Computação Forense em Redes Definidas por Software (SDN): Uma revisão de literatura

Bruno Anselmo Guilhen[1], Regina Melo Silveira[2], Sergio Takeo Kofuji[1]

[1]Departamento de Eng. de Sistemas Eletrônicos – Universidade de São Paulo (USP)
Av. Luciano Gualberto, 158. CEP: 05508-010 – São Paulo – SP – Brasil

[2]Departamento de Engenharia de Computação – Universidade de São Paulo (USP)
Av. Luciano Gualberto, 158. CEP: 05508-010 – São Paulo – SP – Brasil

{brunoguilhen,kofuji}@usp.br, regina@larc.usp.br

Abstract. *Software Defined Networks (SDN) represent the state of the art in network structures that are being adopted by many companies and service providers. Along with this new challenge of deploying and operating software-based networks, there is a need to ensure security in all aspects of the network. In this context, the topic of computer forensics in SDN networks arises, which aims to establish mechanisms to carry out the correct survey and ascertain data on security incidents. Therefore, the article contributes with a literature review by carrying out a survey of the main forensic techniques that have been applied in SDN networks compared to traditional forensic techniques as they relate and complement each other.*

Resumo. *As redes definidas por software (SDN) representam o estado da arte em estruturas de redes que estão sendo adotadas por diversas empresas e provedores de serviços. Junto deste novo desafio de implantar e operar redes baseadas em software, existe a necessidade de garantir a segurança em todos os aspectos da rede. Neste contexto, surge a temática da computação forense em redes SDN, que visa estabelecer os mecanismos para fazer o levantamento correto e apurar os dados sobre os incidentes de segurança. Portanto, o artigo contribui com uma revisão de literatura ao realizar um levantamento das principais técnicas forenses que foram aplicadas em redes SDN comparando com as técnicas forenses tradicionais como elas se relacionam e se completam.*

1. Introdução

A Internet sofreu grandes mutações ultimamente, novas tecnologias, tais como, serviços em nuvem, Internet das Coisas, BigData, Blockchain, fizeram com que diversos produtos e operações migrassem de ambientes locais para remotos e aumentassem consideravelmente a necessidade de processamento das redes atuais (Chica, Imbachi, & Veja, 2020).

Além de sobrecarregar a infraestrutura de roteadores da Internet, os novos serviços possuem requisitos mais elevados de flexibilidade, confiabilidade e escalabilidade exigindo um novo paradigma de encaminhamento de pacotes na rede, bem como, novos elementos de segurança (Kreutz, et al., 2015). Por isso, diversas instituições acadêmicas e a indústria se debruçaram para estudar uma solução para a Internet do futuro, uma nova arquitetura de rede conhecida como "Redes Definidas por Software (SDN)" (Oktian, Lee, Lee, & Lam, 2017).

O estudo feito por (Chica, Imbachi, & Veja, 2020) e (Kreutz, et al., 2015) coloca SDN na vanguarda das arquiteturas de rede para o gerenciamento e inovação em redes de comunicação. Uma característica fundamental da arquitetura SDN é a separação física do plano de controle do plano de "encaminhamento" de dados, substituindo o plano de controle fechado tradicional por um plano de controle de software aberto (Allouzi, 2018). Além disso, tem-se a função de controle logicamente centralizada permitindo os recursos de programação da rede (Oktian, Lee, Lee, & Lam, 2017). A Figura 1 ilustra a arquitetura SDN.

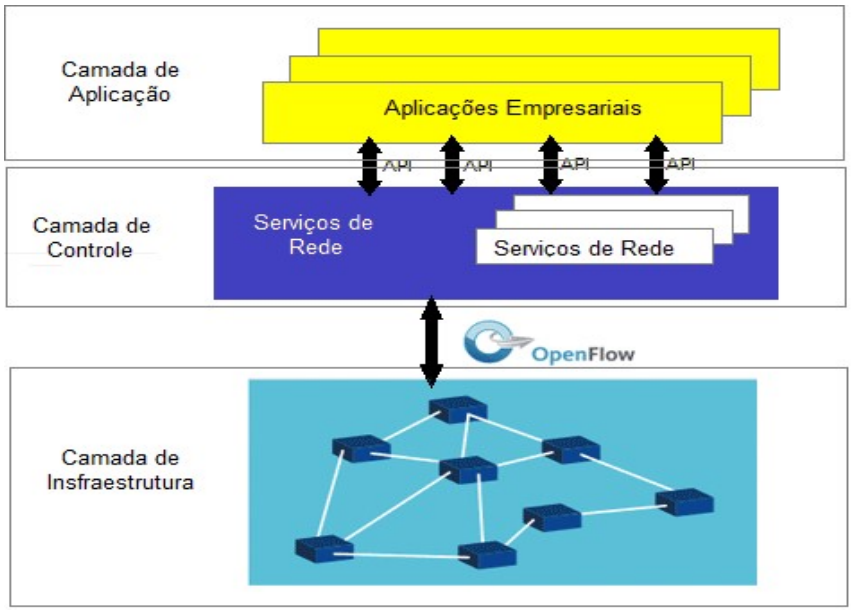

Figura 1. Arquitetura de Redes SDN. (Long, 2021)

A rápida evolução das redes SDN, a sua implantação em diversos tipos de ambientes, tais como, Datacenters, ISPs, nuvem, entre outros, trouxe a preocupação com os requisitos de segurança, estudo necessário para encerrar importante lacuna que permite maior quantidade de empresas utilizando essa tecnologia (Chica, Imbachi, & Veja, 2020).

