

FORENSE COMPUTACIONAL COMO ESTRATÉGIA PARA INVESTIGAÇÃO DE INCIDENTES DE CRIMES CIBERNÉTICOS EM TELEMEDICINA

NADJILA TEJO MACHADO^{1,4}, LEONARDO JUAN RAMIREZ LOPEZ^{2,4}, FELIPE RODRIGUES MARTINEZ BASILE^{3,4}

¹ Graduanda em Tecnologia de Análise e Desenvolvimento de Sistemas, Discente do PIVICT, IFSP, Campus Pirituba, nadjila.tejo@aluno.ifsp.edu.br

² Professor Titular da Universidade Militar Nueva Granada, Líder Grupo de Pesquisa TIGUM, Campus Bogotá, leonardo.ramirez@unimilitar.edu.co

³ Professor do curso de Redes de Computadores, ISFP, Campus Pirituba, felipe.basile@ifsp.edu.br

⁴ Grupo de Informática e Tecnologia em Educação e Sociedade, GITES

Área de conhecimento (Tabela CNPq): 1.03.03.04-9 Sistemas de Informação

Apresentado no

10º Congresso de Inovação, Ciência e Tecnologia do IFSP ou no 4º Congresso de Pós-Graduação do IFSP, 27 e 28 de novembro de 2019- Sorocaba-SP, Brasil

RESUMO: A telemedicina melhorou a conduta profissional na área da saúde por meio do gerenciamento dos dados do paciente que permite a melhor tomada de decisão médica. Contudo, demanda estratégias contra incidentes de crimes em sistemas de computação em telemedicina se acrescenta cada dia. O trabalho é uma revisão narrativa realizada desde as bases de dados de Google Acadêmico e Pubmed. A estratégia forense computacional pode esclarecer os ataques por meio da simulado no ambiente virtual de configurações de hardware e soluções de software utilizadas em sistemas de informações gerenciais aplicadas na telemedicina na qual, determina a dinâmica do crime, materialidade e autoria do ato. Assim, a forense computacional é uma estratégia eficaz o processo investigativo e resolutivo dos crimes cibernéticos em telemedicina.

PALAVRAS-CHAVE: confidencialidade; crimes; incidentes; roubo de dados; segurança computacional; telemedicina.

COMPUTATIONAL FORENSIC AS A STRATEGY FOR INVESTIGATION OF CYBERCRIME INCIDENTS IN TELEMEDICINE

ABSTRACT: Telemedicine has improved professional conduct in healthcare by patient data management that enables better medical decision making. However, demand strategies against crime incidents in telemedicine computing systems if adds up every day. The paper is a narrative review performed from the Google Scholar and Pubmed databases. Computational forensic strategy can clarify the attacks by simulating the virtual environment of hardware configurations and software solutions used in management information systems applied in telemedicine in which it determines the dynamics of crime, materiality and authorship of the act. Thus, computational forensics is an effective strategy investigative and resolving process of cybercrimes in telemedicine.

KEYWORDS: confidentiality; cybercrime; incidents; computer security; data theft; telemedicine.

INTRODUÇÃO

A telemedicina usa tecnologia de informação e comunicação pela oferta de serviços de cuidados com a saúde com a ampliação da atenção e cobertura, o fator crítico é a distância (MALDONADO, 2016). A telemedicina se relaciona à tecnologia da informação de saúde na aplicação de registros médicos eletrônicos nos sistemas de informação em saúde (BASILE et al.; 2016). O registro médico em papel abriu espaço para o armazenamento eletrônico e compartilhamento de dados para melhorar o

atendimento (JARRETT, 2017). Os registros eletrônicos possuem desafios e problemas de segurança da tecnologia da informação (BABULAK, JIN, KIM, 2014). A gestão de segurança em telemedicina trouxe preocupação devido a demanda legislação e regulamentos para proteção dos dados caso ocorra um incidente (COVENTRY; BRANLEY, 2018). A transmissão de dados apresenta pontos frágeis de segurança, ainda que a integridade e autenticidade dos dados sejam asseguradas por algoritmos de criptografia (BASILE et al.; 2016). A transmissão de dados em telemedicina está na Figura 1.

