UNIVERSIDADE FEDERAL FLUMINENSE

ALESSANDRO MONTEIRO DA COSTA

UM MÉTODO PARA ANÁLISE FORENSE SOBRE DADOS ARMAZENADOS EM APLICAÇÕES EM NUVEM

Niterói

2023

ALESSANDRO MONTEIRO DA COSTA

UM MÉTODO PARA ANÁLISE FORENSE SOBRE DADOS ARMAZENADOS EM APLICAÇÕES EM NUVEM

Dissertação apresentada ao Programa de Pós-Graduação em Computação da Universidade Federal Fluminense, como requisito parcial para obtenção do Grau de Mestre. Área de Concentração: Ciência da Computação.

Orientador:
Prof. Dr. RAPHAEL CARLOS SANTOS MACHADO

Niterói
2023

Ficha catalográfica automática - SDC/BEE
Gerada com informações fornecidas pelo autor

C837m Costa, Alessandro Monteiro da
UM MÉTODO PARA ANÁLISE FORENSE SOBRE DADOS ARMAZENADOS EM APLICAÇÕES EM NUVEM / Alessandro Monteiro da Costa. - 2023.
63 f.

Orientador: RAPHAEL CARLOS SANTOS MACHADO.
Dissertação (mestrado)-Universidade Federal Fluminense, Instituto de Computação, Niterói, 2023.

1. Nuvem. 2. Computação em Nuvem. 3. Produção intelectual. I. MACHADO, RAPHAEL CARLOS SANTOS, orientador. II. Universidade Federal Fluminense. Instituto de Computação.III. Título.

CDD - XXX

Bibliotecário responsável: Debora do Nascimento - CRB7/6368

ALESSANDRO MONTEIRO DA COSTA

UM MÉTODO PARA ANÁLISE FORENSE SOBRE DADOS ARMAZENADOS EM APLICAÇÕES EM NUVEM

Dissertação apresentada ao Programa de Pós-Graduação em Computação da Universidade Federal Fluminense, como requisito parcial para obtenção do Grau de Mestre. Área de Concentração: Ciência de Computação.

Aprovada em Junho de 2023.

BANCA EXAMINADORA

Prof. Dr. RAPHAEL CARLOS SANTOS MACHADO – Orientador, UFF

Prof. Dr. JOSÉ VITERBO FILHO, UFF

Prof. Dr. WILSON DE SOUZA MELO JUNIOR, INMETRO

Niterói

2023

Dedico este trabalho primeiramente a Deus, por ser essencial em minha vida, e a minha família que, com muito carinho e apoio, não mediram esforços para que eu chegasse até esta etapa da minha vida.

AGRADECIMENTOS

Primeiramente a Deus por ter me orientado nos momentos difíceis e ter permitido meu ingresso e a conclusão do curso em questão.

À Marinha do Brasil, mais especificamente a Diretoria de Comunicações e Tecnologia da Informação da Marinha (DCTIM), e a CC (T) Katia, por ter fornecido todo apoio necessário a realização do curso.

À minha noiva Mariane por ter me incentivado e compreendido os momentos ausentes e dedicados a conclusão do curso, bem como pelo amor, dedicação e companheirismo, sem os quais este trabalho não teria sido possível.

À minha família, em especial a minha Mãe, pelo suporte e incentivo que me foi dado durante o curso.

Aos meus amigos da Marinha do Brasil e demais órgãos de Segurança Pública do Estado pelos contributos para a realização deste trabalho.

Ao amigo e professor do Instituto Federal do Rio de Janeiro (IFRJ) Flávio Medeiros Henriques pela ajuda, paciência, disponibilidade e disposição sem as quais não teria sido possível a conclusão deste trabalho.

Ao meu orientador por ter dividido comigo seu tempo e conhecimento.

E, por fim, a todos os que estiveram comigo durante a jornada e contribuíram direta e indiretamente para a conclusão desta etapa.

O que prevemos raramente ocorre; o que menos esperamos geralmente acontece. (Benjamin Disraeli).

RESUMO

A Ciência Forense compreende um conjunto de conhecimentos técnico-científicos utilizados para desvendar atos ilícitos. O crescente uso de dispositivos e aplicativos eletrônicos e a crescente demanda por espaço de armazenamento popularizaram o uso da computação em nuvem. Sendo a realização de uma investigação forense na nuvem diferente da forense digital tradicional e que a conclusão de um caso exige muito mais do que uma simples identificação de evidências, fazendo-se necessário o correlacionamento de todos os dados e fontes obtidas, seja para ratificar uma suspeita ou para delinear novos caminhos na busca por novas evidências, este trabalho realiza uma revisão rápida de literatura, com o objetivo de identificar métodos e modelos anteriormente utilizados na aquisição de dados da nuvem, e a proposição de um método para a realização de um exame pericial em nuvem aplicável e testável em um caso real.

Palavras-chave: Forense na nuvem; Forense digital; Aquisição na nuvem; Aquisição de dados na nuvem.

ABSTRACT

Forensic Science comprises a set of technical scientific knowledge used to solve illicit acts. The growing use of electronic devices and applications and the growing demand for storage space have popularized the use of cloud computing. Since carrying out a forensic investigation in the cloud is different from traditional digital forensics and the conclusion of a case requires much more than the simple identification of evidence, making it necessary to correlate all the data and sources obtained, whether to ratify a suspicion or to outline new paths in the search for new evidence, this work performs a rapid review of the literature, to identify methods and models previously used in the acquisition of data from the cloud, and the proposition of a method for carrying out an examination Applicable and testable cloud expertise in a real case.

Keywords: Cloud forensics; Digital forensics; Cloud acquisition; Cloud data acquisition.

LISTA DE FIGURAS

LISTA DE TABELAS

SUMÁRIO

1. INTRODUÇÃO

Hodiernamente, dispositivos computacionais são utilizados em praticamente todos os aspectos de nossas atividades. Por diversas vezes, tais dispositivos estão envolvidos em atividades relacionadas a ações criminosas e, como os crimes costumam deixar vestígios, é de grande valia que sejam analisados devido as informações ali constantes/armazenadas. Como exemplo, cita-se o aumento de 99,5% no número de denúncias de pornografia envolvendo crianças e adolescentes tramitada por meio do mensageiro eletrônico Telegram. Vale salientar que o aplicativo possui um ambiente propício para ações criminosas, visto a falta de cooperação por parte da empresa responsável pelo aplicativo [1].

A aquisição e análise de qualquer forma de informação digital que possa ser usada como prova é o que se conhece como computação forense. Segundo Eleutério [2], “a Computação Forense objetiva 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-lhes validade probatório em juízo”. Denominamos, então, Computação Forense o conjunto de técnicas que viabilizam a preservação, extração, análise e formalização, para apresentação em juízo, das informações presentes nos mais variados dispositivos computacionais envolvidos em atividades criminosas.

Nas últimas duas décadas tem-se observado um aumento na utilização dos dispositivos eletrônicos e, consequentemente, uma maior demanda por espaço de armazenamento em nuvem, levando as autoridades e agentes da lei a introduzirem um novo campo na área forense ora denominado forense em nuvem [3, 4, 5].

Por anos, a perícia digital confiou no sistema de arquivos (data de criação, modificação, autor, etc.), examinando arquivos excluídos, realizando correspondência de palavras-chave e procurando hábitos ou atividades comuns do usuário; contudo, com a evolução dos dispositivos, surgiu o armazenamento de dados para além dos discos rígidos locais, passando a incluir o armazenamento em nuvem, cuja a aplicação de ferramentas forenses tradicionais não são mais eficazes [6]. Como exemplo, cita-se uma câmera de monitoramento inteligente. O dispositivo

supramencionado é responsável por capturar e processar as imagens de registro para, posteriormente, armazená-las e transferi-las para um outro dispositivo e/ou local de armazenamento. Tudo isso só é possível graças a tecnologia em nuvem, pois provê a substituição de toda a infraestrutura necessária para a operação do serviço permitindo com que o usuário não tenha que se preocupar com todo o *overhead*[1] necessário para o seu funcionamento. [8].

Diversos são os estudos baseados em dispositivos computacionais, assim como diversas ferramentas forenses tradicionais, tanto proprietárias quanto gratuitas, são disponibilizadas de modo a auxiliarem a aquisição dos dados e sua análise. Como exemplo, citam-se *Forensic Toolkit* (FTK), *EnCase*, *Volatility*, IPED, *Xplico,* UFED, *MOBILedit*, *Oxygen Forensic* [9, 10, 11, 12]; contudo, como em uma investigação os dispositivos podem não estarem acessíveis ao software de investigação tradicional e/ou os dados de interesse não estarem mais disponíveis fisicamente no dispositivo, torna-se necessário a análise forense no ambiente em nuvem, pois, em grande parte, os dados acabam por ficarem ali armazenados [6].

1.1 DEFINIÇÃO DO PROBLEMA

Na literatura observamos inúmeros trabalhos revisando processos forenses e diversos modelos propostos; entretanto, poucos foram desenvolvidos com um viés prático e aplicável em um eventual pós-incidente/crime em andamento [5, 13, 14, 15, 16, 17, 18, 19]. Em sua totalidade, as soluções demandam um ambiente previamente configurado o que pressupõe a necessidade de uma mentalidade voltada à forense por parte da instituição. Embora existam diversos modelos de referência, foi identificado que metodologias devidamente testadas para ambientes não convencionais ainda carecem de melhorias [20].

As metodologias, procedimentos, ferramentas e arquiteturas atuais não são projetadas para lidar ou auxiliar a perícia digital em ambientes de nuvem. Soma-se a isso a pouca motivação que os provedores de serviço possuem para prestar a devida assistência, a menos que sejam forçados a fazê-lo pela aplicação da lei. Portanto, os óbices relacionados a forense na nuvem vêm se tornando cada vez

[1] Conjunto de despesas/custos ligados à operação de uma empresa e que não são vinculados ao fornecimento ou produção de um produto ou serviço [7].

mais problemáticos e as soluções necessitam ser buscadas com certa urgência [21]. Diante do exposto, essa necessidade aparece como um ponto importante a ser transpassado.

1.2 OBJETIVOS

O objetivo deste trabalho é propor uma metodologia de forense em nuvem aplicável e testada em um caso real.

Para alcançar o objetivo supramencionado foram definidos os seguintes objetivos específicos:

• Consolidar a fundamentação teórica por meio de uma revisão rápida de literatura;-

• Realizar perícia em dispositivos computacionais com acesso à nuvem, oriunda de um caso real, baseado em uma revisão rápida de literatura; e

• Estabelecer uma metodologia a partir da realização do exame pericial.

1.3 CONTRIBUIÇÃO

Como contribuição primária se tem a adoção de um modelo aplicável a casos reais, com garantia de integridade dos dados e validade probatória em juízo.

Como contribuições secundárias tem-se:

- A proposta de uma metodologia para apoiar os investigadores na realização de perícias oriundas de ambientes hiperconvergentes; e
- A identificação de pontos de coleta a serem utilizados em investigações forenses.

1.4 ESTRUTURA DA DISSERTAÇÃO

A dissertação está estruturada da seguinte maneira: O Capítulo 2 contém os conceitos correlatos a computação em nuvem, virtualização e forense digital para melhor entendimento do trabalho. O capítulo 3 apresenta a metodologia utilizada para o desenvolvimento do trabalho. O Capítulo 4 apresenta a avaliação experimental onde se tem o planejamento e a execução do experimento. O Capítulo 5 contém a proposta do ciclo de vida. Por fim, no Capítulo 6 tem-se apresentadas as considerações finais, bem como as limitações e trabalhos futuros.

2. REFERENCIAL TEÓRICO

Neste capítulo vamos apresentar os conceitos correlatos a computação em nuvem e forense computacional para melhor entendimento do trabalho. Na Seção 2.1 é introduzido o tema computação em nuvem e sua fundamentação. Na Seção 2.2 são discutidos os aspectos relacionados a virtualização e, por fim, a Seção 2.3 trata da forense digital.

2.1 COMPUTAÇÃO EM NUVEM

A computação em nuvem é um modelo que objetiva possibilitar acesso de rede onipresente, de modo conveniente e sob demanda a um conjunto compartilhado de recursos de computação configuráveis que podem ser rapidamente provisionados e liberados com esforço mínimo de gerenciamento ou interação do provedor de serviços [22]. Resumidamente, o modelo em nuvem é composto por características essenciais, modelos de serviço e de desenvolvimento; contudo, de modo a obter um melhor entendimento do trabalho apenas serão definidos os modelos de serviço e os de desenvolvimento.

2.1.1 MODELO DE SERVIÇO

Software como um serviço (*Software as a Service* - SaaS): A capacidade fornecida ao consumidor é a de uso dos aplicativos disponibilizados pelo provedor de nuvem. Os aplicativos são acessíveis a partir de vários dispositivos clientes por meio de uma interface, como um navegador Web, por exemplo [22].

Plataforma como um serviço (Platform as a Service - PaaS): A capacidade fornecida ao consumidor é a de desenvolvimento e hospedagem de seus aplicativos, sejam eles criados por meio de linguagens de programação, bibliotecas, serviços e ferramentas e/ou adquiridos pelo consumidor [22, 23].

Infraestrutura como um serviço (*Infrastructure as a Service* – IaaS)*:* A capacidade fornecida ao consumidor é a de processamento, armazenamento, redes e outros recursos de computação fundamentais onde o consumidor pode implantar e executar software arbitrário, que podem incluir sistemas operacionais e aplicativos [22]. Nesse modelo, o consumidor possui, apenas, controle sobre os sistemas

operacionais, armazenamento e aplicativos implantados. Na maioria dos casos, ao consumidor é fornecido uma instância de máquina virtual configurada em termos de CPU, RAM e acesso à rede com base na seleção inicial do usuário [23].

2.1.2 MODELO DE DESENVOLVIMENTO

Segundo o [22], tem-se 04 (quatro) modelos de desenvolvimento definidos:

Nuvem privada: A infraestrutura de nuvem é provisionada para uso exclusivo de uma única organização, composta por vários consumidores. Ela pode ser de propriedade, gerenciado e operado pela organização, por um terceiro ou por alguma combinação deles, podendo existir dentro ou fora das instalações de uma organização.

Nuvem comunitária: A infraestrutura de nuvem é provisionada para uso exclusivo de uma comunidade específica de consumidores de organizações, que compartilham as mesmas preocupações, como missão, requisitos de segurança, política e aspectos de conformidade. Ela pode ser de propriedade, administrado e operado por uma ou mais organizações, por um terceiro ou alguma combinação deles, e pode existir dentro ou fora das instalações de uma organização.

Nuvem pública: A infraestrutura de nuvem é provisionada para uso aberto pelo público em geral. Ela pode ser de propriedade, gerenciada e operada por uma organização empresarial, acadêmica ou governamental, ou alguma combinação delas. Ela existe nas instalações do provedor de nuvem.

Nuvem híbrida: A infraestrutura de nuvem é uma composição de duas ou mais infraestruturas de nuvem distintas (privadas, comunitárias ou públicas) que permanecem como entidades únicas, mas unidas por tecnologia padronizada ou proprietária que permite a portabilidade de dados e aplicações (ex: rompimento de nuvem para balanceamento de carga entre nuvens).

2.2 VIRTUALIZAÇÃO

Virtualização é a tecnologia utilizada para criar representações virtuais de servidores, armazenamento, redes a partir de um único ambiente físico. O software de virtualização possibilita o “particionamento” de um hardware físico em diversas máquinas virtuais (VM – Virtual Machine) possibilitando que as Organizações utilizem seus recursos de hardware com maior eficiência e, consequentemente, com um maior retorno sobre seus investimentos [24, 25].

Uma VM é um container de software (arquivo de computador/imagem que se comporta como um dispositivo físico/hardware), rigorosamente isolado, contendo Sistema Operacional (SO) e aplicativos. A VM é particionada do restante do sistema garantindo a não interferência do software existente em uma VM no sistema operacional primário do dispositivo físico à qual ela está instalada (host), conforme pode ser observado na Figura 1. Vale salientar, nesse instante, que a diferença básica entre uma VM e um dispositivo físico está em sua “concepção”, pois uma é garantida por software e a outra por hardware, respectivamente [24, 25].

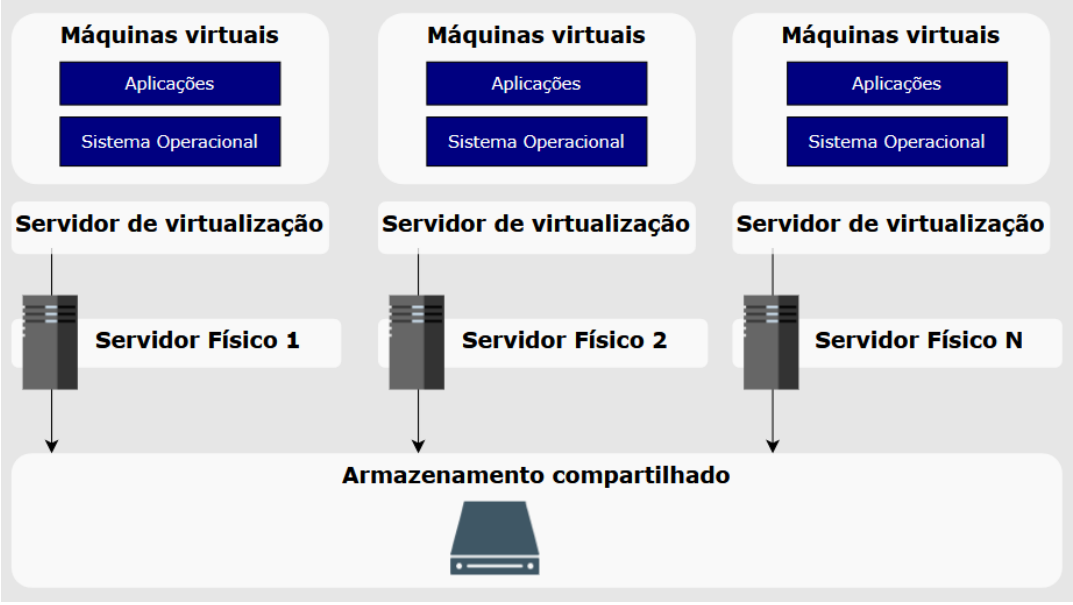


Figura 1. Ambiente virtual

Diversos são os tipos de virtualização existentes, dentre os quais tem-se: de servidores, de armazenamento, de rede, de dados, de desktops.

A virtualização de servidores é um processo que particiona um servidor físico em servidores virtuais, permitindo que vários SO sejam executados em um único hardware, de modo eficiente; A virtualização de armazenamento é um processo que combina as funções de *Network Attached Storage*[2] (NAS) e *Storage Area Network*[3] (SAN). Esse tipo de virtualização utiliza todo o armazenamento de dados físicos existentes, criando uma grande unidade de armazenamento virtual, que pode ser atribuída e controlada por meio de um software de gerenciamento garantindo, assim, a otimização de diversas atividades; A virtualização de rede é um processo que combina os serviços de rede (*switches*, roteadores, *firewall*) e permite que os aplicativos sejam executados, em uma rede virtual, como se estivessem em uma rede física; A virtualização de dados provê o interfaceamento, por meio de uma camada de software, entre dados (dados coletados de diversas fontes e formatos) e aplicação (que faz uso deles); A virtualização de desktops é um processo que permite uma resposta mais rápida ao surgimento de novas oportunidades e/ou necessidades de um determinado local de trabalho [24, 25].

Embora pareçam iguais, virtualização e computação em nuvem possuem propostas distintas, pois, conforme já mencionado, a virtualização possibilita a criação de variados ambientes a partir de um único dispositivo físico (hardware), enquanto a computação em nuvem propõe a entrega de soluções completas baseadas em modelo de serviços. Assim, pode-se inferir que a virtualização viabiliza a computação em nuvem.

2.2.1 AMBIENTES VIRTUALIZADOS

Diversos são os sistemas que possibilitam a virtualização, dentre os mais comumente conhecidos e utilizados tem-se: VMware, VirtualBox, Hyper-V, Citrix.

VMware é um fornecedor popular de sistemas de virtualização com, aproximadamente, 40% de participação no mercado de software de infraestrutura hiperconvergentes, juntamente com Citrix, Oracle e Microsoft [28, 29]. Os produtos oferecidos pela VMware incluem VMware Workstation, VMware Server e VMware

[2] NAS são servidores de armazenamento, em nível de arquivo, que fornecem acesso a dados, por meio de um ponto de acesso único, a um grupo heterogêneo de clientes [26].

[3] SAN é uma rede de alta velocidade independente e dedicada que interconecta e oferece pools compartilhados de dispositivos de armazenamento a vários servidores [27].

ESXi, entre outros [30]. Com a crescente tendência de virtualização, cada vez mais os sistemas de produção, as estações de trabalho e os desktops estão sendo virtualizados. Sendo um provedor popular, os ambientes virtuais VMware provavelmente serão encontrados por investigadores forenses. Para abordar o aumento da exposição a VMs, esta pesquisa se concentrará na aquisição e análise de produtos VMware.

Para fins de Estudo, adotou-se o sistema VMware, pois, além de ser amplamente utilizado no mercado, possui uma vasta documentação e o caso real, objeto do estudo, faz uso do VMware vSphere.

2.2.2 ARQUIVOS DO AMBIENTE VMWARE

Uma VM consiste em vários arquivos armazenados em um dispositivo de armazenamento, tendo como principais o arquivo de configuração (vmx), o arquivo de disco virtual (vmdk), o arquivo de configuração NVRAM (nvram) e o arquivo de log (log).

- “vmdk” - possui as características do disco rígido virtual, ou seja, armazenam o conteúdo das unidades de disco da máquina virtual;
- “nvram” - armazena as informações do BIOS para a máquina virtual;
- “vmx” – arquivo de configuração da máquina virtual. Arquivo de texto que contém as configurações de hardware e sistema operacional da máquina virtual; e
- “log” – contém os logs de atividade da máquina virtual atual.

Além dos arquivos supramencionados, podem ser encontrados:

- “vmsd” – arquivo que armazena informações e metadados sobre o *snapshot* da máquina virtual;
- “vmem” – arquivo de backup de paginação da máquina virtual;
- “vmxf” - Arquivos adicionais/complementares de configuração da máquina virtual;
- “vmsn” - Arquivo de dados do *snapshot* da máquina virtual; e
- “vmss” – arquivo que contém o estado de uma máquina virtual suspensa [31].

2.3 FORENSE DIGITAL

A Tecnologia da Informação está sempre se desenvolvendo e a cada novo desenvolvimento tem-se um papel maior em nossas vidas. A recuperação de evidências de dispositivos eletrônicos agora faz parte da atividade investigativa, tanto em âmbito público quanto privado. Os métodos de recuperação de evidências eletrônicas, mantendo a continuidade e integridade das evidências podem parecer complexos e caros, mas a experiência mostrou que, se tratados corretamente, produzirão evidências convincentes e econômicas [32].

A padronização da perícia digital é, como em qualquer outra ciência forense, uma obrigação. Ter um processo estruturado e formalizado que assegure a confiabilidade e integridade da perícia é de suma importância para que as evidenciais não sejam questionadas e, consequentemente, o resultado pericial tenha uma maior admissibilidade perante o juízo [20].

Não é demais enfatizar que as regras das provas convencionais se aplicam igualmente às provas eletrônicas baseadas em computador, tanto quanto ao material obtido de outras fontes. É sempre de responsabilidade do “oficial de justiça” assegurar o cumprimento da legislação e, em particular, certificar-se de que os procedimentos adotados na apreensão de quaisquer bens sejam efetuados de acordo com o estatuto e a jurisprudência em vigor [32].

A forense digital enfrenta desafios constantes para estar a par das tecnologias mais recentes que possam ser usadas para apresentar pistas relevantes em uma investigação [33]. É comum que os investigadores, durante uma diligência, considerem apenas um determinado dispositivo computacional para prover a aquisição de dados visto a associação com os métodos tradicionais; contudo, à medida que o armazenamento de dados evolui, a aplicação de técnicas de aquisição já conhecidas pode não ser suficientes e aplicáveis à aquisição de dados oriundos do armazenamento em nuvem necessitando, assim, de aprimoramentos [06]. Salienta-se que os clientes que fazem uso dos serviços em nuvem possuem acesso e controle limitados em todos os níveis dentro do ambiente e, sequer, possuem conhecimento de onde seus dados estão localizados fisicamente dificultando, caso

necessário, a realização de uma aquisição física do disco, conforme procedimento adotado nas perícias tradicionais [21].

Até onde é sabido, não foram identificadas soluções forenses que pudessem ser utilizadas nas plataformas de nuvem sem estarem previamente configuradas. Soma-se a isso a não identificação de um modelo único de processo forense admissível em um tribunal, para o ambiente de computação em nuvem, no tocante a aquisição e análise de dados não relacionados a ataques cibernéticos e de rede.

Embora existam diversas soluções projetadas e desenvolvidas para coletas e análise de dados, existe uma lacuna deixada por elas quando se faz necessário seu uso em ambiente de nuvem, pois ou foram projetadas para serem executadas na estação de trabalho do investigador ou nos servidores de hospedagem em nuvem (onde os arquivos de logs estão armazenados) [13].

2.3.1 CICLO DE VIDA DA FORENSE DIGITAL

Martini e Choo [23] apresentaram uma estrutura forense para computação em nuvem baseada em dois frameworks amplamente utilizados por McKemmish [34] e Kent *et al*. [35].

Ajijola [36] apresentou uma revisão e avaliação das diretrizes forenses da ISO/IEC 27037: 2012 [37] e do NIST SP 800-101 Rev.1 [33].

Kyei *et al*. [38] efetuou um estudo comparativo dos modelos de investigação forense digital existentes e propôs um modelo aprimorado, de modo a torná-lo mais adequado para a investigação e acusação. Vale ressaltar que o modelo, ora denominado ESDFIM (*Enhanced Systematic Digital Forensic Investigation Model*) não cobriu todos os aspectos da investigação de crimes cibernéticos, mas concentrou-se, principalmente, no processo de obtenção de evidências digitais.

Com base nas propostas e sabendo que nenhum dos padrões são únicos, ou seja, não abordam todos os processos investigativos relacionados a forense digital [36], adotou-se o ciclo de vida apresentado em [23] e [34], conforme figura 2.

Figura 2. Ciclo de vida da forense digital

A fase de “Identificação da evidência e Preservação” está preocupada com a identificação das fontes da evidência na investigação. Na primeira rodada, as evidências identificadas, provavelmente, serão os dispositivos físicos (*desktop, notebooks, smartphones, smartwatch*). Após efetuada a análise, poderá ocorrer uma segunda iteração cuja preocupação será em identificar serviços e provedores de nuvem relevantes para o caso, possíveis evidências armazenadas em nuvem e os processos para preservação dessas possíveis evidências. Ressalta-se, nesse momento, a necessidade em garantir a preservação adequada da evidência, independentemente da fonte identificada;

A fase de “Coleta” está preocupada com a captura dos dados. Vale salientar que, possivelmente, existirá variação nos métodos de coleta para cada tipo de modelo de serviço e de desenvolvimento;

A fase “Exame e Análise” baseia-se no exame e na análise dos dados. Nessa fase que o uso da computação em nuvem, provavelmente, será descoberto, levando a uma segunda (ou mais) iteração(ões) do processo; e

A fase de “Formalização e Apresentação” está relacionada com a apresentação legal das provas recolhidas, ou seja, com a elaboração do laudo pericial [23].

3. METODOLOGIA PARA O DESENVOLVIMENTO DO TRABALHO

Diversas pesquisas relacionadas a forense digital no âmbito da nuvem, mais especificamente em IaaS, foram desenvolvidas; contudo, todas dependiam da coleta e armazenamento de imagens das VM e a inclusão do provedor e/ou agentes como parte central da solução [14, 21, 18]. Vale ressaltar que: (1) para obter êxito nas propostas, faziam-se necessárias configurações prévias no provedor; e (2) os eventos para os quais as propostas foram desenvolvidas e submetidas possuíam uma maior relação com análise de rede (ataques cibernéticos, metadados de sistemas, *logs*) e não com eventos relacionados a análise de dados oriundos dos mais variados tipos de dispositivos computacionais (*notebooks*, *Hard Disk* - HD, *smartphones*, *smartwatches*) com armazenamento em nuvem.

A metodologia proposta, então, foca na admissão da perícia junto ao juízo de modo a evitar quaisquer questionamentos por parte da defesa do indiciado.

Este guia foi desenvolvido, especificamente, para um caso real onde não existiam configurações prévias que permitissem os peritos a fazer a aquisição dos dados da nuvem, para posterior análise em laboratório, incluindo os oriundos das VM de uma infraestrutura de nuvem privada. Vale mencionar que para a análise experimental e, posterior aplicação no caso real, fez-se uso do conceito de “Aprendizagem pela Experiência”, também denominado “Modelo de Aprendizagem Experiencial” (ELM) que considera um ciclo básico de quatro elementos, incluindo: (1) experiência concreta; (2) observação e reflexão sobre a experiência, (3) formação de conceitos abstratos baseados na reflexão; e (4) testar novos conceitos; corroborando com a aplicação de abordagens de como aprender pela experiência para realizar continuamente a análise sistemática de um sistema para prover relatórios eficazes de casos [39].

As possibilidades forenses oferecidas pela metodologia proposta são de grande valia para a forense digital, pois podem evitar que a perícia seja refutada na elucidação dos mais variados tipos de crimes.

Para tal, tem-se como os princípios da evidencia eletrônica baseados em computador: (1) Nenhuma ação tomada por agências/agentes da lei deve alterar os

dados mantidos em um computador ou mídia de armazenamento que possam ser solicitados em um tribunal; (2) Nas circunstâncias em que uma pessoa considera necessário acessar dados originais mantidos em um computador ou mídia de armazenamento, essa pessoa deve ser competente para fazê-lo e ser capaz de fornecer provas explicando a relevância e as implicações de suas ações; (3) Uma trilha de auditoria ou outro registro de todos os processos aplicados à evidência eletrônica baseada em computador deve ser criada e preservada, além de ser possível a reprodução dos exames e obtenção do mesmo resultado; e (4) A pessoa encarregada da investigação tem a responsabilidade geral de garantir que a lei e os princípios supramencionados sejam cumpridos [32].

