MODELO PARA PLANEJAMENTO E DESENVOLVIMENTO DE CADEIA DE CUSTÓDIA DE FORENSE DIGITAL EM CENÁRIOS QUE ENVOLVAM DISPOSITIVOS IOT

Guilherme Schneider [1*], Avelino Francisco Zorzo [1]
[1] Pontifícia Universidade Católica do Rio Grande do Sul (PUCRS) - Porto Alegre – RS
g.schneider94@edu.pucrs.br, *avelino.zorzo@pucrs.br*

RESUMO
O mercado de Internet das Coisas (Internet of Things - IoT) vivenciou um crescimento acelerado nos últimos anos e, com a propagação destes sistemas, a Internet está hoje inundada de endereços IP relacionados a dispositivos IoT. Este trabalho mapeia o processo investigativo de Forense Digital em cenários que envolvam estes dispositivos, propondo as alterações necessárias para adaptação do modelo investigativo.
Palavras-chave: Forense Digital, Internet das Coisas.

Introdução
Para analisar e definir a autenticidade de uma evidência digital, de tal forma a não ser contestada em um tribunal, o processo investigativo precisa ser planejado, de modo a estabelecer a documentação cronológica que registre a sequência de ações - cadeia de custódia - das investigações. Diversos autores fazem este apontamento como fator crítico para a condução de investigações em cenários que envolvam dispositivos IoT (Dawson and Akinbi 2021, Castelo Gomez et al. 2021). Por isso, este trabalho buscou mapear o processo investigativo e adaptá-lo para investigações Forense Digitais no contexto IoT.

Objetivos
Este trabalho tem como objetivo apresentar uma metodologia forense para auxiliar a obtenção de evidências e a construção da cadeia de custódia em investigações Forense Digitais sobre cenários que envolvam dispositivos IoT.

Métodos
Este estudo foi definido em 3 etapas. Sendo a primeira de carácter exploratório, tendo como objetivo investigar os modelos de perícia digital tradicionais e traçar um comparativo quanto aos fatores que afetariam as investigações forense quando aplicados no contexto IoT. Na segunda etapa, buscou-se adequar o processo investigativo, propondo as alterações necessárias no fluxo de trabalho para caracterização de um modelo investigativo adaptado ao cenário IoT. Por fim, a última etapa tem como o objetivo avaliar o modelo proposto em entrevista por especialistas.

Resultados e Discussão
Os resultados preliminares indicam a necessidade de um modelo investigativo adaptado com alto fator de planejamento. Nesse sentido, o modelo foi organizado em 3 fases: Planejamento, Execução e Conclusão, onde cada fase é composta por diferentes etapas com objetivos específicos. A principal contribuição deste estudo está associada à fase de planejamento, constituída pelas etapas de pré-investigação e identificação. A partir delas, define-se um plano de ação com o objetivo de otimizar o processo investigativo e gerenciar a cadeia de custódia.

Conclusão
A heterogeneidade de dados, dispositivos e protocolos de comunicação afetam diretamente o processo investigativo do contexto IoT. Nesse sentido, o presente trabalho apresenta uma metodologia forense com maior ênfase na fase de planejamento, indicando melhoria significativa no planejamento e construção de cadeia de custódia em cenários IoT.

Referências bibliográficas
DAWSON, Liam; AKINBI, Alex. Challenges and opportunities for wearable IoT forensics: TomTom Spark 3 as a case study. **Forensic Science International: Reports**, v. 3, p. 100198, 2021.
CASTELO GÓMEZ, Juan Manuel et al. A context-centered methodology for IoT forensic investigations. **International Journal of Information Security**, v. 20, p. 647-673, 2021.