A Vida Secreta dos Dispositivos Móveis: Análise de Logs de Dispositivos Android à Luz da Perícia Computacional e da Inteligência Cibernética

João Benedito dos Santos Junior[1], *Gustavo Azevedo Naldoni*[2], *Cleyson Rodrigo Brene*[3], *Gabriela Amore Ribeiro Majeau*[2]

[1]Docente do Departamento de Ciência da Computação da PUC Minas *Campus* de Poços de Caldas – MG, Brasil | Perito Forense Computacional
[2]Alunos de Graduação do Curso de Ciência da Computação da PUC Minas *Campus* de Poços de Caldas – MG, Brasil
[3]Delegado de Polícia Civil do Estado de Minas Gerais – PCMG, Delegacia Regional de Poços de Caldas – MG, Brasil

joao@pucpcaldas.br, naldoni.gustavo@gmail.com, cleyson.brene@policiacivil.mg.gov.br, gabrielaribeirocampestre@gmail.com

Abstract: *The analysis of mobile device logs has become an essential tool in Digital Forensics, particularly in the context of criminal investigations and security audits. Devices with the Android Operating System, widely used globally, generate a substantial amount of log data that can provide valuable information about user activities, device behavior, and potential intrusions or suspicious activities. This article aims to explore the utility of logs extracted from Android devices using ADB (Android Debug Bridge) commands to assist in forensic investigations. The analyzed log files include account, alarm, battery, dbinfo, dumpsys, fingerprint, location, netstats, notification, power, telecom, usagestats, and wifi.*

Resumo: *A análise de logs de dispositivos móveis tem se tornado uma ferramenta essencial na Perícia Computacional, especialmente no contexto de investigações criminais e auditorias de segurança. Dispositivos com Sistema Operacional Android, amplamente utilizados globalmente, geram uma quantidade substancial de dados de log que podem fornecer informações valiosas sobre as atividades do usuário, o comportamento do dispositivo e possíveis intrusões ou atividades suspeitas. Este artigo, pretende explorar a utilidade dos logs extraídos de dispositivos Android utilizando comandos ADB (Android Debug Bridge) para auxiliar em investigações forenses. Os arquivos de log analisados incluem account, alarm, battery, dbinfo, dumpsys, fingerprint, location, netstats, notification, power, telecom, usagestats e wifi.*

1 INTRODUÇÃO

A análise de *logs* de dispositivos móveis pode ser um componente fundamental nas atividades da Perícia Computacional, especialmente no contexto de investigações criminais. Observa-se um aumento significativo do uso de dipositivos móveis para comunicação, transações financeiras, armazenamento de informações pessoais e profissionais, gerenciamento de atividades cotidianas, dentre outras atividades, o que torna a análise de *logs* uma tarefa essencial para investigadores forenses e agentes de inteligência cibernética.

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`, `alarm`, `battery`, `bluetooth`, `dbinfo`, `dumpsys`, `fingerprint`, `location`, `netstats`, `notification`, `power`, `telecom`, `usagestats` e `wifi`. Cada um desses *logs* oferece uma visão única e específica das operações e atividades realizadas no dispositivo.

2. UMA BREVE REVISÃO DE LITERATURA

Diversos estudos recentes enfatizam a importância e os desafios dessa prática, explorando desde as técnicas de extração de dados até a análise detalhada de *logs*. Cam et al. (2023) analisaram a sistemas e subsistemas destinados à análise forense de dispositivos com Sistema Operacional Android, destacando a complexidade envolvida na extração e interpretação de dados extraídos [1]. Mahalik e Crognale (2023) abordam uma análise forense aprofundada de smartphones, com um foco particular nas técnicas e ferramentas utilizadas para a aquisição de dados de dispositivos Android [2]. Oxygen Forensic Detective, na sua atualização 14.2, introduz avanços significativos na extração de dados de dispositivos Android, oferecendo recursos aprimorados que permitem uma análise mais detalhada e precisa [3]. O trabalho de Lwin (2020) compara as abordagens forenses para dispositivos iOS e Android, ressaltando as diferenças e desafios inerentes a cada sistema operacional [4]. Casey et al. (2020) exploraram métodos avançados de aquisição de dados em dispositivos Android, enfatizando a necessidade de abordagens inovadoras para lidar com os desafios impostos por novos padrões de segurança e criptografia [5].

