

BAB 1

PENDAHULUAN

1.1 Latar Belakang

Kapolri Jenderal Pol Tito Karnavian mengatakan, penggunaan aplikasi *Telegram* oleh kelompok teroris di Indonesia bukan sebuah hal yang mengejutkan. Banyak teroris yang tertangkap mengakui bahwa komunikasi sesama anggota mereka dilakukan melalui aplikasi *Telegram*. Salah satunya digunakan pada saat kasus teror di kawasan MH Thamrin, Jakarta Pusat, Januari 2016 lalu. Tito mengatakan bahwa aplikasi tersebut menjadi favorit kelompok teroris karena melindungi privasi penggunanya [1]. Berdasarkan kasus tersebut maka dengan adanya ilmu forensik yang terus berkembang, kasus tersebut dapat di atasi dengan ilmu forensik yang dapat menganalisa barang bukti digital dari perangkat *mobile* di aplikasi *Telegram*. Metode yang cocok untuk kasus tersebut ialah dengan menggunakan ilmu forensik pada perangkat Android untuk aplikasi *Telegram* agar mendapatkan barang bukti digital.

Hasil forensik ini diharapkan dapat alat bukti yang sah secara hukum untuk penyelesaian kasus teroris dan cybercrime. Dalam pasal UU Nomor 19 Tahun 2016 mengenai Informasi dan Transaksi elektronik ("UU ITE") terkandung pada pasal 5 menyebutkan bahwa informasi elektronik atau dokumen elektronik merupakan alat bukti yang sah secara hukum di negara Indonesia [2]. Terkandung dalam pasal 6 informasi elektronik atau dokumen elektronik dianggap sah informasinya bila di dalamnya dapat diakses, ditampilkan, dijamin keutuhannya, dan dapat dipertanggungjawabkan sehingga menerangkan suatu keadaan [3].

Penelitian melakukan Forensik *Android* pada aplikasi pesan *Telegram*. *Smartphone* yang di gunakan ialah Samsung Galaxy K Zoom SM-C11 versi *Android* 4.1.1. Model penelitian ini, meliputi penggunaan *user* seperti install, login, memasukan/memperbaharui/menghapus kontak, pertukaran pesan, berbagi lokasi, serta penghapusan komunikasi. Tools yang digunakan memakai software SQLite Browser dan Hex Editor Neo v6.54.01.6478 untuk menganalisis file cache4.db yang jadikan bukti digital dan untuk *rooting device* menggunakan aplikasi Android Debug tool v1.32, Odin v3.09, ADB Fastboot v1.4.3, CF Auto Root, serta untuk menemukan file db menggunakan aplikasi Root Browser Classic v2.7.9.0.

1.2 Rumusan Masalah

Berdasarkan latar belakang di atas dapat di rumuskan permasalahan yang akan di selesaikan dalam Proyek Akhir ini adalah:

- a. Bagaimana menemukan bukti digital pada aplikasi *Telegram* di Android untuk memecahkan kasus terorisme?
- b. Bagaimana menganalisis, mempresentasikan barang bukti digital pada *Telegram* yang dapat membantu mendapatkan barang bukti digital dengan forensik Android?

1.3 Tujuan

Sesuai dengan permasalahan yang telah di rumuskan, maka tujuan dari Proyek Akhir ini untuk mengetahui:

- a. Menerapkan metode Android forensik dalam aplikasi *Telegram*, untuk mendapatkan barang bukti dari kasus terorisme.
- b. Melakukan langkah metode identifikasi serta mengumpulkan barang bukti digital, untuk dilakukan proses selanjutnya yaitu menganalisa barang bukti lalu mempresentasikan barang bukti.

1.4 Batasan Masalah

Berdasarkan identifikasi masalah yang telah di uraikan di atas, maka permasalahan dibatasi pada:

- a. Analisis yang di lakukan adalah pembacaan artefak *smartphone* sesuai dengan skenario kasus.
- b. Pengembalian / pemulihan (*recovery*) barang bukti digital berupa aktivitas pengguna aplikasi yang dicurigai.
- c. Media / *File user* yang dihapus tidak bisa di *recovery* kembali.
- d. Menggunakan tools forensik Android, Android Debug tool v1.32, SQLite Browser v3.8.0, Busybox v4.1, Root Browser Classic v2.7.9.0, Odin v3.09,

ADB Fastboot v1.4.3, CF Auto Root, Hex Editor Neo v6.54.01, Oxygen Forensic v12.

- e. *Smartphone* yang sudah di root terlebih dahulu sebelum dilakukan forensik

1.5 Definisi Operasional

Forensik perangkat mobile merupakan cabang dari forensik digital yang berkaitan dengan pemulihan bukti digital atau data dari perangkat mobile di bawah kondisi forensik. Perangkat selular biasanya mengacu pada ponsel, namun juga bisa berhubungan dengan perangkat digital yang memiliki memori internal baik dan kemampuan komunikasi, termasuk perangkat PDA, perangkat GPS dan komputer tablet [4].

Telegram adalah sebuah aplikasi pesan media sosial yang digunakan pengguna untuk mengirimkan sebuah percakapan rahasia dengan fitur yang tersedia seperti video, gambar, dll.

1.6 Metode Pengerjaan

Metode Forensik ini menggunakan metode NIST (*National Institute of Standards Technology*) dengan tahapan sebagai berikut:

- a. Identifikasi kasus masalah.
- b. Mengumpulkan alat atau bahan dan persiapan berdasarkan data yang di ambil.
- c. Melakukan analisis terhadap aktivitas *user* pada aplikasi *Telegram* tersebut.
- d. Pemecahan masalah terhadap kasus tersebut berdasarkan bukti digital aktivitas *user* yang didapatkan.
- e. Melakukan pengujian terhadap bukti digital yang didapatkan.
- f. Mempresentasikan hasil akhir data artefak berupa file .db yang tersimpan berbeda di direktori Android tersebut.

1.7 Jadwal Pengerjaan

Tabel 1.1 Jadwal Pengerjaan

Kegiatan dan Waktu Pelaksanaan	2021															
	Maret				April				Mei				Juni			
	1	2	3	4	1	2	3	4	1	2	3	4	1	2	3	4
Identifikasi		■	■	■												
Persiapan Alat dan Bahan				■	■	■										
Analisis								■	■	■						
Pemecahan Masalah										■	■					
Pengujian													■			
Presentasi	■	■	■	■	■	■	■	■	■	■	■	■			■	