Jurnal Infosecure Vol.4 No.1, Maret 2023
p-ISSN: 2087-1023
MTI-UNLA

Analisis Whatsapp Forensic Pada Android Menggunakan Whatsapp Backup

Hamdan Abdul Aziz[1], Arief Zulianto[2], Toto Suharto[3]

Magister Teknik Informatika, Universitas Langlang Buana[123]

[1]hamdan.nfs@gmail.com

Abstrak— Perkembangan internet dan teknologi saat ini telah mengakibatkan konvergensi berbagai kebutuhan dalam satu perangkat, yakni smartphone. Sebuah laporan dari ww.idc.com mencatat bahwa Android mendominasi pasar smartphone dengan pangsa sebesar 85%. Kebutuhan masyarakat dalam era internet ini berpusat pada penggunaan aplikasi perpesanan instan, yang digunakan untuk memfasilitasi komunikasi antara individu dengan keluarga, rekan bisnis, dan teman-teman. Aplikasi perpesanan instan ini mencakup berbagai variasi, dengan salah satunya adalah WhatsApp. Penggunaan WhatsApp oleh masyarakat mencakup beragam kebutuhan, baik dalam konteks bisnis maupun pribadi. Namun, disamping penggunaan yang sah, aplikasi ini juga rentan terhadap penyalahgunaan oleh individu dengan niat jahat, termasuk penipuan, pelanggaran privasi, dan kejahatan siber lainnya. Peningkatan jumlah tindakan kriminal ini mendorong perlunya ilmu forensik mobile dalam menyelidiki perangkat Android dan aplikasi WhatsApp. Salah satunya adalah dengan pengambilan data pada whatsapp backup. Pada penelitian ini dihasilkan, ada cara penggunaan open source dalam pengambilan data whatsapp backup dan hasil yang didapat sama dengan penggunaan tools berbayar.

Kata kunci— *Android, Backup, Open source, Whatsapp*

I. PENDAHULUAN

Perkembangan internet dan teknologi saat ini telah mengakibatkan konvergensi berbagai kebutuhan dalam satu perangkat, yakni smartphone, yang didukung oleh beragam aplikasi yang terhubung ke internet. Di zaman sekarang, dominasi di pasar smartphone terbagi antara dua sistem operasi utama, yaitu iOS yang dikembangkan oleh Apple, dan Android yang dikembangkan oleh Google. iOS telah menjadi bagian tak terpisahkan dari iPhone, sementara Android digunakan sebagai sistem operasi pada berbagai merek smartphone, seperti Samsung, Xiaomi, OPPO, dan banyak lainnya. Sebuah laporan dari ww.idc.com mencatat bahwa Android mendominasi pasar smartphone dengan pangsa sebesar 85%. Selain itu, perkembangan industri smartphone diperkirakan akan terus tumbuh, dengan perkiraan mencapai 3,8 miliar pengguna[3].

Kebutuhan masyarakat dalam era internet ini berpusat pada penggunaan aplikasi perpesanan instan, yang digunakan untuk memfasilitasi komunikasi antara individu dengan keluarga, rekan bisnis, dan teman-teman. Aplikasi perpesanan instan ini mencakup berbagai variasi, dengan salah satunya adalah WhatsApp. WhatsApp adalah salah satu aplikasi perpesanan instan yang paling dominan dalam penggunaannya saat ini. Dengan lebih dari 1 miliar pengguna aktif, WhatsApp memegang peran penting dalam ekosistem aplikasi perpesanan instan.

Penggunaan WhatsApp oleh masyarakat mencakup beragam kebutuhan, baik dalam konteks bisnis maupun pribadi. Namun, disamping penggunaan yang sah, aplikasi ini juga rentan terhadap penyalahgunaan oleh individu dengan niat jahat, termasuk penipuan, pelanggaran privasi, dan kejahatan siber lainnya. Penyalahgunaan teknologi informasi di perangkat seluler telah mengakibatkan kerugian yang signifikan dalam konteks keamanan jaringan[1].

Peningkatan jumlah tindakan kriminal ini mendorong perlunya ilmu forensik mobile dalam menyelidiki perangkat Android dan aplikasi WhatsApp. Tetapi dengan mahalnya tools mobile forensic, banyak penyidik di kepolisian tidak bisa mengambil data whatsapp. Untuk itu diperlukan tools untuk pengambilan data menggunakan open source.

Pada penelitian ini, akan diuraikan bagaimana teknik pengambilan data whatsapp forensic menggunakan whatsapp backup dengan menggunakan tools open source.

