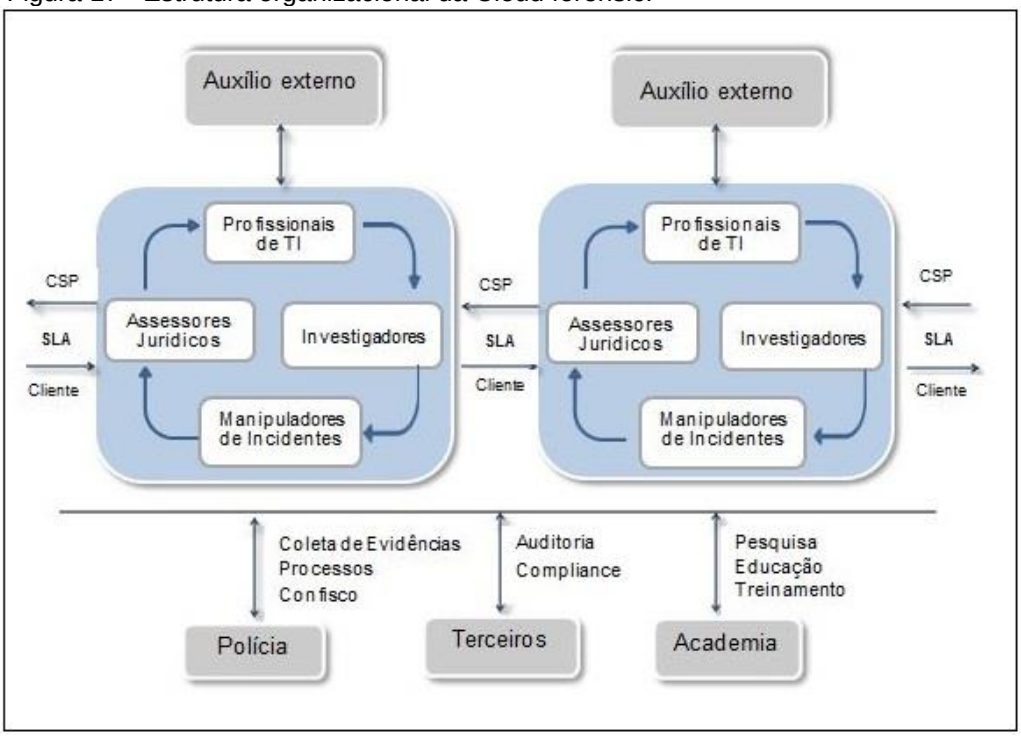
b) acordo de nível de serviço: neste caso são definidos os acordos entre o provedor da *cloud e o cliente.* Os termos de uso devem ser relativos às investigações forenses, devendo conter os seguintes pontos (DIDINÉ, 2011):

a) serviços prestados, técnicas suportadas, acesso concedido pelo *CSP* para o cliente sobre investigação forense,
b) garantias de que a investigação forense esteja segura em ambientes multijurisdicionais e multiarrendamento, no que diz respeito a regulamentos, confidencialidade dos dados dos usuários e políticas de privacidade,
c) limites de confiança, responsabilidades e papeis entre o provedor e o cliente sobre a investigação forense;

4.2.2 Dimensão organizacional

A investigação forense em ambientes *Cloud Computing* envolve sempre pelo menos duas partes: O servidor (CSP) e o cliente *cloud.* A figura 17 ilustra a estrutura organizacional da *cloud forensic*, visando á realização das atividades de modo eficaz e eficiente (DIDONÉ, 2011; RUAN, 2013).

Figura 17 - Estrutura organizacional da Cloud forensic.



Fonte: Adaptado de Ruan (2011).

A estrutura organizacional de cada *cloud*, tem como objetivo estabelecer uma unidade especializada de cada organização, fornecedores e clientes de serviços de *cloud*. É necessário definir uma estrutura de pessoal interno,

colaboração provedora para cliente e a ajuda externa para serem criadas as seguintes funções (RUAN, 2013):

a) **investigadores:** são responsáveis pela investigação (tanto no lado do provedor quanto do cliente), trabalhando com auxílio externo ou a aplicação da lei, quando necessário;
b) **profissionais de *TI*:** este conta com uma vasta gama de profissionais entre eles, hackers éticos, administradores de segurança, arquiteto de segurança em nuvem, grupo de apoio técnico, que contribuem com as investigações com base nos seus conhecimentos, facilitam aos investigadores o acesso a cena do crime, podendo também realizar a coleta de dados;
c) **manipuladores de incidentes:** é um grupo responsável por uma gama específica de incidentes de segurança na nuvem, bem como o acesso não autorizado aos dados, vazamento de dados, perda não intencional de dados, quebra de sigilo arrendatário, uso inadequado do sistema, inserções de códigos maliciosos, ataque malicioso, entre outros. É necessário que os provedores tenham um plano escrito com incidentes de segurança classificados em diferentes níveis da nuvem, objetivando a redução de danos causados;
d) **assessor jurídico:** é de fundamental importância ter um ou mais assessores jurídicos familiarizados com questões jurisdicionais e locação (*tenant)* na nuvem, para que não sejam violadas leis tanto nacionais como internacionais;
e) **auxílio externo:** é recomendável que os provedores *cloud* tenham em conta uma combinação de seus funcionários e das partes externas para executar tarefas forenses, como por exemplo, investigações sobre casos civis e as investigações sobre cadeia externa de dependências.

É importante que as organizações provedoras de *Cloud Computing* possam deste modo determinar com antecedência as ações que serão realizadas pela assistência externa referente às atividades forenses, deixando bem claro as políticas relevantes, diretrizes e acordos que sejam transparentes aos seus clientes e quando necessário a aplicação da legislação.

4.2.3 Dimensão técnica

Ela envolve um conjunto de ferramentas, procedimentos e metodologias que permitem a realização do processo forense em ambientes *Cloud Computing*, onde são destacados os seguintes aspetos chaves:

a) coleta de dados forense: consistem no processo de rotulagem, identificação, registro e aquisição de dados forenses das possíveis fontes. Estas fontes de dados na nuvem incluem artefatos do lado do cliente que residem nas instalações do cliente, e o artefato do provedor que residem na infraestrutura de provedor (DIDINÉ, 2011; RUAN, 2013);

b) elasticidade e forense *in vivo*: a rápida elasticidade é uma das características da *Cloud Computing* que mais se destacam, por este motivo, é de extrema importância que as ferramentas usadas em perícia sejam também elásticas e possam trabalhar com grande volume de dados. É também de extrema importância que as ferramentas realizem a análise pericial ao vivo em rede, pois existem outras características chave em uma *cloud* (RUAN, 2013);

c) segregação de evidências: é uma característica da *Cloud Computing* o conjunto (*pooling*) de recursos que permitem a redução de custos e o compartilhamento de recursos de TI. No entanto o uso do multiarrendamento (*multi-tenancy*) na *cloud forensic* envolve o processo inverso da segregação de evidências, para tal, é necessário o desenvolvimento de ferramentas e procedimentos para separar os dados do usuário em diferentes modelos de implantação e serviços (RUAN, 2013);

d) investigação em ambientes virtualizados: a virtualização é uma das tecnologias chave utilizadas na implementação de serviços *Cloud Computing. N*o entanto as ferramentas e os procedimentos para sua investigação ainda estão sendo desenvolvidos. Por outro lado, as investigações na maioria dos casos ainda requerem a recuperação de evidências a partir de localização física. Um dos desafios de segurança na *cloud forensic* é a perda de controle de dados, para solucionar estes desafios é proposto o desenvolvimento de ferramentas e procedimentos

para a localização física dos dados num dado período de tempo, tendo em conta a jurisdição dos locais físicos (RUAN, 2013);

e) pró-Atividade: podem ser criadas medidas proativas como um mecanismo para facilitar a investigação forense. Nessas medidas incluem-se o desenvolvimento de aplicativos na nuvem que possibilitam a coleta proativa dos dados forenses na cloud, tanto do lado do provedor quanto do lado do cliente.

4.3 CLOUD CRIME

A *Cloud Crime* é todo ou qualquer crime que ocorre na *Cloud* ou que envolva ambientes *Cloud Computing* (CASEY, 2000). Ela é sujeita a crimes e também pode ser usada como ferramenta ou objeto para prática de crimes:

a) **ferramenta para o crime**: criminosos podem usar a nuvem para planejar ou realizar uma ação criminal, nela podem ser armazenadas e compartilhadas evidências relacionadas a crimes, bem como pode ser utilizada para atacar outras nuvens;

b) **objeto do crime**: ocorre quando o provedor é invadido por um criminoso e o mesmo obtenha dados e informações de outros usuários a partir do servidor;

c) **sujeito ou assunto do crime**: ocorre quando a *cloud* é o local onde ocorre o crime, por exemplo, modificação de dados sem a autorização do dono da conta, e o roubo de identidade dos usuários da nuvem.

4.4 CLOUD FORENSIC E SEU USO

Atualmente o uso da *Cloud Forensic* é feito da seguinte maneira *(*RUAN, 2013):

a) investigação:

a) investigação sobre *Cloud Crime* e política de violação em multijurisdicional e multiarrendamento (multi-tenant),
b) investigação sobre transações suspeitas, operações e sistemas na nuvem para resposta a incidentes,
c) reconstrução de eventos na nuvem,

d) fornecer elementos de prova admissíveis para o tribunal,

e) colaboração com a aplicação da lei no confisco de recursos;

b) resolução de problemas:

a) localização de arquivo de dados e anfitriões virtualmente e fisicamente em ambientes *Cloud Computing*,

a) para determinar a causa raiz para eventos únicos ou tendências abrangendo vários eventos ao longo do tempo, e desenvolver novas estratégias para ajudar a prevenir a recorrência de incidentes semelhantes,

b) delinear um evento e avaliar o estado atual de um evento na nuvem,

c) a resolução de problemas funcionais em aplicações e serviços na *Cloud,*

d) resolver problemas operacionais em sistemas,

e) tratamento de incidentes de segurança;

c) monitoramento de logs:

a) coletar, analisar e correlacionar as entradas de *log* em vários sistemas na *Cloud Computing*, auxiliar na auditoria, conformidade regulamentar e outros esforços;

d) sistema de recuperação de dados na Cloud:

a) recuperação de dados que tenham sido eliminados ou modificado de forma intencional ou acidental,

b) recuperação de dados criptografados, quando a chave de criptografia foi perdida,

c) sistemas de recuperação de danos ou ataque acidental,

d) aquisição de dados que estão sendo redistribuídos, ou que precisam ser reformados;

e) conformidade regulamentar:

a) ajudar as organizações no cumprimento de exigências, como a proteção de informações confidenciais, mantendo certos registros para fins de auditoria, notificando partes afetadas quando a informação protegida é exposta, entre outros.

4.4.1 Metodologia de processo de perícia forense

Ao longo do tempo, variados modelos de processos foram desenvolvidos para perícia forense digital, a NIST destacou os oito passos mais usados nos Estados Unidos, sendo todos eles baseadas nas leis existentes no país:

a) busca pela autoridade – nela a autoridade legal é indispensável em uma investigação coletiva onde seja necessário a busca ou apreensão dos dados;
b) cadeia de custódia – nela para contextos legais, é necessário a documentação cronológica de manipulação de evidências, para que sejam evitadas acusações de adulteração de provas ou conduta;
c) imagem e função *hash* - nela quando encontradas as evidências digitais, elas devem ser duplicadas e, posteriormente, deve ser gerado um *hash* para validar a integridade da cópia;
d) ferramentas de validação – são de extrema importância para garantir a confiabilidade e exatidão das ferramentas utilizadas para análise forense;
e) análise – nela são executadas técnicas de análise e investigação para examinar as provas;
f) repetibilidade e reprodutibilidade – exige que os procedimentos de análise devem ser repetidos pelo mesmo ou por outro perito;
g) relatório – nessa etapa o perito deve documentar todo o seu processo de análise e conclusões para o uso de outras pessoas;
h) apresentação - em casos específico, o perito tem de apresentar o seu laudo em um tribunal ou em alguma audiência.

A metodologia de perícia forense em ambientes *Cloud Computing* não difere muito das outras, o único processo diferente e um dos mais desafiadores é na coleta, o acesso as informações é mais complexo pois na maior parte dos casos elas encontram-se em jurisdições diferentes.

4.4.2 Método de acesso aos dados forenses

Para que seja possível a realização de uma perícia forense em *Cloud Computing*, é necessário algum método de acesso aos dados. Embora não hajam métodos padronizados por falta de uma legislação apropriada, existem alguns procedimentos que podem dar acesso aos dados (DYKSTRA, RIEHL, 2012; NIST, 2014):

a) **por meio judicial:** em alguns países, tais como como Estados Unidos da América, Brasil, Angola e entre outros, a lei permite que polícia possa coletar os dados, em casos de crimes contra instituições do estado. No caso de processo judicial de um cliente comum, o tribunal solicita os dados ao provedor e destaca um perito para realizar a análise forense dos dados;

b) **por carta ou pelo suporte técnico:** os clientes que pretendem ter acesso aos seus dados, podem fazê-lo por meio de uma carta que deve ser encaminhada ao provedor do serviço ou utilizar o serviço de suporte ao cliente e solicitar os dados. Despendendo da política de privacidade, acesso aos dados da *Cloud* e até da falta de comprometimento do provedor, o cliente corre o risco de não ter acesso à esses dados;

c) **por backup ou pasta de sincronização:** este recurso está disponível em vários provedores, ele possibilita ao usuário criar uma pasta de sincronização com a sua conta, e automaticamente ela realiza o *download* todos os dados existentes na *Cloud.* Isso possibilita aos usuários e aos peritos, terem acesso aos dados existentes na *Cloud*, inclusive os dados apagados, desde que eles tenham sido apagados após a instalação da pasta de sincronização.

Alguns provedores criaram mecanismos para que o usuário tenha acesso aos seus dados apagados, tal recurso é a pasta reciclagem, ela preserva as informações apagadas por no máximo 30 dias, após este prazo os dados são excluídos definitivamente.

4.5 DESAFIOS DA CLOUD FORENSICS

Diante do que foi abordado ao longo do presente capítulo, tem se ainda muitos desafios. Na dimensão técnica, existem ferramentas e procedimentos muito limitados em todos os cinco principais componentes. Na dimensão legal atualmente não existe qualquer acordo entre as provedoras de *Cloud Computing* sobre a investigação colaborativa (NIST, 2014; RUAN, 2013). O direito internacional cibernético e as políticas devem evoluir para ajudar a resolver as questões que envolvem investigações de Multijurisdição.

4.5.1 Desafios na coleta de dados forense

Os clientes de serviços em nuvem deparam-se com a redução do acesso aos dados forenses independentemente da plataforama ou modelo de serviço usado. Na Infraestrutura como serviço (*IaaS*) os clientes não têm acesso restrito aos dados necessários para uma perícia forense. Já no Software como Serviços (*SaaS*) os clientes podem ter pouco ou nenhum acesso aos dados, essa diminuição do acesso aos dados forenses, é uma realidade muito diferente do que normalmente aparenta, os clientes de *Cloud Computing* na sua maioria têm pouco ou nenhum controle e conhecimento da localização física dos seus dados. Os provedores ocultam intencionalmene os dados de clientes para facilitar a replicação e movimentação de dados. Além disso, há uma falta de condições adequadas de utilização no *Service Level Agreement* (*SLA*) para permitir a prontidão forense geral na *Cloud*. Muitos *CSPs* não prestam serviços ou disponibilizam interfaces para os clientes coletarem dados forenses (NIST, 2014; RUAN, 2013).

4.5.2 Desafios na forense *in vivo*, elástica e estática.

Um dos desafios para descoberta de dados e coleta de evidências, é a proliferação de terminais móveis. Existe uma grande quantidade de recursos ligados à sincronização da *cloud* por causa do impacto dos crimes e da carga de trabalho de investigação exacerbada em *Cloud* Computing. O tempo de sincronização é fundamental para os *logs* de auditoria, que são usados como fonte de evidência na investigação. A sincronização exata de tempo foi sempre um problema na rede

forense, e torna-se ainda mais desafiador em um ambiente *Cloud*, pois a data e hora devem ser sincronizadas através de múltiplas máquinas físicas espalhadas em várias regiões geográficas, entre infraestrutura e clientes (RUAN, 2013).

4.5.3 Desafios na segregação da evidência

Em uma *Cloud* diferentes instâncias em execução numa única máquina física são isoladas umas das outras por meio de virtualização. As instâncias vizinhas não têm mais acesso há instâncias do que qualquer outro host na Internet. Instâncias vizinhas se comportam como se fossem hosts separados. Instâncias de clientes não têm acesso a discos físicos e sim em discos virtualizados. No nível físico, os *logs* de auditoria do sistema de recursos compartilhados, coletam dados de vários inquilinos. É um desafio para os *CSPs* e para as autoridades legais segregar recursos durante as investigações, sem violar a confidencialidade dos outros inquilinos que compartilham a infraestrutura. Outra questão é que o recurso de fácil utilização de modelos de *Cloud, que* contribui para um sistema de registo fraco. Isso facilita o anonimato, o que torna mais fácil para os criminosos esconderem suas identidades e mais difícil para os investigadores identificar e rastrear os suspeitos. Os *CSPs* usam criptografia para dados em separado entre os clientes, quando esse recurso não está disponível os clientes são incentivados a criptografar seus dados sensíveis antes de enviá-lo. A separação deve ser normalizada em *SLAs* e o acesso às chaves criptográficas deve ser formalizado em acordos entre os *CSPs*, clientes e órgãos de legislação (NIST, 2014; RUAN, 2013).

4.5.4 Desafios na cadeia de dependência externa

Os *CSPCs* e boa parte dos aplicativos de *Cloud,* em muitas ocasiões dependem de outros CSPCs, como por exemplo, um *CSPC* provendo uma aplicação de email (*SaaS*), pode depender de um outro terceiro para fornecer recursos ou sediar arquivos de *log* (*PaaS*), e que por sua vez pode depender de um parceiro que forneça uma infraestrutura para armazenar arquivos de *log* (*IaaS*). Apesar de que muitos especialistas e pessoas ligadas à tecnologia preverem que a indústria está caminhando em direção a *Cloud* integradas, os *CSPCs* tem uma abordagem distinta para solucionar este problema:

a) a correlação de atividades em *CSPCs* é também um enorme desafio, a investigação na cadeia de dependências entre os *CSPCs,* pode depender das investigações de cada um dos elos da cadeia de nível de complexidade das dependências;
b) qualquer corrupção ou interrupção na cadeia ou uma eventual falta de coordenação de responsabilidades entre as partes envolvidas, podem originar problemas.

4.5.5 Desafios referentes ao acordo de nível de serviço (*SLA)*

A falta de inclusão de importantes termos referentes à investigação forense até ao momento no *SLA*, ocorre porque existe a falta de conscientização do cliente, a falta de transparência por parte do *CSP* e sobre tudo a falta de regulamentação Internacional. Uma boa parte dos clientes e usuários da *Cloud Computing,* ainda não estão conscientes dos possíveis problemas que podem surgir nas investigações forenses nesses ambientes e o seu significado. Uma das consequências é que eles podem acabar não sabendo sobre o que aconteceu caso os dados sejam perdidos em atividade criminosa e não terem o direito de exigir qualquer indenização. Neste caso, os *CSPCs* não estão dispostos a garantir transparência aos clientes sobre as investigações forenses porque ou não sabem investigar crimes ocorridos na *Cloud* ou os métodos e técnicas que eles usam, são ou estão susceptíveis de serem problemáticos na multijurisdição. Isso acontece porque o progresso de qualquer lei e regulamentos, incluindo leis e regulamentos de crimes cibernéticos é muito lento, por outro lado a *Cloud Computing* está emergindo muito rapidamente como um novo campo de batalha de crimes cibernéticos para os *Crackers* (*hackers* do mal) que estão cada vez melhor equipados com ferramentas e técnicas mais atualizadas e eficazes que as dos investigadores, policiais e de provedores de *Cloud Computing* (NIST, 2014; RUAN, 2013).

4.5.6 Desafios referentes à multijurisdição e multiarrendamento

As diferentes legislações entre os países que têm os provedores e os países em que se encontram os clientes, são os desafios jurídicos da Multijurisdição

e multiarrendamento. As diferenças entre as jurisdições afeta as seguintes questões (NIST, 2014; RUAN, 2013):

a) que tipo de dados podem ser acessados e recuperados em uma jurisdição diferente da qual a máquina física se encontra;
b) como conduzir a recuperação de provas sem violar a privacidade, privilégio ou direitos dos inquilinos de acordo com as políticas e regulamentos de privacidade nas organizações e jurisdição específica;
c) que tipo de prova é admissível em tribunal na jurisdição específica;
d) que tipo de cadeia de custódia é necessária na preservação de provas, na jurisdição em que o dado forense passou durante uma investigação na *Cloud*.

Todas estas questões são aplicadas aos desafios de multijurisdição e multiarrendamento, e elas continuarão a ser um desafio enquanto não forem estabelecidas leis e regras internacionais para a regulamentação do uso da *Cloud Computing*.

No capítulo seguinte, encontram-se alguns trabalhos cuja temática envolve perícia forense e *Cloud Computing*. Estes trabalhos são de vital importância, pois eles servem para se ter uma base do que já tem sido feito na área.

5 TRABALHOS CORRELATOS

No decorrer da pesquisa, foram analisados alguns trabalhos com temas semelhantes, mas com foco em outras áreas da perícia forense computacional em ambientes *Cloud Computing*. Abaixo é feita um breve resumo de alguns trabalhos que abordam temáticas de perícia forense computacional e *Cloud Computing*.

5.1 PROCEDIMENTOS COMPUTACIONAIS NO AUXÍLIO À PERÍCIA FORENSE APLICADA EM WEB BROWSERS

O trabalho foi apresentado por Sidney Roberto da Silva Webba, no curso de Ciência da Computação, pela Universidade do Extremo Sul Catarinense, no ano de 2010, como Trabalho de Conclusão do Curso, para obtenção do grau de Bacharel, sob orientação do Prof. MSc. Paulo João Martins.

Este trabalho teve como objetivo analisar e aplicar alguns procedimentos de perícia forense computacional, e teve como foco a coleta e análise de evidências em web browsers, bem como, contribuir socialmente aumentando o leque de pesquisas sobre o tema. O trabalho também contou com a elaboração de um estudo de caso fictício simulando a condução de uma perícia forense computacional, utilizando a metodologia SOP aplicando as suas 6 etapas: autorização e preparação, identificação, coleta e preservação, exame e análise, documentação e reconstrução da cena do crime. Conclui-se que se conseguiu estudar e aplicar os conceitos de perícia forense computacional, analisando com sucesso muitos dos arquivos de *cache*, *cookies*, histórico de navegação e outros, dos *browsers Internet Explorer* e *Firefox*, utilizando-se das ferramentas Pasco, Galleta, *Web Historian*, *Firefox3Extractor*, Mozilla *Cache View* e *PasswordFox*.

O mesmo também contou com detalhes sobre o processo de perícia forense aplicada à informática e a importância de seguir procedimentos específicos imediatamente depois de um crime por computador.

