WhatsApp como prova judicial: verificação de efetividade de ferramentas forenses

aluno(a): Zwaig, Y. C / research@tadeu.work / *(11) 94972-5989* / FT/UNICAMP - Faculdade de Tecnologia da Universidade Estadual de Campinas.
orientador(a): Marli de Freitas Gomes Hernandez / marli@ft.unicamp.br / *(19) 99181-5143* / FT/UNICAMP
Coautora: Marbilia Possagnolo Sergio / marbilia.sergio@cti.gov.br / *(19) 99700-6804* / *CTI* - Centro de Tecnologia da Informação Renato Archer

RESUMO: Para verificar a integridade artefatos do WhatsApp, a perícia conta com ferramentas forense baseadas nos parâmetros do NIST[2]. Este trabalho busca avaliar a eficácia de sete ferramentas quanto a identificação de fraude na análise de um conteúdo alterado em uma conversa. As alterações foram realizadas utilizando a ferramenta AlterWhats [3] desenvolvida para este fim. Como resultado tem-se que duas delas não conseguiram extrair os dados do emulador, impossibilitando suas avaliações, as demais não detectaram as alterações realizadas. A contribuição, além do desenvolvimento da ferramenta AlterWhats, foi a de demonstrar que, devido a falha de verificação da integridade da mensagem torna possível que as ferramentas testadas façam um diagnóstico forense falho.

Palavras-chave*: WhatsApp, ferramentas forenses,* evidência jurídica
Área: 1.03.03.04-9- Sistemas de Informação; ***Órgão de financiamento****: CNPq - PIBIC CTI.*

1. INTRODUÇÂO

Conversas do WhatsApp já são usadas como evidência jurídica. Embora a criptografia ponta a ponta do WhatsApp impeça uma interceptação convencional, no Brasil, o acesso às mensagens se dá, com mandados de busca e apreensão dos dispositivos onde elas estão armazenadas. No Brasil não existe uma legislação quanto a obtenção de provas por meio eletrônico, mas, inúmeras conversas são utilizadas como evidência jurídica. Por exemplo, o caso do Neymar em junho de 2019 onde um vídeo o inocentou da acusação de violência contra uma mulher [1].

Para verificar a integridade artefatos do WhatsApp, a perícia conta com ferramentas forense baseadas nos parâmetros do NIST[2]. Assim, este trabalho de pesquisa pretendeu avaliar a eficácia destas ferramentas na identificação de fraudes na analise do conteúdo do WhatsApp. Este trabalho de pesquisa se propôs a identificar ferramentas forense livre e testa-las em conversas previamente alteradas, com uso da ferramenta AlterWhats [3] desenvolvida para este fim.

Nos próximos tópicos são apresentadas a base teórica, a metodologia, os resultados obtidos e conclusão sobre o trabalho.

2. BASE TEORICA

Para o desenvolvimento dessa pesquisa, foi realizada a revisão literária nas bases de dados da IEEE e da WOS. Utilizou-se como argumento de pesquisa o termo “WhatsApp” obtendo-se um total de 1259 publicações. Os títulos e resumos das publicações selecionadas foram incluídos na versão de 2020 do aplicativo SW3T [4]. O Sw3T é uma ferramenta de apoio a revisão literária que permite a analise a documentação de seus resultados titulo a titulo. Foram selecionados treze artigos que focam em atividades forense e que utilizam ferramentas para analise de conteúdo do WhatsApp assim como os que descrevem a configuração do aplicativo WhatsApp.

No levantamento das ferramentas foram selecionadas 7 aplicações forense de possível acesso sem custo. Foi desenvolvido o software **AlterWhats** para realizar alterações de artefatos em conversas do WhatsApp com base em especificações disponível do aplicativo.