Explorando a segurança em redes SDN verifica-se que uma preocupação recorrente são as vulnerabilidades de softwares (Kreutz, Ramos, & Verissimo, 2013). Principalmente quando se observa a centralização do plano de controle, item da SDN que pode representar um ponto de falha (Abdullaziz, Wang, & Chen, 2019). A segurança precisa ser avaliada como um serviço que protege os recursos da rede contra acessos e ataques não autorizados. Isso ocorre porque, embora o controle de acesso de usuários tenha sido incluída no Ethane (Casado, McKeown, & Shenker, 2019), outros parâmetros de segurança precisam ser melhor analisados e abordados ao projetar uma arquitetura SDN (Han, et al., 2019).

Do ponto de vista de camadas, nota-se que a segurança da camada de transporte (TLS) é opcional no protocolo OpenFlow. O TLS possui requisitos complexos de configuração, por esta razão nem sempre é adotado por alguns switches e controladores habilitados para OpenFlow (Abdullaziz, Wang, & Chen, 2019). A consequência será a falta de verificação de alguns dispositivos de encaminhamento, neste caso, brechas de segurança surgem, bem como, ataques de negação de serviços (DoS) podem ser estruturados nos controladores SDN (Allouzi, 2018).

Outros tipos de ataques podem ser associados ao SDN, tais como, no controlador, em switches OpenFlow, hosts e interfaces de comunicação (Han, et al., 2019). Conforme reportado por (Abdullaziz, Wang, & Chen, 2019) e (Han, et al., 2019) um controlador comprometido permite o envio de instruções falsas ou maliciosas, através da modificação de regras de fluxo, para switches OpenFlow. Assim, a consequência natural do desvio de tráfego é a alteração no desempenho da rede, o vazamento de informações e a perda de pacotes (Han, et al., 2019).

Diante da proeminente ascensão das redes SDN e dos problemas de segurança apresentados destaca-se como objetivo da pesquisa analisar quais dados podem ser coletados e analisados diante de um problema de segurança, ou seja, o papel de coleta, análise e apresentação de respostas a incidentes fica a cargo de uma área conhecida como ciência forense. Neste caso, o artigo contribui com uma revisão de literatura para levantar e analisar os principais caminhos para a perícia em redes SDN e faz uma comparação com o processo de perícia tradicional.

O artigo está organizado da seguinte forma: a seção 2 apresenta a fundamentação teórica para os temas abordados. Na seção 3 o levantamento de projetos em SDN forense e na 4 apresenta-se as conclusões da nossa contribuição para a pesquisa.

2. Fundamentação Teórica

Neste tópico serão transcritas as principais definições sobre segurança em redes controladas por software, a computação forense tradicional e a forense em SDN.

2.1. Segurança em SDN

Diversos são os estudos relativos ao campo de segurança em redes SDN. Alguns sobre os mecanismos de autenticação (Tang, Liu, He, Yu, & Qin, 2019), outros lidam com pontos de falha (Aydeger, Saputro, & Akkaya, 2019), ataques de negação de serviços (Abdullaziz, Wang, & Chen, 2019). A pesquisa dos diversos pontos críticos da segurança em redes SDN contribui para entender como a computação forense pode buscar evidências e elucidar, da melhor maneira possível, os incidentes de segurança (Duy, et al., 2019).

De acordo com as ideias propostas por (Abdullaziz, Wang, & Chen, 2019) a percepção de segurança em SDN tem dois aspectos, um deles refere-se a segurança por meio de SDN, o outro na segurança do SDN. Por um lado, a segurança por meio de SDN se concentra na utilização de recursos SDN para resolver problemas de segurança de rede tradicionais. O outro ponto discutido sobre segurança SDN, são os desafios de se ter um ponto único de falha, alguns pesquisadores (Allouzi, 2018) e (Aydeger, Saputro, & Akkaya, 2019) tratam o controle centralizado como um risco, em outros trabalhos (Oktian, Lee, Lee, & Lam, 2017) e (Aydeger, Saputro, & Akkaya, 2019) são vistos como vantagem, visto que, a centralização permite o controle mais rígido das regras de segurança.

