Analisis Forensik Recovery pada Smartphone Android Menggunakan Metode National Institute Of Justice (NIJ)

Imam Riadi[1], Sunardi[2], Sahiruddin[*3]
[1]Program Studi Sistem Informasi, Universitas Ahmad Dahlan
[2]Program Studi Teknik Elektro, Universitas Ahmad Dahlan
[*3]Program Studi Teknik Informatika, Universitas Ahmad Dahlan
e-mail: [1]imam.riadi@is.uad.ac.id, [2]sunardi@mti.uad.ac.id,
[*3]sahiruddinbuton@gmail.com

Abstrak

keberadaan smartphone saat ini dianggap sangat membantu aktifitas manusia dalam melakukan pekerjaan sehari- hari. Berkembangnya fitur-fitur yang ada pada smartphone memudahkan para penggunanya beraktifitas seperti melakukan pekerjaan kantor, bisnis, e-banking, dan untuk berinteraksi dengan pengguna lain di media sosial. Perkembangan smartphone tidak hanya memberikan dampak positif tetapi bisa berdampak negatif ketika perkembangan tersebut dimanfaatkan untuk melakukan tindakan kejahatan. Saat ini terdapat banyak kasus penghapusan barang bukti kejahatan yang dilakukan oleh tersangka untuk mengilangkan bukti kejahatan yang dilakukan oleh seorang pelaku. Hal ini menjadi tantangan bagi forensika teknologi informasi dan penegak hukum melakukan penyelidikan secara forensik terhadap smartphone dari tersangka dalam sebuah kasus kejahatan untuk mendapatkan kembali bukti digital yang akan dijadikan sebagai barang bukti dalam sebuah persidangan. Penelitian ini menggunakan tools MOBILedit Forensic, Wondershare dr. Fone for Android, dan Belkasoft Evidence Center untuk memperoleh bukti digital serta menggunakan metode National Institute of Justice (NIJ) yaitu dengan mengidentifikasi, mengusulkan solusi, melakukan uji solusi yang ditawarkan, mengevaluasi dan melaporkan hasil. Dari hasil pengujian tool forensik yang peneliti gunakan, tool MOBILedit Forensic tidak bisa mengembalikan data yang sudah dihapus, tool Wondershare dr. Fone For Android berhasil mengembalikan data kontak, log panggilan,dan pesan yang sudah dihapus, sementara tool Belkasoft Evidence Center hanya bisa mengembalikan data kontak, dan log panggilan yang sudah dihapus.

Kata kunci*— Forensik, Recovery, Smartphone, Android, NIJ.*

1. PENDAHULUAN

Perangkat seluler mengalami perkembangan yang sangat pesat seiring dengan perkembangan teknologi. [1]. Perkembangan teknologi tidak hanya membawa dampak positif tetapi juga memiliki dampak negatif. perkembangan teknologi memilki sisi negatif.. salah satu dampak negatif yang dimaksud adalah ketika perkembangan teknologo dimanfaatkan untuk suatu tindakan kejahatan yang melanggar hukum. Salah satu bentuk teknologi yang perkembangannya dapat langsung dinikmati dan diaplikasikan dalam kehidupan sehari-hari adalah telepon genggam (*smartphone*).

Handphone mengalami perkembangan teknologi yang sangat signifikan yang mana dahulu hanya digunakan untuk berkomunikasi via suara maupun pesan singkat (*Short Message Service*), handphone kini telah berkembang dengan fitur-

fitur yang disesuaikan dengan perkembangan zaman dan kebutuhan dari penggunanya. bahkan dapat dibilang keberadaan *smartphone* esangat membantu aktifitas penggunanya untuk melakukan pekerjaan kantor, bisnis, *e-banking*, maupun berinteraksi dengan pengguna lain di media sosial seperti *Facebook*, *Twitter, Path, Blackberry Messenger*, *Instagram*, dan lain sebagainya[2]. *Smartphone* secara perlahan mulai menggantikan peran komputer dengan meningkatkan jumlah fitur dan aplikasi yang tersedia pada perangkat seluler [1]. *Smartphone* berbasis android termasuk salah satu jenis *smartphone* yang paling diminati dan memiliki banyak pengguna [3].

