JISKa, Vol. 6, No. 1, JANUARI, 2021, Pp. 9 – 20
ISSN: 2527 – 5836 (print) | 2528 – 0074 (online)

Forensik *Mobile* pada Layanan Media Sosial LinkedIn

Imam Riadi [(1)], Anton Yudhana [(2)], Mush'ab Al Barra [(3)*]
[1] Sistem Informasi, Fakultas Sains dan Teknologi Terapan, Universitas Ahmad Dahlan, Yogyakarta
[2] Teknik Elektro, Fakultas Teknologi Industri, Universitas Ahmad Dahlan, Yogyakarta
[3] Teknik Informatika, Fakultas Teknologi Industri, Universitas Ahmad Dahlan, Yogyakarta
e-mail : imam.riadi@is.uad.ac.id, eyudhana@ee.uad.ac.id,
mushab1689048040@webmail.uad.ac.id.
* Penulis korespondensi.
Artikel ini diajukan 12 Mei 2020, direvisi 1 Juni 2020, diterima 1 Juni 2020, dan dipublikasikan 20 Januari 2021.

Abstract

The research explores mobile forensic on LinkedIn social media. Forensic mobile finds digital evidence of job hoax cases in LinkedIn, investigation using the NIST *(National Institute of Standard and Technology) method. Data collection techniques using Andriller tools in investigations. Data examination using tools Root Browser, Autopsy in the forensic process. data analysis using tools MOBILedit in the forensic process. The investigation found digital evidence of log activity, a status update on LinkedIn. Other results found in the investigation are 17 WiFi password, 117 download history, 263 phone calls, 1 file deleted, 1 file hidden, and 1 file raised, the research has reached the expected target.*

Keywords: Digital Forensic, Mobile Forensic, Social Media, LinkedIn, NIST

Abstrak

Penelitian membahas tentang forensik *mobile* di media sosial LinkedIn, forensik *mobile* menemukan bukti digital pada kasus *hoax* lowongan kerja LinkedIn, Investigasi menggunakan metode NIST *(National Institute of Standard and Technology)*. Teknik pengumpulan data menggunakan *tools* Andriller*,* diinvestigasi, pengujian data menggunakan *tools* Root Browser*,* Autopsy diproses forensik, Analisis data menggunakan *tools* MOBILedit diproses forensik. Investigasi menemukan bukti digital *log activity, status update* di LinkedIn. Hasil lain ditemukan pada investigasi adalah 17 *password* WiFi, 117 *download history*, 263 panggilan telepon, 1 *file* terhapus, 1 *file* disembunyikan dan 1 *file* dimunculkan, penelitian telah mencapai target yang diharapkan.

Kata Kunci: Forensik Digital, Forensik *Mobile*, Media Sosial, LinkedIn, NIST

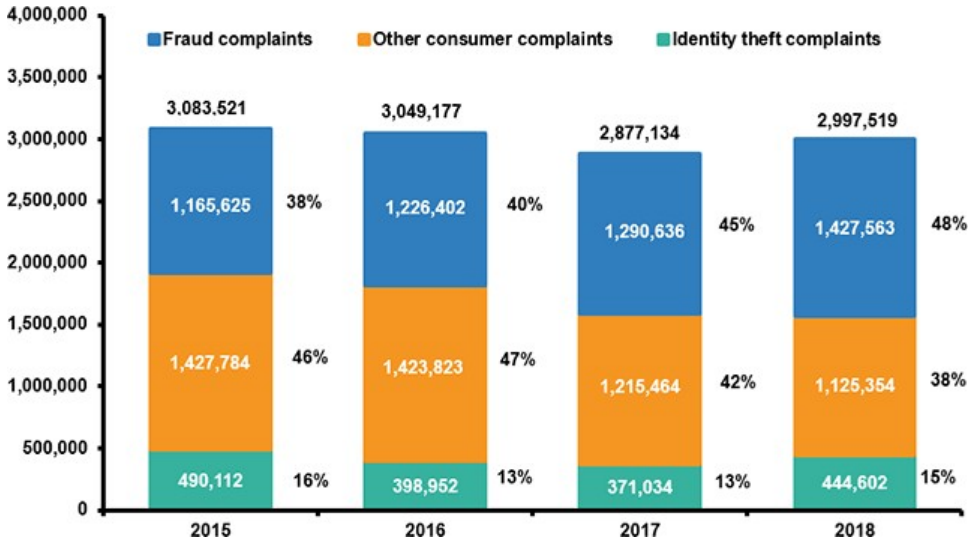
1. PENDAHULUAN

Majunya perkembangan teknologi informasi dan komunikasi berdampak pada seluruh lini kehidupan, di mana saat ini berdasarkan riset dari *We Are Social* 2017, Jumlah pengguna internet di dunia mencapai angka 3,8 milyar, dengan penetrasi 51% dari populasi penduduk dunia, pesatnya pertumbuhan pengguna internet tersebut selain berdampak pada majunya tingkat pertumbuhan di sektor jejaring sosial dan *e-commerce*.

Pesatnya perkembangan teknologi informasi mendorong majunya pertumbuhan pengguna jejaring sosial skala global, serta perkembangan perangkat *mobile device* yang terus berevolusi dari tahun ke tahun, seperti munculnya generasi Android yang terus *uptodate* mulai dari Android 1.0, 2.0, 3,0, 4,0, Lollipop, Jellybean, Marshmalllow, Kitkat, Oreo, hingga Android Pie dan Android R, evolusi dari Android tersebut berubah sesuai dengan kebutuhan akan kecepatan akses informasi serta *digital disruption* yang mempersingkat jarak, ruang dan waktu.