2.1. Ferramentas Forense

Umar et at [2] utilizam 3 ferramentas forenses, com base nos parâmetros NIST, para a analise de artefatos do WhatsApp. Entre elas, destaca-se a ferramenta “WhatsApp Key/DB Extractor” utilizada nesse trabalho. As demais ferramentas não são de fácil acesso ou de custo alto para obtenção inviabilizando sua utilização. Alissa et al [5] descrevem formas de obtenção dos dados em uma investigação forense e mostra facilidades para obtenção de dados via

arquivos do WhatsApp. O artigo também expõe 4 ferramentas forenses das quais três foram utilizadas neste trabalho, além da “WhatsApp Key/DB Extractor” cita “Guasap” e “Elcomosft WhatsApp Explorer”(versão de teste).

Anglano [6] expõem a composição dos artefatos do WhatsApp auxiliando na identificação de seus elementos. Após uma ampla pesquisa, foram escolhidas as seguintes ferramentas citadas em outros artigos, que são gratuitas ou com versão de teste:

1. Guasap Forensic (Versão de 09 de Julho de 2019)[7]
2. WhatsApp Key/DB Extractor (Versão de 21 de Outubro de 2016)[8]
3. WhatsApp Viewer (Versão de 29 de Julho de 2019) [9]
4. WhatsApp Xtract (Versão de 25 de Abril de 2018)[10]
5. Bring2lite (Versão de 05 de Agosto de 2019)[11]
6. Elcomsoft Explorer Forense (Versão de teste obtida em maio de 2020) [12]
7. WhatsApp Parser (Versão de 18 de Junho de 2020) [13]

2.2. Configuração do Aplicativo WhatsApp

Os artefatos do WhatsApp são armazenados em banco de dados, arquivos de backups e de logs (responsável por guardar histórico de eventos do aplicativo). Os arquivos relevantes para este experimento são apresentados na Tabela 1.

Tabela 1 - Arquivos do WhatsApp utilizados neste experimento

#	Conteúdo armazenado	Diretório comum	Nome do Arquivo
1	*Conversas, mensagens*	*/data/data/com.WhatsApp/databases/*	*msgstore.db (SQLite)*
2	*Contatos*	*/data/data/com.WhatsApp/databases/*	*wa.db (SQLite)*
3	*Backups do msgstore*	*/sdcard/WhatsApp/Databases/*	*msgstore-{DATA}.db.crypt12*
4	*Backups diversos*	*/sdcard/WhatsApp/Backups/*	**.db.crypt1*
5	*Arquivos recebidos/enviados*	*/sdcard/WhatsApp/Media/*	*
6	*Arquivos de log*	*/data/data/com.WhatsApp/files/Logs/*	*WhatsApp.log WhatsApp-{DATA}.log.gz*

Foram objetos deste experimento os artefatos {1}, {3}, {6} da Tabela 1. Sendo:

- **Conteúdo do banco msgstore {1}:** que contém todas as informações sobre conversas e mensagens. Entre as tabelas relevantes para esta pesquisa, destacam-se oito delas, sendo:
  1. Listagem de chats do usuário chat
  2. Listagem de chats do usuário chat_list
  3. Conteúdo das mensagens message_ftsv2
  4. Conteúdo das mensagens message_ftsv2_content
  5. Desconhecido message_ftsv2_docsize
  6. Conteúdo e dados sobre uma mensagem
  7. Conteúdo das mensagens messages_fts
  8. Conteúdo das mensagens messages_fts_content
- **Backups do msgstore {3}**: seus dados são criptografados, mas, há diversas ferramentas que decodificam esse backup [9] e ferramentas que tentam pegar essa chave sem acesso root [8]. Esse backup é importante pois ele contém informações antes da alteração pelo software AlterWhats, então é interessante sobrescrevê-lo ou remover o conteúdo seguramente.
- **Arquivos de Log {6}:** contém todas as iterações feita pelo usuário e pelo sistema. Por exemplo, o recebimento de mensagens e o bloqueio de usuários [14]. Esse arquivo guarda informações que podem desmentir alguma alteração.