Dampak negatif dari perkembangan *smartphone* terhadap penggunanya adalah berkaitan dengan Pencurian dan penghapusan data untuk menghilangkan bukti kejahatan yang dilakukan oleh pelaku. Bukti digital ini dapat berupa data yang ada pada *smartphone* seperti data kontak, log panggilan, pesan, video, gambar dan file dokumen yang akan dijadikan sebagai bukti kejahatan dalam persidangan [4].

Hal ini menjadi tantangan bagi Forensika teknologi informasi dan penegak hukum untuk melakukan penyelidikan terhadap barang bukti dari tersangka dalam kasus kejahatan karena bukti digital yang akan dijadikan sebagai barang telah dihapus oleh pelaku sehingga untuk mendapatkan kembali bukti digital, Forensika teknologi informasi dan penegak hukum dituntut untuk melakukan analisis forensik recovery data dalam mengembalikan data yang telah dihapus tersebut. Pengambilan barang bukti digital pada penelitian ini yaitu dengan menggunakan metode yang dikembangkan oleh *National Institute of Justice* (NIJ) [5][6]. Penelitian ini diharapkan dapat memberikan gambaran umum bagaimana proses forensik yang dapat dilakukan untuk mengembalikan data yang hilang atau terhapus pada *smartphone* android.

2. METODE PENELITIAN

2.1 Digital Forensik

Digital Forensik atau Forensika Digital adalah penerapan ilmu pengetahuan dan teknologi komputer yang digunakan untuk kepentingan bukti hukum (*pro justice*), yang dalam hal ini adalah untuk membuktikan kejahaatan-kejahatan yang menggunakan teknologi tinggi atau komputer secara alamiah agar dapat memanfaatkan bukti digital untuk melawan pelaku kejahatan. [7]. Digital forensik memiliki banyak bidang, salah satunya adalah *Mobile* Forensik [8]. Digital Forensik pada intinya adalah dapat menemukan bukti digital yang biasa tersimpan pada penyimpanan komputer sementara, penyimpanan permanen, USB, CD, lalu lintas jaringan, dan lainya [8].

2.2 Mobile Forensik

Mobile Forensik adalah ilmu yang melakukan proses pemulihan bukti digital dari perangkat seluler menggunakan cara yang sesuai dengan kondisi dan metode forensik [9]. Penggunaan mobile seperti *smartphone* dengan berbagai macam tipe dan *system* operasi untuk kejahatan sudah semakin tinggi jumlahnya, tetapi dengan adanya forensik untuk perangkat mobile dapat membantu mengatasi kasus kejahatan yang berhubungan dengan perangkat *mobile* khususnya *smartphone* [10]. *Mobile* forensik dibutuhkan karena layanan berbasis *mobile* semakin meningkat dan penggunanya semakin banyak dengan semakin populernya komputasi *dan mobile commerce*, kebutuhan akan transaksi *mobile* juga semakin tinggi. Kualitas dan kecepatan penyedia layanan *mobile* harus sebanding dengan transaksi *mobile* yang terjadi. Tantangan transaksi *mobile* terletak pada jumlah transaksi *mobile* yang terjadi, yang terletak pada sejumlah besar penyedia layanan *mobile* dengan jaringan berkecepatan tinggi dan aman. Transaksi *online* yang dilakukan dengan menggunakan perangkat

mobile harus memiliki keamanan yang tinggi dan melindungi pengguna dari penyalahgunaan orang-orang yang tidak bertanggung jawab [11].

2.3 MOBILedit Forensik

MOBILedit Forensik adalah suatu software yang berfungsi untuk penyelidikan atau pengambilan data pada *smartphone*. *Software* ini dapat membaca pesan, catatan panggilan, membaca SIM *card* dan lain sebagainya. Versi *lite* MOBILedit dapat di-*download* dari internet. Instalasi MOBILedit tidaklah terlampau sulit. Seperti juga Oxygen, MOBILedit membutuhkan kondisi USB *debugging mode enabled* di ponsel. Ponsel dapat terkoneksi baik menggunakan kabel langsung maupun menggunakan koneksi *wireless*. Hal ini memberikan keuntungan untuk jenis ponsel yang tidak dapat didetekesi menggunakan software ini dapat diutilisasi menggunakan koneksi wireless. MOBILedit akan menginstal aplikasi kecil di ponsel untuk menarik data. Data yang diekstrak dibatasi hanya *contacts*, *call lists, messages* dan file.

