seminário de iniciação científica
ISNN: 2358-6052
ISSN 2558-6052

FORENSE DIGITAL E RESPOSTA A INCIDENTES: ESTUDO E ELABORAÇÃO DE MATERIAL DIDÁTICO

Autores: Rafael Alvarenga de Azevedo e Mário Luiz Rodrigues Oliveira

RESUMO

A rede mundial de computadores é largamente usada nos diversos setores da sociedade. Tanto pessoas físicas como jurídicas usufruem dos serviços digitais existentes. Quanto mais usuários na Internet, mais informações trafegam na rede. Enquanto isso, há indivíduos mal-intencionados que buscam comprometer informações confidenciais para extorquir vítimas, ou vender materiais pessoais de várias pessoas mediante vazamento de dados, por exemplo. Portanto, não somente é fundamental o reajuste das leis para punir cibercriminosos, mas também é crucial o treinamento de profissionais para responder aos diversos incidentes relacionados a essa nova categoria de delito. Logo, busca-se fomentar a capacitação de profissionais para lidar com os diversos percalços da área de Forense Digital e Resposta a Incidentes (FDRI), visto que esta estuda maneiras de lidar com ameaças cibernéticas como vazamento de dados e ataques *ransomware*. Consequentemente, propôs-se uma revisão sistemática da literatura para tentar identificar as técnicas e ferramentas disponíveis no estado da arte, no período de 2010 a 2020. Após revisão sistemática de 205 artigos, selecionou-se 79 artigos para leitura completa. Em seguida, evidenciou-se a existência de técnicas e ferramentas aplicáveis nas seguintes subáreas de FDRI: análise de malware, análise de logs, análise forense em redes de computadores, análise de inteligência, análise forense de memória volátil e análise forense de sistema de arquivos. Além disso, obteve-se compilados com as melhores práticas de FDRI, a enumeração de 18 crimes cometidos com uso de sistemas computacionais, a identificação dos desafios dessa área, e as tendências que envolvem estudos de Inteligência Artificial e Dispositivos Móveis. Ainda, constatou-se em estudo de caso como aparatos digitais podem ser usados, por um perito, para reconstruir ações de usuários em uma máquina investigada de uma situação fictícia. Por último, elaborou-se um material didático para introduzir um estudante na área de FDRI, à medida que técnicas e ferramentas são estudadas sob a ótica das subáreas apresentadas.

INTRODUÇÃO:

A Internet é amplamente utilizada por diversos indivíduos no planeta, incluindo pessoas físicas, empresas nacionais e corporações multinacionais. Enquanto isso, surgem novas possibilidades de aproveitamento por parte dos criminosos. Sendo assim, um novo tipo de crime entra em voga, o cibernético. Além da necessidade da criação e vigência de novas leis, há também uma demanda por profissionais capacitados para lidar com os diversos problemas da área de FDRI. Pois, há desafios envolvidos na contenção de incidentes como vazamento de dados e ataques *ransomware*. No entanto, pouco se explora as técnicas e ferramentas utilizadas por um perito no tratamento de ameaças correlatas. Portanto, propõe-se uma revisão sistemática da literatura para identificar e compreender quais as técnicas e ferramentas usadas em FDRI, de modo a contribuir na capacitação de recurso humano.

O Governo Brasileiro (2020), colocou em vigor, no dia 18 de setembro de 2020, a nova lei geral de proteção de dados - ou LGPD - (BRASIL, 2018). Esta legislação tem por objetivo proteger os dados pessoais de todo cidadão que resida no Brasil. Importa registrar a relevância dessa legislação considerando que o Brasil tem sofrido diversos casos graves de vazamento de dados. Exemplo disso, incidente reportado em diversos veículos da mídia televisiva e escrita (VEJA, 2021), e detectado pela empresa de segurança digital *PSafe*. Esta identificou em seu sistema de monitoramento a divulgação indevida de 40 milhões de CNPJs de empresas nacionais e 223 milhões de CPFs, esse número inclui brasileiros vivos e mortos. Tais dados foram divulgados na *dark web* - rede de computador focado em práticas ilícitas. Porém, não foi possível rastrear a identidade dos criminosos devido à barreira de anonimidade utilizada pelos fraudadores ao acessarem esse tipo de rede (VEJA,2021).

