1- HISTÓRICO:

Em virtude ao atendimento a REQUISIÇÃO DE PERÍCIA Nº 00001-2024-105756-7, datada de 26/04/2024, referente a OCORRÊNCIA Nº 00481/2024-100062-0 – QUATRO BOCAS – DELEGACIA DE POLICIA – 3ª RISP, e assinado pela autoridade acima mencionada, solicitando Perícia em aparelho celular a fim de extração de dados (registro de chamadas, contatos, fotos, imagens, áudios, vídeos, conversas de aplicativos e de mensagens de texto) e análise de conteúdo, a fim de colaborar com as investigações de crimes de tráfico de drogas. O aparelho de telefonia celular foi recebido pelo perito signatário para exame pericial onde se constatou que o aparelho encontrava-se lacrado no saco de evidências (ver Ilustração 01 e 02), em seguida foi deslacrado pelo Perito. Após ligar o aparelho, o Perito observou que o mesmo estava em modo avião conforme Ilustração 06.

2 - DO OBJETIVO:

A presente perícia tem por finalidade a extração de dados (ativos e recuperados) e análise de conteúdo com base na Requisição de Perícia supracitada.

3 - DO MATERIAL:

Foi encaminhado para exame 01 (um) aparelho celular na cor preta, marca XIOMI, modelo REDMI 10A (Xiaomi 220233L2G), número de série 38902/62YP12815, IMEI (slot 1) 861144064580420 / 78, possuindo os itens a seguir:

- 01 (um) cartão SIM, da operadora de telefonia móvel CLARO, ICCID 89550532990145516024, conforme Ilustração 07.

- 01 (um) cartão SIM, da operadora de telefonia móvel CLARO, ICCID 89550537970033180427, conforme Ilustração 08.

4 - DA METODOLOGIA:

A metodologia aplicada durante a perícia foi a seguinte:

- Caracterização do material encaminhado a exame pericial;

- Extração/decodificação dos dados;

- Composição e redação do laudo pericial.

5 - CONSIDERAÇÕES DE ORDEM TÉCNICO-PERICIAIS:

As informações de data e hora de cada registro refletem a data e a hora configurada no aparelho no momento em que ocorreu o evento. Sendo, portanto, tidas somente como referência, podendo não refletir a data e hora real em que ocorreu o evento.

- Hash: é uma sequência de bits que busca identificar um arquivo ou informação unicamente. Um método para transformar dados de tal forma que o resultado seja (quase) exclusivo.

6 - DO EXAME

Inicialmente foi realizada a análise e inspeção do material para constatar o seu correto funcionamento. Em seguida o perito iniciou os exames para levantamento e extração dos dados armazenados no mesmo. Os dados encontrados foram transcritos abaixo:

6.1 - FUNCIONAMENTO:

O aparelho apresentou funcionamento normal durante os exames. O aparelho apresenta danos e fissuras em seu display (ver “Ilustração 04”).

6.2 – EXTRAÇÃO E DECODIFICAÇÃO DOS DADOS:

Foi realizada a extração e decodificação dos dados armazenados no aparelho de telefonia celular utilizando-se a Ferramenta Forense “UFED 4PC” (versão 7.68.0.809) e o Software Forense “PHYSICAL ANALYZER” (versão 7.67.0.15) ambos da CELLEBRITE. A extração realizada foi do tipo “File System ”. Com o procedimento foi possível obter arquivos de mensagens sms’s e de aplicativos, fotos, imagens, áudios, vídeos, documentos, localização GPS, histórico da web, lista de contatos e registro de chamadas.

Para atendimento a requisição pericial, os dados do aparelho celular (mensagens sms’s e de aplicativos, fotos, imagens, áudios, vídeos, documentos, localização GPS, histórico da web, lista de contatos e registro de chamadas), foram salvos em relatórios gerados pela Ferramenta Forense “UFED 4PC” e o Software Forense “PHYSICAL ANALYZER”. O relatório encontra-se disponível no DVD-R da marca MAXPRINT com capacidade de 4.7 GB, anexo ao laudo pericial, no caminho da pasta “\Relatório\_UFED\_2024.01.032308\Xiaomi\_220233L2G”, podendo ser visualizado por meio da execução do arquivo “CellebriteReader.exe”.

Em análise ao conteúdo foi possível identificar informações com relevância ao caso.

- Foram encontradas mensagens suspeitas no status do aplicativo WhatsApp do usuário “Deus No Controle” (559184391093@s.whatsapp.net), conforme Ilustração 11.

- Foram marcadas TAG’s em imagens suspeitas de transações bancárias (total de 350) no aparelho de telefonia celular em questão, conforme Ilustração 09 e 10.

Pode haver outros elementos de interesse a investigação.

7 - ANEXOS INTEGRANTES DO LAUDO:

Uma mídia óptica (DVD-R) da marca MAXPRINT foi gravada e acompanha este laudo na forma de anexo digital. Os diretórios e arquivos que foram gravados no anexo digital estão descritos no item 6 – DO EXAME. A mídia óptica utilizada não permite alteração de seus dados após a gravação. Os valores de código hash de cada arquivo foram calculados utilizando o algoritmo MD5 e estão listados, seguidos do nome de seu respectivo arquivo, no arquivo "Hashes.txt". O arquivo "Hashes.txt" encontra-se gravado no diretório raiz da mídia óptica e o valor de seu código hash calculado utilizando o algoritmo MD5 é: “f143fe4fef58d3c5139600eb2bf8f5a9”.

8 - CONCLUSÃO:

Diante da minuciosa análise realizada no aparelho celular REDMI 10A (Xiaomi 220233L2G), e dos dados obtidos, o perito concluiu o relatório sobre o funcionamento e os dados armazenados no dispositivo, conforme descrito no item 3 - DO MATERIAL. As informações detalhadas encontram-se transcritas no laudo, disponível no item 6 - DO EXAME. O presente laudo, assinado pelo perito responsável, está acompanhado de uma mídia óptica como anexo digital. O material periciado está sendo encaminhado devidamente acondicionado em saco de evidências, devidamente lacrado com o lacre de A230069731, e será mantido na Central de Custódia da DECCC (Diretoria Estadual de Combate a Crimes Cibernéticos) da Polícia Civil do Estado do Pará.