ForensicWork: Desenvolvimento de um *Framework* para Perícia Forense em Computação na Nuvem

Cátia Oliveira de Jesus, Mailson Sousa Couto

Instituto Federal de Educação, Ciência e Tecnologia da Bahia (IFBA)
Av. Amazonas, 3150 - Zabelê, Vitória da Conquista - BA, 45030-220 – Brasil

catia.infor@gmail.com, mailsoncouto@ifba.edu.br

Abstract. *When a crime is practiced through cloud service platforms, the police investigation finds serious obstacles that could compromise the elucidation of the case and even the culpability of the culprits, given the difficulty in locating the evidence of the crime, which may have been committed in different countries, and disseminated on several servers. Given this type of situation, which is increasingly present in modern and computerized society, this article proposes to develop a conceptual framework that allows the exploration of data stored in cloud services in a timely manner, respecting the legislation of the different jurisdictions involved and the chain of custody, so as to systematize the investigative process in the virtual environment.*

Resumo. *Quando um delito é praticado por intermédio de plataformas de serviços em nuvem, a investigação policial encontra sérios entraves que podem comprometer a elucidação do caso e inclusive responsabilização dos culpados, dada a dificuldade em se localizar as provas do ilícito, que pode ter sido cometido em diferentes países, e disseminado em diversos servidores. Tendo em conta esse tipo de situação, cada vez mais presente na sociedade moderna e informatizada, esse artigo se propõe a desenvolver um framework conceitual que possibilite a exploração de dados armazenados em serviços em nuvem em tempo hábil, respeitando a legislação das diferentes jurisdições envolvidas e a cadeia de custódia, de modo a sistematizar o processo investigatório no ambiente virtual.*

1. Introdução

A evolução da tecnologia e o crescimento exponencial do número de pessoas e dispositivos conectados à Internet em todo o mundo, têm tornado a *web* um ambiente altamente propício para a execução de práticas criminosas. Neste cenário, surgiu a Perícia Forense Computacional. Segundo [Sá 2011], a palavra Perícia é proveniente do latim *Peritia*, cujo significado é conhecimento ou experiência, podendo também ser definida como um instrumento especial de constatação, prova ou demonstração científica da veracidade de situações, coisas ou fatos [Alberto 2012]. Assim, a perícia forense computacional pode ser entendida como o processo de identificar, preservar, analisar e apresentar provas digitais relativas a um determinado delito de forma legal e aceitável perante um tribunal de justiça.

Um processo de investigação criminal deve considerar a utilização de métodos e protocolos bem definidos, visando à análise eficaz e ampla aceitação na esfera jurídica. Em uma investigação forense, as provas digitais podem ser extraídas de diferentes fontes, como discos rígidos, memórias, sistemas operacionais, dispositivos móveis e no ambiente de rede.

Todas as modalidades de perícia citadas no parágrafo anterior já possuem metodologias de coleta, extração e análise bem definidas, que são formalmente aceitáveis nos tribunais e amplamente difundidas entre os profissionais técnicos que realizam tais procedimentos, ao contrário da perícia em nuvem. Sob esta perspectiva, este trabalho desenvolve um estudo para apresentar os desafios, e os avanços da investigação forense no âmbito da computação em nuvem, esboçando um panorama geral do andamento das investigações criminais nesta esfera e apresentando um modelo conceitual de *framework* que permita sistematizar tal processo.

2. Revisão Teórica

A computação em nuvem surgiu da ideia de se utilizar, em qualquer lugar e independentemente de plataforma, diversas aplicações armazenadas na Internet, sem a necessidade de instalação prévia no dispositivo em que se deseja utilizar tal produto. De acordo com [Hurwitz et al. 2010], a nuvem pode ser entendida como um agrupamento de módulos processadores que oferecem serviços e conexões, permitindo assim a entrega da computação como um serviço. Aplicações em nuvem incluem a oferta de *software*, infraestrutura e armazenamento, tudo isso através da Internet, seja com componentes separados, seja uma plataforma completa, com base na demanda do usuário.

2.1. Computação Forense na Nuvem

A computação forense é definida por [Galvão 2009] como a ciência que trata de todos os processos de investigação forense e análise de incidentes que ocorreram por meio de dispositivos computacionais, contribuindo assim com a identificação e comprovação da autoria de tais delitos. De acordo com [Reis et al 2004] a computação forense visa realizar uma investigação com o maior nível de transparência possível, sendo então necessário que o profissional responsável pela perícia seja muito cuidadoso com todas as possíveis evidências, para que estas possam se tornar provas confiáveis perante a justiça.