5.2 FERRAMENTAS E METODOLOGIAS PARA RESPOSTA A INCIDENTES, ESTUDO DE CASO “HELIX 3”

O trabalho foi apresentado por Aguinaldo Gregório Cristiano, no curso de ciência da computação, pela Universidade do Extremo Sul Catarinense, no ano de 2011, como Trabalho de Conclusão do Curso, para obtenção do grau de Bacharel, sob orientação do Prof. MSc. Paulo João Martins.

Este trabalho teve como objetivo estudar algumas técnicas e metodologias para resposta a incidentes presentes no Helix, objetivando dar facilidade ao uso direcionado por usuários na aplicação das mesmas. No mesmo trabalho foram realizadas pesquisas bibliográficas sobre perícia forense, resposta a incidentes e sobre ferramentas presentes no Helix; para demonstrar o funcionamento das ferramentas e a aplicação dos métodos foi objeto de análise um caso de estudo; a metodologia usada para realização da análise no caso de estudo foi a SOP. Ao final foram atingidos os objetivos propostos e foram encontradas evidências bastante sólidas, que incriminam o suspeito, nomeadamente arquivos de texto, imagens e páginas de Internet salvas. Tendo sido consideradas muito eficientes às ferramentas de recuperação de dados em particular o Autopsy presente no Helix.

5.3 O IMPACTO DO CLOUD COMPUTING NO PROCESSO DE PERÍCIA DIGITAL

O trabalho foi apresentado por Robson da Silva Ramos e Nicholas Istenes Eses, no curso de ciência da computação, pela Universidade Presbiteriana Mackenzie, no ano de 2010, como Artigo Cientifico, para obtenção do grau de Pós Graduação, sob orientação da Prof (a). MSc. Vera Kaiser Sanches Kerr.

Este trabalho teve como objetivo apresentar os impactos e desafios trazidos ao processo de perícia forense digital de acordo com o novo cenário de *Cloud Computing*, bem como uma análise dos problemas trazidos a este processo no Brasil de acordo com a legislação atualmente aplicada para esta prática sugerindo a adoção de alguns procedimentos para minimização dos problemas que possam surgir.

5.4 CLOUD COMPUTING APLICADA AO CENÁRIO CORPORATIVO

O trabalho foi apresentado por Gabriela Nubling, no curso de Tecnologia em Processamento de Dados, pela Faculdade de Tecnologia de São Paulo, no ano

de 2011, como Trabalho de Conclusão do Curso, para obtenção do grau Técnico Superior em Informática, sob orientação do Prof. MSc. Shigueo Tomomitsu.

Este trabalho teve como objetivo Analisar e estudar como e quando implantar a tecnologia *Cloud Computing* em uma empresa, quais os requisitos tecnológicos necessários e ampliar os conhecimentos que as empresas têm de *Cloud Computing*, e consequentemente seu destaque dentro da Tecnologia da Informação.

5.5 CLOUD FORENSICS: AN OVERVIEW

O trabalho foi apresentado por Keyun Ruan, no Centro de Investigação para Cybercrime, pela University College Dublin da Irlanda, no ano de 2011, como artigo científico, sob orientação do Prof. Joe Carthy e do Prof. Tahar Kechadi.

Este trabalho teve como objetivo a definição da uma nova área de nuvem forense, bem como analisar seus desafios e oportunidades.

5.6 NIST CLOUD COMPUTING FORENSIC SCIENCE CHALLENGES

Este trabalho foi disponibilizado por Michaela Iorga, na National Institute of Standards and Technology, pela U.S. Department of Commerce, no ano de 2014, como trabalho científico, sob supervisão de Penny Pritzker.

O trabalho teve como objetivo categorizar e discutir os desafios enfrentados por especialistas forenses ao responder a incidentes ocorridos em um ecossistema de computação em nuvem. Nele os desafios são apresentados juntamente com a literatura associada que lhes faz referência. O objetivo imediato do documento é começar um diálogo sobre questões de ciência forense em ecossistemas de computação em nuvem. O objetivo em longo prazo desse trabalho foi para ganhar uma compreensão mais profunda dessas questões (desafios) e identificar as tecnologias e padrões que possam atenuá-los.

6 MÉTODO PROCEDIMENTO E FERRAMENTAS PARA PERÍCIA FORENSE EM CLOUD COMPUTING

O advogado, professor e coordenador do curso de direito eletrônico da Escola da Magistratura do Estado do Rio de Janeiro (*EMERJ*) *Walter Capanema*, aborda *Cloud Computing* como um contrato de prestação de serviços, em que uma empresa permite o uso de seus recursos computacionais por clientes. Estes ambientes são recursos computacionais muito usado e difundido pelas grandes empresas de tecnologia nos últimos anos, eles vêm acompanhados de muita praticidade, flexibilidade, economia, tendo como veículo e seu maior aliado à Internet (NUBLING, 2011). Um dos desafios para os usuários deste recurso, tem sido a proteção e recuperação dos dados, bem como a coleta de evidências em caso de ocorrência de algum crime digital ou perda de dados nesses ambientes.

O presente trabalho aborda sobre a perícia forense, *Cloud Computing*, a nova área científica que engloba as duas áreas que é a *Cloud Forensic e* os seus desafios, seguido de um estudo de caso onde foi possível aplicar método, técnica e ferramentas para busca e coleta de evidências e na solução a um suposto crime ocorrido em ambiente *Cloud Computing,* visto que este trabalho é apenas um estudo de caso. Neste estudo foi implantada a evidência e posteriormente foi coletada e periciada (o ambiente escolhido foi o *Google Drive*), com o objetivo de contribuir com a comunidade científica, com mais um trabalho agrupando as mais diversas informações na perícia forense em ambiente de *Cloud Computing*, com base nas metodologias e recursos forenses capazes de buscar evidências nestes ambientes.

Para a presente pesquisa, foram realizados estudos dos serviços de *Cloud Computing* Pública (*SaaS*) mais usados pelos usuários, entre eles encontravam-se o *Google Drive, DropBox e OneDrive*. Foi então escolhido o *Google Drive* para pesquisa, em função do espaço de armazenamento gratuito (que é de 15 GB), pelas ferramentas e recursos à ele incorporado e pelo seu crescente número de usuários.

Uma vez escolhido o ambiente para a realização da pesquisa, foi criado um estudo de caso referente ao processo de perícia em um ambiente *Cloud Computing.*

6.1 ESTUDO DE CASO

Foi adaptado um estudo de caso do livro “Investigação e Perícia Forense Computacional” de Claudemir Queiroz e Raffael Vargas, que permite demonstrar os procedimentos para busca de evidências.

No presente caso a empresa CELF Pesquisa e Produção está envolvida em escândalos por conta de evasão de documentos sigilosos referentes a sua situação financeira, investimentos e projetos futuros. A empresa tem um corpo administrativo composto por um presidente, quatro administradores e dois assessores, no entanto, só os sete têm acesso às informações vazadas e disponibilizadas para visualização e download na Internet. Sabendo que só um dos sete membros do conselho administrativo poderia ser o criminoso, o presidente convocou uma investigação. No decorrer da mesma, as suspeitas caem em torno de um dos assessores, foi decretada apreensão do *notebook* do membro e chamado um perito para encontrar evidências que levem a confirmação da suspeita.

Ao tomar posse do caso, o perito constatou que os documentos vazados encontram-se em uma *Cloud* pública *Google Drive*. Tratando-se de um crime digital praticado com o auxílio da *Cloud Computing,* foi solicitado o material apreendido para realizar as análises periciais dos mesmos e serem aplicados todos os procedimentos necessários com o objetivo de serem encontradas o máximo de evidências que possam servir de provas que levem ao infrator.

6.2 METODOLOGIA

Para o desenvolvimento do presente trabalho foram adotadas as seguintes metodologias: Na primeira etapa foi realizado o Levantamento bibliográfico, crimes digitais, *Cloud Computing*, legislação entre outros, a maior parte dos trabalhos são em língua Inglesa, parte do material é proveniente de bases de dados que dispõe publicações de artigos científicos, trabalhos de conclusão de curso e congressos relacionados ao tema.

A segunda etapa é destinada a realização do estudo de caso, tendo como objetivo demostrar os procedimentos e ferramentas para realizar a busca de evidências para solucionar o caso.

Martins e Theóphilo (2009) afirmam que um estudo de caso:

> Trata-se de uma investigação empírica que pesquisa fenômenos dentro de seu contexto real [...] onde o pesquisador não tem controlo sobre eventos e variáveis, buscando apreender a totalidade de uma situação e criativamente descrever, compreender e interpretar a complexidade de um caso concreto. [...] possibilita a penetração na realidade social, não conseguida pela avaliação quantitativa.

Quando se trata de perícia forense computacional, cada caso tem as suas particularidades, portanto, não existem modelos específicos para cada caso, existem sequências de práticas metodológicas para se realizar uma perícia. Para este caso foi escolhida a *Standard Operating Procedures* (*SOP*) que é muito usada no Brasil. As suas etapas foram definidas no capítulo 2, na figura 18 pode ser visualizada e segue as etapas: Autorização e Preparação, Identificação, Coleta e Preservação, Imagem Forense, Exame e Análise, Documentação, Relatório e Revisão.

Figura 18 - Metodologia SOP para Resposta ao Caso de Estudo.

Fonte: Schultz (2008).

Para que a perícia forense fosse realizada com êxito, foram respeitadas todas as regras básicas que um perito deve seguir, nesse estudo de caso foi feita

uma imagem autêntica do cenário do crime, prevenindo assim a alteração da cena do crime com a realização da perícia com ferramentas foss[1].

6.2.1 Autorização

Para a realização do seguinte trabalho não foi necessário uma autorização legal, pois o mesmo trata-se que um estudo de caso fictício para fins acadêmicos. Porém foram levados em conta todos os procedimentos da metodologia *SOP* e foram asseguradas as normas na preparação e organização das informações.

6.2.2 Coleta da prova

A coleta da prova é de crucial importância na perícia forense, ela marca o começo da investigação forense e as evidências devem ser coletadas seguindo as normas e cuidados.

Tratando-se de perícia em ambientes *Cloud Computing*, o desafio está no acesso aos dados, visto que os servidores encontram-se em países diferentes e com políticas diferentes (RUAN, 2013). Sendo que o ambiente em que ocorreu o incidente é o *Google Drive* e que, a empresa *Google* tem uma representação no Brasil, foi adotata a metodologia de acesso aos dados forenses da conta, para tal foi encaminhado ao orgão uma carta (anexo B) solicitando os dados forenses da conta, não tendo sido respondida até a conclusão desta pesquisa. Foi então adotado o método de acesso aos dados pelo suporte técnico (anexo C), tendo sido recuperado todos os dados apagados da conta *Cloud*. Os dados foram recuperados, porém eles foram disponibilizados na própria *Cloud*.

Segundo Fabiano Rabaneda advogado e especialista em direito eletrônico e tecnologia da informação, os dados existentes em uma *Cloud* não podem só ser obtidos através do provedor e sim por meio de *backup*. Os *backups* de dados na *Cloud* são uma solução que muitos provedores criaram para que o usuário tenha os dados sob seu domínio. Em alguns casos específicos como *DropBox*, *Google Drive*, *OneDrive* entre outros, ao baixar e instalar o software do provedor, é

[1] Foss: significa Free and Open Source Software

criada uma pasta sincronizada com a conta, onde todos os dados existentes na *Cloud* são baixados para o computador ou outro dispositivo computacional, servindo como *backup*. Sendo esta pasta sincronizada o único meio criado pelos provedores para que o usuário tenha uma réplica (cópia) do que existe na *Cloud*, o perito pode usar a mesma para extrair os dados da *Cloud* e buscar evidências na mesma.

A perícia no presente estudo de caso será realizada sobre um *backup* de sincronização com uma conta *Cloud Google Drive,* e o sistema operacional que gerencia o computador e seus dados é *o Windows 7 Professional.*

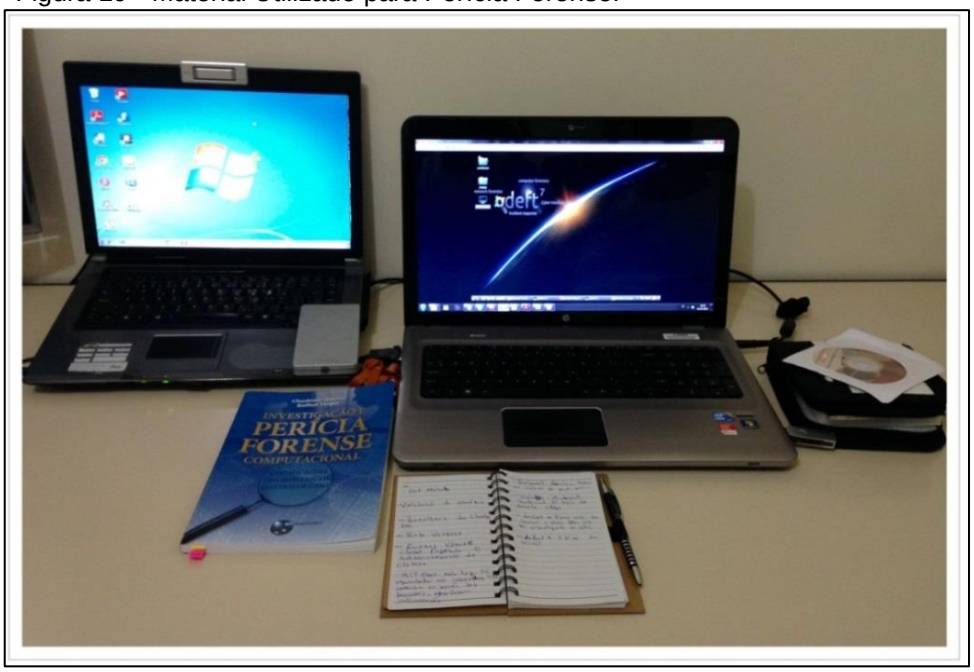
6.2.3 Preparação do equipamento

Para que seja realizada uma perícia forense é imprescindível a criação de condições para que ela tenha o máximo de eficácia. Estas condições são espaço disponível para manusear os equipamentos, hardware e softwares. Para tal, foi criado um laboratório com duas máquinas, seguindo todos os pré-requisitos para uma perícia forense. Os computadores utilizados no laboratório (Figura 19) apresentam as seguintes configurações:

a) computador *Asus F5SL*:
   a) disco rígido 320 *GB*,
   b) memória ram 3 *GB*,
   c) sistema operacional *Windows 7 profissional 64 bits*,
   d) processador *intel pentium(R) dual CPU T230 1.60 Ghz;*

b) computador *HP Pavilion Dv7-4087cl*:
   a) disco rígido 760 *GB*,
   b) memória ram 6 *GB*,
   c) sistemas *operacional Ubuntu Deft 7* e *Windows 7 profissional 64 bits*,
   d) Processador Intel Core (TM) i5 CPU M 430 2.27 Ghz,
   c) *software* livre para perícia forense *Deft 7.2, Autopsy*, entre outros,
   d) um disco rígido externo de 500 GB.

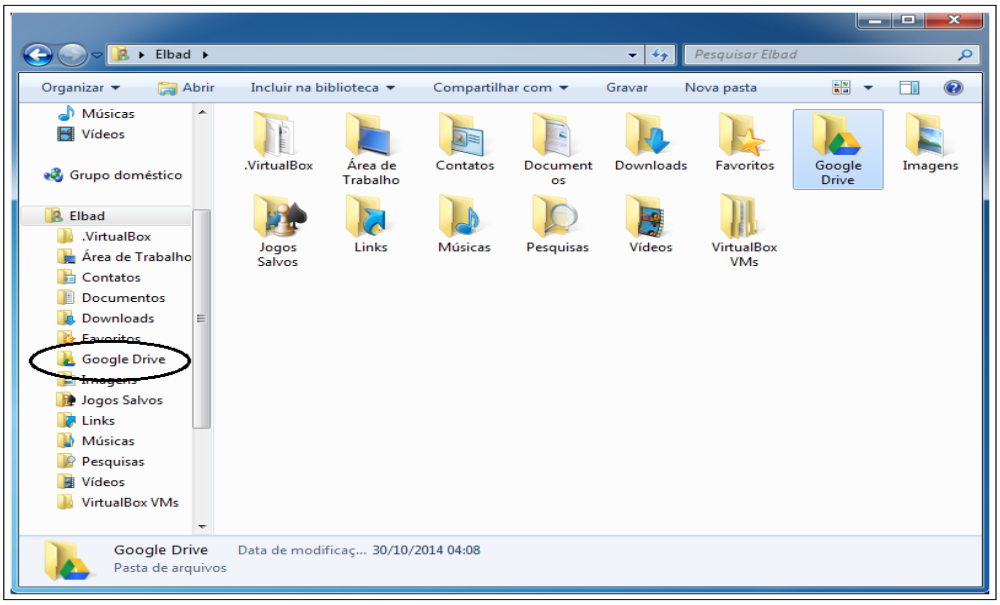
Figura 19 - Material Utilizado para Perícia Forense.



Fonte: Do autor.

No computador *Asus F5SL* foi preparado o cenário do crime com a criação de uma *Cloud* pública *Google Drive* e instalação da pasta de sincronização, nela foram adicionados os diretórios ou pastas a serem periciadas. Já o computador *HP Pavilion Dv7-4087cl* foi usado para manipular a evidência, para tal foi instalado o *software* livre para perícia forense *Deft 7.2.*

Figura 20 - Imagem da pasta de sincronização Google Drive.

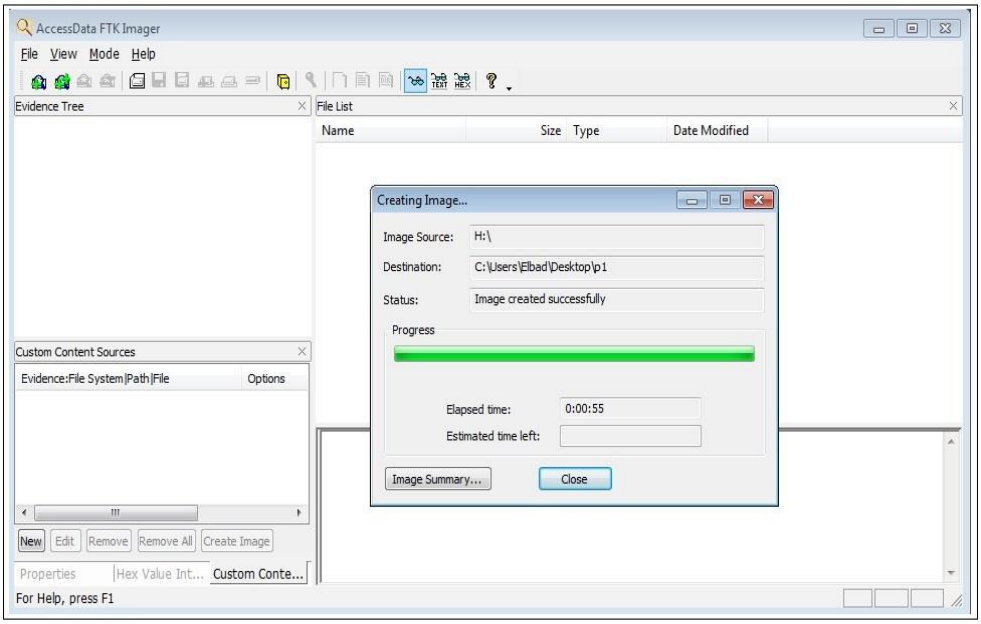


Fonte: Do autor.

6.2.4 Imagem forense

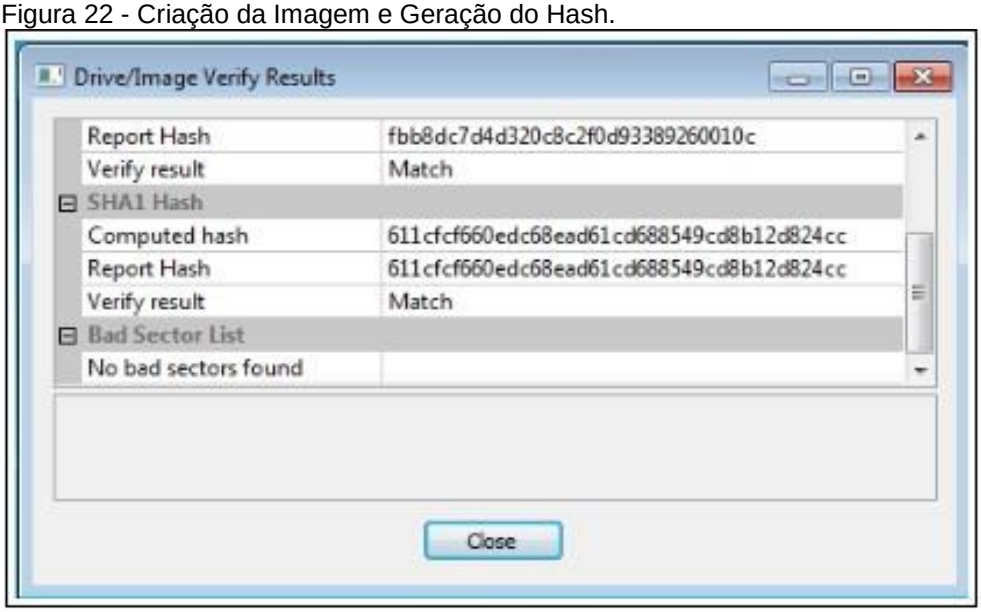
Para a realização da análise dos dados, foi antes criada com êxito uma imagem da partição onde encontram-se os dados, por meio da ferramenta AccessData *FTK Imager* e ao final foi gerado um *Hash* com o algoritmo *Md5 e Sha1*. Posteriormente foi coletada e armazenada em um *HD* externo formatado com capacidade de 500 *GB*.

Figura 21 - Criação da Imagem e Geração do Hash.



Fonte: Ftk imager.

Figura 22 - Criação da Imagem e Geração do Hash.



Fonte: Ftk imager.

6.2.5 Exame e análise

Para a realização do exame e análise, primeiramente foram duplicadas as imagens para que no caso de perda dos dados ou alteração do cenário por conta dos procedimentos de perícia, o perito não tenha de realizar a coleta. Posteriormente foi copiada para o ambiente do *DEFT 7.2* uma das cópias da imagem para análise forense.