Majunya perkembangan teknologi tersebut juga berdampak pada sektor kejahatan dunia maya, atau yang populer dikenal dengan istilah *cybercrime,* mulai dari kasus *hoax*, penipuan *online*, pembobolan identitas, dan lain sebagainya. Penjabaran dari beberapa kasus kejahatan dunia

maya tersebut ditunjukan berdasarkan survei statistik *Insurance Information Institute*, sebagaimana grafik statistik dari tahun 2015 hingga 2018 yang terlihat pada Gambar 1.



Gambar 1. Statistik kejahatan *cyber* dalam skala global.

Teknik *static forensic* (NIST) dapat diterapkan dalam mengungkap kasus *hoax* di jejaring sosial, di mana *static forensic* memiliki beberapa tahapan yang harus dijalankan untuk menemukan bukti digital yang dapat dihadirkan di persidangan, tahapan tersebut yang pertama adalah, *collection* yang bertujuan mengumpulkan bukti bukti digital, kedua adalah *examination* yaitu menelusuri data yang tersembunyi atau data yang telah dihapus, ketiga adalah *analysis* yaitu melakukan penyelidikan terhadap bukti-bukti yang telah ditemukan, keempat adalah menyusun secara mendetail hasil penyelidikan dalam sebuah bentuk laporan. *Tools* yang digunakan dalam menjalankan investigasi adalah MOBILedit, Andriller, Root Browser, dan Autopsy.

Skenario investigasi yang dijalankan yaitu penyelidikan laporan kasus *hoax* dari korban yang menjadi target kejahatan, pengumpulan *sample* berupa akun LinkedIn dan ponsel pelaku, berikutnya adalah penyusunan laporan penemuan bukti digital yang telah memenuhi *standard* investigasi *static forensic* (NIST) untuk dihadirkan di persidangan. Bukti digital tersebut sangat menentukan berjalannya proses persidangan secara obyektif berdasarkan bukti digital yang telah diproses sesuai standar investigasi *static forensic* (NIST).

Rumusan masalahnya yaitu: bagaimana melakukan analisa forensik *mobile* terhadap ponsel Android serta akun LinkedIn menggunakan teknik *static forensic*; bagaimana melakukan investigasi pada ponsel Android serta akun LinkedIn menggunakan metode NIST; bagaimana melakukan analisa forensik *mobile* terhadap ponsel Android serta akun LinkedIn menggunakan tools MOBILedit, Andriller, Root Browser, Autopsy untuk menemukan bukti digital.

Tujuan dari penelitian ini adalah menambah wawasan dan keterampilan di bidang forensik digital yang diperlukan dalam menjawab rumusan masalah di atas, salah satunya forensik digital pada aplikasi *mobile* atau forensik *mobile,* kontribusinya berkaitan dengan bertambahnya wawasan dan keterampilan di bidang forensik *mobile*.

Cybercrime adalah perbuatan melanggar hukum dengan menggunakan teknologi komputer yang memanfaatkan kecanggihan perkembangan teknologi internet. *Cybercrime* adalah istilah yang mengacu pada aktivitas kriminal dengan komputer atau jaringan komputer untuk dijadikan alat, sasaran, atau tempat kejadian perkara. *Cybercrime* terbagi menjadi berbagai jenis kejahatan yaitu penipuan lelang *online*, cek pemalsuan, penipuan kredit/kartu, penipuan kepercayaan, penipuan identitas, pornografi. *Cybercrime* dapat terjadi di semua perangkat elektronik, seperti *smartphone* Android (Riadi, Yudhana, et al., 2018).

LinkedIn adalah jaringan profesional terbesar di dunia di internet. Anda dapat menggunakan LinkedIn untuk menemukan pekerjaan atau magang yang tepat, menghubungkan dan memperkuat hubungan profesional, dan mempelajari keterampilan yang Anda butuhkan untuk sukses dalam karier Anda. Anda dapat mengakses LinkedIn dari desktop, aplikasi seluler LinkedIn, pengalaman web seluler, atau aplikasi seluler Android LinkedIn Lite (LinkedIn, 2020).

Android adalah sebuah sistem operasi *open source* berbasis Linux, Android telah dikembangkan oleh Google sebagai sistem operasi terbuka yang memberikan kebebasan bagi pengembang perangkat keras dan operator seluler untuk mengembangkan aplikasi dan sistem operasinya. Android mendorong pengembang untuk membangun sejumlah besar aplikasi dan mengunggahnya ke Pasar Android. Aplikasi tersebut dapat digunakan oleh pengguna dengan mengunduhnya dari Android Market, lalu melakukan instalasi pada *smartphone* (Tamma et al., 2020).

Andriller merupakan salah satu *software* yang dapat digunakan untuk tujuan analisis forensik pada *smartphone*. Ini aplikasi adalah aplikasi lintas platform yang beroperasi Microsoft Windows dan Ubuntu Linux. Andriller memiliki kemampuan untuk melakukan analisis non-destruktif di Android perangkat, seperti: mengekstrak dan mendekode data secara otomatis, membuka kunci pola layar kunci, mengangkat Data SMS dan MMS, dan *database* aplikasi. Andriller juga dapat menghasilkan laporan dalam format HTML dan Excel (Karen Kent, et,al).

