

# WhatsApp Forensics: Análise forense e investigação digital

Não restam dúvidas que uma análise de um dispositivo móvel que contenha WhatsApp a qualquer momento chegará nas mãos de qualquer profissional de computação forense. Crimes, fraudes e ilícitos podem ser praticados por intermédio do mensageiro.

Recém comprado pelo Facebook, o aplicativo é padrão em comunicação instantânea no Brasil, e constantemente objeto de estudos, quando o tema é [“quebrar” sua criptografia](#). Porém são raras pesquisas que se dediquem a tratar sobre a auditoria ou mesmo sobre a computação forense aplicada aos rastros deixados por este aplicativo, repise-se, febre no Brasil.

Além de texto plano a aplicação também permite o compartilhamento de fotos e vídeos, com uma agravante, o sistema de “aceitação” é precário. Se alguém compartilha conteúdo ilícito ou te insere em um “grupo” para atividades ilegais, é você quem deve estar esperto e sair ou recusar o conteúdo.

Neste [excelente guia](#) sobre “Live Memory Forensics” às fls 73 e seguintes, temos uma importante referência de Estudos para a coleta de evidências no WhatsApp. Um plugin com a utilização do Volatility permite realizar o parsing das conversações persistentes na memória.

Lembrando que o Volatility tem uma API pública e vem com um extensível sistema de plugins que permitem a escrita de novos códigos e a extração de novos artefatos, daí porque trata-se de um importante aliado para análise de memória de dispositivos móveis.

Outro [trabalho interessante vem da Índia](#), especificamente,

escrito por profissionais e pesquisadores do “Institute of Forensic Science”, Guajarat. Ele também envolve análise não volátil e se aplica ao concorrente, o VIBER. Porém os pesquisadores utilizaram o UFED (solução proprietária) para todo o trabalho.

Em síntese, para uma análise não volátil é interessante que o examinador colete os seguintes arquivos (Lembrando que a pasta Media e ProfilePictures não são encriptadas):



Ocorre que a empresa cifrou seus dbs, não sendo mais tão simples a coleta e análise das conversações e outros elementos. Hoje identificamos um msgstore.db.crypt:



Fonte:

<http://resources.infosecinstitute.com/android-architecture-forensics/>

Alguns [scripts \(python\)](#) chegaram a ser criados para quebrar a criptografia, mas hoje não estão funcionais, [mas estude os códigos aqui](#):



Fonte: [yagil5/whatsapp-hacking-2013-lucideus-tech-private-limited](#)

Alguns textos recomendam submeter o arquivo crypt ao <http://www.recovermessages.com/> que “em tese” quebraria a criptografia da última versão do aplicativo. Não realizei testes, tampouco posso atestar a veracidade.

Diante das proteções implementadas, mais e mais ganha-se relevância a análise de memória dos dispositivos móveis. Especificamente quando falamos de WhatsApp, muitos artefatos na RAM não estarão criptografados, como estão no disco. Assim, fica recomendada esta pesquisa [Forensic Analysis of WhatsApp](#)

[on Android Smartphones](#) de junho de 2013, que é muito interessante a medida em que conclui que os mensageiros contemporâneos usam sistemas similares para armazenar mensagens e atualizar os bancos de dados. A pesquisa apresenta o whatsappRamXtract um bash script que pode ler um arquivo de memória extrair fragmentos gerados pelo comunicador.

Recomendo também aos interessados, considerando a imprescindível necessidade do perito em dominar o Volatility, que acessem periodicamente o [Volatility Labs Blog](#) e mantenham-se atualizados acerca das iniciativas para tunar a ferramenta, sobretudo a adaptando às características das novas aplicações, bem como sobre os desafios da forense em memória.

Não custa lembrar, o presente texto orienta para os estudos e pesquisas na área forense. Qualquer utilização não autorizada pela justiça ou mal-intencionada poderá ser considerada criminosa, sujeitando os infratores às penas da Lei.