Como aponta estudo realizado pela IBM em 2019, 77% das organizações não têm um plano de resposta a incidentes de segurança cibernética (REDAÇÃO, 2019). Além disso, há um aumento na incidência de crimes cibernéticos, tornando necessária a contratação de peritos digitais (LIMA, 2020). Apesar dos setores público e privado demonstrarem preocupação com a segurança das suas aplicações digitais, as ameaças cibernéticas são inevitáveis e devem ser combatidas a todo custo. Assim, a capacitação de recurso humano, na área de FDRI, é primordial para ajudar a impugnar essa problemática.

seminário de iniciação científica
ISNN: 2358-6052
ISSN 2558-6052

Uma revisão sistemática da literatura (SLR, do inglês *systematic literature review*) é um meio para identificar, avaliar e interpretar todas as pesquisas recentes relacionadas a um assunto em particular. Pesquisas individuais que contribuem para uma revisão sistemática são chamadas primárias, e a revisão, secundária (KITCHENHAM; CHARTERS, 2007).

Com essa técnica de estudo, é possível sintetizar trabalhos existentes de forma justa. Para conseguir colocá-la em prática, é necessário seguir uma estratégia de pesquisa. Esta, deve permitir que a totalidade da pesquisa possa ser avaliada. Pesquisadores em processo de construção de uma revisão sistemática devem procurar pesquisas que não suportam sua hipótese inicial, bem como estudos que suportam (KITCHENHAM; CHARTERS, 2007).

A realização de uma revisão sistemática pode ser separada em três etapas: planejamento, condução e relatório. Na primeira, são feitas a identificação da necessidade da pesquisa, a especificação da pergunta da pesquisa, o desenvolvimento de um protocolo para revisão e a avaliação deste protocolo. Em segunda instância, é feita a extração de todos os estudos primários; bem como a avaliação, monitoramento e síntese destes. No último momento, o relatório é formatado e avaliado (KITCHENHAM; CHARTERS, 2007).

Na sequência, na seção Metodologia, apresenta-se o protocolo usado na realização da SLR, bem como se explicita o processo forense empregado na elaboração do estudo de caso deste artigo. Ainda, explica-se a metodologia de elaboração do material didático. Por conseguinte, na seção de Resultados, análises qualitativas são apresentadas sobre as técnicas e ferramentas extraídas dos estudos primários da SLR, detalhamento sobre o estudo de caso, e dados sobre o material didático criado. Finalmente, conclui-se o estudo na seção apropriada.

METODOLOGIA:

Para realização da SLR, adaptou-se o procedimento proposto por Senocak (2019). Ainda, o estudo de caso se deu através da utilização do processo forense recomendado pelo NIST (KENT et al., 2006). Tal processo foi escolhido devido à sua ampla utilização/citação, percebida na leitura dos estudos primários. Isto posto, detalham-se, nas próximas seções, o protocolo usado e o processo forense executado.

Formulação de Perguntas

Questionava-se a existência das técnicas e ferramentas da área de FDRI, com a intenção de compreender como elas são utilizadas pelos especialistas. De acordo com Roberts (2016), espera-se que o profissional seja capacitado nas seguintes subáreas: análise de malware, análise de logs, análise forense em redes de computadores, análise de inteligência, análise forense de memória volátil e análise forense de sistema de arquivos.

Contudo, não há, atualmente, um compilado com as técnicas e ferramentas do estado da arte do período de 2010 a 2020. Deste modo, propuseram-se as seguintes questões:

- “Quais as técnicas e ferramentas existentes na área de FDRI ?”;
- “Quais os principais crimes cometidos com uso de sistemas computacionais ?”;
- “Quais as melhores práticas na área de FDRI ?”.

Com o intuito de responder a tais perguntas, identificaram-se como palavras-chave e sinônimos os termos:

- Sinônimos de “Forense Digital”: computação forense, análise forense, informática forense;
- Palavras-chave: Resposta a incidentes; análise de malware, análise de logs, análise forense em redes de computadores, análise de inteligência, análise forense de memória volátil e análise forense de sistema de arquivos.