3. METODOLOGIA

Para esta pesquisa foi adotado a metodologia de pesquisa-ação onde se pretendeu, através de um experimento, qualificar as ferramentas forense quanto a eficácia na detecção de conversas modificadas do WhatsApp. Os resultados de cada atividade foram analisados quanto a sua adequação e necessidade de ajuste e reexecução. Durante a pesquisa, a metodologia viabilizou a inclusão de atividades não previstas inicialmente. As atividades realizadas foram:

- **Revisão literária** – com o objetivo de identificar publicações científicas relacionadas a processo forense que valida a integridade das informações contidas no WhatsApp e as vulnerabilidades e funcionalidades do WhatsApp;

- **Entendimento das funcionalidades do WhatsApp** de forma a identificar sua estrutura física e logica a fim de estabelecer a melhor forma de realizar alterações nos artefatos; Especificação do ambiente de desenvolvimento;
- **Software AlterWhats [3]**, sua especificação e codificação para efetuar alterações no conteúdo de conversas no WhatsApp. Fora utilizado o Android Debug Bridge (adb)[15] e linguagem PHP para o seu desenvolvimento.
- **Identificação de ferramentas forenses** mais populares e estabelecer quais são passíveis de serem utilizadas neste experimento;
- **Realização de testes** com diversas ferramentas forenses para confirmar a alteração não é detectada pelas ferramentas;

4. RESULTADO

Destacam-se dois tipos de resultado, o da alteração efetuado pelo aplicativo AlterWhats onde se evidencia seu uso e **os resultados da execução das** ferramentas forenses selecionadas.

4.1. Quanto ao uso software AlterWhats

Alteração realizada pelo AlterWhats em uma conversa, conforme figura 1, teve como objetivo alterar o valor da divida de $10 para $10000 (dólares), e a data de sua cobrança de 05/10/2020 para 04/09/2020 e corromper os logs e backups.

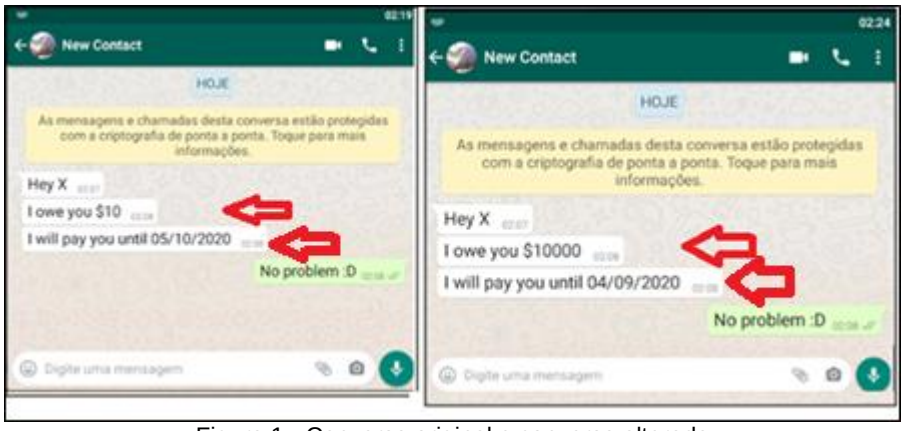

Figura 1 - Conversa original e conversa alterada

O software AlterWhats interpreta a conversa como se observa na Figura 2. Onde o software oferece varias funcionalidades, o conteúdo da conversa original e a lista dos últimos comandos por ele realizados.