3. UMA SÍNTESE SOBRE OS ARQUIVOS DE *LOG*

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 a incidentes cibernéticos. Neste sentido, é relevante compreender, de forma breve, as informações contidas em cada um dos arquivos de *log* 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 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 dumpsys***, que é bastante abrangente, captura o estado atual do sistema, incluindo memória,

processos em execução, estado dos serviços e mais, sendo uma fonte importante de informações sobre o funcionamento interno do dispositivo. O ***log fingerprint*** relaciona-se ao sensor de impressões digitais do dispositivo, registrando eventos de autenticação biométrica e falhas, podendo ser usado para verificar tentativas de acesso não autorizado. 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 usagestats*** contém estatísticas detalhadas sobre o uso de aplicativos, incluindo tempo de uso, frequência de abertura e comportamento de uso, sendo importante para analisar os hábitos 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 ***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.

4. ESTUDO DE CASO, ANÁLISE DOS *LOGS* E RESULTADOS PRELIMINARES

Para o contexto em que este trabalho está inserido, um estudo de caso foi realizado, tomando-se como referência um conjunto de arquivos de *log* extraído de um *smartphone* com Sistema Operacional Android, resultante de um cenário em que o aparelho pode estar associado a um suspeito do cometimento de um determinado ilícito. Neste sentido, foram definidas 05 (cinco) hipóteses, na forma de **quesitos periciais**, para realização da análise forense nos exames periciais e apresentação das respostas, caso seja possível: 1) qual era a principal conta de usuário associada ao aparelho; 2) em que período do dia {`manhã, tarde, noite`} o usuário fez uso do aparelho com maior frequência; 3) quais aplicativos foram utilizados com maior frequência pelo usuário do aparelho; 4) o aparelho apresentou algum tipo de anormalidade durante o seu tempo de uso; 5) em quais redes o aparelho esteve conectado durante o seu uso; 6) há alguma informação *surpreendente* e que possa indicar caminhos para investigações no mundo real.

Em ambiente laboratorial, foram analisados os 14 (quatorze) arquivos de texto, contendo os *logs* extraídos via ADB. Essa análise foi realizada, exclusivamente, com uso da ferramenta NotePad++, não sendo utilizada qualquer ferramenta para análise automática de *logs*. Essa metodologia foi definida para que fosse possível ampliar a capacidade de aprendizado sobre a estrutura e conteúdo dos *logs*. Como ação complementar a este trabalho, uma ferramenta, baseada em raspagem (*scrapping*) de dados com expressões regulares (RegEx – *Regular Expression*), está em fase inicial de desenvolvimento, usufruindo do conhecimento aqui reportado.

De um modo geral, foi possível observar e localizar nos arquivos analisados, informações necessárias e suficientes para verificar a quais redes *wireless* o aparelho foi conectado, os dados de carga da bateria do dispositivo, a conta de usuário vinculada ao aparelho, quais aplicativos foram utilizados e as notificações emitidas durante o uso do aparelho. Na análise do ***log account,*** observou que um determinado nome de usuário estava vinculado ao aparelho, e as contas de usuário estavam vinculadas a esse nome. Na análise dos *logs* ***notification , power, telecom, usagestats e wifi***, verificou-se que o usuário fez o uso do aparelho em maior frequência no período noturno entre 19:00 e 22:00 horas. Na análise dos logs de ***notification*** e ***fingerprint***, as redes sociais, tais como WhatsApp, Facebook e Instagram, os aplicativos de banco, como é o caso do Santander, e outros aplicativos, tais como Justiça Eleitoral e Serasa, foram os mais utilizados pelo usuário. No caso da análise dos logs ***power, batery***, observou-se que o aparelho esteve em boas condições de uso, não sendo encontrados momentos de

instabilidade e/ou anormalidade que pudessem provocar algum dano ao aparelho. Por fim, nas análises de conectividade (***wifi***), obsevou-se que o aparelho esteve conectado a um conjunto de redes wireless, localizadas, principalmente, em duas cidades específicas, dentre outras que foram registradas.

