Uso de Técnicas da Perícia Computacional para Análise de Logs de Dispositivos Móveis e Reconstrução de Eventos

Guilherme Silva Rabelo[1], João Benedito dos Santos Junior[2]

[1]Departamento de Ciência da Computação
Pontifícia Universidade Católica de Minas Gerais(PUCMG)
R. Dom José Gaspar, 500 , Belo Horizonte – MG – Brasil

sguilhermerabelo@gmail.com, joao@pucpcaldas.br

Abstract. *Computer Forensics and Cyber Intelligence are fundamental nowadays, serving as pillars in protecting against cybercrime and maintaining digital security. These disciplines are essential for analyzing and interpreting digital evidence, ensuring data integrity, and identifying illicit activities. With the in- crease in cyber threats, the importance of these areas is only growing, providing effective means of investigating and mitigating risks. Focusing on the analysis of mobile device logs, this article proposes an innovative web application designed to collect, filter and analyze these logs from Android devices, making it easier to identify suspicious activity and improving the forensic investigation process by filtering data by date and generating detailed reports.*

Resumo. *A perícia computacional e a Inteligência Cibernética são fundamentais nos dias de hoje, servindo como pilares na proteção contra crimes cibernéticos e na manutenção da segurança digital. Essas disciplinas são essenciais para a análise e interpretação de evidências digitais, garantindo a integridade dos dados e a identificação de atividades ilícitas. Com o aumento das ameaças cibernéticas, a importância dessas áreas só cresce, proporcionando meios eficazes para investigar e mitigar riscos. Focando na análise de logs de dispositivos móveis, este artigo propõe uma aplicação web inovadora projetada para coletar, filtrar e analisar esses logs de dispositivos Android, facilitando a identificação de atividades suspeitas e aprimorando o processo de investigação forense através da filtragem dos dados por datas e da geração de relatórios detalhados.*

1. Introdução

A importância da perícia computacional e da Inteligência Cibernética tem crescido exponencialmente, tornando-se fundamentais na proteção contra crimes cibernéticos e na manutenção da segurança digital. Essas disciplinas desempenham um papel essencial na análise e interpretação de evidências digitais, garantindo a integridade dos dados e a identificação de atividades ilícitas. Com o aumento das ameaças cibernéticas, a importância dessas áreas só cresce, sendo necessário criar soluções eficazes a fim de investigar e mitigar riscos.

Dentro desse contexto, a análise de *logs* de dispositivos móveis surge como uma ferramenta essencial para esse cenário. Dispositivos Android, amplamente utilizados, geram uma vasta quantidade de dados que podem revelar informações importantes e detalhadas que ajudam no momento da perícia criminal. Este artigo propõe o desenvolvimento

de uma aplicação web inovadora para coletar, filtrar e analisar esses *logs*, proporcionando uma visão detalhada e cronológica das atividades registradas. A plataforma permitirá a filtragem dos dados por datas e a geração de relatórios, facilitando a identificação de atividades suspeitas e aprimorando o processo de investigação forense.

Os *logs* de um dispositivo Android capturam uma vasta quantidade de eventos e estados do sistema, podendo oferecer dependendo da capacidade de análise de um(a) perito(a) e/ou investigador(a) uma visão detalhada das operações internas do dispositivo, revelando aspectos de uma espécie de vida secreta dos aparelhos e aplicações. Através de comandos ADB (*Android Debug Bridge*), é possível extrair dados que incluem registros de chamadas, localização GPS (*Global Positioning System*), utilização de aplicativos, consumo de bateria, status de operação das redes de comunicação, entre outros. A importância da análise de *logs* em dispositivos móveis pode ser exemplificada através de muitos cenários. Em casos de crimes digitais, como hacking, fraudes financeiras ou as mais diversas formas de assédio pelo meio cibernético, os *logs* podem fornecer evidências sobre a cronologia dos eventos, as ações do usuário e as interações com o dispositivo. Da mesma forma, em muitas situações, a análise de *logs* pode contribuir na identificação de vulnerabilidades, monitorar a integridade do sistema e detectar comportamentos anômalos que possam indicar uma ou mais falhas em sistemas de segurança.

Este artigo explora, de forma preliminar, a utilidade dos *logs* extraídos de dispositivos Android utilizando comandos ADB. A análise desses *logs* não só auxilia na reconstrução de eventos passados e na identificação de atividades suspeitas, mas também fornece uma base para a implementação de melhores práticas de segurança e a criação de perfis de uso. O foco deste estudo inclui os seguintes arquivos de log: *account*, *alam*, *battery*, *biometric*, *bluetooth*, *dbinfo*, *fingerprint*, *location*, *netstats*, *notification*, *power*, *telecom*, e *wifi*. Cada um desses *logs* oferece uma visão única e específica das operações e atividades realizadas no dispositivo.

2. Referencial Teórico

2.1. Perícia Computacional e Inteligência Cibernética

A perícia computacional e a inteligência cibernética têm se tornado componentes cruciais no combate aos crimes cibernéticos e na garantia da segurança digital. Com a crescente dependência de dispositivos digitais e a complexidade das ameaças cibernéticas, essas disciplinas oferecem meios eficazes para investigar, identificar e mitigar riscos [Brustolin et al. 2022]. A análise de evidências digitais é fundamental para a identificação de atividades ilícitas e a preservação da integridade dos dados, proporcionando uma base sólida para investigações criminais [Wendt and Jorge 2013].

