REALIZANDO EXTRAÇÃO DE DADOS EM APARELHOS ANDROID UTILIZANDO O SOFTWARE FORENSE - AVILLA FORENSICS

O *software* utilizado na extração de dados nesse tutorial é desenvolvido pelo Agente de Polícia do Estado de São Paulo, Daniel Avilla.

AVILLA FORENSICS é um *software* forense utilizado para realizar extrações de dados dos aparelhos móveis.

Emerson Borges Machado
emerson.borges@policiacivil.mg.gov.br

REQUISITOS MÍNIMOS:

Dispositivo: Ativado a Depuração USB.
Sistema Operacional: Windows 10 atualizado.
Para Extração: Sistemas 32 ou 64 Bits.
Conversão Backup .AB para .TAR: Sistemas 32 ou 64 Bits e o JAVA instalado.
Relatório IPED PF: Sistema 64 Bits e JAVA 64 Bits instalado.

PROGRAMAS NECESSÁRIOS:

DOWNLOAD AVILLA FORENSICS: DOWNLOAD AQUI

DOWNLOAD JAVA: DOWNLOAD AQUI

DOWNLOAD WINRAR: DOWNLOAD AQUI

VÍDEO TUTORIAL:

https://youtu.be/KuSmct1Qa30

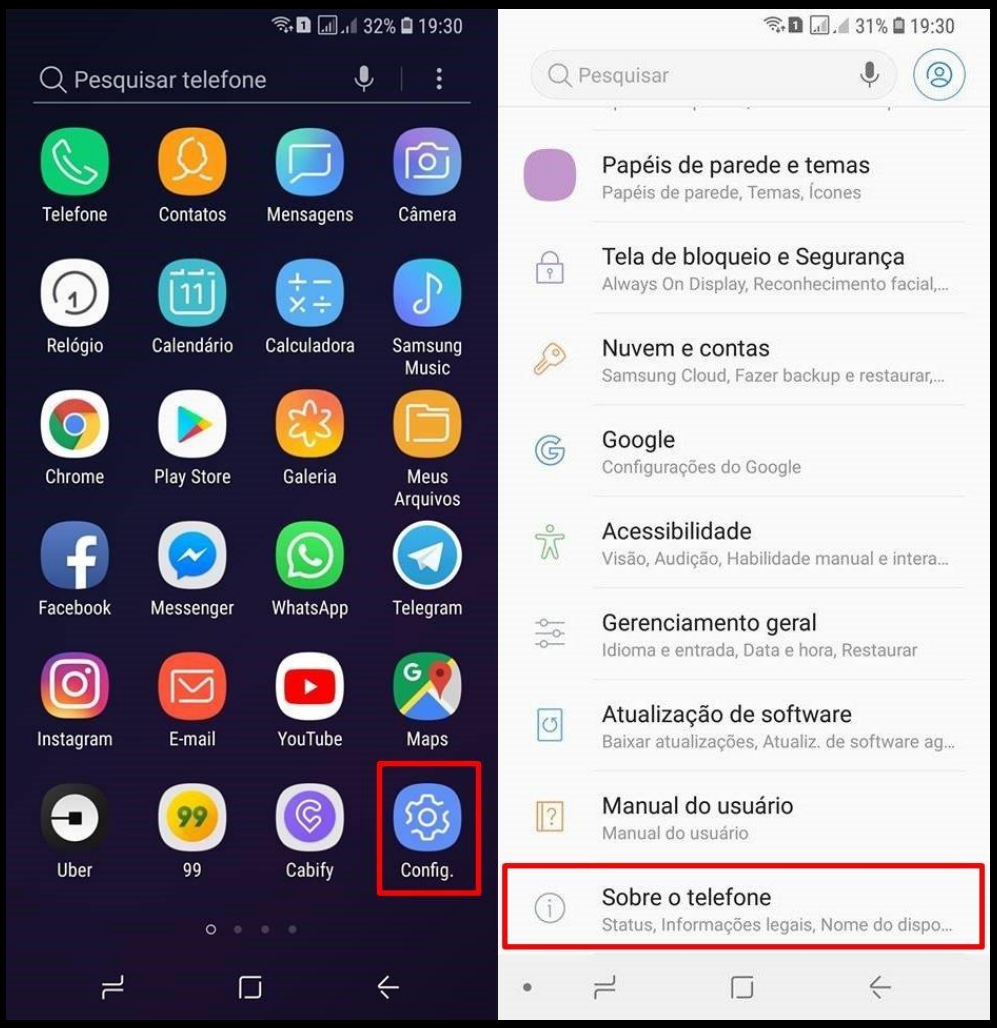
Emerson Borges Machado
emerson.borges@policiacivil.mg.gov.br

PREPARANDO O APARELHO CELULAR

Para iniciarmos devemos preparar o aparelho celular para que seja feita a comunicação com o *ADB - Android Debug Bridge*, para isso iremos ativar o **MODO DEPURAÇÃO USB** do aparelho celular, princípio básico utilizado nas extrações forense em dispositivos móveis (android).

SIGA FIELMENTE AS ETAPAS:

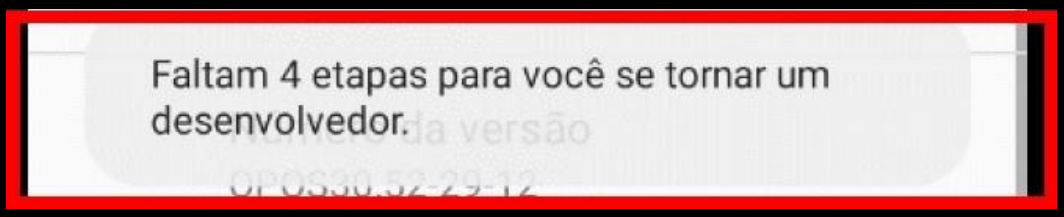
Acesse as **configurações do aparelho celular** e desce até a opção **Sobre o telefone**.



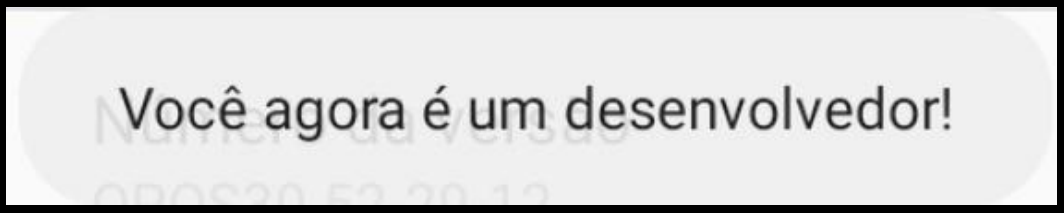
Entre na opção **Informações do software**, e vá até a opção **Número de compilação** e clique 7 (sete) VEZES.

Emerson Borges Machado
emerson.borges@policiacivil.mg.gov.br

Durante esse processo o aparelho irá exibir um alerta informando quantas etapas faltam para liberar o **MODO DESENVOLVEDOR**.