MOBILedit Forensic merupakan *tool* forensik yang memungkinkan penyidik untuk memperoleh secara logik, mencari dan memeriksa perangkat ponsel. *Tool* ini menggunakan beberapa mekanisme konektivitas terutama konektivitas nirkabel dibandingkan *tool* sejenis. Software ini cukup baik digunakan untuk memperoleh informasi sistem telepon dan informasi lainnya seperti daftar kontak dan pesan (Nasirudin et al., 2020; Novrianda et al., 2014)

“Forensik digital adalah cabang ilmu baru yang berasal dari sinonim kata forensik komputer, definisinya telah diperluas untuk mencakup semua teknologi digital, sedangkan forensik komputer didefinisikan sebagai kumpulan teknik dan alat yang digunakan untuk menemukan bukti dalam komputer” (Kävrestad, 2018). Begitupun Raharjo (2013) menyebutkan bahwa forensik digital merupakan bagian dari ilmu forensik yang melingkupi penemuan dan investigasi materi (data) yang ditemukan pada perangkat digital.

Budiman (2001), dalam tugas akhirnya berkesimpulan, dalam digital *forensic*, Metode yang banyak digunakan adalah *search*, *seizure* dan pencarian informasi. Search dan seizure merupakan metode yang paling banyak digunakan, sedangkan pencarian informasi (*information search*) sebagai pelengkap data bukti tersebut.

Mobile forensics merupakan ilmu turunan dari ilmu pengetahuan *digital forensics* atau yang lebih dikenal sebagai komputer forensik. *Digital forensics* merupakan metode ilmiah yang mempelajari tentang cara pemeliharaan, pengumpulan, validasi, analisis, interprestasi, dokumentasi dan presentasi bukti digital yang bersala dari sumber-sumber digital untuk tujuan menfasilitasi rekontruksi peristiwa pidana atau membantu untuk mengantisipasi tindakan yang terbukti melanggar prosedur yang telah ditentukan (Riadi, Umar, & Nasrulloh, 2018). Atau bisa dikatakan *mobile forensic* merupakan ilmu yang melakukan proses *recovery* bukti digital dari perangkat *mobile* menggunakan cara yang sesuai dengan *forensic* (Madiyanto et al., 2017).

“Bukti digital adalah data-data yang dikumpulkan dari semua jenis penyimpanan digital yang menjadi subjek pemeriksaan forensik komputer. Dengan demikian segala sesuatu yang membawa informasi digital dapat menjadi subjek penelitian, dan setiap pembawa informasi yang ditargetkan untuk pemeriksaan harus diperlakukan sebagai bukti” (Kävrestad, 2018).

bukti digital adalah data yang disimpan atau dikirimkan menggunakan komputer yang dapat mendukung atau menyangkal sebuah pelanggaran tertentu, atau bisa juga disebut sebagai petunjuk yang mengarahkan kepada elemen-elemen penting yang berkaitan dengan sebuah pelanggaran (Riadi, Umar, et al., 2018; Wahyudi, 2016).

2. METODE PENELITIAN

Penelitian ini menggunakan tahapan forensik *(National Institute of Standard and Technology)* NIST (Kunang & Khristian, 2016). sebagaimana dijelaskan pada Gambar 2.

Gambar 2. Tahapan forensik NIST.

Gambar 2 menunjukkan fase dari NIST *(National Institute of Standard and Technology)* yang menjadi metodologi dasar dari proses forensik digital pada *smartphone*. Metode forensik NIST *(National Institute of Standard and Technology),* terbagi menjadi empat tahapan yaitu pengumpulan, pemeriksaan, analisis, dan presentasi (Yudhana et al., 2018).

2.1. Pengumpulan *(Collection)*

Pengumpulan (*collection*) yaitu meneliti bahan investigasi untuk menemukan bukti-bukti digital yang berkaitan dengan penyelidikan. Media digital yang dapat dijadikan sebagai barang bukti adalah sistem operasi Android, media penyimpanan misal aplikasi jejaring sosial LinkedIn*,* SIM *card,* Google Drive*, e-mail, handphone,* SMS*, log file browsing history*, dsb.

2.2. Pemeriksaan *(Examination)*

Pemeriksaan (*examination*) yaitu menelusuri data yang tersembunyi atau data terhapus dengan menggunakan *software*, contohnya Root Browser*,* Autopsy.

2.3. Analisis *(Analysis)*

Analisis (*analysis*) yaitu melakukan penyelidikan terhadap bukti-bukti yang telah ditemukan. Analisis ini dapat dilakukan pada data data sebagai berikut: alamat *url* yang telah dikunjungi, pesan *e-mail*, dokumen, *file* yang dihapus atau diformat, *password, hidden file, log event viewers* dan *log* aplikasi, dsb.

2.4. Presentasi *(Presentation)*

Presentasi (*presentation*) yaitu menjabarkan secara mendetail laporan hasil penyelidikan dengan bukti-bukti yang sudah diproses secara mendalam dan dapat dipertanggungjawabkan secara ilmiah di peradilan, laporan tersebut memuat hasil hasil forensik yang dibutuhkan seperti *log activity, screenshot* bukti digital dari *status update* pelaku, untuk penjabaran pada laporan atau *reporting* disusun sesuai kebutuhan di persidangan, tidak perlu menyusun *reporting* yang mendetail dari proses *collection* hingga *analysis* dalam penyusunan laporan. Proses penelitian memerlukan beberapa alat dan bahan sebagaimana dijelaskan pada Tabel 1.

Tabel 1. Alat dan Bahan Penelitian.

No	Alat dan Bahan Penelitian	Keterangan
1	Ponsel Samsung Galaxy SM J111F	Bahan
2	*Memory Card*	Bahan
3	Laptop	Alat
4	*Card Reader*	Alat
5	*Software* Autopsy	Alat
6	*Software* Andriller *(trial)*	Alat
7	Root Browser *Apps*	Alat
8	*Software* MOBILedit (berbayar)	Alat

Tabel 1 merupakan penjabaran dari alat dan bahan yang dibutuhkan dalam investigasi atau proses forensik, alat dan bahan tersebut terbagi menjadi dua yaitu alat dan bahan yang

digunakan untuk melakukan investigasi seperti *software* Autopsy, Andriller, Root Browser yang digunakan untuk memproses bahan menjadi bukti digital, sesuai prosedur forensik statik NIST.