De modo a corroborar com os princípios elencados, Kruse *et al.* [40] cita três atividades que devem se manter consistentes em uma metodologia forense: (1) adquirir a evidência sem alterar ou danificar o original; (2) autenticar que os dados da evidência recuperada sejam os mesmos que os dados originais apreendidos; e (3) analisar os dados sem modificá-los.

3.1 REVISÃO RÁPIDA DE LITERATURA

A revisão rápida (RR) é um método que simplifica as etapas de uma revisão sistemática de literatura de modo a produzir informações suficientes para solucionar, em tempo hábil, um determinado problema. Apesar de o método ser rigoroso, explícito e sistemático, ele permite concessões à amplitude/profundidade do processo, limitando os aspectos particulares do processo de uma revisão sistemática [41]

A metodologia identifica várias técnicas legítimas que podem ser utilizadas para reduzir o tempo de execução. Isso inclui usar estratégias de pesquisa mais amplas e/ou menos sofisticadas, conduzir uma revisão de revisões, restringir a quantidade de literatura cinza, extrair apenas variáveis-chave e realizar apenas uma avaliação de qualidade "simples" [41].

A pesquisa foi efetuada por meio da RR, com uma abordagem exploratória e qualitativa, permitindo, assim, a coleta de informações, sua descrição e o ponto de vista do autor.

A pesquisa coletou dados da coleção da *Web of Science* - Coleção Principal (*Clarivate Analytics*), por meio da plataforma da Capes onde foi possível efetuar a indexação de artigos/citações, por meio de assinaturas, de modo a alcançar os objetivos supramencionados.

A revisão foi realizada com base na elaboração de uma *string* de busca de modo a realizar um filtro nos estudos não correlacionados. A execução da *string* baseou-se em três grupos de palavras relacionadas ao tema proposto. O primeiro grupo é composto de palavras relacionadas ao termo de interesse (*cloud forensics*). O segundo grupo é composto de palavras relacionadas ao processo de interesse (*methodology, acquisition*) e o terceiro grupo é composto de palavras relacionadas a termos associados ao tema do trabalho (*forensic, digital forensic*).

As palavras-chave foram, então, adicionadas a fórmula, constante na Tabela 1, para consulta na plataforma supramencionada. A construção da lógica da pesquisa, desse modo, contemplou em sua primeira fase uma RR com o objetivo de identificar métodos e modelos previamente utilizados na aquisição e análise de dados oriundos da nuvem e, em seguida, aplicá-los em um estudo de caso, cujo propósito foi especificar e validar um processo para auxiliar na perícia de um caso real.

Tabela 1: Protocolo de pesquisa

TS=((("Cloud forensics")) AND (("methodology") OR ("acquisition")) AND (("Forensic") OR ("Digital Forensic")))

A execução da *string* retornou 40 (quarenta) estudos. Foram, então, aplicados aos estudos obtidos os critérios descritos na Tabela 2. A primeira rodada de avaliação buscou remover os estudos duplicados, tendo sido identificados 02 (dois) estudos. A partir da leitura do título e *abstract*/resumo, também foram aplicados os critérios de inclusão e exclusão, onde foram removidos os artigos que diretamente não possuíam correlação com o estudo, conforme apresentado na Figura 3: Seleção dos artigos. Os critérios de inclusão são os itens que permitirão manter o artigo para a seleção e os de exclusão são itens observados para a eliminação de um artigo da pesquisa.

Aos artigos não removidos foi realizada uma leitura completa, e, novamente, aplicados os critérios de inclusão e exclusão, obtendo, como resultado, um total de 14 (quatorze) estudos que possibilitaram o embasamento do trabalho em questão.

Como resultado do processo, foram utilizados 13 (treze) estudos listados na Tabela 3. Nesse conjunto, tem-se 1 (uma) publicação do ano de 2022; 3 (três) publicações do ano de 2019; 2 (duas) publicações do ano de 2018; 2 (duas) publicações do ano de 2016; 3 (três) publicações do ano de 2015; 1 (uma) publicação do ano de 2014; e 1 (uma) publicação do ano de 2013, sendo considerados os estudos até o mês de Janeiro de 2023.

Tabela 2: Critérios de inclusão e exclusão do artigo

Critério	**Descrição**
Inclusão (I1)	Estudos que contém assuntos referentes a aquisição e análise de ambientes virtuais e modelos de serviço de interesse
Inclusão (I2)	Apenas estudos escritos em inglês
Exclusão (E1)	Estudos que não focam nos processos de aquisição e análise forense
Exclusão (E2)	Estudos duplicados
Exclusão (E3)	Estudos do tipo *Short Paper*, com 03 páginas ou menos
Exclusão (E4)	Estudos anteriores ao ano de 2013
Exclusão (E5)	Resumos

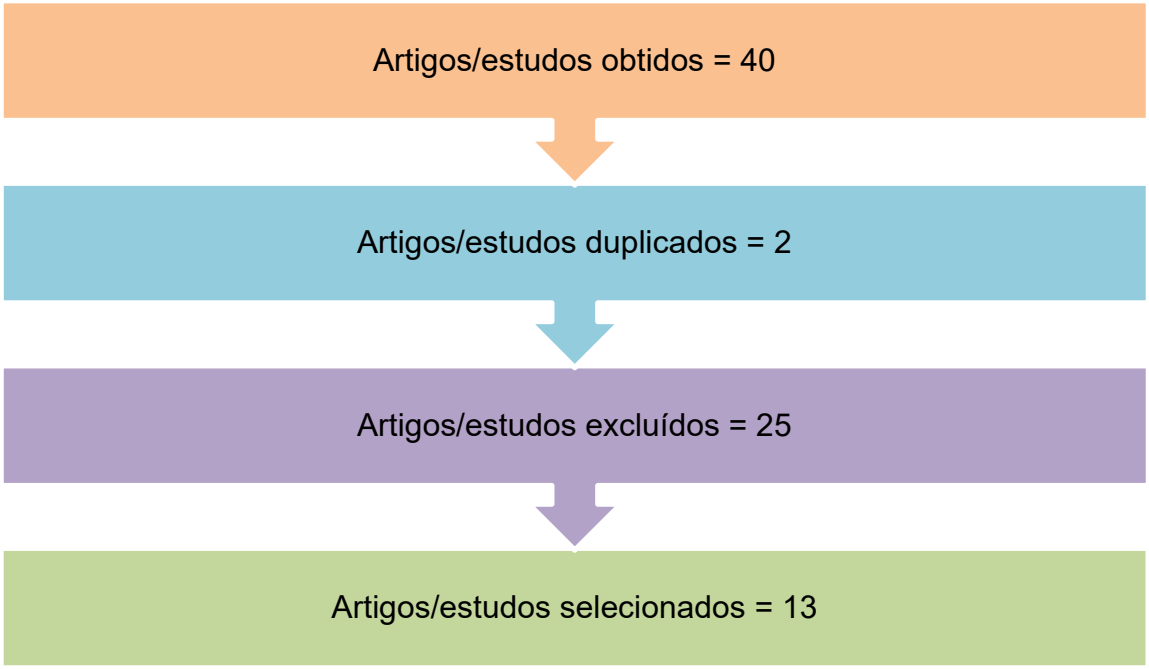


Figura 3: Seleção dos artigos

Tabela 3: Estudos Utilizados

Título do estudo	Referência	Ano
A Fog-Based Digital Forensics Investigation Framework for IoT Systems	Al-Masri *et al*.	2018
Towards the Development of a Cloud Forensics Methodology: A conceptual Model	Simou *et al*.	2015
Digital Forensic Architecture for Cloud Computing Systems: Methods of Evidence Identification, Segregation, Collection and Partial Analysis	Povar e Geethakumari	2016
BiSHM: Evidence detection and preservation model for cloud forensics	Purnaye	2022
SNAPS Towards building snapshot based provenance system for virtual machines in the cloud environment	Raju e Geethakumari	2019
Analysis of the Current State of Cloud Forensics The Evolving Nature of Digital Forensics	Yankson e Davis	2019
A Forensic Acquisition and Analysis System for IaaS: Architectural Model and Experiment	Alqahtany *et al*.	2016
A comparison of major issues for the development of forensics in cloud computing	Aydin e Jacob	2013
Forensic Process as a Service (FPaaS) for Cloud Computing	Eleyan e Eleyan	2015
Cloud forecasting: Legal visibility issues in saturated environments	Brow *et al*.	2018
Digital Forensics Investigations in the Cloud	Thethi e Keane	2014
A Survey of Various Frameworks and Solutions in all Branches of Digital Forensics with a Focus on Cloud Forensics	Alkhanafseh *et al*.	2019
Cloud Forensic Investigation: A Sneak-Peek into Acquisition	Raju *et al*.	2015

3.1.1 RESULTADO DA REVISÃO RÁPIDA DE LITERATURA

Esta seção apresenta alguns trabalhos relacionados objetivando a identificação de métodos e modelos previamente utilizados na aquisição de dados oriundos da nuvem.

Al-Masri *et al.* [6] comenta, em seu artigo, sobre a evolução do armazenamento de dados para além dos discos rígidos tradicionais, passando a incluir o armazenamento em nuvem. Nesse sentido, torna-se necessário a qualificação dos investigadores sobre como utilizar a nuvem para efetuar a coleta de evidências, pois a aplicação das ferramentas forenses tradicionais não são mais úteis ou aplicáveis nesse novo cenário. Para tal, o autor cita que é comum que as ferramentas de software forense criem um arquivo referente ao caso de modo a manter um registro de todos os dados específicos, daquele caso, envolvidos em uma investigação citando, como exemplo, o software “EnCase”. Para efetuar a coleta dos dados com o software de investigação, faz-se necessário o acesso total aos dispositivos que fazem parte do caso/evidência e como, em um ambiente de computação em nuvem, nem sempre o acesso é possível, ora pelos dados estarem armazenados em localidades distintas, ora por estarem em hardwares distintos, o uso nem sempre será possível. O autor menciona, ainda, que a análise forense na nuvem é uma importante área de pesquisa; contudo, a maioria dos trabalhos existentes estão concentrados em delinear os desafios associados à realização de investigações digitais na nuvem e muita pouca pesquisa foi conduzida para propor modelos ou soluções que possam potencialmente resolver os problemas inerentes à preservação de evidências digitais no nível da nuvem.

Simou *et al.* [5] apresentou um modelo conceitual para apoiar o desenvolvimento de um método e processo de forense em nuvem para auxiliar os desenvolvedores de sistemas na construção e prestação de melhores serviços e aos investigadores na realização de suas análises. O autor relata que o aumento no número do comportamento criminoso e/ou crimes nesses ambientes causa grande preocupação nos Provedores de Serviços, usuários e Agentes da Lei devido à falta de técnicas, metodologias, políticas e padrões; e que a diferença principal entre o ambiente digital/tradicional e o de nuvem é o acesso aos dispositivos e evidências. No ambiente tradicional, apreender o hardware que contém os dados e ter acesso

aos discos rígidos e provas é um processo “simples”; enquanto no ambiente de nuvem torna-se um pouco mais complexo, pois as informações de interesse (sistemas, dados) podem estar armazenadas em diferentes localidades, tornando a apreensão física do dispositivo computacional uma tarefa árdua. Nessa linha, foi realizado um estudo sobre os desafios e metodologias até então propostas e identificados os conceitos relacionados. Após, foi produzido um modelo conceitual e aplicado a um estudo de caso de modo a demonstrar como os diferentes conceitos e suas categorias se aplicam a uma investigação forense de nuvem; contudo, (1) a aplicação foi executada em um ambiente fictício, com a investigação sendo iniciada no momento do incidente ou no momento que estivesse sendo descoberta; e (2) o estudo de caso trata sobre uma invasão de servidor corporativo somado ao roubo de dados no cenário de nuvem. Vale salientar que o modelo proposto possui aplicabilidade para eventos referentes a incidentes de rede. Quando o evento a ser discutido está relacionado a um crime em curso, por exemplo a identificação de conteúdo de cunho pornográfico e sua propagação, o modelo proposto carece de adaptações para que possa ser aplicado.

Povar e Geethakumari [13] buscou projetar uma arquitetura forense digital para sistemas de computação em nuvem, listar os métodos de identificação, segregação e aquisição de fontes de evidências e descrever métodos para uma análise parcial de evidências relacionadas a uma conta de usuário em uma nuvem privada. O autor relata que para a análise forense digital tradicional tem-se diversas ferramentas comerciais e de código aberto e que podem ajudar, até certo ponto, os investigadores na execução da perícia em um ambiente virtual, mais especificamente na análise do disco virtual; contudo, elas podem falhar na conclusão do processo de investigação, principalmente na análise dos logs. Assim, faz-se necessário que os investigadores forenses e/ou pesquisadores adaptem as práticas forenses digitais tradicionais existentes e desenvolvam novos modelos forenses que permitam aos investigadores realizar a forense digital na nuvem. Conforme supracitado, o trabalho propôs uma arquitetura de forense digital para plataformas de computação em nuvem baseado na arquitetura OpenStack[4], objetivando fornecer serviços de investigação forense para coleta de dados,

[4] OpenStack “é uma plataforma *open source* que utiliza recursos virtuais agrupados para criar e gerenciar nuvens públicas e privadas” [42].

aquisição de dados híbridos e análise de eventos parciais. Outro ponto comentado no trabalho é a proposta de soluções para um exame inicial de dados das VM (disco rígido virtual e memória física de uma VM), minimizando o tempo de processamento das evidências digitais nos locais onde os artefatos de evidências digitais são mais prováveis de estarem presentes. Vale salientar que para a execução do experimento foi configurado um ambiente do zero objetivando o fornecimento de serviços de investigação forense; contudo, para os cenários já em curso nem sempre a aplicação será possível, visto a não existência de tais serviços previamente disponíveis e/ou com possibilidade de serem configurados. Além disso, a solução foi aplicada na plataforma supramencionada, não tendo sido testada em outras.

Purnaye [14] propôs um sistema, para o modelo IaaS, equipado com um agente de Inteligência Artificial para classificação de dados a serem utilizados como evidência denominado BiSHM (*Binary classification of Evidence using Smart Hypervisor Monitoring*). O autor cita que a aquisição de evidências na nuvem requer um grande esforço devido à inacessibilidade física, à falta de ferramentas forenses desenvolvidas e a elevada quantidade de dados existentes no ambiente. Para tal, o trabalho propõe uma nova abordagem para detecção e preservação de evidências fazendo uso de um agente de IA (inteligência Artificial). Diferentemente dos demais trabalhos já desenvolvidos, a instalação do agente não é feita na VM e sim no *hypervisor* proporcionando uma invasão mínima de privacidade. O modelo proposto (BiSHM) objetiva preservar os dados gerados durante um ataque partindo de e/ou terminando em uma VM, ou seja, a solução possui foco em evidências de análise de dados oriundas de eventos de rede. Além disso, o escopo da pesquisa apresentada limita-se à aquisição de evidências de memória e o sistema proposto é implementado e avaliado na plataforma de nuvem privada KVM (*Kernel Virtual Machine*). Assim, quando o evento a ser discutido estiver relacionado a um crime em curso e/ou o objetivo for a identificação de arquivos dentro de um Sistema de arquivos e e-mail, por exemplo, o modelo proposto não poderá ser aplicado.

Raju e Geethakumari [15] examinou os desafios da aquisição e análise de *snapshots* de uma VM, sugeriu o uso de modelos CFR (*Cloud Forensic Readiness*) e projetou um framework chamado SNAPS (*Snapshots based Provenance Aware System*) para se adequar à investigação forense em nuvem. O autor cita que o

processo seguido para a realização da forense tradicional não pode ser aplicado diretamente à nuvem devido a razões técnicas, a saber: inacessibilidade física (na nuvem não é possível ter acesso ao hardware físico); Multitenancy (uma evidência pode conter eventos de outros usuários); e correlação das evidências (por ter natureza distribuída, as evidências podem abranger vários recursos de nuvem). Torna-se, então, implícito a necessidade de conceber abordagens para aquisição e análise de *snapshots* oriundas da nuvem para lidar com os problemas associados a forense. Soma-se a isso o fato da existência de técnicas anti-forenses que podem ser aplicadas, tais como: exclusão da VM, desativação dos recursos de monitoramento e exclusão do *snapshot*. Ressalta-se, oportunamente, que: (1) o trabalho versa sobre incidentes relacionados a redes de computadores, tais como: ataques de negação de serviços, ataques de injeção de malware na nuvem, ataques de *phishing*, ataques de reversão de VM, esteganografia, entre outros; (2) o modelo proposto deve ser aplicado antes do incidente acontecer; (3) possui como foco a análise de vdisk, vRAM, *snapshots*, volumes, Service logs e VM logs; e (4) faz uso da plataforma OpenStack.

Yankson e Davis [16] examinou os tipos de serviços oferecidos pelos provedores de nuvem, os desafios atuais, os métodos de aquisição e análise e as soluções encontradas durante cada etapa de uma investigação. O artigo cita que diversos trabalhos analisaram os desafios da investigação forense na nuvem; contudo, um número limitado avançou no desenvolvimento de uma solução completa para todos os aspectos da forense na nuvem. Ressalta-se, oportunamente, que a maioria dos trabalhos se baseiam na exploração de metodologias forenses para dar suporte a investigação de incidentes de segurança, ou seja, possui foco em evidências relacionadas a eventos de rede. Foram apresentados os desafios atuais oferecidos pelos provedores de serviços (CSPs – *Cloud Service Providers*) relacionando-os às etapas da perícia em nuvem (identificação, preservação, coleta, exame, análise e apresentação). Vale observar, com um pouco mais de detalhe, os aspectos de duas etapas: identificação e preservação. Na etapa de “identificação” o autor comenta que no modelo IaaS, o investigador poderá ter acesso às VM e aos arquivos de log; no entanto, nos modelos PaaS ou SaaS o investigador não terá acesso ao hardware e/ou VM e terá que contar com o CSP para o fornecimento de provas. Na etapa de “preservação”, se a integridade dos dados não for mantida, as

provas podem ser consideradas sem valor. Devido à natureza da perícia na nuvem, o autor afirma ser provável que ocorram erros durante o estado de preservação de dados, pois vários atores lidam com as evidências. Foram apresentadas, ainda, 04 (quatro) tecnologias utilizadas na etapa de coleta de evidências para análise forense em nuvem, a saber: OWADE, FROST, CloudTrail, and Magnet Forensics Dropbox Decryptor. Por fim, o autor comenta que uma análise da cena do crime só é possível com o uso dos *snapshots* e que é possível recuperar dados excluídos de uma VM, desde que esses dados não tenham sido substituídos; no entanto, caso o cliente tenha feito a exclusão dessa instância, os dados passam a ser irrecuperáveis.

Alqahtany *et al.* [21] propôs um sistema para a aquisição e análise forense em um modelo IaaS a fim de garantir que as organizações permaneçam no controle total ao invés de dependerem dos CSPs e investigar as implicações técnicas e os custos resultantes do sistema na operação diária de um sistema em nuvem. O trabalho relata que as arquiteturas de nuvem atuais não oferecem suporte aos investigadores, não estão em conformidade com os procedimentos forenses digitais e os provedores geralmente não possuem ferramentas e recursos apropriados para realizar, de modo adequado, a aquisição e análise. Soma-se a isso, a dependência em relação aos CSPs, sendo considerado um dos desafios mais significativos a ser superado. O autor cita que poucas pesquisas sobre como realizar investigações digitais de maneira forense foram conduzidas e que os CSPs possuem pouca motivação para prestar assistência pós incidente. Em suma, a arquitetura disponibilizada pelos CSPs não foi/é projetada com a mentalidade forense. O trabalho concluiu que em investigações forenses normais só é possível adquirir uma imagem do sistema após o incidente; contudo, o sistema proposto possui a capacidade de obter uma imagem forense antes e depois de um incidente de maneira independente dos CSPs, fornecendo controle total dos dados ao cliente; contudo, vale ressaltar que a solução depende da instalação de um agente na máquina do cliente, ou seja, o ambiente deverá estar configurado antes da ocorrência do incidente.

Aydin e Jacob [17] analisou diversas áreas relacionadas a computação forense em nuvem, as partes interessadas, os possíveis projetos que poderiam auxiliar na análise e os principais problemas existentes, sendo muitos relacionados a

gravação, armazenamento e aquisição de dados. O autor cita que em ambientes tradicionais, qualquer problema pode ser facilmente investigado graças ao fácil acesso às máquinas físicas e quando necessário, as provas podem ser apreendidas para investigações criminais; contudo, no ambiente em nuvem isso é dificultado, pois as VMs são executadas a partir de datacenters, com dados podendo ser armazenados em outras localidades, cruzando, por vezes, várias jurisdições tornando-se um problema para a aquisição de evidências. Fontes variadas sugerem diferentes etapas para uma investigação forense digital, dependendo do nível de detalhe que desejam incluir e apresenta um modelo simplificado composto por quatro etapas: Identificação, Coleta, Exame e Reporte e comenta que problemas em qualquer etapa individual criará um efeito dominó, com dificuldades para quaisquer etapas posteriores do processo. Como exemplo, o autor cita que problemas com a coleta de provas poderiam criar uma justificativa para posterior questionamento em tribunal. Identificar uma instância(s) e até mesmo a coleta de evidências em si pode não ser uma tarefa simples, especialmente devido às diversas maneiras pelas quais os serviços em nuvem são oferecidos. No decorrer do artigo são analisadas as partes interessadas (usuários, provedores de nuvem, governo e aplicação da lei) que estarão envolvidas no desenvolvimento da análise forense de nuvem. Vale salientar que o principal objetivo da parte interessada “aplicação da lei” será demonstrar que quaisquer ferramentas e práticas forenses recém-desenvolvidas são compatíveis com as diretrizes estabelecidas e são aceitáveis para um tribunal. No tocante aos problemas tem-se os fatores que, provavelmente, farão diferença nas tentativas de registrar informações que possam ser úteis para um investigador (privacidade, sobrecarga de rede e desempenho, integridade, Granularidade). A preocupação com os quesitos de integridade merece destaque, pois como os serviços em nuvem são fornecidos a partir de um local sem acesso físico a seus usuários, o método tradicional de apreensão de evidências seria muito difícil de confiar. Soma-se a isso a necessidade de adaptação da cadeia de custódia[5], pois conseguir comprovar que os dados permanecem os mesmos desde o momento da apreensão na nuvem será um ponto importante a ser resolvido. Por fim, no quesito projeto tem-se a apresentação de possíveis soluções com os quais os dados podem

[5] Documento que registra a ordem cronológica ou trilha em papel, apresentando a apreensão, custódia, controle, transferência, análise e disposição de provas físicas ou eletrônicas [16].

ser coletados ou retidos para uso em investigações posteriores (coletas de atividades na VM e forense como serviço).

Eleyan e Eleyan [18] apresentou um processo forense em nuvem, composto por 04 fases (identificação, coleta/aquisição e preservação, exame/processamento e análise e divulgação dos resultados). Além disso, propôs/desenvolveu um processo forense como serviço, denominado de FPaaS (*forensic proces as a service*), por meio da linguagem BPEL (*Business Process Execution Language*). O autor comenta que os investigadores enfrentam desafios durante a realização de uma perícia na nuvem, pois carecem de ferramentas e técnicas relacionadas a esse contexto. Ainda comenta que em um ambiente de nuvem os investigadores podem não ter acesso físico a evidência, como em um sistema de computação tradicional, criando novos desafios técnicos e jurídicos e, consequentemente, possibilitando o surgimento de uma nova área de pesquisa. Durante o trabalho é relatado que o serviço proposto pode ser implantado nos modelos de serviço IaaS, PaaS e SaaS e que mais trabalhos são necessários para desenvolver cada serviço no processo forense e implementar o FPaaS.

Brown *et al.* [43] investigou e analisou as medidas forenses digitais em ambientes de nuvem para obtenção de provas admissíveis em processos criminais sujeitos à jurisdição federal nos Estados Unidos da América (EUA). Como hipótese subjacente de pesquisa, baseou-se no fato dos investigadores não poderem analisar os servidores de provedores de modelos de serviço SaaS, de maneira aceitável para admissibilidade da prova, mantendo total conformidade legal com os aspectos relacionados a privacidade. O autor cita que pesquisadores já questionam a adequação/utilização de ferramentas e métodos forenses tradicionalmente aceitos para obtenção de evidências oriundas de ambientes de nuvem e que estabelecer uma base para a admissibilidade dá origem a preocupações adicionais. Além disso, tem-se os fatores relacionados a proteção das informações a serem recuperadas, visto os aspectos relacionados a privacidade em vigor. Foi representado/ilustrado o equilíbrio, entre privacidade e integridade dos dados, que os investigadores devem ter ao coletar evidencias, pois se a parte que adquirir ou analisar os dados não tiver as permissões legais necessárias, qualquer evidência produzida poderá ser excluída/ignorada. Em um ambiente de nuvem, o valor probatório da evidência

digital é diminuído pela volatilidade do conteúdo armazenado e, consequentemente, tem-se reduzida sua admissibilidade em um julgamento. Assim, estabelecer a confiabilidade de qualquer dado acessível em rede representa um desafio significativo e a falta de um processo padronizado no qual os prestadores de serviços possam seguir, faz com que seja difícil estabelecer a confiabilidade do método utilizado em cada caso. Por fim, o autor comenta que durante a análise forense de conteúdo, oriundo de provedores de serviço do tipo SaaS, existe o risco de invasão da privacidade de suspeitos, de outros usuários de contas e até mesmo de assinantes de serviços não relacionados no processo/ação em curso.

Thethi e Keane [44] abordam os aspectos e determinam a relação entre os tempos de aquisição para as diferentes capacidades de armazenamento, por meio da aquisição remota, para obter dados oriundos de máquinas virtuais na nuvem; e utiliza um estudo de caso hipotético para investigar a importância de utilizar uma abordagem parcial e completa para a aquisição de dados e para determinar como cada abordagem afeta a duração e a precisão da investigação forense. Os resultados indicaram que a relação entre o tempo de aquisição da imagem e os diferentes volumes de armazenamento não são lineares, devido a diversos fatores, dentre os quais destaca-se à Internet. No tocante a aquisição, por exemplo, foi observada que o FTK *Remote Agent* provou ser mais eficiente em relação a outros métodos de aquisição, apresentando uma redução de quase 12% no tempo. O artigo cita que apesar da extensa pesquisa no campo da nuvem, não existem dados comparativos completos sobre as ferramentas tradicionais de aquisição e não há muita ênfase na avaliação do tempo necessário para a aquisição dos dados. Tal fato deve-se aos pesquisadores considerarem as ferramentas atuais incapazes de lidar com os dados volumosos e/ou não utilizarem essas ferramentas. Além disso, as linhas do tempo produzidas com a ajuda do estudo de caso mostraram que a abordagem híbrida deve ser preferida à abordagem completa, especialmente em cenários críticos de tempo. Por fim, o autor apresenta uma discussão sobre o impacto da investigação na nuvem onde comenta que o ambiente é um excelente instrumento para criminosos, visto a facilidade de criação e exclusão das VMs, levando, por vezes, à eliminação completa das evidências. Soma-se a isto os aspectos legais que possibilitam o não fornecimento da imagem completa do disco rígido no qual aquela determinada VM reside, por parte do CSP.

Alkhanafseh *et al.* [19] apresentou o levantamento das diversas estruturas e soluções forenses existentes com foco em forense de nuvem. Discutiu as diferentes classes forenses (perícia de computador, rede, móvel, computação em nuvem e *internet of things* - IoT), seus frameworks, desafios e soluções. Abordou o aspecto metodológico, os desafios existentes e efetuou uma comparação detalhada com as desvantagens, diferenças e semelhanças das estruturas de computação em nuvem sugeridas. O artigo cita que o principal objetivo da perícia forense digital é detectar, extrair e analisar evidências da mídia digital e prepará-las para a acusação, de modo que um caso possa ser apresentado em um tribunal; que os investigadores devem implementar procedimentos forenses consistentes e precisamente definidos; e que o processo de investigação para um determinado dispositivo pode não ser o utilizado para um outro dispositivo, sendo, portanto, difícil encontrar um processo que seja compatível com todos os dispositivos e ambientes existentes. De modo geral, não existe uma estrutura padrão para o processo de investigação, pois ele depende da área de investigação e de uma variedade de casos. Assim, nenhum dos frameworks propostos/identificados possui um propósito geral de modo a ser utilizado em qualquer tipo de investigação. Além disso, existem questões que não são levadas em consideração nas estruturas propostas, salientando a confidencialidade, conscientização de segurança e precisão do processo de investigação, mais especificamente os relacionados a coleta de evidências e etapas de exame. No tocante aos desafios, o autor cita a unificação do formato dos *logs*, visto a grande variedade de soluções existentes; a falta de termos e condições no contrato de nível de serviço (SLA), pois o contrato é o principal ponto e condições entre o usuário e o CSP; a falta de perícia forense, especialmente ao nível da computação em nuvem; a diminuição do acesso a dados forenses e controle sobre dados em todos os níveis do lado do cliente; a falta de colaboração internacional e mecanismo legislativo no acesso e intercâmbio entre as nações; e a integridade e estabilidade, pois a análise forense depende da comunicação cliente-servidor. Por fim, o autor apresenta as principais soluções para a realização da forense em nuvem e conclui que a maioria das estruturas incluídas na pesquisa se concentra na solução de problemas específicos e que não foram encontrados frameworks que levassem em consideração os aspectos de segurança e privacidade, os quais estão se tornando muito importantes e frequentes na computação em nuvem, especialmente quando se trata de servidores remotos e documentação dos participantes da nuvem.

Raju *et al.* [45] analisou os principais desafios envolvidos na fase de aquisição de ambientes em nuvem e desenvolveu uma ferramenta para adquirir evidências de máquinas virtuais para uso na plataforma de nuvem OpenStack. A solução possibilita a um investigador adquirir evidências referentes a memória virtual, disco virtual e logs de serviço. A ferramenta pode ser utilizada tanto pelo provedor de nuvem quanto pelo investigador, seja ele interno ou externo àquela determinada Instituição. Salienta-se que a solução proposta foi desenvolvida, especificamente, para ambientes de nuvem OpenStack, aplicadas ao modelo IaaS e com o CSP fornecendo o devido suporte, pois esse, segundo os autores, é o aspecto mais importante para a realização da perícia. Realizar análises forenses em nuvem podem levar não apenas a desafios técnicos, mas também a desafios organizacionais e legais, sendo a segurança e privacidade dos dados na nuvem pontos a serem observados. Durante o trabalho, ainda são discutidos alguns desafios relevantes na fase de aquisição (aquisição seletiva de dados, volatilidade dos dados, aquisição de dados com o ambiente em execução, recuperação de dados e segregação das evidências) e salientado que se várias plataformas de nuvem estiverem envolvidas em um determinado incidente, as ferramentas utilizadas para aquisição e análise deverão abordar a variabilidade nas infraestruturas de nuvem, visto cada modelo (IaaS, PaaS, SaaS) fornecer um tipo de acesso diferente ao investigador.

Com base nos trabalhos analisados, observou-se, até a presente data, propostas de soluções forenses voltadas para incidentes de redes de computadores aplicáveis em ambientes controlados. Além disso, foi observado a possibilidade de serem analisados os arquivos de configuração oriundos das VM, sendo de grande valia para o desenvolvimento deste trabalho. Além disso, a análise dos arquivos de configuração seria uma boa maneira de possibilitar a reprodução do exame pericial. Evidencia-se que na literatura não foi identificado uma solução capaz de nortear/auxiliar os investigadores na elucidação de eventos em curso, cujo ambiente seja desconhecido, fazendo uso dos métodos/ferramentas tradicionais.

4. AVALIAÇÃO EXPERIMENTAL

4.1 PLANEJAMENTO DO EXPERIMENTO

O estudo em questão foca na admissão de um caso real onde são demonstradas as etapas a serem percorridas em cumprimento a uma diligência requisitada pelo juízo, oriunda de um inquérito.

Inicialmente os peritos receberam os documentos referentes a perícia e observaram o possível uso de recursos oriundos da nuvem, por parte do indiciado. Como ainda não haviam se deparado com uma perícia dessa natureza, fez-se necessário o planejamento e a execução de testes, em um ambiente controlado, antes da execução no ambiente real.

O planejamento incluiu o levantamento do ambiente a ser analisado, conforme Figura 4 e Tabela 4, e a configuração de um ambiente virtual, conforme Tabela 5.

O cenário envolve a investigação de estações de trabalho, servidor de arquivo e caixa de correio eletrônico, de modo a responder as seguintes questões: (1) foi encontrado o arquivo <nome do arquivo> no servidor de arquivos; (2) é possível informar quem criou; (3) é possível informar se o arquivo foi compartilhado por meio de correio eletrônico; e (4) se o arquivo poderia ser acessado por outros usuários, são respondidas ao longo do Estudo de Caso.

Para tal, conforme supracitado, fez-se necessário o estabelecimento de um ambiente controlado para a realização de testes, antes da realização do exame pericial, de modo a minimizar a possibilidade de contaminação dos dados de interesse e, consequentemente, possíveis questionamentos por parte da defesa do indiciado.

A instituição periciada disponibiliza aos seus colaboradores um servidor de arquivos e de correio eletrônico, apenas para uso corporativo, sendo considerado/caracterizado como um serviço em nuvem IaaS e SaaS, respectivamente. Vale salientar que: (1) o servidor de arquivos é considerado um modelo de serviço IaaS, pois a configuração e manutenção do servidor é de

responsabilidade/administração da Filial A. A Matriz disponibiliza apenas os recursos de processamento, armazenamento, redes, entre outros; (2) O serviço de correio eletrônico é considerado um serviço SaaS, pois está sob a administração da Matriz, sendo ela a responsável por disponibilizar o serviço/aplicativo aos consumidores.

O ambiente controlado, então, decorre da instalação e configuração de um servidor de arquivos e de correio eletrônico.

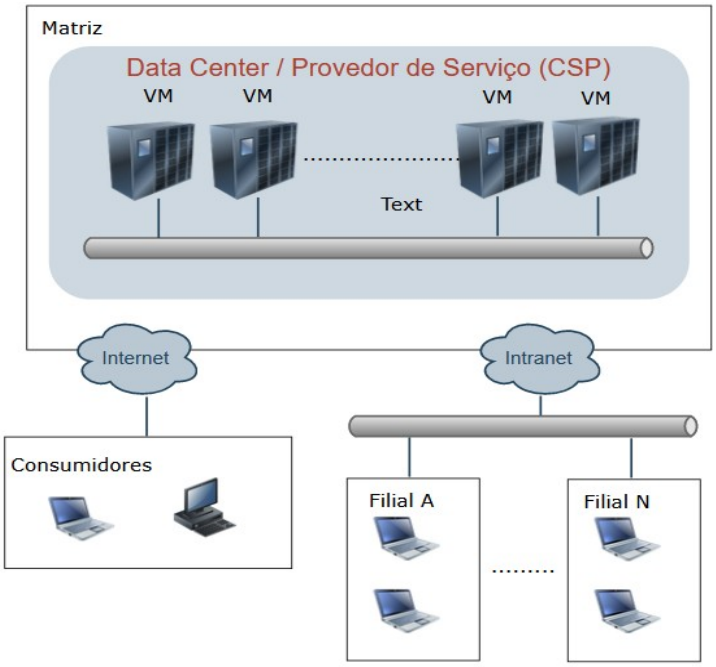


Figura 4: Arquitetura simplificada

Tabela 4: Característica do ambiente a ser examinado

Ambiente de virtualização	VMware vSphere
Servidor de arquivos	Samba/Linux ()
Servidor de Correio Eletrônico	Zimbra/Ubuntu (versão não informada)

Tabela 5: Característica do ambiente controlado

Ambiente de virtualização	VMware workstation
Servidor de arquivos/Sistema Operacional	Samba/Debian 11.6.0

4.2 EXECUÇÃO DO EXPERIMENTO

4.2.1.AMBIENTE CONTROLADO

De modo a identificar um método/maneira de realizar o exame e a possibilidade de utilizar os softwares tradicionais para indexar e analisar imagens oriundas de arquivos “vmdk”, foi configurado um ambiente similar ao real, conforme abaixo.

Como configurações iniciais tem-se:

1) No servidor de arquivos:
    a. O estabelecimento do serviço samba, conforme Figura 5;
    b. A adição do usuário de interesse, ora denominado “indiciado”, conforme Figura 6; e
    c. A adição da imagem de interesse, ora denominada “imginteresse.jpg”, e seu respectivo hash, conforme Figuras 7 e 8, respectivamente.

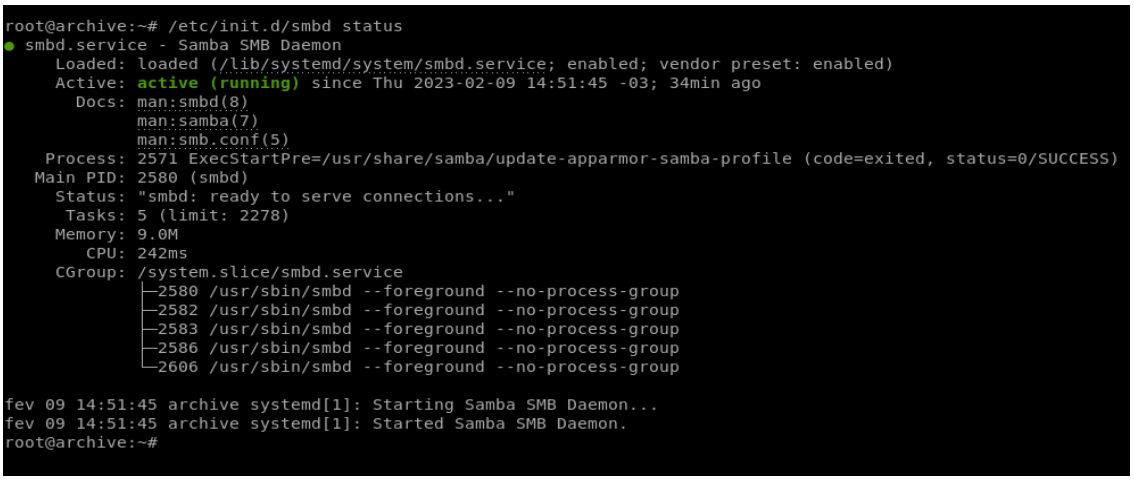


Figura 5: Estabelecimento do samba

Figura 6: Usuário de interesse

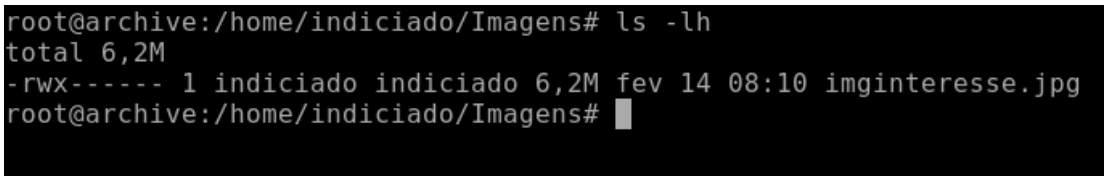


Figura 7: Objeto de interesse

Figura 8: Hash do objeto de interesse

Com base nas informações obtidas no referencial teórico e, após devidamente configurado o ambiente, foram traçadas duas linhas de ação para a elucidação dos fatos: (1) os peritos optaram em analisar, primeiramente, os dispositivos físicos de modo a identificar os possíveis arquivos de interesse e a existência do uso de recursos na nuvem; e (2) identificar o modelo de

desenvolvimento/serviço utilizado e obter os arquivos do disco rígido virtual e/ou uma instância da máquina virtual.

Como a aquisição e análise de dispositivos computacionais tradicionais era de conhecimento dos peritos e não faz parte do escopo deste trabalho, a linha de ação 1 não será abordada. No tocante a linha de ação 2, tem-se a aquisição dos arquivos com a extensão “vmdk” (disco físico virtual). Ressalta-se, nesse momento, a existência do arquivo “vmdk original” e mais um, proveniente do *snapshot*, conforme figura 9.

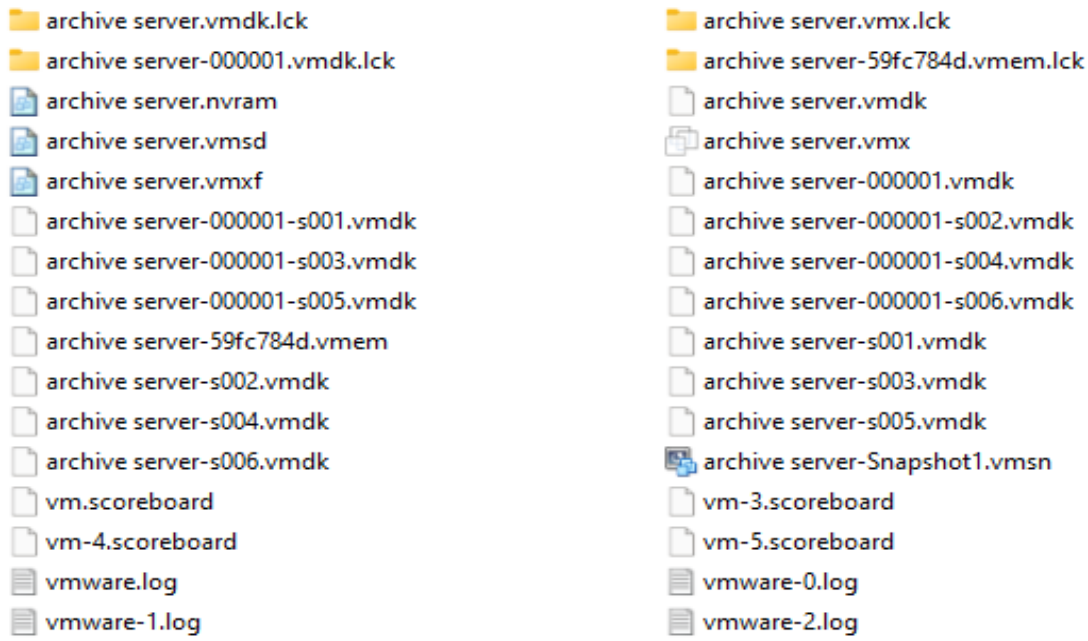


Figura 9: Arquivos de configuração do servidor de arquivos

A análise foi executada a partir do arquivo “vmdk” pertencente ao arquivo original. Vale ressaltar que devido a fragmentação dos arquivos, foi necessário unificá-los em um único arquivo. O arquivo “vmdk” foi, então, submetido ao Indexador e Processador de Evidências Digitais (IPED), logrando êxito na obtenção dos dados de interesse, conforme observado nas Figuras 10, 11, 12 e 13.