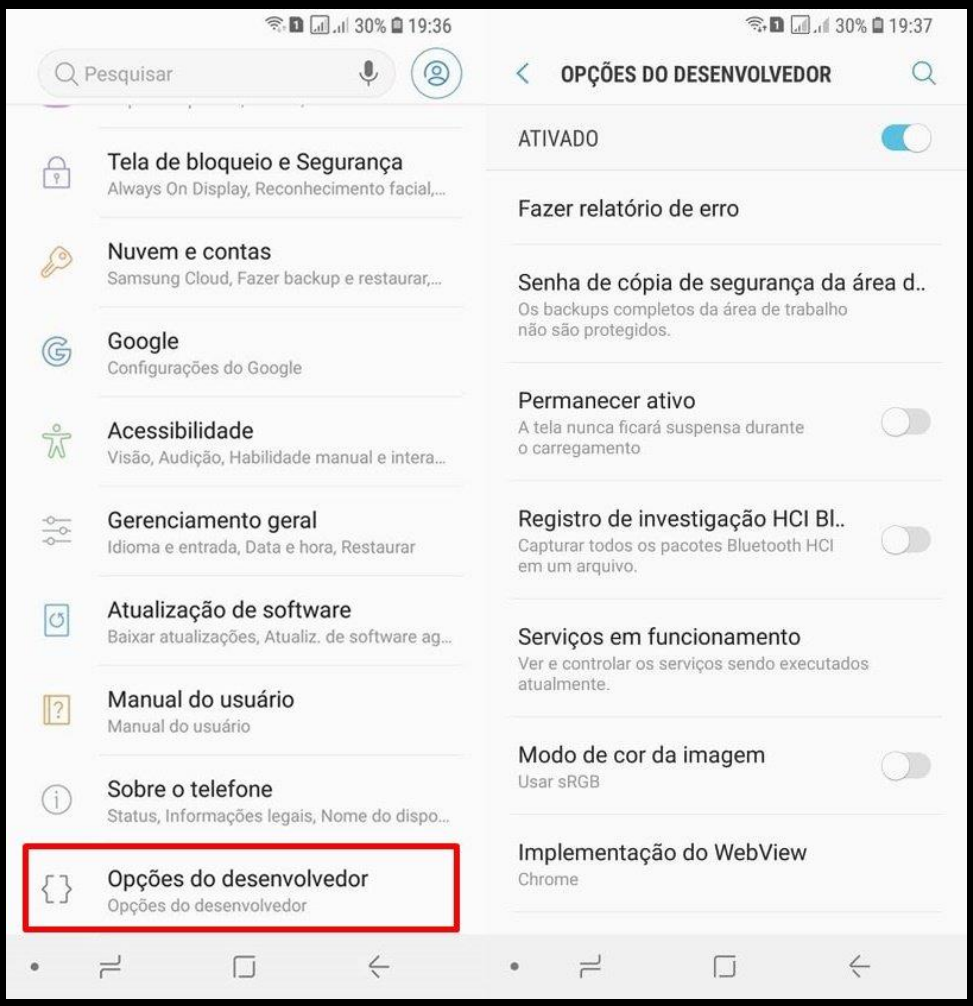


Quando liberado o sistema irá exibir o seguinte alerta:



Emerson Borges Machado
emerson.borges@policiacivil.mg.gov.br

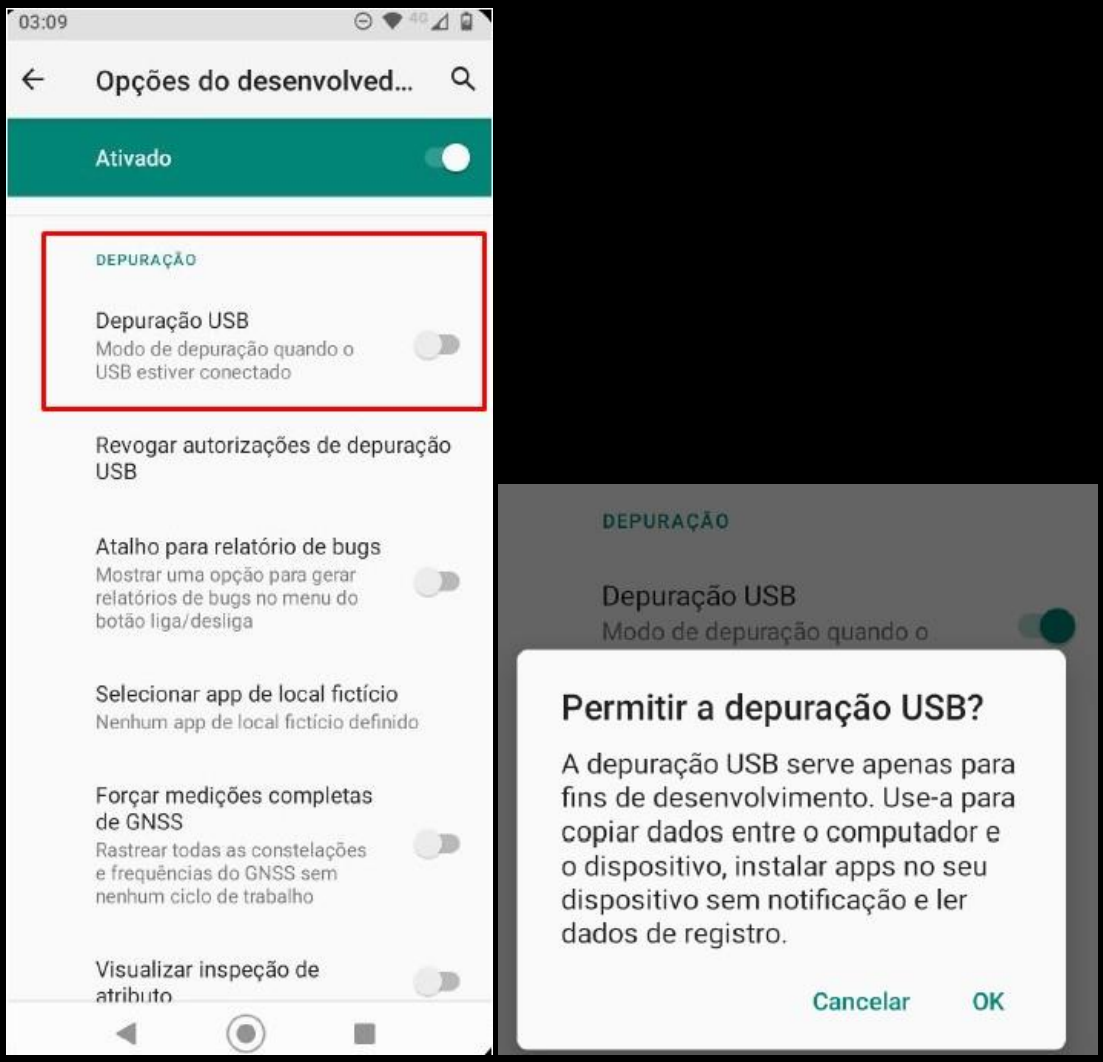
Após liberado o **MODO DESENVOLVEDOR**, volte em "**Configurações**" e role a barra lateral até o final. Você vai perceber que o "**Modo Desenvolvedor**" foi ativado e já aparece nas opções.



Emerson Borges Machado
emerson.borges@policiacivil.mg.gov.br

ATENÇÃO NESSA ETAPA!

Dentro das **OPÇÕES DO DESENVOLVEDOR**, iremos ativar o modo **DEPURAÇÃO USB**.

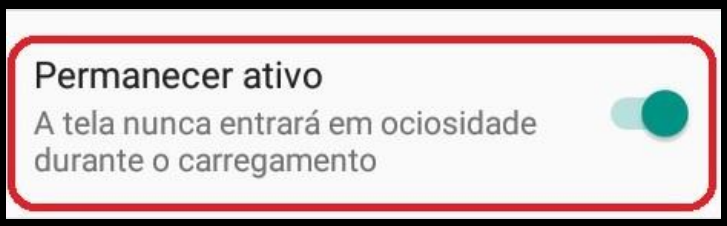


PERMITIR A DEPURAÇÃO USB?

Clique em **OK**.

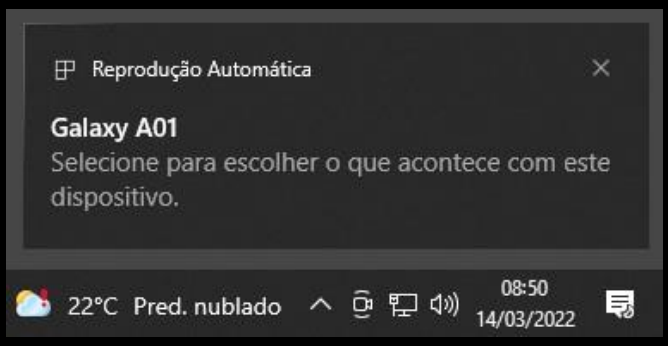
Ainda dentro das Opções do Desenvolvedor **ATIVE** também a opção **PERMANECER ATIVO**.

Emerson Borges Machado
emerson.borges@policiacivil.mg.gov.br



Feito esses passos **conecte o aparelho celular na porta USB do computador** e **permita o acesso ao telefone** assim que for solicitado.

*** Quando o aparelho celular é conectado na porta USB do computador a seguinte caixa de alerta é informada pelo Windows. Esse alerta informa que o aparelho celular está em comunicação com o sistema operacional.



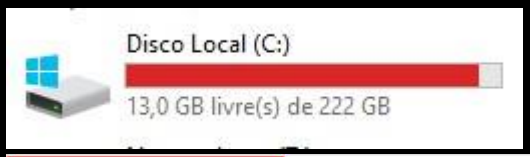
Esses são os passos necessários para deixar o aparelho celular preparado para ser utilizado no **Avilla Forensics**.