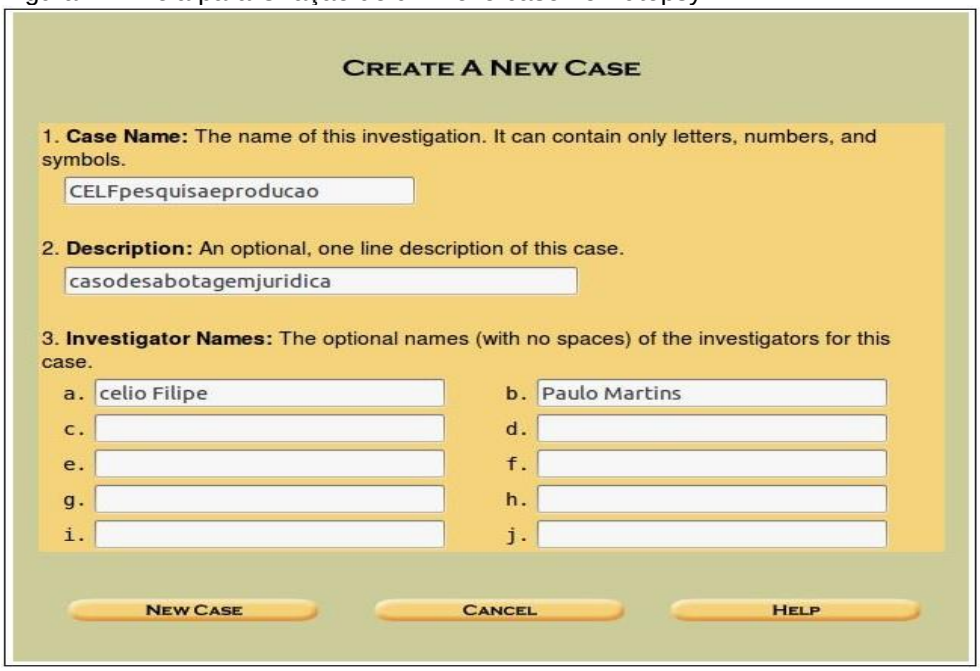
Uma vez a imagem copiada no ambiente, é executada a ferramenta de análise forense '*Autopsy'* existente no ambiente *DEFT* (Figura 23). Na ferramenta *Autopsy* é possível abrir um caso (*Open Case*) já existente, criar um novo caso ou recorrer a opção ajuda onde é possível encontrar informações de como utilizar a ferramenta *Autopsy.*

Neste estudo objetiva-se dar resposta a um incidente novo, e foi escolhida a opção de criação de um novo caso (*New Case*), contendo as informações pré-definidas na tela do Autopsy (Figura 24), as informações são: o nome do caso (*Case Name*), uma descrição previa do caso (*Description*), e os nomes dos investigadores envolvidos (*Investigator Names*).

Figura 23 - Tela Inicial da Ferramenta de Análise Autopsy.

Fonte: Autopsy (2014).

Figura 24 - Tela para Criação de um novo caso no Autopsy.

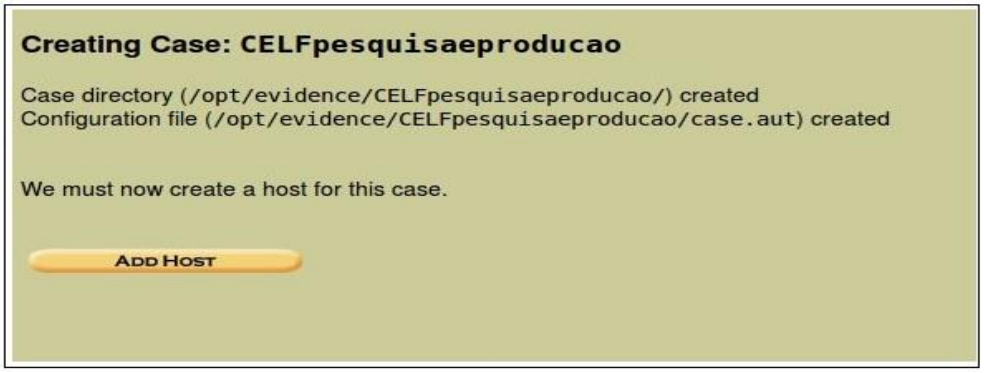


Fonte: Autopsy (2014).

Neste caso, foram definidos os seguintes itens: nome do Caso (*Case Name*) CELF pesquisa e producao, descrição do caso (*Description*) caso de sabotagem jurídica, nome dos investigadores (*Investigator Name)* Celio Filipe e Paulo Martins. Os dados inseridos nos passos devem conter o máximo de informações possíveis porque elas fazem parte do relatório final quando o perito dar como encerrado o caso.

O passo a seguir é armazenar todas as informações inseridas em um diretório criado pelo *Autopsy* com o nome (otp/evidence/CELFpesquisaeproducao/).

Figura 25 - Tela da criação do diretorio.



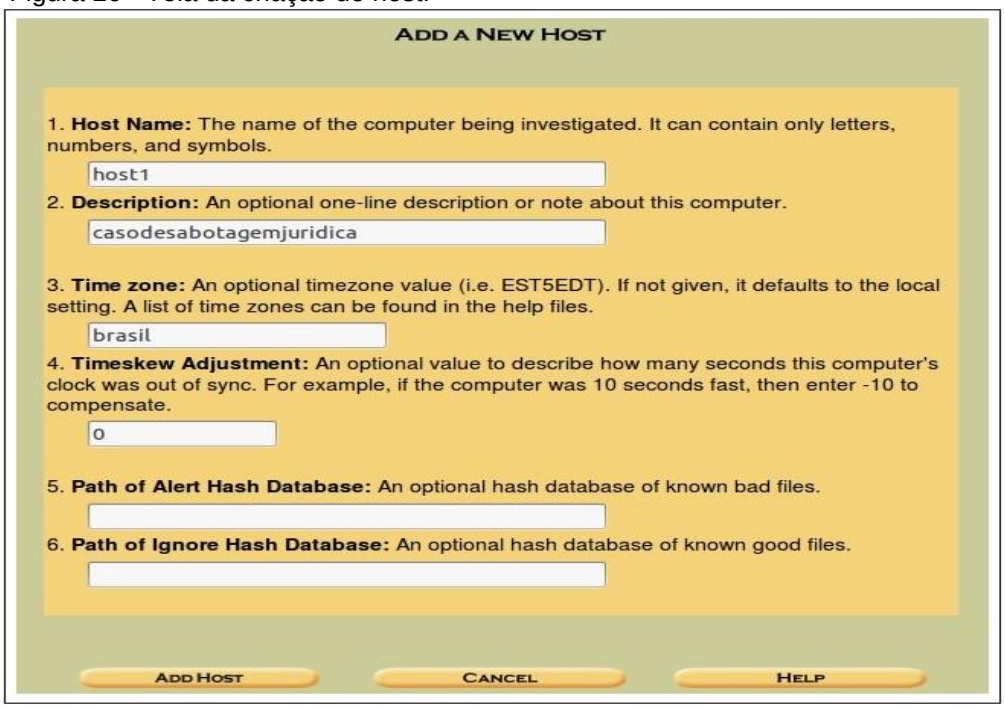
.

Fonte: Autopsy (2014).

Uma vez o caso criado, é preciso identificar o nome do computador (*host Name)* a ser periciado, seguido de uma previa descrição referente a perícia, a hora

do local em que o perito se encontra que é inserida no *Time zone*, os *clocks* devem ser inseridos no *Timeskew Adjustment,* o *Path of alert hash database* serve para criar um banco de dados e posteriormente armazenar todos os códigos *hash* gerados no decorrer da análise.

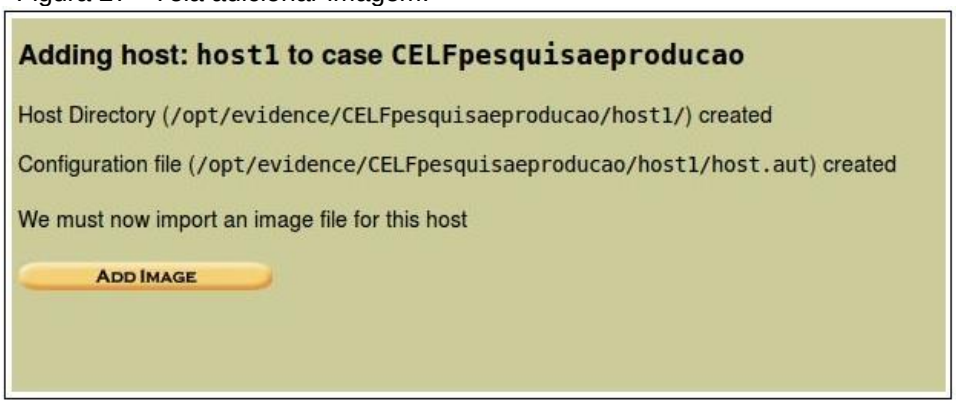
Figura 26 - Tela da criação do host.



Fonte: Autopsy (2014).

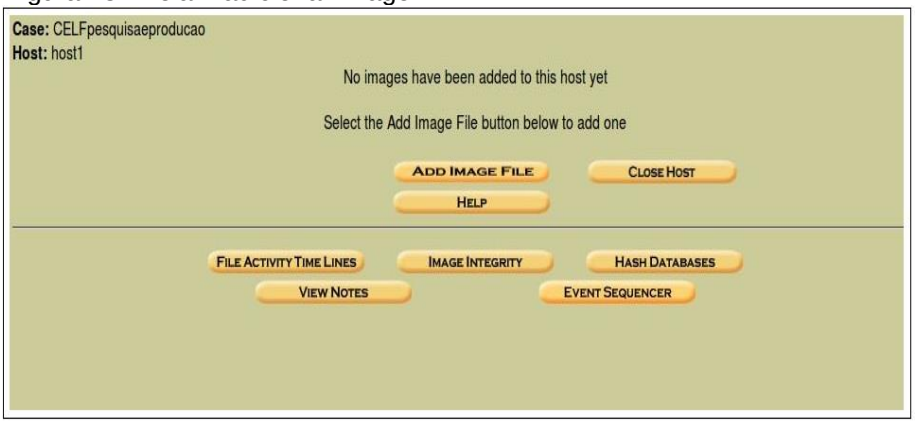
Após a criação do *host* é adicionada a cópia da imagem forense já criada e devem ser observados os seguintes aspectos: não são permitidos espaços ao escrever o diretório da imagem, nas imagens no formato *RAW* geradas por partes devem ser utilizados asterisco (“*”) como extensão.

Figura 27 - Tela adicionar imagem.



Fonte: Autopsy (2014).

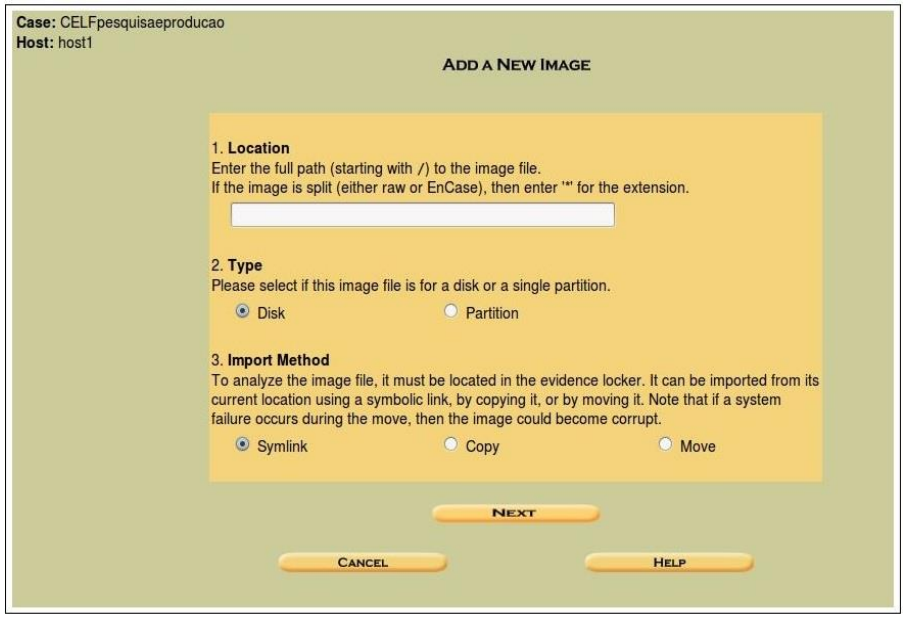
Figura 28 - Tela 2 adicionar imagem.



Fonte: Autopsy (2014).

A coleta de dados no disco rígido pode ser feita de várias formas, caso o disco possua várias partições e o perito não saiba em qual delas estão às evidências, é prudente que o perito faça a cópia de todas as partições bit-a-bit. No presente estudo de caso, foi criada uma partição exclusiva para o ambiente a ser periciado com 20 Gb, portanto foi copiada apenas uma partição.

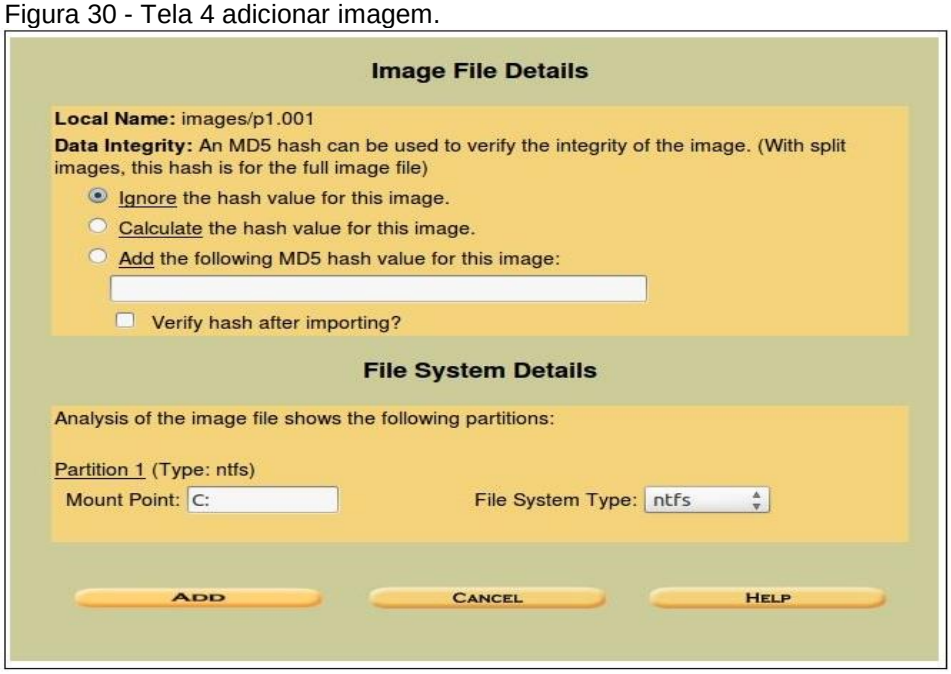
Figura 29 - Tela 3 adicionar a localização da imagem.



Fonte: Autopsy (2014).

Uma vez copiada a partição, é feita a importação dela para o *Autopsy*, o método usado foi a partir do local da imagem “*Symlink”*, no qual é criado um *link* para o diretório onde encontra-se a imagem que é passada por parâmetro. Existem também outros dois métodos, um cópia a imagem “Copy” e o outro move a mesma para o diretório onde está sendo criado o caso “Move”.

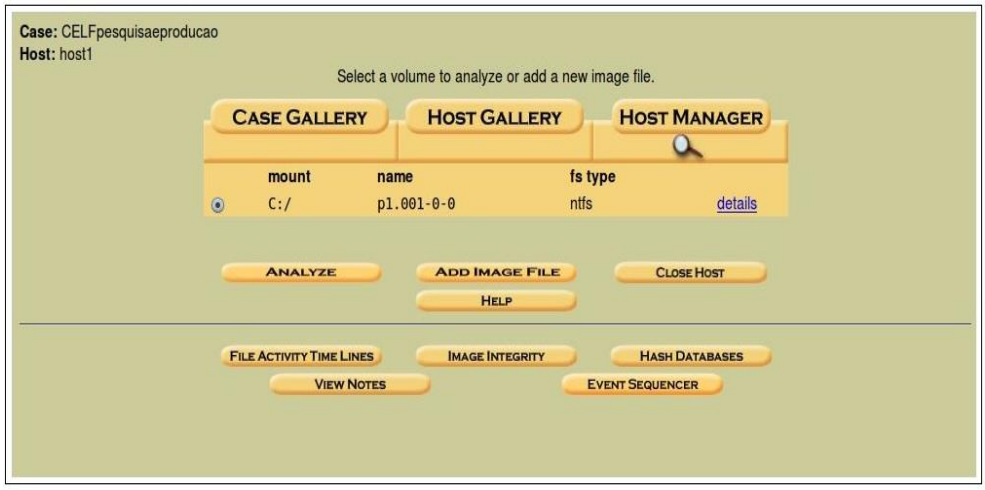
Figura 30 - Tela 4 adicionar imagem.



Fonte: Autopsy (2014).

Na figura 31, é ilustrado o momento após a imagem ser adicionada para análise, nesta etapa pode ser adicionado o código *hash (*gerado quando foi criada a imagem). Posteriormente são apresentados os dados de partição da imagem o que significa que a imagem foi bem extraída e copiada para o *Autopsy.*

Figura 31 - Tela 5 Análise Forense.



Fonte: Autopsy (2014).

A figura 32 ilustra algumas informações como o tipo de arquivo do sistema, o ponto de montagem da partição.

a) *analyze* – é a partir dela que se começa a busca de informações por meio de uma minuciosa busca e análise nos diretórios, na estrutura e nos seus arquivos;

b) *Add image file* – tem a função de adicionar mais imagens no ambiente de perícia;

c) *close host* – serve para fechar o *host* ou encerrar a análise;

d) *help* – contem informações de como usar a ferramenta.

e) *file activity timeline* – permite criar uma *timeline* dos eventos ocorridos;

f) *image integrity* – permite verificar o estado da integridade da imagem, fazendo a comparação dos *hash* armazenados na base de dados;

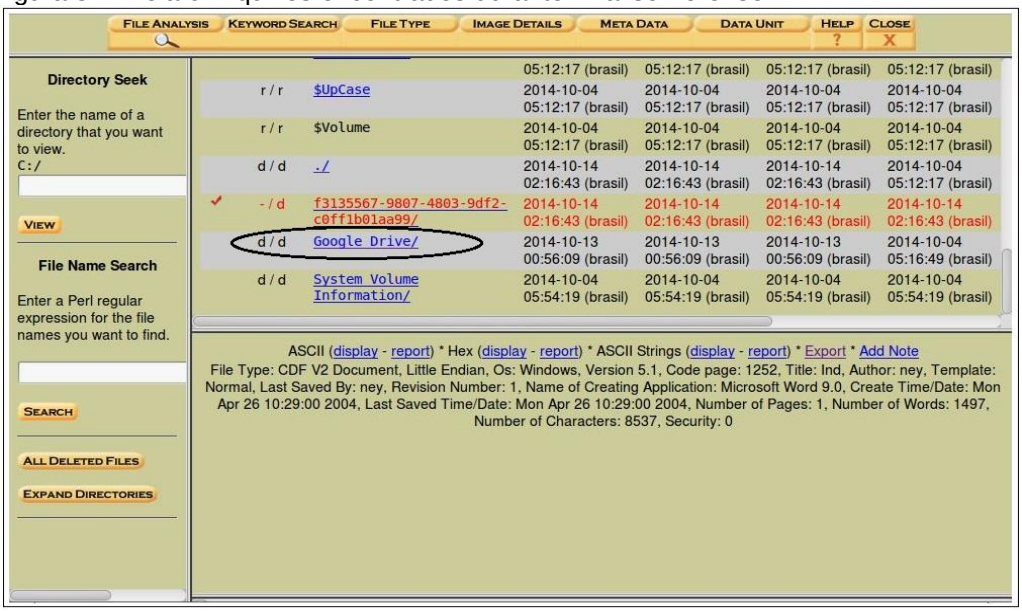
g) *hash database* – mostra os *hash* armazenados no banco de dados;

h) *view notes* – tem armazenadas as notas criadas no decorrer da análise forense;

i) *event sequencer* – contém uma sequência de eventos.

Para começar a busca e análise das informações na imagem, foi escolhida a opção *Analyze,* ela é feita de maneira visual e no decorrer da sua busca, foram encontradas todas as informações existentes na partição.

Figura 32 - Tela 6 Arquivos encontrados durante Análise Forense.



Fonte: Autopsy (2014).

É possível visualizar na figura 32, todos os arquivos existentes na partição, inclusive os apagados (em vermelho). No diretório Google Drive/ encontram-se os dados sincronizados com a *cloud* (*backup* físico do cliente) e são neste diretório que podem ser encontradas as provas do crime (figura 34).

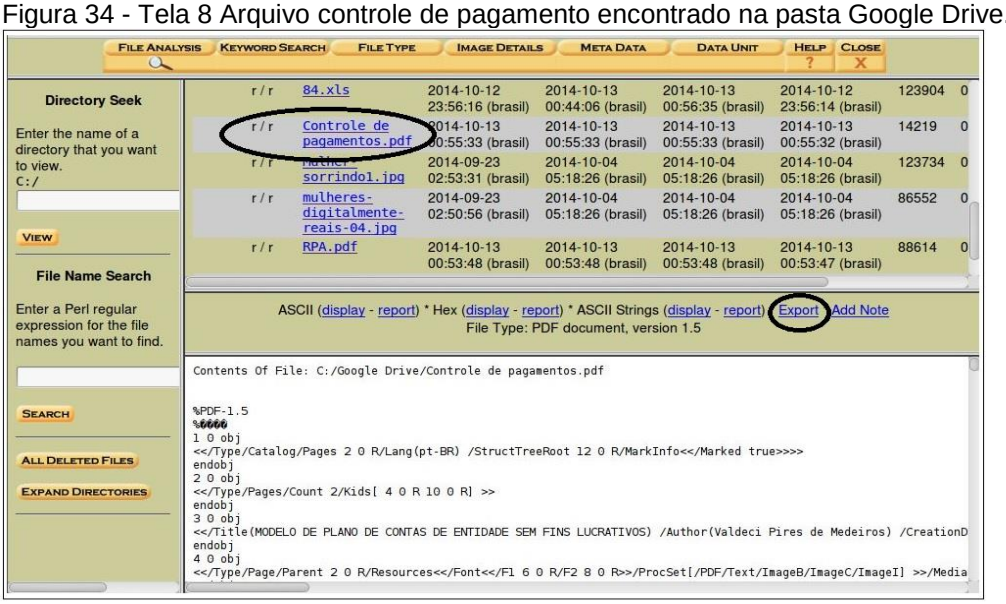
Figura 33 - Tela 7 Arquivos encontrados na pasta Google Drive.

Fonte: Autopsy (2014).

No diretório do *Google Drive* podem ser visualizados vários arquivos num total de doze, o que realça a atenção do perito é que muitos desses arquivos encontram-se nos formatos *doc, Pdf*, Xls e Jpg, o que aumenta a probabilidade de serem encontradas provas, visto que os arquivos vazados têm alguns destes formatos.

Um arquivo suspeito visualizado é o arquivo denominado “controle de pagamentos.pdf” que é também o nome de um arquivo vazado contendo todos os pagamentos efetuados pela empresa nos últimos meses (figura 34).

Figura 34 - Tela 8 Arquivo controle de pagamento encontrado na pasta Google Drive.



Fonte: Autopsy (2014).