2.2. Análise de Logs de Dispositivos Móveis

A análise de *logs* de dispositivos móveis é uma prática vital dentro da perícia computacional. Dispositivos Android, amplamente utilizados em diversas atividades diárias, geram uma quantidade substancial de dados que podem revelar comportamentos e atividades críticas para investigações forenses. Segundo o estudo [Tamma et al. 2020], a utilização de comandos ADB permite a extração de diversos tipos de *logs*, como registros de chamadas, localização GPS, datas, e uso de aplicativos, que são essenciais para a reconstrução de eventos e identificação de atividades suspeitas.

Além disso, a importância da análise de *logs* em dispositivos móveis é evidenciada pela capacidade desses dados de fornecer uma visão detalhada das operações internas do dispositivo. Os *logs* capturam uma vasta quantidade de eventos e estados do sistema, oferecendo insights sobre a "vida secreta"dos dispositivos e suas aplicações [Junior et al. 2024]. Esse tipo de análise é crucial em cenários de crimes digitais, como hacking, fraudes financeiras e assédio cibernético, pois permite uma cronologia precisa dos eventos e ações do usuário.

2.3. Aplicações Web para Análise Forense

Com o avanço da tecnologia, aplicações web têm se mostrado ferramentas poderosas para auxiliar na análise forense. Essas plataformas oferecem a capacidade de coletar, filtrar e analisar dados de maneira eficiente, melhorando a precisão e a rapidez das investigações [Marziale III 2009]. A implementação de ferramentas de análise de *logs* baseadas na nuvem, como descrito no estudo [Alshabibi et al. 2024], demonstra como essas soluções podem proporcionar uma visão abrangente e detalhada dos dados, facilitando a identificação de atividades anômalas e melhorando as práticas de segurança.

A proposta de desenvolvimento de uma aplicação web para coletar, filtrar e analisar *logs* de dispositivos Android se baseia nessa premissa. Tal plataforma permitirá a filtragem dos dados por datas e a geração de relatórios detalhados, aprimorando o processo de investigação forense [Tidmarsh 2023]. Essas ferramentas são essenciais para fornecer evidências robustas e apoiar as investigações em um ambiente cada vez mais digital e complexo.

2.4. Plataformas Web para Análise e Visualização de Técnicas Forenses

O trabalho [Silva and dos Santos Junior 2024] propõe uma solução voltada para o registro e compartilhamento de dados relacionados a investigações e perícias. Essa plataforma, ao fornecer serviços de armazenamento de evidências digitais e aplicação de filtros inteligentes, facilita a troca de informações entre investigadores e peritos. Embora o foco do trabalho seja o compartilhamento e a correlação de dados, ele apresenta conceitos relevantes para a criação de sistemas voltados à análise de *logs*, como a estrutura de armazenamento de dados, a organização eficiente das informações e a importância de sistemas que permitam uma análise mais detalhada e a identificação de padrões.

2.5. Estudo de Caso, Análise Forense dos Logs

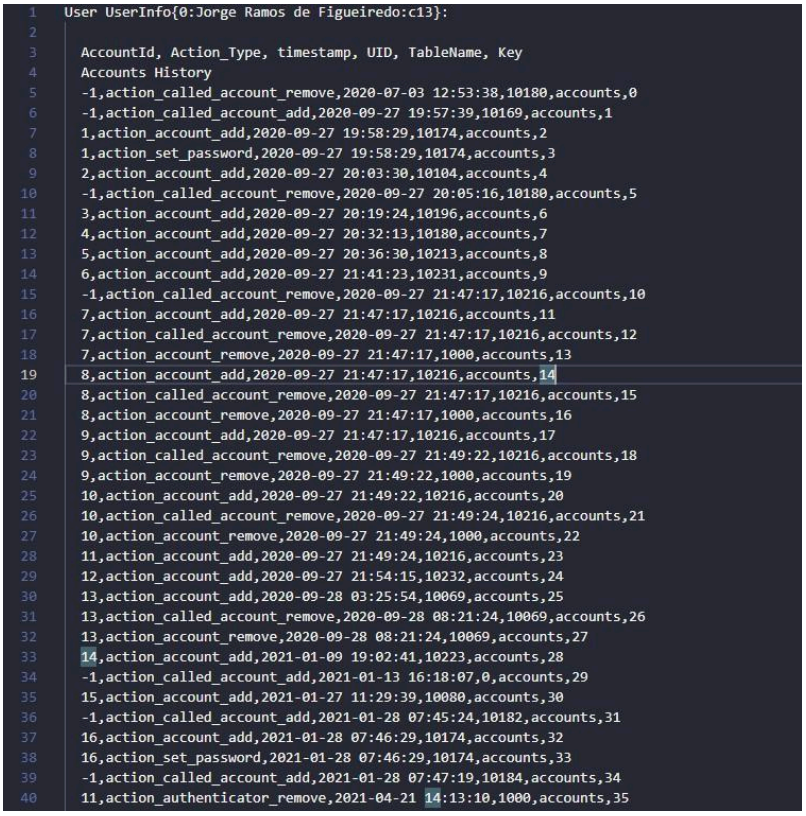
A análise de *logs* de dispositivos móveis tem se mostrado uma ferramenta fundamental em investigações digitais. Como demonstrado no estudo de caso apresentado em [Junior et al. 2024] , a extração e análise detalhada de *logs* de um smartphone Android podem fornecer um rico conjunto de informações para responder a diversos questionamentos forenses.

