ABSTRACT

More than 1000 million users active based on survey 2017 and growing is increasing every year. WhatsApp has a table database that is stored classifield in the system Android system that is always updated in realtime. This database is automatically backed up with autobackup features that are different from the main database. The backup database has a .crypt12 file format. This crypt12 file can not be accessed because it has been encrypted.

Several studies have discussed of WhatsApp forensics use "logical extraction" method.

The Question of forensics when a user application use test chat and has been deleted. This purpose to remove the poll from the WhatsApp user. In this case we can actually see the deleted conversation by looking at the crypt12 from WhatsApp with descrip the data base. There are several tools for descrip crypt12 files. In this study we will compare tools to describe WhatsApp data base files. The results in analyzing forensic tests of the crypt12 file and the original file basically have the same contents, but there is a difference because in the backup process is not an update real time.

Key : *Forensics, Digital Forensics, Mobile Forensics, Android Forensics, WhatsApp Forensics, Forensics Tools, Instant Messaging.*

ABSTRAK

Dengan lebih dari 1000 juta pengguna aktif berdasarkan survey 2017 perkembangan ini semakin meningkat setiap tahunnya. Perlu diketahui bahwa WhatsApp mempunyai suatu tabel database yang tersimpan secara rahasia didalam sistem sistem Android yang selalu update secara realtime. Database ini selalu dicadangkan secara otomatis melalui fitur autobackup yang tersimpan berbeda dengan database utama. Database hasil backup ini mempunyai format file .*crypt12*. File *crypt12* ini tidak dapat diakses secara sembarang karena telah dienkripsi oleh aplikasi ini.

Beberapa penelitian telah banyak membahas tentang WhatsApp forensics diperangkat android dengan menggunakan beberapa medode salah satunya adalah metode "*logical Extraction*".

Dalam melakukan uji coba forensics muncul permasalahan ketika akan dilakukan uji forensics pengguna aplikasi telah menghapus percakapan yang telah dilakukan ini bertujuan untuk menghilangkan jajak dari pengguna WhatsApp. Didalam kasus ini sebenarnya kita dapat melihat percakapan yang telah dihapus dengan melihat data *crypt12* dari WhatsApp dengan cara mendeskripsikan data base tersebut. Ada beberapa tools untuk mendeskripsikan file *crypt12*. Pada penelitian ini akan membandingkan tools untuk mendeskripsikan file data base WhatsApp. Hasil penelitian menghasilkan dalam menganalisa uji forensics tidak lah cukup hanya mengandalkan tools yang dibandingkan akan tetapi harus melihat database hasil deskripsi. File *crypt12* dan file asli dalam sistem mempunyai struktur data yang sama tetapi jika lihat dari segi isi data terjadi perbedaan dikarenakan dalam proses backup tidak lah update secara real time karena WhatsApp hanya akan membackup setiap 24 jam sekali.

Kata Kunci : *Forensics, Digital Forensics, Mobile Forensics, Android Forensics, WhatsApp Forensics, Foreniscs Tools, Instant Messaging*.