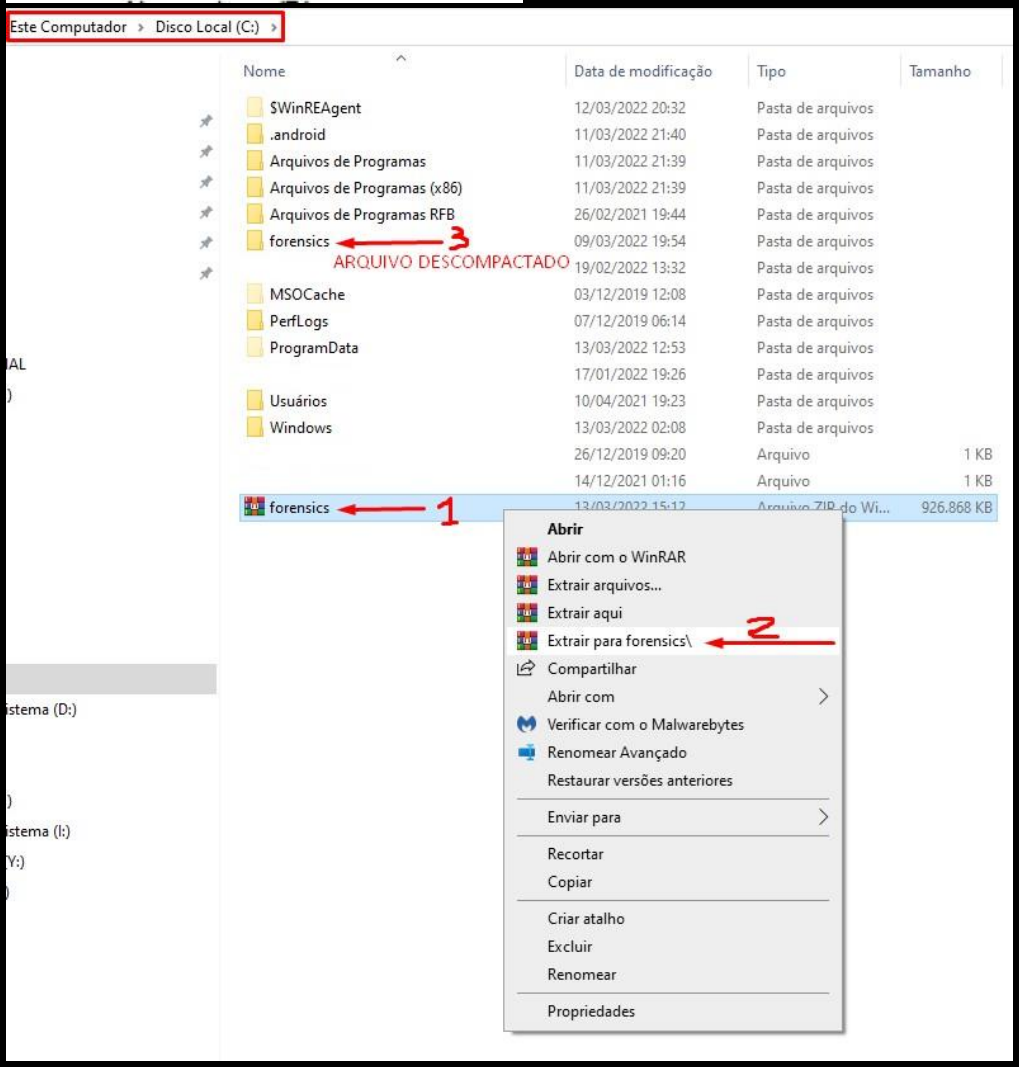
Emerson Borges Machado
emerson.borges@policiacivil.mg.gov.br

*** As opções **Sobre o telefone**, **Informações do software** e **Número de compilação**, podem variar o local de onde são encontradas, dependendo do fabricante do aparelho, modelo e versão do android. Basta uma busca no Google “como liberar o modo desenvolvedor do aparelho XYZ”, para encontrar informações precisas de um determinado modelo/fabricante.

INFORMAÇÃO IMPORTANTE!

Após realizar o download do **AVILLA FORENSICS** (download aqui), o software vem zipado (.zip), use o WINRAR (download aqui), e descompacta o arquivo dentro do **MEU COMPUTADOR => DISCO LOCAL (C:)**

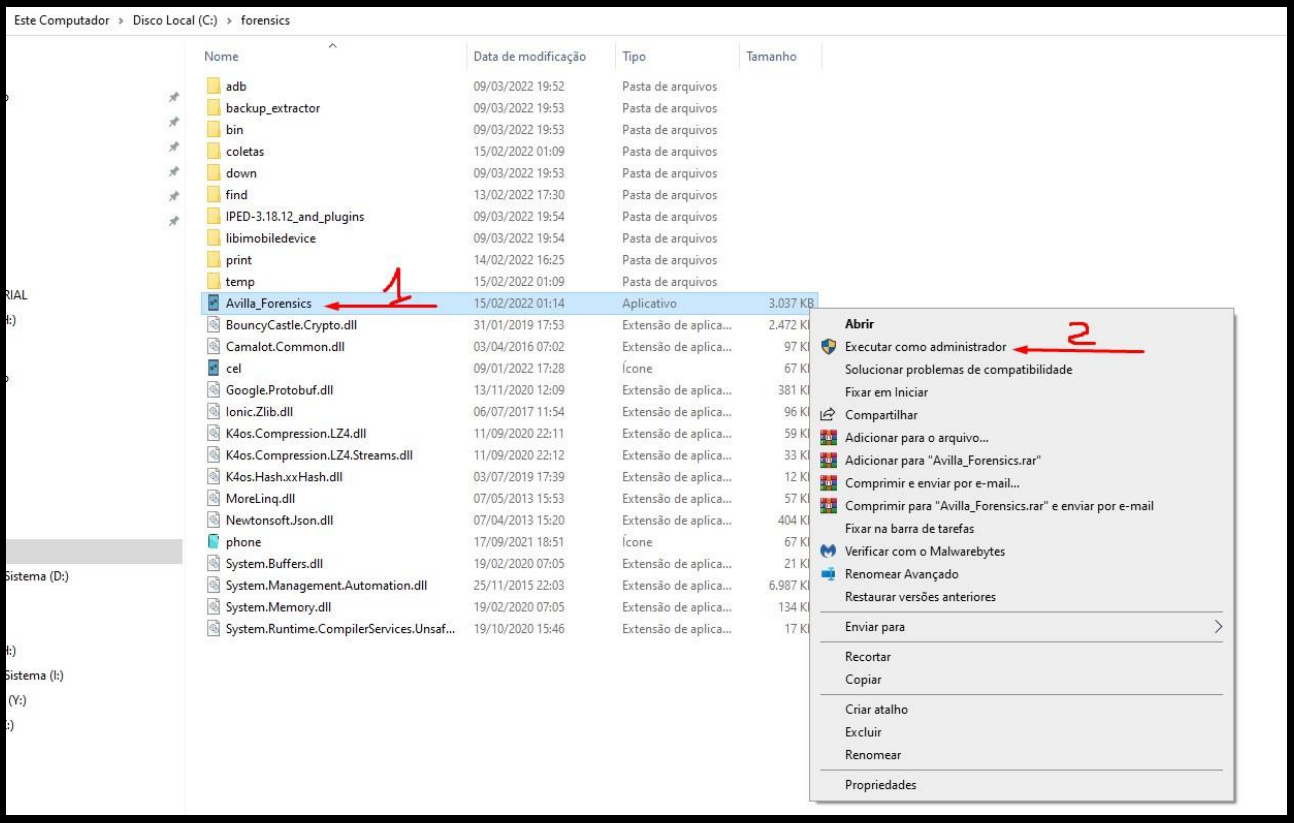




Emerson Borges Machado
emerson.borges@policiacivil.mg.gov.br

REALIZANDO EXTRAÇÃO LÓGICA – BACKUP ADB - ANDROID

Dentro da pasta **forensics**, clique com o **botão direito** em cima do arquivo **Avilla_Forensics** e clique para executá-lo como administrador.



Com o **Avilla Forensics** aberto iremos começar a realizar a extração **LÓGICA** do aparelho celular. O primeiro passo é realizar o teste de conexão entre o celular e o software.

1) Entre na opção **BACKUP ADB.**
2) Clique em **TESTAR CONEXÃO**.

Emerson Borges Machado
emerson.borges@policiacivil.mg.gov.br

Se estiver ocorrendo comunicação entre o aparelho celular e o software, irá aparecer na "**List of devices attached**", o modelo do aparelho celular.

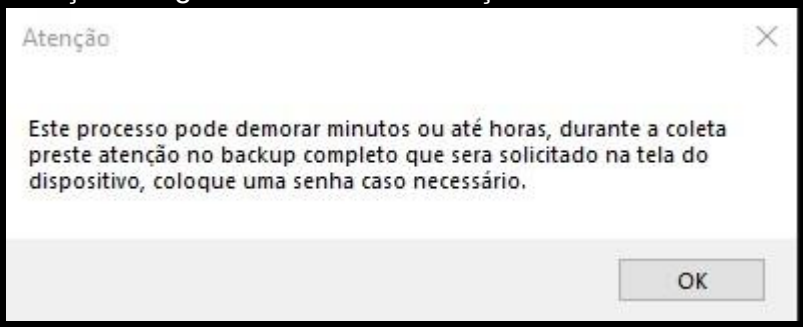
```
List of devices attached
R9XN402XLJB          device product:a01qub model:SM_A015M device:a01q transport_id:1
```

O próximo passo é escolher a pasta onde será salvo a extração, basta clicar em "**SALVAR EM:**" e selecionar a pasta.

```
>> Destino:  C:\Users\PCMG-AIP\Desktop\TUTORIAL\EXTRACAO\backup-2022-03-14-09-22-33.ab
```

Feito isso clica em "**EXTRAIR**".

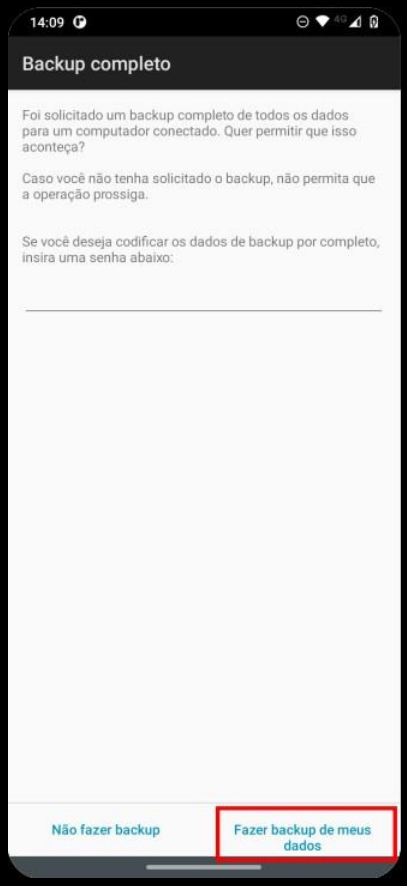
Quando iniciar o processo de extração irá aparecer caixas de alertas, leia com atenção e siga fielmente as instruções.



Nesse momento no aparelho celular irá aparecer a tela de **BACKUP**, se estiver habilitada a opção **FAZER BACKUP DE MEUS DADOS** basta clicar nela, se

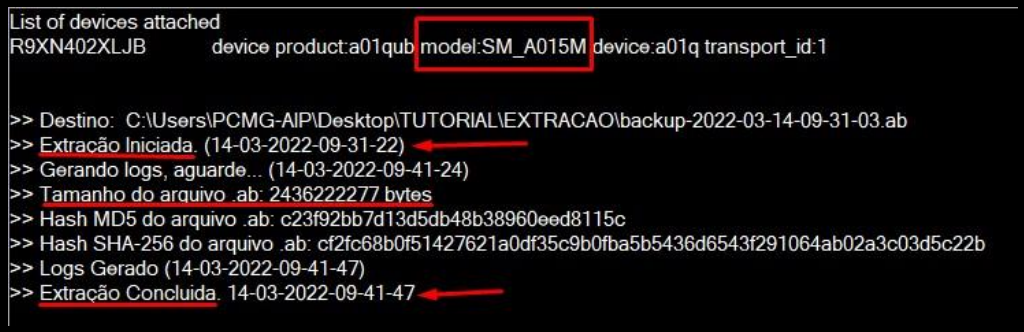
Emerson Borges Machado
emerson.borges@policiacivil.mg.gov.br

não, informe uma senha de sua escolha para que a opção fique habilitada. Pode utilizar uma senha básica padrão, como exemplo 12345.



O software começará a fazer o backup dos dados do aparelho celular, basta aguardar a conclusão do processo.

Quando a extração for concluída será informado na tela de informações do software, conforme imagem a seguir:



A extração no formato **.AB** estará na pasta que foi selecionada no início do processo, que no caso do tutorial é **DESKTOP\TUTORIAL\EXTRACAO.**

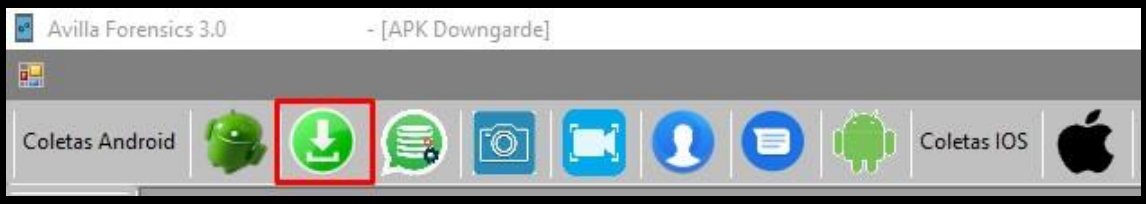
Emerson Borges Machado
emerson.borges@policiacivil.mg.gov.br

Assim fica concluído o módulo de extração lógica **BACKUP ADB** do **Avilla Forensics**.

Mais adiante iremos fazer a conversão do arquivo **.AB** para **.TAR**, extensão de arquivo que é aceito pelo software **IPED** da **Polícia Federal**.

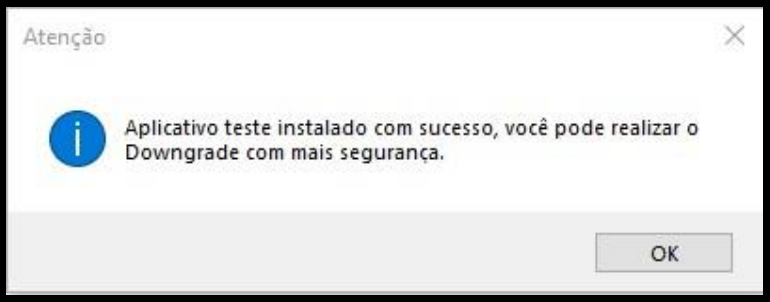
APK DOWNGRADE - EXTRAÇÃO DE DADOS WHATSAPP – ANDROID

Agora que você já esta mais familiarizado com o **Avilla Forensics**, acesse a opção **APK DOWNGRADE**.



Clique em **TESTAR CONEXÃO**, e se a comunicação estiver OK, irá apresentar a "**List of devices attached**" o **modelo do aparelho celular**, da mesma forma que realizamos no passo anterior do tutorial.

O próximo passo é clicar em **APLICAÇÃO TESTE**, nesse momento será instalado no aparelho celular o aplicativo "**Aplicacao Teste**".



Perceba-se que o aplicativo teste vai estar aberto na tela do aparelho celular.

Realizado essas etapas o próximo passo é escolher qual aplicativo iremos realizar o downgrade, que no nosso caso do tutorial será o **Whatsapp**. Para isso clique em **DETECTAR**.

Emerson Borges Machado
emerson.borges@policiacivil.mg.gov.br

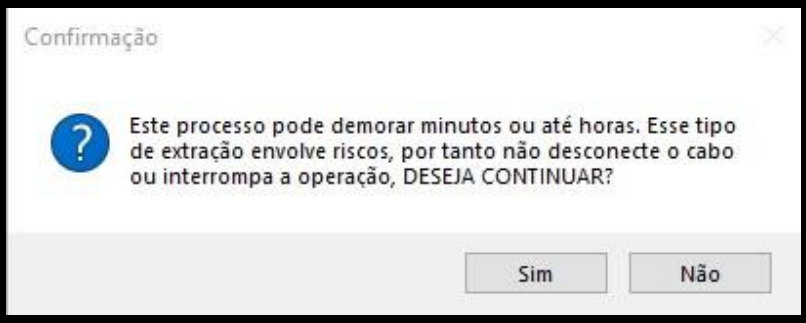
Selecione o **com.whatsapp**.