Antes, a maioria das atividades de computação era realizada de forma local, na própria máquina, porém, é notável a tendência de migração destas atividades para a nuvem, sejam elas lícitas ou ilícitas. Com o fenômeno da virtualização, a forense computacional teve de se adaptar às peculiaridades destes ambientes virtualizados, quando um perito tem o desafio de realizar a análise forense em alguma plataforma da nuvem, ele esbarra em diversas questões técnicas e jurídicas, que em muitas vezes inviabilizam até o serviço.

Além das questões técnicas desta tecnologia, como criptografia, formatos de dados desconhecidos e descentralização do armazenamento, é preciso lidar com as questões jurídicas de cada país. [Reilly 2010] questiona a falta de ferramentas específicas para auxiliar os especialistas com investigações na nuvem, e afirma que esta

escassez de instrumentos acaba inviabilizando muitas perícias. Para [Gellman 2009], por se tratar de uma tecnologia distribuída geograficamente entre diferentes nações, é preciso que os peritos atuem de forma cordial com a justiça, selando acordos nacionais e internacionais, para que se respeitem tanto as jurisdições de cada Estado, quanto às questões de privacidade dos usuários. Neste contexto, [Reilly 2010] chama a atenção para a falta de material que indique como devem ser executados os processos de investigação nos ambientes em nuvem, e conclui sinalizando a necessidade de desenvolvimento de novas metodologias ou aperfeiçoamento das existentes.

3. Trabalhos Relacionados

Diante de toda a relevância que o tema em questão representa, outros *frameworks* em computação em nuvem já foram propostos por pesquisadores e, assim, contribuíram bastante com o desenvolvimento deste projeto. A seguir será apresentado um resumo de alguns destes trabalhos.

[Karie et. al. 2013] abordam as principais dificuldades encontradas no processo da investigação forense na nuvem, devido a sua infraestrutura complexa. Neste sentido, eles propuseram um quadro conceitual que apresenta os diferentes componentes essenciais da computação compartilhada, como os serviços e os provedores. Os autores afirmam que o quadro proposto expõe de forma clara os processos envolvidos e a estrutura da nuvem, reduzindo assim a complexidade do entendimento de tal tecnologia, e isso ajuda os pesquisadores a compreender os procedimentos e técnicas que precisam ser adotados em uma investigação, bem como auxilia a concepção de novas ferramentas para automatizar ou melhorar uma perícia nesse tipo de ambiente.

[Sibiya et al. 2012] desenvolveram um *framework* denominado *Live Digital Forensic Framework for a Cloud* (LDF2C), projetado para resolver o problema da associação dos dados armazenados na nuvem ao usuário que de fato é o proprietário, além de indicar mecanismos que podem ser utilizados para a coleta de evidências em aplicações virtualizadas. O LDF2C é implementado em um servidor virtual e possui um algoritmo utilizado para descobrir arquivos de *log* de locais considerados relevantes, como a área de trabalho remota hospedada ou o dispositivo cliente acessado. Quando acionado, ele executa a análise forense entre duas organizações virtuais e monitora a interação.

Outro trabalho relevante é o de [Mohan 2016], que a abordou os problemas que ocorrem em investigações cujos dados são dinâmicos e distribuídos em diversos servidores espalhados pelo mundo. O autor sugere um modelo baseado em *logs* para ajudar a reduzir a complexidade da perícia, permitindo coletar rapidamente informações na nuvem através dos registros de *logs*.

4. ForensicWork

Para [Wangler e Paheerathan 2000], os *frameworks* podem ser classificados em duas categorias básicas: vertical e horizontal. Os verticais são aqueles cuja atuação envolve a resolução de problemas de escopo bem definido e especificado. Já os horizontais são mais genéricos e possuem uma atuação ampla, não existindo um domínio específico. Sendo assim, o *framework* conceitual proposto neste artigo pode ser classificado como

vertical, pois o objetivo é ser aplicado exclusivamente no âmbito de investigações forenses em nuvem.