Através da busca pelas técnicas e ferramentas de FDRI, pretendia-se a identificação e compilação dos resultados, para classificá-los nas subáreas enumeradas. Consequentemente, a população do estudo é composta por publicações feitas por pesquisadores ou profissionais da área de FDRI, aplicáveis no ambiente acadêmico ou no mercado.

Seleção de Fontes

As fontes foram selecionadas através de uma consulta específica, em bases de dados de renome com publicações na área de FDRI. Escolheu-se a língua inglesa como língua padrão, devido às diversas aplicações apresentadas pela comunidade internacional. Para efetuar a seleção de estudos, recorreu-se a

seminário de iniciação científica
ISNN: 2358-6052
ISSN 2558-6052
uma *string* de busca específica e às seguintes bases de dados: ACM, ScienceDirect, Periódicos CAPES (CAFe), Google Scholar.

Em primeira instância, utilizou-se o Google Scholar para realizar um teste de sanidade com a consulta especializada abaixo:

-book ("computer forensics" OR "forensic analysis" OR "digital forensics") AND ("and" OR "&") AND ("incident" AND ("analysis" OR "response")) AND ("tools" OR "techniques")

A ferramenta retornou 11.700 publicações. Foram excluídas as citações nos filtros complementares do motor de busca. Mas esses resultados não foram usados na fase de seleção de estudos.

Em segunda instância, parametrizou-se a *string* de busca inicial para cada uma das bases de dados restantes. Na base de dados ACM, a consulta 1 considera o período de publicação de 2010 a 2020, e a opção *Research Article* marcada. O motor de busca retornou 401 artigos, porém apenas 48 deles eram gratuitos ou públicos. No ambiente da ScienceDirect, a consulta 2 é limitada pelo período de publicação de 2010 a 2020, pela área de Ciência da Computação, e pelas opções *Research Article* e *Open Access* marcadas. A ferramenta retornou 157 artigos, dada a consulta 2. Por meio do site Periódicos CAPES (CAFe), a consulta 3 teve como restrições complementares: busca avançada por artigos em língua inglesa, período de publicação entre 2010 e 2020, e tópico *Computer Science* de pesquisa. A busca retornou 311 resultados, porém apenas 1 artigo estava acessível no momento da pesquisa.

As consultas parametrizadas encontram-se em https://pastebin.com/NZeDGbNe.

Seleção de Estudos

Posto que as bases de dados forneciam acesso a artigos 206 em língua inglesa, selecionaram-se sistematicamente os estudos primários da SLR. Primeiramente, realizou-se a leitura do título e do resumo. Em seguida, leu-se a conclusão. Por conseguinte, leram-se a introdução e a metodologia. Por fim, leu-se 79 artigos por completo, para extrair as informações.

Vale ressaltar que em cada etapa do procedimento de seleção, manteve-se o estudo corrente para próxima classificação quando havia dúvida se o texto responderia a alguma questão da pesquisa ou não.

Extração de informações

Filtrou-se pelas técnicas e ferramentas utilizadas, ou produzidas, nos estudos primários. Sendo assim, enumerou-se o título do estudo, autores, quais subáreas da FDRI suas técnicas ou ferramentas se aplicavam e seu ano de publicação. Os resultados da pesquisa foram sintetizados na seção Resultados deste artigo, e divulgados em uma tabela pública no *Google Docs* (https://bit.ly/3OZ03tw).

Processo Forense do Estudo de Caso

O estudo de caso proposto é realizado a fim de capacitar recurso humano, enquanto técnicas e ferramentas forenses são utilizadas para elaborar um relatório pericial, diante de uma situação fictícia. Dessa forma, configurou-se um ambiente de testes para feitura da análise pericial premeditada pelo NIST. Enfim, efetivou-se o procedimento composto pelos seguintes passos: Coleta, Exame, Análise e Relatório (KENT et al., 2006).