Os *logs* que são extraídos dos dispositivos móveis com sistema operacional Android podem ser importantes em investigação, perícia, inteligência e resposta a incidentes, contendo informações sobre o uso de aplicativos, localização do dispositivo, estatísticas de uso, conectividade, dentre outras. Os avanços contidos neste trabalho estão relacionados com o estabelecimento de relações e vínculos entre as informações extraídas, para ampliar a capacidade de análise por parte de investigadores, peritos, agentes de inteligência e respondentes de incidentes cibernéticos. Neste sentido, é relevante compreender, de

forma breve, as informações contidas em cada um dos arquivos de *logs* analisados. O ***log account*** contém informações sobre as contas de usuário configuradas no dispositivo, incluindo detalhes como tipos de conta (e-mail, redes sociais, dentre outros) e eventos relacionados à autenticação e sincronização. O ***log alarm*** registra eventos de alarme configurados no dispositivo, como despertadores e lembretes, podendo contribuir para determinar a rotina do usuário e horários de atividades. O ***log battery*** fornece dados sobre o consumo de bateria, incluindo histórico de carga e descarga, uso de aplicativos e serviços que impactam o consumo de energia, podendo ser útil para entender o comportamento do dispositivo ao longo do tempo. O ***log biometric*** fornece informações detalhadas sobre o uso de biometria no dispositivo, incluindo histórico de acessos realizados por meio de reconhecimento facial, impressão digital ou outros métodos biométricos. Esses dados podem indicar os aplicativos e serviços que utilizam autenticação biométrica, horários de acesso e possíveis alterações ou configurações relacionadas ao sistema de biometria. Esse log é útil para monitorar o uso de biometria, garantindo segurança e identificando padrões de autenticação no dispositivo ao longo do tempo.O ***log fingerprint*** apresenta registros específicos relacionados ao uso de autenticação por impressão digital no dispositivo. Ele inclui informações como o histórico de leituras bem-sucedidas e falhas, aplicativos e serviços que solicitaram autenticação e eventuais alterações nas configurações ou no cadastro das impressões digitais. Esse *log* é essencial para rastrear o desempenho do sensor de impressão digital, identificar possíveis problemas de leitura e analisar o comportamento de autenticação por essa tecnologia ao longo do tempo. O ***log power*** fornece detalhes sobre o estado de energia do dispositivo, incluindo eventos de ligar/desligar, estado de suspensão e eventos de carregamento, colaborando para determinar um perfil do uso do dispositivo. O ***log dbinfo*** contém informações sobre os bancos de dados, especialmente SQLite, usados pelos aplicativos instalados no dispositivo; esse tipo de informação pode incluir registros de atividades e dados de uso de aplicativos. O ***log location*** registra dados de localização do dispositivo, como coordenadas GPS e torres de celular conectadas, sendo essencial para determinar os movimentos do usuário. O ***log notification*** registra todas as notificações recebidas e gerenciadas pelo dispositivo, incluindo conteúdo de mensagens e alertas de aplicativos, sendo útil para entender a comunicação do usuário. O ***log netstats*** contém estatísticas sobre o uso da rede, incluindo dados sobre tráfego de rede móvel e wi-fi, consumo de dados por aplicativo e sessões de conectividade. O ***log telecom*** inclui registros de chamadas telefônicas, mensagens de texto e outras atividades de telecomunicação, sendo essencial para investigações que envolvem comunicações do usuário. Os ***logs wifi*** e ***logs bluetooth*** registram eventos relacionados à conectividade, incluindo redes conectadas, falhas de conexão e mudanças de rede, pareamentos com outros aparelhos e centrais multimídia (como é o caso de alguns modelos e marcas de automóveis), podendo ser usado para mapear a movimentação do dispositivo em diferentes redes.

No estudo de caso apresentado, foram definidos vários quesitos periciais para guiar a análise forense dos *logs*. Esses quesitos buscavam responder perguntas essenciais sobre o uso do dispositivo, tais como: qual era a principal conta de usuário associada ao aparelho, quais aplicativos foram mais utilizados, e se houve algum comportamento anômalo durante o uso. Para isso, os pesquisadores analisaram 14 arquivos de log extraídos via ADB (*Android Debug Bridge*) usando a ferramenta NotePad++. Essa abordagem manual foi escolhida para aumentar a compreensão sobre a estrutura e o conteúdo dos *logs*, embora uma ferramenta baseada em expressões regulares esteja sendo desenvolvida para

