



GOVERNO DO ESTADO DE RORAIMA
"Amazônia: Patrimônio dos Brasileiros"
POLÍCIA CIVIL DE RORAIMA
INSTITUTO DE CRIMINALÍSTICA
"PERITO CRIMINAL DIMAS ALMEIDA"



Laudo nº 053/2021/SEPAEL/DPI/IC/PC/SESP/RR

LAUDO DE EXAME PERICIAL CRIMINAL

Aos vinte e seis (26) dias do mês de julho (07) do ano dois mil e vinte e um (2021), no SEPAEL (Setor de Perícias em Audiovisual e Eletrônicos - Laboratório de Fonética e Informática Forense) do Instituto de Criminalística da Polícia Civil de Roraima, em conformidade com a legislação vigente, foi designado pelo Diretor do INSTITUTO DE CRIMINALÍSTICA DO ESTADO DE RORAIMA, Perito Criminal STTEFANI PINHEIRO RIBEIRO, o Perito Criminal ANAXIMANDRO SOARES COIMBRA para realizar os exames pertinentes, com o objetivo de ser atendida a solicitação da Excelentíssima Senhora Delegada de Polícia Civil, **Gianne Delgado Gomes**, da Delegacia de Repressão a Entorpecentes - DRE, contida na **Requisição de Exame Pericial 134/2021-DRE**, datada de 23/07/2021, referente ao **APF nº 1587/2021-DRE**, descrevendo com a verdade tudo o quanto possa interessar à Justiça e atendendo ao solicitado abaixo transcrito.

"Identificação / Descrição dos objetos";

"Qual a lista de contatos? (agenda telefônica com descrição dos nomes e telefones)";

"Qual o histórico das ligações recebidas e efetuadas?";

"Transcrição das mensagens (SMS, MMS)";

"Qual linha(s) telefônica(s) (número) era(m) utilizado(s) no aparelho e qual a operadora?";

"Outros dados que julgar úteis".



OC.053.2021



GOVERNO DO ESTADO DE RORAIMA
“Amazônia: Patrimônio dos Brasileiros”
POLÍCIA CIVIL DE RORAIMA
INSTITUTO DE CRIMINALÍSTICA
“PERITO CRIMINAL DIMAS ALMEIDA”



Laudo nº 053/2021/SEPAEL/DPI/IC/PC/SESP/RR

1 DO MATERIAL RECEBIDO

1.1 Identificação/descrição

#Item 01 – Aparelho Celular da marca Motorola®, de cor branca, modelo: XT2013-1, IMEI: 354148109979574, com um chip SIMCARD com logotipo da Operadora VIVO®², (ICCID³ nº 89551094160065336692960), desprovido de: cartão de memória removível, carregador de bateria, cabos e demais acessórios, doravante denominado simplesmente **Celular.1**.



#Item 02 – Aparelho Celular da marca Xiaomi®, de cor grafite, modelo: M200C3MG. IMEI1: 864066059871976. IMEI2:864066059871984, com dois chips SIMCARD, um com logotipo da Operadora VIVO®, (ICCID nº 8955109526001580044980), outro com logotipo da Operadora CLARO®, (ICCID nº 89550531970040250854), Com um Micro SD San Disk®, com capacidade nominal de 2GB, desprovido de: carregador de bateria, cabos e demais acessórios, doravante denominado simplesmente **Celular.2**.



2 DOS EXAMES

Com o apoio dos equipamentos e programas computacionais que compõe a estação laboratorial de Fonética e Informática Forense, procedeu-se aos exames necessários sobre o material descrito no item “1 DO MATERIAL RECEBIDO”, a fim de atender à requisição em epígrafe.

Dentre os programas utilizados, merece destaque o **UFEDTouch⁴** (*Universal Forensic Extraction Device*) que é uma ferramenta especializada na análise de dispositivos

²Com o programa de **Mobilidade** de operadora por parte dos usuários, é possível que o Chip SimCard seja de uma operadora e o número e a conta de outra.