RESULTADOS E DISCUSSÕES:

Os resultados, detalhados nesta seção, foram obtidos após a fase de Extração de Informações da SLR. Sintetizaram-se as informações extraídas, de maneira a efetuar a compilação das melhores práticas usadas nos processos forenses, a compilação dos principais crimes cometidos com uso de sistemas computacionais e a identificação das tendências e desafios da área de FDRI. Em seguida, realizou-se um estudo de caso, de maneira a verificar, pragmaticamente, o funcionamento de algumas técnicas e ferramentas encontradas nos artigos lidos. Por último, elaborou-se um material didático introdutório sobre FDRI.

Com base nessa amostra, nota-se uma ampla utilização de técnicas e ferramentas da subárea de análise de memória volátil. De acordo com Garfinkel (2010), uma das dificuldades que um perito encontra é adquirir cópias forenses de dispositivos de armazenamento com capacidades crescentes. Para tentar combater tal problema, a proposta de triagem forense, como explicam Vidas, Kaplan e Geiger (2014), pode

ISSN 2558-6052

ser usada. Uma vez que se baseia na ideia de triagem da medicina para escolher componentes lógicos mais relevantes para responder a um incidente. Sendo assim, a triagem forense tem sido usada em aparelhos ligados para tentar reduzir o tempo de uma investigação, enquanto vestígios são agilmente identificados em memória volátil.

Por outro lado, existem técnicas anti-forenses que inviabilizam a aquisição de cópias forenses em dada investigação. Dado que a maioria das ferramentas periciais pode ser acessada por criminosos, estes estudam-nas para encontrar formas de impedir seu funcionamento. Stüttgen e Cohen (2013) mostraram que com uso de *rootkits*, usuários mal-intencionados conseguiam burlar 6 ferramentas populares de coleta de cópia de memória volátil. Por conseguinte, chegaram à conclusão de que a melhor maneira de contornar técnicas anti-forenses é não utilizar chamadas de sistema do sistema operacional hospedeiro. Mas sim efetuar acesso direto à memória (DMA), como fizeram Latzo, Brost e Freiling (2020). Portanto, defende-se o uso de dispositivos que realizam DMA, para adquirir cópias forenses da memória volátil de um sistema.

Organizações dispõem de sistemas de detecção de intrusão (IDS do inglês *Intrusion Detection System*) para ajudar no reconhecimento de ameaças dentro de sua rede. Entretanto, as ameaças mudam com o tempo, e também os objetivos dos cibercriminosos. Todavia, tais sistemas não conseguem identificar novas formas de ataque, apenas conhecidas (CAPOBIANCO et al., 2019). Consequentemente, sustenta-se o compartilhamento de informações entre organizações sobre ataques ocorridos em suas redes. Como fizeram Ardi e Heidemann (2018), ao detectar *bots* em sua rede. Ainda, há esforços para criação de esquemas de troca de informações de uma investigação, como, por exemplo, a linguagem CybOX, proposta por Casey, Back e Barnum (2015).

Com a popularização da computação na nuvem, novos serviços passaram a ser fornecidos na Web através de aplicações distribuídas transparentes, isto é, aplicativos mantidos por servidores ao redor do mundo e com localização transparente ao usuário. Por isso, a análise forense se torna inviável em casos em que o perito não tem acesso ao dispositivo físico de um caso. Dessa maneira, pesquisadores propõem formas de adquirir cópias forenses de dispositivos da nuvem. Como defendido por Dykstra e Sherman (2012) - ao realizarem experimentos sobre formas de se obter cópias digitais de discos da nuvem -, o uso de *management planes* fornecidos pelas empresas da nuvem é o mais recomendado. Essa técnica consiste em fornecer ao cliente uma interface para requisição de cópia forense, coletada pelo provedor da nuvem no nível do sistema operacional hospedeiro. Como fizeram Dykstra e Sherman (2013), através da ferramenta FROST.

