

Manual para utilização dos *Scripts* para UFED para carga de extração automatizada de *screenshots* com conversas do aplicativo Facebook Messenger (FBM) para Android

GNU GENERAL PUBLIC LICENSE -Copyright: 2019 Alberto Magno <alberto.magno@gmail.com>

Para extração fotográfica de mensagens do aplicativo Facebook Messenger - FBM, foi construído script, denominado `extracaoAVC_Facebook.py`, na linguagem python (versão 2.7) para operar remotamente o dispositivo efetuando *screenshots* da tela das mensagens contidas na lista de bate-papos do aplicativo.

Para essa operação foi utilizado o projeto denominado AndroidViewClient (disponível em <https://github.com/dtmilano/AndroidViewClient/>) que consiste de uma biblioteca em python de ferramentas que simplificam a criação de scripts de teste abstraindo detalhes da ferramenta monkeyrunner do ADT (<https://developer.android.com/studio/test/monkeyrunner/>), fornecendo uma visão hierárquica instantânea dos componentes apresentados no visor do dispositivo.

Devido a simulação de operações de toque, de arraste, e outras no dispositivo estarem intimamente ligadas a características físicas do dispositivo, podem ser necessários ajustes em literais numéricos ou textuais associados a coordenadas de tela ou nome de componentes visuais. Também, devido ao fato de que o próprio aplicativo FBM possuir diferentes versões com mudanças na ordem e estrutura dos componentes visuais e também pelo fato de que a construção dos elementos gráficos que compõem as telas do aplicativos serem construídas dinamicamente, no momento, não é possível vincular a navegação remota a identificadores, restringindo a operação a posições e títulos dos componentes visuais. Outras formas de operação para automatização de extrações como a do aplicativo WhatsApp foram realizadas de forma mais simples do que as utilizadas nesse script, porém não puderam ser replicadas devidas a características dinâmicas adotadas na codificação do FBM.

Para carga das imagens dos *screenshots* com os bate-papos extraídos em projetos no Cellebrite Ufed Physical Analyser (UfedPA), foi desenvolvido o *script* denominado `spi_ufed_FBM_photoXtract.py`, que realiza a carga dos bate-papos e coloca cada imagem contendo *screenshots* das mensagens do bate-papo como se fossem anexos de mensagens.

Uso do script de extração fotográfica

Primeiramente, é necessário que o ambiente de execução python esteja operacional e que se tenha instalado o pacote do AVC. Uma forma de se instalar é através do instalador padrão:

```
pip install androidviewclient
```

Outras formas de instalação e possível solução para problemas estão descritos em:

<https://github.com/dtmilano/AndroidViewClient/wiki>

Inicialmente escolhe-se o diretório base para extração, coloca-se o arquivo do *script* nesse diretório, e executa-se da seguinte forma:

```
python extracaoAVC_Facebook.py
```

O script cria um diretório principal com o padrão de nomenclatura:

```
FBMphotoXtract_YYYY-MM-DDTHHmmSS.ms
```


E dentro desse diretório, é criado subdiretórios nominados com o nome de cada bate-papo e dentro do respectivo diretório são gravados os arquivos dos *screenshots* das mensagens.

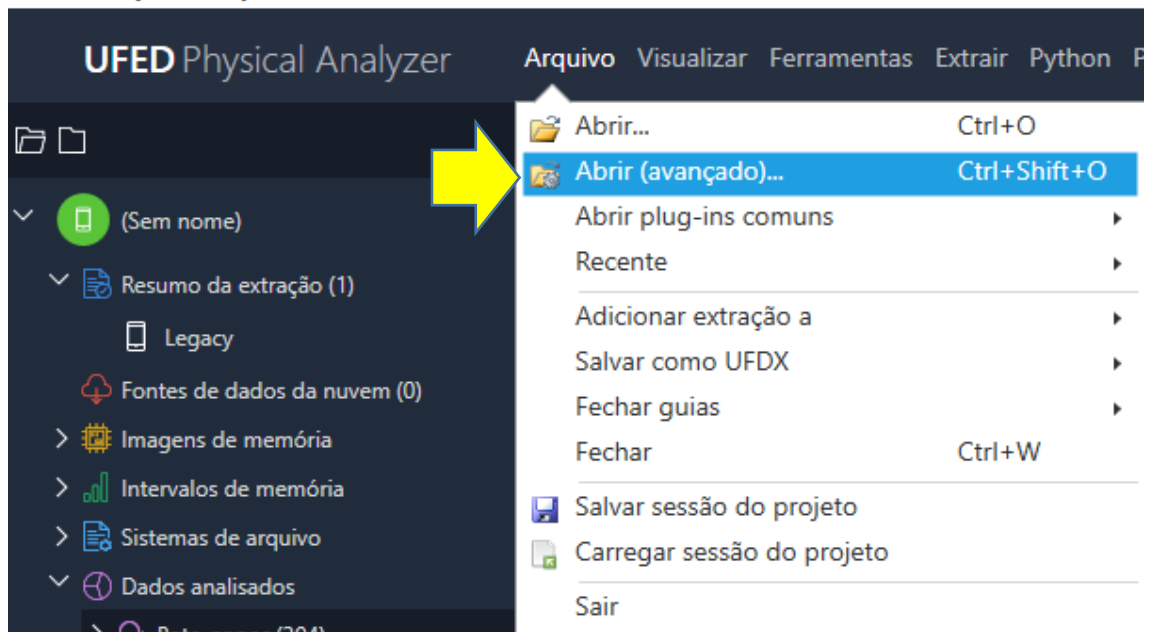
Podem ocorrer problemas de operação, como queda do servidor ADB do host (o AVC utiliza de um cliente ADB para várias operações). Com isso, pode ser interessante comentar parte do *script* para não chamar a função `toStart()`, que posiciona a lista de bate-papos no início, para permitir continuar a extração do bate-papo situado no início da lista visível.