A Figura 1 ilustra a modelagem inicial do *framework* que, por enquanto, é composto por seis etapas básicas, sendo estas:

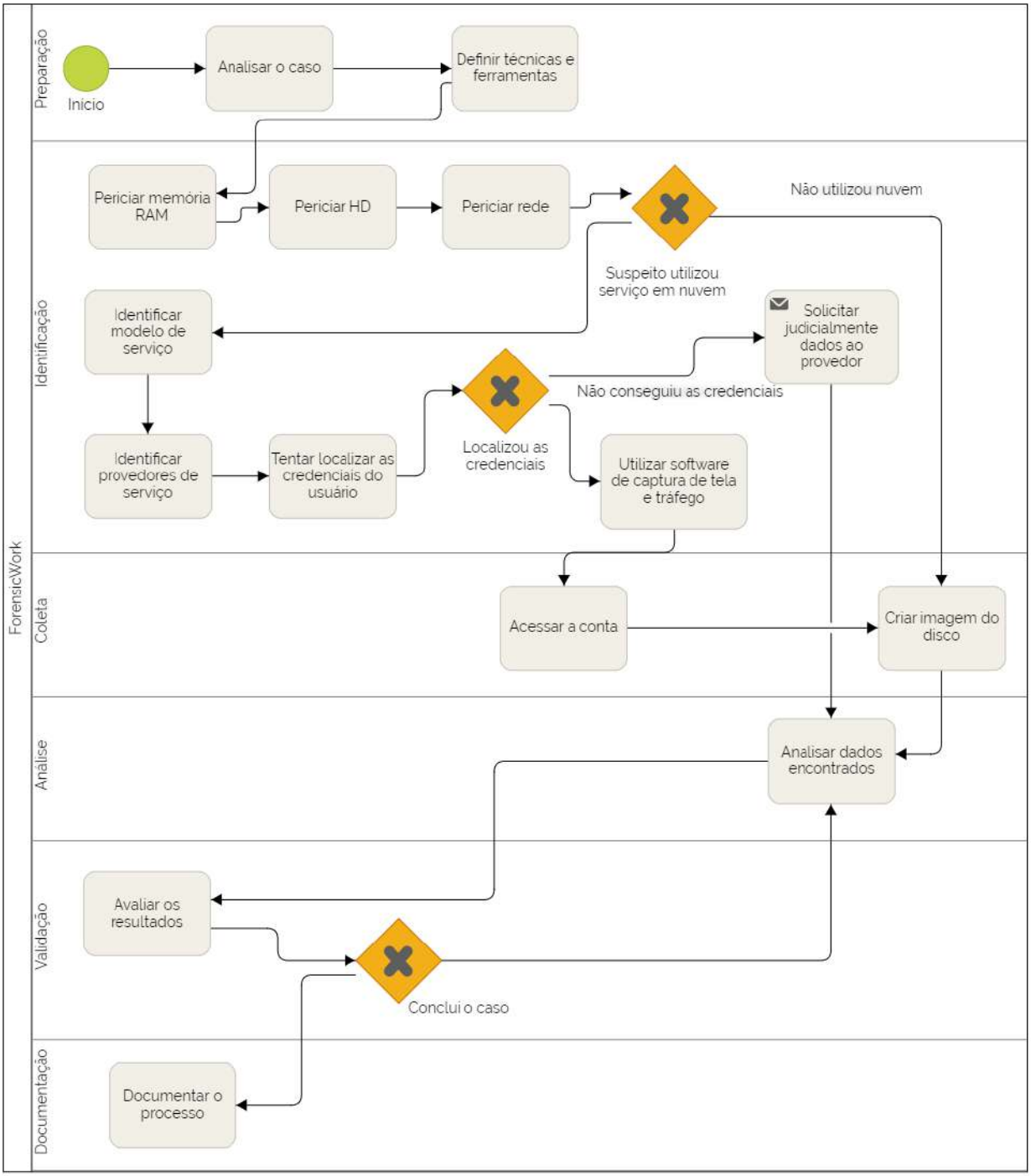

Figura 1. Fluxo de atividades do *framework* proposto.