Outrossim, quando um incidente ocorre em função de um malware, e este agrega novas técnicas de invasão, é necessária uma análise aprofundada de seu comportamento para mitigá-lo em uma rede. Existem ferramentas automatizadas, como Cuckoo Sandbox, capazes de gerar relatórios sobre o comportamento de um programa fornecido pelo usuário. Porém, esse tipo de ferramenta é limitado em assistir o analista de malware que estiver trabalhando com amostras parcialmente reconhecidas. Koki, Abdullah e Jhanjh (2020) usaram Cuckoo Sandbox para criar a ferramenta PEDA, que no que lhe concerne consegue detectar *crypto-ransomwares* antes deles agirem no sistema vítima. Ainda, há pesquisas sobre formas de abstrair conceitos dessa área para peritos menos experientes. Exemplo disso, o plugin *hooktracer* desenvolvido por Case et al. (2019), para a ferramenta Volatility Framework. Ele facilita a análise e busca por *API hooks* em uma máquina investigada. Logo, é possível desenvolver ferramentas que auxiliem peritos inexperientes na análise de malware, mas também é necessário treiná-los para poderem descobrir novas formas de responder a incidentes decorrentes de malwares inovadores.

Em concordância com Okutan e Çebi (2019), identificou-se 18 tipos de crimes cometidos com uso de computadores, sendo eles: uso de Malwares; Phishing; Ataque “Man in the Middle”; Trojans; Ataques de Negação de Serviço; Ciberterrorismo; Cyberstalking; Pornografia infantil; Roubo de identidade; Fraude cibernética; Key Logger; Screen Logger; Evil Twin; Botnet; Engenharia Social; Worms; Sniffer e Ciberbullying.

Em suma, e em consonância com Garfinkel (2010), os maiores desafios da área de FDRI são: dificuldade em realizar cópias de discos cada vez maiores; utilização frequente de memórias flash; uso de diferentes sistemas operacionais e sistemas de arquivos; dificuldade em analisar múltiplos dispositivos em casos complexos; existência de dados criptografados que quando recuperados não são facilmente processados; utilização de computação na nuvem; existência de vírus que residem na memória principal do computador e exigem análise forense mais específica.

Pesquisadores começaram a aplicar conhecimentos de Inteligência Artificial (IA) nas diversas fases do processo de análise forense clássico, e também a explorar análise forense em dispositivos móveis. Como evidenciado por Du et al. (2020), algoritmos de IA vem sendo utilizados para fazer: recuperação de dados, triagem forense de dispositivos, análise de redes, análise forense de dados criptografados (criptoanálise), reconstrução de eventos e linha do tempo, análise forense em aparelhos multimídia e

seminário de iniciação científica
ISNN: 2358-6052
ISSN 2558-6052

fingerprinting. Ademais, Sharmalc, Arora e Sakthive (2020) propuseram um novo procedimento forense para coletar e configurar evidências em dispositivos Android. A abordagem é chamada *Enhanced Mobile Cloud Forensic Process*. Ela aproveita os registros e arquivos de aplicativos de redes sociais, para montar o perfil de um suspeito. Em seguida, rastreia diversas informações no celular e nos servidores na nuvem ligados às contas virtuais do usuário.

Estudo de Caso

O gerente de uma empresa desconfia que um de seus funcionários esteja fazendo *downloads* indevidos em sua estação de trabalho, e também de que ele esteja passando tempo demais em programas aparentemente desconhecidos no meio do expediente. Certo dia o gerente resolveu verificar o histórico de navegação do *browser* do computador usado pelo funcionário, porém não achou nenhum registro de acesso a sites indevidos, ou sequer downloads indevidos. Sabendo que o funcionário, no horário comercial, mexia em sites estranhos, o gerente resolveu contratar um perito particular para investigar o caso.

Para realização deste estudo de caso, montou-se um ambiente de testes com duas máquinas: a investigada e a do perito.

Máquina Investigada: máquina virtual com o sistema operacional Windows 7 Enterprise 32 bits (licença de teste de 90 dias), com 2GB de RAM, processador de 2 núcleos e 40 GB de armazenamento. Obteve-se um arquivo *vmdk* (disponível em https://archive.org/details/ie11.win7.virtualbox).

Máquina do perito: máquina com o sistema operacional Manjaro Linux, com as seguintes ferramentas instaladas: Virtualbox; Autopsy; Falcon Sandbox (instanciado em https://www.hybrid-analysis.com/).