2.4 Wondershare dr. Fone for Android

Wondershare dr. Fone for Android merupakan salah satu aplikasi komputer yang berfungsi untuk mengembalikan data yang terhapus atau terformat secara tidak sengaja pada perangkat *smartphone* android. Wondeshare adalah aplikasi terbaik untuk mengembalikan data yang terhapus berupa pesan, kontak, log panggilan, foto, video, audio, dan dokumen. Penggunaan aplikasi Wondershare sangatlah mudah karena pengguna dapat lansung menginstal pada PC atau laptop. Aplikasi Wondershare ini juga dapat gunakan di semua sistem operasi seperti windows xp,7,8 bahkan yang terbaru adalah windows 10.

2.5 Belkasoft Evidence Center

Situs resmi, www.Belkasoft.com, memberikan informasi bahwa Belkasoft Evidence Center merupakan salah satu perangkat lunak yang direkomendasikan para praktisi Forensika digital untuk digunakan karena memiliki kemampuan untuk memperoleh, mencari, menganalisis, menyimpan berbagai bukti digital yang ditemukan, baik didalam komputer maupun perangkat *mobile*. Belkasoft mampu melakukan ekstraksi bukti digital dari berbagai sumber dengan menganalisis *hard drive, drive image cloud, memory dumps, iOS, Blackberry*, android dan berbagai jenis *platform* lain. Belkasoft akan secara otomatis menganalisis sumber data dan memberikan artefak yang paling penting yang dapat digunakan penyidik untuk meninjau, memeriksa menganalisis atau membuat sebuah laporan.

2.6 Metode Penelitian

Metode penelitian yang digunakan berdasarkan pedoman forensik perangkat mobile yang dibuat oleh *National Institute of Justice* (NIJ) dengan langkah-langkah sebagai berikut :

1. Identifikasi

   Peneliti mengidentifikasi masalah dan mengumpulkan informasi tentang masalah yang akan dihadapi.

2. Solusi

   peneliti Mengajukan solusi yang mungkin untuk dilakukan dalam pemecahan masalah dari hasil identifikasi masalah dan informasi dari hasil tahap pertama.

3. Uji coba

   Setelah mendapatkan solusi yang mungkin di lakukan dari tahap kedua, peneliti kemudian melakukan uji coba terhadap *smartphone* dari setiap solusi yang mungkin dilakukan untuk pemecahan masalah.

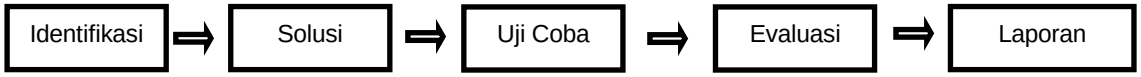
4. Evaluasi

   Melakukan evaluasi dari hasil yang di dapat dari hasil uji coba yang dilakukan dari setiap solusi agar di lakukan untuk pemecahan masalah

5. Laporan

Tahap ini adalah tahap untuk menyelesaikan prosedur dari setiap langkah yang telah di lakukan pada tahapan sebelumnya untuk melaporkan hasil yang di dapat dari pemecahan masalah.

Metode penelitian yang digunakan berdasarkan pedoman forensik perangkat *mobile* yang dikembangkan oleh *National Institute of Justice* (NIJ) dapat dilihat pada Gambar 1.



Gambar 1. Pedoman forensik perangkat *mobile* yang dikembangkan oleh NIJ

3. HASIL DAN PEMBAHASAN

Penelitian yang dilakukan dengan sebuah simulasi kasus pada *smartphone* seseorang yang mengalami kehilangan data berupa data pesan, history panggilan, kontak, gambar, video dan file dokumen yang telah dihapus. Pada simulasi kasus ini, peneliti menggunakan sebuah *smartphone* dengan merek Samsung Galaxy J5.

3.1. Identifikasi

Identifikasi merupakan tahapan paling awal dalam metode NIJ *Mobile* Forensik. Proses yang dlakukan pada tahap ini diantaranya adalah melakukan identifikasi permasalahan yang akan diselesaikan. Permasalahan dalam penelitian ini adalah bagaimana proses forensik untuk mengembalikan data yang telah dihapus pada *smartphone* yang dijadikan sebagai barang bukti.

Setelah dilakukan identifikasi permasalahan yang dihadapi, peneliti akan melakukan pendokumentasian dengan mencatat merek, model, spesifikasi, dan hal lain yang berkaitan dengan *smartphone* tersebut. Gambar 2 merupakan gambar *smartphone* yang menjadi barang bukti.

Gambar 2. *Smartphone* yang menjadi barang bukti

3.2. Solusi

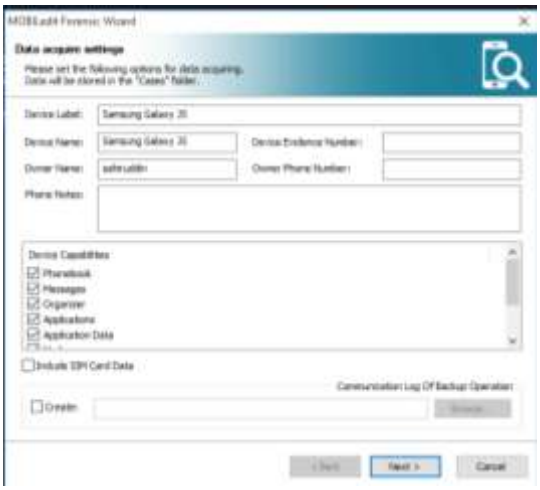
Tahap selanjutnya adalah tahap dimana peneliti mengajukan solusi yang dilakukan untuk pemecahan masalah dari hasil identifikasi masalah dan informasi hasil tahap pertama. Tahap ini peneliti mengajukan solusi untuk mengembalikan data yang telah dihapus dengan menggunakan 3 *tool* forensik yaitu MOBILedit forensics, Wondershare dr. Fone for Android, dan Belkasoft Evidence Center

3.3. Uji Coba

Tahap Uji Coba merupakan tahapan percobaan *tool* forensik untuk mendapatkan bukti digital yang digunakan sebagai pemecahan masalah yang dihadapi. Proses uji *tool* forensik pada penelitian ini adalah sebagai berikut :

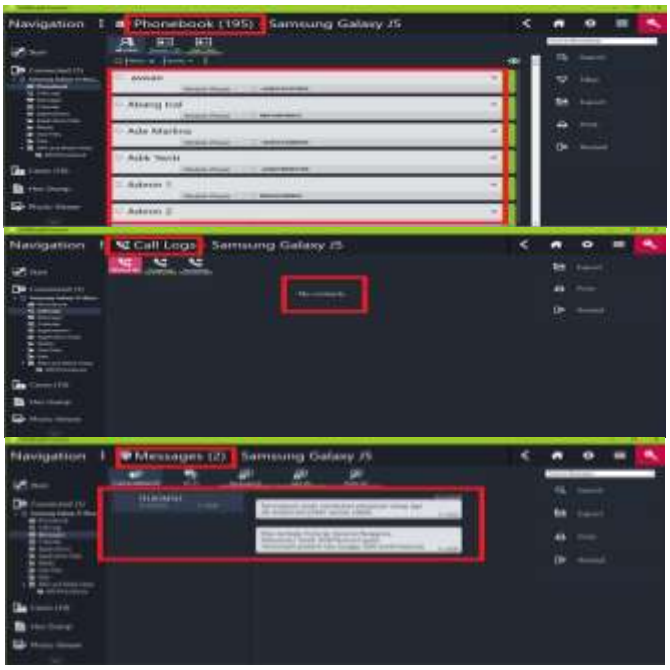
3.3.1 Uji Coba dengan MOBILedit

Tool pertama yang digunakan pada tahap uji coba adalah dengan MOBILedit. Proses ekstraksi data menggunakan MOBILedit sangat mudah yaitu *smartphone* harus terkoneksi dengan PC atau laptop tempat *tool* MOBILedit di-install. Gambar 3 menunjukkan *smartphone* telah terkoneksi oleh MOBILedit.