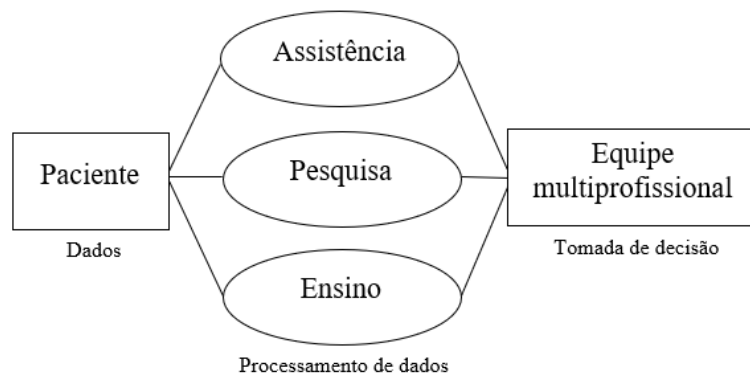


Figura 1. Transmissão de dados em telemedicina para o intercâmbio de informações entre equipes multiprofissionais para assistência, pesquisa e ensino.

A transmissão de dados em telemedicina na figura 1 mostra o intercâmbio das informações entre a equipe multiprofissional. A privacidade dos dados transmitidos garante a confidencialidade dos dados, principalmente pela demanda de segurança na conectividade (BASILE; LOPEZ; AMATE, 2019). Contudo, caso ocorra o crime cibernético, a forense computacional auxilia na investigação. A ciência forense é o conjunto de conhecimentos científicos e técnicas de diversas áreas da ciência (criminologia, computação, medicina legal, patologia, entre outras) aplicadas em conjunto para sanar a questão a ser respondida, na qual, dão suporte às investigações relativas à justiça civil e criminal como a busca da verdade (VALLIM, 2017). A forense computacional desenvolve hipóteses e responde a perguntas sobre o incidente/crime com a coleta de provas que auxilia o esclarecimento do incidente (CARRIER; SPAFFORD, 2004). A forense computacional preserva a integridade dos dados (KENT et al., 2006).

MATERIAL E MÉTODOS

A presente revisão narrativa é a etapa inicial do projeto aprovado pelo PIVICT, na qual, visa o entendimento da importância da forense computacional na solução de crimes cibernéticos. Além de destacar a importância da investigação estruturada cientificamente, para resolução de crimes cibernéticos que ocorrem no exercício da telemedicina. Basicamente, o projeto de iniciação científica pode ser dividido em três etapas consecutivas:

A primeira etapa, retratará pesquisa exploratória em base de dados multidisciplinar/interdisciplinar correlacionando segurança, telemedicina, computação, forense computacional. O início das pesquisas procurou investigar a base Pubmed, o motor de buscas do Google Acadêmico, onde foram digitadas as palavras-chave: “computational forensics/forense computacional”, “cybersecurity/cibersegurança”, “telemedicine/telemedicina”. A revisão utilizou livros da área de forense computacional. A pesquisa ocorreu nos meses de julho e agosto do ano de 2019. A seleção inicial dos estudos permeou a leitura do título e resumo, após a etapa os artigos foram lidos na íntegra.

A segunda etapa destacará o levantamento das ferramentas tecnológicas que configuram hardware e uso de software no processo de investigação, coleta e análise do relatório do incidente de roubo de dados em telemedicina.

A terceira etapa permitirá o trabalho colaborativo (BRASIL-COLÔMBIA) com a criação de perímetro digital do exercício da telemedicina, e consequente simulação do ataque a proteção perimetral digital. A ambientação tecnológica, permitirá a avaliação da eficácia das ferramentas de rede a serem utilizadas para investigação forense computacional em telemedicina.

