Perícia Digital nos Chats e Diálogos do Ministro Sérgio Moro com Procuradores da Lava Jato. As conversas divulgadas são confiáveis?

Muito tem se discutido sobre as graves violações que em tese teriam praticado o Ministro Sérgio Moro em conversas (chats) com procuradores da operação lava jato. Os textos foram apresentados pelo The Intercept, que vem protegendo a fonte.

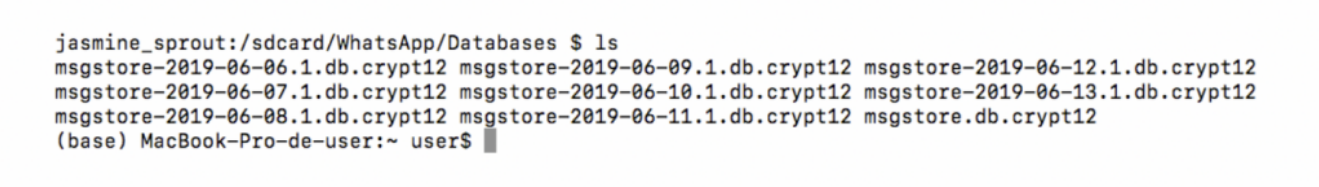
Sem adentrar em questões jurídicas ou até mesmo éticas, fato é que por demais temerário qualquer decisão com base em "textos" que supostamente representariam chats.

A perícia em informática demonstra-se fundamental. Uma pericia em informática tem condições de, em se avaliando os arquivos, identificar fontes, metadados, assinaturas e demais padrões que possam levar à conclusão da autenticidade dos referidos textos. Sem isso, qualquer argumentação é passível de descrédito.

Hoje existem inúmeras aplicações capazes de simularem chats. Outras, mais avançadas, conseguem até fazer inserções em arquivos originários dos comunicadores. Logo, diante do suposto vazamento de dados do Telegram e WhatsApp e considerando inúmeras Fakes que

já surgiram na
Internet (retratando chats inexistentes) a prova técnica poderá esclarecer a
questão.

A exemplo, as conversas do WhatsApp ficam armazenadas de forma criptografada em arquivos de bancos de dados em /sdcard/WhstaApp/Databases:



Tendo acesso à chave (key), que fica salva
diretamente no dispositivo (pasta /data) pode-se tentar extrair as mensagens,
identificando se existiram (autências e integras) ou não. De se destacar que o
WhatsApp também armazena um msgstore sem criptografia, utilizado para dados de
transição e que pode ser acessado com um celular em modo root.

Por sua vez, o Telegram, também adota
criptografia, mas ao contrário do WhatsApp não é ponta a ponta mas cliente-servidor,
sendo a ponta a ponta somente a criptografia do “chat secreto”. De qualquer forma,
considerando que o próprio Telegram já informara que não fora hackeado, caso
sejam íntegros, os chats podem ter sido obtidos por meio de códigos maliciosos,
acesso físico ao dispositivo ou Chip swap e suas consequências.

Ainda assim, para se provar a autenticidade de um chat ou conversa do Telegram, é preciso avaliar os arquivos e dados gerados. Satrya, Daely e Nugroho (2016), apresentam a pesquisa *“Digital Forensic Analysis of Telegram Messenger”,* onde

oferecem a estrutura de dados do aplicativo, inclusive a possibilidade de recuperação de mensagens, a partir do dispositivo:

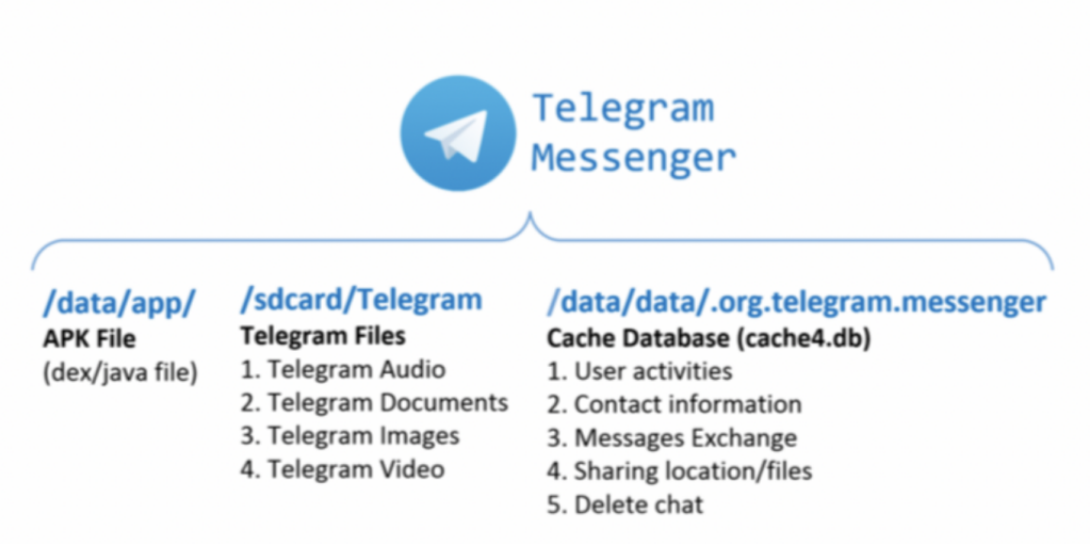


Fig. 1: Structure Telegram Forensics Analysis
Satrya, Daely e Nugroho (2016)

Como se verifica, embora o aplicativo armazene as conversas em seus servidores, o arquivo cache4.db, no equipamento, armazena ou conteúdo, ainda que parcial, com destaque para a tabela messages que armazena as mensagens trocadas e um MID (message ID específico) para cada mensagem, além de dados como data e hora.

