BAB I
PENDAHULUAN

1.1 Latar Belakang Masalah

Perkembangan teknologi mendorong orang memanfaatkan teknologi untuk berbagai bidang kehidupan, termasuk cara berkomunikasi. Salah satu teknologi komunikasi yang semakin berkembang adalah penggunaan aplikasi *instant messenger* sebagai aplikasi bertukar pesan yang semakin banyak digunakan. Terdata pada Januari 2021 pengguna internet yang menggunakan *instant messenger* sebanyak 300 juta pengguna [1]. Salah satu aplikasi *instant messanger* adalah BiP *messenger*.

Aplikasi BiP *messenger* digunakan oleh pengguna untuk berkomunikasi dengan *voice* atau *video calling* secara *personal* maupun *broadcast messages* di grup. Aplikasi *instant messenger* ini dapat digunakan pada perangkat *mobile* atau komputer *desktop* atau laptop [2]. Aplikasi ini juga dapat digunakan oleh siber untuk melakukan tindak kejahatan.

RAM menyimpan data atau informasi sementara, dan aplikasi yang sedang berjalan di belakang layar, sehingga dimungkinkan pengguna lain dapat mengakses komputer melalui *remote device* dapat mengambil data yang terdapat di RAM. Dibutuhkan *skill* cukup baik untuk mampu melakukan *remote device* perangkat komputer *desktop* atau laptop, serta mengambil data atau informasi yang terdapat di RAM.

1.2 Rumusan Masalah

Permasalahan terkait penelitian ini dapat dirumuskan sebagai berikut:

a. Bagaimana cara menggunakan teknik *live forensics* pada aplikasi BiP *Messenger* untuk mendapatkan data komunikasi *user*?
b. Bukti digital apa saja yang dapat diperoleh dari RAM perangkat laptop tersangka menggunakan teknik *live forensics*?

1.3 Batasan Masalah

Batasan masalah akan difokuskan pada permasalahan yang diangkat, yaitu:

a. Menggunakan komputer laptop sebagai *attacker* untuk mendapatkan data di RAM perangkat komputer tersangka.
b. Menggunakan komputer laptop untuk melakukan analisis data dan menerapkan *live forensics*.
c. Menggunakan aplikasi BiP *messenger* versi 3.70.23 pada perangkat *smartphone* dan komputer.
d. Peneliti membuat skenario percakapan *user*, skenario serangan, dan pengumpulan data *digital forensics*.
e. Menggunakan 2 percobaan skenario yaitu percobaan 1 dengan penghapusan seluruh isi pesan (teks, gambar, dan video) dan percobaan 2 dengan melakukan penghapusan pada beberapa isi pesan teks.
f. Koneksi perangkat komputer *attacker* dengan perangkat *smartphone* target menggunakan *WiFi*.
g. Menggunakan *tools DumpIt* untuk pengambilan data digital. *WinHex* untuk analisa data digital.
h. Bukti digital yang didapat berupa data percakapan pada BiP *Messenger*.

1.4 Tujuan Penelitian

a. Membuktikan teknik pengambilan data pada RAM komputer tersangka (praktek *attacker*).
b. Melakukan teknik *live forensics* untuk memperoleh bukti adanya percakapan dengan menggunakan BiP *Messenger*.
c. Mendapatkan bukti digital dari perangkat pelaku.

1.5 Manfaat Penelitian

Manfaat yang dapat diberikan dari penelitian ini adalah:

a. Mencari bukti digital pada aplikasi BiP *messenger* dari aktivitas kejahatan digital dengan menggunakan teknik *live forensics* agar dapat dijadikan bukti digital pihak kepolisian untuk mengungkap kejahatan apa yang telah terjadi.

1.6 Sistematika Penulisan

Bagian skripsi yang berisi sistematika dengan pembagian bab yang akan diuraikan dalam skripsi secara menyeluruh, runtut dan dijelaskan dalam garis besar.

Bab I Pendahuluan

Bab ini berisi latar belakang, rumusan masalah, batasan masalah, tujuan penelitian, manfaat penelitian, dan sistematika penulisan.

Bab II Landasan Teori

Bab ini berisi referensi pendukung pada penelitian sebelumnya yang mendukung penulisan penelitian ini.

Bab III Metodologi Penelitian,

Bab ini berisi metode penelitian, masalah yang terdapat pada obyek, aplikasi yang dianalisis, solusi yang diusulkan, dan detail alat yang digunakan.

Bab IV Pembahasan

Bab ini berisi rancangan proyek, implementasi, analisis hasil akhir penelitian, dan pembahasan hasil penelitian.

Bab V Penutup

Bab ini berisi kesimpulan dari hasil akhir penilaian proyek, dan saran.