Gambar 3. Tampilan *Smartphone* yang sudah terkoneksi dengan MOBILedit

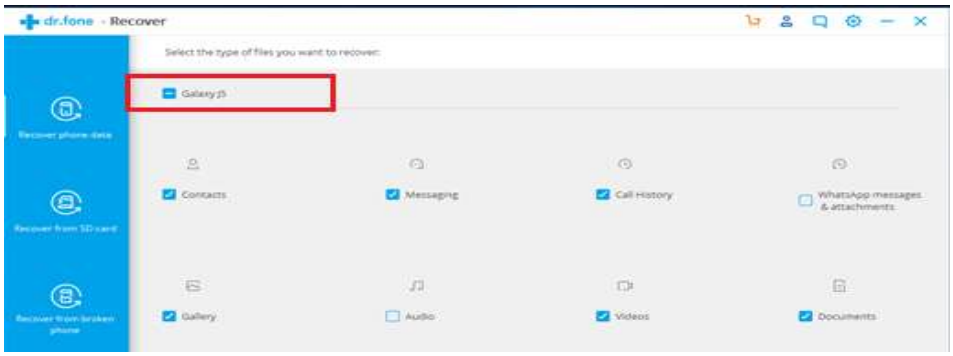
Setelah *smartphone* terkoneksi dengan MOBILedit, peneliti selanjutnya akan melakukan proses ekstraksi data untuk mengembalikan data yang ada pada perangkat smarphone android yang dijadikan sebagai barang bukti untuk mengungkap kasus kejahatan.. Pada proses ekstraksi dengan MOBILedit, data yang terhapus tidak dapat dikembalikan, MOBILedit hanya dapat menampilkan data yang ada pada *smartphone* berupa data kontak, log panggilan dan pesan. Tampilan hasil ekstraksi oleh MOBILedit ditunjukan gambar 4.



Gambar 4. Tampilan hasil ekstraksi oleh MOBILedit

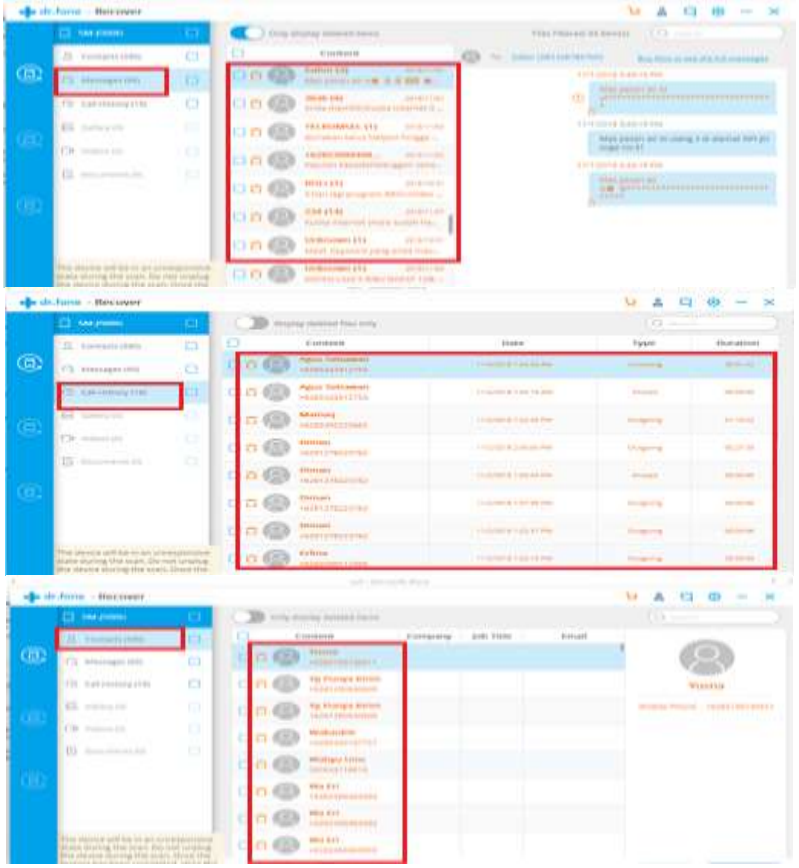
3.3.2 Uji Coba dengan Wondershare

Tool forensik berikutnya yang digunakan pada penelitian ini yaitu Wondershare dr. Fone for Android. Penggunaan Wondeshare juga membutuhkan koneksi komputer atau laptop tempat Wondershare di-*install*. Gambar 5 menunjukan smatphone telah terkoneksi oleh Wondershare.



Gambar 5. *smartphone* terkoneksi oleh Wondershare

Setelah *smartphone* terkoneksi oleh Wondeshare, langka selanjutnya adalah proses ekstraksi data. Berbeda dengan MOBILedit, ekstraksi dengan Wondershare memperoleh hasil yang sangat signifikan yaitu dapat mengembalikan data yang telah dihapus berupa data kontak, log panggilan dan pesan pada perangkat *smartphone* android. Hasil ekstraksi oleh Wondeshare dapat dilihat pada gambar 6.