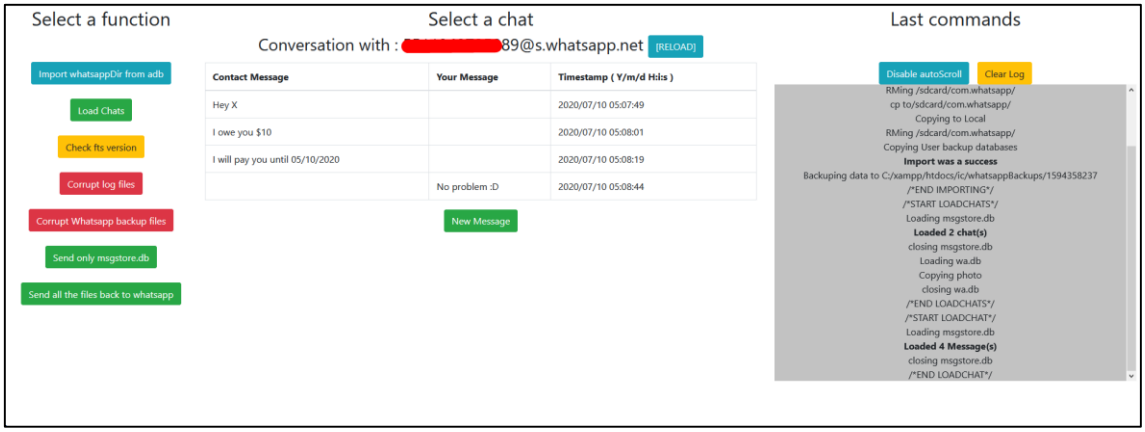

Figura 2 – Interpretação do Software AlterWhats sobre a conversa antes da alteração realizada

Após as alterações realizadas, o AlterWhats apresenta a nova interpretação onde o valor e a data estão alterados. Veja a Figura 3 que mesmo após as alterações a interpretação é a mesma, apenas com as alterações efetuadas.

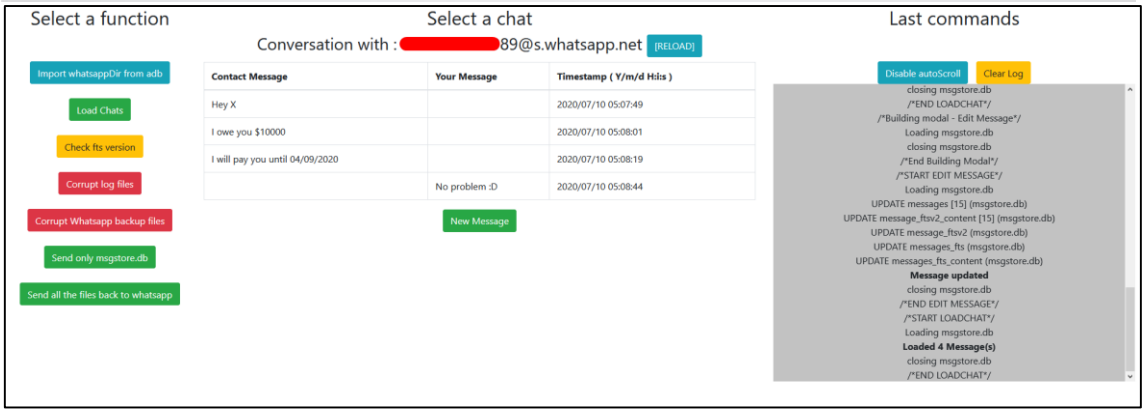

Figura 3 - Interpretação do Software AlterWhats depois da alteração realizada.

Após a alteração de uma mensagem, para garantir que não tenha vestígios, o conteúdo das diversas tabelas do msgstore foram ajustadas. É importante ressaltar que algumas tabelas não têm chave primaria definida, então usou-se “rowid” padrão do SQLite.

Em seguida, os arquivos do WhatsApp alterados no AlterWhats foram enviados para o celular e realizado um backup na nuvem. Apenas mudar o conteúdo no dispositivo do autor não é suficiente já que o outro participante da conversa ainda tem a conversa “original”. Assim, considerou-se o uso de bugs no código do WhatsApp para forçar a exclusão/inclusão dos dados no celular do outro participante ou se utilizar vulnerabilidades mais avançadas que permitam excluir seletivamente os dados [16] [17] [18].