A pesquisa proposta por (Tang, Liu, He, Yu, & Qin, 2019) evidencia os problemas de segurança causados pela comunicação entre dispositivos e o custo causado pela introdução de esquemas de segurança. Na proposta, o autor lista um esquema de autenticação bidirecional de identidade leve (LTWA), que cria uma barreira impedindo que um invasor falsifique ou adultere mensagens de interação de autenticação, estabelecendo, assim, uma conexão confiável ponta a ponta na rede de acesso.

Em (Han, et al., 2019) o autor fornece uma análise sobre várias questões de segurança, principalmente as contramedidas que devem ser tomadas para mitigar alguns ataques, tais como, Denial of Servie (DoS), DoS distribuído (DDoS), ataques de Spoofing e injeção maliciosa. Ao analisar os ataques, a pesquisa oferece uma visão de como detectar, mitigar e investigar os pontos fortes e fracos de um controlador SDN.

2.2. Computação Forense Tradicional

Quando um incidente de segurança ocorre em um sistema computacional, a computação forense entra em ação para garantir todo o processo de investigação desse fato (CSA, 2013). O objetivo da forense digital (ou computação forense) é realizar uma investigação estruturada em ocorrências passadas e em curso de processamento e transmissão de dados, mantendo uma cadeia de evidências documentadas, que pode ser reproduzida de forma inequívoca e validada por terceiros competentes (Brezinski & Killalea, 2002). Essa cadeia de evidências recebe o nome de cadeia de custódia. Cada etapa da cadeia de custódia precisa de garantias (princípio da Confidencialidade, Integridade e Autenticidade) para que todas as provas obtidas possam ser validadas em um processo judicial (Farmer & Venema, 2016).

De acordo com a IETF RFC3227, a investigação digital deve ser estruturada em cinco etapas principais: coleta, extração, análise, informação e documentação (Brezinski & Killalea, 2002).

Já em (CSA, 2013) a base comum para a prática da forense tradicional segue os seguintes princípios: identificação, coleta, aquisição e preservação.

Ao juntar as práticas forenses apresentadas em (CSA, 2013) e (Farmer & Venema, 2016) obtém-se uma sequência de aquisição ainda mais detalhada apresentada na Figura 2 a seguir.

Figura 2. Prática Forense Tradicional (CSA, 2013), (Brezinski & Killalea, 2002).

Portanto, de acordo com a Figura 2 pode-se definir os elementos da prática forense tradicional com os seguintes termos:

- Identificação: processo inicial da ciência forense que visa separar os arquivos que serão utilizados como prova.
- Coleta e aquisição: ação que visa extrair e copiar os arquivos identificados.
- Preservação: técnica para garantir que tudo o que foi coletado poderá ser analisado com garantias de integridade.
- Análise: técnica que busca solucionar o problema levantado do ponto de vista pericial, indicando e respondendo, quando possível, as indagações: quem, como e quando as ações foram realizadas.
- Documentação: processo final da prática forense que transforma em laudo (documento) tudo o que foi analisado.

O método forense apresentado até aqui é conhecido como tradicional, ou seja, aquele realizado em máquina local, onde os dados são extraídos da memória volátil (memória RAM) ou não volátil (discos magnéticos, ópticos ou de estado sólido). O

desafio agora é estabelecer os mesmos parâmetros para dados armazenados em redes SDN.

2.3. Computação Forense em SDN

Ao realizar uma comparação entre a análise forense em redes tradicionais e em redes SDN a pesquisa proposta por (Khan, et al., 2016) mostra que o plano de dados e de controle do SDN, por possuírem desacoplamento, permite que a captura e análise de dados seja realizada mais facilmente no SDN do que numa rede tradicional, visto que, na rede tradicional será preciso recuperar evidências dos pacotes transmitidos da origem ao destino e no SDN isso pode ser realizado em cada ponto do desacoplamento.

Seguindo o método forense apresentado na Figura 2 para aquisição de dados (CSA, 2013), o trabalho proposto por (Khan, et al., 2016) mostra uma estrutura similar, porém, aplicada em redes controladas por software. A Figura 3, mostra o esquema de análise forense em SDN.