RESULTADOS E DISCUSSÃO

O presente trabalho ilustra a necessidade de gestão da segurança da informação em telemedicina e introduz o estudo da forense computacional com estratégia para tratamento de incidentes pós crime cibernético. A tecnologia melhorou a prestação de cuidados na área da saúde (COVENTRY; BRANLEY, 2018). Os dispositivos médicos aumentam a capacidade de comunicação entre os sistemas de monitoramento remoto, eles transmitem informações clínicas dos pacientes para os médicos. O paciente pode ter algum acometimento identificado e é contatado para determinada ação. Por exemplo, os dispositivos cardíacos podem transmitir dados sobre insuficiência cardíaca e para executar uma possível ação no paciente. A tecnologia melhora o atendimento ao paciente, mas tem possíveis riscos à segurança dos dados do paciente (KRAMER, 2017). O aumento da conectividade a redes de computadores expôs dispositivos médicos a novas vulnerabilidades de segurança cibernética. A saúde é atraente para o cibercrime por duas razões fundamentais: fonte valiosa de dados e segurança ineficiente. A segurança cibernética é fundamental para a segurança do paciente (COVENTRY; BRANLEY, 2018). A segurança cibernética demanda a administração da informação para evitar roubo de informações protegidas de saúde do paciente. As violações da segurança incluem sequestros de registros de saúde demandando resgate (JARRETT, 2017), roubo de informações sobre saúde e ataques a dispositivos médicos implantados. Os incidentes de violações podem reduzir a confiança do paciente, prejudicam os sistemas de saúde e ameaçar a vida (COVENTRY; BRANLEY, 2018). Caso ocorra o incidente de roubo de dados, a forense computacional auxilia na elucidação do crime cibernético. A perícia forense computacional consiste em procedimentos e metodologias que investigam e armazenam evidências para responder se houve ou não o crime (QUEIROZ; VARGAS, 2010). Os autores tem perspectivas diferentes quanto às etapas da forense computacional, contudo podemos destacar de modo adaptado essas etapas por Vallim (2017) na Figura 2.

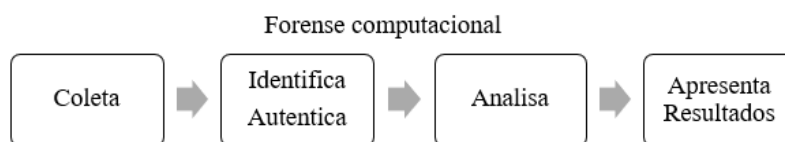


Figura 2. Etapas da Forense Computacional.

A forense computacional ilustrada na figura 2 utiliza métodos científicos para atuar na busca da verdade científica e objetividade, conforme visto anteriormente, possibilitando a produção de laudo para a apresentação da evidência digital com validade probatória em juízo. A etapa inicia com a preparação do planejamento do que deverá ser realizado durante o processo. A perícia forense identifica o ambiente físico como a conectividade da rede e digital como tablets e celulares. A preservação das evidências permite que a mesma que não sejam perdidas e não seja contaminada pelo perito de acordo com o princípio de troca de Locard. A coleta e validação dos dados permite a extração das evidências pode ser com o sistema ligado na busca de singularidades do sistema operacional, processos executados ou em standby e dispositivos de entrada e saída, ou com o sistema desligado na extração física possibilitando a recuperação de informações deletadas ou lógica com informações visíveis das provas. Após a coleta dos dados, a análise dos dados ou metadados (estes ajudam a criar a linha do tempo dos registros de eventos do arquivo: tempo de modificação, tempo de acesso, tempo de alteração e criação) em laboratório (VALLIM, 2017) de provas como os computadores pessoais, laptops, servidores, estações de trabalho ou outras mídias eletrônicas, bem como o processamento dos dados (QUEIROZ; VARGAS, 2010) identifica vestígios verdadeiros, forjados ou ilusórios. A análise forense das evidências permite a realização de exames, reconstrução da linha do tempo, identificando das ações realizadas no dispositivo eletrônico, para permitir o reconhecimento de possíveis métodos antiforenses (como a alteração de metadados), bem como, a identificação dos envolvidos (VALLIM, 2017). Após essa etapa, o profissional que irá investigar o caso pode desenvolver hipóteses sobre eventos anteriores na cena do crime (CARRIER; SPAFFORD, 2004). As etapas da forense computacional desencadeiam na estrutura baseada em eventos que podem desenvolver hipóteses e responder a perguntas sobre um incidente ou crime. As hipóteses são desenvolvidas coletando provas que podem auxiliar no esclarecimento do incidente (CARRIER; SPAFFORD, 2004). A cadeia de custódia contribui para manter e documentar a história cronológica da evidência são provenientes do procedimento investigativo, na qual, podem ser expressos no laudo pericial emitido pelo perito judicial, laudo oficial, parecer técnico emitido pelo