automatizar parte do processo. Na **Figura 1** pode-se observar *logs* **account** como exemplo dos arquivos extraídos pela perícia.



```
User UserInfo{0:Jorge Ramos de Figueiredo:c13}:

  AccountId, Action_Type, timestamp, UID, TableName, Key
  Accounts History
  -1,action_called_account_remove,2020-07-03 12:53:38,10180,accounts,0
  -1,action_called_account_add,2020-09-27 19:57:39,10169,accounts,1
  1,action_account_add,2020-09-27 19:58:29,10174,accounts,2
  1,action_set_password,2020-09-27 19:58:29,10174,accounts,3
  2,action_account_add,2020-09-27 20:03:30,10104,accounts,4
  -1,action_called_account_remove,2020-09-27 20:05:16,10180,accounts,5
  3,action_account_add,2020-09-27 20:19:24,10196,accounts,6
  4,action_account_add,2020-09-27 20:32:13,10180,accounts,7
  5,action_account_add,2020-09-27 20:36:30,10213,accounts,8
  6,action_account_add,2020-09-27 21:41:23,10231,accounts,9
  -1,action_called_account_remove,2020-09-27 21:47:17,10216,accounts,10
  7,action_account_add,2020-09-27 21:47:17,10216,accounts,11
  7,action_called_account_remove,2020-09-27 21:47:17,10216,accounts,12
  7,action_account_remove,2020-09-27 21:47:17,1000,accounts,13
  8,action_account_add,2020-09-27 21:47:17,10216,accounts,14
  8,action_called_account_remove,2020-09-27 21:47:17,10216,accounts,15
  8,action_account_remove,2020-09-27 21:47:17,1000,accounts,16
  9,action_account_add,2020-09-27 21:47:17,10216,accounts,17
  9,action_called_account_remove,2020-09-27 21:49:22,10216,accounts,18
  9,action_account_remove,2020-09-27 21:49:22,1000,accounts,19
  10,action_account_add,2020-09-27 21:49:22,10216,accounts,20
  10,action_called_account_remove,2020-09-27 21:49:24,10216,accounts,21
  10,action_account_remove,2020-09-27 21:49:24,1000,accounts,22
  11,action_account_add,2020-09-27 21:49:24,10216,accounts,23
  12,action_account_add,2020-09-27 21:54:15,10232,accounts,24
  13,action_account_add,2020-09-28 03:25:54,10069,accounts,25
  13,action_called_account_remove,2020-09-28 08:21:24,10069,accounts,26
  13,action_account_remove,2020-09-28 08:21:24,10069,accounts,27
  14,action_account_add,2021-01-09 19:02:41,10223,accounts,28
  -1,action_called_account_add,2021-01-13 16:18:07,0,accounts,29
  15,action_account_add,2021-01-27 11:29:39,10080,accounts,30
  -1,action_called_account_add,2021-01-28 07:45:24,10182,accounts,31
  16,action_account_add,2021-01-28 07:46:29,10174,accounts,32
  16,action_set_password,2021-01-28 07:46:29,10174,accounts,33
  -1,action_called_account_add,2021-01-28 07:47:19,10184,accounts,34
  11,action_authenticator_remove,2021-04-21 14:13:10,1000,accounts,35
```

Figura 1. Informações extraídas do arquivo de log account

Os resultados preliminares do estudo de caso mostram que a análise dos *logs* forneceu informações valiosas sobre o uso do dispositivo. Foi possível identificar as redes wireless às quais o dispositivo se conectou, os níveis de carga da bateria, as contas de usuário vinculadas, e os aplicativos mais frequentemente usados. A análise também revelou que o dispositivo era mais utilizado durante o período noturno e que não apresentou sinais de anormalidade ou instabilidade significativa. Essas descobertas ilustram a importância da análise de *logs* em investigações cibernéticas e reforçam o valor dessas técnicas para a perícia computacional e a inteligência cibernética.

3. Metodologia

Essa seção descreve o processo de desenvolvimento da plataforma web proposta neste artigo, abordando as etapas de implementação, as ferramentas utilizadas e as técnicas adotadas para garantir a eficácia na visualização dos *logs*.

3.1. Tecnologias

As tecnologias adotadas para o desenvolvimento do Log Forensic foram o [Quasar contributors 2024] e a ferramenta JSON Server [typicode 2024]. As APIs foram criadas na ferramenta JSON Server que permite gerar rapidamente uma API RESTful a partir de um JSON. Ela é uma biblioteca em Node.js que simula um servidor REST- ful completo, permitindo definir *endpoints*. Esses *endpoints* são rotas que entregam

os dados que estão no arquivo db.json. Nesse arquivo os *logs* foram tratados e transformados no formato JSON e a partir disso popula-se os arquivos fornecidos pelo estudo [Junior et al. 2024]. A **Figura 2** demonstra um exemplo dos *logs* de *account* do arquivo *db.json*.

Figura 2. Account JSON

O Quasar é um *framework* de Vue.js e tem sido uma escolha sólida para os desenvolvedores que buscam eficiência e praticidade na construção de interfaces de usuário. Com uma ampla gama de componentes pré-construídos, desde botões e barras de navegação até listas e formulários, o Quasar proporciona uma base robusta para o desenvolvimento. Sua adaptação responsiva permite que os aplicativos se ajustem automaticamente em diferentes dispositivos, garantindo uma experiência consistente em *desktops*, celulares e web. Além disso, sua abordagem de multiplataforma com um único código fonte simplifica o processo de desenvolvimento, permitindo que os aplicativos sejam implantados em iOS, Android e aplicativos web responsivos sem a necessidade de escrever código adicional para cada plataforma.

Um dos principais atrativos do Quasar é sua coleção de *plugins* integrados, que incluem recursos como notificações, armazenamento local e autenticação. Isso acelera significativamente o desenvolvimento, permitindo que os desenvolvedores se concentrem nas funcionalidades específicas de seus aplicativos. Além disso, o Quasar otimiza o processo de compilação com uma abordagem *just-in-time* (JIT) durante o desenvolvimento, enquanto na produção utiliza a compilação *ahead-of-time* (AOT) para gerar um código nativo altamente otimizado. Com uma documentação detalhada e uma comunidade ativa pronta para ajudar e compartilhar conhecimento, o *framework* oferece uma solução abrangente e eficiente para o desenvolvimento de aplicativos [Vue.js contributors 2024].

3.2. Atividades Realizadas

O desenvolvimento do software foi dividido em pequenas *sprints*, a fim de estar sempre determinando um prazo e uma pequena entrega. Isso ajuda na organização e revisão das etapas de desenvolvimento. Logo na primeira *sprints* ocorreu um estudo aprofundado no Vue e no Quasar, dito isso as documentações dessa linguagem e *framework* serviu como material de prática, a fim de conhecer e se familiarizar inicialmente. Após esse estudo, outro estudo foi realizado em cima de um material fornecido pelo professor orientador, onde apresenta uma série de exemplos e tutoriais para iniciantes no Quasar. Esse processo gerou muito conhecimento sobre as ferramentas SDK existentes, como também sobre a biblioteca de IU em *widgets*, onde apresenta uma coleção diversa de elementos que foram utilizados para personalizar a aplicação.

