Modelo Integrado para Forense Computacional em Cenários Envolvendo Aplicações IoT*

Guilherme Schneider[1], Avelino Francisco Zorzo[1], Roben Castagna Lunardi[2]

[1]Pontifícia Universidade Católica do Rio Grande do Sul (PUCRS)
Porto Alegre – RS – Brazil

[2]Instituto Federal de Educação, Ciência e Tecnologia do Rio Grande do Sul (IFRS)
Porto Alegre – RS – Brazil

g.schneider94@edu.pucrs.br, avelino.zorzo@pucrs.br,
roben.lunardi@restinga.ifrs.edu.br

Abstract. *The heterogeneity of data, devices, and communication protocols within the Internet of Things (IoT) domain significantly affects the investigative process of Computer Forensics. This study focuses on analyzing the distinctive features of scenarios like smart homes, smart offices, and smart buildings to propose an investigative model tailored to the IoT context. The effectiveness of the proposed model was assessed by Digital Forensics experts using a qualitative approach based on the technology acceptance model (TAM). The evaluation results demonstrate that the specialists found the model to be highly applicable and emphasize the necessity for greater investment in the planning stages of research conducted in intelligent environments.*

Resumo. *A heterogeneidade de dados, dispositivos e protocolos de comunicação relacionados ao domínio Internet of Things (IoT) estão afetando diretamente o processo investigativo da Forense Computacional. Nesse sentido, este trabalho tem como objetivo analisar características de cenários como smart homes, smart offices e smart building para propor um modelo investigativo adaptado ao contexto IoT. A proposta foi avaliada por especialistas em Forense Computacional sobre abordagem qualitativa baseada no modelo de aceitação de tecnologia (TAM). Os resultados da avaliação indicam a adesão do modelo pelos especialistas e a necessidade de maior investimento nas etapas de planejamento das investigações executadas sobre ambientes inteligentes.*

1. Introdução

A Forense Computacional está relacionada ao processo de aplicação de métodos científicos para adquirir e analisar informações armazenadas em mídias digitais para compreender os eventos relacionados a determinado incidente [OliveiraJr et al. 2020]. Stoyanova *et al.* [Stoyanova et al. 2020] afirmam que a área de Forense em IoT pode ser considerada uma subdivisão da Forense Digital tradicional. Embora ambas as disciplinas compartilhem o objetivo de identificar e extrair informações de maneira legal, é importante

*O presente trabalho foi financiado por subsídios concedidos pela Chamada INCT – MCTI/CNPq/CAPES/FAPs nº 16/2014; CAPES (Coordenação de Aperfeiçoamento de Pessoal de Nível Superior - Código de financiamento 001), CNPq (Conselho Nacional de Pesquisa Científica - 06250/2021-7) e FAPERGS (Fundação de Amparo a Pesquisa do Estado do Rio Grande do Sul - 17/2551-0000520-1). Ainda, recebeu apoio da PUCRS e do IFRS.

ressaltar que enfrentam desafios distintos. Diferentemente da Forense Digital tradicional, que concentra-se em examinar computadores, *smartphones*, servidores e *gateways*, a Forense em IoT lida com fontes de evidência de natureza mais abrangente. Isso inclui não apenas dispositivos tradicionais, mas também veículos e semáforos inteligentes, sistemas de monitoramento de bebês ou pacientes, e até mesmo dispositivos médicos implantados em seres humanos ou animais [Stoyanova et al. 2020]. Ainda, é pertinente observar que os dados de interesse forense podem ser coletados a partir de uma variedade diversificada de fontes. Isso engloba não apenas dispositivos mas também redes internas, como *firewalls* e roteadores, e serviços de armazenamento em nuvem [Yang et al. 2020].

Além disso, para analisar e definir a autenticidade de uma evidência digital, o processo investigativo precisa ser planejado, de modo a estabelecer uma documentação cronológica que registra a cadeia de custódia das investigações [Prado et al. 2015]. Esta documentação indica todas as ações executadas durante a investigação - junto de seus responsáveis - de tal forma a possibilitar a rastreabilidade probatória do processo investigativo. Neste sentido, a otimização do processo investigativo requer uma pesquisa aprofundada para validação dos dispositivos de interesse forense e definição de quais partes dos dados coletados são necessários examinar [Quick and Choo 2018]. Portanto, o processo investigativo demanda modelos de planejamento para lidar adequadamente com a complexividade das investigações Forense em IoT. Diversos trabalhos fazem este apontamento como fator crítico para a condução de investigações em cenários IoT [Dawson and Akinbi 2021, Castelo Gómez et al. 2021, Qatawneh et al. 2019, Stoyanova et al. 2020, Lutta et al. 2021]. Apesar de haver modelos propostos recentemente, ainda são resultados de abordagens experimentais e por consequência muito específicos, não podendo servir como um modelo de investigação Forense IoT comum e abrangente.

Por isso, este trabalho busca mapear o processo investigativo estabelecido na Forense Computacional tradicional, propondo alterações necessárias no fluxo de trabalho para caracterização de um modelo abrangente adaptado a cenários que envolvam aplicações IoT. Esta proposta foi avaliada por especialistas, utilizando uma prova de conceito desenvolvida para um estudo de viabilidade. Os resultados obtidos indicam que a proposta foi amplamente aceita em termos de utilidade percebida pelos especialistas, resultando em melhorias na documentação e no planejamento das investigações. Nesse sentido, destaca-se como a principal contribuição deste trabalho a proposição de uma fase de **Planejamento**, que compreende a etapa de *pré-investigação* proposta pelos autores e a adaptação da etapa de *identificação*. A partir dessas etapas, os autores propõem a elaboração de um plano de ação que objetiva gerenciar o processo investigativo.