3. HASIL DAN PEMBAHASAN

3.1. Pengumpulan *(Collection)*

Pengumpulan alat bukti berupa ponsel Samsung Galaxy SM-J111F, Sebagaimana gambar *smartphone device* berikut.

Gambar 3. Samsung Galaxy SM-J111F.

Spesifikasi *device* ponsel *Samsung Galaxy SM-J111F* dapat dilihat pada Tabel 2, informasi spesifikasi *device* bermanfaat bagi investigator untuk mengetahui rekam jejak aktivitas pada ponsel yang digunakan pelaku kejahatan. Mengumpulkan data *smartphone* sangat penting untuk dilakukan dengan tujuan mengetahui informasi IMEI, dan sebagainya.

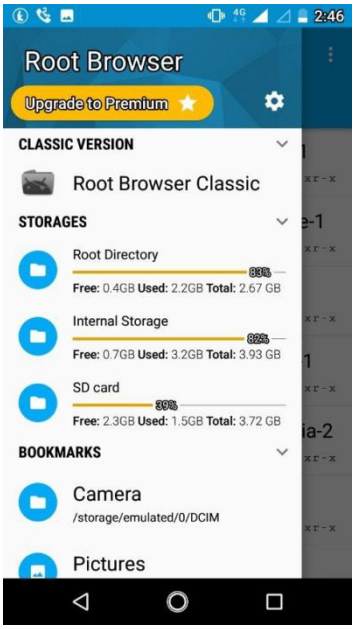
Tabel 2. Informasi *Device*.

ADB *serial*	420091eab46ec400
Shell permissions	shell
Manufacturer	SAMSUNG
Model	SM-J111F
IMEI	Unknown
Android version	5.1.1
Build name	
WiFi MAC	c0:87:eb:e3:2b:cd
Local time	2019-03-04 17:29:07
Android time	SE Standard Asia time
Account	com.google:mushab2017@gmail.com com.google:mushab2024@gmail.com com.google:mushab2019@gmail.com com.google:satuwebnetwork@gmail.com
System	WiFi password(17)
System	Android Download History(117)
Communication data	Samsung Call Logs (263)

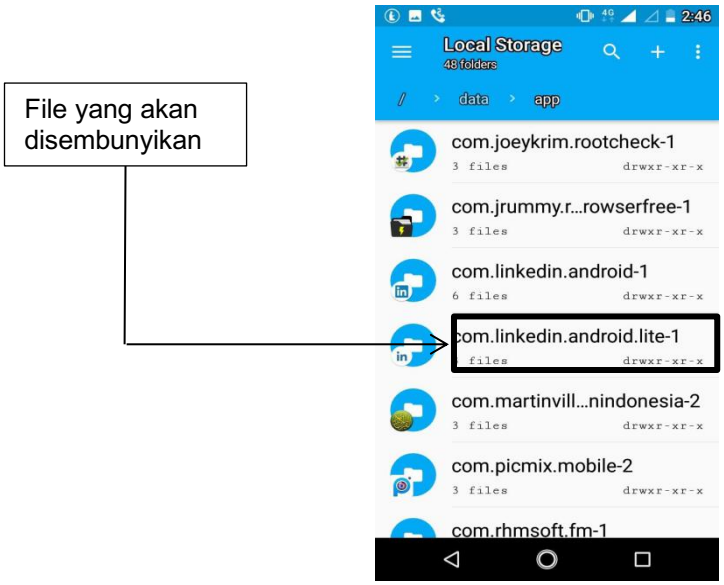
Tabel 2, hasil ekstraksi Andriller, tampak spesifikasi mesin ponsel yaitu ADB *serial, manufacture, model,* IMEI, Android *version, build name,* WiFi MAC, *local time,* Android *time, account,* WiFi *password,* Android *Download History, Communication data* berupa *log* panggilan telepon pada ponsel Android.

3.2. *Examination* dengan Root Browser *Apps*

Tools untuk menyembunyikan dan menampilkan data yang disembunyikan menggunakan aplikasi Root Browser, aplikasi Android ini memiliki versi tidak berbayar, selain juga memiliki layanan premium dengan fitur yang lebih lengkap, aplikasi ini dapat diunduh di Google Play Store, antarmuka Root Browser bisa dilihat pada Gambar 4.



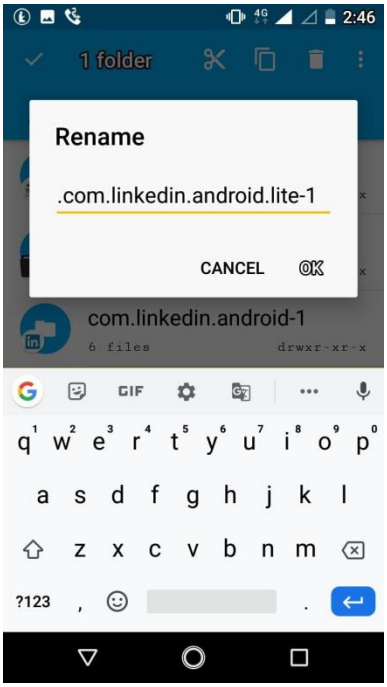
Gambar 4. Root Browser *apps.*



Gambar 5. *Folder* dan aplikasi LinkedIn.