assistente técnico ou relatório técnico emitido pelo perito extrajudicial (VALLIM, 2017) que previamente arrecadou o dispositivo que contém a evidência digital, autenticou o dispositivo arrecadado, analisou o dado arrecadado, sem modificá-lo, identificou o dispositivo a ser arrecadado e apresentou eventuais resultados, de forma rastreável, contra eventuais alterações (SANTANA; SANTOS, RAMOS, 2017). A perícia prova a autenticidade do objeto digital pelas técnicas de identificação de adulteração digital como na marca d'água falsa, fotos alteradas e falsificadas que geram um novo arquivo de correspondência convincente (POPESCU; FARID, 2004). O investigador forense computacional encontra casos em que o alvo é uma máquina virtual ou conjunto de máquinas virtuais (HAY; NANCE, 2008). Os peritos terão ferramentas de software comercial ou open source e hardware como bloqueadores de escrita, duplicação de mídias, aquisição segura e adequada das evidências e sanitização das mídias para serem usadas em outras perícias sem fragmentos anteriores (VALLIM, 2017). De acordo com o Centro de Estudos, Resposta e Tratamento de Incidentes de Segurança no Brasil (CERT), 676.514 incidentes foram reportados ao CERT no Brasil em 2018 (CERT, 2019). A figura 3 ilustra como a forense computacional pode auxiliar a telemedicina no processo investigativo.

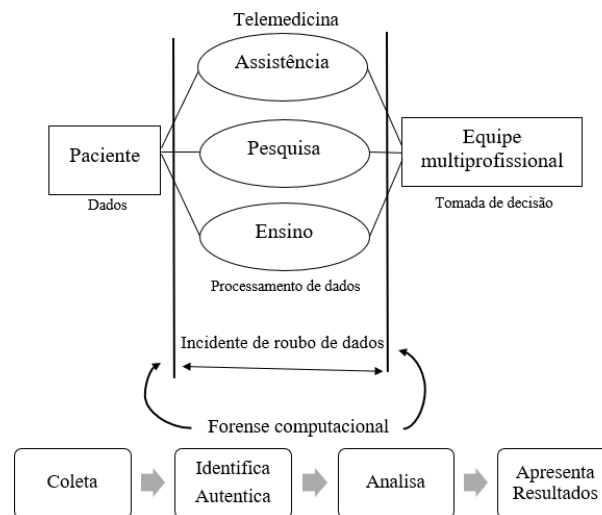


Figura 3. Processo investigativo da forense computacional no incidente de roubo de dados em telemedicina.

A forense computacional pode auxiliar a telemedicina mediante um incidente de roubo de dados por meio do processo investigativo, como ilustrado na figura 3. O investigador forense computacional verifica o aumento da complexidade dos casos e o número de incidentes de roubo de dados. A complexidade dos casos está crescendo porque os alvos forenses envolvem mais de um computador e possuem centenas de gigabytes ou terabytes de armazenamento (RICHARD III; ROUSSEV, 2006). O número de incidentes de ataque é motivado pelo ganho financeiro por serem dados muito valiosos. Outros ataques são motivados por ganhos políticos ou até mesmo pela guerra cibernética. Os documentos extraviados ou roubado podem expor centenas de pacientes a uma possível violação, pois, as informações eletrônicas estão disponíveis em várias redes e uma violação de privacidade tem o potencial de afetar milhões de pessoas (COVENTRY; BRANLEY, 2018). Nos EUA, a Lei de Portabilidade e Responsabilidade em Seguros de Saúde de 1996 garante a proteção de informações eletrônicas de saúde. O Regulamento Geral de Proteção de Dados de 2018 visa a privacidade de dados na Europa (COVENTRY; BRANLEY, 2018). O Brasil precisa avançar nas legislações e regulamentos que asseguraram a proteção dos dados. As leis Lei Nº 13.853 de 2019 e Nº 13.709 de 2018 que delimita a Lei Geral de Proteção de Dados Pessoais citam a proteção dos dados na área da saúde. Contudo, as leis necessitam de maior detalhamento para a conduta na telemedicina.

CONCLUSÕES

A forense computacional esclarece o crime cibernético em telemedicina pela determinação da dinâmica do crime, materialidade e autoria do ato. A forense computacional coleta a evidência digital, identifica a autenticidade dos dados arrecadados, analisa o dado coletado sem alterá-lo; identifica o

dispositivo a ser arrecadado e apresentação de eventuais resultados para a resolução das hipóteses do crime. A telemedicina acessa informações de saúde do paciente para assegurar a assistência médica, a confidencialidade dos dados de saúde transmitidos objetiva a segurança da informação.