³O **Cartão SIM** ou **SIMCARD** (SubscriberIdentity Module - Módulo de Identificação do Assinante) é utilizado em aparelhos de telefonia celular para identificar o usuário no sistema, e costuma armazenar dados como informações do assinante, agenda, preferências (configurações), serviços contratados, SMS e outras informações. É visualmente identificado e individualizado pelo número serial do chip, único no mundo inteiro, gravado no corte plug-in, denominado ICCID – IntegratedCircuitCardIdentification.

⁴O “**UFEDTouch**” é um dispositivo portátil de perícia forense digital de última geração, desenvolvida pela **Cellebrite®** para acelerar de forma inteligente a obtenção de provas forenses, garantindo sempre um acesso seguro e confiável às provas forenses e, garantindo a cadeia de custódia.

Assinatura

O verso deste Laudo segue em branco



GOVERNO DO ESTADO DE RORAIMA
“Amazônia: Patrimônio dos Brasileiros”
POLÍCIA CIVIL DE RORAIMA
INSTITUTO DE CRIMINALÍSTICA
“PERITO CRIMINAL DIMAS ALMEIDA”



Laudo nº 053/2021/SEPAEL/DPI/IC/PC/SESP/RR

móveis como celulares e tablets. Tal ferramenta faz uma varredura no aparelho e disponibiliza os dados coletados na forma de um relatório próprio, navegável, interativo, contendo diversas informações e detalhes sobre cada arquivo capturado.

3 DOS DADOS ENCONTRADOS NO DISPOSITIVO.

Considerando o solicitado no expediente requisitório, informo que o conteúdo dos equipamentos examinados, tais como imagens, vídeos, mensagens SMS, registros com assuntos e conteúdos diversos, foram extraídos em consonância com a descrição que se segue:

O aparelho **Celular.1** (*Motorola branco*) e **Celular.2** (*Xiaomi grafite*) se apresentavam **funcionantes e sem senha de bloqueio de tela inicial**. No entanto, não foi possível aplicar as configurações de “**Acesso Root**” dos Aparelhos que, somada às configurações dos celulares e à política de segurança interna dos próprios equipamentos, impediu o acesso completo ao conteúdo da memória interna de maneira convencional, através do programa “UFED”⁵, e assim impedindo a plena extração de dados. Todos os dados disponíveis foram extraídos pelo UFED.

Não foram extraídas: dados contidos na "nuvem", mensagens de WhatsApp e redes sociais.

Todos os dados encontrados podem ser acessados através “LaudoEletrônico”, disponibilizado na mídia eletrônica em anexo, contendo diversas informações e detalhes sobre cada arquivo capturado, devendo, para tanto, ser executado conforme o Tutorial disponibilizado na raiz do Anexo Eletrônico.

Salientamos que, no caso dos aparelhos celulares sem o “**Acesso Root**”, nos remetemos ao posicionamento de que não será possível a extração de todas as informações “da árvore de programação” do aparelho, resultando em uma extração “parcial de dados”.

Vide Item **6 CONSIDERAÇÕES TÉCNICO-PERICIAIS**.

⁵ É de bom alvitre informar que neste SEPAEL percebemos que a velocidade de atualização dos equipamentos forenses (tal qual o UFEDTouch) não acompanha a velocidade de atualização de “patches” de segurança de aparelhos celulares e afins. Ou seja, as medidas de segurança para os dados de usuários de aparelhos celulares, são as mesmas que dificultam, e até mesmo impedem, as extrações de dados forenses que embasam as investigações policiais e os demais procedimentos forenses voltados para a persecução penal.



GOVERNO DO ESTADO DE RORAIMA
“Amazônia: Patrimônio dos Brasileiros”
POLÍCIA CIVIL DE RORAIMA
INSTITUTO DE CRIMINALÍSTICA
“PERITO CRIMINAL DIMAS ALMEIDA”



Laudo nº 053/2021/SEPAEL/DPI/IC/PC/SESP/RR

Neste ponto cumpre salientar que o citado equipamento UFED, utilizado para realizar as extrações dos dados e conteúdo multimídia dos celulares neste Laboratório de perícias, encontra-se com suas bases de dados desatualizadas desde julho de 2018, o que nos leva a inferir que os erros e falhas na extração dos celulares certamente tem relação direta com o fato citado.