É possível realizar a pré-visualização do seu conteúdo clicando no documento, e se quiser melhorar a visualização, é só clicar em "*Export*. É possível também exibir os arquivos e gerar um relatório com as opções *ASCII (display - report), Hex (display - report), ASCII String (display – report):*

a) ***ASCII (display – report)*** – possibilita gerar um relatório com "*report"* contendo as informações de data de acesso, de criação e o lugar em que ele está alocado;

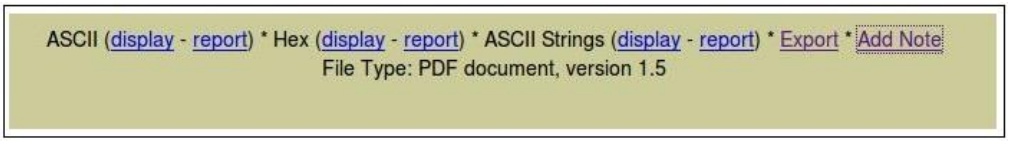
b) ***Hex (display - report)*** – possibilita gerar um relatório com "report" contendo as informações de data de acesso, de criação, lugar em que ele está alocado e a sua exibição é em Hexadecimal;

c) ***ASCII string (display – report)*** – possibilita gerar um relatório com "*report"* contendo as informações de data de acesso, de criação, lugar em que ele está alocado e a sua exibição é em Strings;

d) ***export*** – possibilita exportar para outro local e analisar a evidência;

e) ***add note*** – possibilita adicionar notas durante a análise das evidências.

Figura 35 - Visualização de arquivos.



Fonte: Autopsy (2014).

Figura 36 - Tela 8 Arquivo controle de pagamento encontrado na pasta Google Drive.

Controle de pagamentos do cliente

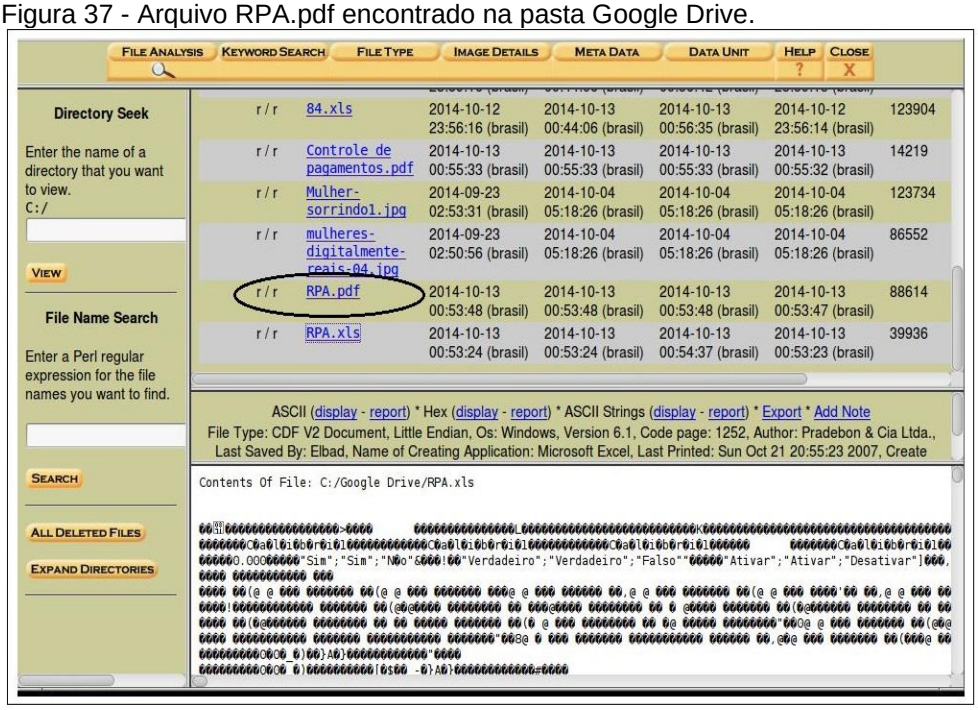
Matricula: 100
Razão Social: Empresa Modelo S/A
Admissão: 10/03/**2014**
Multa p/ Atraso: 10%
Juros: 1%
Emitido em: **12/10/2014**

Mensalidade	Competencia	Vencimento	Valor	meses em atraso	Valor atualiz.
001	abr	09/04/2014	R$ 50,00	4	R$ 757,00
002	mai	09/05/2014	R$ 50,00	3	R$ 656,50
003	jun	08/06/2014	R$ 50,00	2	R$ 656,00
004	jul	08/07/2014	R$ 50,00	1	R$ 655,50
005	ago	07/08/2014	R$ 50,00	0	R$ 650,00
006	set	06/09/2014	R$ 50,00	0	R$ 650,00

Fonte: Autopsy (2014).

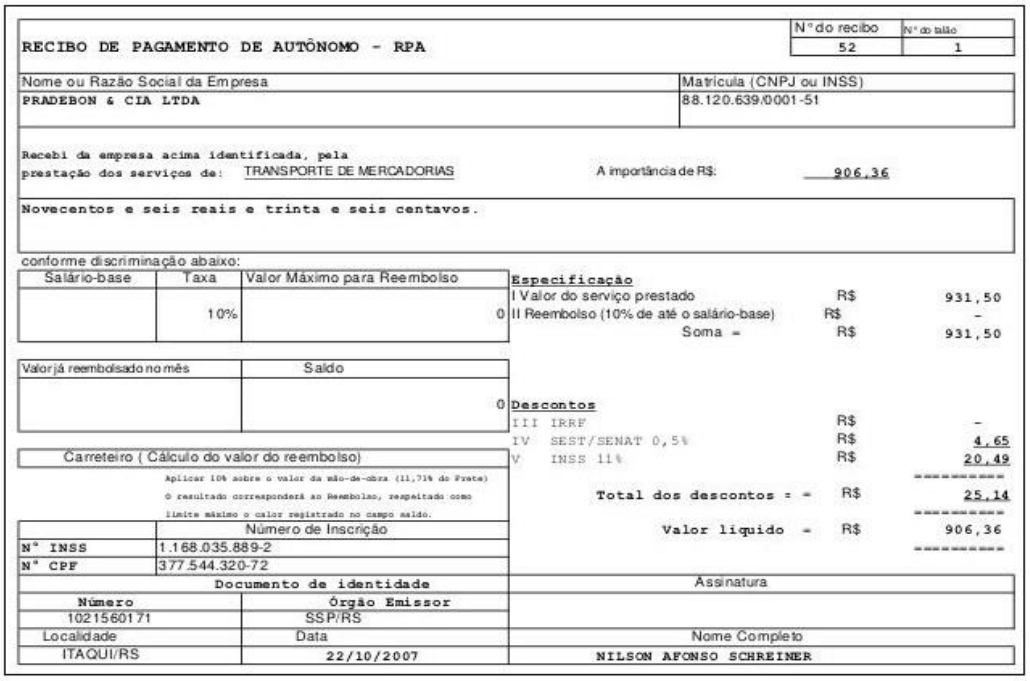
É possível visualizar também na figura 37 a existência de outros arquivos suspeitos, o arquivo *RPA* (com extensões *pdf* e *Xls*) criado no dia 13 de Outubro de 2014 à 00h53 minutos, foi exportado para análise e nele foram encontrados recibos de pagamentos efetuados pela empresa e estes recibos fazem parte das informações disponibilizadas na rede.

Figura 37 - Arquivo RPA.pdf encontrado na pasta Google Drive.



Fonte: Autopsy (2014).

Figura 38 - Arquivo RPA encontrado e exportado para visualização.



RECIBO DE PAGAMENTO DE AUTÔNOMO - RPA

Nº do recibo	Nº do talão
52	1

Nome ou Razão Social da Empresa	Matrícula (CNPJ ou INSS)
PRADEBON & CIA LTDA	88.120.639/0001-51

Recebi da empresa acima identificada, pela prestação dos serviços de: TRANSPORTE DE MERCADORIAS — A importância de R$: 906,36

Novecentos e seis reais e trinta e seis centavos.

conforme discriminação abaixo:

Salário-base	Taxa	Valor Máximo para Reembolso
	10%	0

Valor já reembolsado no mês	Saldo
	0

Carreteiro (Cálculo do valor do reembolso)

Aplicar 10% sobre o valor da mão-de-obra (11,71% do Frete)
O resultado corresponderá ao Reembolso, respeitado como limite máximo o valor registrado no campo saldo.

	Número de Inscrição
Nº INSS	1.168.035.889-2
Nº CPF	377.544.320-72

Documento de identidade	
Número	Órgão Emissor
1021560171	SSP/RS
Localidade	Data
ITAQUI/RS	22/10/2007

Especificação		
I Valor do serviço prestado	R$	931,50
II Reembolso (10% de até o salário-base)	R$	-
Soma =	R$	931,50
Descontos		
III IRRF	R$	-
IV SEST/SENAT 0,5%	R$	4,65
V INSS 11%	R$	20,49
Total dos descontos =	R$	25,14
Valor liquido =	R$	906,36

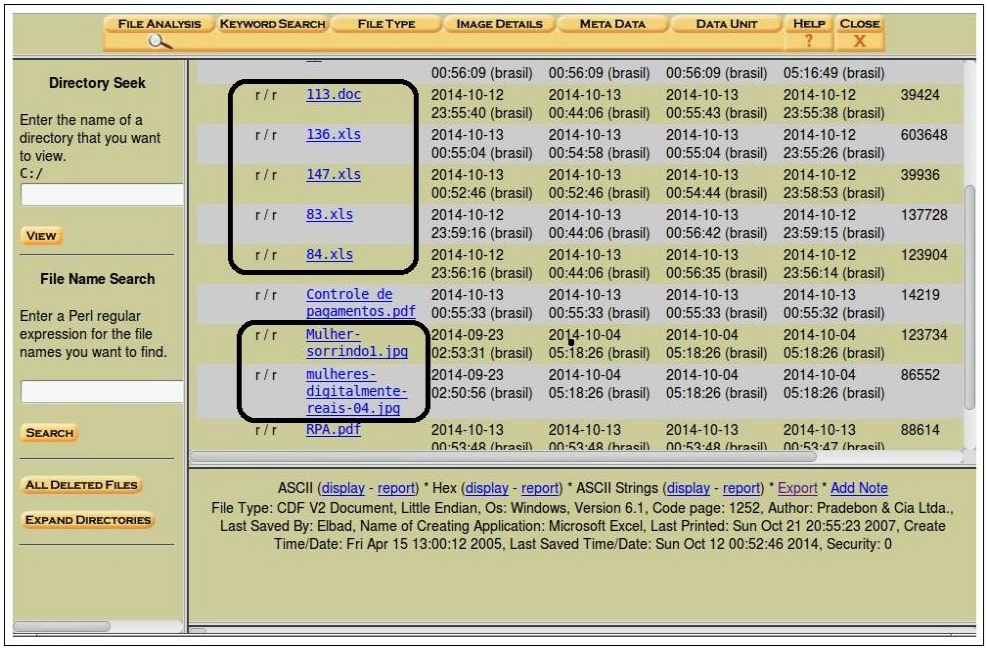
Assinatura

Nome Completo: NILSON AFONSO SCHREINER

Fonte: Autor.

Foram também encontrados quatro documentos ligados a contabilidade da empresa CELF pesquisa e produção, porém, não fazem parte dos documentos vazados. Dois arquivos no formato *jpg* denominados “Mulheres-digitalmente-reais-04.jpg” e “Mulher-sorrindo1.jpg” foram encontrados e não têm alguma ligação aparente com o caso.

Figura 39 - Arquivos encontrados que não fazem parte do leque de documentos vazados.



Fonte: Autopsy (2014).

Foram efetuadas buscas em arquivos apagados usando a função “*All Deleted Filles”* não tendo sido encontrado qualquer arquivo deletado referente à pasta *Google Drive*.

6.2.6 Documentação

Pelo fato de ser um caso fictício, esta documentação não é acompanhada de uma cópia da autorização judicial para coleta das evidências. Porém, foi gerada uma cadeia de custódia tendo como base as informações obtidas no estudo de caso e nos objetos usados para criar o cenário. Os dados necessários são: nome do perito responsável, hora da criação da imagem do cenário, métodos usados para sua obtenção, entre outros.

Figura 40 - Formulário de Cadeia de Custódia.

EVIDÊNCIA ELETRÔNICA

FORMULÁRIO DE CADEIA DE CUSTÓDIA

Caso Num.: 01 **Pag.:** **De:19/10/2014**

MÍDIA ELETRÔNICA/DETALHES EQUIPAMENTO

Item:	Descrição:		
Computador	Computador apreendido para investigação de evazão de documentos confidenciais		
Fabricante:	Modelo:	Num. de serie:	
Asus	F5SL	YMAXPFGBPCM6Q3QM	

DETALHES SOBRE A IMAGEM DOS DADOS

Data/Hora:	Criada por:	Método usado:	Nome da Imagem:	Partes:
00:09:18	Célio Filipe	bit-a-bit	p1.dd	1
Drive:	HASH:			
C	611cfcf660edc68ead61cd688549cd8b12d824cc			

CADEIA DE CUSTÓDIA

Destino:	Data/Hora:	Origem:	Destino	Motivo:
	Data: 14-10-2014	Nome/Org.: CELF pesquisa e Produção	Nome/Org.: Sector G	
Laboratórios Forense	Hora: 22:15:28	Assinatura: Dr. Alvaro Silva	Assinatura: Célio Filipe	Análise de evidências
	Data:	Nome/Org.:	Nome/Org.:	
	Hora:	Assinatura:	Assinatura:	

Fonte: Autor.

Todo processo de perícia foi baseado nas informações recuperadas pelo suporte Google Drive e extraídas da *Cloud* com o auxílio da pasta de sincronização e posteriormente o perito realizou a validação usando o algoritmo de *hash md5* que correspondeu ao *hash* inicial criado na geração da imagem. Para realização da perícia, foi usada a metodologia *SOP,* e foram seguidas as suas regras de documentação dos dados referentes à investigação, elas são os dados de todos os *logs* realizados durante a investigação, dados esses desde a criação até o encerramento do caso (Apêndice B).

6.2.7 Relatório/Revisão

Nesta etapa encontram-se todas as informações relevantes do trabalho para auxiliar aos pesquisadores e comunidade em geral.

O estudo de caso no ambiente *Google Drive*, com as práticas e os passos necessários para busca de evidências de um crime praticado por meio de uma *cloud* pública. As evidências foram periciadas em uma pasta de sincronização do *Google Drive e* para análise do cenário foram utilizadas as seguintes ferramentas de perícia:

a) ***AccessData FTK Imager*:** ferramenta usada para criar a imagem do ambiente a ser periciado;
b) ***Deft 7.2***: ferramenta usada para manusear a imagem;
c) **Autopsty:** software usado para análise da imagem e busca de evidências.

Com estas ferramentas de perícia, foram realizadas buscas e análise de evidências, com o finalidade de dar resposta ao incidente ocorrido. No decorrer da análise, foram encontrados um total de dez (10) arquivos, entre eles dois suspeitos por terem uma correlação com o caso. Portanto, estes dois arquivos encontrados podem ser usados para instauração de um processo contra o funcionário e servir como prova da sua participação no crime. Os outros oito arquivos encontrados, não podem ser usados como prova pois, não têm qualquer correlação com os arquivos vazados.

6.3 RESULTADOS OBTIDOS

No decorrer da pesquisa, foram alcançadas os seguintes objetivos específicos:

a) aplicar os conceitos sobre perícia forense computacional - que compreendeu em descrever e aplicar os conceitos de perícia forense computacional e realizar uma abordagem mais didática e técnica sobre o assunto, que foi realizado com êxito no capítulo dois;
b) compreender como ocorrem os crimes digitais e como manter a segurança da informação – foi o segundo objetivo alcançado, com a abordagem e inclusão de novos factos e algumas leis vigentes no Brasil e uma visão geral sobre como elas são em outros países;
c) compreender e aplicar os conceitos de *Cloud Computing* – foi o terceiro objetivo alcançado, que compreendeu em realizar uma abordagem na essência da *Cloud Computing*, seus modelos de implantação, modelos de serviço, segurança, benefícios, desafios, bem como retratar algumas ferramentas para sua criação e gerenciamento;
d) descrever e relatar algumas ferramentas de código aberto e software livre usadas na busca e análise de evidências – foi alcançado, com a abordagem de alguns sistemas e ferramentas que auxiliam o perito na busca de evidências. Porém também foram descritos alguns desafios no processo de perícia forense em ambientes *Cloud Computing*;
e) relatar e documentar um estudo de caso, de forma a elucidar a referida pesquisa, com as evidências obtidas – foi o último objetivo proposto e alcançado, contando com a criação de um estudo de caso e com a realização da perícia com base no estudo de caso, que foi possível ser solucionado, graças ao mecanismo que alguns provedores de *Cloud* pública disponibilizam aos seus clientes, que entre outros, possibilita a criação uma pasta sincronizada em um dispositivo, onde podem conter todas as informações da *Cloud* permitindo assim, a busca de evidências sem precisar do envio dos

dados pelo provedor que por sua vez não os forneceu quando solicitado.

Uma vez alcançados os objetivos específicos, acredita-se ter atingido também o objetivo geral, pois foi possível realizar a pesquisa de procedimento e ferramentas para dar resposta a um incidente ocorrido na *Cloud Computing.*

7 CONCLUSÃO

O ambiente de *Cloud Computing,* surgiu como um benefício para redução de custos de empresas, instituições, usuários comuns e não só, tendo sido atualmente muito utilizada para armazenamento de informação. Esta tecnologia surge com a promessa de revolucionar a maneira como as informações são armazenadas e manuseadas. Porém, este ambiente tem alguns problemas no quesito segurança, principalmente no que se refere a prática de crimes digitais nesse ambiente. Para solucionar esses crimes, existe a perícia forense, mas que se esbarra com as questões legais pertinentes de cada país, visto que os seus dados podem estar em lugares totalmente diferentes, para isso precisa-se de melhorias na legislação, tanto nacional como na internacional e ferramentas ou mecanismos que possibilitem a extração dos dados, tornando dessa forma mais fácíl o processo de perícia forense nesses ambientes.

Foram encontrados alguns obstáculos no decorrer da pesquisa, entre eles estiveram a obtenção dos dados por meio do provedor, a escolha do estudo de caso a ser tratado, a não existência de legislação brasileira e internacional pertinente e a falta de ferramentas forenses para coleta de informações dos ambientes pesquisados. Porém esses obstáculos foram superados com a descoberta da pasta de sincronização e *backup* de alguns serviços de *Cloud* pública, sendo possível solucionar o estudo de caso onde foi possível apresentar e aplicar método, procedimento e ferramentas para perícia forense em *Cloud Computing.*

Concluindo, este trabalho apresenta as oportunidades para trabalhos futuros na área de perícia forense em ambientes *Cloud Computing*, tais como: estudo de outros métodos de perícia forense para estes ambientes, o desenvolvimento de ferramentas para extração de dados forenses nesses ambientes, bem como a criação de regras e propostas de leis para padronizar o acesso aos dados forenses.

REFERÊNCIAS

ADDED. **Soluções em Tecnologia da Informação – ISO9001:2008.** Disponível em: <http://www.added.com.br/news/saas-paas-iaas/>. Acesso em: 20 maio 2014.

AMAZON. **Aws Documentation:** Amazon Elastic Compute Cloud**.** Disponível em: < http://docs.aws.amazon.com/AWSEC2/latest/UserGuide/concepts.html >. Acesso em: 20 ago. 2014.

BAKER; CASWELL. **Snort Intrusion Detection and Prevention Toolkit**. Boston: Addison Wesley, 2004.

BERNARDO, Adauto de Souza. **Técnicas Computacionais no Auxílio à Perícia Forense na Análise de Evidências em Servidores GNU/LINUX.** TCC. – Universidade do Extremo Sul Catarinense – Unesc, 2006.

BONINI; OLIVEIRA JUNIOR. **Um catálogo de tecnologias e ferramentas para o desenvolvimento de sistemas em nuvem.** Disponível em: < https://www.google.com.br/search?q=Um+cat%C3%A1logo+de+tecnologias+e+ferramentas+para+o+desenvolvimento+de+sistemas+em+nuvem&oq=Um+cat%C3%A1logo+de+tecnologias+e+ferramentas+para+o+desenvolvimento+de+sistemas+em+nuvem&aqs=chrome..69i57j69i64.3545j0j7&sourceid=chrome&es_sm=93&ie=UTF-8t>. Acesso em: 20 Agos. 2014.

BERTOGLIO, Daniel Dalalana. **Perícia Forense:** Proposta de uma Metodologia de Coleta de Indícios para Ambiente Windows. Trabalho de Conclusão de Curso - Curso de Ciência da Computação, Departamento de Instituto de Ciências Exatas e Tecnológicas, Centro Universitário Feevale, Novo Hamburgo, 2008.

BRASIL. Lei 12737/2012. **Lei que Dispõe sobre a tipificação criminal de delitos informáticos.** Disponível em: <http://www4.planalto.gov.br/legislacao/legislacao-1/leis-ordinarias/2012-leis-ordinarias#content>. Acesso em: 28 mar. 2014.

B2NET. **ISS RealSecure SiteProtector** Disponível em: <http://www.b2net.co.uk/iss /iss_realsecure_siteprotector.htm> Acesso em: 14 set. 2014.

_____. Lei Nº 12.737, de 30 de Novembro de 2012. **Dispõe Sobre a Tipificação Criminal de Delitos Informáticos.** Disponível em: <https://www.planalto.gov.br/ccivil_03/_ato2011-2014/2012/lei/l12737.htm >. Acesso em: 11 maio 2014.

_____. Lei Ordinária 12.965. **Marco Civil da Internet.** Disponível em: < http://marcocivil.org.br/o-que-e-o-marco-civil-no-brasil/>. Acesso em: 30 jun. 2014.

CAMPELLO, WEBER**. O Sistema de Detecção de Intrusão Asgaard**. Disponível em: <labcom.inf.ufrgs.br/ceseg/anais/2001/05.pdf> Acesso em: 16 set. 2014.

CAPANEMA. **Cloud Computing**: A visão de um advogado. Disponivel em: < http://pt.slideshare.net/waltercapanema/cloud-computing-a-viso-de-um-advogado>. Acesso em: 26 set. 2014

CARRIER, Brian. **File System Forensic Analysis**. Indiana: Addison Wesley Professional, 2005.

CARUSO, Carlos A. A.; STEFFEN, Flávio Deny. **Segurança em Informática e de Informações.** 2. ed. São Paulo: SENAC, 1999.
CASEY, Eoghan. **Digital Evidence and Computer Crime:** Forensic Science, Computers, and the Internet. Londres: Academic Press, 2004.

_____. Crime **Investigation:** forensic tools and technology. 2. ed. London: Academic Press, 2003.

CASTRO, Rita de C.; SOUSA, Verônica L. Pimentel. **Segurança em Cloud Computing:** Governança e Gerenciamento de Riscos de Segurança, 2010. Disponível em: <http://www.infobrasil.inf.br/userfiles/26-05-S5-1-68740-Seguranca%20em%20Cloud.pdf>. Acesso em: 26 abr. 2014.

CERT.br. **Incidentes Reportados ao CERT.br de janeiro a dezembro de 2013.** Disponivel em: <http://www.cert.br/stats/incidentes/2013-jan-dec/análise.html>. Acesso em: 10 de maio 2014.

_____. **Estatísticas dos Incidentes Reportados ao CERT.br**. Disponivel em: < http://www.cert.br/stats/incidentes >. Acesso em: 12 maio 2014.

