OS DESAFIOS DA FORENSE COMPUTACIONAL NA COMPUTAÇÃO EM NUVEM[]

Ieda Maria de Souza

Resumo: A computação em nuvem surgiu com uma nova proposta da computação tradicional, ambiente onde o uso de aplicações ou armazenamento são disponibilizados para os usuários através da internet. A tecnologia da virtualização oferece diversos benefícios, mas com ela também cresce as possibilidades de crimes cibernéticos, por isso os peritos forenses digitais vêm enfrentando desafios na realização da forense em nuvem para obter e preservar as provas legais. Nestes ambientes quem possui a evidência digitais são os provedores de serviços, normalmente em *datacenters* localizados em diversas partes do mundo e com um grande volume de dados o que torna muito difícil extrair as provas. A pesquisa tem o objetivo de investigar os desafios enfrentados pela forense computacional diante o ambiente de computação em nuvem e mostrar alguns modelos de forense em nuvem.

Palavras-chave: Computação em Nuvem. Forense computacional. Forense em Nuvem.

1 INTRODUÇÃO

Com a crescente evolução da tecnologia e a democratização das telecomunicações a sociedade mudou sua forma de se relacionar e trabalhar. Uma das novidades tecnológicas com forte crescimento é a computação em nuvem que vem sendo usada largamente em todo o mundo devido aos seus grandes benefícios como a facilidade de acesso, economia de recursos, escalabilidade, negócios, entre outros. Na mesma velocidade de crescimento das novas tecnologias também cresce os crimes cibernético, o que traz uma maior preocupação no momento de contratar um provedor.

Apesar dos provedores de serviço em nuvem garantirem a confiabilidade e a segurança os ataques realizados neste ambientes são difíceis de serem investigados, trazendo grandes desafios aos peritos forenses digitais. As dificuldades são apresentadas ao perito na forma de coletar os dados que muitas vezes se encontram distribuídos geograficamente, acesso as informações que podem estar sob a responsabilidade do provedor ou questões

[] Acadêmica do curso Pós-Graduação em Gestão de Segurança da Informação da Universidade do Sul de Santa Catarina. http://www.unisul.br.

legais. A pesquisa questiona o seguinte problema: Quais os desafios enfrentados pela forense computacional diante os ambientes de computação em nuvem?

A pesquisa tem o objetivo de investigar os desafios enfrentados pela forense computacional diante os ambientes de computação em nuvem e apresentar algumas soluções que podem ser usadas numa perícia em nuvem. Para alcançar os objetivos desta pesquisa o trabalho ocorreu de forma exploratória buscando juntar uma base teórica e conceitual para apresentar o tema do trabalho. A metodologia aplicada no projeto inicia-se com a pesquisa bibliográfica e buscou-se aprofundar sobre os conceitos de forense computacional e computação em nuvem. Assim como os principais desafios enfrentados pelos peritos nestes ambientes onde as práticas de crimes cibernéticos estão cada vez mais comuns, desafios estes que podem ter origem tecnológica, humano ou legal. A pesquisa também aborda algumas ferramentas que podem ser implementadas pelos provedores para auxiliar e facilitar o trabalho dos peritos quando necessidade de alguma investigação.

Dessa forma, este trabalho realiza um estudo com os conceitos de computação em nuvem, forense computacional, os desafios e oportunidades enfrentados pelos peritos digitais na realização das investigações em ambientes de nuvem e uma proposta de forense como um serviço, com apresentação de alguns exemplo que podem facilitar o trabalhos dos peritos na preservação das evidências.

2 COMPUTAÇÃO EM NUVEM

Por muito tempo o uso de grandes computadores conhecidos como mainframes foram utilizados pelas organizações como arquitetura padrão de mercado. Com a necessidade de otimizar os recursos na década de 80 inicia-se o uso da computação cliente/servidor, barateando o custo de equipamentos com aplicações rodando localmente, mas que também haviam limitações. Assim com o crescimento da internet e a possibilidade de interligação das redes com baixo custo se tornou atrativo para as empresas, surgindo assim a computação em nuvem.

Para Veras (2012), a computação em nuvem é a substituição do gerenciamento dos ativos de TI usados localmente por funcionalidades e serviços contratados conforme a demanda. Estas funcionalidades e serviços são desenvolvidas usando novas tecnologias como

a virtualização, aplicações e infraestrutura orientados a serviço usando protocolos da internet como meio para redução de custo de hardware e software. A computação em nuvem permite que aplicações rodem em ambientes de larga escala e com uso elástico de recursos.