2. Trabalhos Relacionados

Trabalhos que buscam modelar o processo investigativo vêm sendo publicados nos últimos anos, no entanto as propostas direcionadas ao domínio IoT ainda carecem de desenvolvimento e validação. Em 2013, Ayers *et al.* descrevem de forma detalhada as etapas de identificação, aquisição, exame/análise e documentação do processo investigativo. Porém, apesar de fornecer diretrizes importantes para a Forense Computacional, o modelo está orientado somente à dispositivos móveis [Ayers et al. 2013]. Contudo, Kohn *et al.* apresentam em seu estudo uma discussão ampla de diversas propostas [Beebe and Clark 2005, Carrier and Spafford 2004, Casey 2001, Cohen 2009, Lee et al. 2001, Tan 2001] utilizadas em investigações de Forense Computacional. Neste

estudo, os autores integram os modelos analisados para o desenvolvimento de sua metodologia [Kohn et al. 2013]. Porém, a proposta não considera as necessidades estabelecidas pelo domínio IoT, quanto a heterogeneidade de dispositivos, protocolos de comunicação e armazenamento em nuvem.

Por outro lado, Qatawneh *et al.* estabelecem um modelo geral para Forense Computacional em IoT [Qatawneh et al. 2019]. Sua principal contribuição está relacionada à etapa de *pré-investigação* e ao processo de compartilhamento das evidências com entidades remotas, porém o modelo adaptado não foi avaliado. Entretanto, Li *et al.* avaliam sua proposta de modelo em um estudo de caso sobre dispositivos Amazon Echo. O modelo classifica os dispositivos IoT como: alvo, ferramenta ou testemunha ao iniciar a investigação. Este procedimento facilita o mapeamento do cenário e apoia os investigadores na definição dos procedimentos a serem aplicados sobre determinado dispositivo [Li et al. 2019]. Apesar de trazer um discussão importante, o cenário analisado fica limitado aos dispositivos Amazon Echo.

Neste sentido, as propostas de modelos investigativos publicadas direcionam-se somente a uma gama específica de dispositivos IoT, focando suas contribuições principalmente às etapas de *aquisição* e *análise* dos dados - fase definida como **Execução** neste trabalho. Além disso, nenhum trabalho encontrado descreve métodos para construção de uma estratégia investigativa que considere cenários complexos que envolvam tanto dispositivos IoT como outras mídias digitais. Por isso, esta proposta busca direcionar seus esforços principalmente à fase de **Planejamento**, com o objetivo de gerar os mecanismos necessários para o gerenciamento do processo investigativo e construção de cadeia de custódia em ambientes inteligentes, como *smart homes, smart offices* e *smart building*.

3. Modelo Proposto

Com o objetivo de desenvolver uma metodologia forense que possa auxiliar na obtenção de evidências e na construção de uma cadeia de custódia em cenários que envolvam dispositivos IoT, o presente modelo propõe uma organização do processo investigativo em três fases distintas: **Planejamento**, **Execução** e **Conclusão**. A Figura 1 apresenta de forma esquemática as três fases do modelo proposto, destacando suas respectivas etapas e as conexões entre as mesmas.

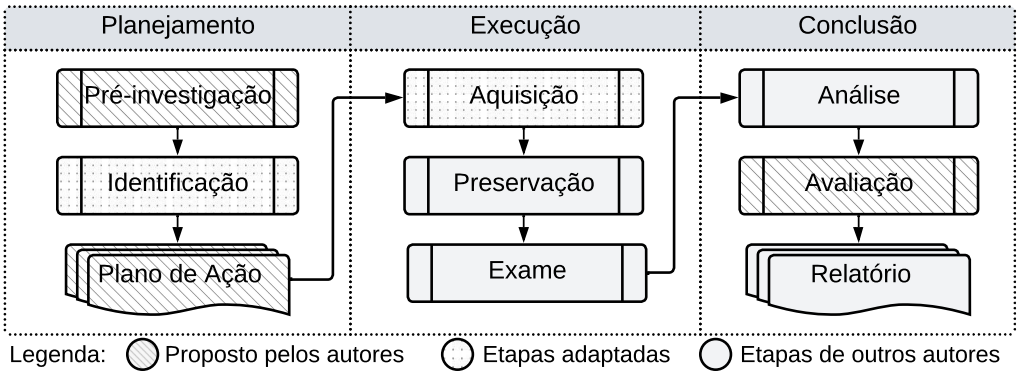

Figura 1. Proposta de modelo integrado para Forense Computacional

A principal contribuição desta proposta reside na sua estruturação modular em três fases, assim como na elaboração de um plano de ação durante a fase de **Planeja-**

mento. O plano de ação é resultado da reestruturação da etapa de identificação descrita na presente proposta. Na Figura 1, foram identificadas as etapas propostas pelos autores e etapas adaptadas durante a elaboração do modelo. Nesse sentido, os ganhos relacionados a estruturação da abordagem em fases permite a utilização do modelo em metodologias híbridas, tanto em conjunto com ferramentas de inteligência artificial que viabilizem a automatização de determinadas tarefas, quanto em combinação com outros modelos de Forense Computacional. Além disso, o investimento significativo em planejamento resulta em uma classificação detalhada das potenciais fontes de evidência. Esta proposta foi desenvolvido de acordo com as diretrizes estabelecidas na norma ISO/IEC 27037:2012 - Diretrizes para identificação, coleta, aquisição e preservação de evidências digitais [ISO/IEC 2012], e foi adaptado para o contexto da Internet das Coisas (IoT) com base em contribuições provenientes de estudos anteriores focados nesse contexto [Li et al. 2019, Salama et al. 2022, Montasari et al. 2020, Stolojescu-Crisan et al. 2021, Lombardi et al. 2021, Achar 2022, Rizal et al. 2018, Reith et al. 2002]. Além disso, foram considerados aspectos descritos no Procedimento Operacional Padrão para a Forense Computacional, publicado pelo Ministério da Justiça Brasileiro [Figueiredo et al. 2013].

3.1. Planejamento

A fase de **Planejamento** tem como objetivo a delimitação dos elementos relacionados à coordenação das investigações, a identificação dos responsáveis e possíveis fontes de evidências. Nessa fase, realiza-se a elaboração de um plano de ação que será executado nas etapas subsequentes de *aquisição* e *exame* dos dados. Além disso, busca-se estabelecer antecipadamente a atribuição de responsabilidades para cada atividade, visando à estruturação da documentação de cadeia de custódia. A fase de **Planejamento** é composta por duas etapas distintas: *pré-investigação* e *identificação*, conforme ilustrado na Figura 1.