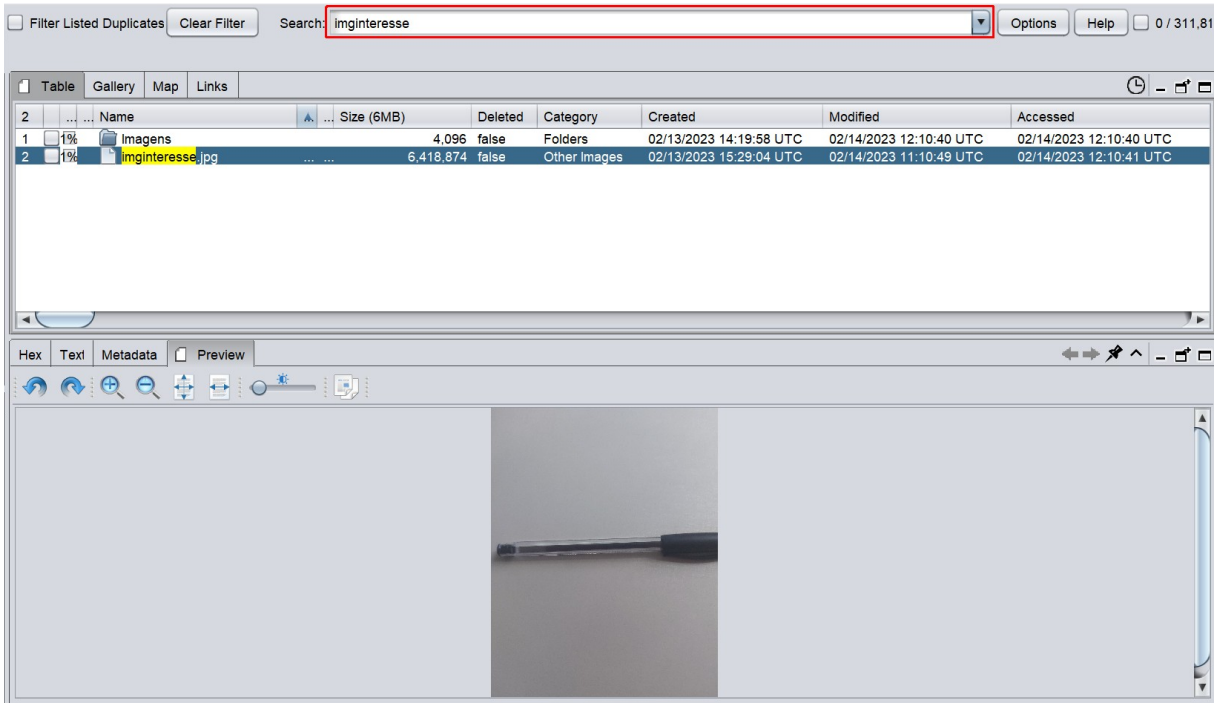


Figura 10: Identificação da imagem de interesse via IPED

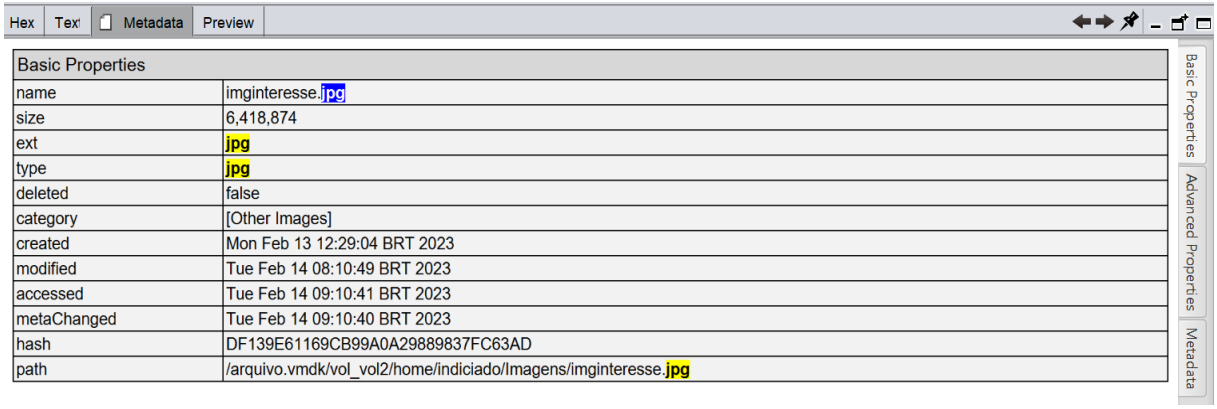


Figura 11: Local de origem via IPED

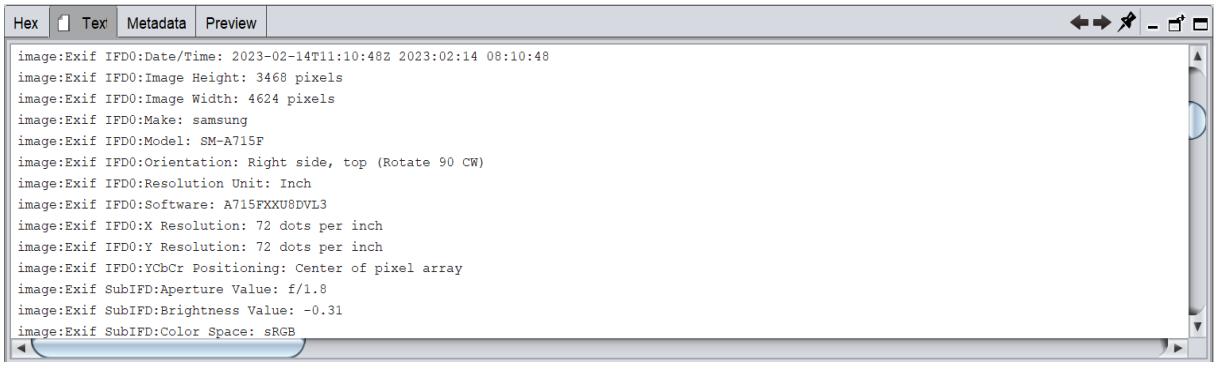


Figura 12: Informações adicionais via IPED

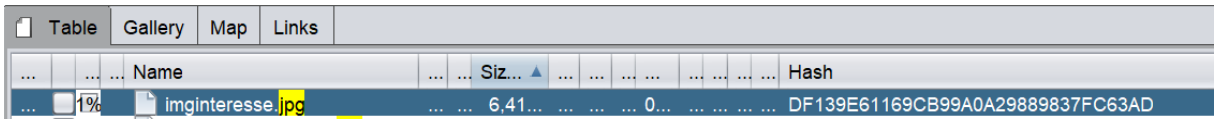


Figura 13: Hash do arquivo via IPED

De modo a validar o resultado obtido via IPED, submeteu-se o mesmo arquivo unificado “vmdk” na ferramenta “*AccessData Forensic Toolkit* (FTK)”, conforme Figuras 14, 15, 16 e 17, tendo sido obtido o mesmo resultado.

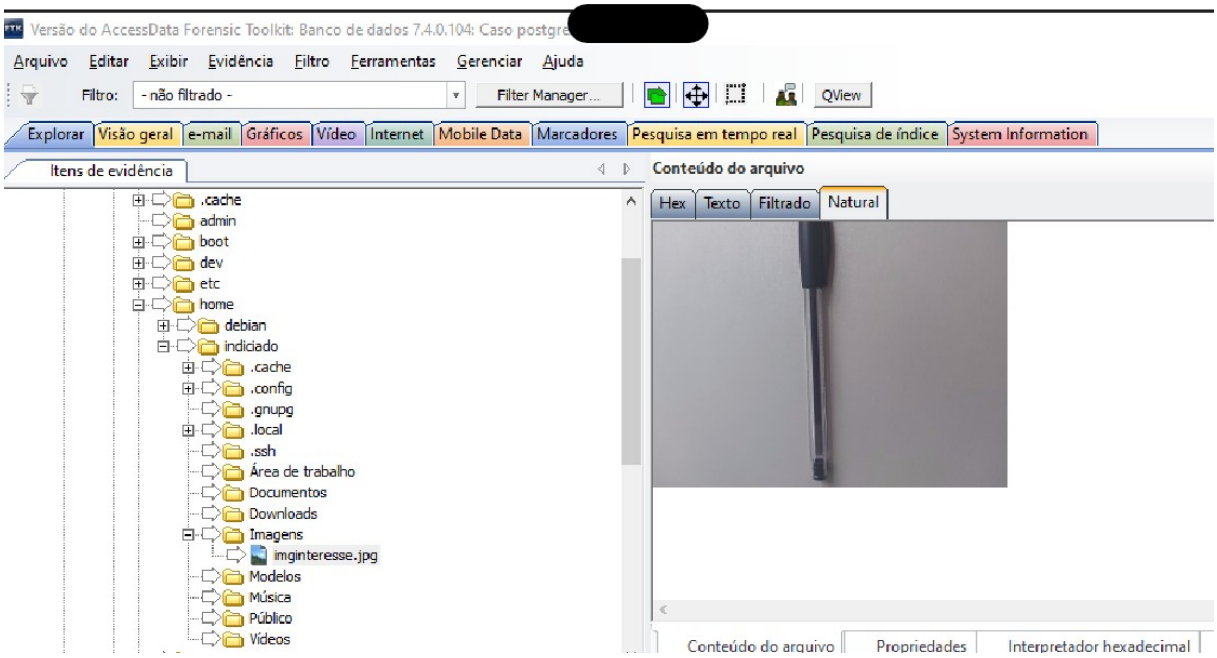


Figura 14: Identificação da imagem de interesse via FTK

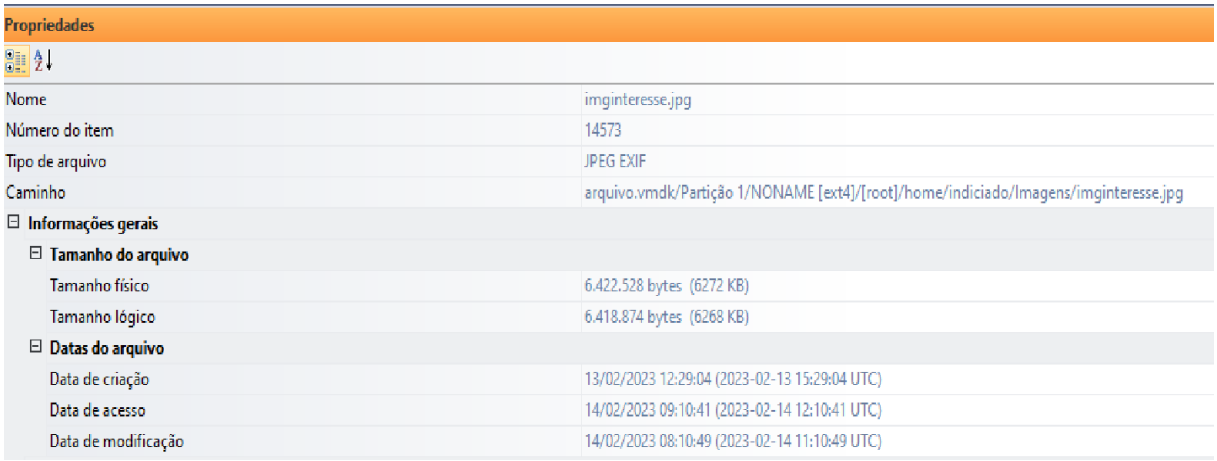
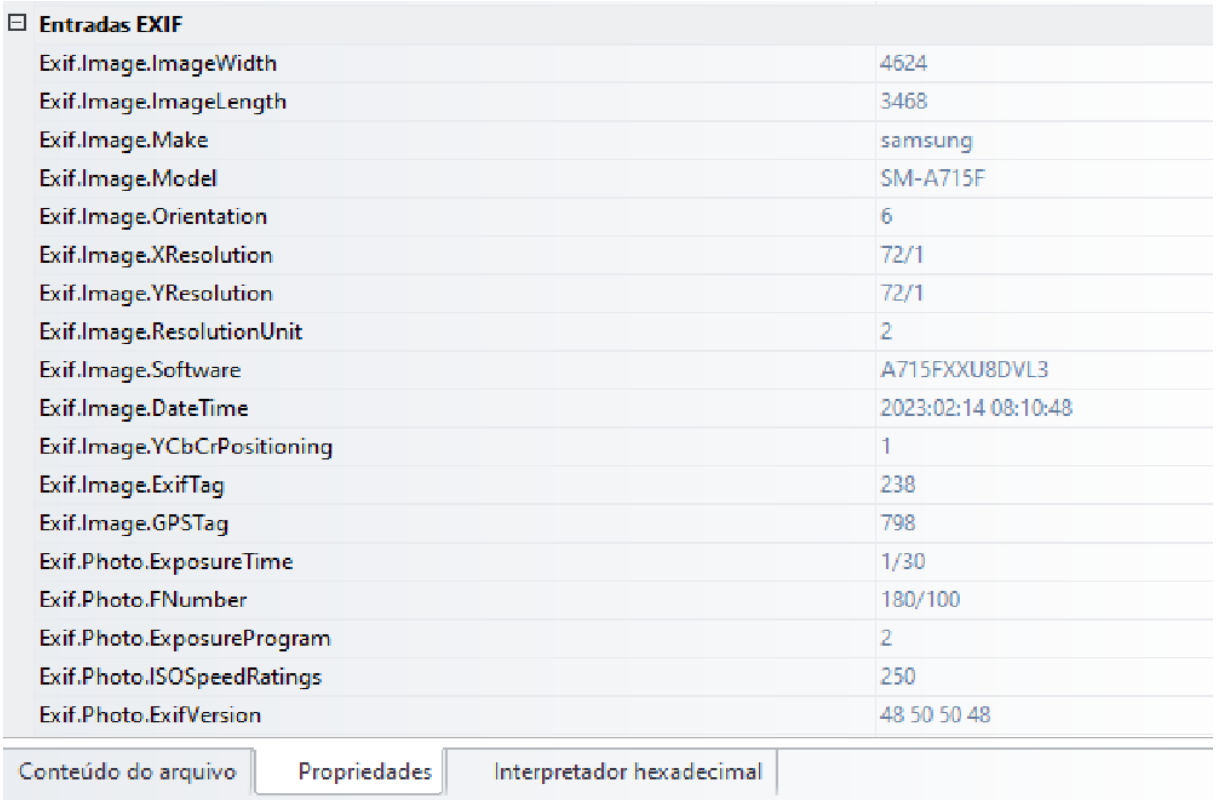


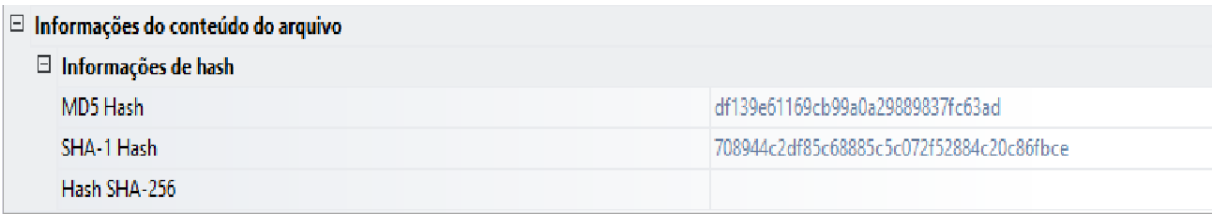
Figura 15: Local de origem via FTK



Entradas EXIF	
Exif.Image.ImageWidth	4624
Exif.Image.ImageLength	3468
Exif.Image.Make	samsung
Exif.Image.Model	SM-A715F
Exif.Image.Orientation	6
Exif.Image.XResolution	72/1
Exif.Image.YResolution	72/1
Exif.Image.ResolutionUnit	2
Exif.Image.Software	A715FXXU8DVL3
Exif.Image.DateTime	2023:02:14 08:10:48
Exif.Image.YCbCrPositioning	1
Exif.Image.ExifTag	238
Exif.Image.GPSTag	798
Exif.Photo.ExposureTime	1/30
Exif.Photo.FNumber	180/100
Exif.Photo.ExposureProgram	2
Exif.Photo.ISOSpeedRatings	250
Exif.Photo.ExifVersion	48 50 50 48

Conteúdo do arquivo | Propriedades | Interpretador hexadecimal

Figura 16: Informações adicionais via FTK



Informações do conteúdo do arquivo	
Informações de hash	
MD5 Hash	df139e61169cb99a0a29889837fc63ad
SHA-1 Hash	708944c2df85c68885c5c072f52884c20c86fbce
Hash SHA-256	

Figura 17: Hash do arquivo via FTK

Como a execução do procedimento supramencionado foi bem sucedido e, partindo da premissa que a análise dar-se-ia da mesma maneira, ou seja, por meio do arquivo “vmdk”, não se fez necessário o estabelecimento e análise do servidor de correio eletrônico, tendo sido iniciada a análise no ambiente real.