Uma das principais referências em computação na nuvem foi definida pela agência governamental não-regulatória de administração de tecnologia do Departamento de Comércio dos Estados Unidos, o NIST (*National Institute of Standards and Techonology*,) segundo sua definição:

> A computação em nuvem é um modelo para habilitar o acesso por rede ubíquo, conveniente e sob demanda a um conjunto compartilhado de recursos de computação (como redes, servidores, armazenamento, aplicações e serviços) que possam ser rapidamente provisionados e liberados com o mínimo de esforço de gerenciamento ou interação com o provedor de serviços. (NIST, 2011)

A computação em nuvem deixou de ser uma tendência e passou a ser uma proposta de negócio cada vez mais utilizada pelas empresas devido as suas características como: alocação de recursos automaticamente, serviços disponibilizados pela Internet a diversos clientes simultaneamente, rapidez de elasticidade dos recursos quando demandando pelo cliente e serviços controlados e monitorados pelos provedores. Os modelos de serviços oferecidos pelos provedores e mais utilizados são a Infraestrutura como Serviço (IaaS), Plataforma como Serviço (PaaS) e Software como um Serviço (SaaS). (NIST, 2011)

- Infraestrutura como Serviço *(IaaS)*: A capacidade de infraestrutura na nuvem que o provedor oferece como serviço ao consumidor, esta infraestrutura engloba um ambiente de rede, servidores e armazenamento disponibilizados conforme a demanda do cliente. Um dos provedores mais conhecidos atualmente no mercado é a Amazon Ec2.
- Plataforma como Serviço (*PaaS*): Ambiente de computação oferecido pelo provedor para que o cliente desenvolve seus aplicativos e disponibilizem na nuvem. Os principais serviços hoje no mercado são os ambientes *AppEngin*e do Google e *Windows Azure* da Microsoft.
- Software como Serviço (*SaaS*): Aplicativos hospedados na nuvem e acessados por aplicações executados por um cliente como *desktop*, *smartphone*, entre outros. Todo o

gerenciamento da rede, servidores, armazenamento é realizado pelo provedor. Nesta modalidade se encaixa serviços como *Dropbox, Google APP, Amazon Web Services.*

A implantação dos modelos de serviço *(IaaS*, *PaaS* e *SaaS*) serão realizados de acordo com os diferentes tipos de acesso e disponibilidade do ambiente, para isso o NIST (2011) propõe quatro modelos de implantação:

- Pública – quando o cliente contrata um recurso que também é compartilhado com outros usuários.
- Privada – Implementada somente para uso de uma organização, podendo ser hospedada dentro da empresa ou no prestador de serviço.
- Comunitária: Infraestrutura compartilhada entre diversas empresas com interesses comuns.
- Híbrida – Infraestrutura que compõe de ou mais modelos de implantação.

Apesar dos provedores de serviço em nuvem garantirem em seus contratos alta disponibilidade e confidencialidade um dos maiores desafios na adoção da computação em nuvem é a segurança da informação. A preocupação com os crimes cibernético não está relacionado somente aos serviços, mas envolve todas as tecnologias, arquitetura, usuários e profissionais e neste contexto o maior desafio para os provedores em nuvem é um número muito grande de processamento e armazenamento das informações, já que os dados podem estar distribuídos em diversas regiões geográficas, cabendo a elas o gerenciamento dos serviços e também a legislação vigente daquele país. O instituto de pesquisa *Gartner* alerta para sete problemas relacionados à segurança nos ambientes de computação em nuvem, entre eles o acesso privilegiado de usuários, *compliance* com regulamentação, localização e segregação dos dados, apoio a investigação, recuperação e acesso aos dados a longo prazo. (COMPUTERWORLD).

3 PERÍCIA FORENSE COMPUTACIONAL

Os avanços tecnológicos trouxeram diversos benefícios para a sociedade como o aumento da comunicação e possibilidade de negócios, mas com ela também veio a realização

das práticas criminosas, como invasão, roubo de informação, pedofilia, entre outros. Para investigação destas práticas surge a computação forense com o objetivo de analisar os crimes cibernéticos utilizando métodos científicos, matemáticos e legais, para que as informações analisadas possam ser caracterizadas como evidências e consequentemente usada como prova legal de fato.

> "Portanto, a Computação Forense tem como objetivo principal determinar a dinâmica, a materialidade e autoria de ilícitos ligados à área de informática, tendo como questão principal a identificação e o processamento de evidências digitais em provas materiais de crime, por meio de métodos técnico-científicos, conferindo-lhe validade probatória em juízo." Eleutério e Machado(2011).

O objetivo da forense computacional é identificar e preservar as evidências, extrair informações, documentar todos os processos e analisar as informações extraídas para encontrar respostas às perguntas conhecidas como 5Ws *(Why, When, Where, What, and Who*) posteriormente a um incidente relacionados a danos criminais, espionagem industrial, investigações financeiras como lavagem de dinheiro ou fraude, violação de política corporativa, abuso infantil, entre outros usados como prova legal diante um tribunal de justiça. (LOPEZ; MOON; PARK, 2016) .