3.1.1. Pré-Investigação

A etapa de *pré-investigação* da se inicia com a solicitação e recebimento da documentação pertinente ao caso ou incidente em questão. Essa fase tem como objetivo documentar os responsáveis pela condução da investigação. Em primeiro lugar, um encarregado geral - oficial designado para o caso - é selecionado para liderar a investigação. Esse profissional deve ser um membro com conhecimento abrangente das exigências legais, técnicas e de coordenação das investigações. Sua responsabilidade é analisar a documentação relacionada ao caso e indicar a equipe de apoio para auxiliar na identificação e elaboração do plano de ação. Além disso, o encarregado geral também conduz a fase de **Conclusão** da investigação, realizando as etapas de *análise* e *avaliação* final.

No entanto, devido a heterogeneidade da arquitetura de IoT, é necessário considerar a possibilidade de envolver especialistas de áreas relacionadas ao incidente, tais como saúde, transporte, cidades inteligentes, entre outras. Esses especialistas podem ser terceiros externos ou profissionais vinculados ao contexto investigado, como o responsável pela tecnologia da informação (TI) na organização em questão. A inclusão de especialistas externos no caso visa fornecer suporte adicional ao processo investigativo, abordando questões específicas relacionadas ao contexto do caso e auxiliando na etapa de *análise* dos dados [Salama et al. 2022]. Todas as definições devem ser associadas a documentação referente ao caso para fins de auditabilidade [ISO/IEC 2012].

3.1.2. Identificação

A etapa de *identificação* tem como objetivo principal a definição e classificação das potenciais fontes de evidências presentes no ambiente. Essas informações são utilizadas para a elaboração do plano de ação, conforme ilustrado na Figura 2. Por exemplo, em sistemas de casas inteligentes, é possível encontrar uma ampla variedade de dispositivos que enviam dados para *hubs* de automação. Esses dispositivos incluem sensores de controle de temperatura, iluminação, energia elétrica, acesso (como portas, portões e garagem), entre outros [Stolojescu-Crisan et al. 2021]. No contexto desses casos, a utilização de soluções como *Building Information Modeling* (BIM) pode auxiliar os investigadores na identificação das possíveis fontes de evidências. Com base nas informações presentes em uma representação digital (BIM), os investigadores conseguem determinar a origem dos dados, onde estão armazenados e em qual formato [Montasari et al. 2020]. No entanto, em alguns cenários pode haver somente um dispositivo inteligente, ou mesmo dispositivos IoT heterogêneos comunicando dados entre diferentes aplicações. Nessas circunstâncias, cabe aos investigadores analisar o cenário, confrontando a documentação relacionada ao caso para identificar as possíveis fontes de evidências.

Uma vez que possíveis fontes de evidências tenham sido identificadas, é fundamental que o perito documente todas as informações relevantes relacionadas a elas e as compare com os detalhes do caso ou incidente em questão, com o objetivo de classificá-las dentro do contexto da investigação. As fontes de evidências relacionadas à IoT devem ser classificadas em três categorias: alvo, ferramenta e testemunha [Li et al. 2019].

Dispositivos classificados como alvos são aqueles que foram foco de ataques cibernéticos, nos quais suas funcionalidades e/ou vulnerabilidades foram exploradas. Nestes cenários, os dispositivos representam o ponto central da investigação. Por outro lado, dispositivos classificados como ferramentas também tiveram suas funcionalidades e/ou vulnerabilidades exploradas, mas em um contexto no qual foram utilizados para atacar outro alvo. Um exemplo disso são os ataques distribuídos de negação de serviço, nos quais vários dispositivos são usados em conjunto para enviar solicitações a um sistema alvo. Por fim, dispositivos classificados como testemunhas são aqueles presentes no cenário analisado que podem conter dados de interesse investigativo relacionados ao indivíduo acusado ou ao incidente em questão. Esta classificação de contexto das fontes de evidências possui baixo custo operacional e suporta tanto a etapa de *análise* das evidências quanto a seleção da abordagem adequada para a aquisição de dados em dispositivos IoT.

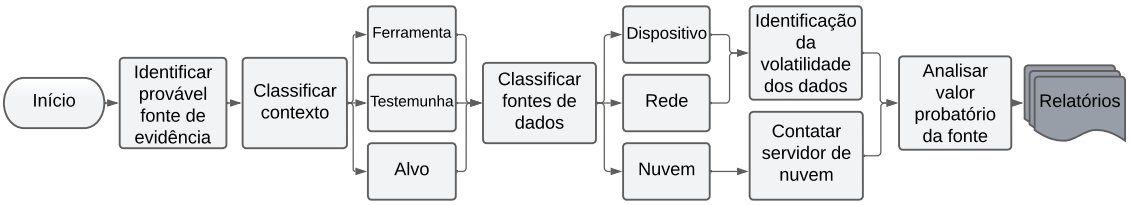

Figura 2. Fluxo de identificação de possíveis fontes de evidências.

Posteriormente, o perito deve classificar os tipos de fontes de evidências de acordo com três camadas da arquitetura da IoT: dispositivo, rede e nuvem [Lombardi et al. 2021, Salama et al. 2022]. É importante destacar que informações relevantes para a investigação podem estar armazenadas em mais de uma camada da aplicação IoT. No entanto, a

identificação individual das fontes de dados é necessária para dar suporte à etapa de definição das estratégias de aquisição. Nesse sentido, as abordagens para a aquisição de dados em dispositivos/sensores devem considerar os recursos disponíveis, as limitações existentes e os tipos de dados presentes na fonte. Por sua vez, as estratégias para a aquisição de dados na camada de rede requerem abordagens diferentes. Em ambos os casos, no entanto, é crucial identificar a volatilidade dos dados a fim de determinar a estratégia de aquisição adequada para dispositivos/sensores e redes. Porém, essa necessidade não está presente quando a fonte de dados é a camada de nuvem [Achar 2022].

