



GOVERNO DO ESTADO DE PERNAMBUCO
SECRETARIA DE DEFESA SOCIAL
GERÊNCIA GERAL DA POLÍCIA CIENTÍFICA
INSTITUTO DE CRIMINALÍSTICA PROFESSOR ARMANDO SAMICO



Dados da Origem:

Nº PROTOCOLO: 889172322017

Ofício: 9043.01.000072/2017/2017 - DEPARTAMENTO DE HOMICIDIOS E PROTECAO A PESSOA - OLINDA

REQUISITANTE: Sra. Delegada FABIANA FERREIRA LEANDRO



Identificação do Laudo: lavuoUwMffh-B08vZbQoFRURpaafgHret-adKH2rvGs1

GGPOC - IC - ICPAS (Recife) - GEPH-DHPP

Laudo Pericial: **24.645/2020**

Dados do exame:

NATUREZA: ANÁLISE EM CELULAR(S)

LOCAL DO EXAME: RUA DOUTOR JOAO LACERDA, Nº 395, CORDEIRO - RECIFE

DATA DO EXAME: 24/08/2020

ENVOLVIDO(S):

Destinatário:

9ª DPH - DHMN

PERITO(A) CRIMINAL: Dr(a). BETSON FERNANDO DELGADO DOS SANTOS ANDRADE

NÃO ACOMPANHA(M) PEÇA(S)



Sumário

1 HISTÓRICO DO CASO	2
2 MATERIAL RECEBIDO PARA ANÁLISE	2
2.1 APARELHO C1	2
3 DO OBJETIVO PERICIAL	5
4 CONSIDERAÇÕES GERAIS	5
5 EXAMES	5
5.1 DOS PROCEDIMENTOS GERAIS	5
5.2 DO APARELHO C1	6
5.2.1 ANÁLISES PRELIMINARES	6
5.2.2 PROCESSO DE EXTRAÇÃO	6
6 CONCLUSÕES	7
7 ENCERRAMENTO	8



LAUDO PERICIAL EM EQUIPAMENTOS ELETRÔNICOS
(TELEFONE CELULAR MÓVEL)
CASO N°158.12/2017 - REP N°1125/2018

1. HISTÓRICO DO CASO

Foi recebido e protocolado pelo Setor Administrativo do Grupo Especializado em Perícias de Homicídios (GEPH), o ofício nº 9043.01.000072/2017, datado de 30/10/2017, incluso no processo SIGEPE nº 8891723-2/2017, oriundo da 9ª Delegacia de Polícia de Homicídios - Metropolitana Norte (9ª DPH - DHMN), a pedido do(a) Delegado(a) de Polícia FABIANA FERREIRA LEANDRO, solicitando Perícia em equipamento eletrônico - aparelho de telefonia móvel, ao Setor de Meios Informáticos e Equipamentos Eletrônicos do GEPH, conforme cópia em anexo. Em 24/08/2020, portanto, o chefe deste setor exarou despacho designando o Perito Criminal BETSON FERNANDO DELGADO DOS SANTOS ANDRADE para proceder ao respectivo exame solicitado e confeccionar o respectivo laudo.

2. MATERIAL RECEBIDO PARA ANÁLISE

2.1. APARELHO C1

Tratava-se de um aparelho de telecomunicação celular de marca Samsung, modelo SM - J500M/DS, cor preta, IMEI(s) 352525087847455 e 352600087847456, contendo, em seu interior:

- Bateria;
- SIM card, denominado SC1, da operadora "Oi" e número ICCID 8955313929 891177965.

A(s) figura(s) abaixo exibe(m) os itens acima listados,



INSTITUTO DE CRIMINALÍSTICA
GEPH/DHPP
SDS GGPOC

GOVERNO DO ESTADO
SECRETARIA DE DEFESA SOCIAL
Pernambuco
GERÊNCIA GERAL DE POLÍCIA CIENTÍFICA
INSTITUTO DE CRIMINALÍSTICA PROF. ARMANDO SAMICO



Figura 1: Fotografia dos equipamentos relativos ao aparelho C1.