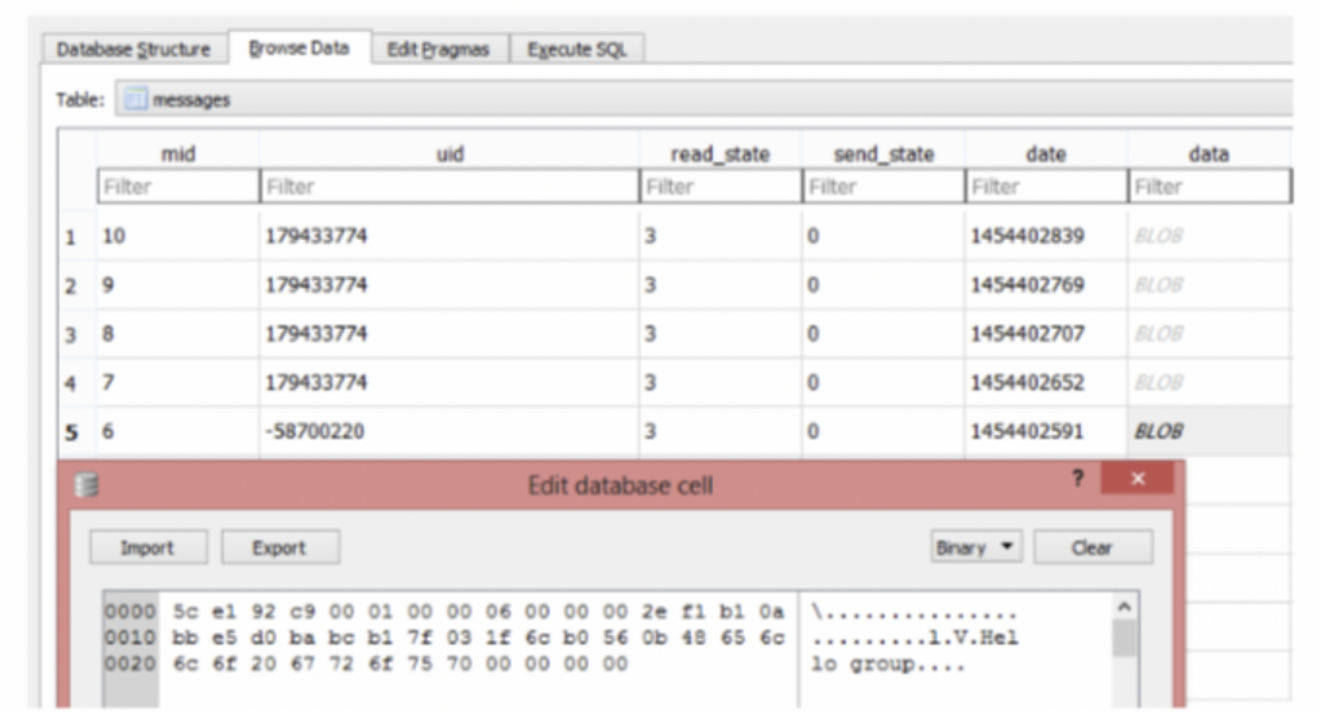


Fig. 2: Evidence database messages in table messages
Satrya, Daely e Nugroho (2016)

Com efeito, uma tentativa de inserção de uma “conversa” diretamente na tabela iria subverter a ordem dos Ids além de perturbar outros pontos do app, razão pela qual a integridade de um “chat” passa necessariamente pela confrontação entre arquivos publicados e sua correlação com as bases dos terminais envolvidos ou servidor. Por outro lado, se não aparecem as evidências das conversas, mas tão somente são postadas ou publicadas supostas “conversas”, prova mais do que frágil, a menos que incontroversa, não sendo recomendada qualquer decisão com base em tais conteúdos. O cenário chama atenção para os cuidados que vítimas de “fakechats” devem tomar. O principal é custodiar adequadamente o equipamento e em caso de divergência, podem periciar o mesmo, de forma buscar avaliar quais “chats” são íntegros e quais não.

REFERÊNCIAS

SATRYA, Gandeva Bayu; NUGROHO; Muhammad; DAELY, Philip Tobianto. **Digital Forensic Analysis of Telegram Messenger on Android Devices.** 2016 International Conference on Information & Communication
Technology and Systems (ICTS), At Surabaya, Indonesia. Disponível em: < https://www.researchgate.net/publication/316530864_Digital_Forensic_Analysis_of_Telegram_Messenger_on_Android_Devices> Acesso em: 13 jun. 2019

José
Antonio Milagre, perito em informática e especialista em crimes
cibernéticos, mestre e doutorando pela UNESP, diretor do Instituto de Perícias
Digitais (IPDIG), professor e coordenador de pós-graduação em computação
forense, autor de dois livros pela editora saraiva. www.josemilagre.com.br