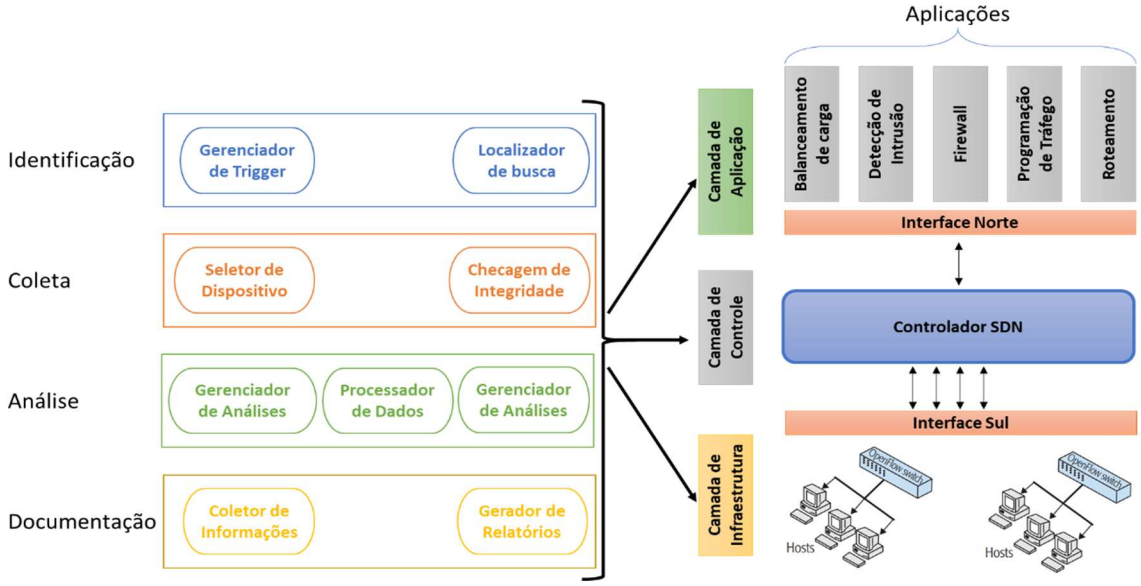

Figura 3. Modelo geral para forense SDN. Adaptado de (Khan, et al., 2016).

Na camada de infraestrutura, onde estão os Switches OpenFlow, visto na Figura 1, as tabelas de fluxo podem indicar o próximo salto do pacote, suas ações serão pautadas conforme especificado pelo controlador. Neste caso, os switches OpenFlow conseguem identificar o próximo salto do pacote, permitindo uma coleta mais precisa de evidências (Khan, et al., 2016). Em redes tradicionais não é tão simples e rápido alterar o destino de um pacote ou mesmo desviar tráfegos maliciosos para um servidor que fará a coleta dos dados, esta vantagem caracteriza às redes controladas por software (Brockelsby & Dutta, 2019).

Quando se compara a análise de logs, nas redes tradicionais esses dados são coletados em diversos dispositivos da rede, por exemplo, firewalls, roteadores, sistemas de detecção de intrusão e outros sistemas da rede que armazenam essas informações. No SDN o controlador é logicamente centralizado permitindo o rastreamento de cada host e o monitoramento de fluxo da rede, informações necessárias para determinar a causa raiz do ataque (Duy, et al., 2019) (Achleitner, Porta, Jaeger, & McDaniel, 2017).

A análise da estrutura da rede e a análise de logs fazem na ciência forense um processo meticuloso e delicado, em redes controladas por software também se aplica o processo descrito na Figura 2, na fase de identificação será possível conceber um recurso de monitoramento de evidências em tempo real sendo vital para a estrutura forense. Esta estrutura pode indicar os locais para coleta de evidências dispostos em três camadas da arquitetura SDN: camada de aplicação, camada de controle e camada de infraestrutura (Duy, et al., 2019). Alguns desafios foram detectados por (Achleitner, Porta, Jaeger, & McDaniel, 2017) e (Pourvahab & Ekbatanifard, 2019) ao analisar os dados das camadas, por exemplo, dados de log confiáveis, desempenho, identificação de fonte e sincronização de evidências entre controladores. Esses desafios ainda precisam de maiores estudos e investigação, seja por administradores de segurança ou pesquisadores que precisam estabelecer determinados padrões de análise forense SDN, arquiteturas e frameworks (Duy, et al., 2019) (Pourvahab & Ekbatanifard, 2019).

Como o mecanismo central da análise forense é a coleta de dados para validação, análise e documentação, torna-se importante entender os elementos que diferenciam as ações de coleta no método tradicional da SDN forense. A Tabela 1 lista os principais parâmetros e destaca algumas diferenças (Khan, et al., 2016).

Tabela 1. Comparação entre forense tradicional e forense SDN.

Parâmetros	Forense Tradicional	Forense SDN
Dispositivo de rede	Roteadores	Switches Openflow
Abordagem forense	Pacotes e Logs	Middle-boxes e aplicativos de controle
Busca por vestígios	Pacotes	Máquinas de estado finito e gráficos de fluxo
Coleta de evidências	Cabeçalhos de pacote e arquivos de log	Estatísticas de fluxo de rede
Escalabilidade	Baixa	Alta
Análise em tempo real	Complexa	Simples
Privacidade de dados	Baixa	Alta

Como discutido a coleta de evidências é vital para o processo de investigação. Porém, estabelecer corretamente o local onde a evidência será coletada pode ser considerado mais importante que propriamente dito coletá-la, visto que, com um local apropriado as evidências serão mais bem aproveitadas. Neste ponto, a forense SDN tem mais vantagens que a tradicional, como visto na tabela 1. A próxima seção faz um levantamento de diversos pontos para coleta de evidências, principalmente logs.