É de bom alvitre informar que, neste SEPAEL, percebemos que a velocidade de atualização dos *softwares* dos equipamentos forenses – *Updates* - (tal qual o UFED Touch) não acompanha a velocidade de atualização de “patches” de segurança de aparelhos celulares e afins.

Ou seja, as medidas de segurança para os dados de usuários de aparelhos celulares, são as mesmas que dificultam, e até mesmo impedem, as extrações de dados forenses que embasam as investigações policiais e os demais procedimentos forenses voltados para a persecução penal.

Por fim, considerando a extração parcial de dados, supramencionada, cumpre salientar, que as respostas aos quesitos contidos na requisição serão embasadas nos dados extraídos pelo programa UFED, ficando a cargo da Autoridade Requisitante a análise do conteúdo dos equipamentos e emissão de juízo de valor sobre o conteúdo coligido. Uma vez verificado o material com interesse probatório que não tenha sido abrangido pela extração do software, solicitamos encaminhar nova requisição para nova tentativa de extração do conteúdo em específico.

4 DA PRESERVAÇÃO E INTEGRIDADE DO MATERIAL (Hashing)

Como forma de assegurar a integridade do material original, foi aplicado ao conteúdo do Anexo Eletrônico, o autenticador “MD5Summer⁶”, que realiza um cálculo de dispersão criptográfica unidirecional de 128 bits sobre registros digitais, e entrega como resultado um arquivo de HashMD5. Assim, qualquer adulteração do arquivo de origem do material encaminhado, poderá ser descoberta com o confronto da numeração hexadecimal gerada pelas chaves criptográficas contidas em nossos registros devendo, para tanto, ser executado conforme o Tutorial disponibilizado na raiz do Anexo Eletrônico.

⁶ Autenticador para dados binários.






Laudo nº 053/2021/SEPAEL/DPI/IC/PC/SESP/RR

5 DO ACESSO E LEITURA DOS DADOS LEVANTADOS

Em função da grande quantidade de informações encontradas e compiladas, os dados citados seguem gravados em um Anexo Eletrônico (CD/DVD), que é parte integrante da presente peça pericial, ficando à cargo da autoridade requisitante a emissão de um juízo valorativo sobre os dados encontrados.

APÓS CONECTADO O DVD, navegue pelo Windows Explorer® até a pasta “RELATÓRIO UFED”, clique sobre o arquivo “LaudoEletronicoUFEDReader.exe”, como na ilustração abaixo. Isto irá abrir o Laudo Eletrônico, que contém informações detalhadas sobre o “item” em questão.

Nome	Data de modificaç...	Tipo	Tamanho
 LaudoEletronicoUFEDReader.exe	27/03/2016 08:17	Aplicativo	136.674 KB
 ReportTabletDazz.ufdr	28/09/2016 06:39	Arquivo UFDR	217.108 KB
 UFEDReader.log	03/10/2016 15:32	Documento de Te...	21 KB

Aguarde o carregamento do programa. O tempo de carregamento é variável e depende das configurações de cada computador. Siga as instruções exibidas na tela.

OBS.1 Caso o Computador tenha dificuldade ou problemas para execução do programa “LaudoEletronicoUFEDReader.exe”, sugerimos copiar a pasta “UFED” e colar em um novo diretório local, e novamente executar o programa “LaudoEletronicoUFEDReader.exe” que se encontra dentro da mesma. Esse procedimento acelera consideravelmente a capacidade de processamento e abertura do citado Laudo eletrônico.

6 CONSIDERAÇÕES TÉCNICO-PERICIAIS

Inicialmente, é de bom alvitre informar que este SEPAEL está equipado com *softwares* (programas) e *hardwares* (equipamentos) que trabalham com “Bloqueio de Escrita”, ou seja, durante os exames dos dispositivos periciados, é permitido ao usuário, neste caso o examinador, somente a leitura e cópia dos dados do mesmo.