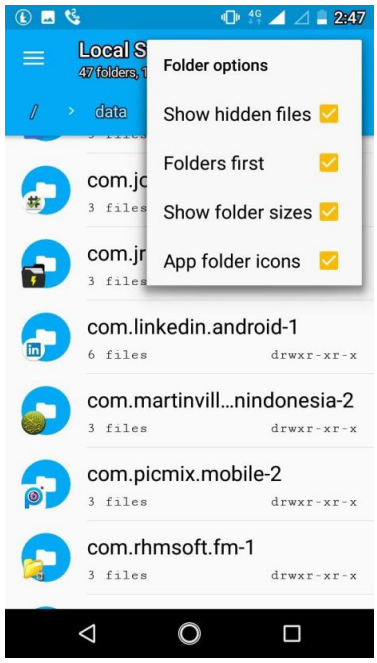
Pada Gambar 5 Root Browser dapat menyembunyikan dan menampilkan *file* tersembunyi meskipun *file* tersebut berada di lokasi *root folder* pada lapisan *file system* Android.

Langkah pertama menyembunyikan data adalah memilih *folder* yang akan disembunyikan dan me-*rename folder* dengan Root Browser sebagaimana tampak pada Gambar 6.



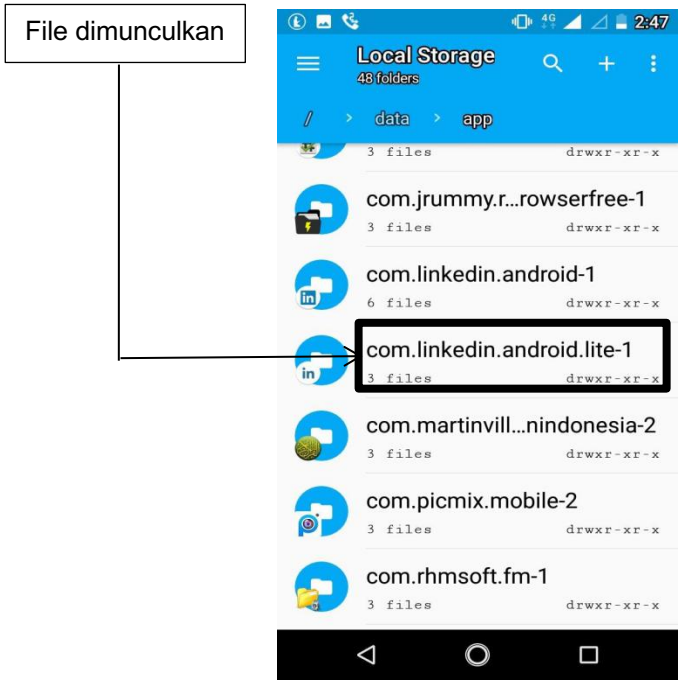
Gambar 6. Menyembunyikan *file* dengan me-*rename folder*.

Gambar 6 menjelaskan bahwa memberikan satu titik di depan nama *folder* akan menyembunyikan *folder* tersebut di dalam direktori *root* di Android. Untuk menampilkan kembali *folder* yang disembunyikan dengan Root Browser dapat dilihat pada Gambar 7.



Gambar 7. Memunculkan *file* tersembunyi.

Pada gambar 7 *file* dimunculkan kembali dengan memilih option *show hidden files* pada menu *folder option*.

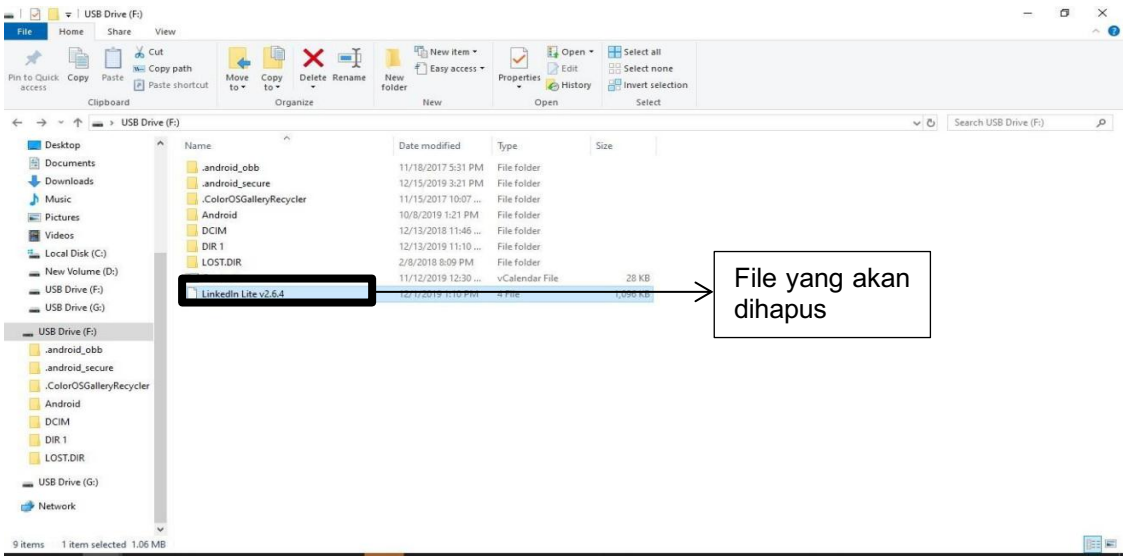


Gambar 8. *Folder* muncul kembali.

Root Browser dapat memunculkan file yang disembunyikan dengan sangat mudah tanpa harus menginstall software atau aplikasi lainnya yang berbayar. Gambar 8 menjelaskan tentang cara menampilkan data tersembunyi dengan Root Browser.