A segunda *sprints* focou-se na criação e aplicação do JSON Server que funciona como um simulador de API RESTful. Essa ferramenta é útil para agilizar o desenvolvimento e testes de aplicativos que dependem de uma API e foi por esse motivo que ela foi escolhida, pois não foi encontrado nenhuma API pública com dados de produtos de estabelecimentos. A partir disso, o JSON foi criado contendo informações sobre os estabelecimentos e sobre os produtos, como também dados sobre descontos e cupons.

O desenvolvimento do projeto foi realizado na segunda, terceira e quarta *sprints*. Foram identificados dois *backlogs*, um para o *frontend* e outro para o *backend* onde cada um criou- se várias tarefas, separadas por prioridade e também pela história a ser implementada. No *backend* as tarefas tinham o foco na modelagem dos dados recebidos da API e através da linguagem Vue.js foi criada essa integração para que o *framework* Quasar receba as informações. Além disso, também foi desenvolvido o algoritmo de comparação que realiza toda a lógica e análise dos preços dos produtos. O outro *backlogs* teve como objetivo a criação das telas do aplicativo seguindo os modelos já criados no Figma, mantendo a identidade utilizando as mesmas cores, fontes, ícones etc.

3.3. Implementação da Plataforma

Na aplicação Log Forensic, os usuários são os investigadores e peritos que vão utilizar a plataforma a fim de analisar com mais detalhes os *logs* fornecidos.Esta ferramenta foi desenvolvida para auxiliar investigadores e peritos na minuciosa avaliação de *logs* extraídos via ADB, organizando-os em tabelas específicas para cada tipo de log. Dessa forma, a ferramenta facilita a visualização e a filtragem dos dados com base em critérios como data e hora, permitindo uma análise detalhada e precisa das informações. Os resultados descritos a seguir demonstram a eficácia da aplicação na identificação de padrões de uso, anomalias e outras informações relevantes que podem contribuir significativamente para investigações cibernéticas.

Nesse cenário, a **Tabela 1** ilustra os requisitos formais do sistema, evidenciando seu funcionamento, desempenho esperado e funcionalidades cruciais. Um requisito funcional descreve, de forma clara e objetiva, o que o sistema deve ser capaz de realizar para atender às necessidades dos usuários. Por exemplo, funcionalidades como filtragem por data e hora, organização em tabelas específicas e exibição clara de padrões de uso são essenciais para o propósito da ferramenta. Esses requisitos são importantes porque garantem que o sistema seja projetado para cumprir os objetivos propostos, proporcionando uma base sólida para o desenvolvimento e a validação. Além disso, eles facilitam o alinhamento entre as expectativas dos usuários e as funcionalidades entregues,

contribuindo para a eficácia da solução no contexto de investigações cibernéticas.

Tabela 1. Requisitos funcionais especificados para a aplicação

Requisito	Descrição
R01	O sistema deve possuir um arquivo de *logs* sobre perícia criminal para o tratamento e análise dos dados.
R02	O sistema deve mostrar tabelas sobre cada tipo de log apresentando uma listagem das informações desse arquivo.
R03	A aplicação deve permitir a pesquisa de qualquer dado na tabela.
R04	A aplicação deve permitir uma ordenação crescente ou decrescente das colunas na tabela.
R05	A plataforma deve permitir a visualização, cadastro, edição e exclusão dos logs.
R06	A plataforma deve permitir a filtragem das linhas na tabela a partir de um intervalo de data ou de hora.

Figura 3. Diagrama de Casos de Uso

A partir da criação dos requisitos funcionais do Log Forensic, foi produzido um modelo de diagrama de casos de uso para compreender melhor as funcionalidades predefinidas da aplicação. Esse diagrama, representado na **Figura 3**, proporciona uma visão clara e simplificada das interações entre os usuários e o sistema. Representações visuais como esta são fundamentais para capturar os principais objetivos do software, delineando as funcionalidades essenciais e suas relações. Além disso, o diagrama de casos de uso possibilita uma análise detalhada das operações do sistema, destacando as áreas críticas e auxiliando na priorização de funcionalidades durante o desenvolvimento. Isso promove

uma melhor estruturação do projeto, reduzindo riscos e aumentando a eficácia da implementação do software.

Após a definição dos requisitos funcionais e a elaboração do modelo de casos de uso, o desenvolvimento do software foi realizado utilizando o Vue.js, um *framework* para aplicações JavaScript. Além disso, foi empregado o Quasar, um *framework* complementar ao Vue.js, que oferece recursos avançados para a criação de interfaces modernas e responsivas, garantindo maior eficiência e qualidade no desenvolvimento da aplicação. Os *logs* foram armazenados em um banco de dados estruturado utilizando o JSON Server, uma biblioteca disponibilizada pelo *npm*. Essa abordagem permitiu a criação de um repositório de dados eficiente e acessível, facilitando o gerenciamento e a consulta dos registros durante o processo de análise. A **Figura 4** representa a arquitetura do software.