Quando uma fonte de dados é classificada como nuvem, é indicado entrar em contato com o provedor de serviços correspondente, informando as questões legais relacionadas ao caso. Esse contato busca estabelecer a cooperação entre o provedor de serviços e a equipe investigativa, como uma tentativa de garantir que os dados armazenados em servidores remotos sejam mantidos até a conclusão da investigação.

Ao término das classificações, o oficial do caso deve analisar o valor probatório das possíveis fontes, considerando as classificações de contexto e as hipóteses presentes na documentação [ISO/IEC 2012]. Esta etapa, apoia a definição do fluxo de aquisições, priorizando fontes de evidências de maior valor probatório.

3.1.3. Plano de Ação

O processo de construção do plano de ação envolve o reconhecimento dos relatórios resultantes da etapa de *identificação*, com o objetivo de definir as abordagens de aquisição, o fluxo de trabalho e os responsáveis por sua execução, conforme ilustrado na Figura 3. A definição das estratégias de aquisição de dados deve levar em consideração todas as classificações documentadas, juntamente com as demais informações obtidas sobre o dispositivo, rede ou serviço em nuvem. Caso haja falta de informações sobre as fontes de evidências, o especialista terceiro designado durante a fase de **Pré-investigação** deve ser considerado. A atuação desse especialista na etapa de definição da estratégia de aquisição proporciona o suporte necessário para obter informações sobre a infraestrutura do sistema, as técnicas de segurança aplicadas, os tipos de dados armazenados, os recursos dos dispositivos, os formatos de dados, entre outros aspectos relevantes.

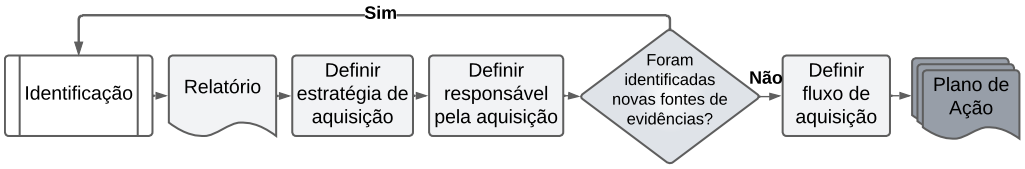

Figura 3. Definição do Plano de Ação.

Em seguida, o responsável pelo caso deve analisar e definir os responsáveis pela aquisição de dados na fonte. Essa definição deve considerar a competência técnica dos agentes envolvidos no caso, visando a alocação eficiente dos recursos humanos disponíveis na investigação e a priorização das fontes de evidências de acordo com seu valor probatório [ISO/IEC 2012]. Ambos os procedimentos de priorização e definição dos responsáveis, têm como objetivo otimizar o fluxo de aquisição e reduzir o tempo de estada dos agentes no cenário do crime.

Após a identificação de todas as fontes de evidências possíveis e a definição dos responsáveis pela *aquisição* de dados, o oficial encarregado do caso estabelece o fluxo de execução das estratégias, registrando previamente o procedimento da equipe durante a etapa de *aquisição*. Portanto, é fundamental que toda a documentação gerada na fase de planejamento esteja devidamente vinculada ao plano de ação, a fim de fornecer controle e facilitar a consulta durante a subsequente fase de **Execução**.

3.2. Execução

A fase de **Execução** tem como objetivo validar os dispositivos identificados como possíveis fontes de evidências e obter dados relevantes para a investigação. Além disso, dados de interesse são filtrados e preparados para posterior análise. Os resultados obtidos nessa etapa são essenciais para a correlação de evidências, a reconstrução dos eventos ocorridos. Para atingir esses objetivos, a fase de **Execução** é composta por três etapas distintas: *aquisição*, *preservação* e *exame*.

3.2.1. Aquisição

A etapa de *aquisição* de dados é conduzida de acordo com o plano de ação estabelecido, com o objetivo de obter dados brutos das fontes de evidências identificadas, conforme representado na Figura 4. Essa etapa tem início com a preparação do local do crime, onde o perímetro da investigação deve ser isolado e preservado de acordo com as diretrizes estabelecidas no Procedimento Operacional Padrão publicado pelo Ministério da Justiça Brasileiro [Figueiredo et al. 2013]. Além disso, parte do processo de preparação do local envolve verificar as condições de segurança, garantindo o bem-estar da equipe pericial. Somente os profissionais envolvidos diretamente na investigação devem ter acesso ao local. Caso haja necessidade de envolvimento de terceiros, a equipe pericial deve documentar a permissão de acesso aos especialistas designados para a investigação.

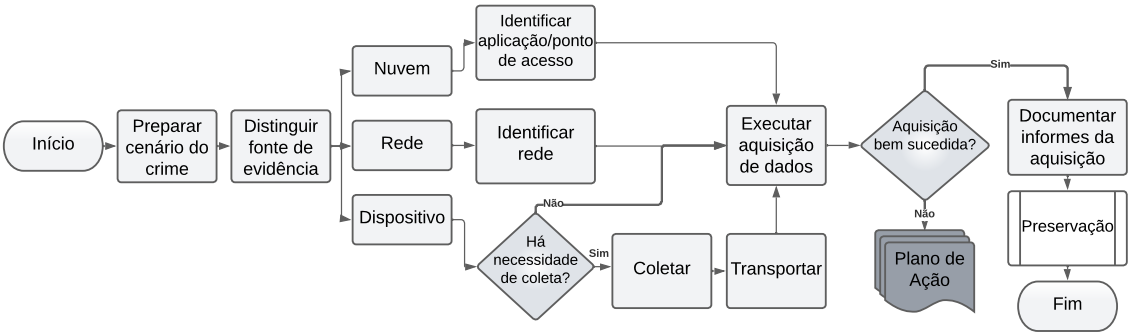

Figura 4. Etapa de aquisição de dados.