Esta técnica impede que o usuário modifique qualquer banco de dados do equipamento em exame, que pode ser a memória interna de um Pendrive, Notebook, ou Celular, por exemplo, impedindo que haja modificação no estado inicial dos dados

O verso deste Laudo segue em branco



GOVERNO DO ESTADO DE RORAIMA
“Amazônia: Patrimônio dos Brasileiros”
POLÍCIA CIVIL DE RORAIMA
INSTITUTO DE CRIMINALÍSTICA
“PERITO CRIMINAL DIMAS ALMEIDA”



Laudo nº 053/2021/SEPAEL/DPI/IC/PC/SESP/RR

contidos na memória do dispositivo em exame.

6.1. O acesso ROOT

Antes de tudo precisamos lembrar que o "Android / IOS (do iPhone)" é um sistema operacional, tal qual o Windows e Linux. Assim, do mesmo jeito que no Windows, para que certas coisas a serem feitas, tais como mudanças profundas no sistema, com acesso a raiz de programação, é necessário que o usuário tenha **privilegios de administrador**. No Android / IOS também acontece: é o “**Acesso Root**”.

Desta forma, sem o Acesso Root, não é possível acessar a “árvore” de programação do sistema e verificar o código de programação, bem como programas instalados na raiz do sistema. A pesquisa de qualquer informação privilegiada sobre essa árvore de programação, em um equipamento Android / IOS, sem “Acesso Root” é, sem dúvida, prejudicada, por conta da proteção intrínseca deste código de programação.

6.2. O Android 7.0 e Superior e o IOS do iPhone

Inicialmente, lembramos que o UFED que faz a extração dos celulares é um equipamento de ponta mas não é à prova de falhas. Por conta das configurações de cada aparelho celular, principalmente as do Sistema Android 7.0 (e superior) e do Sistema IOS do iPhone, somada à nova política de segurança interna dos equipamentos da Geração 5 (G5) e superiores, é possível que o mesmo impeça o acesso ao conteúdo da memória interna de maneira convencional através do UFED, e muitas informações podem estar suprimidas no relatório UFED, uma vez que congregam fortes medidas de segurança para dados dos usuário.

Na outra ponta, percebemos que a velocidade de atualização dos equipamentos forenses (tal qual o UFED Touch) não acompanha a velocidade de atualização de “patches” de segurança de aparelhos celulares e afins, ou seja, as medidas de segurança para os dados de usuários de aparelhos celulares são as mesmas que dificultam, e até mesmo impedem, as extrações de dados forenses que embasam as investigações policiais e os demais procedimentos forenses voltados para a persecução penal. Em tempo, informo que essas novas medidas de segurança de dados dos usuários de aparelhos celulares, qual sejam Geração 5 (e superior) de Celulares e o Sistema Android 7.0 e superior, bem como do



GOVERNO DO ESTADO DE RORAIMA
“Amazônia: Patrimônio dos Brasileiros”
POLÍCIA CIVIL DE RORAIMA
INSTITUTO DE CRIMINALÍSTICA
“PERITO CRIMINAL DIMAS ALMEIDA”



Laudo nº 053/2021/SEPAEL/DPI/IC/PC/SESP/RR

Sistema IOS do iPhone, vem impedindo a extração de dados, especificadamente de aplicativos de mensagens, tais como Whatsapp®, Facebook® e outros afins, e assim, dificultando, e até mesmo obstruindo os trabalhos deste Setor. Dramaticamente, o UFED só tem a capacidade de realizar extrações até a versão 6.5 do sistema Andróid, e na lista de aparelhos que o UFED tem capacidade de realizar extrações de dados, não consta qualquer aparelho G5.

Por conta das medidas de segurança citadas, é possível que não sejam extraídos todos os áudios PTT-XXXX (que são àqueles gravados pelo Whatsapp diretamente para outra pessoa) ou os áudios AUD-XXX (que são aqueles que recebemos de alguém, via Whatsapp ou não, e enviamos para uma terceira pessoa, mesmo que sejam do tipo PTT-XXX pois eles se transformarão em AUD-XXX).