II. METODE

Metode yang digunakan dalam penelitian ini. Yang pertama adalah penelitian kualitatif, yaitu menggunakan penelitian library research, yang diambil dari berbagai kepustakaan seperti buku, artikel dan hasil penelitian. Serta Penelitian yang dilakukan pada tulisan ini adalah analisis whatsapp forensic pada android menggunakan whatsapp backup.

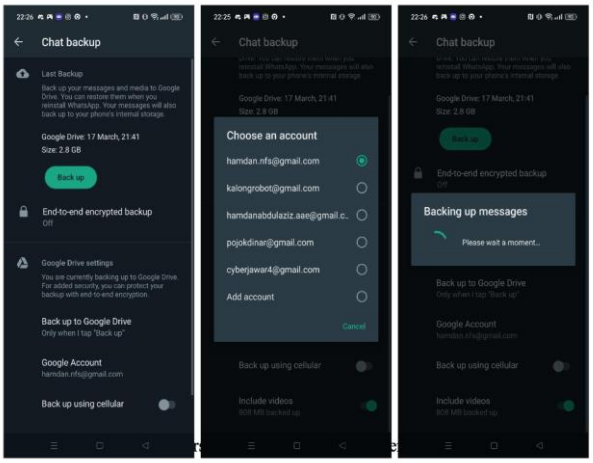
Kemudian langkah selanjutnya adalah melakukan proses pengambilan data dan analisis whatsapp backup menggunakan tools *open source.*

III. HASIL DAN PEMBAHASAN

Hasil dan pembahasan pada pembahasan penelitian ini adalah :

A. Pengambilan data backup

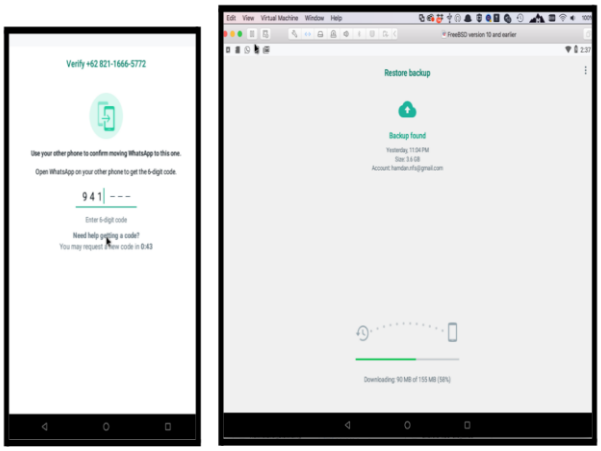
Dalam penelitian ini akan menguraikan metodologi yang dapat digunakan untuk mengekstraksi database WhatsApp pada perangkat yang menjadi subjek penyelidikan. Tahap awal dalam proses ini adalah mengambil salinan cadangan (backup) database tersebut sebelum melakukan proses pengamanan perangkat Android (airplane mode). Data cadangan ini kemudian harus disimpan dan diserahkan kepada pihak penyelidik melalui email.



Gambar. 1 Whatsapp Backup

B. *Melakukan Login Kembali*

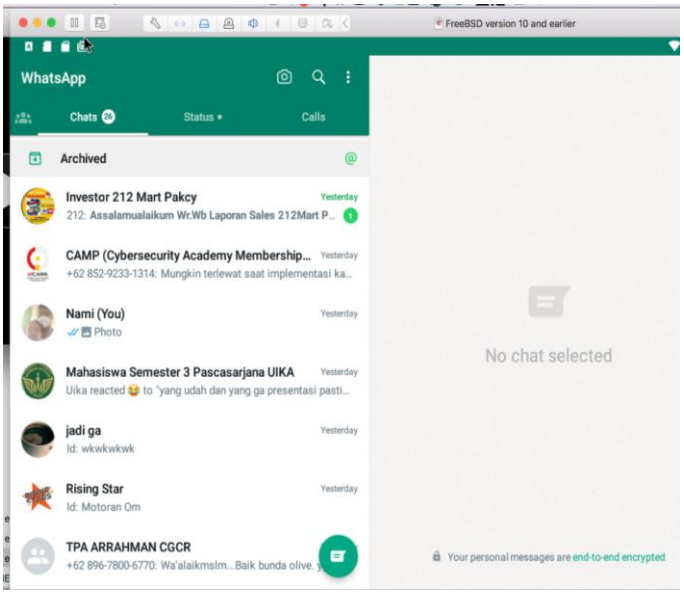
Selanjutnya, kita akan menjalankan proses login kembali ke aplikasi WhatsApp pada perangkat Android yang telah di-root. Untuk melakukan ini, kami akan memanfaatkan lingkungan virtual menggunakan Android-x86 yang diinstal di dalam platform seperti VMware atau VirtualBox. Proses login ini akan melibatkan penggunaan nomor telepon WhatsApp yang telah digunakan oleh tersangka pada perangkat Android sebelumnya.