Agora basta clicar em **SALVAR EM:** e selecionar a pasta que a extração será salva.

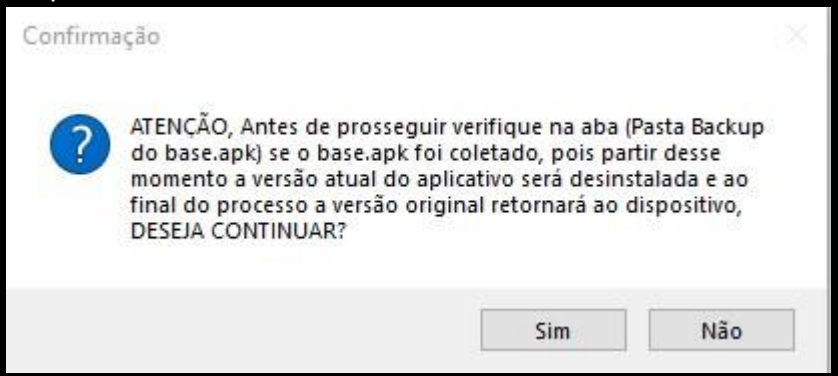
ATENÇÃO!

Nas próximas etapas, siga fielmente as instruções que serão apresentadas nos alertas do **Avilla Forensics** e também na **tela do aparelho celular**.

Clique em **EXTRAIR**.

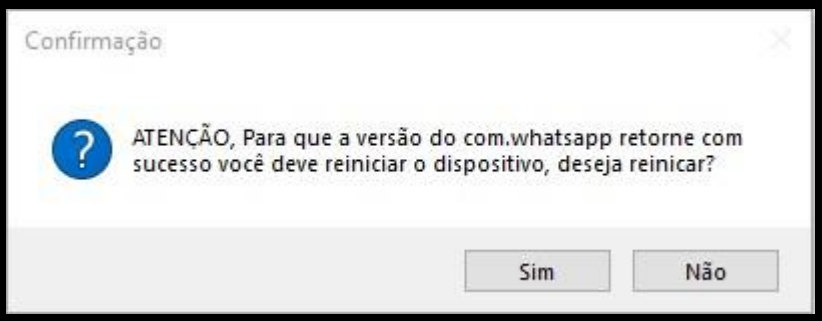


Clique em Sim.

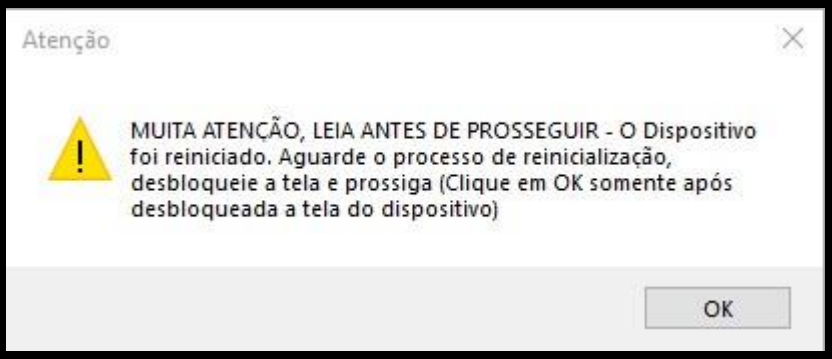


Emerson Borges Machado
emerson.borges@policiacivil.mg.gov.br

PASTA BACKUP localizado no canto inferior direito do **Avilla Forensics**.

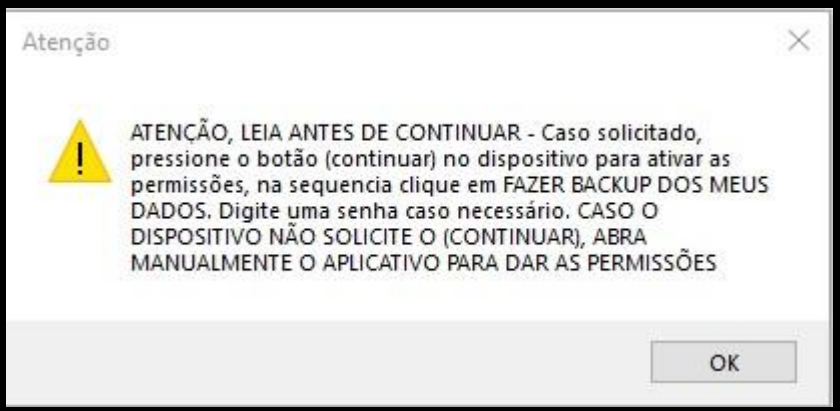


O alerta informa que será necessário reiniciar o aparelho celular, clique em sim.



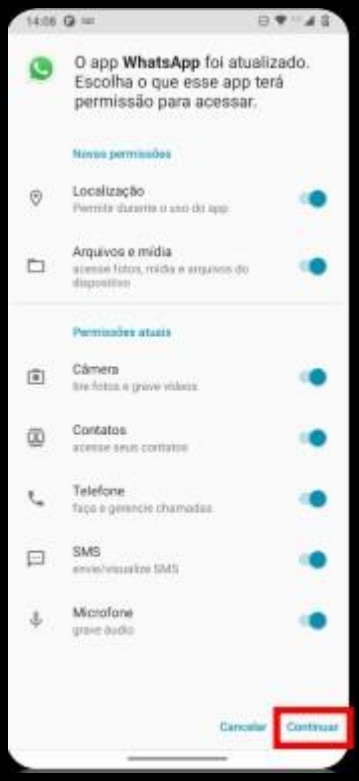
Clique em OK somente após o aparelho celular ter reiniciado por completo e caso tenha senha e/ou bloqueio de tela, certifique-se que tenha feito o desbloqueio do mesmo.

ATENÇÃO NESSA ETAPA!



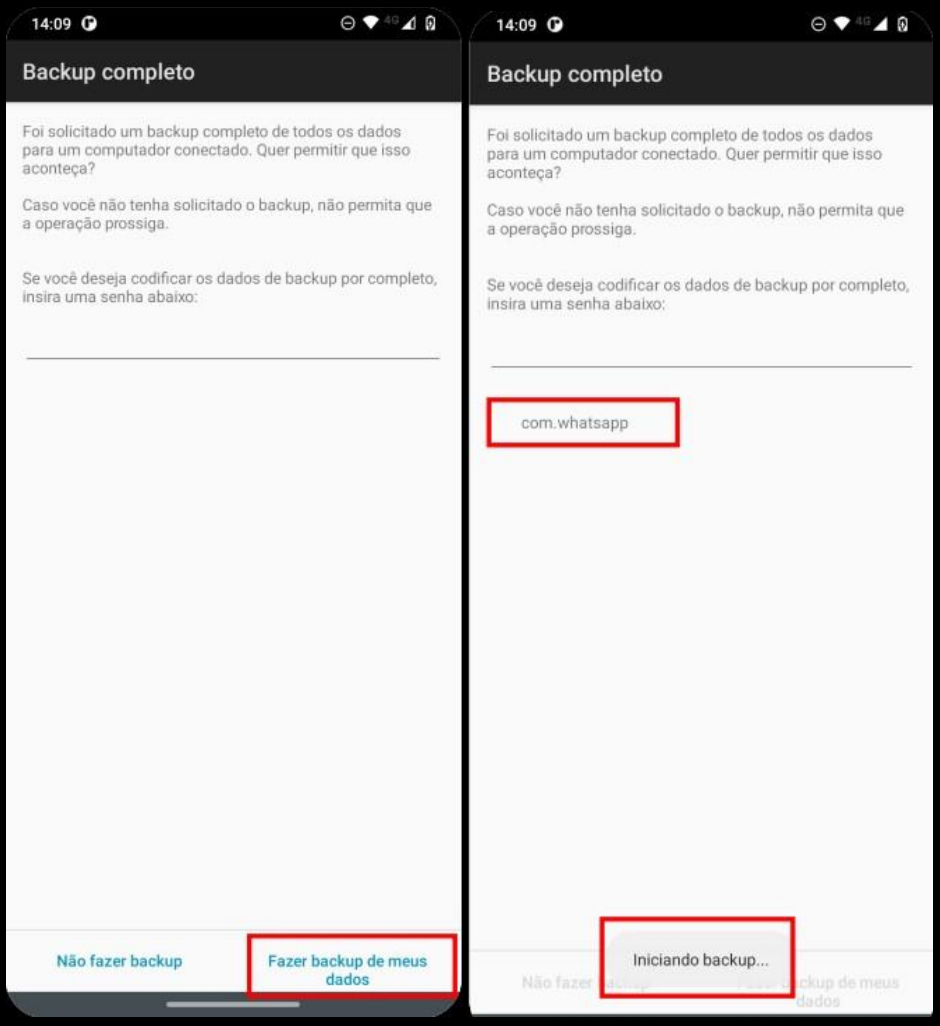
Emerson Borges Machado
emerson.borges@policiacivil.mg.gov.br

Nesse momento foi desinstalado a versão atual do **Whatsapp** e instalado uma versão exploit do aplicativo (**com.whatsapp**), para dar as permissões necessárias, abre o aplicativo no aparelho celular e clique em **CONTINUAR**.