Após a preparação do local, a equipe pericial deve iniciar a aquisição dos dados de acordo com o plano de ação estabelecido. O primeiro passo é identificar a fonte de evidência conforme classificada na etapa de *identificação*. No caso de dispositivos, é necessário avaliar se precisa coletar e transportar o dispositivo para realizar a aquisição em laboratório. Essa decisão deve levar em consideração diferentes aspectos do dispositivo, como sua capacidade de armazenamento de dados não voláteis, o estado do dispositivo, a presença de criptografia completa do disco ou a possibilidade de senhas e chaves estarem presentes como dados voláteis. Além disso, é preciso considerar as exigências legais

da jurisdição aplicável e as restrições de tempo da investigação. Portanto, é recomendado priorizar a aquisição de dados no local, o que proporciona uma maior otimização e relação custo-benefício para a investigação. No caso de coleta da fonte de evidência, o perito responsável pela aquisição deve acompanhar o transporte do dispositivo, garantindo a integridade da cadeia de custódia e a documentação dos informes da aquisição [ISO/IEC 2012].

Nos casos em que a fonte de evidência é classificada como rede, é necessário identificar o tipo de rede presente na infraestrutura do local. Essa camada pode incluir diversos formatos, como *Body Area Networks (BAN), Personal Area Networks (PAN), Home/Hospital Area Networks (HAN), Local Area Networks (LAN), Wide Area Networks (WAN)*, entre outros. Em um ambiente IoT, é possível encontrar uma combinação de diferentes formatos de redes, portanto, o processo de identificação das redes é crucial para o sucesso na aquisição de dados de *log* [Rizal et al. 2018]. Por outro lado, quando as fontes de evidência são classificadas como nuvem, é primordial identificar os pontos de acesso aos dados. As ferramentas de aquisição de dados em nuvem utilizam credenciais para acessar os dados armazenados em servidores privados por meio de dispositivos móveis ou computadores. Além disso, informações gerenciadas por aplicativos em *smartphones* também podem ser adquiridas da memória do dispositivo [Achar 2022].

Diante disso, a estratégia de aquisição de dados, estabelecida durante a fase de **Planejamento**, é implementada na respectiva fonte de evidência. Após a conclusão da extração dos dados brutos, realiza-se uma avaliação prévia da aquisição para verificar sua efetividade. No caso em que não são identificados dados, procede-se à revisão do plano de ação, a fim de investigar as razões e, se necessário, estabelecer uma nova abordagem para essa fonte específica. Por outro lado, quando a aquisição é bem-sucedida, o perito responsável registra as informações relevantes do processo no relatório geral e procede à etapa de *preservação* dos dados.

3.2.2. Preservação

A etapa de *preservação* tem como objetivo assegurar a integridade e a preservação do estado original da potencial evidência. Um procedimento comumente adotado é a geração de cópia dos dados, acompanhada de um identificador único (ID) que a vincula ao item original. Esse ID é mantido ao longo do ciclo de vida da evidência durante a investigação e também é citado no relatório final. Adicionalmente, é essencial realizar uma função de verificação (*hash*) em ambas as cópias geradas para garantir sua integridade e associação ao respectivo ID. Para reforçar a autenticidade e o não-repúdio, o perito responsável deve assinar digitalmente ambas as cópias, juntamente com o valor resultante do *hash*. Esses procedimentos são documentados e anexados ao relatório geral da investigação. Essa etapa busca estabelecer os fundamentos necessários para garantir a não espoliação ou adulteração de dados nas fases subsequentes. Caso ocorram alterações inevitáveis posteriormente, o perito responsável deve registrar todas as ações adicionais, a fim de garantir a rastreabilidade da cadeia de custódia da evidência [ISO/IEC 2012].

3.2.3. Exame

A etapa de *exame* tem como objetivo identificar e filtrar os dados probatórios para a investigação, como demonstrado no fluxo na Figura 5. Nesse sentido, é necessário anali-

sar as possíveis técnicas de segurança aplicadas aos dados brutos, a fim de determinar a abordagem adequada para o *exame*. É importante ressaltar que as técnicas ou ferramentas utilizadas para examinar as evidências devem ser aplicadas exclusivamente à cópia dos dados, preservando assim a integridade da aquisição original. No processo de identificação dos dados, é necessário investigar as pastas e diretórios presentes na imagem gerada, a fim de identificar arquivos relevantes e descartar os irrelevantes para a investigação. Além disso, arquivos de interesse forense podem estar presentes na imagem gerada mesmo após terem sido deletados pelos usuários. A tentativa de identificação de arquivos deletados e dados residuais presentes na memória de um dispositivo antecede a filtragem de dados. À vista disso, o processo de filtragem dos dados tem como objetivo eliminar o chamado ”lixo digital”, que pode incluir arquivos do sistema, duplicados e outros dados que não sejam relevantes para a investigação. Além disso, o perito responsável deve classificar e agrupar os dados relacionados, visando otimizar a etapa de *análise* das evidências. Por fim, a etapa de *preservação* é executada novamente para garantir a integridade dos dados examinados.

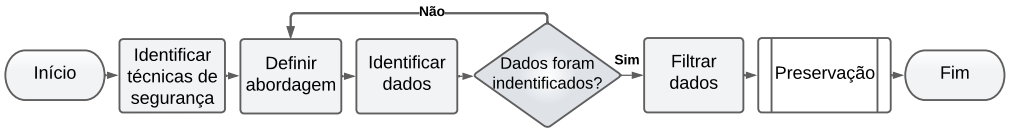

Figura 5. Exame em dados brutos

3.3. Conclusão

A fase de **Conclusão** tem como objetivo analisar e correlacionar as informações relacionadas à investigação, visando gerar as evidências necessárias para a resolução das hipóteses presentes no caso. Os resultados esperados provenientes da aplicação desta fase são detalhados no relatório final. O relatório investigativo, juntamente da documentação da cadeia de custódia, constitui os artefatos que serão discutidos em tribunal de justiça. Para tal fim, a fase de **Conclusão** é composta por duas etapas: *análise* e *avaliação*, descritas a seguir.