Figura 2: Fotografia dos equipamentos relativos ao aparelho C1.



Figura 3: Fotografia dos equipamentos relativos ao aparelho C1.



Figura 4: Fotografia dos equipamentos relativos ao aparelho C1.



3. DO OBJETIVO PERICIAL

A perícia tem a finalidade de verificar o estado em que os equipamentos se encontram, bem como de extrair dados encontrados na memória dos dispositivos eletrônicos encaminhados para perícia, visando responder aos quesitos do ofício supracitado.

4. CONSIDERAÇÕES GERAIS

Com fulcro na correta interpretação dos exames e análises por parte do leitor deste trabalho técnico, se faz necessário realizar algumas observações, a saber:

- Datas e horários listados a seguir correspondem aos dados armazenados na memória dos aparelhos. Esses dados só correspondem à realidade se o relógio e o calendário do equipamento estiverem devidamente ajustados no momento das respectivas mensagens/ligações;
- Os históricos de mensagens e de chamadas, bem como arquivos de imagens e de vídeos, podem ser apagados pelo usuário. Nem todos os dados apagados que são recuperados pelas técnicas forenses estão íntegros, pois podem estar totalmente ou parcialmente corrompidos;
- Arquivos apagados nem sempre são restaurados em sua totalidade;
- Não disponho de elementos materiais para informar se o aparelho recebido para análise foi objeto de roubo ou furto. Esta informação pode ser obtida pela autoridade policial, junto ao CEMI – Cadastro de Estações Móveis Impedidas;
- Através do código IMSI é possível identificar, junto à operadora telefônica, o assinante da linha. Já o ICCID representa o número de identidade do cartão SIM usado no parelho;
- Para a identificação dos arquivos digitais, são utilizadas as Somas de Verificação, que são assinaturas digitais (sequências alfanuméricas) obtidas através de algoritmos (MD5 e SHA1), que resultam numa identificação única;
- O equipamento recebido para exames segue com o Laudo Pericial.

5. EXAMES

5.1. DOS PROCEDIMENTOS GERAIS

O exame em aparelho celular móvel inicia primeiramente com uma higienização através de material absorvente embebido em etanol. Concluída esta etapa, é realizada uma inspeção visual para verificar sua integridade física e observar se o mesmo encontra-se apto para uso. Além disso, é verificado se a bateria está em boas condições de uso e se possui energia suficiente para manter o aparelho operante e dar continuidade ao exame. Caso não possua energia, será usado um carregador específico para carregá-la. Por último, caso o celular



não acompanhe a bateria de fábrica, ele será conectado a um cabo específico fornecido pelo pacote forense UFED.

Após essa etapa de preparação do aparelho, é iniciado o processo de extração dos dados armazenados, que consiste em submeter o dispositivo à análise por equipamento ou *software* forense adequado, visando obter o máximo de dados possível, e consequentemente dar luz aos quesitos elaborados pela autoridade. A extração é capaz de obter dados como: bate-papos (Whatsapp, Facebook Messenger, Instagram, entre outros), contatos, registro de chamadas, *e-mails*, histórico da web, locais do dispositivo, mensagens SMS, redes sem fio conectadas, registro de chamadas, imagens, vídeos, áudios, etc. Além disso, arquivos apagados podem ser recuperados em determinados casos, uma vez que a recuperação de arquivos é feita em espaços ainda não alocados, e à medida que novos arquivos são criados, tais espaços são ocupados, sobrepondo os dados anteriores, e deste modo dificultando a recuperação de informações apagadas. O êxito da extração dos dados depende de diversos fatores, tais como: aparelho bloqueado/desbloqueado, versão do sistema operacional, *patch* de segurança, tipo do sistema operacional (iOS, Android, etc.), fabricante, dentre outros. Recomenda-se que o celular encaminhado esteja desbloqueado, ou que seja informado o padrão/senha/PIN de desbloqueio, pois alguns algoritmos criptográficos usados nos aparelhos atuais não são possíveis de superar, prejudicando o exame pericial.