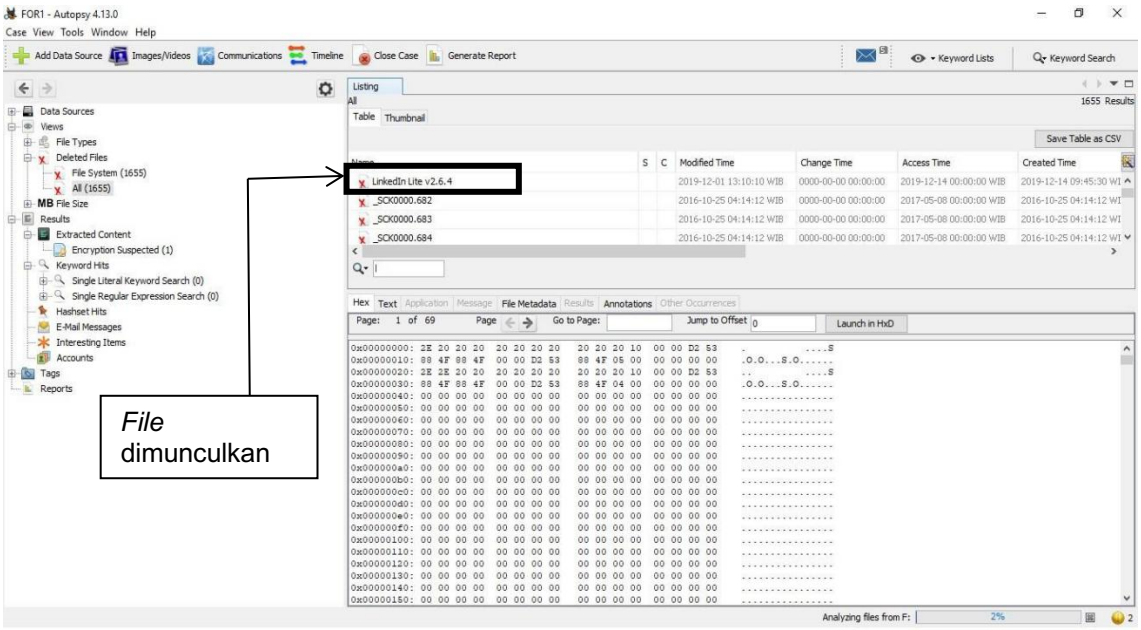
3.2.1. *Examination* Kedua dengan Autopsy

Menampilkan data yang terhapus dengan Autopsy, yaitu dengan mem-*backup* terlebih dahulu aplikasi LinkedIn dari ponsel pada *memory card* atau *flashdisk* maupun media penyimpanan eksternal lainnya.



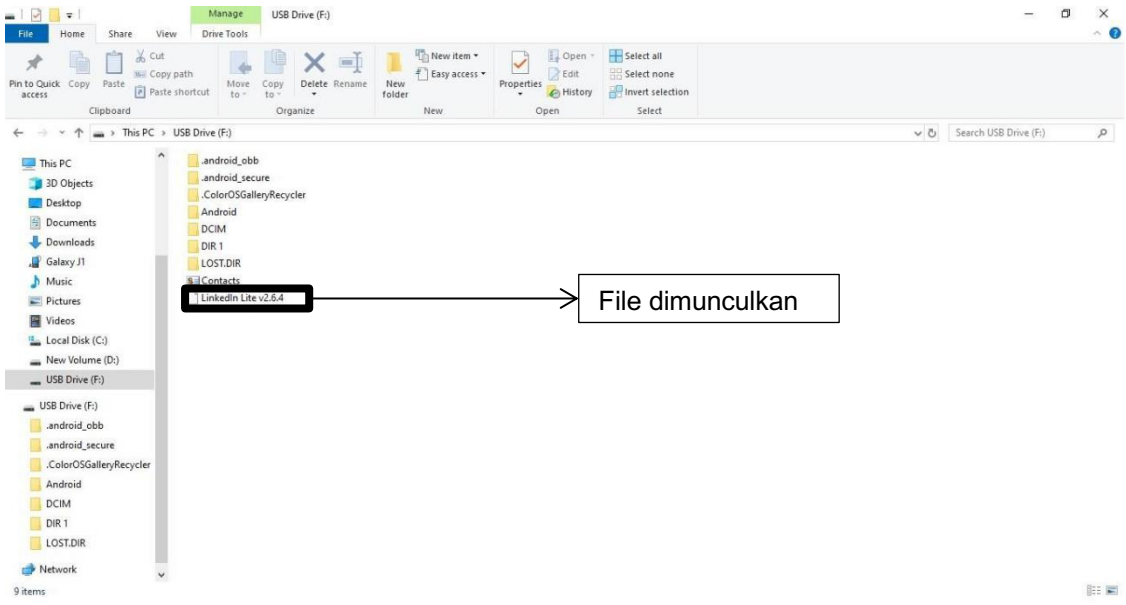
Gambar 9. Aplikasi LinkedIn pada *Micro SD*.

Gambar 9 merupakan *file* LinkedIn yang tersimpan pada *micro SD* Android, *file* tersebut akan dihapus untuk dimunculkan kembali dengan Autopsy.



Gambar 10. Hasil *recovery deleted file*.

Gambar 10 merupakan hasil temuan *file* terhapus dari aplikasi LinkedIn pada *micro SD*, data ekstraksi tersebut dapat dimunculkan kembali pada *micro SD*.