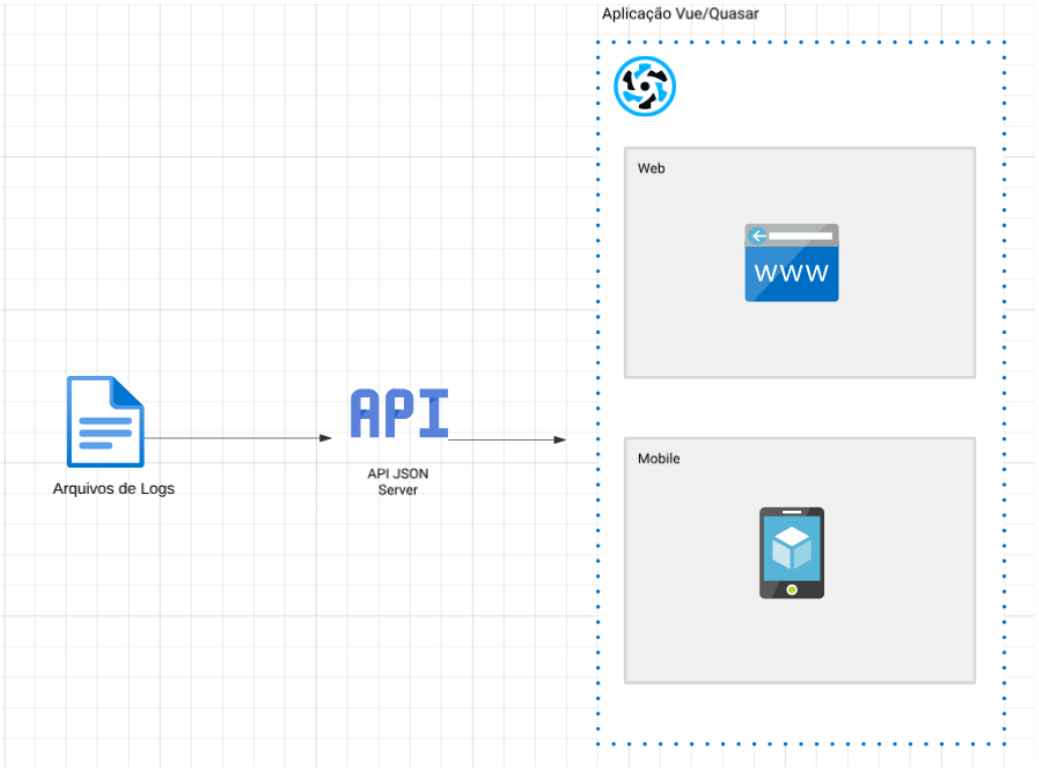


Figura 4. Esquema da Arquitetura do Sistema

A API disponibilizada pelo JSON Server já fornece endpoints pré-configurados que acessam diretamente o arquivo de banco de dados, onde as informações dos *logs* estão organizadas por tipo. A partir desses endpoints, o front-end consegue realizar qualquer tipo de requisição, como *GET*, *POST*, *UPDATE* e *DELETE*, garantindo uma integração simples e eficiente, facilitando a manipulação e exibição dos dados na interface do usuário. As **Tabelas 2** e **3** apresentam exemplos de endpoints relacionados aos *logs* de *fingerprint* e *power*.

Tabela 2. Endpoints fingerprints

Método	URL	Ação
POST	/fingerprint	Criar
UPDATE	/fingerprint/id	Atualizar os Dados
GET	/fingerprint	Exibir os Dados
DELETE	/fingerprint/id	Deletar

Tabela 3. Endpoints power

Método	URL	Ação
POST	/power	Criar
UPDATE	/power/id	Atualizar os Dados
GET	/power	Exibir os Dados
DELETE	/power/id	Deletar

4. Resultados

Nesta seção, são apresentados os resultados obtidos a partir dos testes realizados com a plataforma web desenvolvida. A aplicação foi projetada para receber dados de um banco de dados local em formato JSON e exibir essas informações de maneira organizada em tabelas interativas. Inicialmente, foram conduzidos testes de usabilidade, realizados pelo autor, com o objetivo de avaliar a interface da plataforma, a interação do usuário com os dados e a eficiência na visualização das informações.

Os resultados obtidos fornecem uma visão crítica sobre o desempenho da ferramenta e sua aplicabilidade em contextos práticos de análise de dados.

Os *prints* apresentados nas **Figuras** de número **5** a **9** mostram algumas das funcionalidades do sistema. A **Figura 5** apresenta a tela inicial da plataforma, juntamente com um exemplo das diversas listagens de logs extraídas do banco de dados do sistema. O exemplo ilustrado mostra as informações detalhadas dos logs de contas, demonstrando como os dados são organizados e exibidos na interface da aplicação.