Os exames forenses são mais conhecidos quando realizados em mídias como discos rígidos, CDs, pendrives, cartões de memória, dispositivos móveis, entre outros. Os discos rígidos internos de PCs ou notebooks devem ser analisados *in loco* ou levados para análise em laboratório. Além destes meios digitais os peritos irão encontrar muitos ambientes onde a coleta dos dados deverá ser realizada em serviços de redes, conhecida como *network forensics* que engloba e-mails, redes sociais, entre outros e por fim as análises de códigos que incluem sistemas, aplicativos e banco de dados.

Os procedimentos adotados para a coleta dos dados deve ser seguido para a obtenção da prova e apresentação judicial, por isso a importância dos seguintes passos:

- Preservação – Esta etapa consiste em preservar o cena do crime ou ambiente computacional para que se possa efetuar a coleta dos dados sem danificar as informações.
- Coleta – Neste momento o perito deverá isolar a área e identificar o que será coletado, garantindo a integridade das evidências.

- Exame – O exame tem o papel de identificar, extrair, filtrar e documentar os dados mais importantes para a investigação.
- Análise – Na etapa de análise os dados serão transformados em informações, onde o perito ira confrontar situações para a etapa de documentar e redigir o laudo.
- Apresentação – Momento de apresentar os resultados da análise, através de um laudo detalhado que possa trazer confiabilidade das evidências. (PALMER, 2001)

4 A COMPUTAÇÃO FORENSE E SEUS DESAFIOS NA COMPUTAÇÃO NA NUVEM

Os serviços em nuvem estão sujeitos a vários incidentes intencionais ou não que ameaçam a segurança, incluindo ameaça à integridade, confidencialidade e disponibilidade dos recursos. Os sistemas são suscetíveis assim como qualquer outra rede e para estes ambientes virtuais foram apontados alguns meios mais vulneráveis à invasão, como pilha de protocolos e serviços, dispositivos de rede, processo em execução do *kernel*, *deamons* de sistemas operacionais, aplicativos que executam com privilégios de *root*, processos que executam fora do *kernel*, *middware* em nuvem e aplicativos em nuvem. (MATHEW e JOSE, 2012).

No ambiente tradicional a perícia computacional desliga o equipamento e faz uma cópia bit a bit dos discos, o que fica praticamente inviável num ambiente de computação em nuvem devido à grande capacidade de armazenamento, criptografia utilizada nos sistemas de arquivos, assim como as questões jurídicas. Por isso a computação forense vem se reestruturando para trazer novas técnicas, soluções e métodos investigativos nestes ambientes, também conhecida por alguns autores como *cloud forensics* ou perícia na nuvem.

Ruan et al. (2011) propõe um modelo tridimensional para categorizar os desafios da forense em computação em nuvem, divididos em dimensão técnica, organizacional e jurídica. Na categorização de dimensão técnica inclui a coleta do dados, elasticidade das ferramentas de forense *in live*, divisão das informações que podem estar compartilhadas em locais diferentes e os requisitos contratuais. Na dimensão organizacional o autor atribui as responsabilidades entre os provedores e usuários da nuvem e na dimensão jurídica estão as questões legais e *SLAs.* Em cada dimensão ele apresenta um conjunto de fatores que definem as ferramentas, métodos, funções e responsabilidades de cada papel na *cloud forensics*.

O mesmo autor conceitua *cloud forensic* como:"….a aplicação da ciência forense digital em ambientes de computação em nuvem, que aborda a perícia em rede ou *network forensics*. Tecnicamente, consiste de uma abordagem forense híbrida (por exemplo, remota, em rede, ao vivo e em larga escala)". Para Ruan et al. (2011) os desafios da forense em nuvem estão relacionados a outras situações como as relacionadas abaixo:

- A jurisdição onde os dados estão armazenados e a falta de colaboração internacional para acesso destes dados localizados em outros países;
- Falta de legislação e regulamentação que facilitem a recuperação de evidências envolvendo dados confidenciais;
- Dificuldade de investigação da cadeia de dependência entre os provedores em nuvem, quando estes terceirizam outros serviços;
- Falta de definição de cláusulas nos contratos com os provedores para preservar e disponibilizar informações necessárias em caso de investigação como l*ogs* do host do sistema operacional, roteadores, *switches*, *firewalls,* logs de plataforma de virtualização, *logs* banco de dados, entre outros;
- Aumento significativo de dispositivos que acessam dados na nuvem, como celulares, notebooks e desktops.
- Divisão dos dados forenses em uma infraestrutura que é compartilhada por diversos usuários;
- Unificação dos formatos de *log* que pode mudar conforme aplicação ou plataforma escolhida;