_____. **Tipologias de Incidentes Reportados ao CERT.br de Janeiro a Dezembro de 2013**. Disponível em: <http://www.cert.br/stats/incidentes/2013-jan-dec/tipos-ataque.html >. Acesso em: 17 maio 2014.

CASEY, E. **Crime Investigation:** forensic tools and technology. 2. ed. London: Academic Press, 2003.

QUEIROZ, Claudemir; VARGAS, Raffael. **Investigação e Perícia Forense Computacional**. Certificações, Leis Processuais, Estudos de Caso. Rio de Janeiro: Brasport, 2010. 134 p.

COMPUTERWORLD. **Nova Lei Informática em Angola e seus Efeitos nas Mídias**. Disponível em: <http://www.computerworld.com.pt/2011/05/23/nova-lei-informatica-em-angola-pode-ter-efeitos-nos-media-sociais>. Acesso em: 05 maio 2014.

CAMPELLO, WEBER. O Sistema de Detecção de Intrusão Asgaard Disponível em: <labcom.inf.ufrgs.br/ceseg/anais/2001/05.pdf> Acesso em: 16 out. 2014.

CRISTIANO, Aguinaldo Gregório. **Ferramentas e Metodologias para Resposta a Incidentes, Estudo de Caso "Helix 3".** TCC. – Universidade do Extremo Sul Catarinense – Unesc, 2011.

CSA. **Top Threats to Cloud Computing V1.0**. Cloud Security Alliance. . Disponível em: <https://cloudsecurityalliance.org/topthreats/csathreats.v1.0.pdf>. Acesso em: 18 out. 2014

DEFT. **Digital Evidence & Forensics Toolkit.** Manual de uso. . Disponível em: <http://www.deftlinux.net/doc/ITA-deft7.pdf >. Acesso em: 09 set. 2014.

DIDONÉ, QUEIRÓZ. **Computação Forense e as oportunidades oferecidas pela Computação em Nuvem**. Disponivel em Disponível em: <http://revista.univar.edu.br/index.php/interdisciplinar/article/view/144 >. Acesso em: 24 abr. 2014.

DROPBOX. **All About Dropbox.** Disponível em: < https://www.dropbox.com/aboutl >. Acesso em: 17 set. 2014.

DUMMLES. **Modelo de Nuvens**. Disponível em: <http://www.dummies.com/how-to/content/what-is-hybrid-cloud-computing.html>. Acesso em: 26 maio 2014.

DYKSTRA, J., SHERMAN, A.T. **Acquiring Forensic Evidence from Infrastructure-as-a-Service Cloud Computing:** Exploring and Evaluating Tools, Trust, and Techniques. Digital Investigation 2012. Supplement: S90–S98. The Proceedings of the Twelfth Annual DFRWS C.

ESES, Ramos. **O Impacto da Cloud Computing no Processo de Perícia Digital**. . Disponível em: < https://rennecloud.files.wordpress.com/2013/07/o-impacto-do-cloud-computing-no-processo-de-pericia-digital.pdf >. Acesso em: 23 maio 2014.

E-FENSE. **HELIX 3 Pro**: **Meeting your computer forensics needs**. Disponível em: <http://accessdata.com/downloads/media/Helix3Pro.pdf> Acesso em: 6 set. 2014.

FERNANDES, Fausto. **Pesquisa aponta que cloud computing ainda não é a bola da vez**. Disponível em: <http://www.ipnews.com.br/telefoniaip/index.php?option=com_content&id=19633&task=view >. Acesso em: 31 maio 2014.

FERRÃO, PLOTZE. **Computação Distribuída:** O Melhor Aproveitamento de Recursos Computacionais. Disponível em: <https://www.google.com.br/url?sa=t&rct=j&q=&esrc=s&source=web&cd=1&cad=rja&uact=8&ved=0CCwQFjAA&url=http%3A%2F%2Fclaretianodf.com.br%2Fdownload%3Fcaminho%3D..%2FSiteManager%2Fupload%2F4%2Frevistas%2Fsumario%2Fpdf%2F78.pdf&ei=WhSEU5L2NcqxsQTVqID4Bg&usg=AFQjCNEpsMaWJnQ_whuqXGUsJdgRwxCkDg&bvm=bv.67720277,d.cWc >. Acesso em: 30 abr. 2014.

FREITAS, OLIVEIRA. **Computação em Nuvens, Visão Comparativa entre as Principais Plataformas de Mercado**. Disponível em: <http://olavooneto.files.wordpress.com/2011/01/computacao_em_nuvens_visao_olavo_neto.pdf>. Acesso em: 20 maio 2014.

GOOGLE. **Tecnologias e Princípios.** Disponível em: < https://www.google.com/policies/technologies/ >. Acesso em: 18 set. 2014.

HAILEYS, Steve. **What is Computer Forensics: CyberSecurity Institute, 2002**. Disponível em: <http://www.cybersecurityinstitute.biz/forensics.htm>. Acesso em: 21 abr. 2014.

HURWITZ J.; BLOOR, R.; KAUFMAN, M. **Cloud Computing for DUMMIES.** HP Special Edition. Indianapolis: Wiley Publishing, INC., 2010.

IBM. **Fundamentos Cloud computing.** IBM, 01 Setembro 2012. Disponivel em: <http://www.ibm.com/developerworks/cloud/library/cl-cloudintro/>. Acesso em: 10 maio 2014.

IDC. **New IDC IT Cloud Services Servey Top Benefits and Challenges, 2009.** Disponível em: < http://blogs.idc.com/ie/?p=730>. Acesso em: 20 jul. 2014.

ISO 2005**. ISO/IEC 27001 - Information technology -** Security techniques - Information security management systems – Requirements. Disponível em: < http://www.iso.org/iso/catalogue_detail?csnumber=42103 >. Acesso em: 18 out. de 2014.

KARLITSCHEC. **OwnCloud:** Contributors Project Founder and Maintainer, General Architecture. Disponível em: < https://owncloud.org/user/?user=frank>. Acesso em: 08 ago. 2014.

KUNDRA, Vivek. **Federal Cloud Computing Strategy.** Disponível em: <http://www.whitehouse.gov/sites/default/files/omb/assets/egov_docs/federal-cloud-computing-strategy.pdf>. Acesso em: 02 jun. 2014.

LIMA, G. **A quantidade de informação gerada no mundo vs a qualidade.** Coruja de TI, 20 Setembro 2010. Disponível em: <http://blog.corujadeti.com.br/a-quantidade-de-informacao-gerada-no-mundo-vs-a-qualidade/>. Acesso em: 17 maio 2014.

MACHADO, LOUREIRO. **Comparação de Ferramentas de Software Livre para Administração de Nuvem Privada.** Disponível em: < http://www.ulbra.inf.br/joomla/images/documentos/TCCs/2011_02/PROJETO_RC_CLAITON_PRADO_MACHADO.pdf >. Acesso em: 02 ago. 2014.

MACHES, Bruce. **The Impact of Cloud Computing on Corporate IT Governance.** Disponível em: <http://www.hpcinthecloud.com/hpcwire/2010-01-25/the_impact_of_cloud_computing_on_corporate_it_governance.html>. Acesso em: 02 jun. 2014.

MARINS, Carlos Eduardo. **Desafios da informática forense no cenário de Cloud Computing**. Disponível em: <www.icofcs.org/2009/ICoFCS2009-PP10.pdf>. Acesso em: 25 mar. 2014.

MARTINS, G. A; THEÓPHILO, C. R**. Metodologia da investigação científica para**

ciências aplicadas – São Paulo: Atlas, 2009.

MELO, Sandro. **Computação forense com software livre:** conceitos, ferramentas e estudos de casos. Rio de Janeiro: Alta Books, 2009.

MICROSOFT. **About OneDrive.** Disponível em: < https://onedrive.live.com/about/pt-br/ >. Acesso em: 17 set. 2014.

MOHAY, G.; ANDERSON, A.; COLLIE, B.; VEL, O.; MCKEMMISH, R. **Computer and Intrusion Forensics.** London: Artech House, 2003.

MOHAMED, A. **History of Cloud Computing.** ComputerWeekly.com, 27 Março 2009. Disponivel em: <http://www.computerweekly.com/Articles/2009/06/10/235429/A-history-of-cloud-computing.htm>. Acesso em: 12 abr. 2014.

MULLER, Nicolas. **Computação nas nuvens, 2008**. Disponível em: <http://www.oficinadanet.com.br/artigo/923/computacao_nas_nuvens>. Acesso em: 03 jun. 2014.

NIST. **The NIST Definition of Cloud Computing, 2009**. Disponível em: <csrc.nist.gov/groups/SNS/cloud-computing/cloud-def-v15.doc>. Acesso em: 22 ago. 2014

_____. **Cloud ComputingStandards Roadmap**. Disponivel em: <http://www.nist.gov/itl/cloud/upload/NIST_SP-500-291_Version-2_2013_June18_FINAL.pdf>. Acesso em: 22 ago. 2014.

_____. **Cloud Computing Forensic Science Challenges**. Disponivel em: <http://csrc.nist.gov/publications/drafts/nistir-8006/draft_nistir_8006.pdf >. Acesso em: 20 ago. 2014.

NMAP. **Security** Disponível em: <http://nmap.org/> Acesso em: 11 Setembro. 2014.

NUBLING, Gabriela. **Cloud Computing aplicada ao Cenário Corporativo, 2011**. Disponível em: < http://www.fateCSP.br/dti/tcc/tcc0038.pdf >. Acesso em: 12 maio 2014.

OPEN GROUP (The Open Group). **Cloud Computing Explained**. San Francisco: The Open Group, 2011.

POPOLIN, JOSÉ. **Análise de Ferramentas para computação forense em sistemas NTFS.** Disponível em: <www.ginux.ufla.br/files/mono-JoseGeraldoPopolin_0.pdf>. Acesso em: 28 mar. 2014.

PROSISE, C.; MANDIA, K. **Incident Response & Computer Forensics**. 2. ed. Berkeley: McGraw-Hill, 2003.

RABANEDA. **A Segurança Das Informações na Clould Computing.** Disponível em: <http://prosaepolitica.com.br/2010/04/23/fabiano-rabaneda-a-seguranca-das-informacoes-na-clould-computing/#.VFmafvnF8rU > Acesso em: 23 set. 2014.

RAIMUNDO, Neto. Implementacão de Ferramenta para Deteccao de Intrusao Disponível em: <www.faete.edu.br/revista/artigo-rneto.pdf> Acesso em: 13 set. 2014.

RUAN, Keyun. **Challenges of cloud forensics**: A survey of the missing capabilities. <http://scholar.google.com/citations?view_op=view_citation&hl=en&user=yWHoDqAAAAAJ&citation_for_view=yWHoDqAAAAAJ:d1gkVwhDpl0C>. Acesso em: 20 ago. 2014.

_____. **Cloud Forensics**: An Overview. Disponível em: <http://www.researchgate.net/profile/Tahar_Kechadi/publication/229021339_Cloud_forensics_An_overview/links/02bfe50f55377829e3000000>. Acesso em: 20 ago. 2014.

_____. **Cloud Forensic Maturity Model.** Disponível em: <http://link.springer.com/chapter/10.1007/978-3-642-39891-9_2#page-1>. Acesso em: 20 ago. 2014.

SACRAMENTO. **Estudo Sobre As Ferramentas de Rede para Perícia Forense:** Estudo De Caso Do Arquivo Evidências. PCAP. Disponível em: <http://saomateus.multivix.edu.br/wp-content/uploads/2013/05/Ferramentas-de-rede-para-pericia-forense.pdf>. Acesso em: 30 abr. 2014.

SCARFONE, Karen, GRANCE, Tim, MASONE, Kelly. Computer Security Incident Handling Guide. Disponível em: <http://csrc.nist.gov/publications/nistpubs/800-61-rev1/SP800-61rev1.pdf> Acesso em: 12 set. 2014.

SCHWEITZER, DOUGLAS. **Incident Response:** Computer Forensics Toolkit. Indiana: Wiley Publishing, 2003.

SOUZA, F. R. C.; MOREIRA, L. O.; MACHADO, J. C. **Computação em Nuvem:** Conceitos, Tecnologias, Aplicações e Desafios. Fortaleza, 2009.

SUN MICROSYSTEMS. **Introduction to Cloud Computing architecture White Paper**. Santa Clara, Junho 2009.

SYMANTEC. **Symantec Intruder Alert 3.6.** Disponível em: <http://www.superwarehouse.com/Symantec_Intruder_Alert_3.6/16-00-00035/p/66787> Acesso em: 13 set. 2014.

TANENBAUM, Andrew S. **Distributed Systems:** Principles and Paradigms.

TAURION, C. **Computação em Nuvem:** Transformando o mundo da tecnologia da informação. Rio de Janeiro: Brasport, 2009.

TECMUNDO. **Comparação:** Google Drive, SkyDrive, Dropbox, Ubuntu One, iCloud, Box e SugarSync. Disponível em: < http://www.tecmundo.com.br/computacao-em-nuvem/22667-comparacao-google-drive-skydrive-dropbox-ubuntu-one-icloud-box-e-sugarsync.htm > Acesso em: 31 out. 2014.

TUTORIALSPOINT. **Community Cloud Model.** Disponível em: <http://www.tutorialspoint.com/cloud_computing/cloud_computing_community_cloud_model.htm>. Acesso em: 20 maio 2014.

VACCA, JOHN R. **Computer Forensics:** Computer Crime Scene Investigation.

WEBBA, Sidney Roberto da Silva. **Procedimentos Computacionais no Auxílio à Perícia Forense Aplicada em Web Browsers.** TCC. – Universidade do Extremo Sul Catarinense – Unesc, 2010.

APÊNDICE (S)

APÊNDICE A - RELATÓRIO COM INFORMAÇÕES DA CRIAÇÃO DE IMAGEM

Created By AccessData® FTK® Imager 2.5.3.14 071018
Case Information:
Case Number: 1
Evidence Number: 1
Unique Description: 1
Examiner: celio
Notes: n1

Information for C:\Users\Elbad\Desktop\p1:
Physical Evidentiary Item (Source) Information:
[Drive Geometry]
Bytes per Sector: 512
Sector Count: 2.170.872
Source data size: 1059 MB
Sector count: 2170872
[Computed Hashes]
MD5 checksum: fbb8dc7d4d320c8c2f0d93389260010c
SHA1 checksum: 611cfcf660edc68ead61cd688549cd8b12d824cc

Image Information:
Acquisition started: Tue Oct 14 00:09:18 2014
Acquisition finished: Tue Oct 14 00:10:13 2014
Segment list:
C:\Users\Elbad\Desktop\p1.001

Image Verification Results:
Verification started: Tue Oct 14 00:10:13 2014
Verification finished: Tue Oct 14 00:10:44 2014
MD5 checksum: fbb8dc7d4d320c8c2f0d93389260010c : verified
SHA1 checksum: 611cfcf660edc68ead61cd688549cd8b12d824cc : verified

APÊNDICE B – OS PRIMEIROS PASSOS REALIZADOS PARA ANÁLISE FORENSE NO AUTOPSY

```
Tue Oct 14 18:36:49 2014: '/usr/local/bin/img_stat' -t "/home/perito/Downloads/p1.001"
Tue Oct 14 18:36:51 2014: '/usr/local/bin/fsstat' -t -i raw "/home/perito/Downloads/p1.001"
Tue Oct 14 18:58:48 2014: '/usr/local/bin/img_stat' -t "/home/perito/Downloads/p1.001"
Tue Oct 14 18:58:48 2014: '/usr/local/bin/fsstat' -o 0 -i raw -f ntfs "/home/perito/Downloads/p1.001"
Tue Oct 14 18:58:48 2014: /bin/cp '/home/perito/Downloads/p1.001'
'/opt/evidence/CELFpesquisaeproducao/host1/images/p1.001'
Tue Oct 14 19:17:59 2014: '/usr/local/bin/fls' -f ntfs -la -z "brasil" -s '0' -o 0 -i raw
'/opt/evidence/CELFpesquisaeproducao/host1/images/p1.001' 5
Tue Oct 14 19:21:23 2014: '/usr/local/bin/fls' -f ntfs -la -z "brasil" -s '0' -o 0 -i raw
'/opt/evidence/CELFpesquisaeproducao/host1/images/p1.001' 35
Tue Oct 14 19:22:39 2014: '/usr/local/bin/fls' -f ntfs -la -z "brasil" -s '0' -o 0 -i raw
'/opt/evidence/CELFpesquisaeproducao/host1/images/p1.001' 35
Tue Oct 14 19:23:56 2014: '/usr/local/bin/fls' -f ntfs -la -z "brasil" -s '0' -o 0 -i raw
'/opt/evidence/CELFpesquisaeproducao/host1/images/p1.001' 5
Tue Oct 14 19:24:02 2014: '/usr/local/bin/fls' -f ntfs -la -z "brasil" -s '0' -o 0 -i raw
'/opt/evidence/CELFpesquisaeproducao/host1/images/p1.001' 35
Tue Oct 14 19:24:05 2014: '/usr/local/bin/icat' -f ntfs  -o 0 -i raw
'/opt/evidence/CELFpesquisaeproducao/host1/images/p1.001' 36-128-1 | '/usr/bin/file' -z -b -
Tue Oct 14 19:24:06 2014: '/usr/local/bin/icat' -f ntfs  -o 0 -i raw
'/opt/evidence/CELFpesquisaeproducao/host1/images/p1.001' 36-128-1 | '/usr/bin/file' -z -b -
Tue Oct 14 19:24:07 2014: '/usr/local/bin/icat' -f ntfs   -o 0 -i raw
'/opt/evidence/CELFpesquisaeproducao/host1/images/p1.001' 36-128-1 | '/usr/bin/file' -z -b -
Tue Oct 14 19:24:07 2014: '/usr/local/bin/icat' -f ntfs   -o 0 -i raw
'/opt/evidence/CELFpesquisaeproducao/host1/images/p1.001' 36-128-1
Tue Oct 14 19:24:16 2014: '/usr/local/bin/icat' -f ntfs  -o 0 -i raw
'/opt/evidence/CELFpesquisaeproducao/host1/images/p1.001' 36-128-1 | '/usr/bin/file' -z -b -
Tue Oct 14 19:24:16 2014: '/usr/local/bin/icat' -f ntfs  -o 0 -i raw
'/opt/evidence/CELFpesquisaeproducao/host1/images/p1.001' 36-128-1 | '/usr/bin/file' -z -b -
Tue Oct 14 19:24:16 2014: '/usr/local/bin/icat' -f ntfs  -o 0 -i raw
'/opt/evidence/CELFpesquisaeproducao/host1/images/p1.001' 36-128-1 | '/usr/bin/file' -z -b -
Tue Oct 14 19:24:16 2014: '/usr/local/bin/icat' -f ntfs  -o 0 -i raw
'/opt/evidence/CELFpesquisaeproducao/host1/images/p1.001' 36-128-1 | '/usr/bin/file' -z -b -
Tue Oct 14 19:24:16 2014: '/usr/local/bin/icat' -f ntfs   -o 0 -i raw
'/opt/evidence/CELFpesquisaeproducao/host1/images/p1.001' 36-128-1 | '/usr/bin/file' -z -b -
Tue Oct 14 19:24:16 2014: '/usr/local/bin/icat' -f ntfs   -o 0 -i raw
'/opt/evidence/CELFpesquisaeproducao/host1/images/p1.001' 36-128-1
Tue Oct 14 19:24:20 2014: '/usr/local/bin/icat' -f ntfs  -o 0 -i raw
'/opt/evidence/CELFpesquisaeproducao/host1/images/p1.001' 36-128-1 | '/usr/bin/file' -z -b -
Tue Oct 14 19:24:20 2014: '/usr/local/bin/icat' -f ntfs  -o 0 -i raw
'/opt/evidence/CELFpesquisaeproducao/host1/images/p1.001' 36-128-1 | '/usr/bin/file' -z -b -
Tue Oct 14 19:24:20 2014: '/usr/local/bin/icat' -f ntfs   -o 0 -i raw
'/opt/evidence/CELFpesquisaeproducao/host1/images/p1.001' 36-128-1 | '/usr/bin/file' -z -b -
```

Forense Computacional: Método Procedimento e Ferramentas para Perícia Forense em Cloud Computing

Célio Fabrício da Conceição Filipe[1], Paulo João Martins[2], Luciano Antunes[2]

[1]Curso de Ciências da Computação – Universidade do Extremo Sul Catarinense (UNESC) – Criciúma, SC – Brasil

[2]Curso de Ciências da Computação – Universidade do Extremo Sul Catarinense (UNESC) – Criciúma, SC – Brasil

celiofilipe23@hotmail.com, pjm@unesc.net, luc@unesc.net,

Abstract. *The Cloud Computing is nowadays one of the trends in the technology market, providing its users a different view on how to store and manage your data and change your way of working. As there are new mechanisms for the use of Cloud Computing, there are still challenges, such as obtaining or recovery of forensic data and perform computer forensics. This research aimed to provide a general approach around the forensic expertise in Cloud Computing, applying a case study to describe a method to retrieve and analyze the data in a Google Drive environment. To carry out the work, followed the following methodology: bibliographic research, preparation of a fictional case study that was solved by applying the Standard Operating Procedures methodology (SOP) in seven (7) steps that are: authorization, equipment preparation, collection and preservation, forensic image, examination and analysis, documentation, reporting and review. It was possible to study and apply the concepts of computer forensics involving Cloud Computing environments, where it was possible to successfully analyze existing files, was then used Deft 7.2 environment, the tools AccessData FTK Imager, Autopsy and synchronization folder of Google Drive , evidence has been found in some of the examined files.*
Keywords: *Cloud Computing. Forensic Expertise. Security. Digital Crimes. Cloud Forensics.*

Resumo. *A Cloud Computing tem sido atualmente uma das tendências no mercado de tecnologia, proporcionando aos seus usuários outra visão sobre como armazenar e gerenciar os seus dados e alterar a sua maneira de trabalhar. Por mais que surjam novos mecanismos para o uso da Cloud Computing, ainda existem desafios, tais como: obtenção ou recuperação de dados forenses, bem como realizar a perícia forense computacional. Esta pesquisa visou fornecer uma abordagem geral em torno da perícia forense em Cloud Computing, aplicando um estudo de caso para descrever um método para recuperar e analisar os dados existentes em um ambiente Google Drive. Para a realização do trabalho, seguiu-se a seguinte metodologia: pesquisa bibliográfica, elaboração de um estudo de caso fictício que foi solucionado aplicando a metodologia SOP em sete (7) etapas que são: autorização, preparação do equipamento, coleta e preservação, imagem forense, exame e análise, documentação, relatório e revisão. Conseguiu-se estudar e aplicar os conceitos de perícia forense computacional envolvendo ambientes Cloud Computing, onde foi possível analisar com sucesso os arquivos existentes, foi então usado o ambiente Deft 7.2, as ferramentas AccessData FTK Imager, Autopsy e a pasta de sincronização do Google Drive, tendo sido encontradas provas em alguns dos arquivos examinados.*

Palavras-chave: Cloud Computing. Perícia Forense. Segurança. Crimes Digitais. Cloud Forensics.