3. Levantamento de Projetos em SDN Forense

A metodologia empregada para realizar a revisão sistemática da literatura foi buscar na Web of Science e no Google Scholar e listar os principais artigos referentes aos assuntos buscados. Na Web of Science realizou-se pesquisa por tópicos, em toda a base, em todos os anos disponíveis. O primeiro termo buscado foi “SDN Security” (SDN AND security), a busca retornou 1.708 artigos, como o termo é muito genérico foi aplicado o filtro

“Artigo mais citado no campo”, com isso, restaram 22 artigos. Destes, 10 foram selecionados para a leitura dos resumos e 7 utilizados para compor o corpo da pesquisa. Para o foco da pesquisa o termo buscado na base da Web of Science foi “Forensics SDN” (Forensics AND SDN) a expressão resultou em 25 artigos de toda a base, destes artigos foram separados 10 artigos para a leitura do resumo e 4 foram utilizados na pesquisa.

Depois de realizar o levantamento de artigos para a estrutura do trabalho, a pesquisa buscou entender dados de diversos projetos de pesquisa para um apanhado geral sobre os problemas de segurança das redes SDN, bem como, quais caminhos seguir para identificar, coletar e analisar corretamente os dados necessários após um incidente de segurança e, assim, realizar a perícia.

A proposta apresentada em (Pourvahab & Ekbatanifard, 2019) descreve um framework para a coleta de evidências forenses de forma confiável, utilizando o ambiente de nuvem e a tecnologia Blockchain. O trabalho se desenvolve utilizando um servidor de autenticação em nuvem, um provedor de serviços (CSP), chaves OpenFlow que são utilizadas para encaminhar dados de usuários com base nas regras de fluxo implantadas pelo controlador e o controlador SDN que contém a lista de regras de fluxo baseado no status da rede. Neste caso, os dados coletados seguiam um caminho até um servidor de nuvem e a integridade de cada um foi mantida através da tecnologia Blockchain. A Figura 4 ilustra o framework proposto na pesquisa (Pourvahab & Ekbatanifard, 2019).

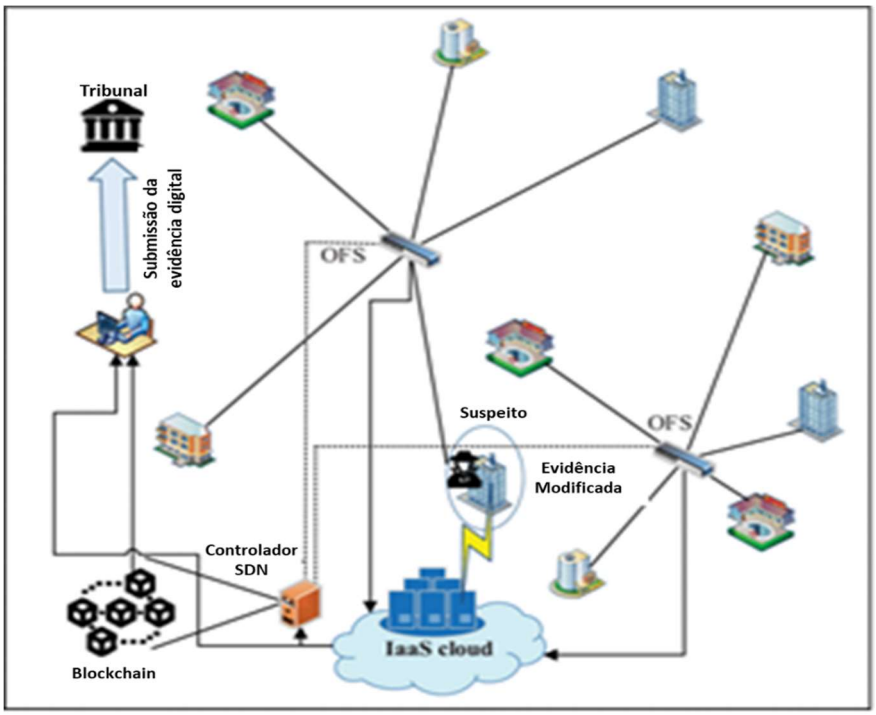

Figura 4. Framework forense proposto por (Pourvahab & Ekbatanifard, 2019)**.**

A pesquisa proposta por (Duy, et al., 2019), também segue a linha de coleta, aquisição e preservação da integridade de “logs” dentro das redes SDN e a garantia da integridade utilizando Blockchain. A diferença para o modelo proposto anteriormente em (Pourvahab & Ekbatanifard, 2019) é que o modelo apresentado em (Duy, et al., 2019) foi dividido em duas etapas: a primeira consiste na coleta de logs, a segunda na análise para o possível armazenamento. O modelo possui uma combinação dos seguintes grupos de componentes:

- Os agentes de coleta de log SDN: são os controladores, switches, hosts que fazem a leitura dos logs em tempo real e encaminham para o elemento de coleta.
- O gerente forense (Forense Manager): é o controlador que reúne todas as informações de log de agentes.
- Coletor e filtro de log: Elementos que atuam baseados em regras e requisitos do administrador, após a aplicação do filtro os arquivos de logs são encaminhados para o gerenciador de logs.
- Gerenciador de logs (Log Manager): o seu papel é analisar, por meio de interações baseadas em API, e em seguida armazenar o log de forma íntegra no armazenador de logs. O armazenamento proposto será autenticado utilizando Blockchain.