O *National Institute of Standards and Techonology* (NIST) fornece uma lista abrangente de 65 desafios que os profissionais enfrentam ao investigar ambientes de nuvem que são divididos entre técnicos, jurídicos e organizacionais. Para o NIST os peritos forenses têm dificuldades em identificar a atribuir responsabilidades aos dados excluídos em nuvem, devido ao grande número de usuários e volumes de dados que compartilham o serviço e que fica difícil dos provedores em nuvem de implementar métodos de backup que possa recuperar estas informações. (NIST, 2014)

A reconstrução de armazenamento virtual em ambientes de nuvem a partir da cópia do disco físico também se torna bastante complexo, pois os algoritmos de reconstrução precisam ser validados ou muitas vezes desenvolvidos. A preservação das evidências pode ser prejudicada devido a falta de conhecimento da arquitetura utilizada, sincronização entre os

servidores, códigos maliciosos, erros de no gerenciamento ou configurações de serviços em nuvem realizados de maneira incorreta.

4.1 AS OPORTUNIDADES DA FORENSE COMPUTACIONAL EM NUVEM

A rápida evolução da computação em nuvem e a necessidade da forense digital se adequar a estes ambientes não traz somente os desafios aos peritos, mas com ela também surgem as oportunidades para a realização da forense nestes ambientes. Ruan et al. (2011) apresenta algumas oportunidades que a computação em nuvem podem oferecer para a investigação forense:

- As evidências de ambientes de computação em nuvem são mais difíceis de serem destruídas, devido a replicação do serviço para outros locais oferecidos pelos provedores de serviço garantindo a durabilidade da guarda das provas.
- O uso da infraestrutura da nuvem, como a capacidade da computação sob demanda, a elasticidade e o processamento distribuído podem tornar a implementação da forense na nuvem mais barato e segura;
- A escalabilidade do ambiente em nuvem facilita o armazenamento, indexação e pesquisa dos *logs* permite o dimensionamento dos recursos nos serviços de perícia em nuvem;
- Por ser uma área de estudo bastante nova é possível aproveitar as oportunidades para estabelecer políticas e padrões de forense em nuvem.
- Aplicações e atividades forenses podem ser administradas e gerenciadas de forma centralizada e fornecido como serviço pelo provedor, também conhecido como, Forense como um serviço (*Forensic-as-a-Service – FaaS).*

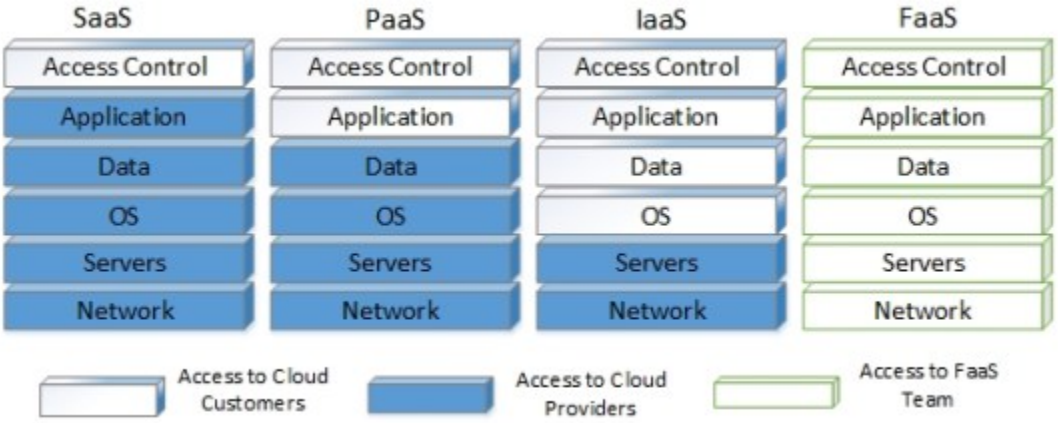
Dentre estas oportunidades a forense como um serviço se destaca por propor uma diminuição do tempo na coleta dos dados que serão periciados usando a infraestrutura da computação em nuvem com o uso de ferramentas da forense digital e programação MapReduce quando há necessidade de análise de grandes conjuntos de dados.

4.2 FORENSE COMO UM SERVIÇO EM COMPUTAÇÃO NA NUVEM

A Forense como um serviço (*Forensic-as-a-Service – FaaS*) vem solucionar o problema de trabalhar com grande capacidade de armazenamento. Seu objetivo é criar um ambiente de estrutura forense digital para ser implantado na nuvem com ferramentas que organizam, filtram e integram as informações com outros sistemas, assegurando que os dados reunidos serão armazenados de forma segura e disponibilizada para equipe de profissionais legais, técnicos e regulamentados pelo governo para realizar a perícia na nuvem. (JESUS et al.,2016)