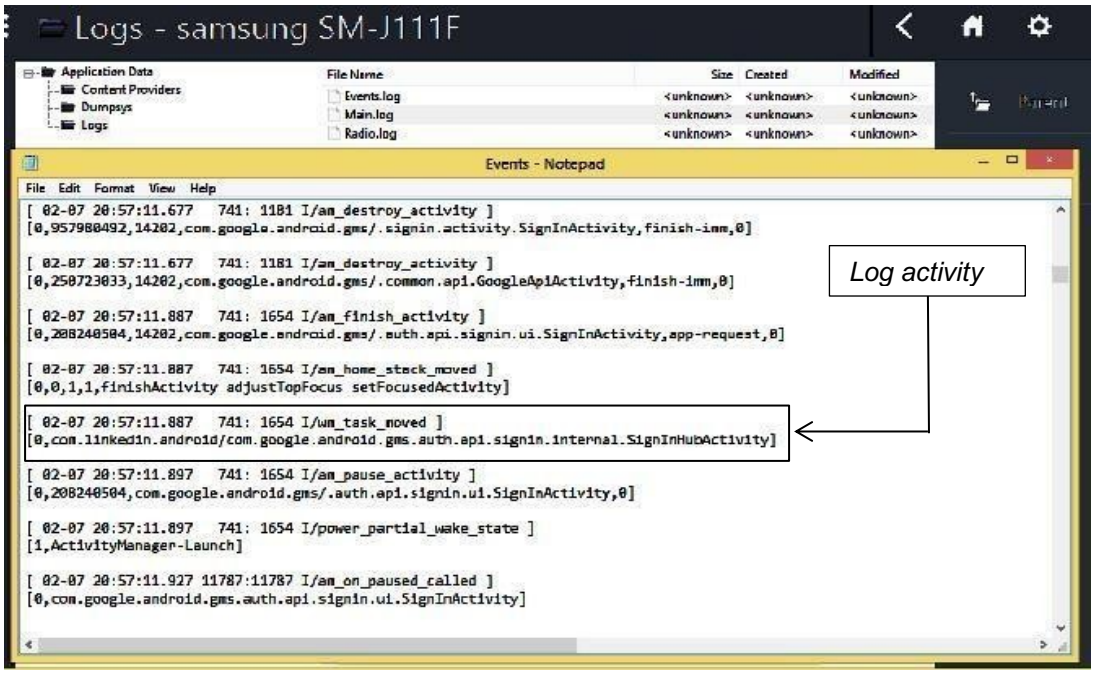


Gambar 11. Pemulihan *file* terhapus.

Gambar 11 menunjukkan *file* yang dimunculkan kembali pada media penyimpanan.

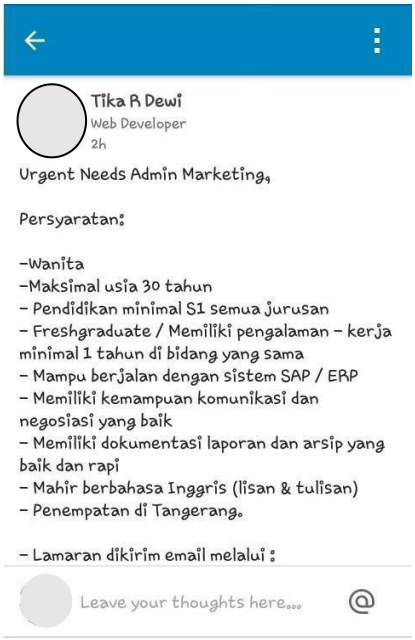
3.3. *Analysis* dengan MOBILedit

Pada tahap pengumpulan data, telah ditelusuri satu jenis aktivitas yang terpantau oleh MOBILedit, di mana data hasil ekstraksi *log activity*, menunjukkan informasi bahwa pelaku *log*in ke akun LinkedIn pada tanggal 07 Februari 2019, pukul 20:57: WIB.



Gambar 12. *File log* aktivitas.

Gambar 12 menunjukkan peristiwa *login* pada akun LinkedIn. Ditemukan juga sebuah cuitan *hoax* pada aplikasi LinkedIn yang digunakan pelaku, di mana pelaku membagikan *hoax* mengenai informasi lowongan kerja pada Gambar 13.



Gambar 13. Cuitan *hoax*.

Gambar 13 merupakan sebuah temuan mengenai cuitan *hoax* yang dibuat oleh tersangka pada waktu kejadian, cuitan ini dapat dijadikan alat bukti *digital* untuk dihadirkan di persidangan.

3.4. Presentasi (*Presentation*)

Menjabarkan secara mendetail laporan hasil penyelidikan dengan bukti-bukti yang sudah diproses secara mendalam dan dapat dipertanggungjawabkan secara ilmiah di hadapan pihak yang berwenang.

Presentation *(reporting)* adalah sebuah proses menyiapkan dan melaporkan informasi hasil temuan dari fase analysis. Faktor yang mempengaruhi laporan termasuk penjelasan alternatif, pertimbangan partisipan, dan informasi aktual (Umar et al., 2018).

Reporting, yaitu melaporkan hasil analisis yang mencakup uraian tindakan yang diambil, penjelasan alat dan prosedur yang dipilih, penentuan tindakan lain yang perlu dilakukan (misalnya, pemeriksaan forensik dari sumber data tambahan, mengamankan identifikasi, atau meningkatkan kontrol keamanan), dan memberikan rekomendasi untuk menyempurnakan aturan, prosedur, alat, dan aspek lain dari proses forensik (Riadi et al., 2017).

Beberapa hal penting yang dicantumkan dalam presentasi adalah: tanggal dan waktu terjadinya pelanggaran, yaitu 07 Februari 2019, pukul 20:57 WIB; permasalahan yang terjadi adalah penyebaran *hoax*; waktu analisa laporan; teknik yang digunakan yaitu investigasi *static forensic.*

Presentation merupakan sebuah ringkasan *conclusion* akhir, dari empat tahapan proses. Pada tahap ini dilakukan penyusunan laporan dari proses forensik yang sudah dijalankan serta hasil temuan dari alat dan bahan bukti yang telah menjadi digital. Laporan tersebut akan digunakan oleh pihak yang berwenang, hakim atau jaksa untuk menjatuhkan dakwaan terhadap pelaku kejahatan siber. Contoh format *presentation* dapat dilihat pada Tabel 3.