1. Introdução

Nos dias de hoje as tecnologias de informação tem evoluído com uma velocidade incontrolável, esta rápida evolução têm trazido inúmeros benefícios a todos, e com ela, também algumas consequências. O computador não é o único meio tecnológico e digital que faz parte do nosso cotidiano, existem hoje outros aparelhos como telefones celulares, tablets entre outros, desempenhando um papel fundamental na organização e difusão de informações, compartilhamento de dados, pesquisas por meio da Internet e no entretenimento. Têm-se muitos benefícios, porém surge um problema no que se refere à falta de segurança.

Com o uso crescente desses meios tecnológicos, bem como a difusão e massificação da Internet, surge a *Cloud Computing* ou computação em nuvem. Nesse modelo é possível armazenar e acessar dados, prover recursos, entre outros serviços. Este recurso tem sido muito difundido e com ele a insegurança por parte dos usuários, por não saberem o lugar físico onde seus dados estão armazenados, até que ponto eles estão seguros e como recuperá-los se forem apagados em um ambiente na nuvem.

Segundo Marins (2009), a *Cloud Computing* é uma expansão genérica que descreve a evolução de tecnologias e processos, compostos de serviços, aplicações, informações e infraestrutura distribuída, de modo que estes possam ser organizados dinamicamente, elástica e rapidamente na medida em que forem consumidos.

Desta forma, o presente trabalho realizou o estudo de algumas plataformas de ambiente em nuvem, que foram definidas no decorrer da pesquisa, bem como o processo de perícia forense usado em um desses ambientes, focando-se na metodologia de coleta e análise de evidências em ambientes *Cloud Computing.*

2. Perícia Forense Computacional

A computação forense é considerada uma ciência multidisciplinar relativamente nova, e quando associada a técnicas de investigação ajuda a determinar e analisar evidências seguindo métodos e procedimentos definidos pelas suas etapas de perícia (DIDONÉ; QUEIRÓZ, 2011).

Segundo Steve Haileys, CEO e professor do Instituto de Segurança Cibernética (*Institute Cyber Security* ICS), a Perícia Forense Computacional é a preservação, identificação, coleta, interpretação e documentação de evidências computacionais, incluindo as regras de processo legal, integridade da evidência, provisão da opinião de especialista em uma corte judicial e relatório do factual da evidência, ou algum outro processo legal com relação ao que foi encontrado (HAILEYS, 2002).

A Computação Forense é uma área de especialização relativamente nova no mundo e tem se desenvolvido muito rápido, principalmente pela necessidade que as instituições legais têm ao atuarem no combate aos crimes eletrônicos. Este processo tem gerado ao longo dos anos, resultados positivos e confiáveis decorrentes de procedimentos e protocolos detalhados com documentações e revisões aceitas pela comunidade cientifica. O uso de metodologia e de protocolos deve ser considerado na prática de investigação, como garantia de aceitação em uma corte judicial (CRISTIANO, 2011; MELO, 2009).

2.1. Crimes Digitais

No mundo atual, a sociedade tem sentido a mudança de certos hábitos e costumes, tem se notado uma mudança no jeito de se comunicar, trabalhar, lecionar, aprender, entre outros. A

proliferação de meios tecnológicos como computadores pessoais, acesso fácil à Internet, e um mercado em expansão relacionado com novos dispositivos de comunicação, mudaram a forma como se gasta o tempo e como se fazem negócios.
Crime do latim *crimen*, é qualquer violação grave da lei moral, civil, religiosa ou ato ilícito cometido em uma sociedade passível de uma sansão penal (WEBBA, 2010).
Crimes digitais são violações graves a lei moral, civil ou ato ilícito cometido por meio de um computador, celular ou qualquer meio digital (tecnológico). Eles podem assemelhar-se a alguns crimes comuns, a única diferença é que no crime comum não é obrigatório o uso de computadores ou alguma tecnologia digital.
Alguns conceituados escritores brasileiros como Pinheiro (2001) em suas obras literárias classificam os crimes em três subgrupos descritos a seguir:

a) **crimes digitais ou virtuais puros** – é toda conduta ilícita que visa lesar o hardware ou o software de um computador ou sistema informatizado;
b) **crimes digitais ou virtuais mistos** – eles utilizam a Internet ou redes de computadores para cometer delitos, não visam sistemas informáticos e são normalmente usados em transações ilegais de valores de contas correntes;
c) **crimes digitais ou virtuais comuns** – utilizam a Internet ou as redes públicas de computadores para realização de qualquer delito, ele consta no código penal.

3. Cloud Computing

Nas últimas décadas o mundo tem convivido com novas tendências tecnológicas, as empresas ao seu redor também têm sido impulsionadas pelas tecnologias de informação. A Internet tem sido o percursor de uma boa parte dessa mudança socioeconómica, e tem levado a mudanças em variados extratos, seja na forma como se comunicam, trabalham, estudam e até como se divertem, nesse segmento surge a *Cloud Cumputing* (LIMA, 2009).
A *Cloud Computing* ou computação em nuvem (tradução literal para o português), segundo o *National Institute of Standards and Technology* (NIST) é um modelo que possibilita acesso de modo conveniente e sob demanda a um conjunto de recursos computacionais configuráveis (por exemplo, redes, servidores, armazenamento, aplicações e serviços) que podem ser rapidamente adquiridos e disponibilizados com mínimo esforço gerencial ou interação com provedor de serviços (NIST, 2009). Ela é constituída em camadas e cada uma oferece níveis distintos de funcionalidades. Esta estratificação dos componentes da nuvem garante um meio para que as camadas tornem-se um bem como energia elétrica, serviço de telefone entre outros. A mercadoria que ela vende é o poder de computação a um custo menor e com isso, poucas despesas para o usuário. Ela está pronta para se tornar o próximo serviço de mega utilidade (IBM, 2012).

3.1 Modelos de Implantação de Cloud Computing

Segundo o princípio de computação em grade (*Grid*) a *Cloud Computing* ou computação em nuvem é a utilização da memória e das capacidades de armazenamento e cálculo de computadores, softwares compartilhados e conectados por meio de uma rede (SISNEMA, 2009). Na *Cloud* os dados são armazenados em serviços que podem ser acessados de qualquer parte do mundo, a qualquer hora e sem haver a necessidade de instalar um banco de dados ou qualquer software, o seu acesso é feito por meio de uma rede privada ou pela Internet (de onde surge a denominação nuvem do inglês *Cloud*) viabilizando o seu uso comparado com o uso de servidores como unidade principal (NUBLING, 2011).
Existem disponíveis vários modelos para se implantar uma *Cloud Computing*, porém dois são primordiais para a existência dos demais, eles são classificados como:

a) ***Cloud* Pública –** é um conjunto de hardware, redes, armazenamento, serviços, aplicações e interfaces, operados por terceiros para uso de qualquer pessoa ou empresa desde que concorde com as políticas do provedor. Nela não podem ser aplicadas restrições de acesso no que concerne ao gerenciamento de redes, também não podem ser utilizadas técnicas para autenticação e autorização (NUBLING, 2011; SOUSA, 2011).
b) ***Cloud* Privada –** tem como base arquiteturas de Data Center que são propriedade de uma única empresa que oferece escalabilidade, flexibilidade, provisionamento, monitoramento e automação. O seu objetivo não é a venda de serviços para clientes externos e sim ter os benefícios de uma nuvem sem abrir mão do controle de administrar os seus próprios dados.

3.1 Modelos de Serviço Cloud Computing

Existem atualmente diversos modelos de serviço de *Cloud Computing*, tal diversidade é benéfica, pois ela permite que a empresa ou pessoa possa adquirir o serviço que melhor se adequa as suas necessidades (TAURION, 2009). A arquitetura de *Cloud Computing* segundo algumas literaturas, é dividida em três camadas distintas que são a *IaaS, PaaS e SaaS*. Estas camadas podem ter seu monitoramento ou gerenciamento independentes das demais camadas, garantindo maior escalabilidade, flexibilidade e reutilização no que diz respeito à adição ou substituição de recursos computacionais sem interferir ou afetar as demais camadas (SOUZA, 2009):

a) **Infrastructure as a Service (Iaas)** - pertence a camada mais baixa e estrutural que é fundamental para o funcionamento de *Coud Computing*, representando toda arquitetura física como *Data centres*, servidores, hardwares e equipamentos de energia e climatização, que possibilitam e garantam o armazenamento e a transmissão de dados e aplicações de maneira rápida por intermédio da Internet (ADDED, 2013). Ele possibilita o acesso a recursos fundamentais, como armazenamento virtual, máquinas virtuais, máquinas físicas, endereço de IP, pacotes de *softwares*, rede local virtual, armazenamento em disco de máquina virtual, entre outros (TUTORIALSPOINT, 2013).
b) **Platform as a Service (PaaS)** - ela é muito utilizada pelos desenvolvedores de aplicações, que aproveitando as bases do IaaS são criadas soluções e recursos necessários para suporte de segurança, sistemas operacionais, escalabilidade, organização de banco de dados e armazenamento (ADDED, 2013). Ele tem como suas maiores características oferecer um ambiente de desenvolvimento baseado em navegadores, ferramentas de serviço web, fluxo de trabalho e processos de aprovação, interação com aplicações da mesma plataforma (TUTORIALSPOINT, 2013).
c) **Software as a Service (Saas)** - é um modelo que permite fornecer um software como um serviço para os usuários finais, ele é um software que é implantado em um serviço hospedado, acessado via Internet e as atualizações são por conta dos fornecedores (TUTORIALSPOINT, 2013). Existem vários módulos SaaS, os mais usuais são os módulos de Finanças e faturamento, Recursos Humanos (RH), *Help Desk* e o *Customer Relationship Management* (CRM) (FREITAS; OLIVEIRA, 2010).

4. Perícia Forense em Ambientes Cloud Computing

Quando se fala de *Cloud Computing* logo surge os seus prós e os seus contras. Os seus benefícios são variados entre eles estão flexibilidade, baixo custo de manutenção, administração, implantação e menor tempo na implantação de novos serviços, porém os seus

desafios também despertam o ceticismo dos usuários dessa nova ferramenta da computação contemporânea. A despeito da descrença, este ambiente continua a crescer, inovar e conquistar setores importantes da sociedade em todo o planeta.
Não obstante aos progressos que são satisfatórios, esta tecnologia ainda tem inúmeros desafios que precisam de um maior engajamento da indústria tecnológica para ultrapassá-los. A perícia nesses ambientes é vista por muitos especialistas de TI não só, como um dos maiores desafios, pois envolvem questões técnicas, legais e organizacionais, o que faz com que surjam alguns questionamentos quanto ao modelo que será implantado, se estará na própria nuvem (*Cloud Forensics*), ou será desenvolvido outros mecanismos para realizar a perícia (DIDONÉ, 2011; DYKSTRA, 2012).

4.1. Cloud Forensics

A NIST (2014) define a *Cloud Computing* forensic como a aplicação de princípios científicos, tecnológicos, prática derivada de métodos para reconstruir eventos passados ou informações apagadas de uma nuvem, por meio de identificação, coleta comprovada, preservação, análise, interpretação e elaboração de relatórios de evidências digitais.
Segundo Ruan (2013), a *Cloud Forensics* é a aplicação da ciência forense digital em modelos de Cloud Computing, tratando como se fosse uma abordagem híbrida forense da rede in vivo e em grande escala para obter as evidências digitais.
Em modo organizacional, a *Cloud Forensic* envolve interação entre os atores da cloud (provedores, consumidores, portador, auditor) com o objetivo de facilitar tanto a nível interno como externo nas investigações (NIST, 2014).

4.2 Cloud Forensic e Seu Uso

Atualmente o uso da *Cloud Forensic* é feito da em investigação, resolução de problemas internos e externos, monitoramento de logs, sistema de recuperação de dados na *Cloud* e conformidade regulamentar *(*RUAN, 2013):

4.3 Metodologia de Processo de Perícia Forense

Ao longo do tempo, variados modelos de processos foram desenvolvidos para perícia forense digital, a NIST destacou os oito passos mais usados nos Estados Unidos, sendo todos eles baseadas nas leis existentes no país e são eles: busca pela autoridade, cadeia de custódia, imagem e função *hash*, ferramentas de validação, análise, repetitividade e reprodutibilidade, relatório e por último a apresentação.
A metodologia de perícia forense em ambientes *Cloud Computing* não difere muito das outras, o único processo diferente e um dos mais desafiadores é na coleta, o acesso as informações é mais complexo pois na maior parte dos casos elas encontram-se em jurisdições diferentes.

4.4 Método de Acesso aos Dados Forenses

Para que seja possível a realização de uma perícia forense em *Cloud Computing*, é necessário algum método de acesso aos dados. Embora não hajam métodos padronizados por falta de uma legislação apropriada, existem alguns procedimentos que podem dar acesso aos dados (DYKSTRA, RIEHL, 2012; NIST, 2014):

a) **por meio judicial:** em alguns países, tais como como Estados Unidos da América, Brasil, Angola e entre outros, a lei permite que polícia possa coletar os dados, em casos de crimes contra instituições do estado. No caso de processo judicial de um cliente comum, o tribunal solicita os dados ao provedor e destaca um perito para realizar a análise forense dos dados;)**por carta ou pelo suporte técnico:** os clientes que pretendem ter acesso aos seus dados, podem fazê-lo por meio de uma carta que deve ser encaminhada ao provedor do serviço ou utilizar o serviço de suporte ao cliente e solicitar os dados. Despendendo da política de privacidade, acesso aos dados da *Cloud* e até da falta de comprometimento do provedor, o cliente corre o risco de não ter acesso à esses dados;
b) **por backup ou pasta de sincronização:** este recurso está disponível em vários provedores, ele possibilita ao usuário criar uma pasta de sincronização com a sua conta, e automaticamente ela realiza o *download* todos os dados existentes na *Cloud.* Isso possibilita aos usuários e aos peritos, terem acesso aos dados existentes na *Cloud*, inclusive os dados apagados, desde que eles tenham sido apagados após a instalação da pasta de sincronização.
c) Alguns provedores criaram mecanismos para que o usuário tenha acesso aos seus dados apagados, tal recurso é a pasta reciclagem, ela preserva as informações apagadas por no máximo 30 dias, após este prazo os dados são excluídos definitivamente.

4.5 Desafios da Cloud Forensics

Diante do que foi abordado ao longo do presente capítulo, tem se ainda muitos desafios. Na dimensão técnica, existem ferramentas e procedimentos muito limitados em todos os cinco principais componentes. Na dimensão legal atualmente não existe qualquer acordo entre as provedoras de *Cloud Computing* sobre a investigação colaborativa (NIST, 2014; RUAN, 2013). O direito internacional cibernético e as políticas devem evoluir para ajudar a resolver as questões que envolvem investigações de Multijurisdição.

5. Método e Procedimento para Perícia Forense em Cloud Computing

O advogado, professor e coordenador do curso de direito eletrônico da Escola da Magistratura do Estado do Rio de Janeiro (*EMERJ*) *Walter Capanema*, aborda *Cloud Computing* como um contrato de prestação de serviços, em que uma empresa permite o uso de seus recursos computacionais por clientes. Estes ambientes são recursos computacionais muito usado e difundido pelas grandes empresas de tecnologia nos últimos anos, eles vêm acompanhados de muita praticidade, flexibilidade, economia, tendo como veículo e seu maior aliado à Internet (NUBLING, 2011). Um dos desafios para os usuários deste recurso, tem sido a proteção e recuperação dos dados, bem como a coleta de evidências em caso de ocorrência de algum crime digital ou perda de dados nesses ambientes.
Para a presente pesquisa, foram realizados estudos dos serviços de *Cloud Computing* Pública (*SaaS*) mais usados pelos usuários, entre eles encontravam-se o *Google Drive*, *DropBox e OneDrive*. Foi então escolhido o *Google Drive* para pesquisa, em função do espaço de armazenamento gratuito (que é de 15 GB), pelas ferramentas e recursos à ele incorporado e pelo seu crescente número de usuários.

Uma vez escolhido o ambiente para a realização da pesquisa, foi criado um estudo de caso referente ao processo de perícia em um ambiente *Cloud Computing.*

5.1 Estudo de Caso

Foi adaptado um estudo de caso do livro "Investigação e Perícia Forense Computacional" de Claudemir Queiroz e Raffael Vargas, que permite demonstrar os procedimentos para busca de evidências. No caso uma empresa estava envolvida em escândalos por conta da exposição de documentos sigilosos referentes a sua situação financeira, investimentos e projetos futuros na internet por meio de uma *Cloud Google Drive* e convocou um perito para realizar busca de evidência para concluir as suspeitas.

5.2 Metodologia

Quando se trata de perícia forense computacional, cada caso tem as suas particularidades, portanto, não existem modelos específicos para cada caso, existem sequências de práticas metodológicas para se realizar uma perícia. Para este caso foi escolhida a *Standard Operating Procedures* (*SOP*) que é muito usada no Brasil. As suas etapas podem ser visualizadas na figura 1, seguem as etapas: Autorização e Preparação, Identificação, Coleta e Preservação, Imagem Forense, Exame e Análise, Documentação, Relatório e Revisão.

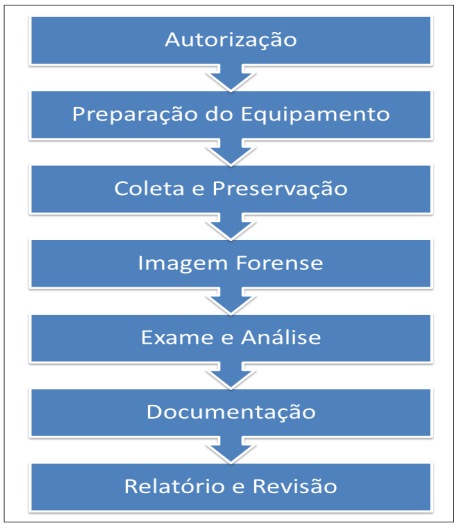


Figura 1- Metodologia SOP.

5.2.1 Autorização

Para a realização do seguinte trabalho não foi necessário uma autorização legal, pois o mesmo trata-se que um estudo de caso fictício para fins acadêmicos. Porém foram levados em conta todos os procedimentos da metodologia *SOP* e foram asseguradas as normas na preparação e organização das informações.

5.2.2 Coleta da prova

Tratando-se de perícia em ambientes *Cloud Computing*, o desafio está no acesso aos dados, visto que os servidores encontram-se em países diferentes e com políticas diferentes (RUAN, 2013). Sendo que o ambiente em que ocorreu o incidente é o *Google Drive* e que, a empresa *Google* tem uma representação no Brasil, foi adotada a metodologia de acesso aos dados forenses da conta, para tal foi encaminhado ao órgão uma carta (anexo B) solicitando os

dados forenses da conta, não tendo sido respondida até a conclusão desta pesquisa. Foi então adotado o método de acesso aos dados pelo suporte técnico (anexo C), tendo sido recuperado todos os dados apagados da conta *Cloud*. Os dados foram recuperados, porém eles foram disponibilizados na própria *Cloud*.
Segundo Fabiano Rabaneda advogado e especialista em direito eletrônico e tecnologia da informação, os dados existentes em uma *Cloud* não podem só ser obtidos através do provedor e sim por meio de *backup*. Os *backups* de dados na *Cloud* são uma solução que muitos provedores criaram para que o usuário tenha os dados sob seu domínio. Em alguns casos específicos como *DropBox*, *Google Drive*, *OneDrive* entre outros, ao baixar e instalar o software do provedor, é criada uma pasta sincronizada com a conta, onde todos os dados existentes na *Cloud* são baixados para o computador ou outro dispositivo computacional, servindo como *backup*. Sendo esta pasta sincronizada o único meio criado pelos provedores para que o usuário tenha uma réplica (cópia) do que existe na *Cloud*, o perito pode usar a mesma para extrair os dados da *Cloud* e buscar evidências na mesma.

5.2.3 Preparação do equipamento

Para que seja realizada uma perícia forense é imprescindível a criação de condições para que ela tenha o máximo de eficácia. Estas condições são espaço disponível para manusear os equipamentos, hardware e softwares. Para tal, foi criado um laboratório com duas máquinas, seguindo todos os pré-requisitos para uma perícia forense. Em um dos computadores foi criado o incidente e o outro foi utilizado para manusear e analisar as evidências.

5.2.4 Imagem forense

Para a realização da análise dos dados, foi antes criada com êxito uma imagem da partição onde encontram-se os dados, por meio da ferramenta AccessData *FTK Imager* e ao final foi gerado um *Hash* com o algoritmo *Md5 e Sha1*. Posteriormente foi coletada e armazenada em um *HD* externo formatado com capacidade de 500 *GB.*

5.2.5 Exame e análise

Para a realização do exame e análise, primeiramente foram duplicadas as imagens para que no caso de perda dos dados ou alteração do cenário por conta dos procedimentos de perícia, o perito não tenha de realizar a coleta. Posteriormente foi copiada para o ambiente do *DEFT 7.2* uma das cópias da imagem para análise forense.
Uma vez a imagem copiada no ambiente, é executada a ferramenta de análise forense '*Autopsy'* existente no ambiente *DEFT* e criado o caso contendo as informações pré-definidas nas telas do Autopsy. Posteriormente foi realizada a análise das informações na imagem, onde foi possível visualizar todos os arquivos existentes na partição, inclusive os apagados. No diretório Google Drive/ encontram-se os dados sincronizados com a *Cloud* (*backup* físico do cliente) e são neste diretório que podem ser encontradas as provas do crime (figura 2).

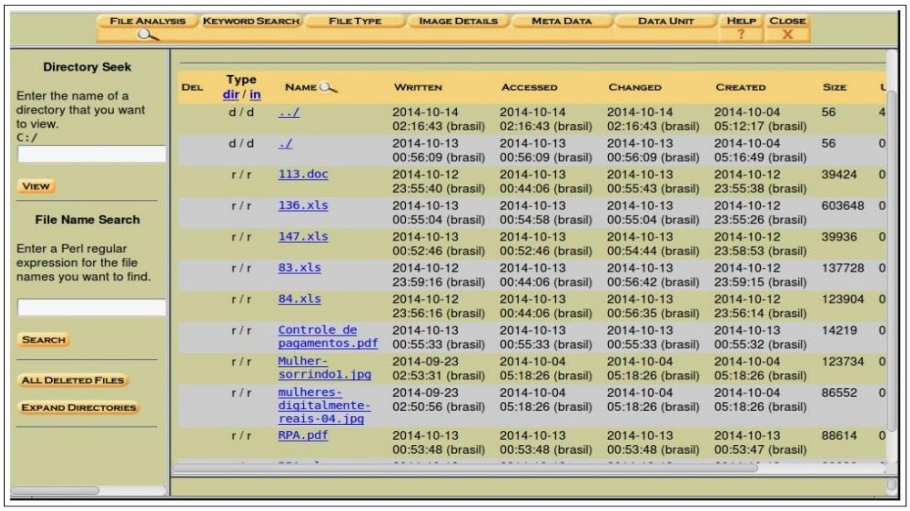


Figura 2 - Tela 7 Arquivos encontrados na pasta Google Drive.