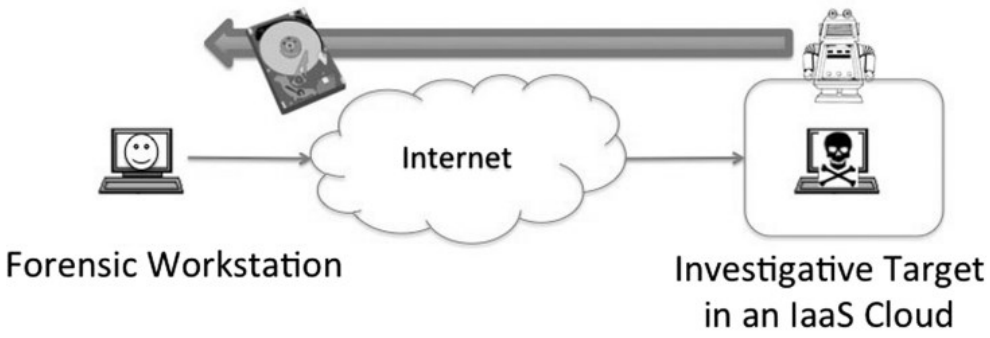
Na computação em nuvem os controles dos dados variam conforme o modelo de serviço contratado. A falta de acesso físico para coleta dos dados e a falta de controle sobre o sistema tornam a aquisição das informações uma tarefa desafiadora da perícia em nuvem. Por isso a importância de incluir no contrato de prestação de serviço alguns requisitos de notificação, identificação, preservação e acesso as fontes de evidências necessárias durante a perícia que normalmente fica sob controle do provedor.

O software como serviço (SaaS) é o modelo onde o cliente tem o menor controle dos dados. Para este ambiente o perito dependerá totalmente do provedor para obter as provas da investigação. Na plataforma como serviço (*PaaS*) é possível ter acesso ao código fonte do sistema e aos *logs* dos usuários. Para obter outras fontes de evidência como *logs* de servidores de aplicação, banco de dados, rede e *logs* portal de gerenciamento *PaaS* o perito deverá solicitar ao provedor. A infraestrutura como serviço (*IaaS*) oferece a maior variedade de fontes de evidências sob controle do cliente, é a plataforma que o perito tem acesso mais próximo de máquinas virtuais e tráfego de rede comparado a outros modelos. (JESUS et al.,2016). A figura 1 mostra os controles de acesso dos dados nas arquiteturas em nuvem e como a *Forensic-as-a-Service* concentra uma série de informações relevantes para a investigação.



Fonte: Nanda e Hansen (2016, p. 3).

Os métodos utilizados para coletar as evidências numa investigação em nuvem dependerá da natureza do caso. A recuperação de dados excluídos na nuvem pode estar limitado ao tipo de sistema de arquivo que o provedor utiliza em seu ambiente. Com sistemas e infraestrutura em nuvem os *snapshots* são grandes aliados dos peritos nas investigações e podem fornecer informações importantes antes, durante e depois de um incidente, possibilitando recriar o ambiente analisado para cada momento que foi realizado o *snapshot* calculando o *hash* de todos os arquivos gerado. As ferramentas utilizadas na forense computacional como *EnCase Enterprise, AccessData FTK, Autopsy,* entre outras também são usadas para aquisição dos dados quando um provedor em nuvem não fornece nenhuma ferramenta para coleta ou mesmo uma nuvem privada. (DYKSTRA, Josiah; SHERMAN, Alan, 2012). Neste caso os dados são coletado remotamente por um equipamento cliente com acesso a internet e que podem ser analisados fora do ambiente de produção, conforme figura abaixo:



Fonte: Dykstra e Sherman (2012, pg. 92)

Uma proposta apresentada por Dykstra e Sherman (2013) é o *Forensics OpenStack Tools* (FROST), conjunto de ferramentas de forense digital integrada a plataforma *OpenStack,* responsável por coletar dados do provedor de nuvem, *logs* de *API*, *firewall* e discos virtuais e disponibilizar através de uma interface de gerenciamento onde os usuários podem controlar e gerenciar seu ambiente de nuvem. Opera no plano de gerenciamento de nuvem sem que seja necessário a interação com o sistema operacional das máquinas virtuais trazendo maior confiabilidade dos dados coletados. Suas principais características são: recuperação de uma imagem de disco de qualquer máquina virtual e validação da sua integridade através de verificação criptográfica. Recuperação de *logs* de todas as solicitações de *API* realizadas para o provedor usando suas credenciais e recuperação dos *logs* do *firewall* do *OpenStack* para qualquer uma das máquinas virtuais do usuário com possibilidade de validar a integridade desses dados.

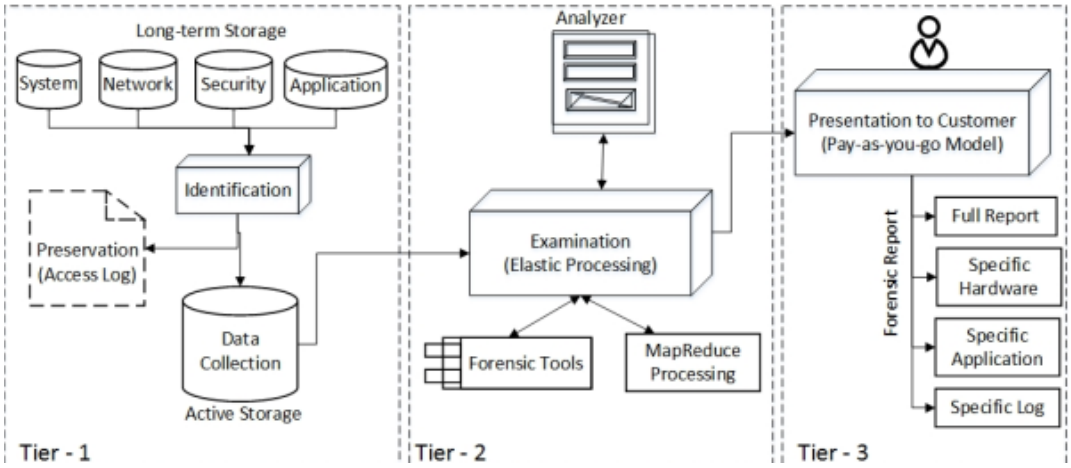
O *OpenStack* tem vários componentes que podem ser utilizados, mas para implementação do FROST foram utilizados os serviços *Nova* e *Horizon*. Em Nova, o serviço controla todas as atividades necessárias para manter o ciclo de vida das instâncias de uma nuvem *OpenStack*. É responsável por gerenciar todas as necessidades de recursos computacionais, rede, autorização, e escalabilidade da nuvem. E o *Horizon* é uma interface web de gerenciamento para o O*penStack* e se comunica com o serviço Nova através de uma API. (DYKSTRA, Josiah; SHERMAN, Alan, 2013)

Muitos trabalhos no campo da forense digital surgem devido a importância da evidência digital nas investigações criminais quando envolvem um ambiente tão complexo e diversificado como a computação em nuvem. Pensando nisso o Instituto forense holandês (NFI), agência do ministério de segurança e justiça criou uma plataforma de forense como um serviço que fornece métodos avançados e ferramentas para a investigação digital, conhecido como XIRAF, agora seu sucessor Hansken implementado para forense em dados distribuídos. Um dos principais objetivos desse sistema é diminuir o tempo de execução do caso, maximização da cobertura de rastreamento e disponibilidade para os envolvidos através de uma interface web com resultados seguros. O XIRAF é um framework que consiste em três componentes: repositório de ferramentas que possui os sistemas de extração de recursos, o gerenciador de extração de recursos que reúne os dados dessas ferramentas, mescla suas saídas XML e armazena o resultado no subsistema de armazenamento. Este consiste em

objetos grandes binários que armazenam dados de evidência bruta e um banco de dados XML que contém todos os recursos extraídos. Para garantir a integridade dos dados ainda é necessário realizar uma imagem do sistema ou dispositivo digital, a diferença é que estas imagens são copiadas para um armazenamento central para ser examinado por um conjunto de ferramentas que vão desde sistemas de extração de arquivos, espaço de disco não alocado, histórico de Internet, bate-papo e base de dados de correios eletrônicos. Estes dados são armazenados em um banco de dados centralizados e fornece ao investigador forense um ambiente de consulta rico em que a navegação, a pesquisa e os modelos de consulta predefinidos são todos expressos em termos de consultas de banco de dados XML. (ALINK et al., 2006)

O modelo proposto por Nanda e Hansen (2016) aborda a *Forensic-as-a-Service* como uma arquitetura de três camadas, onde cada nível é projetado para que mantenha a integridade e o isolamento dos dados. Na camada deste modelo é definido o momento da coleta de todos os dados relacionados aos serviços dos clientes, estes dados são armazenados em quatro categorias: sistema, segurança, rede e aplicação. Estes são compactados e são marcados com um identificador único de cada cliente e também com identificador de pesquisa para facilitar no momento da busca. Os dados são divididos em dois tipos de armazenamento, os ativos e os de longo prazo, os ativos são utilizados para guardar os dados com investigações forenses que estão curso e os de longo prazo são armazenados dentro das categorias definidas acima, no dois modelos de armazenamento a criptografia é aplicada e alterada a cada dia.

A camada dois será realizado o exame dos dados coletados da camada um e tem a capacidade de processamento MapReduce usado para análise de grande quantidade de dados. Na camada três inclui o módulo apresentação que é uma interface disponível ao cliente onde pode ser gerado diversos relatórios completos ou específicos de acordo com a necessidade, pagando pelo que usa ou *pay-as-you-go*. (NANDA; HANSEN, 2016). Segue abaixo a figura do modelo proposto pelos autores para uma ambiente de infraestrutura de nuvem baseada no *OpenStack* com ferramentas forenses como *Sleuth* and *Autopsy.*



Fonte: Nanda e Hansen (2016, p. 4).