3.3.1. Análise

A etapa de *análise* tem como objetivo correlacionar as evidências e reconstruir a cena do crime ou os eventos associados à investigação. Seguindo as contribuições de Reith, Carr e Gunsch (2002), essa etapa deve determinar a relevância das evidências e reconstruir fragmentos de dados para formular conclusões embasadas [Reith et al. 2002]. Ainda, é fundamental que os resultados dessa etapa sejam apresentados de forma apropriada para serem discutidos em um ambiente judicial, envolvendo profissionais de diversas áreas. Desta forma, o responsável pela investigação deve responder as hipóteses do caso e reconstruir os eventos associados. É crucial que toda a construção argumentativa esteja respaldada por evidências documentadas e referenciadas com um número identificador único. Portanto, todas as provas apresentarão rastreadores que permitirão a reprodutibilidade das etapas de *aquisição* e *exame*. É importante ressaltar que, caso alguma informação conclusiva não esteja adequadamente associada a um identificador, o processo investigativo pode ser questionado e potencialmente invalidado em juízo.

3.3.2. Avaliação

A etapa de *avaliação* tem como objetivo analisar os resultados obtidos a fim de determinar o encerramento do caso e revisar a documentação gerada nas fases de **Planejamento** e **Execução**. O processo de avaliação dos resultados provenientes da *análise* busca verificar a suficiência das evidências para encerrar o caso. No caso de possíveis lacunas na construção argumentativa resultante da análise, o responsável pelo caso deve justificar a necessidade de novas identificações ou o encerramento do caso. Caso seja necessária a execução de novas identificações, o processo investigativo deve retomar a fase de planejamento, avaliando as ações tomadas desde a etapa definida para identificação de evidências. Se os resultados avaliados determinarem o encerramento do caso, antes disso, é essencial que toda a documentação produzida nas fases de **Planejamento** e **Execução** seja revisada. Devem ser checados os registros dos responsáveis pelas identificações, aquisições e exames de dados, juntamente com os números identificadores de cada evidência digital e sua cópia ”master”. Essa etapa garante novamente a reprodutibilidade do processo, além de assegurar a autenticidade e confiabilidade das evidências digitais presentes no caso [ISO/IEC 2012].

4. Estudo de Viabilidade da Proposta

Nesta seção, são abordadas as estratégias de avaliação com o objetivo de verificar a viabilidade do modelo proposto em relação aos fluxos de trabalho utilizados por especialistas em investigações forenses. Para tal propósito, optou-se por realizar uma pesquisa qualitativa, baseada no Modelo de Aceitação de Tecnologia (TAM) [Davis 1989]. O objetivo foi compreender a utilidade e a facilidade de uso do modelo proposto, a partir da percepção de especialistas e pesquisadores na área de Forense Computacional. A estratégia de amostragem utilizada foi não probabilística, mais especificamente a amostragem por conveniência seguida de *snowballing* [Goodman 1961]. Essa abordagem permitiu selecionar participantes que possuíam experiência e conhecimentos relevantes para contribuir com a pesquisa, levando em consideração critérios de conveniência e disponibilidade.

Para aplicação do estudo foram projetados uma série de instrumentos. Primeiramente, foi desenvolvida uma prova de conceito do modelo e disponibilizada em formato web em uma versão em branco e outra preenchida com resultados do desafio DFRWS Digital Forensic Challenge (2018) [Zhang et al. 2020]. Este evento é promovido por uma das principais conferências de Forense Digital. Enquanto o cenário abordado neste estudo diz respeito à simulação de uma invasão em um laboratório de drogas, envolvendo uma rede SOHO IoT. Além disso, aplicou-se um questionário com questões em escala Likert, com base nos fatores Utilidade Percebida (UP) e Facilidade de Uso Percebida (FU) do modelo TAM. Além disso, definimos uma questão relacionada ao *Net Promoter Score* (NPS) [Pradini et al. 2019], e outras três questões abertas, afim de avaliar: a visão geral dos especialistas e as dificuldades percebidas para aplicação do modelo. A análise dos dados foi fundamentado na Grounded Theory [Strauss and Corbin 1990], por meio do método de *Coding*.

Adicionalmente, foi realizado um teste piloto como etapa preliminar à execução do estudo de viabilidade da proposta. Dois pesquisadores, com uma média de experiência de 4 anos em Forense Computacional, participaram desse teste piloto e forneceram suas percepções em relação aos instrumentos utilizados. Durante o teste, não foram observados

quaisquer erros de consistência nos resultados obtidos. É importante ressaltar que os dados coletados nessa fase foram excluídos da análise dos resultados descrita a seguir.

4.1. Análise dos Resultados

Primeiramente, para identificar o perfil dos participantes do estudo, foram realizadas seis perguntas com o objetivo de obter informações sobre a área de atuação, tempo de experiência e nível de conhecimento em relação às aplicações IoT. Dos sete especialistas participantes, três indicaram atuar no campo acadêmico como professores/pesquisadores. Dois especialistas possuem ocupações profissionais como peritos/agentes de segurança, e os outros dois têm experiência tanto no ambiente acadêmico quanto no profissional da Forense Digital. O tempo médio de experiência declarado pelos entrevistados foi de sete anos e meio de atuação em Forense Digital. Já a avaliação do nível de conhecimento dos participantes sobre o contexto IoT foi realizada utilizando uma escala Likert de cinco pontos. A média geral obtida foi de 3,71, com desvio padrão de 1,27 e moda de 4. Em resumo, os dados extraídos sugerem um alto nível de conhecimento por parte dos especialista em Forense Digital em relação ao contexto da IoT. A seguir, a Tabela 1 apresenta as respostas dos sete especialistas em relação à Utilidade Percebida e à Facilidade de Uso.