4.2. Quanto aos Testes das ferramentas:

Como resultado dos testes, tem-se que as ferramentas **Guasap Forensic** (v9/jul/12019) e **WhatsApp Key/DB Extracto**r (V21/out/2016) não conseguiram extrair os dados do emulador, impossibilitando a avaliação. Já as temais obte-se:

- ✓ O **WhatsApp Viewer** mostrou as mensagens editadas, e um campo a mais após a primeira mensagem, provavelmente a troca de chaves entre os contatos. Vestígio da alteração não foi detectado.
- ✓ O **WhatsApp Xtract** não verifica alterações na msgstore, só checa o conteúdo do banco de dados, mostrando as mensagens editadas. Vestígio da alteração não foi detectado.
- ✓ O **Bring2lite** obtém as linhas excluídas de tabelas Sqlite. Assim, ao executa-lo todas as tabelas que tem a informação original foram recuperadas, mas a informação contida nelas é a alterada pelo software AlterWhats. Vestígio da alteração não foi detectados.
- ✓ O **Elcomsoft Explorer for WhatsApp (trial)** não verifica alterações e as mensagens modificadas são exibidas normalmente. Vestígio da alteração não foi detectado.
- ✓ O **WhatsApp Parser** tsó lê e exibe o editado. Vestígio da alteração não foi detectado.

Observa-se que as cinco ferramentas testadas não detectaram a alteração.

5. CONCLUSÃO

Este trabalho de pesquisa se propôs a testar ferramentas forense, de acesso livres, em conversas previamente alteradas. Observou-se que com a ferramenta AlterWhats, desenvolvida neste projeto, foi possível realizar alterações imperceptíveis para cinco ferramentas forense assim, afirma-se que embora estas ferramentas forenses possam detectar diversas tentativas de fraude, através da analise e comparação de seus arquivos e back-ups, ainda é possível que fraudes não sejam detectadas e forneçam resultados negativos quanto à existência de fraude. A estratégia Alemã de coletar conteúdo em tempo real utilizando softwares maliciosos parece ser uma solução consistente no caso de investigações.

Ao estudar as possibilidades a partir do entendimento do funcionamento do WhatsApp e seus artefatos, foi possível identificar que com o uso de backup na nuvem, é possível alterar os artefatos do WhatsApp em um dispositivo com privilégios de alteração de sistema (*root)* e encaminhá-lo para outro dispositivo desprovido de tais privilégios, dificultando a comprovação de que os artefatos de uma conversa foram manipulados.

O trabalho limitou-se a testar as ferramentas forense gratuitas, cabe a continuação dos testes utilizando outras ferramentas forenses disponíveis no mercado. A revisão literária focou em duas Bases Dados. Embora as BDs sejam fortes em temas relacionados a segurança da informação, cabe a expansão do levantamento para outras bases a fim de identificar mais

ferramentas, relatos de vulnerabilidade e estudos similares quanto a eficácia das ferramentas forense. Futuros trabalhos também podem destinja os componentes do Whatsapp afim de viabilizar eventuais melhorias visando evitar fraudes.

Nunca fora segredo ser possível alterar mensagens de conversas do WhatsApp, mas, não foi encontrado estudo sobre a manipulação dos artefatos em investigações forenses. Assim, a importante contribuição deste trabalho é a demonstrar que, devido a existência de falha de verificação da integridade da mensagem após sua saída dos servidores do WhatsApp, torna-se possível alterações não detectáveis de artefatos (como mensagens). Uma vez que as ferramentas forenses testadas não possuem métodos para verificar a integridade, portanto afirma-se que as ferramentas forenses podem produzir resultados errôneos.