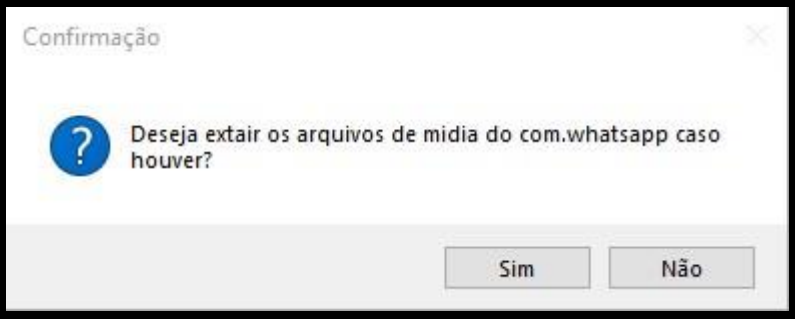


Após clicar em **CONTINUAR**, volte para o **Avilla Forensics** e clique em OK.

Emerson Borges Machado
emerson.borges@policiacivil.mg.gov.br



Nesse momento no aparelho celular irá aparecer a tela de **BACKUP**, se estiver habilitada a opção **FAZER BACKUP DE MEUS DADOS** basta clicar nela, se não, informe uma senha de sua escolha para que a opção fique habilitada. Pode utilizar uma senha básica padrão, como exemplo 12345.



Clique em **Sim**.

Emerson Borges Machado
emerson.borges@policiacivil.mg.gov.br

```
>> Tamanho do arquivo .ab: 40201221 bytes
>> Hash MD5 do arquivo .ab: 204aa7a841541b69434c4eaa8f4a6526
>> Hash SHA-256 do arquivo .ab: 3cb996f3d4207ee8c4d688368167021ed208f9f520b14016c0d0770b6e67a23e
>> Logs Gerado (14-03-2022-11-27-22)
>> Extração do com.whatsapp concluída (14-03-2022-11-27-22)
```

Extração concluída.

CONVERTER .AB PARA .TAR E UTILIZAR O SOFTWARE IPED DA POLÍCIA FEDERAL PARA INDEXAR OS ARQUIVOS EXTRAÍDOS

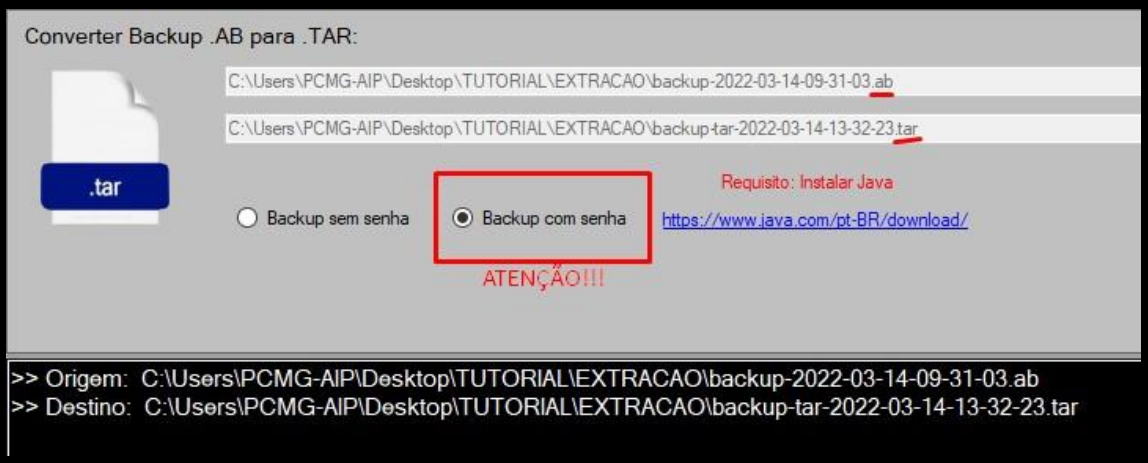
Realizada as extrações **BACKUP ADB** e **APK DOWNGRADE,** agora iremos fazer a conversão dos arquivos .**AB** para **.TAR** para que seja possível realizar a analise do conteúdo que foi extraído do aparelho celular.

Entre na opção destacada para realizar a conversão.

Em **SELECIONAR**, escolha o arquivo **.AB** que foi realizado na extração **BACKUP ADB**, em seguida escolha o local onde será salvo o arquivo na extensão **.TAR**.

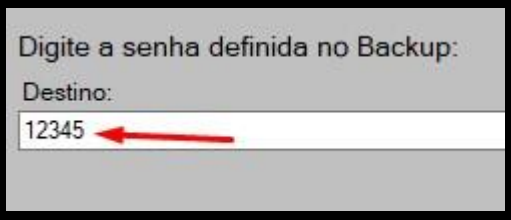
******* Eu salvo dentro da mesma pasta que foi criada quando foi realizada a extração, para que fique juntos tanto o arquivo **.AB** quanto o **.TAR**.

Emerson Borges Machado
emerson.borges@policiacivil.mg.gov.br

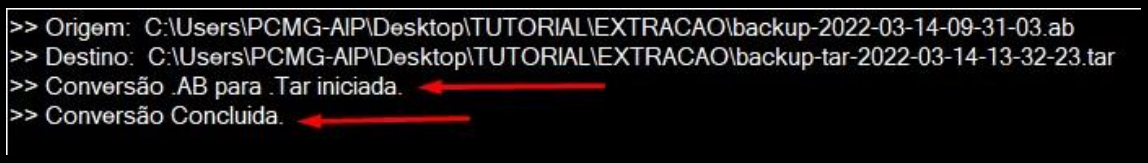


Repare que o destino da pasta no **.TAR** é o mesmo do **.AB**.

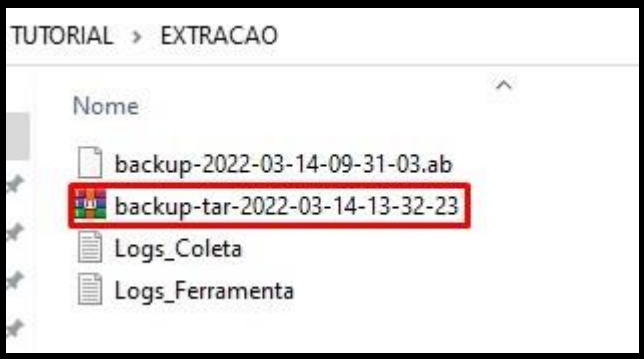
Se no momento de realizar a extração você informou uma senha para ativar a opção **FAZER BACKUP DE MEUS DADOS**, nesse momento você deve marcar **BACKUP COM SENHA** e quando clicar em **CONVERTER**, será solicitado a senha e você deve digitá-la no campo informado.



Agora aperte OK e a conversão irá se iniciar.

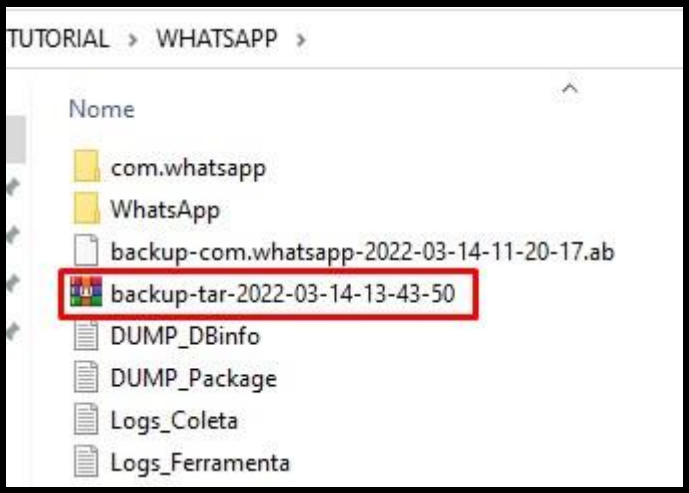


Conversão concluída. Agora o arquivo no formato **.TAR** estará dentro da pasta selecionada.