Tabela 1. Resultados

Perguntas	R1	R2	R3	R4	R5	R6	R7	Moda
UP1. Facilitação do trabalho	4	4	2	4	4	4	4	**4**
UP2. Melhoria de desempenho	4	5	2	3	4	4	4	**4**
UP3. Abrangência das etapas investigativas	4	5	5	5	5	4	2	**5**
UP4. Aumento da eficácia	4	5	2	4	4	4	3	**4**
UP5. Beneficiação por maior planejamento	3	5	4	5	4	4	2	**4**
UP6. Melhoria no gerenciamento dos artefatos	4	5	3	4	5	5	4	**4/5**
UP7. Utilidade Geral	4	4	2	3	4	4	4	**4**
FU1. Clareza e compreensão	4	4	4	2	4	4	4	**4**
FU2. Facilidade na visualização das etapas	4	5	5	4	5	5	4	**5**
FU3. Facilidade em planejamento	4	5	4	3	4	5	4	**4**
FU4. Facilidade na documentação	4	5	4	4	4	5	4	**4**
FU5. Facilidade geral	4	4	4	2	4	4	4	**4**

Legenda: Discordo totalmente: 1; Discordo: 2; Neutro: 3; Concordo: 4; Concordo totalmente: 5

Ao analisar somente as questões relacionadas à Utilidade Percebida, observa-se que, de forma geral, as respostas se concentram nos rótulos de ”concordo” ou ”concordo totalmente”. Isso indica que a maioria dos especialistas considera a proposta do modelo útil para a Forense Digital em cenários envolvendo aplicações IoT. Na questão UP1, que diz respeito à facilidade de trabalho proporcionada pelo uso do modelo proposto, 85% dos especialistas indicaram o rótulo ”concordo” em suas respostas. Além disso, questões relacionadas à melhoria de desempenho e aumento da eficácia do trabalho (UP2 e UP4), 71% das respostas estão nos rótulos ”concordo” e ”concordo totalmente”, com ambas as modas sendo relacionadas ao rótulo ”concordo”. Ainda nesse contexto, é importante destacar a questão referente à abrangência da proposta em relação às etapas da Forense Digital (UP3), que foi a única questão relacionada à Utilidade Percebida com uma moda de 5. Isso indica que a maioria dos especialistas concorda totalmente com a abrangência do modelo proposto em relação aos seus próprios fluxos de trabalho na perícia digital. Além disso, os benefícios relacionados ao planejamento aprimorado e ao aprimoramento no gerenciamento dos artefatos pela utilização da proposta foram significativamente aprovados pelos especialistas. Em resumo, a questão relacionada à utilidade geral da proposta (UP7) reflete o mesmo padrão de respostas positivas.

Quanto as questões relacionadas à avaliação da Facilidade de Uso do modelo proposto, de maneira geral, esse fator também foi bem avaliado pelos participantes. Questões que dizem respeito à facilidade na visualização das etapas e na documentação (FU2 e FU4) receberam respostas predominantemente nos rótulos ”concordo” e ”concordo totalmente”. Além disso, na questão relacionada à facilidade de planejamento das investigações (FU3) a partir da utilização do modelo proposto, não houveram discordância. Apenas as questões referentes à clareza da proposta (FU1) e à facilidade geral na utilização do modelo receberam respostas com o rótulo ”discordo”. No entanto, ambas as questões obtiveram 85% das respostas nos rótulos ”concordo”. Isso indica que, de maneira geral, os participantes percebem o modelo como sendo de fácil aplicação, mas reconhecem a necessidade de aprimoramento em termos de ferramentas que melhorem a visualização e o gerenciamento das etapas investigativas. Esse ponto é corroborado pelos resultados do *Net Promoter Score* (NPS), onde a análise dos dados revelou uma porcentagem neutra (0%) de promoção da proposta pelos sete especialistas. Isso reforça que apesar dos resultados positivos da avaliação, a proposta ainda encontra-se na zona de aperfeiçoamento.

Em resumo, a codificação e análise das questões destacam a necessidade do desenvolvimento de ferramentas para o gerenciamento dos artefatos e o preenchimento das informações relacionadas ao modelo. No entanto, os especialistas observam que, na maioria das vezes, a execução dos mandados em investigações não é realizada pelos mesmos profissionais que lidam com as evidências em laboratório. Por esse motivo, a flexibilidade do modelo e um suporte mais abrangente aos agentes de segurança para a classificação prévia das fontes de evidências melhoram o gerenciamento das investigações de Forense Computacional em cenários como *smart homes, smart offices* e *smart building*. Ou seja, o modelo proposto indica melhorias significativas nas etapas de *planejamento* e execução dos mandados em investigações envolvendo dispositivos IoT.

5. Conclusão

O mercado de IoT experimentou um crescimento significativo nos últimos anos e, com a proliferação desses sistemas, a Internet agora está inundada de endereços IP associados a dispositivos IoT. Devido ao monitoramento contínuo do ambiente em que estão inseridos, essas aplicações tendem a ser fontes valiosas de informações para a caracterização de evidências em investigações de Forense Computacional. Por isso, este estudo teve como objetivo mapear o processo investigativo da Forense Computacional tradicional em cenários envolvendo aplicações IoT, a fim de propor as alterações necessárias para adaptar o modelo investigativo. O modelo proposto abrange os ambientes da Internet das Coisas (IoT), incluindo *smart homes, smart offices* e *smart buildings*, com base nas diretrizes estabelecidas pelo Procedimento Operacional Padrão publicado pelo Ministério da Justiça Brasileiro [Figueiredo et al. 2013] e pela Norma ISO/IEC 27037:2012 - Diretrizes para identificação, coleta, aquisição e preservação de evidência digital [ISO/IEC 2012].

Para avaliar a viabilidade da proposta, foi desenvolvido um protótipo do modelo e conduzido um estudo de avaliação por especialistas. Os resultados obtidos indicam uma alta aceitação na utilidade percebida, com uma média de 3,96 em uma escala de 1 a 5 para a soma dos fatores avaliados. A proposta demonstrou fornecer melhorias significativas no planejamento das investigações, além de auxiliar no processo de documentação das mesmas. Além disso, os especialistas ressaltaram que, na maioria dos casos, os mandados judiciais são executados por agentes com um nível menor de conhecimento técnico em

Forense Computacional. Nesse sentido, a proposta possibilita uma classificação prévia das potenciais fontes de evidências, fornecendo suporte para o processo de aquisição e análise dos dados em laboratório.