- Preparação: é feita uma análise do caso para determinar quais tipos de dispositivos serão periciados e quais as ferramentas e *softwares* que poderão ser utilizados;

- Identificação: são realizadas as perícias convencionais na memória RAM e no armazenamento local do dispositivo, bem como na rede, em busca de dados que indiquem a utilização de algum serviço virtualizado ou dados importantes para a investigação. Caso haja indícios do uso de algum serviço em nuvem, tenta-se definir qual foi o modelo de serviço, qual o provedor, e possíveis credencias de acesso. De posse das credenciais, deve-se utilizar *softwares* para captura de tela e análise de tráfego da rede. Caso não se consiga o acesso a conta, uma solicitação judicial deve ser emitida ao provedor em questão.
- Coleta: caso a conta do suspeito tenha sido acessada, os dados devem ser baixados para perícia, e devem ser realizadas imagens do disco do dispositivo para posterior análise.
- Análise: algumas análises deverão ser realizadas em cima dos dados coletados.
- Validação: caso os dados encontrados sejam suficientes para concluir o processo, passa-se para a próxima etapa.
- Documentação: é feita a documentação com base na cadeia de custódia.

5. Conclusões e Trabalhos Futuros

O armazenamento de dados em nuvem tem representado um grande desafio para os profissionais da computação forense. A computação em nuvem oferece diferentes tipos de serviços e cada um deles possibilita a prática de atividades criminosas. No processo de investigação, as principais dificuldades enfrentadas pelos peritos estão nas fases de identificação e levantamento das provas.

Após ser determinado que uma conta de armazenamento em nuvem possui provas relevantes para um inquérito, o examinador deve comunicar judicialmente aos prestadores de serviços envolvidos para que a conta daquele usuário seja periciada e que seus dados não possam ser alterados. Além disso, outros dados podem ser obtidos através da aquisição dos arquivos de *log* do *software* cliente, arquivos de captura de tráfego de rede e captura dos dados disponíveis na memória do dispositivo.

Ainda em fase inicial, esta pesquisa visa contribuir com a melhora da compreensão do processo investigatório de crimes cometidos na nuvem, bem como oferecer aos peritos um *framework* para sistematizar o processo investigatório neste ambiente. Nas próximas etapas deste trabalho, pretende-se detalhar mais o escopo do *framework*, deixando os processos mais bem definidos, além da inclusão da fase de testes, definindo-se as ferramentas e *softwares* específicos para a validação do mesmo.

Referências

Alberto, Valder Luiz Palombo. (2012). Perícia Contábil. São Paulo: Editora Atlas, 5.

Galvão, Ricardo Kléber (2009). Perícia Forense Computacional SegInfo 2009 :: IV Workshop de Segurança da Informação. http://grsecurity.com.br/apostilas/forense/seginfo2009_2_rk.pdf

Gellman, R. (2009). Privacy in the Clouds: Risks to Privacy and Confidentiality from Cloud Computing. World Privacy Forum. http://www.worldprivacyforum.org/pdf/WPF_Cloud_Privacy_Report.pdf

Hurwitz, Judith; bloor, Robin; Kaufman, Marcia. (2010). Cloud Computing For Dummies. HPSpecial Edition. Indianapolis: Wiley Publishing.

Mohan, Aswathy. (2016), A Log-Based Approach to Make Digital Forensic Easier on Cloud Computing. International Research Journal of Latest Trends in Engineering and Technology (IRJLTET).

N.M. Karie and H.S. Venter, "An Ontological Framework for a Cloud Forensic Environment," in the Proceedings of the European.

Reilly, D.; Wren, C.; Berry, T. (2010). Cloud Computing: Forensic Challenges for Law Enforcement. International Conference for Internet Technology and Secured Transactions (ICITST). p. 1-7.

Reis, Marcelo Abdalla dos, Geus, Paulo Lácio de. (2004) Análise Forense de Intrusões em Sistemas Computacionais: Técnicas, Procedimentos e Ferramentas. Instituto de Computação - Universidade Estadual de Campinas.

Sá, Antonio Lopes de.(2011) Perícia Contábil. São Paulo: Editora Atlas, 10. Ed.

Sibiya, G., Venter, H. S., & Fogwill, T. (2012). Digital forensic framework for a cloud environment. IIMC International Information Management Corporation.

Wangler, B. and S.J. Paheerathan (2000), Horizontal and Vertical Integration of Organizational IT Systems, in Information Systems Engineering: State of the Art and Research Themes, (S. Brinkkemper, E. Lindencrona and A. Solvberg (eds.)), Springer.