Por fim, uma vez realizada a extração, um relatório será gerado com o conteúdo de interesse solicitado no ofício e encaminhado por mídia anexa ao Laudo Pericial.

5.2. DO APARELHO C1

5.2.1. ANÁLISES PRELIMINARES

Ao ser iniciada a análise no referido aparelho, não foi observada a existência de avarias à mera inspeção externa. Após executado o processo de ligar o aparelho, foi constatado ele se encontrava em regular estado de operação. Também foi verificado que seu sistema operacional era o Android, e se encontrava em modo avião, segundo as recomendações para a preservação da cadeia de custódia.

5.2.2. PROCESSO DE EXTRAÇÃO

Seguiu-se, então, à extração e análise do aparelho C1, através do Equipamento UFED Touch, da empresa Cellebrite. Foram realizadas tentativas de extração, segundo o descrito a seguir:

1. No aparelho C1 (extração física);
2. No *SIM card* SC1 (extração lógica).

Como resultado da extração, foram gerados dois arquivos:

- Relatório completo da extração, em formato PDF, com tamanho 60 MB, e nome "**Relatório.pdf**";

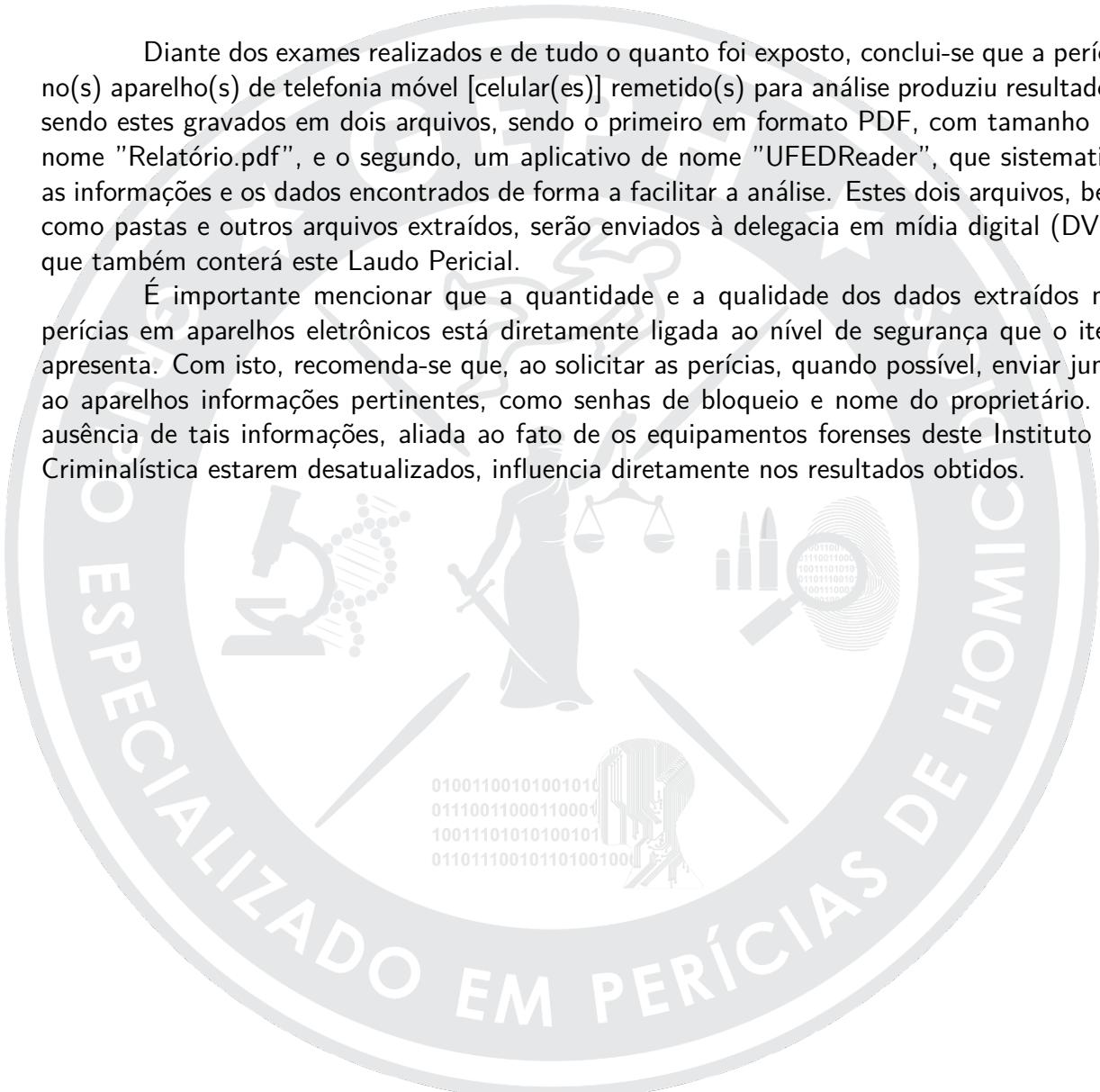


- Aplicativo UFEDReader, que sistematiza dos dados de forma a criar um ambiente de leitura e análise facilitado.

6. CONCLUSÕES

Diante dos exames realizados e de tudo o quanto foi exposto, conclui-se que a perícia no(s) aparelho(s) de telefonia móvel [celular(es)] remetido(s) para análise produziu resultados, sendo estes gravados em dois arquivos, sendo o primeiro em formato PDF, com tamanho , e nome "Relatório.pdf", e o segundo, um aplicativo de nome "UFEDReader", que sistematiza as informações e os dados encontrados de forma a facilitar a análise. Estes dois arquivos, bem como pastas e outros arquivos extraídos, serão enviados à delegacia em mídia digital (DVD) que também conterá este Laudo Pericial.