Uso do script de carga da extração fotográfica

Os passos para uso do script `spi_ufed_FBM_photoXtract.py` são os seguintes:

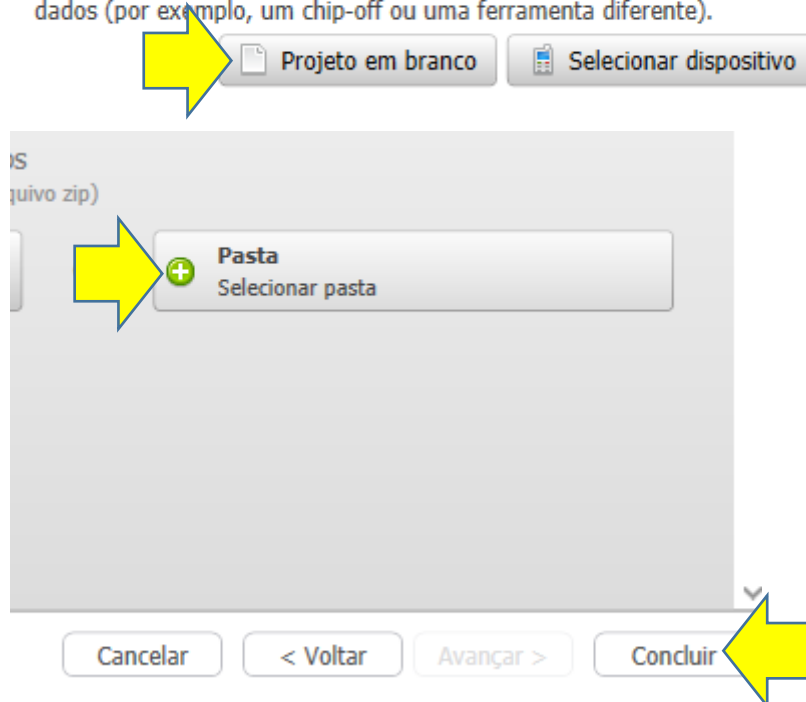
- 1- Copiar o script `spi_ufed_FBM_photoXtract.py` um nível acima do diretório gerado pela execução do script anterior (hierarquicamente acima do diretório “FBMphotoXtract_YYYY-MM-DDTHHmmSS.ms”).
- 2- No UFED Physical Analyser, fazer importação do diretório FBMphotoXtract_YYYY-MM-DDTHHmmSS.ms através do seguinte procedimento ilustrado a seguir:

 UFED Physical Analyzer

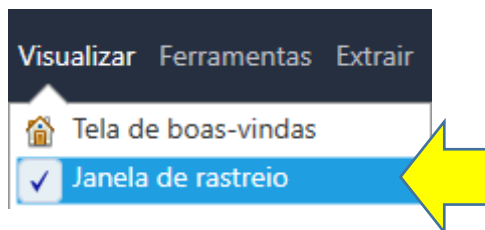


Iniciar sem um arquivo UFD

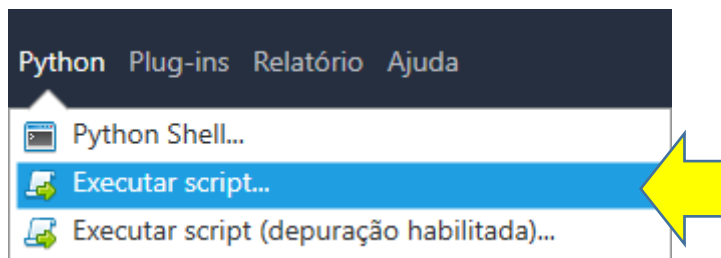
Use essa opção caso tenha sido usado outro método para extrair os dados (por exemplo, um chip-off ou uma ferramenta diferente).

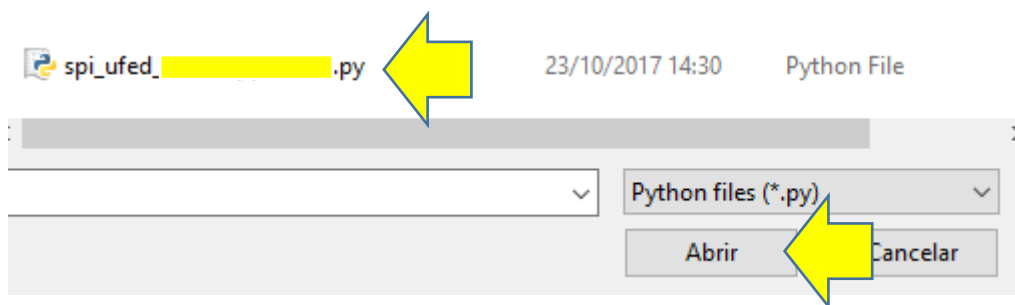


- 3- Recomenda-se habilitar a janela de rastreo antes da execução do script para acompanhamento de eventuais mensagens informativas ou de erro que possam ser apresentadas durante a execução do script. Para isso habilite a janela de rastreo na opção da interface de usuário ilustrada abaixo:



- 4- 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

O script de carga da extração fotográfica para o UFED PA faz em ordem temporal decrescente da data de modificação da geração dos snapshots, visando manter correspondência com o ordenamento dos bate-papos apresentado no aplicativo. Os snapshots para cada bate-papo também são inseridos como anexos das mensagens de cada bate-papo na ordem temporal decrescente como apresentada pelo aplicativo.