4.2.2. AMBIENTE REAL

Tendo como base o modelo apresentado por [23] e [34] e os testes provenientes do ambiente controlado, descrito acima, deu-se início ao processo pericial; contudo, faz-se necessário a inclusão de mais uma etapa no ciclo de vida apresentado, pois a designação dos peritos e o conhecimento do que está sendo

investigado (quesitos) é de suma importância para o correto andamento do processo pericial/elucidação dos fatos.

Inicialmente foram verificados e validados o(s) ofício(s) referente(s) a designação de peritos e seus quesitos. A partir desse instante deu-se início a perícia.

Foram recebidos os dispositivos computacionais a serem periciados e suas respectivas cadeias de custódia, dentre os quais tem-se: 03 (três) Desktop e 03 (três) HD. Assim, foi efetuado o bloqueio de escrita dos discos, a cópia fiel das imagens, por meio da ferramenta *Acess Data FTK Imager*, e gerado seus respectivos *hashes*.

De modo a efetuar a recuperação de arquivos e indexação dos dados, oriundos dos dispositivos físicos (Desktop e HD), foi utilizada a ferramenta forense IPED (Indexador e Processador de Evidências Digital).–

Como indícios de armazenamento em nuvem foram encontrados, fez-se necessário o levantamento das informações inerentes aos recursos em nuvem utilizados pela Instituição a qual o indiciado trabalhava. Assim, observou-se o uso dos modelos de serviço IaaS, para os serviços de armazenamento, e SaaS, para os serviços de e-mail. Partiu-se, então, para a obtenção da informação referente ao modelo de desenvolvimento em uso, obtendo como resposta a nuvem privada.

Diante do exposto, foi feito contato com o CSP de serviços do tipo IaaS para identificar:

- A tecnologia utilizada
    - Identificou-se o uso do sistema de virtualização VMware vSphere; logo, os dados de interesse estariam presentes nos arquivos “vmdk”;
- A disposição das VM dentro do ambiente computacional, ou seja, os aspectos referentes a localização e segregação das instâncias/dados
    - Identificou-se que o servidor de arquivo possuía apenas uma VM; logo, os dados estavam dispostos em um único local. Além disso, foi identificado a existência de *backups*/*snapshots*;

- A quantidade de discos virtuais existentes
    - Identificou-se que o sistema possuía um único disco virtual;
- A quantidade de dados existentes no servidor
    - O servidor possuía aproximadamente 6TB de dados;
- Se o CSP possuía configurado serviços de investigação forense para coleta, aquisição e análise de dados
    - O CSP não possuía tais recursos configurados; e
- Se o CSP de serviços forneceria o arquivo “vmdk” para análise.
    - O arquivo seria disponibilizado.

Após obtidas as informações, os investigadores optaram pela cópia dos arquivos “vmdk”. Fez-se a primeira tentativa, com o ambiente em produção, não obtendo êxito. Foi identificado, então, a possibilidade de paralização dos serviços. Assim, os serviços foram colocados em “baixa/down” e efetuada uma nova tentativa de aquisição, também sem êxito. Cabe ressaltar que a tentativa persistiu por 66h e acredita-se que a falha na execução tenha sido ocasionada pela elevada quantidade de dados existentes. Diante do exposto, a perícia foi realizada por meio da técnica/método Live Forensics[6].

Com indícios de propagação de imagens via correio eletrônico corporativo, fez-se necessário contato com o CSP de serviços do tipo SaaS para identificar a tecnologia utilizada; a disposição das VM dentro do ambiente computacional, ou seja, os aspectos referentes a localização e segregação das instâncias/dados; a quantidade de discos virtuais existentes; a quantidade de dados existentes no servidor; se o CSP possuía configurado serviços de investigação forense para coleta, aquisição e análise de dados; e se o CSP de serviços forneceria o arquivo “vmdk” para análise; contudo, por se tratar de uma base dados com, aproximadamente, 25 TB (vinte e cinco), a obtenção dos arquivos “vmdk” não foi possibilitada.

Assim, por se tratar de um serviço de correio corporativo, os investigadores optaram por: (1) verificar a existência de políticas sobre o uso adequado do e-mail corporativo; (2) verificar o “termo de utilização” e sua assinatura, por parte do

[6] Live Forensics é o método de realização de exame pericial em ambiente de sistema ativo e em execução [46].

indiciado, de modo a evitar questionamentos relacionados a Lei Geral de Proteção de Dados (LGPD); (3) solicitar o congelamento da conta do indiciado; (4) solicitar uma cópia da base de dados; e (5) solicitar a criação de uma cópia da conta de correio, com o auxílio do CSP, de modo a possibilitar a análise dos e-mails ali existentes, garantindo, assim, a integridade da base de dados e a reprodução do exame pericial.

Para a análise dos dados oriundos do armazenamento em nuvem e correio eletrônico fez-necessário o uso da técnica *Live Forensics*. No tocante ao armazenamento, foram identificados os serviços ali configurados (servidor de arquivos) de modo a tentar identificar os detalhes dos arquivos (quem e quando foram criados, quem acessou e/ou modificou, entre outros); contudo, devido a falhas na configuração do servidor, tais informações não puderam ser obtidas. Cabe salientar que os diretórios onde existiam os indícios do crime tiveram suas permissões modificadas para apenas leitura evitando, assim, a contaminação da prova. No tocante ao e-mail, conforme supracitado, foi disponibilizado uma cópia da conta de correio eletrônico para análise dos dados. Como não foram encontrados indícios de troca de e-mails, provavelmente devido a possíveis exclusões, foram solicitados os backups existentes para análise.

Após findadas as buscas pelas informações necessárias para a resposta aos quesitos, foi elaborado o laudo pericial com o resultado, as evidências digitais encontradas e os procedimentos, métodos, técnicas e ferramentas utilizadas durante o decorrer da perícia.

5. PROPOSTA DO CICLO DE VIDA

5.1. FASES DO CICLO DE VIDA

Levando em consideração os resultados da revisão rápida de literatura e os procedimentos desenvolvidos no estudo de caso para neutralizar algumas das principais limitações da forense digital na nuvem, será apresentada nesta seção uma proposta metodológica a partir do ciclo de vida da Forense Digital discutido na seção 2.3.1 (Figura 2). Salienta-se, oportunamente, conforme já supracitado, a necessidade da inclusão de mais uma etapa no ciclo de vida, a etapa de verificação e validação dos documentos e identificar modelo de serviço e desenvolvimento.

Figura 18: Metodologia proposta

Para realização de forense digital na nuvem, conforme demonstrado no caso analisado, é importante adicionar a etapa de verificação e validação dos documentos, pois a nomeação do perito e o conhecimento do que será investigado são de suma importância para que seja garantida a corretude processual e o investigador possa dirimir eventuais dúvidas referentes aos quesitos propostos.

Sendo assim, com a adaptação do modelo de ciclo de vida da forense digital ao contexto de perícias na nuvem, conforme o caso apresentado/analisado, podemos detalhar os procedimentos de execução da metodologia proposta conforme descrito na Figura 19.

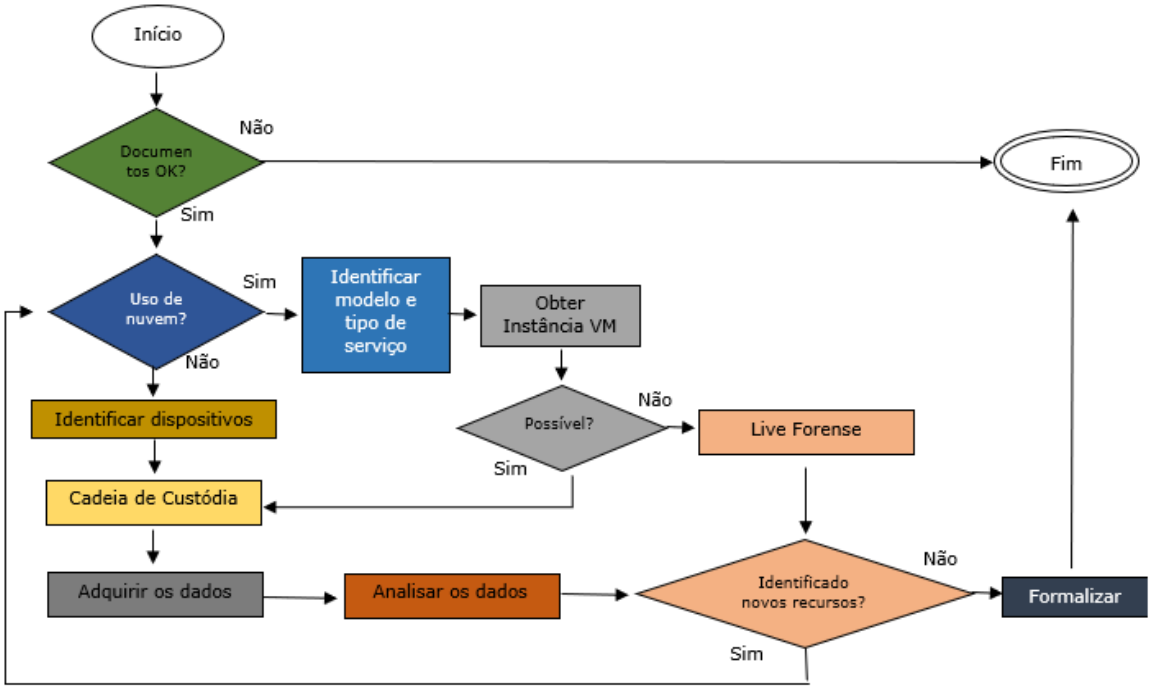


Figura 19: Fluxo de execução da metodologia proposta

Os tópicos a seguir descrevem cada uma das etapas descritas nas Figuras 18 e 19, as quais descrevem o modelo de forense digital na nuvem proposto neste trabalho.

5.1.1. ETAPA 01: VERIFICAÇÃO E VALIDAÇÃO DOS DOCUMENTOS

Essa etapa é de suma importância para o início da metodologia proposta, pois é ela que garante a corretude pericial e processual.

O primeiro passo, então, é verificar os documentos necessários para o início do exame, dentre os quais: nomeação dos peritos e quesitos/fatos a serem elucidados.

5.1.2. ETAPA 02: IDENTIFICAR MODELO DE SERVIÇO E DESENVOLVIMENTO

Nessa etapa, caso já tenha sido identificado o uso de recursos oriundos da nuvem, devem ser observados os modelos de serviço (IaaS, PaaS, SaaS), de desenvolvimento (privada, pública, comunitária, híbrida) e os CSP envolvidos, pois a partir dessas informações será possível saber como proceder nas demais etapas.

O primeiro passo, então, é identificar os dispositivos computacionais com armazenamento em nuvem a serem periciados, bem como as informações supracitadas para que a execução das demais etapas seja possibilitada.

Vale ressaltar que o foco do trabalho são os modelos de serviço IaaS e SaaS para uma nuvem privada, não sendo descritos os detalhes para os demais tipos de serviço e desenvolvimento.

5.1.3. ETAPA 03: IDENTIFICAR EVIDÊNCIAS

Nessa fase devem ser observados os dispositivos computacionais que possam conter as evidências desejadas, ficando atento ao modo de acondicionamento deles, e suas respectivas cadeias de custódia.

Caso o dispositivo computacional a ser periciado seja físico (HD, SSD, *notebook*, servidor, *smartphone*) deve-se garantir que as informações ali armazenadas não sejam alteradas durante o processo de aquisição da imagem (cópia fiel). Caso identificado o uso de recursos em nuvem, deve-se atentar para o disposto no item 4.2.

5.1.4. ETAPA 04: AQUISIÇÃO DOS DADOS

Essa etapa objetiva recuperar as informações contidas na imagem adquirida na etapa anterior. Nesse momento tem-se: a recuperação de arquivos, incluindo os apagados; a indexação de dados; e a recuperação de dados na nuvem, caso já tenha sido identificado o seu uso.

Primeiramente deve ser selecionada a ferramenta mais adequada para a aquisição dos dados. Dentre as ferramentas existentes e mais conhecidas tem-se: *Forensic Toolkit* (FTK), EnCase, UFED 4PC.

Para os dispositivos computacionais tradicionais, o investigador deverá estar atento às técnicas de bloqueio de escrita existentes para que eventuais modificações não ocorram. Em se tratando de dados oriundos da nuvem, deve-se efetuar contato com o provedor de serviços de modo a identificar a localização dos dados, a disposição das VM dentro do ambiente computacional e as tecnologias utilizadas. Após, deve ser identificado a quantidade de discos virtuais e *snapshots* existentes, os eventuais *backups* que por ventura tenham sido efetuados e se o CSP possui configurado serviços de investigação forense para coleta, aquisição e análise de dados. Caso não existam tais serviços configurados, o investigador deverá observar os quesitos previamente definidos e efetuar a cópia dos "arquivos do ambiente" de interesse, gerando seus respectivos *hashes*. Caso as cópias não sejam possíveis de serem efetuadas, a investigação deverá seguir com o método *Live Forensics*.

5.1.5. ETAPA 05: ANÁLISE DOS DADOS

Objetiva examinar os dados que possuam correlação com o evento e a identificação de novos dispositivos e/ou recursos de armazenamentos de interesse a serem analisados. Nesse momento poderão ocorrer novas iterações no processo.

O investigador deverá, então, selecionar as ferramentas mais adequadas para que os quesitos possam ser respondidos. Como exemplo, citam-se os softwares IPED *Digital Forensic Tool*, FTK, EnCase, CAINE, X-Ways *Forensics Winhex*, UFED *Physical Analyzer.*

5.1.6. ETAPA 06: FORMALIZAÇÃO

Objetiva fazer a apresentação legal das provas recolhidas, por meio do laudo pericial, e efetuar a entrega à autoridade competente. Vale ressaltar que todos os procedimentos, métodos, técnicas e ferramentas deverão estar descritos no laudo possibilitando, assim, sua reprodução e validação.

Neste capítulo foi apresentado uma proposta metodológica, juntamente com seu fluxo de execução, para auxiliar os investigadores na realização de exame pericial em dispositivos computacionais com acesso a nuvem, oriundo de um cenário onde não exista conhecimento prévio do ambiente a ser analisado.

5.2. VALIDAÇÃO DO CICLO DE VIDA

Com base no sucesso da aplicação do método em um caso real (singular), o método/modelo foi disponibilizado para aplicação em outros 7 casos, obtendo os resultados apresentados na tabela 6: Avaliação. Conforme apresentado, foram disponibilizados três tipos de resultados possíveis:

(1) Completo: o método auxiliou a realização do exame pericial;

(2) Em parte: o método auxiliou, em parte, a realização do exame pericial; e

(3) Não auxiliou: o método não auxiliou na realização do exame.

