BAB 5
PENUTUP

Kesimpulan

1. Dalam melakukan analisis forensik digital pada aplikasi desktop LINE Messenger pada sistem operasi Windows 10 untuk mendapatkan bukti terkait kasus penipuan online, langkah-langkah berikut dapat diikuti. Pertama, lakukan pengambilan salinan forensik dari sistem yang terlibat dalam kasus tersebut dengan metode yang sah. Selanjutnya, fokuskan pada analisis *volatile memory* (RAM) menggunakan alat forensik seperti WinHex. Gunakan *keyword* yang telah dijabarkan dalam tabel pada bab 4 sebagai atribut pencarian untuk mencari percakapan terkait penipuan online di dalam RAM. Selain itu, lakukan analisis disk VM menggunakan alat forensik seperti FTK Imager. Telusuri sisa/*cache* dari percakapan dalam bentuk file media yang ada di disk VM dan cari log aplikasi LINE untuk mendapatkan informasi aktivitas pengguna. Identifikasi file gambar dengan konten asli yang ditemukan dalam kasus tersebut dan periksa metadata serta atribut file untuk mengumpulkan informasi tambahan. Selanjutnya, rekonstruksi percakapan berdasarkan identifikasi pengirim, penerima, dan isi percakapan yang direkam dalam volatile memory. Perhatikan bahwa nomor telepon dan password akun telah dienkripsi oleh aplikasi LINE Messenger, menunjukkan tingkat keamanan yang kuat. Jika diperlukan, pertimbangkan langkah-langkah tambahan atau bantuan dari ahli yang memiliki keahlian khusus. Terakhir, dokumentasikan secara rinci temuan yang relevan, memastikan catatan dan dokumen tersebut memenuhi standar forensik dan dapat digunakan sebagai bukti dalam kasus penipuan online.

2. Dalam upaya menemukan bukti percakapan di *volatile memory*, penyelidik dapat menggunakan *keyword* yang spesifik dan menjadi atribut pada aplikasi LINE. Daftar *keyword* ini telah dijabarkan oleh penyelidik dalam tabel pada bab 4. Penggunaan keyword ini dapat membantu para penyelidik untuk menemukan artefak yang relevan dengan lebih cepat dan akurat. Salah satu keunikan dari percakapan di aplikasi LINE adalah bahwa percakapan akan direkam dalam volatile memory dengan menggunakan gabungan dari tiga identifikasi, yaitu identifikasi pengirim, penerima, dan isi percakapan. Dengan menggunakan identifikasi ini, pencarian percakapan menjadi lebih akurat sebagai bukti dalam kasus penipuan. Selain itu, identifikasi percakapan juga dapat menjadi acuan untuk menemukan timestamp dari percakapan tersebut. Pada disk VM, artefak yang ditemukan

meliputi sisa/cache dari percakapan yang berupa file media, termasuk file asli maupun yang telah dikompresi atau mengalami penyesuaian. Disk VM juga menyimpan log aplikasi LINE. Dalam proses pencarian bukti di *volatile memory*, alat bantu seperti WinHex dapat menjadi pilihan yang lebih efektif karena menggunakan algoritma pencarian yang lebih efisien daripada FTK Imager. FTK Imager akan melakukan pemindaian pada seluruh data terlebih dahulu, yang dapat memperlambat proses investigasi. Sementara itu, untuk pencarian bukti pada disk VM, FTK Imager merupakan pilihan yang lebih baik, karena penggunaan WinHex dapat terkendala dengan banyaknya folder sensitif yang tidak dapat diakses. *Volatile memory* menyimpan jumlah data yang signifikan yang dapat digunakan sebagai bukti dalam penelitian. Dari penjelasan di atas, terlihat bahwa semua percakapan hanya dapat ditemukan di *volatile memory*. Oleh karena itu, disarankan untuk melakukan penyelidikan langsung pada volatile memory menggunakan metode forensik guna memperoleh lebih banyak bukti yang relevan.

3. Berdasarkan hasil penelitian, terdapat perbedaan signifikan dalam tiga kasus yang dianalisis. Pada kasus pertama, ditemukan bahwa seluruh populasi data termasuk file gambar dengan konten asli yang tersimpan dalam disk VM. Selain itu, artefak berupa percakapan yang digunakan oleh tersangka dalam melakukan penipuan juga ditemukan secara lengkap. Percakapan tersebut disimpan dengan mencatat data pengirim, penerima, dan isi percakapan. Pada kasus kedua, terdapat beberapa percakapan yang tidak memiliki nilai identifikasi pengirim dan penerima, sehingga membuat penyelidik kesulitan dalam menentukan keabsahan percakapan sebagai bukti yang dapat digunakan. Selain itu, dalam kasus ini juga ditemukan sebagian file gambar dengan konten asli. Pada kasus pertama dan kedua, penyelidik berhasil memperoleh seluruh data yang ada di populasi, kecuali nomor telepon dan password akun. Hal ini mengindikasikan bahwa kedua artefak tersebut telah dienkripsi dengan baik oleh aplikasi LINE Messenger sehingga sulit ditemukan dengan mudah. Pada kasus ketiga, penyelidik hanya mampu menemukan media file berupa gambar yang tersisa. Sisanya, dalam kasus ketiga hanya terdapat log aplikasi LINE, termasuk saat pencopotan aplikasi.

Saran

1. Untuk kasus kedua, di mana beberapa percakapan tidak memiliki identifikasi pengirim dan penerima, disarankan untuk mempertimbangkan pendekatan alternatif yang dapat membantu dalam mengidentifikasi keaslian dan validitas percakapan tersebut. Penggunaan teknik analisis jaringan sosial atau pendekatan forensik lainnya yang mempertimbangkan konteks keseluruhan dapat membantu meningkatkan validitas bukti yang ditemukan.
2. Dalam kasus ketiga, di mana hanya file gambar dan log aplikasi LINE yang ditemukan, disarankan untuk mempertimbangkan metode analisis tambahan yang dapat membantu mengungkapkan bukti yang lebih signifikan. Penggunaan teknik steganografi atau rekuperasi data yang terhapus secara cermat dapat memperluas cakupan penelitian dan memperoleh bukti tambahan.
3. Dalam upaya menemukan bukti percakapan di volatile memory, disarankan untuk menggunakan keyword yang telah dijabarkan dalam tabel pada bab 4. Pemilihan keyword yang spesifik dan relevan akan membantu meningkatkan efisiensi dan akurasi pencarian artefak yang diinginkan.
4. Dalam proses pencarian bukti di volatile memory, disarankan untuk mempertimbangkan penggunaan alat bantu seperti WinHex yang menggunakan algoritma pencarian yang lebih efisien daripada FTK Imager. Ini akan mempercepat proses investigasi dengan menghindari pemindaian seluruh data.
5. Untuk pencarian bukti pada disk VM, disarankan menggunakan FTK Imager sebagai pilihan yang lebih baik daripada WinHex. Memperoleh akses ke folder-folder sensitif yang tidak dapat diakses dengan WinHex akan memungkinkan penemuan artefak yang lebih lengkap.