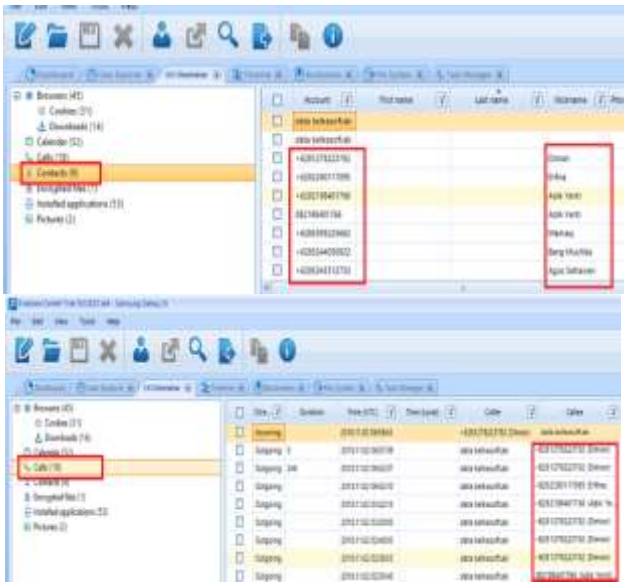
Gambar 6. Tampilan hasil ekstraksi oleh Wondershare

3.3.3 Uji Coba dengan Belkasoft

Tool ketiga yang digunakan pada penelitian ini yaitu dengan Belkasoft Evidence Center. Proses ekstraksi ini sama dengan proses ekstraksi dengan MOBILedit dan Wondershare yaitu *smartphone* terlebih dahulu harus terneksi dengan PC atau laptop yang telah terinstal oleh Belkasoft. Gambar 7 adalah tampilan *smartphone* yang sudah terhubung dengan Belkasoft.

Gambar 7. *Smartphone* telah terkoneksi oleh Belkasoft

Setelah *smartphone* terhubung dengan Belkasoft, selanjutnya adalah proses ekstraksi data. Belkasoft dapat mengembalikan data yang telah dihapus berupa data kontak, dan log panggilan. Tampilan hasil ekstraksi data oleh Belkasoft dapat ditunjukkan gambar 8.



Gambar 8. Tampilan hasil ekstraksi data oleh Belkasoft

3.3.4 Evaluasi

Pada tahap ini peneliti akan mengevaluasi data yang sudah diperoleh dan menyimpulkan hasil uji coba dari setiap *tool* yang digunakan. Tabel hasil evaluasi dapat dilihat pada Tabel 1.

Tabel 1. Hasil Evaluasi

Hasil Ekstraksi pada Samsung Galaxy J5					
Tool	Pesan	History Panggilan	Kontak	Gambar	Video
MOBILedit Forensic	2	0	195	0	0

Wondershare dr. Fone for Android	95	19	590	0	0
Belkasoft Evidence Center	0	19	9	0	0

Pada Tabel 1 Wondershare berhasil Mengembalikan data yang sudah di hapus berupa data pesan, history panggilan, dan kontak, Belkasoft hanya dapat mengembalikan data terhapus berupa history panggilan, dan kontak, sementara *tool* MOBILedit tidak dapat mengembalikan data yang telah dihapus. MOBILedit Forensic hanya dapat menampilkna data yang belum terhapus di *smartphone* android.

3.3.5 Laporan

Tahap ini merupakan tahap hasil evaluasi, yang mencakup metodologi forensik yang dilakukan, teknik, dan *tool* yang digunakan, ada atau tidaknya tindakan, pedoman, prosedur, perangkat, dan aspek lain yang sekiranya diringkasan mengenai barang bukti dan prosedur forensikyang dilakukan serta perbandingan *tool* forensik yang digunakan. Informasi perangkat yang akan dilaporkan yaitu sebuah *smartphone* berbasis android dengan rincian merk : Samsung, Model : J5, Nomor Model : SM-J500G, OS : Android, Versi OS : 5.1 Lollipop. Data terhapus yang akan dikembalikan yaitu data kontak, log panggilan, pesan, gambar dan video, dan *tool* yang digunakan adalah MOBILedit, Wondershare, dan Belkasoft. Tabel 2 merupakan perbandingan hasil ekstraksi dari masing-masing *tool.*