Gambar. 2 Login Kembali Whatsapp

C. *Whatsapp Pada Android yang sudah ter rooting*

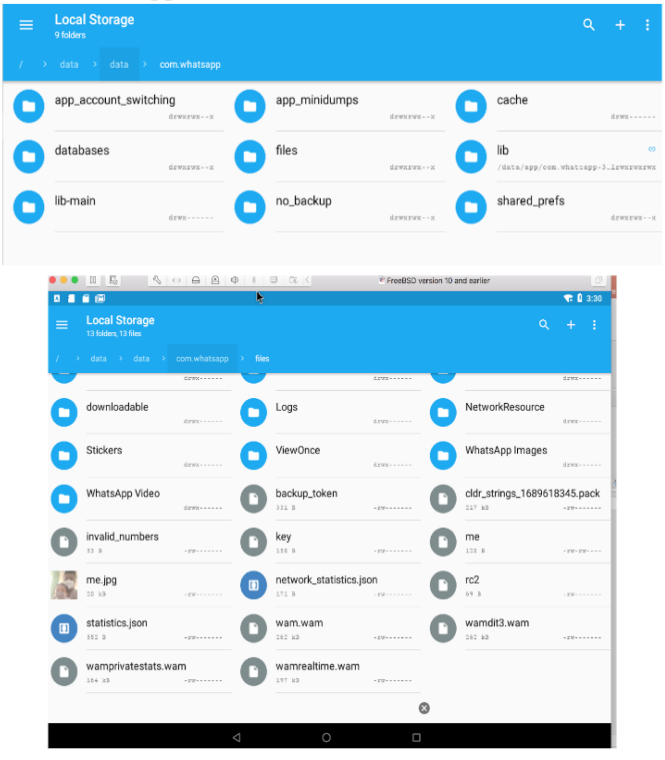
Setelah selesai login whatsapp, maka hasil yang didapatkan adalah whatsapp yang sesuai dengan hasil dari backup sebelumnya. Dan akan sama dengan whatsapp dari smartphone android yang sebelumnya di backup. Hasil yang didapatkan adalah chat, call log, shared media, dan media bisa didapatkan.



Gambar. 3 Whatsapp Setelah login kembali

D. *Analisa Hasil pengambilan data Whatsapp Backup*

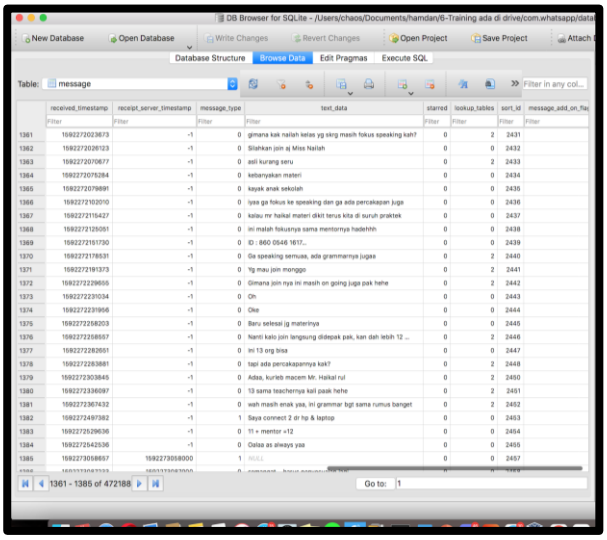
Kemudian, karena android yang dipakai sudah di rooting, maka kita bisa chek ke file manager. Dan bisa melihat data whatsapp di /data/data/com.whatsapp



Gambar. 4 File Database Whatsapp

E. *Analisis Database Whatsapp*

Setelah kita mendapatkan database yaitu wa.db dan msgstore.db. maka database bisa kita buka menggunakan sqlitebrowser. Dan data-data chat bisa kita buka semua.



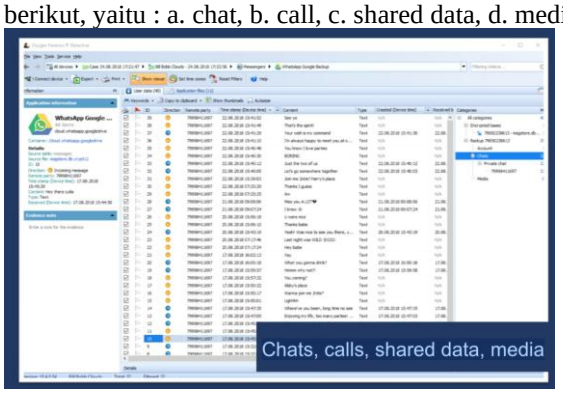
Gambar. 5 Analisis Database Whatasapp

F. Hasil yang didapatkan

Berdasarkan penelitian yang dilakukan, data yang dapat dihasilkan dari penggunaan tools open source dalam pengambilan data whatsapp Backup adalah : a. File Database, b. Media, c. Call log, d. Chat, e. key, f. shared data.