Desta forma, adicionalmente, na raiz do anexo eletrônico, está disponibilizada (nos casos possíveis e pertinentes) a extração direta dos arquivos de áudio PTT-XXX, copiados diretamente do dispositivo examinado. Eles ficam separados por dia, e guardados dentro de pastas identificados por uma sequência numérica, na pasta “\\whatsapp\\media\\whatsapp_voice_notes”.

Por todo o exposto retro descrito, este signatário não descarta a possibilidade da presença de outros dados considerados relevantes na memória dos aparelhos, ficando a cargo da Autoridade Requisitante a análise final do conteúdo do equipamento e emissão de juízo de valor sobre o conteúdo coligido. Uma vez verificado o material com interesse probatório que não tenha sido abrangido pela extração do software, encaminhar requisição para extração do conteúdo em específico.

7 DAS RESPOSTAS AOS QUESITOS.

Inicialmente informo que as informações solicitadas foram extraídas pelo UFED, em consonância com o descrito no Item 3 DOS DADOS ENCONTRADOS NO DISPOSITIVO e Item 6 CONSIDERAÇÕES TÉCNICO-PERICIAIS. As respostas aos quesitos contidos na requisição serão embasadas nos dados extraídos pelo programa UFED, ficando a cargo da Autoridade Requisitante a análise do conteúdo do equipamento

O verso deste Laudo segue em branco



GOVERNO DO ESTADO DE RORAIMA
“Amazônia: Patrimônio dos Brasileiros”
POLÍCIA CIVIL DE RORAIMA
INSTITUTO DE CRIMINALÍSTICA
“PERITO CRIMINAL DIMAS ALMEIDA”



Laudo nº 053/2021/SEPAEL/DPI/IC/PC/SESP/RR

e emissão de juízo de valor sobre o material coligido. Uma vez verificado o material com interesse probatório que não tenha sido abrangido pela extração do software, solicitamos encaminhar nova requisição para nova tentativa de extração do conteúdo em específico.

7.1 “Identificação / Descrição dos objetos”;

R.: Ver Item 1 DO MATERIAL RECEBIDO, subitem 1.1 Identificação/descrição.

7.2 “Qual a lista de contatos? (agenda telefônica com descrição dos nomes e telefones)”;

R.: As informações que puderam ser extraídas foram agrupadas e podem ser acessadas através das abas “**Contacts**” do aplicativo UFED, disponibilizado em mídia em anexo, devendo, para tanto, ser executado diretamente pelo Windows Explorer®, conforme o Tutorial disponibilizado na raiz do Anexo Eletrônico.

7.3 “Qual o histórico das ligações recebidas e efetuadas?”;

R.: As informações que puderam ser extraídas foram agrupadas e podem ser acessadas através das abas “**Call Logs**” do aplicativo UFED, disponibilizado em mídia em anexo, devendo, para tanto, ser executado diretamente pelo Windows Explorer®, conforme o Tutorial disponibilizado na raiz do Anexo Eletrônico.

7.4 “Transcrição das mensagens (SMS, MMS)”;

R.: As informações que puderam ser extraídas foram agrupadas e podem ser acessadas através das abas “**SMS Messages**” e “**MMS**” do aplicativo UFED, disponibilizado em mídia em anexo, devendo, para tanto, ser executado diretamente pelo Windows Explorer®, conforme o Tutorial disponibilizado na raiz do Anexo Eletrônico.

7.5 “Qual linha(s) telefônica(s) (número) era(m) utilizado(s) no aparelho e qual a operadora?”;

R.: As informações solicitadas, não estão “visíveis” em todos os Chips, mas quando acessadas pelo programa UFED, estão disponibilizadas através das abas “**Sim Data**” (onde é exibido o número MSISDN do SimCard (número usado pelo aparelho)) ou através da aba “**UserAccount**” (onde é exibido o nome do usuário e o número usado pelo aparelho);



GOVERNO DO ESTADO DE RORAIMA
“Amazônia: Patrimônio dos Brasileiros”
POLÍCIA CIVIL DE RORAIMA
INSTITUTO DE CRIMINALÍSTICA
“PERITO CRIMINAL DIMAS ALMEIDA”



Laudo nº 053/2021/SEPAEL/DPI/IC/PC/SESP/RR

7.6 “Outros dados que julgar úteis”.