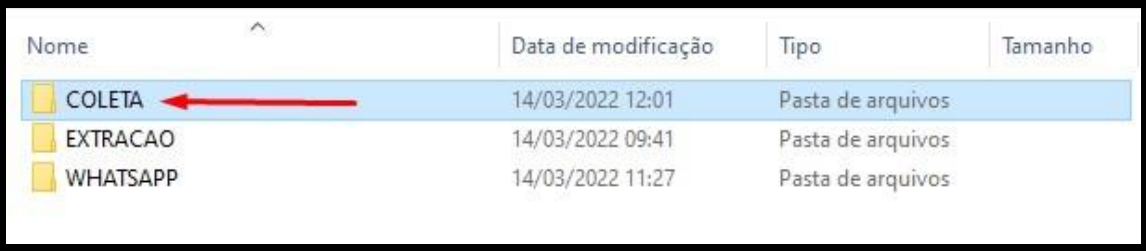


Emerson Borges Machado
emerson.borges@policiacivil.mg.gov.br

Faça o mesmo processo para a extração **APK DOWNGRADE** (**whatsapp**).



*** Como realizamos dois tipos de extração o **BACKUP ADB** e **APK DOWNGRADE**, vamos criar uma nova pasta e incluir todos os arquivos necessários para realizarmos a indexação do **IPED**.



Criei uma nova pasta com o nome **COLETA**.

Repare na imagem que possuí três pastas, sendo elas:

EXTRACAO: pasta contendo a extração BACKUP ADB.
WHATSAPP: pasta contendo a extração APK DOWNGRADE (Whatsapp).
COLETA: pasta que iremos juntar os arquivos convertidos em **.TAR** das extrações **BACKUP ADB** e **APK DOWNGRADE** juntamente com a pasta **com.whatsapp** ou **Whatsapp**.

*** Quando a biometria do aparelho celular estiver desativada, por padrão os arquivos de mídias são salvos no seguinte caminho:

/sdcard/WhatsApp

Emerson Borges Machado
emerson.borges@policiacivil.mg.gov.br

Agora quando o usuário ativa a biometria as mídias passam a serem salvas no caminho abaixo:

/sdcard/Android/media/com.whatsapp/

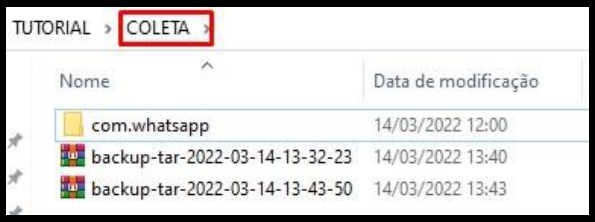
Por isso é preciso ficar atento a esse detalhe para saber qual a pasta deve ser selecionada no momento que for fazer a indexação.

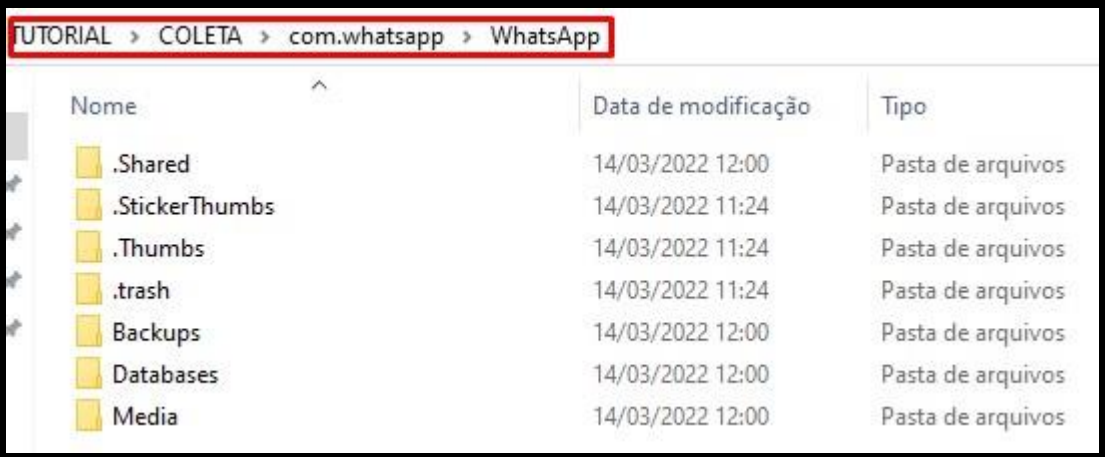
No aparelho celular utilizado na produção desse tutorial, a biometria estava ativada.

Então, dentro da pasta **COLETA** incluímos os arquivos de extração:

1) **backup-tar-2022-03-14-13-32-23** (BACKUP ADB);
2) **backup-tar-2022-03-14-13-43-50** (APK DOWNGRADE);
3) e a pasta **com.whatsapp** (pasta que contém os arquivos de mídia).

Ficando da seguinte forma:





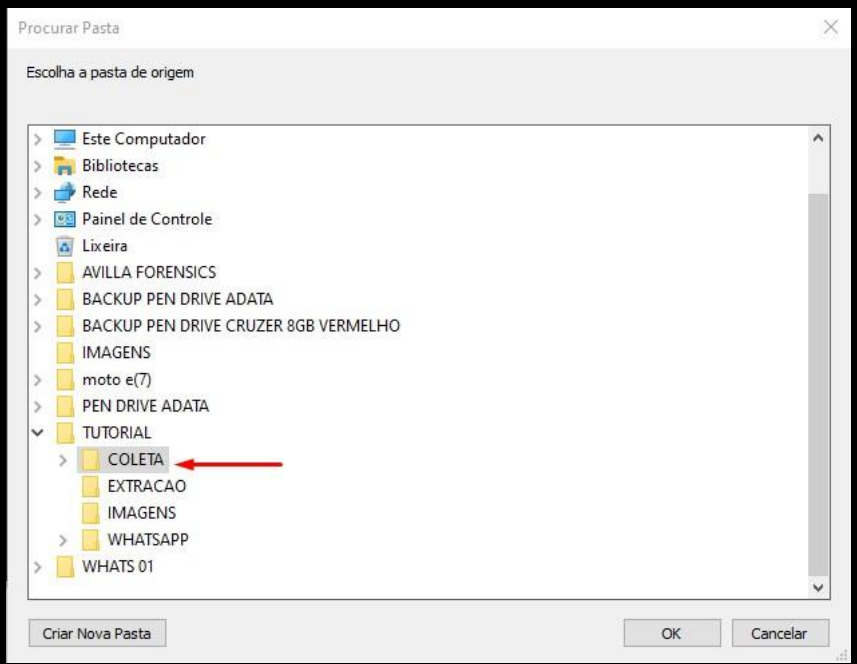
Organizado a nossa estrutura de pasta, agora iremos realizar a indexação da pasta para que seja possível realizar a analise do conteúdo através do **IPED**.

Emerson Borges Machado
emerson.borges@policiacivil.mg.gov.br

Acesse a opção do **IPED**.

Marque a opção **INDEXAR PASTA**.

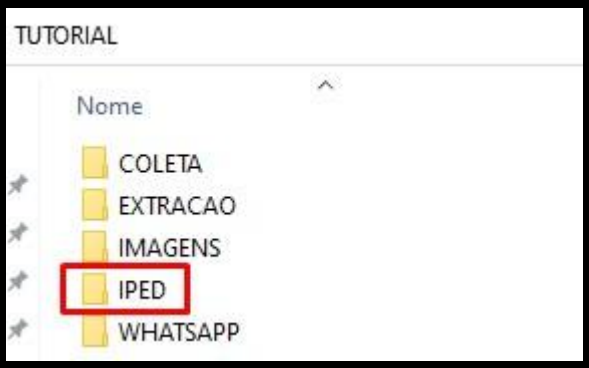
Em **SELECIONAR** informe o caminho da pasta que criamos no caso do tutorial a pasta **COLETA.**

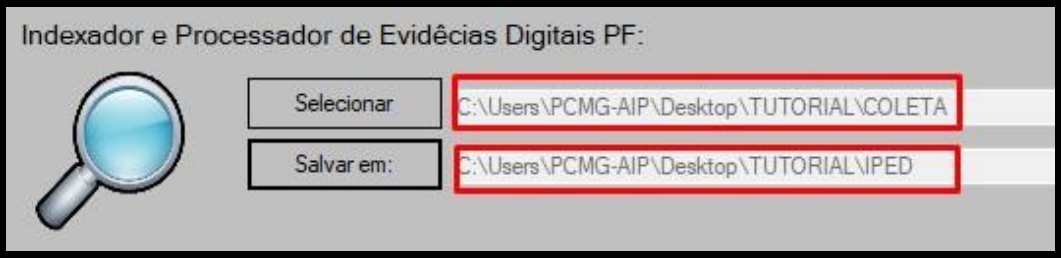


Emerson Borges Machado
emerson.borges@policiacivil.mg.gov.br

Em **SALVAR EM:** seleciona a pasta que ficará salva a indexação do **IPED**.