É importante mencionar que a quantidade e a qualidade dos dados extraídos nas perícias em aparelhos eletrônicos está diretamente ligada ao nível de segurança que o item apresenta. Com isto, recomenda-se que, ao solicitar as perícias, quando possível, enviar junto ao aparelhos informações pertinentes, como senhas de bloqueio e nome do proprietário. A ausência de tais informações, aliada ao fato de os equipamentos forenses deste Instituto de Criminalística estarem desatualizados, influencia diretamente nos resultados obtidos.





7. ENCERRAMENTO

Eu, **BETSON FERNANDO DELGADO DOS SANTOS ANDRADE**, Perito Criminal deste Instituto de Criminalística no GEPH/DHPP, confeccionei o presente **LAUDO PERICIAL EM EQUIPAMENTOS ELETRÔNICOS (TELEFONE CELULAR MÓVEL)**, consistindo de arquivo digital em formato pdf, certificado em meio digital (Certificado ICP - Brasil), possuindo quatro (4) figuras com legendas explicativas, e oito(8) páginas à exceção da capa, em tamanho oficial, encimadas pelo timbre do Estado de Pernambuco. É importante mencionar que versões impressas deste documento equivalem a cópias não autenticadas, visto que somente o arquivo PDF contém a assinatura digital passível de verificação e validação por uma Autoridade Certificadora.

Segue em mídia tipo DVD o Laudo Pericial em tela, além dos dados extraídos e organizados em relatório digital.

SECRETARIA DE DEFESA SOCIAL – GERÊNCIA GERAL DE POLÍCIA CIENTÍFICA – INSTITUTO DE CRIMINALÍSTICA PROFESSOR ARMANDO SAMICO – GRUPO ESPECIALIZADO EM PERÍCIAS DE HOMICÍDIOS (GEPH)-DO IC - DHPP.

Betson Fernando Delgado dos Santos Andrade
Perito Criminal
Matrícula 386.990-3

0100110010100101
01110011000110001
10011101010100101
01101110010110100100

Recife, 24 de agosto de 2020.