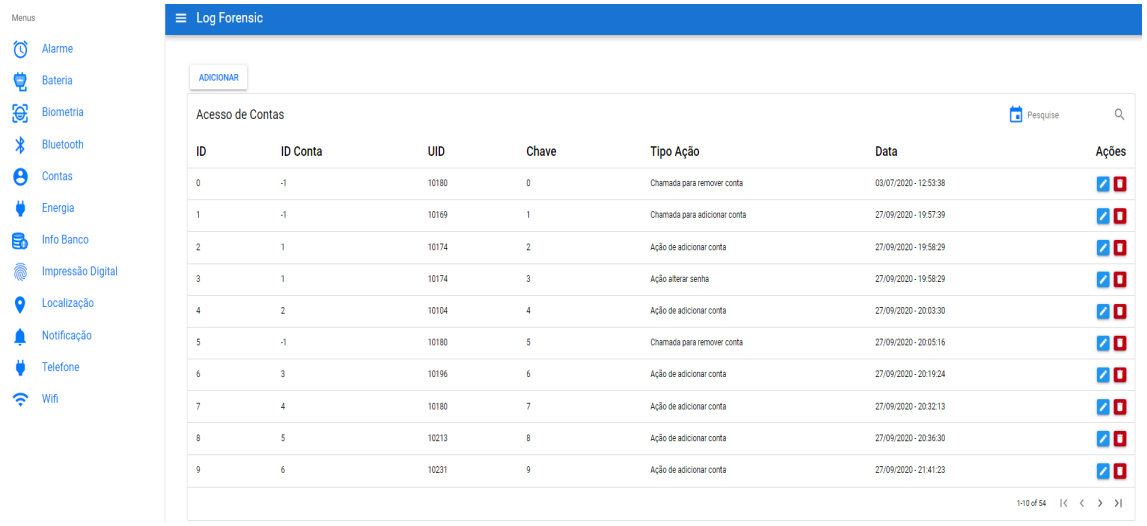


Figura 5. Tela de listagem de contas

A **Figura 6** ilustra a funcionalidade de filtragem dos dados exibidos na tabela, utilizando a seleção de um intervalo de datas por meio do componente QDate do Quasar Framework. Este componente permite ao usuário escolher de forma intuitiva um intervalo de datas, que é utilizado para filtrar os *logs* apresentados na tabela. A filtragem é realizada de forma dinâmica, ajustando os dados exibidos conforme o intervalo selecionado. O QDate oferece uma interface amigável para o usuário, com suporte a seleção de datas individuais ou intervalos, e é altamente personalizável, garantindo uma experiência fluida e eficiente na análise dos dados.

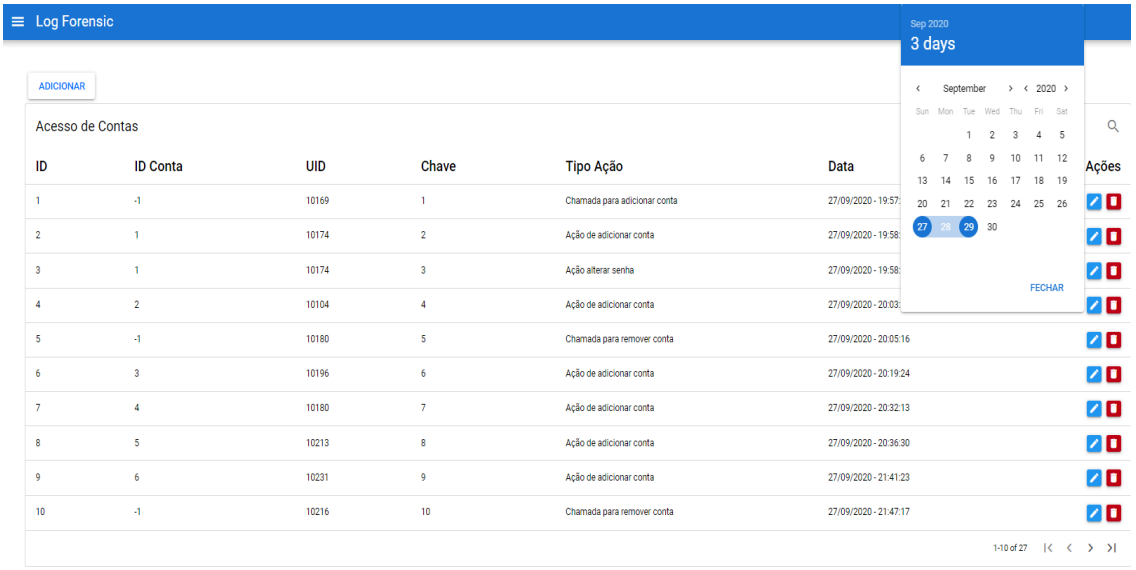


Figura 6. Componente de filtragem de datas

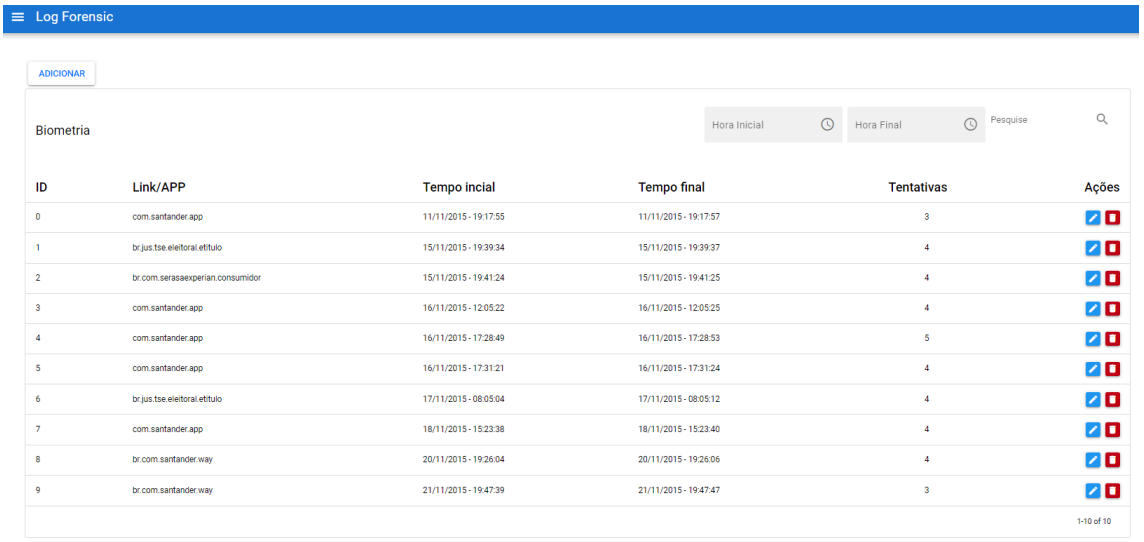


Figura 7. Tela de listagem de biometria

As **Figuras 7**, **8** e **9** ilustram a funcionalidade de filtragem dos dados na plataforma, agora utilizando o componente QTime do Quasar Framework. Essas figuras mostram como o usuário pode selecionar um intervalo de tempo para refinar a visualização dos *logs* apresentados na tabela. O QTime permite a escolha intuitiva de um horário específico ou de um intervalo de tempo, oferecendo uma interface prática para a seleção de horas e minutos.