A sequência dos estudos deverá continuar a pesquisa exploratória sobre telemedicina, e forense computacional, considerando o enfoque em ferramentas de software, e o desenvolvimento de perímetro digital internacional entre Brasil e Colômbia para simulação do ataque a proteção perimetral digital em uma rede de telemedicina. Portanto, tais estudos buscarão respostas para a observação de que forense computacional pode ser utilizada como estratégia para o esclarecimento de incidentes cibernéticos para coleta de evidências que ajudem na investigação.

AGRADECIMENTOS

Agradecimento ao IFSP *Campus* Pirituba pelo suporte no desenvolvimento do projeto e para PIVICT pela viabilização da iniciação científica. Agradecemos ao professor Leonardo Juan Ramirez Lopez na colaboração do ambiente virtual internacional.

REFERÊNCIAS

BASILE, F.R.M. et al. Segurança de transferência de dados em Telessaúde e Telemedicina. In: Proteção à privacidade e acesso às informações em saúde: tecnologias, direitos e ética. 2016. p. 279-298.

BASILE, F. R. M.; LOPEZ, L. J. R.; AMATE, F. C. Método para realizar copias de seguridad de imágenes médicas basado en tareas automatizadas. JINT Journal of Industrial Neo-Technologies, v. 6, n. 1, p. 26-33, 2019.

BABULAK, E.; JIN, M.; KIM, Y.S. Future e-Health, QoS Provision and Cybersecurity Challenges. Journal of the Institute of Industrial Applications Engineers, v.2, n.3, p.113–121, 2014.

CARRIER, B.; SPAFFORD, E. H. An event-based digital forensic investigation framework. In: Proceedings of the Fourth Digital Forensics Research Workshop. 2004. p. 11-13.

CENTRO DE ESTUDOS, RESPOSTA E TRATAMENTO DE INCIDENTES DE SEGURANÇA NO BRASIL. Incidentes Reportados ao CERT.br - Janeiro a Dezembro de 2018. Disponível em: < <https://www.cert.br/stats/incidentes/2018-jan-dec/tipos-ataque.html>>. Acesso em: 24 ago 2019.

COVENTRY, L.; BRANLEY, D. Cybersecurity in healthcare: A narrative review of trends, threats and ways forward. Maturitas, n.113, p.48–52, 2018.

HAY, B.; NANCE, K. Forensics examination of volatile system data using virtual introspection. ACM SIGOPS Operating Systems Review, v. 42, n. 3, p. 74-82, 2008.

JARRETT, M.P. Cybersecurity—A Serious Patient Care Concern. JAMA, v.318 n.14, p. 1319-1320, 2017.

Kent, K.; Chevalier, S.; Grance, T.; Dang, H. Guide to integrating forensic techniques into incident response. NIST Special Publications, n. 800-86, 2006. 121 p.

KRAMER, D.B. Cybersecurity Concerns and Medical Devices: Lessons From a Pacemaker Advisory. JAMA, v.318 n.21, p.2077-2078, 2017.

MALDONADO, J, M. S. V.; MARQUES, A. B.; CRUZ, A. Telemedicina: desafios à sua difusão no Brasil. Cadernos de Saúde Pública, Rio de Janeiro, v. 32, supl. 2, e00155615, 2016.

POPESCU, A.C.; FARID, H. Statistical tools for digital forensics. In: International Workshop on Information Hiding. Springer, Berlin, Heidelberg, 2004. p. 128-147.

QUEIROZ, C.; VARGAS, R. Investigação e perícia forense computacional: certificações, leis processuais e estudos de caso. Rio de Janeiro: Brasport, 2010.

RICHARD III, G.G.; ROUSSEV, V. Next-generation digital forensics. Communications of the ACM, v. 49, n. 2, p. 76-80, 2006.

SANTANA, K.G.; OLIVEIRA, P.R.L.; RAMOS, D.S. Perícia Cibernética: a evolução do trabalho científico pericial informatizado ante aos desafios tecnológicos de ataques virtuais nos sistemas de segurança. Revista Dat@venia, v.9, n.1, p.101-111, 2017.

VALLIM, A.P.A. Forense computacional e criptografia. São Paulo: Senac São Paulo, 2017.