A Figura 5 a seguir ilustra o trabalho proposto e cada uma de suas partes.

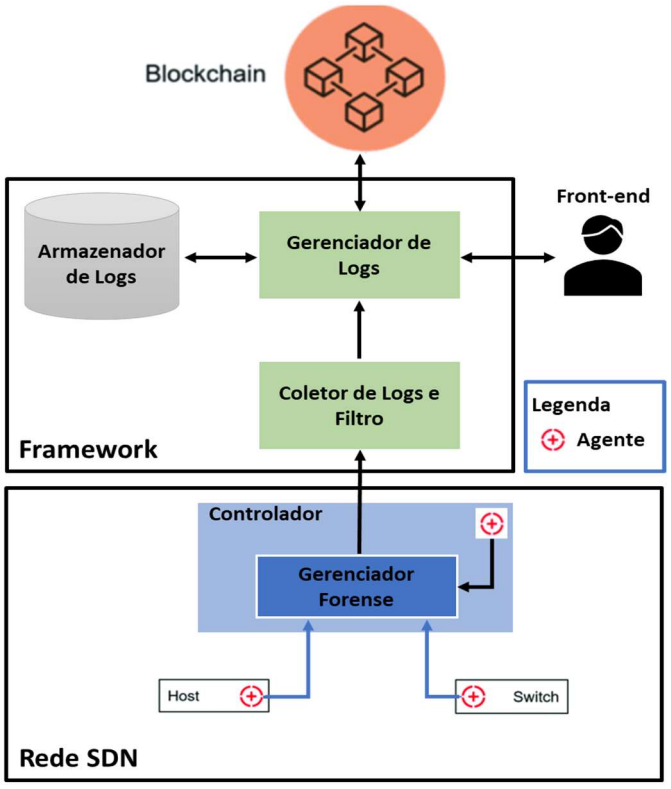

Figura 5. Estrutura de coleta, análise e armazenamento de logs em redes SDN proposto por (Duy, et al., 2019)**.**

O trabalho proposto por (Achleitner, Porta, Jaeger, & McDaniel, 2017) focou em mostrar as falhas de segurança que a composição minuciosa das regras de fluxo do controlador SDN possui. O desafio foi reconstruir regras internas de um elemento de rede habilitado para OpenFlow, indicando quais informações de pacote foram usadas para criar a correspondência e quais foram aplicadas aos pacotes. Foi produzido um scanner baseado na ferramenta NMAP que recebeu o nome de SDNMAP que foi capaz de reconstruir com uma precisão de 96% as regras de fluxo entre os terminais de rede. A contribuição forense do artigo perpassa pelo fato de que será possível percorrer o caminho criado por um invasor mesmo que ele tente destruir seus rastros e ainda criar camadas de segurança para proteger as regras de fluxo adotadas.

O trabalho mostrado em (Khan, et al., 2016) cria uma lista de locais dentro da SDN que servem para a coleta de evidências. Baseado no que foi apresentado tópico 2.2 deste artigo e devidamente ilustrado pela Figura 2, o principal trabalho do perito é saber quais locais devem ser alvos da coleta e aquisição de dados para que a análise e a documentação apresentem fielmente o evento que será relatado. Por isso, o trabalho mostra que determinar onde coletar é mais importante que de fato coletar. Muitos investigadores aproveitam o fato de o SDN possuir um elemento controlador para buscar suas evidências apenas nele. Porém, se o controlador estiver sob ataque, os dados ali coletados podem ter sua integridade comprometida.

Assim, o trabalho de pesquisa de (Khan, et al., 2016) apresenta, conforme mostrado na Figura 6, uma lista de locais, em todas as camadas da estrutura SDN, para a identificação, coleta e aquisição de evidências.