É um processo natural da forense computacional que novas ferramentas e métodos auxiliem os peritos nos ambientes de computação em nuvem, principalmente quando este ambiente fica sob a responsabilidade de um provedor de acesso. Apesar de novas soluções surgirem para a realização da coleta e análise dos dados, os peritos ainda tem grandes desafios quanto a distribuição geográfica dos dados e a quanto a terceirização de serviço entre os provedores de serviço.

5 CONCLUSÃO

A computação em nuvem se consolidou no mercado proporcionando as empresas baixo custo em infraestrutura, grande capacidade de armazenamento e disponibilidade de seus serviços. Mas como toda nova tecnologia além dos benefícios também surgem novas práticas de crimes cibernéticos. Dessa forma o artigo buscou apresentar os diversos desafios enfrentados pelos peritos numa investigação forense em serviços de nuvem, assim como os cuidados na coleta dos dados nestes ambientes com grande capacidade de armazenamento e processamento. Também foi apresentado a importância na definição no momento da contratação de cláusulas claras sobre a posse dos dados e como os provedores irão disponibilizar estas informações relevantes para a investigação.

Os peritos também encontram oportunidades na realização de perícias em nuvem,

como o uso da infraestrutura e escalabilidade destes ambientes para realizar a coleta e armazenamento dos dados, esta é uma oportunidade que muitos provedores tem usado para oferecer outros serviços como a forense como um serviço que tem a proposta de reunir e guardar as informações usando ferramentas forenses para disponibilizar como serviço aos seus clientes quando necessário.

Novas tecnologias surgem a toda hora e para cumprir o propósito de entrega do parecer técnico os peritos contam com novos métodos e ferramentas que auxiliem nas coletas e identificação das provas periciais de forma rápida e segura, por isso é importante estar sempre buscando alternativas para a realização das investigações.

Algumas propostas realizadas por diversas ferramentas em ambientes distintos foram apresentadas neste artigo como o FROST, ferramenta forense que pode ser aplicado na plataforma *Openstack*, assim como o XIRAF, *framework* desenvolvido pelo governo holandês para a realização da forense em grandes ambientes garantindo a confiabilidade da investigação.

THE CHALLENGES OF COMPUTATIONAL FORENSICS IN CLOUD COMPUTING

Abstract: Cloud computing has come up with a new proposal for traditional computing, where the use AND storage applications are made to be available for users over the internet. Virtualization technology offers a number of benefits, but it also increases the potential of cybercrime. In this way, digital forensics experts are facing challenges in performing cloud forensics so they can obtain and preserve legal evidences. In these environments, people who have the evidence are the service providers, usually in data centers located in different parts of the world and with a large amount of data, which makes it almost impossible to extract the evidence. The research aims to investigate the challenges faced by computer forensics in the face of the cloud computing environment and showcase some cloud forensics models. .

Keewords: Cloud computing. Computer Forensics. Cloud Forensics.

REFERENCIAS

ALINK, Wouter et al (Org.). **XIRAF – XML-based indexing and querying for digital forensics**. Elsevier. Amsterdam, ago. 2006. p. 50-58. Disponível em: <https://www.dfrws.org/sites/default/files/session-files/paper-xiraf_-_ultimate_forensic_querying.pdf>. Acesso em: 21 abr. 2017.

CSA, CLOUD SECURITY ALLIANCE (Org.). **GUIA DE SEGURANÇA PARA ÁREAS CRÍTICAS FOCADO EM COMPUTAÇÃO EM NUVEM V3.0.** Estados Unidos: Cloud Security Alliance, 2011. Disponível em: <https://chapters.cloudsecurityalliance.org/brazil/files/2017/02/Guia-CSA-v-3.0.1-PT-BR-Final.pdf>. Acesso em: 20 fev. 2017.

COMPUTERWORLD: **Desvendando o Cloud Computing. Executive Briefing Computerworld.** Disponível em: <http://lt.idg.com.br/uol/EB_CW_cloud_computer.pdf>. Acesso em 04 de fev. 2017.

DAMACENA. Barbara Larissa Cândido. **DESAFIOS DA PERICIA FORENSE EM UM AMBIENTE DE COMPUTAÇÃO NAS NUVENS**. Dissertação de Graduação na UNIPLAC – 2014. Lages, SC. Disponível em: <http://revista.uniplac.net/ojs/index.php/tc_si/article/view/1911> Acesso em: 04.02.2017.

DIDONÉ, Dener. **COMPUTAÇÃO EM NUVEM E OPORTUNIDADES PARA A FORENSE COMPUTACIONAL**. Dissertação de Mestrado na UFPE – 2011. Recife, PE. Disponível em: <http://repositorio.ufpe.br/bitstream/handle/123456789/2745/arquivo6996_1.pdf?sequence=1&isAllowed=y> Acesso em: 28.01.2017.