Relatório: utilizando o programa *vboxmanage* (comando 1), criou-se uma cópia do disco da máquina investigada. Em seguida, realizou-se o exame do sistema de arquivos usando a ferramenta Autopsy. Diversos artefatos foram identificados ao realizar a análise automatizada com os *Ingest Modules* do Autopsy.

Conforme requisitado, realizou-se uma busca por arquivos baixados pelo navegador (Google Chrome). Sendo assim, identificaram-se diferentes informações apagadas como o Histórico de Navegação e Histórico de Downloads, ao identificar os arquivos de cache *data_1* e *data_2*, armazenados no diretório 1 - recuperado com o módulo *Photorec* do Autopsy.

Como registrado pelo link 1, o funcionário baixou o cliente torrent *qBittorrent* às 2021-12-28 16:05:48 BRT (data de criação do arquivo 1). Em seguida, como identificado no link 2, o usuário baixou os arquivos 2 e 3 ao realizar uma busca no site *ThePirateBay* (site conhecido por fornecer acesso à cópia ilícita de diversos arquivos). Afinal, os arquivos 2 e 3 foram baixados - às 2021-12-28 16:09:18 BRT e 2021-12-28 16:09:20 BRT, respectivamente - usando a ferramenta *qBittorrent*.

Além disso, descobriu-se outra busca (link 3), desta vez por uma ferramenta ilícita de ativação do sistema operacional Windows. Encontrado no histórico apagado do arquivo *data_2*, o link 3 fornece ao usuário um link para o site MEGA para aquisição do arquivo 4 (criado às 2021-12-28 16:56:20 BRT). Portanto, o funcionário também baixou um software ativador de sistema operacional proprietário.

Para verificar se o arquivo 4 era um software malicioso, realizou-se uma análise de malware através da ferramenta Falcon Sandbox, para tentar compreender o comportamento do programa executado em ambiente isolado.

O arquivo 4 contém um executável chamado 'Microsoft Toolkit.exe'. Este executável é do tipo *PEEXE*, e contém funções que requisitam informações de depuração do kernel do Windows. Além disso, possui código de proteção contra *dumping* de memória. Ademais, é classificado como programa malicioso por 22 de 61 softwares antivírus. O relatório detalhado gerado pela ferramenta Falcon Sandbox pode ser visualizado em https://tinyurl.com/yy4g3akg e https://tinyurl.com/y6n29ukc.

Os arquivos, diretórios, links e comandos encontram-se em https://pastebin.com/Qu3agC36.

Material Didático

Desenvolveu-se um material didático para introduzir estudantes na área de Forense Digital e Resposta a Incidentes. Organizou-se o texto aplicando a abordagem de Aprendizagem Ativa, de forma que o leitor possa concretizar o conhecimento através da leitura e prática dos diferentes conceitos envolvidos em cada uma das subáreas de FDRI. O material didático foi disponibilizado publicamente em um repositório do *Github* (https://is.gd/xL5K7c), no formato da ferramenta LaTeX.

seminário de iniciação científica
ISNN: 2358-6052
ISSN 2558-6052

CONCLUSÕES:

Mediante a Revisão Sistemática da Literatura conduzida, depreendeu-se quais técnicas e ferramentas um perito de FDRI dispõe para trabalhar, segundo o estado da arte no período de 2010 a 2020. Por meio da leitura de 79 artigos, dos 205 selecionados, identificaram-se as técnicas e ferramentas de FDRI, em uma tabela do *Google Docs*. Enumerou-se 18 crimes cometidos com o uso de sistemas computacionais. E realizou-se uma análise qualitativa para identificar as melhores práticas para resolver os tipos de problemas apresentados pelos autores dessa amostra de estudos primários.

Outrossim, descobriu-se que os maiores desafios da área tratam-se de: realizar cópias de discos cada vez maiores; utilização frequente de memórias *flash*; uso de diferentes sistemas operacionais e sistemas de arquivos; dificuldade em analisar múltiplos dispositivos em casos complexos; existência de dados criptografados que quando recuperados não são facilmente processados; utilização de computação na nuvem e existência de vírus que residem na memória principal do computador e exigem análise forense mais específica. Finalmente, percebeu-se que há esforços da academia para aplicação de conhecimentos de Inteligência Artificial em FDRI, e, também, para fazer o tratamento adequado de dispositivos móveis em uma investigação.

