RESET DE FÁBRICA EM DISPOSITIVOS MÓVEIS: IMPLICAÇÕES FORENSES NA DESTRUIÇÃO DE PROVAS DIGITAIS

Marcelo Antônio Sampaio Lemos Costa[1*]

[1*]Instituto de Criminalística Afrânio Peixoto, Departamento de Polícia Técnica, Salvador, Bahia, Brasil
e-mail: marcelo.sampaio@dpt.ba.gov.br

Introdução

A apreensão de dispositivos móveis é uma etapa essencial em investigações criminais modernas, dada a vasta quantidade de informações armazenadas nesses equipamentos. Contudo, tem-se observado um aumento de situações em que alvos de mandados realizam o reset de fábrica do aparelho antes ou durante a intervenção policial, destruindo potenciais provas. Este artigo visa discutir os impactos técnicos e legais dessa prática.

Objetivos

- Analisar os impactos técnicos do reset de fábrica em dispositivos móveis durante ações de busca e apreensão;
- Identificar os artefatos que podem indicar a realização do reset e sua temporalidade;
- Apontar os aspectos legais e as possibilidades de responsabilização penal pela destruição de provas digitais;
- Apresentar metodologias periciais aplicáveis na identificação e mitigação desse cenário.

Metodologia

O presente trabalho é de natureza aplicada, com abordagem qualitativa e exploratória. A metodologia adotada incluiu: (i) revisão bibliográfica em fontes técnico-científicas de domínio público, como manuais do NIST, SWGDE, publicações acadêmicas e literatura forense; e (ii) avaliação prática de dispositivos móveis submetidos a reset, por meio de extrações e análises técnicas utilizando a ferramenta Cellebrite Inseyets PA.

Foram examinados registros remanescentes, logs e estruturas de partição para verificar a persistência de dados e indicadores de obstrução digital em dez dispositivos de telefonia móvel conforme Tabela 1 a seguir:

Marca	Modelo	Versão S.O.
Apple	iPhone 6	12.5.7 (16H81)
Apple	iPhone 15	18.3.2 (22D82)
Apple	iPhone X	16.7.11 (20H360)
Motorola	Moto G42	Android 13
Samsung	SM-J610G (J6)	Android 9
Samsung	SM-G610M (J7)	Android 7
Samsung	SM-G9650 (Gal. 9+)	Android 10
Samsung	SM-A705MN (Gal. A70)	Android 9
Xiaomi	Redmi Note 11	Android 11
Xiaomi	Redmi Note 12	Android 15

Tabela 1 - Dispositivos

Resultados e Discussão

A análise demonstrou que, mesmo após o reset de fábrica, é possível identificar indícios técnicos relacionados a dados persistentes. No estudo conduzido, os dispositivos foram submetidos a reset com data e hora controladas, permitindo a observação precisa das alterações e registros do sistema. A perícia digital comprovou tecnicamente que o reset foi executado de forma deliberada e em momento compatível com a ação policial. O cruzamento desses elementos com os dispositivos legais permitiu caracterizar a tentativa de obstrução à investigação criminal, conforme o artigo 347 do Código Penal e o artigo 2º da Lei 12.850/13.

Verificou-se ainda que alguns dados permanecem após o reset, localizados em áreas específicas do sistema. Em dispositivos Apple, informações como o status de redefinição são extraídas por ferramentas como o Cellebrite Inseyets, sob o campo DeviceInfoFactoryReset. Em aparelhos Samsung, registros similares podem estar na pasta /efs, e em dispositivos Xiaomi, na pasta /data/property/persistent_properties. Isso reforça a necessidade de mapeamento contínuo dos artefatos conforme a versão do sistema, o modelo e o fabricante.

Conclusão

A destruição de provas digitais por reset de fábrica representa uma ameaça recorrente em operações de campo. No entanto, é tecnicamente viável comprovar que a exclusão foi realizada no momento do cumprimento do mandado. A pronta atuação pericial, com ferramentas adequadas e conhecimento especializado, é essencial para mitigar perdas e embasar a responsabilização legal dos envolvidos. Compreender tecnicamente os efeitos do reset de fábrica permite aprimorar a resposta pericial diante de tentativas de obstrução digital.

Palavras-chave

reset de fábrica; destruição de provas; dispositivos móveis; logs persistentes

Agradecimentos

Departamento de Polícia Técnica do Estado da Bahia
ASBAC – Associação dos Peritos Criminais do Estado da Bahia

Referências bibliográficas

[1]NIST SP 800-101 Rev.1
[2]SWGDE Best Practices for Mobile Device Evidence Collection
[3]Android Open Source Project: https://source.android.com
[4]Casey, E. Digital Evidence and Computer Crime
[5]Carrier, B. File System Forensic Analysis