No entanto, a área de Forense Computacional ainda enfrenta desafios relacionados às ferramentas de aquisição e análise de dados em aplicações IoT. Como perspectiva para futuras pesquisas, pretende-se expandir o protótipo desenvolvido visando a criação de bases de dados correlacionadas. Assim, busca-se superar os desafios identificados em relação à facilidade de uso da proposta e capacitá-la para gerar dados que possibilitem construções inteligentes baseadas em históricos forenses.

Referências

Achar, S. (2022). Cloud computing forensics. *International Journal of Computer Engineering and Technology*, 13(3).

Ayers, R., Brothers, S., and Jansen, W. (2013). Guidelines on mobile device forensics (draft). *NIST Special Publication*, 800:101.

Beebe, N. L. and Clark, J. G. (2005). A hierarchical, objectives-based framework for the digital investigations process. *Digital Investigation*, 2(2):147–167.

Carrier, B. and Spafford, E. (2004). An event-based digital forensic investigation framework. *Digital Investigation*.

Casey, E. (2001). *Handbook of computer crime investigation: forensic tools and technology*. Elsevier.

Castelo Gómez, J. M., Carrillo Mondéjar, J., Roldán Gómez, J., and Martínez Martínez, J. L. (2021). A context-centered methodology for iot forensic investigations. *International Journal of Information Security*, 20(5):647–673.

Cohen, F. B. (2009). *Digital forensic evidence examination*, volume 101. Asp Press.

Davis, F. D. (1989). Perceived usefulness, perceived ease of use, and user acceptance of information technology. *MIS quarterly*, pages 319–340.

Dawson, L. and Akinbi, A. (2021). Challenges and opportunities for wearable iot forensics: Tomtom spark 3 as a case study. *Forensic Science International: Reports*, 3:100198.

Figueiredo, I. S. d., Brito, C. C. d. S., Godoy, M. d. F. P. d. C., et al. (2013). Procedimento operacional padrão: perícia criminal.

Goodman, L. A. (1961). Snowball sampling. *The annals of mathematical statistics*, pages 148–170.

ISO/IEC (2012). ISO/IEC 27037:2012 Guidelines for identification, collection, acquisition and preservation of digital evidence.

Kohn, M. D., Eloff, M. M., and Eloff, J. H. (2013). Integrated digital forensic process model. *Computers & Security*, 38:103–115.

Lee, H. C., Palmbach, T., and Miller, M. T. (2001). *Henry Lee's crime scene handbook*.

Li, S., Choo, K.-K. R., Sun, Q., Buchanan, W. J., and Cao, J. (2019). Iot forensics: Amazon echo as a use case. *IEEE Internet of Things Journal*, 6(4):6487–6497.

Lombardi, M., Pascale, F., and Santaniello, D. (2021). Internet of things: A general overview between architectures, protocols and applications. *Information*, 12(2):87.

Lutta, P., Sedky, M., Hassan, M., Jayawickrama, U., and Bastaki, B. B. (2021). The complexity of internet of things forensics: A state-of-the-art review. *Forensic Science International: Digital Investigation*, 38:301210.

Montasari, R., Hill, R., Montaseri, F., Jahankhani, H., and Hosseinian-Far, A. (2020). Internet of things devices: digital forensic process and data reduction. *International Journal of Electronic Security and Digital Forensics*, 12(4):424–436.

OliveiraJr, E., Zorzo, A. F., and Neu, C. V. (2020). Towards a conceptual model for promoting digital forensics experiments. *Forensic Science International: Digital Investigation*, 35:301014.

Pradini, R. S., Kriswibowo, R., and Ramdani, F. (2019). Usability evaluation on the sipr website uses the system usability scale and net promoter score. In *2019 International Conference on Sustainable Information Engineering and Technology (SIET)*. IEEE.

Prado, G., Silveira, E. D., Valente, M. M. G., and Giacomolli, N. J. (2015). A quebra da cadeia de custódia das provas no processo penal brasileiro. In Valente, M. M. G., editor, *Prova Penal: Estado Democrático de Direito*, volume 1, pages 13–37.

Qatawneh, M., Almobaideen, W., Khanafseh, M., and Al Qatawneh, I. (2019). Dfim: A new digital forensics investigation model for internet of things. *Journal of Theoretical and Applied Information Technology*, 97(24).

Quick, D. and Choo, K.-K. R. (2018). Iot device forensics and data reduction. *IEEE Access*, 6:47566–47574.

Reith, M., Carr, C., and Gunsch, G. (2002). An examination of digital forensic models. *International Journal of digital evidence*, 1(3):1–12.

Rizal, R., Riadi, I., and Prayudi, Y. (2018). Network forensics for detecting flooding attack on internet of things (iot) device. *Int. J. Cyber-Security Digit. Forensics*, 7(4):382–390.

Salama, U., Yao, L., and Paik, H.-Y. (2022). A multilevel collective framework for internet of things digital forensic investigation. *Computer*, 55(2):44–53.

Stolojescu-Crisan, C., Crisan, C., and Butunoi, B.-P. (2021). An iot-based smart home automation system. *Sensors*, 21(11):3784.

Stoyanova, M., Nikoloudakis, Y., Panagiotakis, S., Pallis, E., and Markakis, E. K. (2020). A survey on the internet of things (iot) forensics: challenges, approaches, and open issues. *IEEE Communications Surveys & Tutorials*, 22(2):1191–1221.

Strauss, A. and Corbin, J. (1990). *Basics of qualitative research*. Sage publications.

Tan, J. (2001). Forensic readiness. *Cambridge, MA:@ Stake*, 1.

Yang, W., Johnstone, M. N., Sikos, L. F., and Wang, S. (2020). Security and forensics in the internet of things: Research advances and challenges. In *2020 Workshop on Emerging Technologies for Security in IoT (ETSecIoT)*, pages 12–17. IEEE.

Zhang, X., Yuen, T. T., and Choo, K.-K. R. (2020). Experiential learning in digital forensics. *Digital Forensic Education: An Experiential Learning Approach*, pages 1–9.