Preparou-se um estudo de caso com o fim de colocar em prática o aprendizado teórico adquirido na leitura dos estudos primários. Além disso, elaborou-se um material didático introdutório acerca de FDRI, com o propósito de contribuir na capacitação de novos profissionais na área. Enfim, formulou-se o material educativo em função das subáreas de FDRI apontadas na SLR, para ficar claro como aplicar as técnicas e ferramentas nos diversos contextos envolvidos.

REFERÊNCIAS BIBLIOGRÁFICAS:

ARDI, Calvin; HEIDEMANN, John. Leveraging controlled information sharing for botnet activity detection. **WTMC '18: Proceedings of the 2018 Workshop on Traffic Measurements for Cybersecurity**, [S. l.], p. 14-20, 20 ago. 2018. Disponível em: https://dl.acm.org/doi/10.1145/3229598.3229602. Acesso em: 9 mai. 2022.

BRASIL. Lei nº 13.709, de 14 de agosto de 2018. Disponível em: https://www.planalto.gov.br/ccivil_03/_ato2015-2018/2018/lei/l13709.htm. Acesso em: 28 fev. 2021.

BRASIL, Governo. LGPD entra em vigor. Ministério da Justiça e Segurança Pública, 21 set. de 2020. Notícias. Disponível em: https://www.gov.br/conarq/pt-br/assuntos/noticias/lgpd-entra-em-vigor. Acesso em: 25 fev. 2021.

CAPOBIANCO, Frank; GEORGE, Rahul; HUANG, Kaiming; JAEGER, Trent; KRISHNAMURTHY, Srikanth; QIAN, Zhiyun; PAYER, Mathias; YU, Paul. Employing Attack Graphs for Intrusion Detection. **NSPW '19: Proceedings of the New Security Paradigms Workshop**, [S. l.], p. 16-30, 1 set. 2019. Disponível em: https://dl.acm.org/doi/10.1145/3368860.3368862. Acesso em: 9 mai. 2022.

CASEY, Eoghan; BACK, Greg; BARNUM, Sean. Leveraging CybOX to standardize representation and exchange of digital forensic information. **Digital Investigation**, [S. l.], p. 102-110, 6 mar. 2015. Disponível em: https://www.sciencedirect.com/science/article/pii/S1742287615000158. Acesso em: 9 mai. 2022.

DU, Xiaoyu; HARGREAVES, Chris; SHEPPARD, John; ANDA, Felix; SAYAKKARA, Asanka; LE-KHAC, Nhien-An; SCANLON, Mark. SoK: Exploring the State of the Art and the Future Potential of Artificial Intelligence in Digital Forensic Investigation. **ARES '20: Proceedings of the 15th International Conference on Availability, Reliability and Security**, [S. l.], p. 1-10, 25 ago. 2020. Disponível em: https://dl.acm.org/doi/10.1145/3407023.3407068. Acesso em: 9 mai. 2022.

DYKSTRA, Josiah; SHERMAN, Alan T. Acquiring forensic evidence from infrastructure-as-a-service cloud computing: Exploring and evaluating tools, trust, and techniques. **Digital Investigation**, [S. l.], p. 90-98, 2 ago. 2012. Disponível em: https://www.sciencedirect.com/science/article/pii/S1742287612000266. Acesso em: 9 mai. 2022.

ISSN 2558-6052

DYKSTRA, Josiah; SHERMAN, Alan T. Design and implementation of FROST: Digital forensic tools for the OpenStack cloud computing platform. **Digital Investigation**, [S. l.], p. 87-95, 3 ago. 2013. Disponível em: https://www.sciencedirect.com/science/article/pii/S174228761300056X. Acesso em: 9 mai. 2022.

GARFINKEL, Simson L. Digital forensics research: The next 10 years. **Digital Investigation**, [S. l.], p. 64-73, 2 ago. 2010. Disponível em: https://www.sciencedirect.com/science/article/pii/S1742287610000368. Acesso em: 9 mai. 2022.