DYKSTRA, Josiah; SHERMAN, Alan. Design and implementation of FROST: Digital forensic tools for the OpenStack cloud computing platform. **Elsevier: Digital Investigation.** Baltimore, p. 87-95. Ago. 2013. Disponível em: <https://www.dfrws.org/sites/default/files/sessionfiles/paperdesign_and_implementation_of_frost_digital_forensic_tools_for_the_openstack_cloud_computing_platform.pdf>. Acesso em: 17 abr. 2017.

DYKSTRA, Josiah; SHERMAN, Alan. Acquiring forensic evidence from infrastructure-as-a-service cloud computing: Exploring and evaluating tools, trust, and techniques. **Elsevier: Digital Investigation.** Baltimore, p. 90-98. out. 2012. Disponível em: <https://www.dfrws.org/sites/default/files/session-files/paper-acquiring_forensic_evidence_from_infrastructure-as-a-service_cloud_computing.pdf>. Acesso em: 15 abr. 2017.

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

FREITAS, Andrey Rodrigues de. **Perícia Forense aplicada à Informática: Ambiente Microsoft**. Rio de Janeiro: Editora Brasport, 2006.

JESUS, Antonio Velho et al (Org.). **Tratado de Computação Forense.** Campinas. São Paulo: Milennium, 2016. 606 p.

LOPEZ, Erik Miranda; MOON Seo Yeon; PARK, Jong Hyuk. **Scenario-Based Digital Forensics Challenges in Cloud Computing**. University of Science and Technology, Korea. Published: 20 Oct. 2016 . Disponível em: <http://www.mdpi.com/2073-8994/8/10/107/pdf>. Acessado em: 08.fev.2017.

MATHEW, Soumya; JOSE, Ann Preetha. Securing Cloud Computing from Different Attacks Using Intrusion Detection Systems. **International Journal Of Advanced Research In Computer And Communication Engineering: Securing Cloud Computing from Different Attacks Using Intrusion Detection Systems.** India, dez. 2012. Seção Vol 1, p. 753-759. Disponível em: <http://www.ijarcce.com/upload/december/3 - Securing Cloud from.pdf>. Acesso em: 7 fev. 2017.

NANDA, Saurav; HANSEN, Raymond. Forensics as a Service: Three-tier Architecture for Cloud based Forensic Analysis. **International Conference On Cloud Computing And Big Data (cloudcom-asia).** Hong Kong, p. 1-8. jun. 2016. Disponível em: <https://www.researchgate.net/profile/Saurav_Nanda/publication/301553168_Forensics_as_a_Service_Threetier_Architecture_for_Cloud_based_Forensic_Analysis/links/579247fd08ae33e89f76d6c0.pdf>. Acesso em: 18 mar. 2017.

NIST - National Institute of Standards and Technology. **The NIST Definition of Cloud Computing: Recommendations of the National Institute of Standards and Technology**. (NIST Special Publication 800-145). Setembro de 2011. Disponível em: <http://nvlpubs.nist.gov/nistpubs/Legacy/SP/nistspecialpublication800-145.pdf> Acesso em: 04 fev. 2017.

NIST - Cloud Computing Forensic Science Working Group. **NIST Cloud Computing Forensic Science Challenges** (Rascunho) (NIST Interagency Report 8006). Junho de 2014. Disponível em <http://csrc.nist.gov/publications/drafts/nistir-8006/draft_nistir_8006.pdf> Acessado em: 03.fev.2016.

PALMER, Gary. **A Road Map for Digital Forensic Research.** Digital Forensic Research Workshop (Dfrws), Report, 2001. Disponível em: <http://www.dfrws.org/sites/default/files/session-files/a_road_map_for_digital_forensic_research.pdf>. Acessado em: 08.fev.2017.

RUAN, Keyun et al. CLOUD FORENSICS. In: PETERSON, Gilbert; SHENOI, Sujeet. **Advances in Digital Forensics VII: 7th IFIP WG 11.9 International Conference on Digital Forensics.** Orlando: Springer, 2011. Cap. 2. p. 1-12. Disponível em: <http://cloudforensicsresearch.org/publication/Cloud_Forensics_An_Overview_7th_IFIP.pdf> . Acesso em: 2 fev. 2017.

SHAW. Adrian L.; BORDBAR, Behzad; SAXON, John; HARRISON, Keith; DALTON, Chris I. **Forensic Virtual Machines: Dynamic defence in the Cloud via Introspection**. Disponível em: <http://www.cs.bham.ac.uk/~bxb/Papres/2014.1.pdf> Acessado em: 09.fev.2017.

VERAS, Manoel. Cloud Computing:nova arquitetura da TI. 1ª ed. Rio de Janeiro: Brasport, 2012, 214 p.