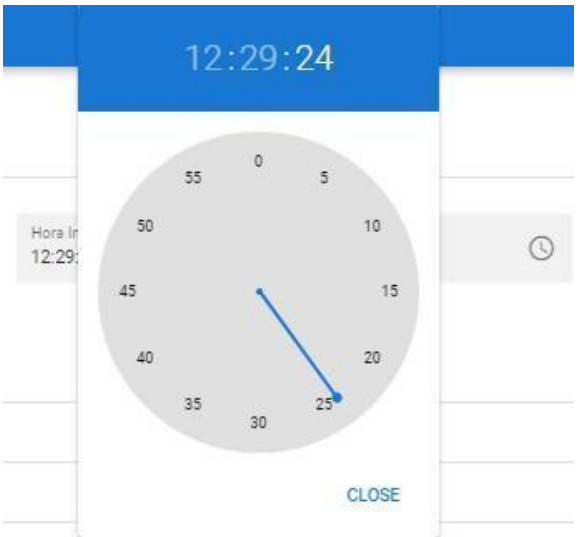


Figura 8. Componente Hora

Figura 9. Componente filtragem horas

A filtragem é realizada de maneira dinâmica, ajustando os dados de acordo com os horários definidos. O componente QTime é altamente personalizável, permitindo que os investigadores filtrem os *logs* com precisão temporal, com a opção de inserir minutos e até segundos, oferecendo maior flexibilidade na análise dos dados.

5. Conclusões e Trabalhos Futuros

Os testes realizados até o momento, embora indicativos de viabilidade, são preliminares e ainda carecem de uma análise mais aprofundada. Os resultados obtidos demonstram o potencial da plataforma na visualização e manipulação de *logs*, mas é necessário realizar uma série de testes adicionais para validar sua robustez em diferentes cenários e garantir que a plataforma atenda a todas as demandas dos usuários. O desempenho, a precisão das filtragens e a interação com o sistema são aspectos que devem ser avaliados em detalhes, de forma a otimizar a experiência do usuário e a confiabilidade da aplicação.

Além disso, é fundamental expandir a funcionalidade da plataforma, desenvolvendo novas telas que permitam a análise dos *logs* de forma mais detalhada, similar a um relatório. Isso possibilitaria aos investigadores extrair informações mais relevantes dos arquivos de *logs*, facilitando a identificação de padrões e anomalias cruciais para as investigações. A implementação de funcionalidades avançadas de análise, como gráficos e indicadores dinâmicos, contribuiria significativamente para a eficiência da ferramenta.

Por fim, a integração direta dos *logs* gerados por técnicas de perícia computacional à plataforma é uma melhoria importante a ser considerada. A ampliação da base de dados e a possibilidade de importar esses *logs* automaticamente tornaria o sistema ainda mais eficaz, reduzindo a necessidade de intervenções manuais e garantindo que os dados estivessem sempre atualizados. Esse aprimoramento, juntamente com a realização de novos testes e o desenvolvimento de funcionalidades adicionais, tem o potencial de transformar a plataforma em uma ferramenta indispensável para a análise forense digital.

Referências

Alshabibi, M. M., Bu Dookhi, A. K., and Rahman, M. M. H. (2024). Enhancing forensic investigations with cloud-based log analysis tools. *Computers*, 13(8):213.

Brustolin, V., Nunes, I. A., and de Assunção, J. Z. (2022). Análise estrutural das estratégias de segurança cibernética do brasil e dos estados unidos. *Revista Brasileira de Estudos de Defesa*, 9(2).

Junior, J. S., Naldoni, G., Brene, C., and Majeau, G. (2024). A vida secreta dos dispositivos móveis: Análise de logs de dispositivos android à luz da perícia computacional e da inteligência cibernética. In *Anais Estendidos do XXIV Simpósio Brasileiro de Se- gurança da Informação e de Sistemas Computacionais*, pages 408–411, Porto Alegre, RS, Brasil. SBC.

Marziale III, L. (2009). *Advanced techniques for improving the efficacy of digital forensics investigations*. PhD thesis, University of New Orleans.

Quasar contributors (2024). Quasar official documentation. https://quasar.dev/docs. Acesso em dezembro 10, 2024.

Silva, G. C. and dos Santos Junior, J. B. (2024). Especificação e implementação de uma plataforma para compartilhamento de dados de investigações e perícias: Uma abordagem centrada na inteligência cibernética. *Instituto de Ciências Exatas e Informática – ICEI, Pontifícia Universidade Católica de Minas Gerais – PUC Minas*.

Tamma, R., Skulkin, O., Mahalik, H., and Bommisetty, S. (2020). Mobile device forensics: An examination of android debug bridge (adb). In *Practical Mobile Forensics - Fourth Edition*. O'Reilly Media, Inc.

Tidmarsh, D. (2023). The importance of mobile forensics and how android log analysis can assist in criminal investigations. *EC-Council*. Acesso em dezembro 10, 2024.

Typicode (2024). JSON Server Readme. https://www.npmjs.com/package/json-server. Acesso em dezembro 10, 2024.

Vue.js contributors (2024). Vue official documentation. https://vuejs.org/guide/introduction. Acesso em dezembro 10, 2024.

Wendt, E. and Jorge, H. V. N. (2013). *Crimes Cibernéticos (2a. edição): Ameaças e procedimentos de investigação*. Brasport.