G. Perbandingan dengan tools berbayar

Berdasarkan oxygen forensic. didapatkan bahwa tools oxygen dapat mendapatkan data whatsapp seperti gambar berikut, yaitu : a. chat, b. call, c. shared data, d. media



Gambar. 6 Data yang dihasilkan oleh oxygen

Berdasarkan hasil data yang didapatkan oleh tools oxygen dan hasil dari penelitian ini, dapat dibandingkan sebagai berikut :

TABEL I
PERBANDINGAN TOOLS OPEN SOURCE DAN OXYGEN

Hasil yang didapatkan	open source	Oxygen
CHATS	V	V
CALLS	V	V
SHARED DATA	V	V
MEDIA	V	V

IV. SIMPULAN

Dari penelitian ini dapat disimpulkan bahwa tools open source bisa digunakan dalam pengambilan data whatsapp backup. Dengan menggunakan tools android x-86 yang terinstall di vmware dengan kondisi android sudah ter rooting. Hasil yang didapatkan adalah chat, call log, database, media bisa terambil sesuai dengan data backup yang diambil. Dan hasil ini sama dengan hasil yang didapatkan oleh tools berbayar oxygen.

Saran untuk penelitian selanjutnya adalah dengan melakukan riset dari sisi kecepatan tools open source dengan tools berbayar.

REFERENSI

[1] Zuraida, M. (2015). Credit Card Fraud (Carding) dan Dampaknya Terhadap Perdagangan Luar Negeri Indonesia. Jurnal Analisis Hubungan Internasional. 4(1): 1627–1642.
[2] Kemkominfo, "SIARAN PERS NO. 17/HM/KOMINFO/01/2019," 22 Januari
[3] https://www.statista.com/forecasts/1143723/smartphone-users-in-the-world
[4] Y. Pratomo, "Kompas.com," 16 April 2018. [Online]. Available: https://tekno.kompas.com/read/2018/04/16/20280017/bandar-narkoba-diringkus-setelah-kirim-foto-telapak-tangan-di-whatsapp.
[5] A. M. Pratama, "Kompas.com," 3 Mei 2017. [Online]. Available: https://megapolitan.kompas.com/read/2017/05/03/20103221/polisi.terus.kumpulkan.bukti.kasus.chat.whatsapp.diduga.rizieq-firza.
[6] K. Fathoni W, "Detik.com," 8 Februari 2019. [Online]. Available: https://inet.detik.com/security/d-4418667/waspada-penipuan-teman-gadungan-di-whatsapp.
[7] S. Wildansyah, "Detik.com," 15 November 2019. [Online]. Available: https://news.detik.com/berita/d-4786560/chatting-wa-jadi-senjata-pelapor-polisikan-andrew-darwis-soal-pemalsuan.
[8] Yadi, I. Z., dan Kunang, Y. N. (2014). Analisis Forensik pada Platform Android. Konferensi Nasional Ilmu Komputer 2014. 141-148.
[9] S.M. N. Al-Azhar, Digital Forensic: Practical Guidlines for Computer Investigation, Jakarta, 2012.
[10] J. Williams, "ACPO Good Practice Guide for Digital Evidence," Association.
[11] K. Kent, S. Chevalier, T. Grance and H. Dang, "NIST SP 800-86: Guide to Integrating Forensic Techniques into Incident Response," National Institute of Standards and Technology, Gaithersburg, 2006.
[12] SWGDE. (2013, September 14). SWGDE Best practice for computer forensics.https://swgde.org/documents/Current%20Documents/2014-09-05%20SWGDE%20Best%20Practices%20for%20Computer%20Forensics%20V3 -1.
[13] R. Ayers, S. Brothers and W. Jansen, "NIST Special Publication 800-101 Revision 1," National Institute of Standards and Technology, 2014.
[14] A. P. Heriyanto, Mobile Forensics: Theory, Yogyakarta: CV. Andi Offset, 2016.
[15] WhatsApp, "WhatsApp Encryption Overview: Technical White Paper,"WhatsApp, 2017.
[16] Upturn, “Mass Extraction” , 2020
[17] Cell on Earth: The Forensic Challenges of Mobile Devices | Stout