R.: Todos os dados que puderam ser extraídos podem ser acessados através “LaudoEletrônico”, disponibilizado na mídia eletrônica em anexo, contendo diversas informações e detalhes sobre cada arquivo capturado, devendo, para tanto, ser executado conforme o Tutorial disponibilizado na raiz do Anexo Eletrônico, bem como através de acesso direto pelo Windows Explorer®.

Adicionalmente, considerando a ausência de extração de dados, descrita no Item 3 DOS DADOS ENCONTRADOS NO DISPOSITIVO e Item 6 CONSIDERAÇÕES TÉCNICO-PERICIAIS, este signatário não descarta a possibilidade da presença de dados considerados relevantes na memória do aparelho examinado, ficando a cargo da Autoridade Requisitante a análise do conteúdo e emissão de juízo de valor sobre o conteúdo coligido. Uma vez verificado o material com interesse probatório que não tenha sido abrangido pela extração do software, encaminhar nova requisição para extração do conteúdo em específico.

É de bom alvitre orientar que o material ora encaminhado, principalmente àqueles que não puderam ter seu conteúdo completamente extraído, seja mantido sob custódia e devidamente lacrado até o deslinde do feito, preservando a integridade dos dados que não puderam ser extraídos e preservados, haja vista a possibilidade de nova extração ou solicitação de uma contraprova conforme determina a legislação em vigência.

Fica a cargo da autoridade requisitante a pronta devolução do material examinado.

8 CONCLUSÕES.

O Perito recebeu no Instituto de Criminalística, o material descrito no item “1 DO MATERIAL RECEBIDO”, sobre o qual foram realizados os Exames Periciais solicitados, em consonância com a **Requisição de Exame Pericial 134/2021-DRE**, datada de 23/07/2021, referente ao **APF nº 1587/2021-DRE**.

9 CONSIDERAÇÕES FINAIS.

Tendo por bem esclarecido o assunto e nada mais havendo a relatar, encerro o presente laudo confeccionado em dez (10) páginas numeradas, devidamente assinadas pelo

O verso deste Laudo segue em branco



GOVERNO DO ESTADO DE RORAIMA
"Amazônia: Patrimônio dos Brasileiros"
POLÍCIA CIVIL DE RORAIMA
INSTITUTO DE CRIMINALÍSTICA
"PERITO CRIMINAL DIMAS ALMEIDA"



Laudo nº 053/2021/SEPAEL/DPI/IC/PC/SESP/RR

Perito que procedeu aos exames, acompanhado de **dois (02) anexos eletrônicos que são parte integrante da presente peça pericial.**

Em tempo, esclarece-se, por oportuno, que esse SEPAEL ainda não tem a capacidade operacional de armazenar grandes quantidades de dados eletrônicos, tais quais estes do material descrito no Item **1 DO MATERIAL RECEBIDO**, em função da ausência de *storage* destinado a guarda de *backups*.

Desta forma, considerando que o material encaminhado em Mídia Eletrônica que ora segue encaminhado anexo a este Laudo (Extrações de conteúdo Multimídia), é único e sujeito à danos e intempéries, **é altamente recomendável que se proceda uma cópia de segurança das MÍDIAS DIGITAIS encaminhadas**, uma vez que esta recepciona os dados levantados e os respectivos Laudos eletrônicos.

Com o laudo segue todo o material descrito no Item **1 DO MATERIAL RECEBIDO**, que estão passivos de pronta restituição, à cargo da autoridade requisitante.

Anaximandro Soares Coimbra

Perito Criminal de Polícia Civil - SEPAEL/DPI/IC/PC/SESP/RR
Matrícula 042000428

Veritas, Scientia et Justitia

O verso deste Laudo segue em branco