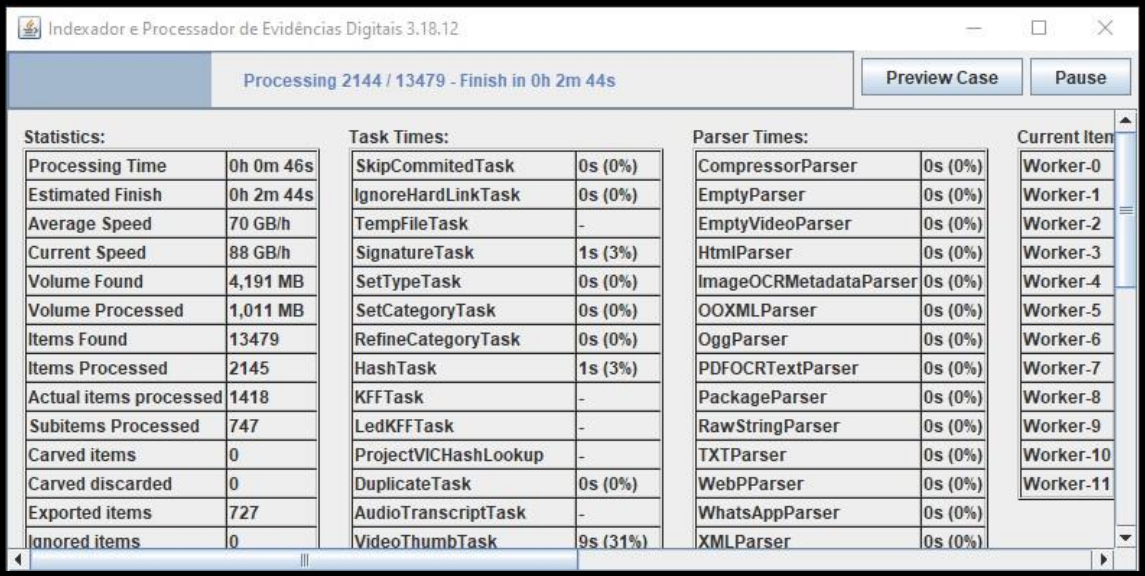
Para ficar organizado, cria uma nova pasta e nomeia-a por **IPED**.





Assim ficou a estrutura do processo.

Agora clique em **GERAR**.



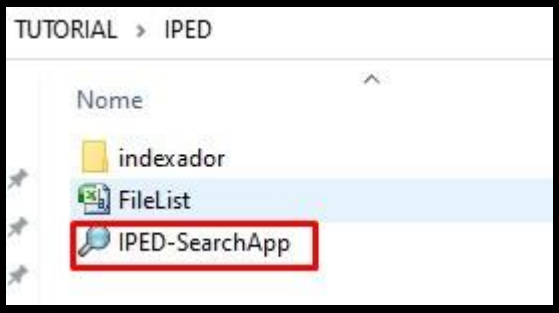
O indexador **IPED** irá começar a carregar as informações.

Emerson Borges Machado
emerson.borges@policiacivil.mg.gov.br

```
>> Origem: C:\Users\PCMG-AIP\Desktop\TUTORIAL\COLETA
>> Destino: C:\Users\PCMG-AIP\Desktop\TUTORIAL\IPED
>> Indexação IPED iniciada.
>> Indexador Gerado.
```

Indexador gerado.

Agora dentro da pasta **IPED** terá o arquivo do indexador **IPED-SearchAPP**, basta dar dois cliques e o mesmo irá abrir com o resultado da extração.



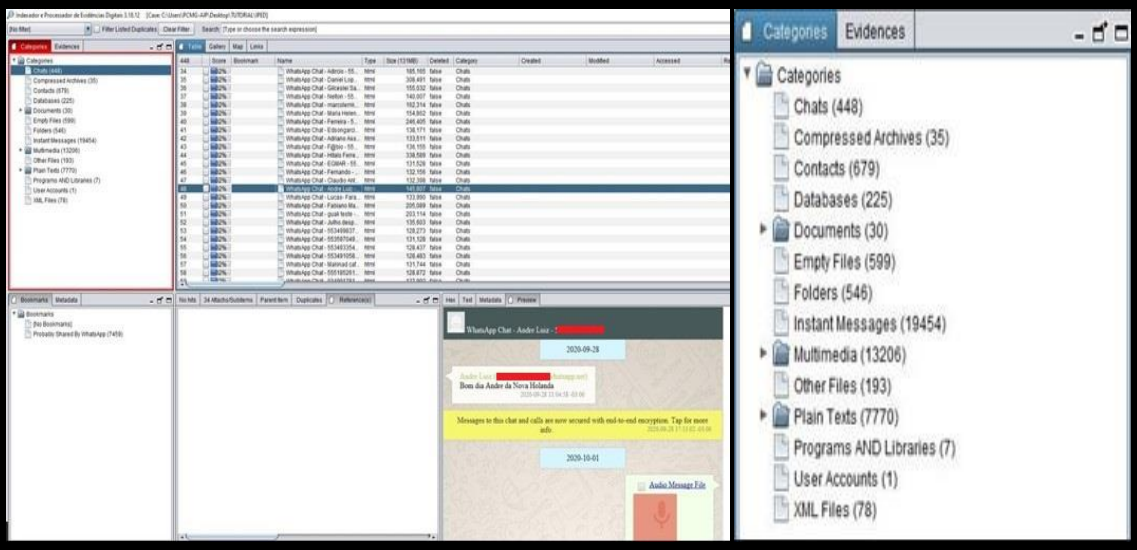
O IPED é um poderoso software desenvolvido por Peritos Criminais da Polícia Federal capaz de lidar com alto processamento de dados, vale destacar que tal ferramenta foi amplamente utilizada na operação Lava Jato.

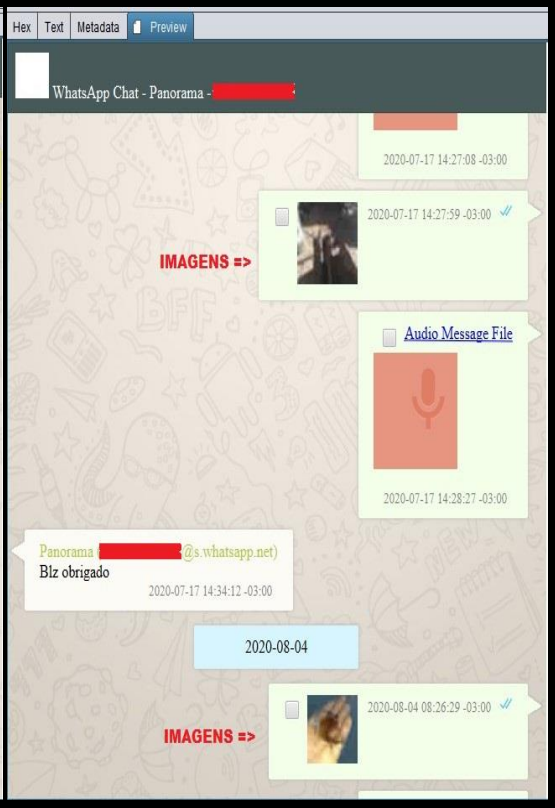
https://servicos.dpf.gov.br/ferramentas/IPED/

https://github.com/sepinf-inc/IPED

Emerson Borges Machado
emerson.borges@policiacivil.mg.gov.br

TELAS DO IPED





Emerson Borges Machado
emerson.borges@policiacivil.mg.gov.br