Tabela 6: Avaliação

Modelo de Serviço	Modelo de Desenvolvimento	Dispositivo Físico	Tipo de Servidor	Resultado
IaaS	Nuvem Privada	Desktop	Arquivos	Completo
IaaS e PaaS	Nuvem Privada	Desktop	Arquivos	Completo
IaaS e PaaS	Nuvem Privada	Notebook	Arquivos e Correio	Completo
IaaS e PaaS	Nuvem Privada	Desktop	Arquivos e Correio	Completo
IaaS e PaaS	Nuvem Privada	Notebook	Arquivos e Correio	Completo
IaaS e SaaS	Nuvem Pública	Smartphone	Arquivos e Correio	Não auxiliou
SaaS	Nuvem Pública	Smartphone	Arquivos e Correio	Em parte

Com base nos dados advindos da tabela 6, tem-se que 71% dos exames realizados chegaram integralmente aos mesmos resultados, enquanto que 29% tiveram de sofrer ajustes nas etapas e/ou não foram atendidos.

De acordo com os especialistas, o método proposto apoia/norteia o trabalho dos investigadores sob diversos aspectos. Primeiramente, eles concordaram que o método auxilia na condução da realização de um exame pericial, principalmente para os examinadores menos experientes. Segundo ponto comentado é que o método, principalmente para exames onde a tramitação do processo possui um maior lapso temporal, pode servir de base para identificar a etapa em que o exame pericial foi interrompido.

Os especialistas aprovaram a adição de mais uma etapa no ciclo de vida da forense e reagiram positivamente ao fluxo de execução da metodologia proposta,

pois constataram que ele favorece, principalmente, a execução/condução de um exame pericial quando se tem diversos dispositivos e investigadores atuando de modo concomitante.

Os especialistas também contribuíram com sugestões para aprimoramento do fluxo de execução. Foi sugerido a derivação de cada etapa do fluxo proposto, de modo a possibilitar que um investigador saiba a maneira exata (ferramenta e arquivo) de conduzir aquele determinado exame.

6. CONSIDERAÇÕES FINAIS

6.1 CONCLUSÃO

Este trabalho possibilitou, por intermédio de uma revisão rápida de literatura, solidificar os conhecimentos sobre computação em nuvem, virtualização e forense digital possibilitando, com isso, a realização de uma perícia, oriunda de um inquérito, em que existiam dispositivos computacionais com acesso a nuvem a serem analisados. Além disso, possibilitou, após a realização do exame pericial, a

proposição de uma metodologia a ser utilizada em ambientes que fizessem uso de recursos em nuvem.

A metodologia proposta é aplicável a dispositivos computacionais com acesso a serviços de nuvem provenientes do modelo de desenvolvimento privado. Diferentemente dos artigos analisados até então, que possuem relação com incidentes de redes, ou seja, possuem foco na elucidação de crimes/fatos utilizando a tecnologia como meio, este trabalho possui foco no uso da tecnologia como ferramenta de apoio, ou seja, estão relacionados com manipulação e geração de imagens, falsificação de assinaturas e documentos, obstrução de justiça e organização criminosa, corrupção ativa e passiva.

Foi observado, durante a pesquisa, que poucos estudos foram desenvolvidos com um viés prático e aplicável a situações em que a tecnologia era utilizada como meio. Além disso, as propostas possuíam um ambiente previamente configurado e controlado, ou seja, já existia uma mentalidade forense previamente estabelecida.

Pelos resultados da pesquisa e natureza do tipo de crime a ser elucidado conclui-se que a inserção de mais uma fase no ciclo de vida da forense digital faz-se necessária para que seja garantida a corretude processual e o investigador possa dirimir eventuais dúvidas referentes aos quesitos propostos pelo juízo.

No que concerne a legalidade do processo/aspectos jurídicos, a metodologia proposta permite cumprir todas as formalidades legais garantindo, assim, a irrefutabilidade do exame pericial.

Outra contribuição a ser mencionada é a identificação de possíveis pontos de coleta a serem utilizados nas investigações forenses, pois com a identificação dos arquivos de ambiente, bem como suas particularidades, constatou-se a possibilidade de análise por meio das ferramentas tradicionais.

6.2 LIMITAÇÕES

Como limitações principais tem-se a elevada quantidade de dados a serem submetidos ao exame e a obrigatoriedade da participação do CSP no processo, visto os investigadores não terem acesso ao ambiente operacional.

Outra limitação a ser considerada refere-se aos aspectos jurídicos da produção das provas, pois, devido à baixa quantidade de estudos relacionados ao tema com viés tecnológico e jurídico, os investigadores acabam tendo dificuldades na maneira de conduzir o exame forense na nuvem.

6.3 TRABALHOS FUTUROS

Este trabalho realizou um exame pericial em dispositivos computacionais com acesso a nuvem, oriundo de um caso real, e propôs uma metodologia de forense em nuvem aplicável em ambientes provenientes de uma nuvem privada. Como sugestões de trabalho futuros tem-se:

- a aplicação da metodologia em ambientes cujos dados de interesse estejam distribuídos em mais de uma instância, pois, por vezes, os dados poderão estar localizados em diferentes ambientes/plataformas, hardwares e localização geográfica;

- a configuração de um sistema forense, em um cenário onde não exista conhecimento prévio do ambiente a ser analisado, para coleta, aquisição de dados e análise de eventos parciais, após o recebimento da solicitação de exame pericial, de modo a possibilitar a análise antecipada de partes do ambiente e garantir que as informações sejam úteis dentro do prazo estabelecido pelo Juízo; e

- o desenvolvimento de uma ferramenta que possibilite a aquisição, análise e transferência de grandes volumes de dados, sem a necessidade de desligamento dos serviços, pois nem sempre a interrupção do serviço será possível devido os mais variados motivos, dentre os quais: prejuízos financeiros, natureza e relevância do serviço oferecido.

REFERÊNCIAS

[1] Sgarioni, M. Denúncias de pornografia infantil no Telegram dobram em um ano, aponta SaferNet, 2022. Disponível em: https://www.mobiletime.com.br/noticias/18/02/2022/denuncias-de-pornografia-infantil-no-telegram-dobraram-em-um-ano-aponta-safernet/. Acessado em: 16JAN2022.

[2] Eleutério, Pedro Monteiro da Silva, Desvendando a computação forense. São Paulo. Novatec Editora, 2010.

[3] Harbawi, M.; Varol, A. An improved digital evidence acquisition model for the Internet of Things forensic I: A theoretical framework. In: 2017 5th International Symposium on Digital Forensic and Security (ISDFS), 2017; pp. 1-6.

[4] Baggili, I.; Oduro, J.; Anthony, K.; Breitinger, F.; McGee, G. Watch What You Wear: Preliminary Forensic Analysis of Smart Watches. In: 2015 10th International Conference on Availability, Reliability and Security, 2015; pp. 303-311.

[5] Simou, S.; Kalloniatis, C.; Mouratidis, H.; Gritzalis, S. Towards the Development of a Cloud Forensics Methodology: A Conceptual Model. Lecture Notes in Business Information Processing 215; pp. 470-481.

[6] Al-Masri, E.; Bai, Y.; Li, J. A Fog-Based Digital Forensics Investigation Framework for IoT Systems. In: 2018 IEEE International Conference on Smart Cloud (SmartCloud), 2018; pp. 196-201.

[7] Overhead – Definição/nota de rodapé.... Camargo, R. O que é Overhead? Conheça a importância de controlar os custos indiretos. Disponível em: https://www.treasy.com.br/blog/overhead/. Acessado em: 16JAN2022.

[8] Ipsense. Internet das coisas e computação em nuvem: como se relacionam? Disponível em: https://www.ipsense.com.br/computacao-na-nuvem/internet-das-coisas-e-computacao-em-nuvem-como-se-relacionam/. Acessado em: 18JAN2022.

[9] Li, S.; Choo, K.; Sun, Q.; Bucharan, W.; Cao, J. IoT Forensics Amazon Echo as a Use Case. In: 2015 Journal of latex class files, vol. 14, no. 8, august 2015.

[10] Lovanshi, M.; Bansal, P. Comparative Study of Digital Forensic Tools. Data Engineering and Applications. Springer, 2019, pp. 195-204.

[11] Singh, S.; Kumar, S. Qualitative Assessment of Digital Forensic Tools. Asian Journal of Electrical Sciences, 2020, vol. 9 no. 1, pp. 25–32.

[12] C. Morin, “Methodology for Forensics Data Reconstruction on Mobile Devices with Android Operating System Applying In-System Programming and Combination Firmware”, Master’s Thesis, University of Brasilia, 2020.

[13] Povar, D; Geethakumari, G. Digital Forensic Architecture for Cloud Computing Systems: Methods of Evidence Identification, Segregation, Collection and Partial

Analysis. Information Systems Design and Intelligent Applications, 2016; pp. 213-225.

[14] Purnaye, P.; Kulkarni, V. BiSHM: Evidence detection and preservation model for cloud forensics. Open Computer Science, vol. 12, no. 1, 2022; pp. 154-170.

[15] Raju, B.; Geethakumari, G. SNAPS: Towards building snapshot based provenance system for virtual machines in the cloud environment. Computers & Security. In: computers & security 86 (2019); pp. 92–111.

[16] Yankson, B.; Davis, A. Analysis of the Current State of Cloud Forensics: The Evolving Nature of Digital Forensics. In: 16th International Conference on Computer Systems and Applications (AICCSA), 2019, pp. 1-8.

[17] Aydin, M.; Jacob, J. A comparison of major issues for the development of forensics in cloud computing. In: The 8th International Conference for Internet Technology and Secured Transactions (ICITST-2013). London, UK, 2013, pp. 77-82.

[18] Eleyan, A.; Eleyan, D. Forensic Process as a Service (FPaaS) for Cloud Computing. In: 2015 European Intelligence and Security Informatics Conference. Manchester, UK, 2015, pp. 157-160.

[19] Alkhanafseh, M.; Qatawneh, M.; Almobaideen, W. A Survey of Various Frameworks and Solutions in all Branches of Digital Forensics with a Focus on Cloud Forensics. In: International Journal of Advanced Computer Science and Applications, 2019.

[20] Gómez, J.; Mondéjar, J.; Gómez, J.; Martínez, J. A context-centered methodology for IoT forensic investigations. In: International Journal of Information Security, 2021. 20; pp. 1-27.

[21] Alqahtany, S.; Clarke, N.; Furnell, S.; Reich, C. A forensic acquisition and analysis system for IaaS: Architectural Model and Experiment. In: 2016 11th International Conference on Availability, Reliability and Security; pp. 1–15.

[22] NIST 2011. The NIST Definition of Cloud Computing. National Institute of Standards and Technology, 2011.

[23] Martini, B.; Choo, K. An integrated conceptual digital forensic framework for cloud computing. Digital Investigation, Volume 9, Issue 2, 2012, pp. 71-80.

[24] AWS. O que é virtualização. Disponível em: https://aws.amazon.com/pt/what-is/virtualization/. Acessado em: 18JAN2022.

[25] Azure. O que é virtualização? Disponível em: https://azure.microsoft.com/pt-br/resources/cloud-computing-dictionary/what-is-virtualization. Acessado em: 18JAN2022.

[26] Red Hat. O que é armazenamento NAS? Disponível em: https://www.redhat.com/pt-br/topics/data-storage/network-attached-storage. Acessado em: 05FEV2023.

[27] VMware. SAN. Disponível em: https://www.vmware.com/br/topics/glossary/content/storage-area-network-san.html. Acessado em: 05FEV2023.

[28] Bravo Tecnologia. Nutanix e VMware lutam pela liderança. Disponível em: https://bravotecnologia.com.br/nutanix-e-vmware-lutam-pela-lideranca/. Acessado em: 10JAN2023.

[29] Mordor Intelligence. Disponível em: https://www.mordorintelligence.com/pt/industry-reports/virtualization-software-market. Acessado em: 10JAN2023.

[30] VMware. Produtos VMware. Disponível em: https://www.vmware.com/br/products.html. Acessado em: 10JAN2023.

[31] VMware. Arquivos de máquina virtual. Disponível em: https://docs.vmware.com/br/VMware-vSphere/7.0/com.vmware.vsphere.vm_admin.doc/GUID-CEFF6D89-8C19-4143-8C26-4B6D6734D2CB.html. Acessado em: 07NOV2022.

[32] Wilkinson, S.; Haagman, D. Good practice guide for computer-based electronic evidence. Disponível em: https://www.7safe.com/docs/default-source/default-document-library/acpo_guidelines_computer_evidence_v4_web.pdf. Acessado em: 10SET2022.

[33] [33] Ayers, R.; Brothers, S.; Jansen, W. Guidelines on mobile device forensics. National Institute of Standards and Technology, 2014. Disponível em: https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-101r1.pdf. Acessado em: 10OUT2022.

[34] McKemmish R. What is forensic computing? Trends & Issues in Crime and Criminal Justice 1999; 118:1–6.

[35] Kent K, Chevalier S, Grance T, Dang H. Guide to integrating forensic techniques into incident response. SP800–86. Gaithersburg: U.S. Department of Commerce; 2006.

[36] Ajijola, A.; Zavarsky, P.; Ruhl, R. A review and comparative evaluation of forensics guidelines of NIST SP 800-101 rev.1:2014 and ISO/IEC 27037:2012. In: IEEE. World Congress on Internet Security (WorldCIS-2014), pp. 66–73.

[37] Standardization, I. O. ISO/IEC 27037:2012: Information technology -Security techniques — Guidelines for identification, collection, acquisition and preservation of digital evidence. ISO/IEC, 2012. Disponível em: https://www.iso.org/standard/44381.html. Acessado em: 10OUT2022.

[38] Kyei, K.; Zavarsky, P.; Lindskog, D.; Ruhl, R. A Review and Comparative Study of Digital Forensic Investigation Models. In: ICDF2C 2012: Digital Forensics and Cyber Crime; Vol 114, pp. 314-327.

[39] Messler, R. Reverse Engineering: Mechanisms, Structures, Systems & Materials. McGraw-Hill Education, 2014.

[40] Kruse, I., Warren, G., Heiser, J. Computer Forensics: Incident Response Essentials. Pearson Education, Boston (2001).

[41] Tricco, A.C., Antony, J., Zarin, W., Strifler, L., Ghassemi, M., Ivory, J., Perrier, L., Hutton, B., Moher, D., Straus, S.E. A scoping review of rapid review methods. BMC Med 13, 224 (2015).

[42] Red Hat. Plataformas Linux: Red Hat OpenStack Platform. Disponível em: https://www.redhat.com/pt-br/technologies/linux-platforms/openstack-platform. Acessado em: 05FEV2023.

[43] Brown, A.; Glisson, W.; Andel, T.; Choo, K. Cloud forecasting: Legal visibility issues in saturated environments. Computer Law & Security Review, Vol 34, Issue 6, 2018, pp. 1278-1290.

[44] Thethi, N.; Keane, A. Digital forensics investigations in the Cloud. In: *2014 IEEE International Advance Computing Conference (IACC)*, Gurgaon, India, 2014, pp. 1475-1480.

[45] Raju, BKSP.; G. M.; Geethakumari, G. Cloud forensic investigation: A sneak-peek into acquisition. In: 2015 International Conference on Computing and Network Communications (CoCoNet), Trivandrum, India, 2015, pp. 348-352.

[46] GSTI. Forense ao vivo (Live Forensics). Disponível em: https://www.portalgsti.com.br/2018/11/forense-ao-vivo-live-forensics.html. Acessado em: 05FEV2023.