REFERENCIAS:

[1] Garcia, Diego, “Neymar diz que vídeo com fotos íntimas foi publicado por assessores” 2019. Disponível em: https://www1.folha.uol.com.br/esporte/2019/06/neymar-diz-que-video-com-fotos-intimas-foi-publicado-por-assessores.shtml Acessado em: 18 Jul 2020

[2] Umar, Rusydi; Riadi, Imam; Zamroni, Guntur. A Comparative Study of Forensic Tools for WhatsApp Analysis using NIST Measurements. International Journal of Advanced Computer Science and Applications, vol. 8, no. 12, pp. 69-75, 2017.

[3] Tuyuribr, “AlterWhats” 2020. Disponível em:https://github.com/tuyuribr/AlterWhats Acessado em: 1/8/2020.

[4] M. P. Sergio, T. d. S. Costa, M. S. d. P. Pessoa and P. S. M. Pedro, "A Semantic Approach to Support the Analysis of Abstracts in a Bibliographical Review," 2019 IEEE 28th International Conference on Enabling Technologies: Infrastructure for Collaborative Enterprises (WETICE), Napoli, Italy, 2019, pp. 259-264, doi: 10.1109/WETICE.2019.00062.

[5] Alissa, K.; Almubairik, N.A.; Alsaleem, L. et al. A comparative study of WhatsApp forensics tools. SN Appl. Sci. 1, 1320 (2019). https://doi.org/10.1007/s42452-019-1312-8.

[6] Anglano, Cosimo. (2014). Forensic Analysis of WhatsApp Messenger on Android Smartphones. Digital Investigation. 11. 10.1016/j.diin.2014.04.003.

[7] Quantika14, “Guasap Forensic” 2019. Disponível em: https://github.com/Quantika14/guasap-WhatsApp-foresincs-tool Acessado em: 18 Jul 2020.

[8] TripCode, “WhatsApp Key/DB Extractor” 2016. Disponível em: https://github.com/EliteAndroidApps/WhatsApp-Key-DB-Extractor Acessado em: 18 Jul 2020.

[9] Mausch, Andreas. “WhatsApp Viewer” 2018. Disponível em : https://github.com/andreas-mausch/WhatsApp-viewer Acessado em: 18 Jul 2020.

[10] Ztedd, “[TOOL] WhatsApp Xtract: Backup Messages Extractor / Database Analyzer / Chat-Backup” 2018. Disponível em: https://forum.xda-developers.com/showthread.php?t=1583021 Acessado em: 18 Jul 2020.

[11] Meng, Christian & Baier, Harald. (2019). bring2lite: A Structural Concept and Tool for Forensic Data Analysis and Recovery of Deleted SQLite Records. Digital Investigation. 29. S31-S41. 10.1016/j.diin.2019.04.017.

[12] Elcomsoft, “Elcomsoft Explorer for WhatsApp”. Disponível em: https://www.elcomsoft.com/exwa.html Acessado em: 18 Jul 2020.

[13] B16f00t, “WhatsApp Parser Toolset” 2020. Disponível em: https://github.com/B16f00t/whapa Acessado em: 18 Jul 2020.

[14] C. Anglano. Forensic analysis of WhatsApp messenger on android smartphones. Digital Investigation. 2014.

[15] Google, “Android Debug Bridge (adb)” 2020. Disponível em: https://developer.android.com/studio/command-line/adb Acessado em: 18 Jul 2020.

[16] MITRE, “CVE-2019-11932” 2019. Disponível em: https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2019-11932 Acessado em: 18 Jul 2020.

[17] Swati Khandelwal, “This Bug Could Have Let Anyone Crash WhatsApp Of All Group Members” 2019. Disponível em:https://thehackernews.com/2019/12/WhatsApp-group-crash.html Acessado: 18/7/2020.

[18] Zerodium, “Our Exploit Acquisition Program” 2020. Disponível em: https://zerodium.com/program.html Acessado em: 18 Jul 2020.