No diretório do Google Drive foram encontrados vários arquivos num total de doze nos formatos *doc*, *Pdf*, Xls e Jpg, o que aumenta a probabilidade de serem encontradas provas, visto que os arquivos vazados têm alguns destes formatos.

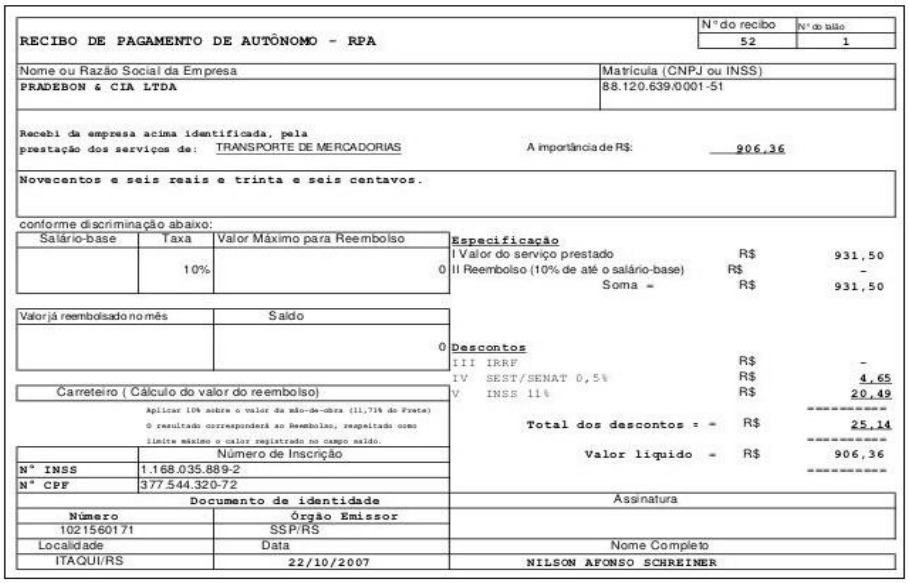
Após a análise foram encontrados dois arquivos suspeitos denominados "controle de pagamentos.pdf" e o arquivo *RPA* (com extensões *pdf* e *Xls*) criados no dia 13 de Outubro de 2014 à 00h53 minutos, que foram exportados para análise e nele foram encontrados recibos de pagamentos efetuados pela empresa e estes recibos fazem parte das informações disponibilizadas para visualização e download pela internet.

Controle de pagamentos do cliente

Matricula: 100
Razão Social: Empresa Modelo S/A
Admissão: 10/03/2014
Multa p/ Atraso: 10%
Juros: 1%
Emitido em: 12/10/2014

Mensalidade	Competencia	Vencimento	Valor	meses em atraso	Valor atualiz.
001	abr	09/04/2014	R$ 50,00	4	R$ 757,00
002	mai	09/05/2014	R$ 50,00	3	R$ 656,50
003	jun	08/06/2014	R$ 50,00	2	R$ 656,00
004	jul	08/07/2014	R$ 50,00	1	R$ 655,50
005	ago	07/08/2014	R$ 50,00	0	R$ 650,00
006	set	06/09/2014	R$ 50,00	0	R$ 650,00

Figura 3 - Arquivo encontrado na pasta Google Drive.



RECIBO DE PAGAMENTO DE AUTÔNOMO - RPA

Nº do recibo	Nº do talão
52	1

Nome ou Razão Social da Empresa	Matrícula (CNPJ ou INSS)
PRADEBON & CIA LTDA	88.120.639/0001-51

Recebi da empresa acima identificada, pela prestação dos serviços de: TRANSPORTE DE MERCADORIAS A importância de R$: 906,36

Novecentos e seis reais e trinta e seis centavos.

conforme discriminação abaixo:

Salário-base	Taxa	Valor Máximo para Reembolso
	10%	0

Especificação		
I Valor do serviço prestado	R$	931,50
II Reembolso (10% de até o salário-base)	R$	-
Soma =	R$	931,50

Valor já reembolsado no mês	Saldo
	0

Descontos		
III IRRF	R$	-
IV SEST/SENAT 0,5%	R$	4,65
V INSS 11%	R$	20,49
Total dos descontos = -	R$	25,14
Valor liquido =	R$	906,36

Carreteiro (Cálculo do valor do reembolso)

Aplicar 10% sobre o valor da mão-de-obra (11,71% do Frete)
O resultado corresponderá ao Reembolso, respeitado como limite máximo o valor registrado no campo saldo.

Número de Inscrição	
Nº INSS	1.168.035.889-2
Nº CPF	377.544.320-72

Documento de identidade	
Número	Órgão Emissor
10215601 71	SSP/RS
Localidade	Data
ITAQUI/RS	22/10/2007

Assinatura

Nome Completo

NILSON AFONSO SCHREINER

Figura 4 - Arquivo RPA encontrado e exportado para visualização.

Foram também analisados os outros documentos, porém, não fazem parte dos documentos vazados. Após a busca no diretório da pasta de sincronização, foram efetuadas buscas em possíveis arquivos apagados da pasta de sincronização, fazendo-se uso da função "*All Deleted Filles"* não tendo sido encontrado qualquer arquivo deletado referente à pasta *Google Drive.*

5.2.6 Documentação

Pelo fato de ser um caso fictício, esta documentação não é acompanhada de uma cópia da autorização judicial para coleta das evidências. Porém, foi gerada uma cadeia de custódia tendo como base as informações obtidas no estudo de caso e nos objetos usados para criar o cenário. Os dados necessários são: nome do perito responsável, hora da criação da imagem do cenário, métodos usados para sua obtenção, entre outros.

5.2.7 Relatório/Revisão

Nesta etapa encontram-se todas as informações relevantes do trabalho para auxiliar aos pesquisadores e comunidade em geral. O estudo de caso no ambiente *Google Drive*, com as práticas e os passos necessários para busca de evidências de um crime praticado por meio de uma *Cloud* pública. As evidências foram periciadas em uma pasta de sincronização do *Google Drive e* para análise do cenário foram utilizadas as seguintes ferramentas de perícia:

a) ***AccessData FTK Imager*:** ferramenta usada para criar a imagem do ambiente a ser periciado;

b) ***Deft 7.2***: ferramenta usada para manusear a imagem;

c) **Autopsty:** software usado para análise da imagem e busca de evidências.

Com estas ferramentas de perícia, foram realizadas buscas e análise de evidências, com o finalidade de dar resposta ao incidente ocorrido. No decorrer da análise, foram encontrados um total de dez (10) arquivos, entre eles dois suspeitos por terem uma correlação com o caso. Portanto, estes dois arquivos encontrados podem ser usados para instauração de um processo contra o funcionário e servir como prova da sua participação no crime. Os outros oito

arquivos encontrados, não podem ser usados como prova pois, não têm qualquer correlação com os arquivos vazados.

6. Conclusão

O presente artigo visou apresentar um método, procedimento e ferramentas para realização de uma perícia forense, para dar resposta a um incidente ocorrido em uma *Cloud* de armazenamento de dados. A pesquisa realizada possibilitou dar uma resposta ao caso, porém, foram encontrados alguns obstáculos no decorrer da pesquisa, entre eles estiveram a obtenção dos dados por meio do provedor, a escolha do estudo de caso a ser tratado, a não existência de legislação brasileira e internacional pertinente e a falta de ferramentas forenses para coleta de informações dos ambientes pesquisados. Porém esses obstáculos foram superados com a descoberta da pasta de sincronização e *backup* de alguns serviços de *Cloud* pública, sendo possível solucionar o estudo de caso onde foi possível apresentar e aplicar método, procedimento e ferramentas para perícia forense em *Cloud Computing.*
Concluindo, este trabalho apresenta as oportunidades para trabalhos futuros na área de perícia forense em ambientes *Cloud Computing*, tais como: estudo de outros métodos de perícia forense para estes ambientes, o desenvolvimento de ferramentas para extração de dados forenses nesses ambientes, bem como a criação de regras e propostas de leis para padronizar o acesso aos dados forenses.

7. Referências

Added. Soluções em Tecnologia da Informação – ISO9001:2008. Disponível em: <http://www.added.com.br/news/saas-paas-iaas/>. Acesso em: 20 maio 2014.

Cristiano AG. Ferramentas e Metodologias para Resposta a Incidentes, Estudo de Caso “Helix 3”. TCC. – Universidade do Extremo Sul Catarinense – Unesc, 2011.

Didoné Q. Computação Forense e as oportunidades oferecidas pela Computação em Nuvem. Disponivel em Disponível em: <http://revista.univar.edu.br/index.php/interdisciplinar/article/view/144 >. Acesso em: 24 abr. 2014.

Dykstra J., Sherman, AT. Acquiring Forensic Evidence from Infrastructure-as-a-Service Cloud Computing: Exploring and Evaluating Tools, Trust, and Techniques. Digital Investigation 2012. Supplement: S90–S98. The Proceedings of the Twelfth Annual DFRWS C.

Ferrão P. Computação Distribuída: O Melhor Aproveitamento de Recursos Computacionais. Disponível em: <https://www.google.com.br/url?sa=t&rct=j&q=&esrc=s&source=web&cd=1&cad=rja&uact=8&ved=0CCwQFjAA&url=http%3A%2F%2Fclaretianodf.com.br%2Fdownload%3Fcaminho%3D..%2FSiteManager%2Fupload%2F4%2Frevistas%2Fsumario%2Fpdf%2F78.pdf&ei=WhSEU5L2NcqxsQTVqID4Bg&usg=AFQjCNEpsMaWJnQ_whuqXGUsJdgRwxCkDg&bvm=bv.67720277,d.cWc >. Acesso em: 30 abr. 2014.

Freitas O. Computação em Nuvens, Visão Comparativa entre as Principais Plataformas de Mercado. Disponível em:

<http://olavooneto.files.wordpress.com/2011/01/computacao_em_nuvens_visao_olavo_neto.pdf>. Acesso em: 20 maio 2014.

Ibm. Fundamentos Cloud computing. IBM, 01 Setembro 2012. Disponivel em: <http://www.ibm.com/developerworks/cloud/library/cl-cloudintro/>. Acesso em: 10 maio 2014.

Lima G. A quantidade de informação gerada no mundo vs a qualidade. Coruja de TI, 20 Setembro 2010. Disponível em: <http://blog.corujadeti.com.br/a-quantidade-de-informacao-gerada-no-mundo-vs-a-qualidade/>. Acesso em: 17 maio 2014.

Marins CE. Desafios da informática forense no cenário de Cloud Computing. Disponível em: <www.icofcs.org/2009/ICoFCS2009-PP10.pdf>. Acesso em: 25 mar. 2014.

Melo S. Computação forense com software livre: conceitos, ferramentas e estudos de casos. Rio de Janeiro: Alta Books, 2009.

Nist. The NIST Definition of Cloud Computing, 2009. Disponível em: <csrc.nist.gov/groups/SNS/cloud-computing/cloud-def-v15.doc>. Acesso em: 22 ago. 2014

_____. Cloud ComputingStandards Roadmap. Disponivel em: <http://www.nist.gov/itl/cloud/upload/NIST_SP-500-291_Version-2_2013_June18_FINAL.pdf>. Acesso em: 22 ago. 2014.

_____. Cloud Computing Forensic Science Challenges. Disponivel em: <http://csrc.nist.gov/publications/drafts/nistir-8006/draft_nistir_8006.pdf >. Acesso em: 20 ago. 2014.

Nubling G. Cloud Computing aplicada ao Cenário Corporativo, 2011. Disponível em: < http://www.fateCSP.br/dti/tcc/tcc0038.pdf >. Acesso em: 12 maio 2014.

Ruan K. Challenges of cloud forensics: A survey of the missing capabilities. <http://scholar.google.com/citations?view_op=view_citation&hl=en&user=yWHoDqAAAAAJ&citation_for_view=yWHoDqAAAAAJ:d1gkVwhDpl0C>. Acesso em: 20 ago. 2014.

_____. Cloud Forensics: An Overview. Disponível em: <http://www.researchgate.net/profile/Tahar_Kechadi/publication/229021339_Cloud_forensics_An_overview/links/02bfe50f55377829e3000000>. Acesso em: 20 ago. 2014.

_____. Cloud Forensic Maturity Model. Disponível em: <http://link.springer.com/chapter/10.1007/978-3-642-39891-9_2#page-1>. Acesso em: 20 ago. 2014.

Souza FRC, MLO, Machado JC. Computação em Nuvem: Conceitos, Tecnologias, Aplicações e Desafios. Fortaleza, 2009.

Taurion C. Computação em Nuvem: Transformando o mundo da tecnologia da informação. Rio de Janeiro: Brasport, 2009.

Tutorialspoint. Community Cloud Model. Disponível em: <http://www.tutorialspoint.com/cloud_computing/cloud_computing_community_cloud_model.htm>. Acesso em: 20 maio 2014.

Webba SRS. Procedimentos Computacionais no Auxílio à Perícia Forense Aplicada em Web Browsers. TCC. – Universidade do Extremo Sul Catarinense – Unesc, 2010.

ANEXO (S)

ANEXO A – LEI ORDINÁRIA 12.965 – MARCO CIVÍL DA INTERNET NO BRASIL

Art. 1º Esta Lei estabelece princípios, garantias, direitos e deveres para o uso da Internet no Brasil e determina as diretrizes para atuação da União, dos Estados, do Distrito Federal e dos Municípios em relação à matéria.

Art. 2º A disciplina do uso da Internet no Brasil tem como fundamento o respeito à liberdade de expressão, bem como:

I – o reconhecimento da escala mundial da rede;

II – os direitos humanos, o desenvolvimento da personalidade e o exercício da cidadania em meios digitais;

III – a pluralidade e a diversidade;

IV – a abertura e a colaboração;

V – a livre iniciativa, a livre concorrência e a defesa do consumidor; e

VI – a finalidade social da rede.

Art. 3º A disciplina do uso da Internet no Brasil tem os seguintes princípios:

I – garantia da liberdade de expressão, comunicação e manifestação de pensamento, nos termos da Constituição Federal;

II – proteção da privacidade;

III – proteção dos dados pessoais, na forma da lei;

IV – preservação e garantia da neutralidade de rede;

V – preservação da estabilidade, segurança e funcionalidade da rede, por meio de medidas técnicas compatíveis com os padrões internacionais e pelo estímulo ao uso de boas práticas;

VI – responsabilização dos agentes de acordo com suas atividades, nos termos da lei;

VII – preservação da natureza participativa da rede;

VIII – liberdade dos modelos de negócios promovidos na Internet, desde que não conflitem com os demais princípios estabelecidos nesta Lei.

Parágrafo único. Os princípios expressos nesta Lei não excluem outros previstos no ordenamento jurídico pátrio relacionados à matéria ou nos tratados internacionais em que a República Federativa do Brasil seja parte.

Art. 4º A disciplina do uso da Internet no Brasil tem por objetivo a promoção:

I – do direito de acesso à Internet a todos;

II – do acesso à informação, ao conhecimento e à participação na vida cultural e na condução dos assuntos públicos;

III – da inovação e do fomento à ampla difusão de novas tecnologias e modelos de uso e acesso; e

IV – da adesão a padrões tecnológicos abertos que permitam a comunicação, a acessibilidade e a interoperabilidade entre aplicações e bases de dados.

Art. 5º Para os efeitos desta Lei, considera-se:

I – Internet: o sistema constituído do conjunto de protocolos lógicos, estruturado em escala mundial para uso público e irrestrito, com a finalidade de possibilitar a comunicação de dados entre terminais por meio de diferentes redes;

II – terminal: o computador ou qualquer dispositivo que se conecte à Internet;

III – endereço de protocolo de Internet (endereço IP): o código atribuído a um terminal de uma rede para permitir sua identificação, definido segundo parâmetros internacionais;

IV – administrador de sistema autônomo: a pessoa física ou jurídica que administra blocos de endereço IP específicos e o respectivo sistema autônomo de roteamento, devidamente cadastrada no ente nacional responsável pelo registro e distribuição de endereços IP geograficamente referentes ao País;

V – conexão à Internet: a habilitação de um terminal para envio e recebimento de pacotes de dados pela Internet, mediante a atribuição ou autenticação de um endereço IP;

VI – registro de conexão: o conjunto de informações referentes à data e hora de início e término de uma conexão à Internet, sua duração e o endereço IP utilizado pelo terminal para o envio e recebimento de pacotes de dados;

VII – aplicações de Internet: o conjunto de funcionalidades que podem ser acessadas por meio de um terminal conectado à Internet; e

VIII – registros de acesso a aplicações de Internet: o conjunto de informações referentes à data e hora de uso de uma determinada aplicação de Internet a partir de um determinado endereço IP.

Art. 6º Na interpretação desta Lei serão levados em conta, além dos fundamentos, princípios e objetivos previstos, a natureza da Internet, seus usos e costumes particulares e sua importância para a promoção do desenvolvimento humano, econômico, social e cultural.

CAPÍTULO II
DOS DIREITOS E GARANTIAS DOS USUÁRIOS

Art. 7º O acesso à Internet é essencial ao exercício da cidadania, e ao usuário são assegurados os seguintes direitos:

I – inviolabilidade da intimidade e da vida privada, sua proteção e indenização pelo dano material ou moral decorrente de sua violação;

II – inviolabilidade e sigilo do fluxo de suas comunicações pela Internet, salvo por ordem judicial, na forma da lei;

III – inviolabilidade e sigilo de suas comunicações privadas armazenadas, salvo por ordem judicial;

IV – não suspensão da conexão à Internet, salvo por débito diretamente decorrente de sua utilização;

V – manutenção da qualidade contratada da conexão à Internet;

VI – informações claras e completas constantes dos contratos de prestação de serviços, com detalhamento sobre o regime de proteção aos registros de conexão e aos registros de acesso a aplicações de Internet, bem como sobre práticas de gerenciamento da rede que possam afetar sua qualidade;

VII – não fornecimento a terceiros de seus dados pessoais, inclusive registros de conexão, e de acesso a aplicações de Internet, salvo mediante consentimento livre, expresso e informado ou nas hipóteses previstas em lei;

VIII – informações claras e completas sobre coleta, uso, armazenamento, tratamento e proteção de seus dados pessoais, que somente poderão ser utilizados para finalidades que:

a) justifiquem sua coleta;

b) não sejam vedadas pela legislação; e

c) estejam especificadas nos contratos de prestação de serviços ou em termos de uso de aplicações de Internet;

IX – consentimento expresso sobre coleta, uso, armazenamento e tratamento de dados pessoais, que deverá ocorrer de forma destacada das demais cláusulas contratuais;

X – exclusão definitiva dos dados pessoais que tiver fornecido a determinada aplicação de Internet, a seu requerimento, ao término da relação entre as partes, ressalvadas as hipóteses de guarda obrigatória de registros previstas nesta Lei;

XI – publicidade e clareza de eventuais políticas de uso dos provedores de conexão à Internet e de aplicações de Internet;

XII – acessibilidade, consideradas as características físico-motoras, perceptivas, sensoriais, intelectuais e mentais do usuário, nos termos da lei; e

XIII – aplicação das normas de proteção e defesa do consumidor nas relações de consumo realizadas na Internet.

Art. 8º A garantia do direito à privacidade e à liberdade de expressão nas comunicações é condição para o pleno exercício do direito de acesso à Internet.

Parágrafo único. São nulas de pleno direito as cláusulas contratuais que violem o disposto no caput , tais como aquelas que:

I – impliquem ofensa à inviolabilidade e ao sigilo das comunicações privadas, pela Internet; ou

II – em contrato de adesão, não ofereçam como alternativa ao contratante a adoção do foro brasileiro para solução de controvérsias decorrentes de serviços prestados no Brasil.

CAPÍTULO III
DA PROVISÃO DE CONEXÃO E DE APLICAÇÕES DE INTERNET

Seção I
Da Neutralidade de Rede

Art. 9º O responsável pela transmissão, comutação ou roteamento tem o dever de tratar de forma isonômica quaisquer pacotes de dados, sem distinção por conteúdo, origem e destino, serviço, terminal ou aplicação.

§ 1º A discriminação ou degradação do tráfego será regulamentada nos termos das atribuições privativas do Presidente da República previstas no inciso IV do art. 84 da Constituição Federal, para a fiel execução desta Lei, ouvidos o Comitê Gestor da Internet e a Agência Nacional de Telecomunicações, e somente poderá decorrer de:

I – requisitos técnicos indispensáveis à prestação adequada dos serviços e aplicações; e

II – priorização de serviços de emergência.

§ 2º Na hipótese de discriminação ou degradação do tráfego prevista no § 1 o , o responsável mencionado no caput deve:

I – abster-se de causar dano aos usuários, na forma do art. 927 da Lei n o 10.406, de 10 de janeiro de 2002 – Código Civil;

II – agir com proporcionalidade, transparência e isonomia;

III – informar previamente de modo transparente, claro e suficientemente descritivo aos seus usuários sobre as práticas de gerenciamento e mitigação de tráfego adotadas, inclusive as relacionadas à segurança da rede; e

IV – oferecer serviços em condições comerciais não discriminatórias e abster-se de praticar condutas anticoncorrenciais.

§ 3º Na provisão de conexão à Internet, onerosa ou gratuita, bem como na transmissão, comutação ou roteamento, é vedado bloquear, monitorar, filtrar ou analisar o conteúdo dos pacotes de dados, respeitado o disposto neste artigo.

Seção II
Da Proteção aos Registros, aos Dados Pessoais e às Comunicações Privadas

Art. 10º A guarda e a disponibilização dos registros de conexão e de acesso a aplicações de Internet de que trata esta Lei, bem como de dados pessoais e do conteúdo de comunicações privadas, devem atender à preservação da intimidade, da vida privada, da honra e da imagem das partes direta ou indiretamente envolvidas.

§ 1º O provedor responsável pela guarda somente será obrigado a disponibilizar os registros mencionados no caput , de forma autônoma ou associados a dados pessoais ou a outras informações que possam contribuir para a identificação do usuário ou do terminal, mediante ordem judicial, na forma do disposto na Seção IV deste Capítulo, respeitado o disposto no art. 7 o .

§ 2º O conteúdo das comunicações privadas somente poderá ser disponibilizado mediante ordem judicial, nas hipóteses e na forma que a lei estabelecer, respeitado o disposto nos incisos II e III do art. 7 o.

§ 3º O disposto no caput não impede o acesso aos dados cadastrais que informem qualificação pessoal, filiação e endereço, na forma da lei, pelas autoridades administrativas que detenham competência legal para a sua requisição.

§ 4º As medidas e os procedimentos de segurança e de sigilo devem ser informados pelo responsável pela provisão de serviços de forma clara e atender a padrões definidos em regulamento, respeitado seu direito de confidencialidade quanto a segredos empresariais.

Art. 11º Em qualquer operação de coleta, armazenamento, guarda e tratamento de registros, de dados pessoais ou de comunicações por provedores de conexão e de aplicações de Internet em que pelo menos um desses atos ocorra em território nacional, deverão ser obrigatoriamente respeitados a legislação brasileira e os direitos à privacidade, à proteção dos dados pessoais e ao sigilo das comunicações privadas e dos registros.

§ 1º O disposto no caput aplica-se aos dados coletados em território nacional e ao conteúdo das comunicações, desde que pelo menos um dos terminais esteja localizado no Brasil.

