BAB V
PENUTUP

5.1 Kesimpulan

Berdasarkan keseluruhan proses implementasi, analisis, dan pembahasan yang telah dilakukan, dapat ditarik beberapa kesimpulan utama yang menjawab rumusan masalah penelitian:

A. Kerangka kerja NIST SP 800-86 terbukti menjadi metodologi yang sangat efektif dan dapat diimplementasikan secara sistematis untuk melakukan investigasi forensik digital pada aplikasi media sosial populer seperti WhatsApp dan TikTok di platform Android. Pendekatan empat fase yang terstruktur—Collection, Examination, Analysis, dan Reporting—memastikan bahwa setiap langkah investigasi berjalan secara metodis, terdokumentasi dengan baik, dan yang terpenting, mampu menjaga integritas barang bukti dari awal hingga akhir.

B. Investigasi pada kedua skenario kasus berhasil mengidentifikasi dan mengekstraksi artefak-artefak digital yang krusial untuk pembuktian.

   A. Untuk kasus penipuan lowongan kerja di WhatsApp, bukti kunci yang berhasil dipulihkan meliputi database pesan terdekripsi (msgstore.db) yang mengungkap komunikasi penipuan, file media (poster dan PDF) yang digunakan sebagai umpan, dan database kontak (wa.db) yang mengidentifikasi pelaku dan korban.

   B. Untuk kasus penipuan konten di TikTok, bukti kunci yang ditemukan mencakup file preferensi akun (aweme_user.xml) yang mengidentifikasi akun pelaku; database pesan langsung (userID_im.db) yang merekonstruksi interaksi dengan korban; dan fragmen video dari direktori cache (cachev2) yang membuktikan keberadaan konten penipuan meskipun telah dihapus dari profil.

C. Kombinasi perangkat lunak FTK Imager, Autopsy, dan WhatsApp Viewer merupakan sebuah toolset yang efektif, efisien, dan dapat diakses (karena bersifat freeware atau open-source). Toolset ini mampu menangani seluruh alur kerja forensik, mulai dari akuisisi data yang forensically sound, pemeriksaan mendalam terhadap sistem file, hingga analisis spesifik seperti dekripsi database, tanpa memerlukan pengembangan skrip kustom menggunakan Python. Hal ini menunjukkan bahwa investigasi yang andal dapat dilakukan oleh praktisi dengan berbagai tingkat keahlian teknis.

D. Integritas barang bukti digital berhasil dijaga dan diverifikasi secara konsisten di seluruh tahapan proses. Penggunaan fungsi hashing (MD5 dan SHA1) oleh FTK Imager pada saat akuisisi dan validasi ulang menggunakan Autopsy memastikan bahwa citra forensik yang dianalisis identik dengan data asli pada saat pengumpulan, yang merupakan prasyarat fundamental untuk admisibilitas bukti di persidangan.

5.2 Saran

Berdasarkan temuan dan pengalaman selama penelitian, berikut adalah beberapa saran yang ditujukan bagi praktisi di lapangan dan untuk pengembangan penelitian di masa depan.

Untuk Praktisi Forensik dan Penegak Hukum:

1. Sangat disarankan untuk mengadopsi kerangka kerja standar seperti NIST SP 800-86 sebagai Prosedur Operasional Standar (SOP) dalam setiap investigasi digital. Standarisasi ini akan meningkatkan kualitas, konsistensi, dan defensibilitas laporan forensik di mata hukum.

2. Investigator harus secara proaktif dan berkelanjutan memperbarui pengetahuan mereka mengenai struktur data dan lokasi artefak pada aplikasi media sosial yang populer. Aplikasi seperti WhatsApp dan TikTok sering melakukan pembaruan yang dapat mengubah lokasi atau format penyimpanan data. Pelatihan reguler sangat direkomendasikan.

3. Dalam menangani kasus yang melibatkan WhatsApp, prioritas utama harus diberikan pada upaya untuk mendapatkan akses root ke perangkat atau menggunakan metode ekstraksi file key dari perangkat non-root yang telah tervalidasi. Mengingat file key adalah titik kritis dalam proses dekripsi, keberhasilan atau kegagalan dalam memperolehnya akan sangat menentukan hasil investigasi.

.