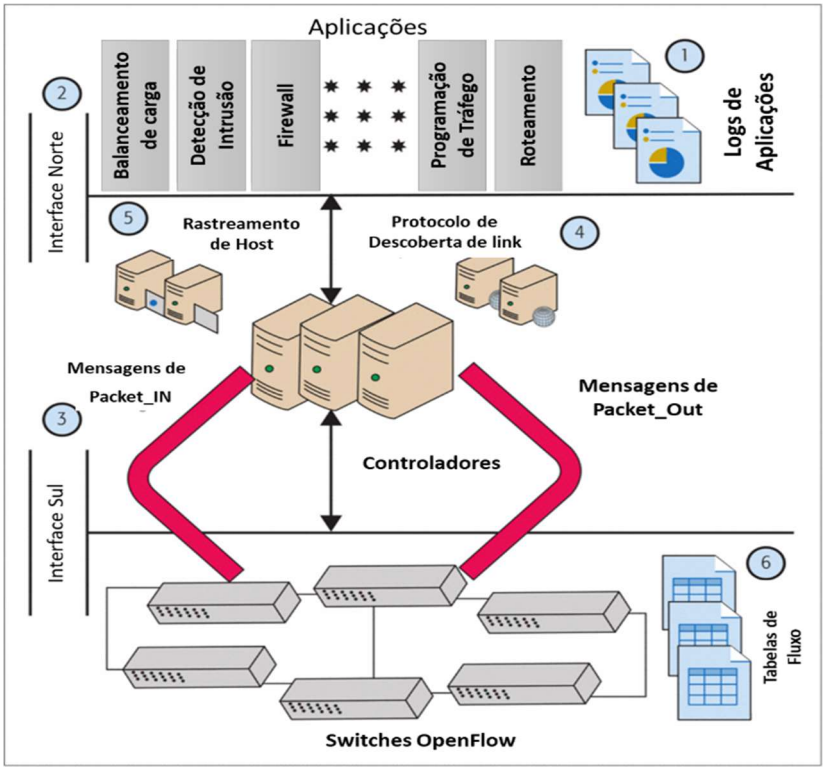

Figura 6. Locais dentro da estrutura SDN para a coleta de evidências forenses proposto por (Khan, et al., 2016)

A partir dos trabalhos apresentados aqui, fizemos uma análise dos principais problemas de segurança e a contribuição que a forense computacional pode fornecer diante dos desafios propostos. Mostramos através da análise do cenário da prática forense em SDN que a coleta de dados através dos logs gerados pela estrutura SDN, pois esta rede possui interfaces (norte e sul) bem definidas, com uma estrutura de fluxo de dados que permite criar os gatilhos para capturar e coletar os logs com mais facilidade e escala do que acontece em redes tradicionais, por esta razão alguns trabalhos realizaram a coleta de dados e os registraram em Blockchain. A Tabela 2 faz uma comparação de cada trabalho estudado e os locais dentro da estrutura SDN que serviram para aquisição e coleta de dados.

Tabela 2. Comparação entre os trabalhos de forense SDN

	Trabalho 1	Trabalho 2	Trabalho 3	Trabalho 4
Tipo de Evidência	Dados da rede, regras de fluxo e Logs	Logs	Dados da rede	Logs, tabelas de fluxos, mensagens
Ponto de Aquisição de evidência	Controlador SDN	Agentes de Coleta de log	SDNMap	Logs de aplicação, Switch OpenFlow, Tabela de Fluxo, HTS
Validação de evidência	Blockchain e Ambiente de Nuvem	Blockchain	Nenhuma	Nenhuma
Framework próprio	CFLOG	SDNLog-Foren	Nenhum	Nenhum

Para melhor formatação da tabela criou-se uma legenda dos trabalhos e suas referências:

- Trabalho 1: Pourvahab & Ekbatanifard, 2019
- Trabalho 2: Duy, et al., 2019
- Trabalho 3: Achleitner, Porta, Jaeger, & McDaniel, 2017
- Trabalho 4: Khan, et al., 2016

4. Conclusões

Quando se investiga uma rede controlada por software, um assunto relativamente recente quando se tem o olhar da utilização em massa desta nova tecnologia, destacam-se os problemas de segurança que são intrínsecos a qualquer sistema de comunicação e transmissão de dados. A pergunta que deve ser respondida será: como realizar a identificação, a coleta, a análise e a documentação das evidências forenses que surgem dos diversos desafios de segurança? A proposta deste artigo foi fazer um levantamento bibliográfico de como trabalhos de pesquisa estão tratando tal problema, analisá-los e classificá-los de forma a identificar os mais relevantes. Além de conseguir comparar como a forense SDN se posiciona em relação ao método tradicional, quando se analisa complexidade, escalabilidade e pontos de extração de evidências, de acordo com os artigos estudados a Forense SDN possui certa vantagem.

Sabe-se que a investigação forense em SDN ainda possui grandes desafios devido à arquitetura multicamadas, que apresenta uma grande quantidade de dados de log em vários locais e com diferentes características. Também possui problemas com as regras de fluxo e estrutura centralizada, que contribuem para a necessidade de uma análise forense bastante aprimorada. Com tal complexidade, não é possível indicar apenas uma técnica, um mecanismo pronto para a realização dos procedimentos forenses em SDN.

Este trabalho de pesquisa fez um levantamento dos caminhos apresentados para forense SDN, que perpassam pela análise de regras de fluxo do OpenFlow, análise de logs com a garantia de integridade utilizando framework e Blockchain, bem como, mostrou os

principais pontos para a coleta de evidências forenses. Considera-se que as pesquisas sobre o assunto ainda são prematuras, por isso há previsão de que, ao longo dos próximos meses, muitas outras técnicas devem ser propostas e validadas.