KENT, Karen; CHEVALIER, Suzanne; GRACE, Tim; DANG, Hung. Guide to Integrating Forensic Techniques into Incident Response. **Computer Security**, [s. l.], 1 ago. 2006. Disponível em: https://nvlpubs.nist.gov/nistpubs/legacy/sp/nistspecialpublication800-86.pdf. Acesso em: 9 mai. 2022.

KITCHENHAM, Barbara; CHARTERS, Stuart. Guidelines for performing systematic literature reviews in software engineering. EBSE Technical Report, Keele e Durham - UK, 2007, n. EBSE 2007-001, p. 16-29, 9 jul. 2007.

KOKI, S.H.; ABDULLAH, Azween; JHANJH, NZ. Early detection of crypto-ransomware using pre-encryption detection algorithm. **Journal of King Saud University - Computer and Information Sciences**, [S. l.], p. 1-16, 4 jul. 2020. Disponível em: https://www.sciencedirect.com/science/article/pii/S1319157820304122. Acesso em: 9 mai. 2022.

LATZO, Tobias; BROST, Julian; FREILING, Felix. BMCLeech: Introducing Stealthy Memory Forensics to BMC. **Digital Investigation**, [S. l.], p. 1-7, 29 mai. 2020. Disponível em: https://www.sciencedirect.com/science/article/pii/S2666281720300147. Acesso em: 9 mai. 2022.

LIMA, Monique. Perito forense digital, profissão em alta na área de segurança cibernética. Revista VOCÊ S/A, 08 abr. 2020. Cotidiano. Disponível em: https://vocesa.abril.com.br/carreira/perito-forense-digital-profissao-em-alta-na-area-de-seguranca-cibernetica/. Acesso em: 12 mai. 2021.

OKUTAN, Ayşe; ÇEBI, Yalçın. A Framework for Cyber Crime Investigation. **Procedia Computer Science**, [S. l.], p. 287-294, 25 out. 2019. Disponível em: https://www.sciencedirect.com/science/article/pii/S1877050919312141. Acesso em: 9 mai. 2022.

REDAÇÃO. Estudo global da IBM aponta que 77% das organizações não têm um plano de resposta a incidentes de segurança cibernética. TI Inside, 15 de abr. de 2019. Mercado (Segurança). Disponível em: https://tiinside.com.br/15/04/2019/estudo-global-da-ibm-aponta-que-77-das-organizacoes-nao-tem-um-plano-de-resposta-a-incidentes-de-seguranca-cibernetica/. Acesso em: 25 fev. 2021.

ROBERTS, Scott J. Introduction to DFIR. Medium, 10 jan. 2016. Disponível em: https://sroberts.medium.com/introduction-to-dfir-d35d5de4c180. Acesso em: 26 fev. 2021.

SENOCAK, G. Revisão Sistemática da Literatura em Engenharia de Software Teoria e Prática. 2019.

SHARMALC, Puneet; ARORA, Deepak; SAKTHIVE, T. Enhanced Forensic Process for Improving Mobile Cloud Traceability in Cloud-Based Mobile Applications. **Procedia Computer Science**, [S. l.], p. 907-917, 16 abr. 2020. Disponível em: https://www.sciencedirect.com/science/article/pii/S1877050920308565. Acesso em: 9 mai. 2022.

STÜTTGEN, Johannes; COHEN, Michael. Anti-forensic resilient memory acquisition. **Digital Investigation**, [S. l.], p. 105-115, 3 ago. 2013. Disponível em: https://www.sciencedirect.com/science/article/pii/S1742287613000583. Acesso em: 9 mai. 2022.

VIDAS, Timothy; KAPLAN, Brian; GEIGER, Matthew. OpenLV: Empowering investigators and first-responders in the digital forensics process. **Digital Investigation**, [S. l.], p. 45-53, 16 abr. 2014. Disponível em: https://www.sciencedirect.com/science/article/pii/S1742287614000115?via%3Dihub. Acesso em: 9 mai. 2022.