Tabel 3. Presentasi Forensik

No	Perkara	Keterangan
1	Tanggal dan waktu terjadinya pelanggaran	07 Februari 2019, Pukul 20:57 WIB.
2	Permasalahan yang terjadi	Penyebaran *Hoax*
3	Waktu analisa laporan	14 Februari 2019
4	Ditemukannya bukti digital, berupa *log* aktivitas, dan *status update*	Sebuah cuitan *hoax*, serta *log* aktivitas *smartphone*
5	Teknik yang digunakan	Investigasi *static forensic*

Tabel 4. Perbandingan Hasil 4 *Tools* Forensik.

No	*Tools* Forensik	Hasil Temuan
1	Andriller	*Password* WiFi, riwayat akses, informasi *device*
2	Root Browser	*File* tersembunyi
3	Autopsy	*Recovery deleted* LinkedIn *apps*

4. KESIMPULAN

Penelitian menggunakan *sample* ponsel Android dan akun LinkedIn. Proses investigasi menggunakan 4 *tools* dengan teknik *static forensic* dan telah ditemukan bukti digital. Hasil forensik telah menemukan bukti digital berupa *log activity dan status update.* Hasil lain yang telah ditemukan dalam investigasi adalah 17 *password WiFi*, 117 *download history*, 263 panggilan telepon, 1 *file* terhapus, 1 *file* disembunyikan dan 1 *file* dimunculkan. *Tools* Andriller telah menemukan spesifikasi, rekam jejak komunikasi data di ponsel Android. MOBILedit menemukan *log activity* di investigasi. Autopsy memunculkan *file* terhapus di ponsel. Root Browser memunculkan *file* tersembunyi diproses forensik. Berdasarkan hasil pengujian yang didapatkan, penelitian ini telah sesuai dengan tujuan yang diharapkan.

DAFTAR PUSTAKA

Budiman, R. (2001). Computer Forensic : Apa dan Bagaimana? In *Fakultas Teknik Elektro dan Informatika*.

Kävrestad, J. (2018). *Fundamentals of digital forensics: Theory, methods, and real-life applications*. Springer Nature Switzerland. https://doi.org/10.1007/978-3-319-96319-8

Kunang, Y. N., & Khristian, A. (2016). Implementasi Prosedur Forensik untuk Analisis Artefak Whatsapp pada Ponsel Android. *Prosiding ANNUAL RESEARCH SEMINAR*, *2*(1), 64–73.

LinkedIn. (2020). *What is LinkedIn and How Can I Use It?* LinkedIn. https://www.linkedin.com/help/linkedin/answer/111663/what-is-linkedin-and-how-can-i-use-it-?lang=en

Madiyanto, S., Mubarok, H., & Widiyasono, N. (2017). Proses Investigasi Mobile Forensics Pada Smartphone Berbasis IOS. *Jurnal Rekayasa Sistem & Industri (JRSI)*, *4*(1), 93–98. https://doi.org/10.25124/jrsi.v4i01.149

Nasirudin, N., Sunardi, S., & Riadi, I. (2020). Analisis Forensik Smartphone Android Menggunakan Metode NIST dan Tool MOBILedit Forensic Express. *Jurnal Informatika Universitas Pamulang*, *5*(1), 89–94. https://doi.org/10.32493/informatika.v5i1.4578

Novrianda, R., Kunang, Y. N., & Shaksono, P. H. (2014). Analisis Forensik Malware Pada Platform Android. *Konferensi Nasional Ilmu Komputer (KONIK)*, 377–385.

Raharjo, B. (2013). SEKILAS MENGENAI FORENSIK DIGITAL. *Jurnal Sosioteknologi*, *12*(29), 384–387. https://doi.org/10.5614/sostek.itbj.2013.12.29.3

Riadi, I., Umar, R., & Firdonsyah, A. (2017). Identification Of Digital Evidence On Android's Blackberry Messenger Using NIST Mobile Forensic Method. *International Journal of Computer Science and Information Security*, *15*(5), 155–160.

Riadi, I., Umar, R., & Nasrulloh, I. M. (2018). ANALISIS FORENSIK DIGITAL PADA FROZEN SOLID STATE DRIVE DENGAN METODE NATIONAL INSTITUTE OF JUSTICE (NIJ). *ELINVO (Electronics, Informatics, and Vocational Education)*, *3*(1), 70–82. https://doi.org/10.21831/elinvo.v3i1.19308

Riadi, I., Yudhana, A., & Putra, M. C. F. (2018). Forensic Tool Comparison on Instagram Digital Evidence Based on Android with The NIST Method. *Scientific Journal of Informatics*, *5*(2), 235–247. https://doi.org/10.15294/sji.v5i2.16545

Tamma, R., Skulkin, O., Mahalik, H., & Bommisetty, S. (2020). *Practical Mobile Forensics* (4th ed.). Packt Publishing.

Umar, R., Yudhana, A., & Nur Faiz, M. (2018). Experimental Analysis of Web Browser Sessions Using Live Forensics Method. *International Journal of Electrical and Computer Engineering (IJECE)*, *8*(5), 2951–2958. https://doi.org/10.11591/ijece.v8i5.pp2951-2958

Wahyudi, E. (2016). *Bukti Digital*.

Yudhana, A., Riadi, I., & Anshori, I. (2018). Analisis Bukti Digital Facebook Messenger Menggunakan Metode Nist. *IT Journal Research and Development*, *3*(1), 13–21. https://doi.org/10.25299/itjrd.2018.vol3(1).1658