Tabel 2. Perbandingan Hasil Ekstraksi Data

Data Yang Berhasil Dikembalikan				
No	Jenis Data	Perangkat Lunak		
		MOBILedit Forensics	Wondershare dr. Fone for Android	Belkasoft Evidence Center
1.	Kontak	x	√	√
2.	Log Panggilan	x	√	√
3.	Pesan	x	√	x
4.	Gambar	x	x	x
5.	Video	x	x	x

Berdasarkan tabel 2 diatas, maka dapat dilihat bahwa setiap *tool* memiliki kemampuan yang berbeda-beda. Pada *tool* Wondershare, data yang telah dihapus berhasil dikembalikan berupa data kontak, pesan dan log panggilan, Belkasoft berhasil dikembalikan data terhapus berupa history panggilan dan kontak, sementara MOBILedit tidak dapat mengembalikan data yang telah dihapus.

4. KESIMPULAN

Hasil yang didapatkan dari proses penelitian mengenai analisis forensik recovery pada *smartphone* android menggunakan metode national institute of justice (NIJ), memberikan kesimpulan sebagai berikut :

1. Data yang telah dihapus pada perangkat *smartphone* android masih dapat dikembalikan menggunakan *tool* Wondershare dan Bekasoft.
2. *Tool* forensik yang digunakan tidak cukup baik untuk mengembalikan data gambar, video dan file dokumen.

3. Wondershare dan Belkasoft dapat menggembalikan data yang telah dihapus berupa data kontak, log panggilan, dan pesan, sedangkan *tool* MOBILedit hanya dapat menampilkan data pada perangkat *smartphone* tetapi tidak dapat mngembalikan data yang terhapus.

DAFTAR PUSTAKA

[1] Z. M. Guntur , U. Rusyidi and R. Imam , "Analisis Forensil Aplikasi Instant Messaging Berbasis Android," in Annual Research Seminar (ARS), Palembang, 2017.

[2] Alamsyah, M. Zanial and Rasmila, "Analisis Forensik Recovery Dengan Keamanan Kode Password Pada Smartphone Android," in Student Colloquium Sistem Informasi & Teknik Informatika (SC-SITI), Palembang, 2014.

[3] F. Arizona, R. Imam and Sunardi, "Analisis Forensik Bukti Digital Blackberry Messenger Pada Android," in Cyber Learning & IT Computer Karawang (CLICK), Karawang, 2016.

[4] Sahiruddin, R. Imam and Sunardi, "Data Recovery Dengan Keamanan Fingerprint Pada Smartphone Android," in SENDI-U 2018, Semarang, 2018.

[5] R. Imam , Y. Anton and C. Muhammad , "Akuisisi Bukti Digital Pada Instragram Messenger Berbasis Android Menggunakan Metode National Institute Of Justice (NIJ)," Jurnal Teknik Informatika dan Sistem Informasi (JUTISI), vol. 4, pp. 219-227, 2018.

[6] "National Instiurte Of Justice (NIJ) Digital Evidence and Forensics," 2016. [Online]. Available: www.nij.gov.

[7] "National Instiurte Of Justice (NIJ) Digital Evidence and Forensics," 2016. [Online]. Available: www.nij.gov.

[8] R. Imam , U. Rusyidi and F. Arizona, "Identification Of Digital Evidence On Android's Blackberry Messenger Using NIST Mobile Forensic Method," International Journal of Computer Science and Information Security (IJSSIC), vol. 15, pp. 155-160, 2017.

[9] R. Imam, Sunardi and F. Arizona , "Forensic Investigation Technique On Android's Blackberry Messenger Using NIST Framework," International Journal of Cyber-Security and Digital Forensics (IJCSDF), vol. 4, pp. 198-205, 2017.

[10] F. N. Muhammad , U. Rusyidi and Y. Anton, "Analisis Live Forensik untuk Perbandingan Keamanan Email Pada Sistem Operasi Propietary," Jurnal Ilmiah ILKOM, vol. 8, pp. 242-247, 2016.

[11] A. Nuril, R. Imam and L. Ahmad, "Forensik SIM Card Cloning Using Authentication Algoritm," *International Journal of Electronics and Information Engineering 4,* pp. 71-81, 2016.