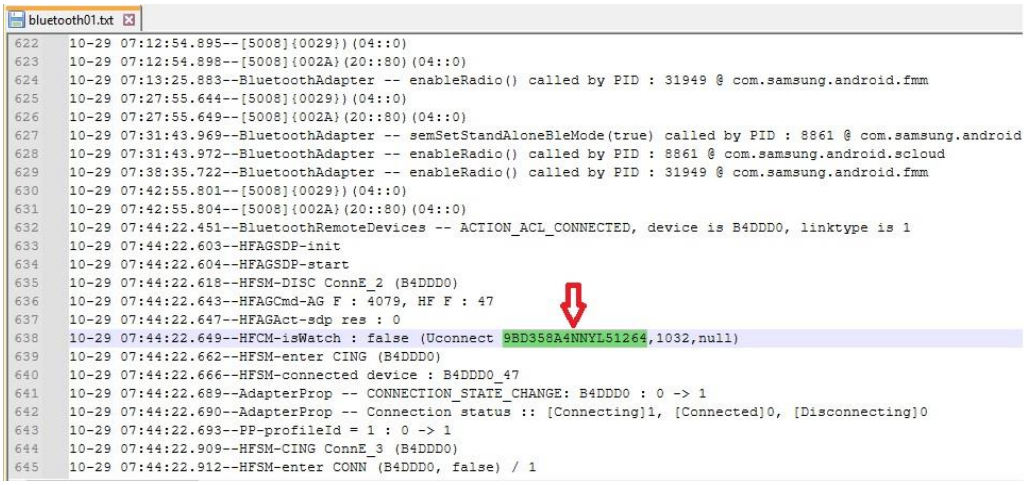

Figura 01: Informações extraídas do arquivo de log *bluetooth*

A **Figura 01** apresenta informações extraídas dos *logs* **bluetooth**, oferecendo informações surpreendentes para investigação, perícia e inteligência. Neste caso específico, pode-se observar a recuperação do número do chassi de um automóvel, que teve sua central multimídia conectada ao aparelho Android, do qual os *logs* foram extraídos e analisados nos exames periciais.

5. CONSIDERAÇÕES FINAIS

O avanço das técnicas e procedimentos da Perícia Computacional está diretamente relacionado à capacidade dos profissionais forenses em oferecer respostas confiáveis e precisas em investigações e ações de inteligência. Além disso, é possível avançar na direção da integração de algoritmos e técnicas da Inteligência Artificial, especialmente com aprendizado de máquina, par ampliar a capacidade de análise de *logs*, permitindo a detecção automatizada de padrões anômalos e a predição de atividades suspeitas. Estudos comparativos entre diferentes sistemas operacionais móveis, como Android e iOS, para identificar melhores práticas e adaptar técnicas eficazes de um sistema para outro, também estão em andamento no contexto em que este trabalho está inserido. Por fim, a análise de *logs* abre espaço para o desenvolvimento de programas de treinamento e capacitação contínua para profissionais forenses, focando nas últimas técnicas e ferramentas de análise de *logs*, bem como nas melhores práticas de segurança cibernética.

REFERÊNCIAS

[1] Cam, N.T., Duy, P.N., Khoa, N.H., Vien, L.H., Truoc, P.T., Huy, T.G. (2023). UIT-ADF: A System for Android Device Forensics. In: Vasant, P., Weber, GW., Marmolejo-Saucedo, J.A., Munapo, E., Thomas, J.J. (eds) Intelligent Computing & Optimization. ICO 2022. https://doi.org/10.1007/978-3-031-19958-5_27.

[2] Mahalik H, Crognale D. FOR585: Smartphone Forensic Analysis In-Depth. SANS Institute. 2023. Available from: https://www.sans.org

[3] Oxygen Forensic Detective. Advanced Android Extraction Updates in Detective 14.2. H-11 Digital Forensics. 2023. Available from: https://h11dfs.com

[4] H. H. Lwin, W. P. Aung and K. K. Lin, "Comparative Analysis of Android Mobile Forensics Tools," 2020 IEEE Conference on Computer Applications (ICCA), Yangon, Myanmar, 2020, pp. 1-6, DOI: 10.1109/ICCA49400.2020.9022838.

[5] Casey E, Bann M, Doyle M, Gerads E. Advanced data acquisition from Android mobile devices. Digital Investigation. 2020;32: S50-S59.