Como proposta de trabalho futuro a contribuição será estendida para novos paradigmas de redes SDN utilizando tecnologias disruptivas que descentralizam o plano de dados do plano de controle, por exemplo, o P4, a arquitetura PISA utilizando P4 e suas variações, assim será possível mapear a atuação da ciência forense nos novos cenários das redes SDN.

Referências

Abdullaziz, O. I., Wang, L. C., & Chen, Y. J. (2019). *"HiAuth: Hidden Authentication for Protecting Software Defined Networks".* IEEE Transactions On Network And Service Management. VOL. 16, NO. 2. June 2019.

Achleitner, S., Porta, T. L., Jaeger, T., & McDaniel, P. (2017). *"Adversarial Network Forensics in Software Defined Networking".* New York: Em Proceedings of the Symposium on SDN Research (SOSR '17). Association for Computing Machinery.

Allouzi, M. A. (2018). *"Advanced Authentication Protocol for Software-Defined Networks".* World Scientific. International Journal of Semantic Computing. Vol. 12, No. 03, pp. 361-371. 2018.

Aydeger, A., Saputro, N., & Akkaya, K. (2019). *"A moving target defense and network forensics framework for ISP networks using SDN and NFV".* Future Generation Computer Systems. ELSEVIER. Volume 94. Pages 496-509. May 2019.

Brezinski, D., & Killalea, T. (2002). *"Guidelines for evidence collection and archiving".* RFC 3227, IETF, 2002.

Brockelsby, W., & Dutta, R. (2019). *"A Graded Approach to Network Forensics with Privacy Concerns".* IEEE Computing Networking and Communications (ICNC) 2019 International Conference on , pp. 292-297.

Casado, M., McKeown, N., & Shenker, S. (08 de november de 2019). From Ethane to SDN and Beyond. *ACM SIGCOMM Computer Communication Review*, 92-95. doi:https://doi.org/10.1145/3371934.3371963

Chica, J. C., Imbachi, J. C., & Veja, J. F. (2020). *"Security in SDN: A comprehensive survey".* Journal of Network and Computer Applications (159). ELSEVIER.

CSA, C. S. (2013). *Mapping the Forensic Standard ISO/IEC 27037 to Cloud Computing, June 2013.*

Duy, T. P., Hoang, H. D., Hien, D. T., Khanh, N. B., Pham, & H., V. (2019). *"SDNLog-Foren: Ensuring the Integrity and Tamper Resistance of Log Files for SDN Forensics using Blockchain".* 6th NAFOSTED Conference on Information and Computer Science (NICS). 2019.

Farmer, D., & Venema, W. (2016). *"Perícia Forense Computacional: Teoria e Prática Aplicada".* São Paulo: Pearson.

Han, T., Jan, S. R., Tan, Z., Usman, M., Jan, M. A., Khan, R., & Xu, Y. (2019). *"A comprehensive survey of security threats and their mitigation techniques for next-generation SDN controllers".* WILEY. Concurrency Computat Pract Exper. 2019. doi:10.1002/cpe.5300.

Khan, S., Gani, A., Wahab, A. W., Abdelaziz, A., Ko, K., Khan, M. K., & Guizani, M. (2016). *"Software-Defined Network Forensics: Motivation, Potential Locations, Requirements, and Challenges".* IEEE Network, vol. 30, no. 6, pp. 6-13, November-December 2016. doi:10.1109/MNET.2016.1600051NM.

Kreutz, D. R., V., F. M., Veríssimo, P. E., Rothenberg, C. E., Azodolmolky, S., & Uhlig, S. (2015). *"Software-Defined Networking: A Comprehensive Survey".* Proceedings of the IEEE, vol. 103, no. 1, pp. 14-76, jan. 2015. doi:10.1109/JPROC.2014.2371999.

Kreutz, D., Ramos, D., & Verissimo, P. (2013). *"Towards secure and dependable software-defined networks".* 2º ACM SIGCOMM Workshop Hot Topics Softw. Defined Network. pp. 55–60.

Long, J. (Março de 2021). *"Software Define Networks".* Fonte: https://www.gta.ufrj.br/grad/16_2/2016SDN/conceitos.html

Oktian, Y. E., Lee, S., Lee, H., & Lam, J. (2017). *"Distributed SDN controller system: A survey on design choice".* Computer Networks Volume 121, 5 July 2017, Pages 100-111. ELSEVIER.

Pourvahab, M., & Ekbatanifard, G. (2019). *"Digital Forensics Architecture for Evidence Collection and Provenance Preservation in IaaS Cloud Environment Using SDN and Blockchain Technology".* IEEE Access, vol. 7, pp. 153349-153364. doi:10.1109/ACCESS.2019.2946

Tang, Y., Liu, T., He, X., Yu, J., & Qin, P. (2019). *"A Lightweight Two-Way Authentication Scheme Between Communication Nodes for Software Defined Optical Access Network".* IEEE Access, vol. 7, pp. 133248-133256, 2019. doi:10.1109/ACCESS.2019.2941084.