§ 2º O disposto no caput aplica-se mesmo que as atividades sejam realizadas por pessoa jurídica sediada no exterior, desde que oferte serviço ao público brasileiro ou pelo menos uma integrante do mesmo grupo econômico possua estabelecimento no Brasil.

§ 3º Os provedores de conexão e de aplicações de Internet deverão prestar, na forma da regulamentação, informações que permitam a verificação quanto ao cumprimento da legislação brasileira referente à coleta, à guarda, ao armazenamento ou ao tratamento de dados, bem como quanto ao respeito à privacidade e ao sigilo de comunicações.

§ 4º Decreto regulamentará o procedimento para apuração de infrações ao disposto neste artigo.

Art. 12º Sem prejuízo das demais sanções cíveis, criminais ou administrativas, as infrações às normas previstas nos arts. 10 e 11 ficam sujeitas, conforme o caso, às seguintes sanções, aplicadas de forma isolada ou cumulativa:

I – advertência, com indicação de prazo para adoção de medidas corretivas;

II – multa de até 10% (dez por cento) do faturamento do grupo econômico no Brasil no seu último exercício, excluídos os tributos, considerados a condição econômica do infrator e o princípio da proporcionalidade entre a gravidade da falta e a intensidade da sanção;

III – suspensão temporária das atividades que envolvam os atos previstos no art. 11; ou

IV – proibição de exercício das atividades que envolvam os atos previstos no art. 11.

Parágrafo único. Tratando-se de empresa estrangeira, responde solidariamente pelo pagamento da multa de que trata o caput sua filial, sucursal, escritório ou estabelecimento situado no País.

Subseção I
Da Guarda de Registros de Conexão

Art. 13º Na provisão de conexão à Internet, cabe ao administrador de sistema autônomo respectivo o dever de manter os registros de conexão, sob sigilo, em ambiente controlado e de segurança, pelo prazo de 1 (um) ano, nos termos do regulamento.

§ 1º A responsabilidade pela manutenção dos registros de conexão não poderá ser transferida a terceiros.

§ 2º A autoridade policial ou administrativa ou o Ministério Público poderá requerer cautelarmente que os registros de conexão sejam guardados por prazo superior ao previsto no caput .

§ 3º Na hipótese do § 2 o , a autoridade requerente terá o prazo de 60 (sessenta) dias, contados a partir do requerimento, para ingressar com o pedido de autorização judicial de acesso aos registros previstos no caput .

§ 4º O provedor responsável pela guarda dos registros deverá manter sigilo em relação ao requerimento previsto no § 2º , que perderá sua eficácia caso o pedido de autorização judicial seja indeferido ou não tenha sido protocolado no prazo previsto no § 3º .

§ 5º Em qualquer hipótese, a disponibilização ao requerente dos registros de que trata este artigo deverá ser precedida de autorização judicial, conforme disposto na Seção IV deste Capítulo.

§ 6º Na aplicação de sanções pelo descumprimento ao disposto neste artigo, serão considerados a natureza e a gravidade da infração, os danos dela resultantes, eventual vantagem auferida pelo infrator, as circunstâncias agravantes, os antecedentes do infrator e a reincidência.

Subseção II
Da Guarda de Registros de Acesso a Aplicações de Internet na Provisão de Conexão

Art. 14º Na provisão de conexão, onerosa ou gratuita, é vedado guardar os registros de acesso a aplicações de Internet.

Subseção III
Da Guarda de Registros de Acesso a Aplicações de Internet na Provisão de Aplicações

Art. 15º O provedor de aplicações de Internet constituído na forma de pessoa jurídica e que exerça essa atividade de forma organizada, profissionalmente e com fins econômicos deverá manter os respectivos registros de acesso a aplicações de Internet, sob sigilo, em ambiente controlado e de segurança, pelo prazo de 6 (seis) meses, nos termos do regulamento.

§ 1º Ordem judicial poderá obrigar, por tempo certo, os provedores de aplicações de Internet que não estão sujeitos ao disposto no caput a guardarem registros de acesso a aplicações de Internet, desde que se trate de registros relativos a fatos específicos em período determinado.

§ 2º A autoridade policial ou administrativa ou o Ministério Público poderão requerer cautelarmente a qualquer provedor de aplicações de Internet que os registros de acesso a aplicações de Internet sejam guardados, inclusive por prazo superior ao previsto no caput , observado o disposto nos §§ 3º e 4º do art. 13º.

§ 3º Em qualquer hipótese, a disponibilização ao requerente dos registros de que trata este artigo deverá ser precedida de autorização judicial, conforme disposto na Seção IV deste Capítulo.

§ 4º Na aplicação de sanções pelo descumprimento ao disposto neste artigo, serão considerados a natureza e a gravidade da infração, os danos dela resultantes, eventual vantagem auferida pelo infrator, as circunstâncias agravantes, os antecedentes do infrator e a reincidência.

Art. 16º Na provisão de aplicações de Internet, onerosa ou gratuita, é vedada a guarda:

I – dos registros de acesso a outras aplicações de Internet sem que o titular dos dados tenha consentido previamente, respeitado o disposto no art. 7º ; ou

II – de dados pessoais que sejam excessivos em relação à finalidade para a qual foi dado consentimento pelo seu titular.

Art. 17º Ressalvadas as hipóteses previstas nesta Lei, a opção por não guardar os registros de acesso a aplicações de Internet não implica responsabilidade sobre danos decorrentes do uso desses serviços por terceiros.

Seção III
Da Responsabilidade por Danos Decorrentes de Conteúdo Gerado por Terceiros

Art. 18º O provedor de conexão à Internet não será responsabilizado civilmente por danos decorrentes de conteúdo gerado por terceiros.

Art. 19º Com o intuito de assegurar a liberdade de expressão e impedir a censura, o provedor de aplicações de Internet somente poderá ser responsabilizado civilmente por danos decorrentes de conteúdo gerado por terceiros se, após ordem judicial específica, não tomar as providências para, no âmbito e nos limites técnicos do seu serviço e dentro do prazo assinalado, tornar indisponível o conteúdo apontado como infringente, ressalvadas as disposições legais em contrário.

§ 1º A ordem judicial de que trata o caput deverá conter, sob pena de nulidade, identificação clara e específica do conteúdo apontado como infringente, que permita a localização inequívoca do material.

§ 2º A aplicação do disposto neste artigo para infrações a direitos de autor ou a direitos conexos depende de previsão legal específica, que deverá respeitar a liberdade de expressão e demais garantias previstas no art. 5 o da Constituição Federal.

§ 3º As causas que versem sobre ressarcimento por danos decorrentes de conteúdos disponibilizados na Internet relacionados à honra, à reputação ou a direitos de personalidade, bem como sobre a indisponibilização desses conteúdos por provedores de aplicações de Internet, poderão ser apresentadas perante os juizados especiais.

§ 4º O juiz, inclusive no procedimento previsto no § 3º , poderá antecipar, total ou parcialmente, os efeitos da tutela pretendida no pedido inicial, existindo prova inequívoca do fato e considerado o interesse da coletividade na disponibilização do conteúdo na Internet, desde que presentes os requisitos de verossimilhança da alegação do autor e de fundado receio de dano irreparável ou de difícil reparação.

Art. 20º Sempre que tiver informações de contato do usuário diretamente responsável pelo conteúdo a que se refere o art. 19, caberá ao provedor de aplicações de Internet comunicar-lhe os motivos e

informações relativos à indisponibilização de conteúdo, com informações que permitam o contraditório e a ampla defesa em juízo, salvo expressa previsão legal ou expressa determinação judicial fundamentada em contrário.

Parágrafo único. Quando solicitado pelo usuário que disponibilizou o conteúdo tornado indisponível, o provedor de aplicações de Internet que exerce essa atividade de forma organizada, profissionalmente e com fins econômicos substituirá o conteúdo tornado indisponível pela motivação ou pela ordem judicial que deu fundamento à indisponibilização.

Art. 21º O provedor de aplicações de Internet que disponibilize conteúdo gerado por terceiros será responsabilizado subsidiariamente pela violação da intimidade decorrente da divulgação, sem autorização de seus participantes, de imagens, de vídeos ou de outros materiais contendo cenas de nudez ou de atos sexuais de caráter privado quando, após o recebimento de notificação pelo participante ou seu representante legal, deixar de promover, de forma diligente, no âmbito e nos limites técnicos do seu serviço, a indisponibilização desse conteúdo.

Parágrafo unico. A notificação prevista no caput deverá conter, sob pena de nulidade, elementos que permitam a identificação específica do material apontado como violador da intimidade do participante e a verificação da legitimidade para apresentação do pedido.

Seção IV
Da Requisição Judicial de Registros

Art. 22º A parte interessada poderá, com o propósito de formar conjunto probatório em processo judicial cível ou penal, em caráter incidental ou autônomo, requerer ao juiz que ordene ao responsável pela guarda o fornecimento de registros de conexão ou de registros de acesso a aplicações de Internet.

Parágrafo único. Sem prejuízo dos demais requisitos legais, o requerimento deverá conter, sob pena de inadmissibilidade:

I – fundados indícios da ocorrência do ilícito;

II – justificativa motivada da utilidade dos registros solicitados para fins de investigação ou instrução probatória; e

III – período ao qual se referem os registros.

Art. 23º Cabe ao juiz tomar as providências necessárias à garantia do sigilo das informações recebidas e à preservação da intimidade, da vida privada, da honra e da imagem do usuário, podendo determinar segredo de justiça, inclusive quanto aos pedidos de guarda de registro.

CAPÍTULO IV
DA ATUAÇÃO DO PODER PÚBLICO

Art. 24º Constituem diretrizes para a atuação da União, dos Estados, do Distrito Federal e dos Municípios no desenvolvimento da Internet no Brasil:

I – estabelecimento de mecanismos de governança multiparticipativa, transparente, colaborativa e democrática, com a participação do governo, do setor empresarial, da sociedade civil e da comunidade acadêmica;

II – promoção da racionalização da gestão, expansão e uso da Internet, com participação do Comitê Gestor da Internet no Brasil;

III – promoção da racionalização e da interoperabilidade tecnológica dos serviços de governo eletrônico, entre os diferentes Poderes e âmbitos da Federação, para permitir o intercâmbio de informações e a celeridade de procedimentos;

IV – promoção da interoperabilidade entre sistemas e terminais diversos, inclusive entre os diferentes âmbitos federativos e diversos setores da sociedade;

V – adoção preferencial de tecnologias, padrões e formatos abertos e livres;

VI – publicidade e disseminação de dados e informações públicos, de forma aberta e estruturada;

VII – otimização da infraestrutura das redes e estímulo à implantação de centros de armazenamento, gerenciamento e disseminação de dados no País, promovendo a qualidade técnica, a inovação e a difusão das aplicações de Internet, sem prejuízo à abertura, à neutralidade e à natureza participativa;

VIII – desenvolvimento de ações e programas de capacitação para uso da Internet;

IX – promoção da cultura e da cidadania; e

X – prestação de serviços públicos de atendimento ao cidadão de forma integrada, eficiente, simplificada e por múltiplos canais de acesso, inclusive remotos.

Art. 25º As aplicações de Internet de entes do poder público devem buscar:

I – compatibilidade dos serviços de governo eletrônico com diversos terminais, sistemas operacionais e aplicativos para seu acesso;

II – acessibilidade a todos os interessados, independentemente de suas capacidades físico-motoras, perceptivas, sensoriais, intelectuais, mentais, culturais e sociais, resguardados os aspectos de sigilo e restrições administrativas e legais;

III – compatibilidade tanto com a leitura humana quanto com o tratamento automatizado das informações;

IV – facilidade de uso dos serviços de governo eletrônico; e

V – fortalecimento da participação social nas políticas públicas.

Art. 26º O cumprimento do dever constitucional do Estado na prestação da educação, em todos os níveis de ensino, inclui a capacitação, integrada a outras práticas educacionais, para o uso seguro, consciente e responsável da Internet como ferramenta para o exercício da cidadania, a promoção da cultura e o desenvolvimento tecnológico.

Art. 27º As iniciativas públicas de fomento à cultura digital e de promoção da Internet como ferramenta social devem:

I – promover a inclusão digital;

II – buscar reduzir as desigualdades, sobretudo entre as diferentes regiões do País, no acesso às tecnologias da informação e comunicação e no seu uso; e

III – fomentar a produção e circulação de conteúdo nacional.

Art. 28º O Estado deve, periodicamente, formular e fomentar estudos, bem como fixar metas, estratégias, planos e cronogramas, referentes ao uso e desenvolvimento da Internet no País.

CAPÍTULO V
DISPOSIÇÕES FINAIS

Art. 29º. O usuário terá a opção de livre escolha na utilização de programa de computador em seu terminal para exercício do controle parental de conteúdo entendido por ele como impróprio a seus filhos menores, desde que respeitados os princípios desta Lei e da Lei n o 8.069, de 13 de julho de 1990 – Estatuto da Criança e do Adolescente.

Parágrafo único. Cabe ao poder público, em conjunto com os provedores de conexão e de aplicações de Internet e a sociedade civil, promover a educação e fornecer informações sobre o uso dos programas de computador previstos no caput , bem como para a definição de boas práticas para a inclusão digital de crianças e adolescentes.

Art. 30º. A defesa dos interesses e dos direitos estabelecidos nesta Lei poderá ser exercida em juízo, individual ou coletivamente, na forma da lei.

Art. 31º. Até a entrada em vigor da lei específica prevista no § 2 o do art. 19, a responsabilidade do provedor de aplicações de Internet por danos decorrentes de conteúdo gerado por terceiros, quando se tratar de infração a direitos de autor ou a direitos conexos, continuará a ser disciplinada pela legislação autoral vigente aplicável na data da entrada em vigor desta Lei.

Art. 32º. Esta Lei entra em vigor após decorridos 60 (sessenta) dias de sua publicação oficial.

Brasília, 23 de abril de 2014; 193 o da Independência e 126 o da República.

DILMA ROUSSEFF
José Eduardo Cardozo
Miriam Belchior
Paulo Bernardo Silva
Clélio Campolina Diniz

ANEXO B – CARTA DE SOLICITAÇÃO DE DADOS AO GOOGLE BRASIL

Brasil, Santa Catarina, Criciúma 28 de Setembro de 2014

AO

GOOGLE BRASIL INTERNET LTDA.

A/C do Serviço de Atendimento ao Cliente

Av. Brigadeiro Faria Lima, 3477 - 18º andar

São Paulo, 04538-133

Brasil,

Assunto: Solicitação de todos os dados (existentes e excluídos) da conta Google Drive, para realização de um estudo científico sobre a análise forense de dados na nuvem.

Prezados

Eu Célio Fabrício da Conceição Filipe em 2012, aderi aos serviços do Google Drive e docs desta empresa, tendo acesso aos recursos padrão e respeitando as políticas da empresa.

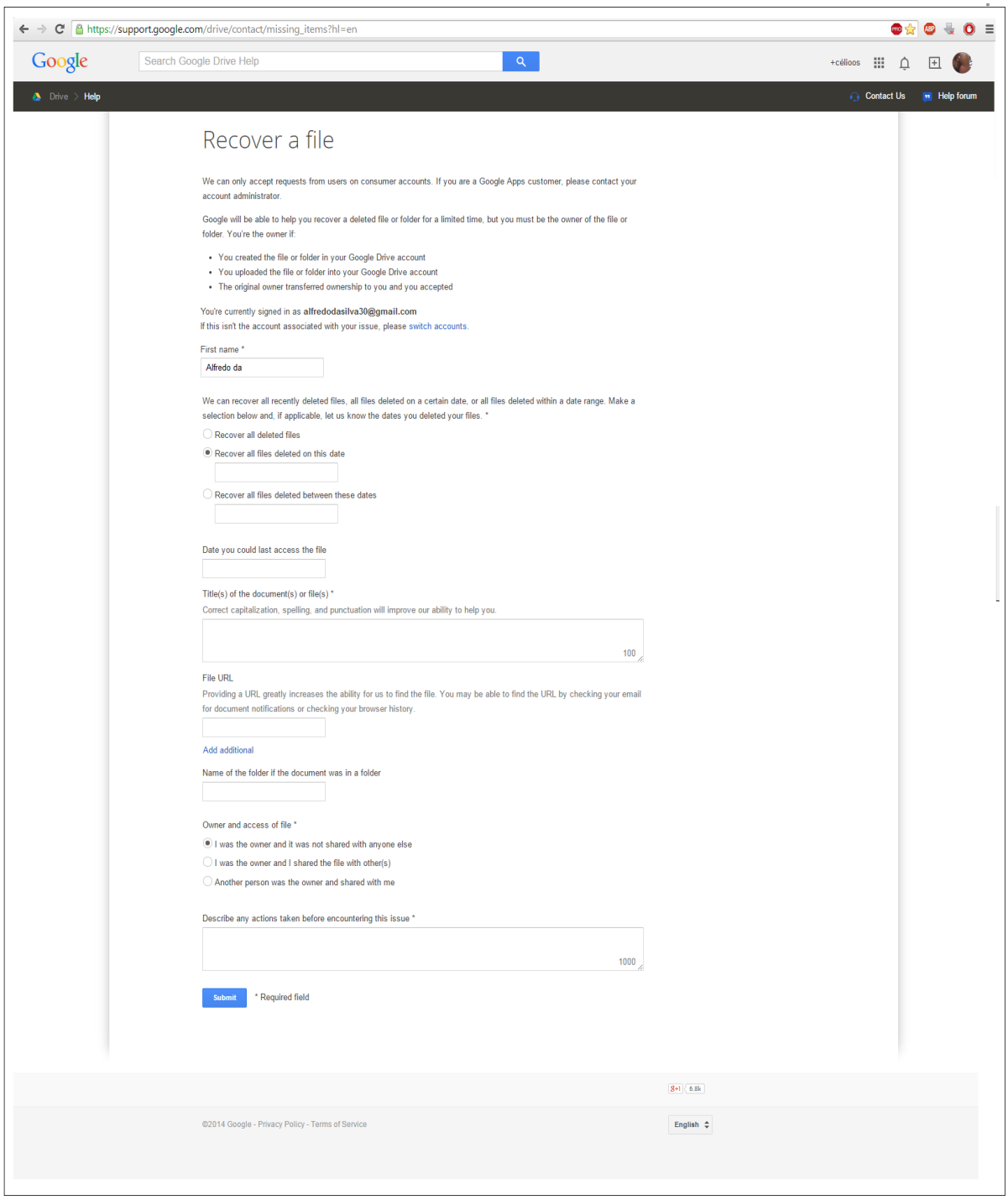
Para fins pessoais e académicos, solicito os dados da minha conta Google Drive desde a sua criação até a presente data, incluindo os dados por mim excluídos. Confirmando que sou o proprietário da conta seguem os meus dados. Email [redacted]@hotmail.com, data de nascimento 13 de abril de 1987, telefone (48) 999[redacted], endereço Rua [redacted], apartamento [redacted], cidade de Criciúma, estado de Santa Catarina.

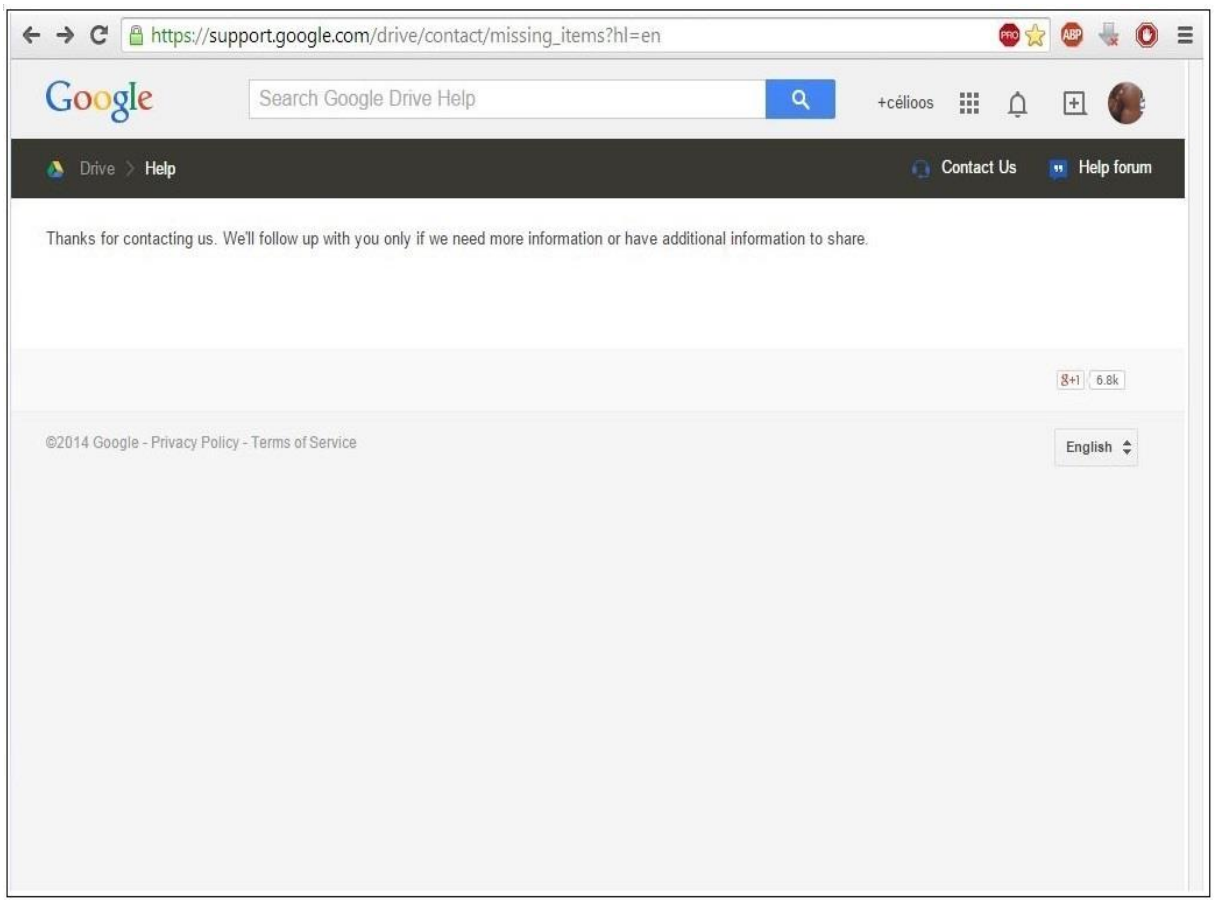
Sem mais algum assunto de momento, aguardo a vossa resposta.

Atenciosamente

Célio Fabrício da Conceição Filipe

ANEXO C – SOLICITAÇÃO DE RECUPERAÇÃO DE DADOS APAGADOS DA CLOUD PELO SUPORTE TÉCNICO DO GOOGLE DRIVE




https://support.google.com/drive/contact/missing_items?hl=en
Google
Search Google Drive Help
+célioos
Drive
Help
Contact Us
Help forum
Thanks for contacting us. We'll follow up with you only if we need more information or have additional information to share.
g+1 6.8k
©2014 Google - Privacy Policy - Terms of Service
English