

## Manual para utilização do Script para UFED para carga de extração de mensagens do WhatsApp por e-mail


GNU GENERAL PUBLIC LICENSE - Copyright: 2018 Alberto Magno <alberto.magno@gmail.com>

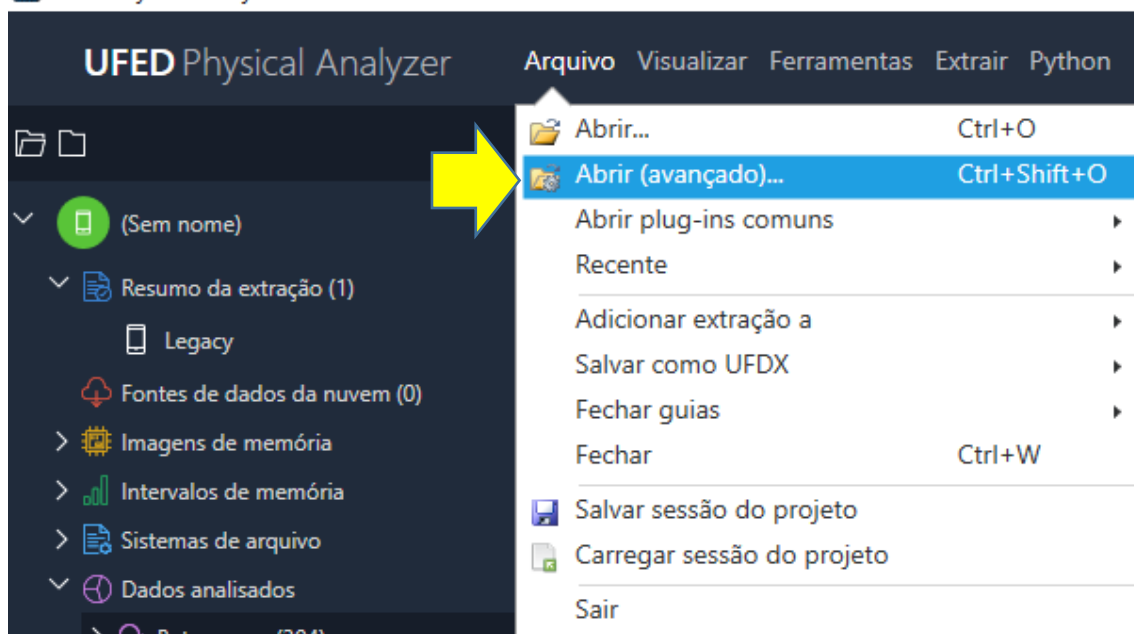
Esse script Python executa a carga de dados extraídos indiretamente por exportação de conversas do aplicativo WhatsApp na estrutura da ferramenta Cellebrite UFED Physical Analyser, incluindo a ligação de eventuais mensagens com seus respectivos anexos.

Foi presumido o formato de datação das mensagens no padrão dd/MM/yyyy, HH24:mm, mas o script está apto a ser adaptado para trabalhar com outros formatos a partir de um pequeno ajuste no código. Também presume-se que o processo de exportação ofereça o arquivo `contacts.txt` com a lista de contatos do aplicativo. Caso não exista esse arquivo no diretório destino da exportação, executar o script denominado `spi_ufed_whatsapp_email.py` como alternativa.

Os passos para uso do script são os seguintes:

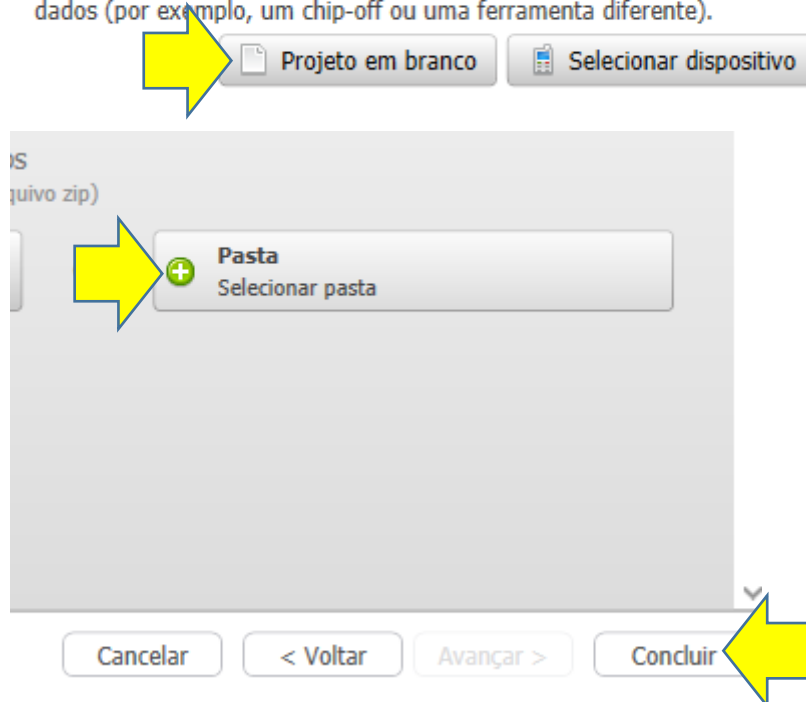
- 1- Verificar a existência ou instalar de programa para e-mail ou simulação de e-mail no dispositivo Android alvo.
- 2- Fazer cópia por exportação para e-mail de todas conversas de interesse do WhatsApp para um mesmo diretório denominado "EmailWhatsApp".
- 3- Copiar o diretório "EmailWhatsApp" da mídia com os dados para um diretório de trabalho e colocar o script `spi_ufed_whatsapp_email.py` no diretório criado (hierarquicamente acima do diretório "EmailWhatsApp").
- 4- No UFED Physical Analyser, fazer importação do diretório (contendo arquivos de conversas, contatos e anexos) como imagem através do seguinte procedimento ilustrado a seguir:

 UFED Physical Analyzer 6.3.12.34

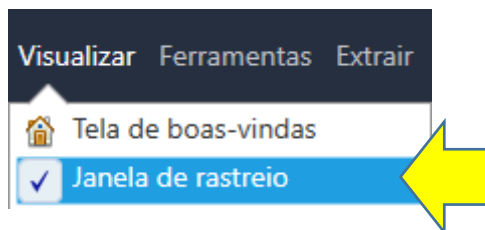


## Iniciar sem um arquivo UFD

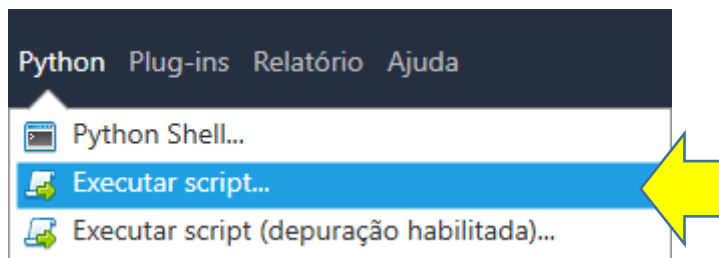
Use essa opção caso tenha sido usado outro método para extrair os dados (por exemplo, um chip-off ou uma ferramenta diferente).

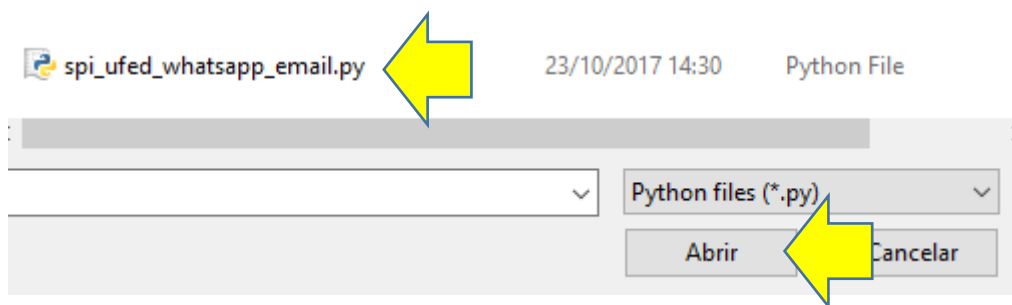


- 5- Recomenda-se habilitar a janela de rastreo antes da execução do script para acompanhamento de eventuais mensagens informativas ou de erro que possam ser apresentadas durante a execução do script. Para isso habilite a janela de rastreo na opção da interface de usuário ilustrada abaixo:



- 6- Executar o script e aguardar a elaboração da carga dos dados indo na janela de execução e escolhendo o script para execução de acordo com a sequência a seguir:





## Observações

Recomenda-se ao fim do processo a execução do PLUGIN nativo `ContactCrossReference` para fazer tradução de números para nomes que eventualmente possa ter em listas de contatos obtidas de outras fontes e carregadas no UFED Physical Analyser. O PLUGIN pode ser executado a partir dos seguintes passos:

