CyberSecurity dan Forensik Digital e-ISSN: 2615-8442
Vol. 6, No. 2, November 2023, hlm. 54-61

Perbandingan Hasil Recovery Tools Mobile Forensic Di Smartphone Android Menggunakan Metode National Institute Of Justice (NIJ)

Muhammad Fadil Fadillah[1], Trihastuti Yuniati[2]

[1,2]Fakultas Informatika, Institut Teknologi Telkom Purwokerto
Email: 16102202@ittelkom-pwt.ac.id[1], trihastuti@ittelkom-pwt.ac.id[2]

Abstrak

Penggunaan *smartphone* di Indonesia mencapai 192,15 juta pengguna aktif pada tahun 2022, menjadikannya pasar terbesar keempat di dunia. Namun, pertumbuhan ini juga berdampak pada meningkatnya tindak kejahatan siber, tercatat sebanyak 8,831 kasus selama tahun tersebut. Penelitian tentang efektivitas alat pemulihan *mobile forensic* pada *smartphone* Android dapat menjadi acuan pemilihan alat uji *mobile forensic* baik untuk kebutuhan penyelidikan maupun akademis. Pada penelitian ini dilakukan pengujian terhadap dua *tools mobile forensic*, yaitu Andriller yang merupakan aplikasi *open source*, dan MOBILedit Forensic Express Pro yang merupakan aplikasi berbayar, untuk mengetahui seberapa tingkat *recovery* yang mampu dilakukan oleh kedua *tools* tersebut. Penelitian dengan metode *National Institute of Justice* (NIJ) menemukan bahwa kedua *software* yang digunakan dapat digunakan untuk analisis *mobile forensic* tanpa akses *root* ke *smartphone*. Hasil pengujian menunjukkan MOBILedit Forensic Express Pro memiliki tingkat pemulihan data yang lebih tinggi (83,33%) dibandingkan dengan Andriller (50%). Dari hasil ini diharapkan dapat membantu dalam memilih alat atau *software mobile forensic* dalam proses penyelidikan maupun kebutuhan akademis.

Kata kunci: *digital forensik, mobile forensic, national institute of justice*

Comparison Of Mobile Forensic Recovery Tools Results On Android Smartphones Using The National Institute Of Justice (NIJ) Method

Abstract

The usage of smartphones in Indonesia reached 192.15 million active users in 2022, making it the fourth largest market in the world. However, this growth has also led to an increase in cybercrime, with 8,831 cases reported during that year. A research on the effectiveness of mobile forensic recovery tools on Android smartphones, can be a reference for selecting mobile forensic testing tools for both investigative and academic needs. In this research, two mobile forensic tools were tested, namely Andriller, which is an open source application, and MOBILedit Forensic Express Pro, which is a paid application, to find out what level of recovery these two tools are capable of. Research using the National Institute of Justice (NIJ) method found that the two software used can be used for mobile forensic analysis without root access to a smartphone. The test results indicated that MOBILedit Forensic Express Pro achieved a higher data recovery rate (83.33%) compared to Andriller (50%). These findings are expected to aid in selecting suitable mobile forensic tools for investigative and academic purposes.

Keywords*: digital forensik, mobile forensic, national institute of justice*

1. PENDAHULUAN

Menurut data Badan Pusat Statistik (BPS) pada tahun 2022, 67,88% penduduk Indonesia yang berumurur 5 tahun ke atas sudah memiliki *handphone* (AHDIAT, 2023). Dengan kenaikan jumlah pengguna tersebut, Indonesia menjadi negara dengan penggunaan *smartphone* terbanyak keempat dengan jumlah 192,15 juta pengguna *smartphone* aktif di dalam negeri sepanjang tahun 2022 (Sadya, 2023).

Jumlah pengguna *smartphone* yang semakin meningkat setiap tahunnya tidak luput dari perkembangan *smartphone* sendiri yang kini makin memiliki banyak fitur dan fungsi yang ringkas untuk digunakan sesuai dengan kebutuhan setiap hari. *Smartphone* dengan sistem operasi android menjadi salah satu *smartphone* dengan pengguna terbanyak di Indonesia, dengan jumlah hingga 86% dari total pengguna *smartphone* di indonesia (Anon., 2023). Perkembangan pesat *smartphone* tidak selamanya membawa dampak positif, pekembangan tersebut juga berpengaruh ke dampak negatif dimana *smartphone* banyak digunakan sebagai alat untuk melakukan suatu tindak kriminal seperti penipuan, transaksi barang ilegal, dan masih banyak lagi tindak kriminal yang dilakukan secara *online*.

Kejahatan pada dunia IT atau IT crime merujuk pada suatu tindakan kejahatan atau kegiatan ilegal dengan menggunakan komputer sebagai alat maupun sebagai target. *Cyber crime* juga didefinikasi sebagai sebuah tindakan kriminal yang menggunakan komputer atau jaringan komputer sebagai media

untuk melakukan tindak kejahatan (Clough, 2015). Tindak kriminal yang terjadi secara *online* meningkat lebih banyak dari tahun ke tahun dengan berbagai jenis tindak kriminal yang terjadi seperti peretasan sistem elektronik, gangguan sistem, manipulasi data, dan lain-lain. Tindak kriminal pada dunia internet juga banyak menyasar kepada para pengguna *smartphone*, tindak kriminal seperti *cyber bullying*, judi *online*, pencemaran nama baik, transaksi ilegal, dan penipuan menjadi marak terjadi di kalangan masyarakat. Hal tersebut terjadi karena makin mudahnya akses terhadapat berbagai informasi. Sebanyak 8.831 kasus terkait tindak kriminal secara siber tercatat sejak 1 januari hingga desember pada tahun 2022 (Anon., 2022).

Tindak kriminal secara *online* umumnya ditindak lanjuti oleh lembaga yang berwenang dengan mengumpulkan barang bukti dan melakukan tindak lanjut terhadap barang bukti yang ada. Hal tersebut merupakan sebuah proses forensik, yaitu pada bidang *digital forensic*. *Digital forensic* merupakan sebuah upaya atau proses yang berdasarkan pada kegiatan mengumpulan, menganalisis, dan menyajikan bukti digital dalam proses pengadilan demi membantu mengungkapkan kejahatan yang terjadi. Proses forensik menggunakan berbagai alat bantu, khusus untuk *digital forensic*, alat bantu yang digunakan berupa *software* yang digunakan untuk mengambil data-data atau bukti yang dapat membantu proses penyelidikan atau barang bukti yang akan membantu proses sidang dalam sebuah kasus kejahatan. *Software* yang digunakan dalam proses digital forensik kini sudah ada berbagai macam berdasarkan kebutuhan atau target forensik, seperti ExifTool, FTK Imager, wireshark, metasploit, oxygen forensic, dan lain-lain (Zbrog, 2022).

Pada penelitian ini merupakan jenis penelitian eksperimental untuk mengetahui perbandingan hasil *recovery* yang mampu dihasilkan oleh perangkat forensik digital, yaitu Andriller yang merupakan aplikasi *open source* dan MOBILEdit Forensic yang berbayar. Pada penelitian ini dilakukan simulasi tindakan kriminal menggunakan aplikasi Whatsapp. Hasil dari penelitian ini diharapkan dapat menjadi pertimbangan dalam menentukan *software* yang dapat bekerja secara maksimal dalam proses forensik, khususnya di bilang *mobile forensic*.

2. TINJAUAN PUSTAKA

Pada penelitian sebelumnya telah dilakukan pengujian *digital forensic* di berbagai studi kasus, misalnya penelitian *digital forensic* pada aplikasi Twitter menggunakan *tool* FTK Imager yang dilakukan secara *live forensic* dengan metode NIJ (Zuhriyanto, Yudhana and Riadi, 2018).

Pada penelitian berikutnya dilakukan uji coba *tool* forensik, yaitu Wondershare dr. Fone for Android dan Oxygen Forensics pada dua buah *smartphone*. Hasil pengujian menunjukkan bahwa Wondershare mampu melakukan *recovery* sebesar 31% pada perangkat pertama dan 25% pada perangkat kedua, sedangkan Oxygen Forensic mampu melakukan *recovery* sebesar 67% dari perangkat pertama dan 69% pada perangkat kedua (Riadi, Sunardi and Sahiruddin, 2020). Penelitian sejenis juga dilakukan kemudian dengan hasil Wondershare mampu melakukan *recovery* sebesar 30% sedangkan Oxygen Forensic mampu melakukan *recovery* sebesar 73% (Umar and Sahiruddin, 2019).

Penelitian berikutnya melakukan uji coba forensik untuk studi kasus aplikasi MiChat dengan menggunakan *tool* MOBILEdit Forensic Express. Hasil penelitian menunjukkan *tool* ini mampu mengekstraksi *database* aplikasi MiChat, yang kemudian dapat dibaca menggunakan SysTools SQLite Viewer (Mahendra and Ari Mogi, 2021). Terdapat juga penelitian yang melakukan uji coba forensik membandingkan tiga *tools*, yaitu MOBILEdit Forensic, Wondershare dr. Fone for Android, dan Belkasoft Evidence Center. Hasil penelitian menunjukkan bahwa MOBILEdit Forensic tidak dapat mengembalikan data yang telah dihapus, sedangkan Wondershare dan Belkasoft dapat mengembalikan data berupa kontak, log panggilan, dan pesan meskipun data tersebut telah dihapus sebelumnya (Riadi, Sunardi and Sahiruddin, 2019).

3. METODE PENELITIAN

3.1. Alat dan Bahan Penelitian

Kebutuhan alat yang akan digunakan pada penilitian ini di identifikasi kedalam dua jenis yaitu kebutuh perangkat keras dan kebutuhan perangkat lunak, berupa:

a. Perangkat Keras

Perangkat keras yang digunakan dalam penelitian ini adalah laptop dengan spesifikasi:

1. Processor: Intel(R) Core(TM) 15-4210U CPU @1.70GHz (4 CPUs) ~2.4GHz.
2. Ukuran Layar: 1366 x 768 pixel
3. Memory: 8 GB DDR3 SDRAM, tipe hard drive: 500GB Serial ATA

Selain perangkat keras di atas, penelitian ini juga membutuhkan perangkat keras berupa USB type-B kabel dan *smartphone* OPPO A37fw dengan spesifikasi sebagai berikut:

1. Sistem Operasi: Android versi 5.1.1
2. Processor : Qualcomm MSM8916 Quad Core
3. Memory: 2 GB RAM

b. Perangkat Lunak

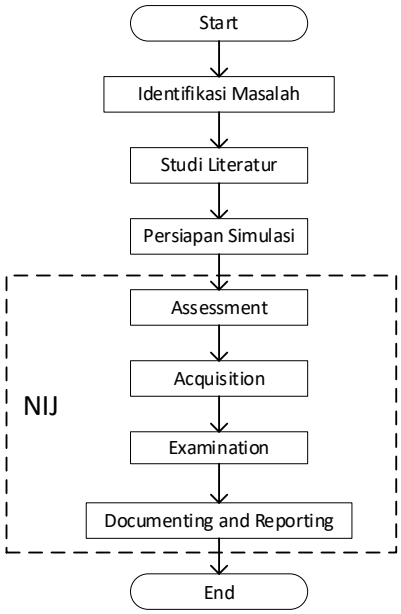
Perangkat lunak yang digunakan dalam penelitian ini adalah sebagai berikut:

1. Sistem Operasi Windows 10
2. Andriller
3. MOBILedit Forensic Express Pro
4. Python 3

3.2. Langkah-Langkah Penelitian

Langkah-langkah penelitian mengikuti alur metode *National Institute of Justice* (NIJ), dimana

NIJ merupakan metode *digital forensic* yang membagi proses forensik digital ke dalam lima tahap yaitu *assessment*, *acquisition*, *examination*, dan *documenting and reporting* (Ashcroft, Daniels and Hart, 1994). Gambar 1 menunjukkan diagram kerja langkah-langkah eksperimen pada penelitian ini yang dilakukan sesuai dengan tahapan metode NIJ.



Gambar 1. Langkah-langkah Penelitian Menggunakan Metode *National Institute of Justice* (NIJ)

Penjelasan dari langkah-langkah penelitian adalah sebagai berikut:

a. Identifikasi Masalah

Tahap pertama yaitu identifikasi masalah yang dijelaskan dalam latar belakang masalah, perumusan masalah, penentuan tujuan dan manfaat penelitian, dan penentuan topik penelitian, yaitu analisis hasil uji *mobile forensic* pada sebuah *smartphone* untuk mendapatkan presentase *recovery* pada masing-masing *tools* forensik yang digunakan.

b. Studi Literatur

Pada tahap ini dilakukan studi literatur yang berhubungan dengan penelitian yang akan dilakukan. Sumber yang digunakan berupa artikel jurnal/prosiding, laporan skripsi, buku, maupun *website* yang membahas masalah terkait penelitian. dalam hal ini, studi literatur yang dikumpulkan meliputi penjelasan mengenai *digital forensic*, *mobile forensic*, metode *national institute of justice* (NIJ), *cybercrime*, serta beberapa literatur terkait lainnya sebagai acuan dalam mengerjakan penelitian.

c. Persiapan Simulasi

Tahap ini merupakan tahap persiapan dimana proses instalasi *tools digital forensic* dilakukan. *Tools* tersebut adalah Andriller dan MOBILedit Forensic. instalasi dilakukan pada perangkat keras berupa laptop yang spesifikasinya telah dijelaskan di bagian 2.A mengenai alat dan bahan.

Selain instalasi *tools digital forensic*, tahap ini juga merupakan tahap dimana data-data yang akan menjadi sampel untuk uji *digital forensic* disiapkan. Data-data tersebut dapat berupa data kontak, gambar, dokumen, dan pesan whatsapp. Data-data tersebut disiapkan masing-masing dengan jumlah yang telah ditentukan. Tabel 1 berikut menunjukkan jumlah data sampel yang digunakan dalam pengujian ini.

Tabel 1. Data Sampel

No.	Jenis Sampel	Jumlah
1	Kontak Seluler	15
2	Gambar	5
3	Dokumen (word, pdf, dll)	5
4	Pesan Whatsapp	5

d. *Assessment*

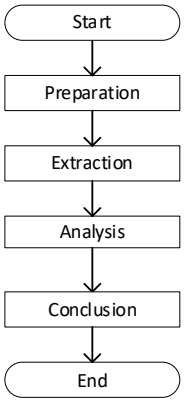
Assessment merupakan tahapan dimana *examiner* melakukan penilaian secara menyeluruh sehubungan dengan ruang lingkup kasus untuk menentukan tindakan yang diambil, termasuk di dalamnya proses identifikasi bukti digital yang akan diperiksa (Ashcroft, Daniels and Hart, 1994). Proses identifikasi merupakan proses pemilihan barang bukti tindak kejahatan yang akan di tindak lanjuti untuk mendukung proses penyelidikan sebuah kejahatan digital. Bukti bukti digital yang dipilih kemudian dilakukan proses identifikasi, pelabelan, perekaman untuk menjaga keutuhan barang bukti.

e. *Acquisition*

Aqcuisition merupakan tahap untuk mendapatkan barang bukti digital asli dengan tetap memperhatikan *chain of custody* (Ashcroft, Daniels and Hart, 1994). Tahap ini merupakan kegiatan untuk mengumpulkan data-data yang dapat mendukung proses penyelidikan untuk pencrian barang bukti kejahatan digital. Di tahap ini, terdapat proses pengambilan data dari sumber data yang relevan dan menjaga integritas barang bukti dari suatu perubahan yang mungkin terjadi.

f. *Examination*

Examination merupakan tahap pemeriksaan terhadap data yang telah diperoleh sesuai prosedur forensik, yaitu meliputi tahap *preparation*, *extraction*, *analysis*, dan *conclusion* (Ashcroft, Daniels and Hart, 1994). Tahap ini juga disebut tahap pemeriksaan data yang dikumpulkan secara forensik baik otomatis maupun secara manual dengan memastikan data yang diperoleh berupa file tersebut asli dan sesuai dengan yang didapat pada tempat kejadian kejahatan siber. Gambar 2 menunjukkan alur langkah di tahap *examination.*



Gambar 2. Langkah-langkah di Tahap *Examination*

Penjelasan tahap *examination*:
1) Preparation: menyiapkan direktori terpisah untuk menyimpan hasil ekstrasi/*recovery* berkas data bukti digital.
2) Extraction: mengekstraksi data dari barang bukti, yaitu *smartphone* OPPO A37fw dengan menggunakan *tools* MOBILedit Forensic Pro dan Andriller.
***3) Analysis*:** setelah berkas data digital berhasil diekstraksi, selanjutnya data tersebut dianalisis secara menyeluruh, meliputi data apa saja yang berhasil diekstraksi.
4) Conclusion: hasil analisis selanjutnya dipaparkan dalam suatu simpulan.

g. *Documenting and Reporting*

Tahap *documenting and reporting* atau dokumentasi dan pelaporan dilakukan sepanjang proses akuisisi barang bukti digital, dari *assessment* hingga analisis hasil ekstraksi. Proses *reporting* atau pelaporan ini secara detail menjelaskan tentang data yang didapatkan, langkah yang dilakukan, *tools* yang digunakan, serta rekomendasi untuk perbaikan kebijakan, metode, atau aspek pendukung lain dalam proses tindakan digital forensik.

4. HASIL DAN PEMBAHASAN

Pada tahap ini dijelaskan hasil eksperimen menggunakan metode NIJ, mulai dari tahap *assessment*, *acquisition*, *examination*, *preparation*, *Extraction*, *analysis*, *conclusion*, dan *documenting and reporting.*

1. Assessment

Pada tahap ini dipilih barang bukti yang akan ditindaklanjuti untuk mendukung proses penyelidikan pada kejahatan digital yang disimulasikan, yaitu berupa *smartphone* OPPO A37fw. Barang bukti tersebut kemudian diberi label, dinonaktifkan dan diisolasi dari jaringan untuk menjaga keutuhan barang bukti.

2. Acquisition

Pada tahap ini dilakukan pengumpulan data-data yang dapat mendukung proses penyelidikan, yaitu data-data bukti digital yang tersimpan di barang bukti *smartphone* OPPO A37fw, khususnya berupa percakapan di aplikasi whatsapp. *Smartphone* tersebut terlebih dahulu dilakukan proses *cloning* data. Hasil *cloning* data tersebut yang kemudian dilakukan *examination* untuk kemudian dianalisis.

3. Examination

Pada tahap ini dilakukan pemeriksaan data yang telah dikumpulkan secara forensik baik dengan cara otomatis maupun manual, serta memastikan data yang didapatkan berupa file asli dan sesuai dengan yang didapatkan pada tempat kejadian kejahatan siber.

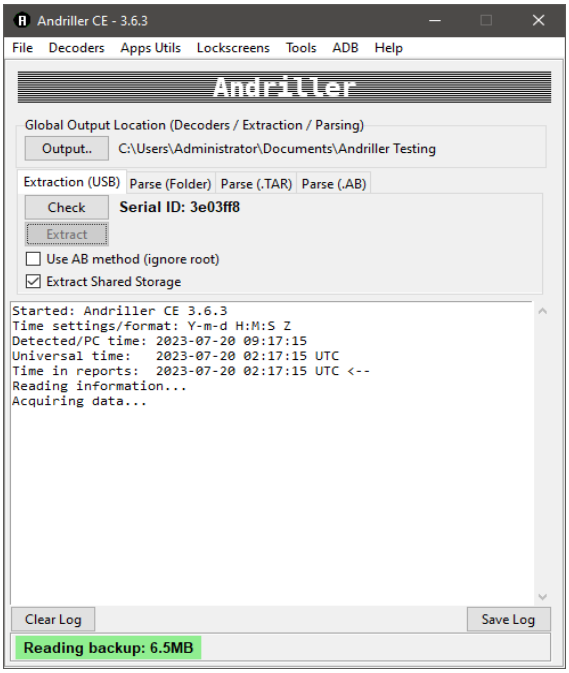
4. *Preparation*

Pada tahap ***preparation*** disiapkan folder untuk menyimpan hasil ekstraksi dari tools Andriller dan MOBILedit Forensics Pro. Selain itu juga dilakukan pengecekan kembali data-data sampel yang digunakan baik yang masih tersedia maupun sudah dalam kedaan terhapus dari *smartphone* yang menjadi objek penelitian.

5. Extraction

Pada tahap ***extraction*** dilakukan proses ekstraksi barang bukti menggunakan *tools* yang sebelumnya sudah diinstall pada laptop, yaitu Andriller dan MOBILedit Forensic Express Pro.

Ekstraksi menggunakan Andriller dilakukan dengan menghubungkan barang bukti *smartphone* dan laptop dengan menggunakan kabel *micro* USB. Setelah terkoneksi, kemudian dilakukan konfigurasi pengekstrak data dari *smartphone*. Gambar 3 menunjukkan proses ekstraksi dengan *tools* Andriller.



Gambar 3. Ekstraksi dengan Andriller

Hasil ekstraksi menggunakan *tool* Andriller lebih lanjut dapat dilihat dengan menekan *link* pada bagian *application* yang ada pada *report* hasil uji coba, sebagaimana terlihat pada Gambar 4.

[Andriller Report]

Type	Data
Serial	3e03ff8
Status	device
Permisson	shell
Ro.Product.Manufacturer	OPPO
Ro.Product.Model	A37f
Ro.Build.Version.Release	5.1.1
Ro.Build.Display.Id	A37fEX_11_190711
Wifi Mac	08:4a:cf:56:a9:eb
Local_Time	2023-07-20 09:27:47 SE Asia Standard Time
Device_Time	2023-07-20 09:27:47 WIB
Accounts	• com.google: oodenta00@gmail.com • com.whatsapp: WhatsApp
Application	Shared Storage (109)
Application	Android Calendar (62)
Application	WhatsApp Contacts (5)

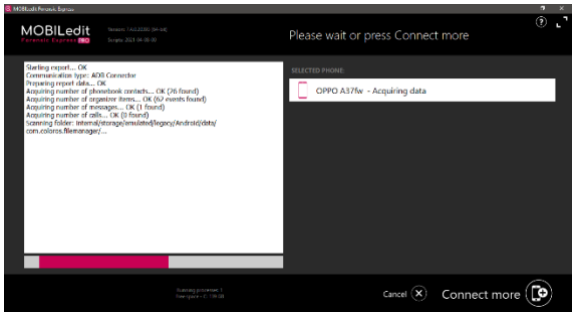
 # andriller.com # (This field is editable in Preferences)

Gambar 4. *Report* Uji *Mobile Forensic* Andriller

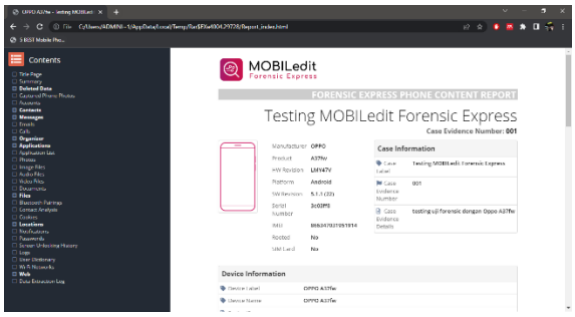
Pada ekstraksi dengan Andriller, dari data sampel yang disiapkan, hanya data sampel gambar dan dokumen yang dapat di-*recovery* secara utuh. Sedangkan pesan whatsapp dan kontak tidak dapat di-*recovery* seluruhnya oleh Andriller. Hasil *recovery* data sampel kontak, dari 15 data sampel yang digunakan, terdapat 5 kontak yang dapat di-*recovery*.

Berikutnya, dilakukan ekstraksi menggunakan MOBILedit Forensic Express Pro. Langkah yang dilakukan yaitu membuka *tool* MOBILedit Forensic Express Pro dan menghubungkan *smartphone* kepada laptop yang akan menjalan *tool*. Setelah terhubung, maka *smartphone* yang digunakan akan terdeteksi di halaman awal MOBILedit Forensic Express Pro. Terdapat 4 jenis ekstrak data yang didukung oleh MOBILedit Forensic Express Pro, yaitu *full content*, *application analysis*, *deleted data only*, *device info only*, *serta parental check*. Dalam pengujian ini dilakukan *full content extract* yang akan melakukan ekstraksi ke seluruh data yang ada di dalam *smartphone*.

Setelah memilih jenis ekstrak data yang diinginkan, selanjutnya melengkapi isian informasi meliputi nama kasus yang dikerjakan, detail *smartphone* yang menjadi barang bukti, hingga nama yang melakukan penyelidikan, serta format *report* yang dihasilkan. Gambar 5 menunjukkan proses ekstraksi. Keluaran dari tes pengujian *mobile forensic* berupa *report* hasil ekstraksi data dari *tool* MOBILedit Forensic Express Pro yang telah dilakukan uji coba dalam bentuk HTML dapat dilihat di Gambar 6.

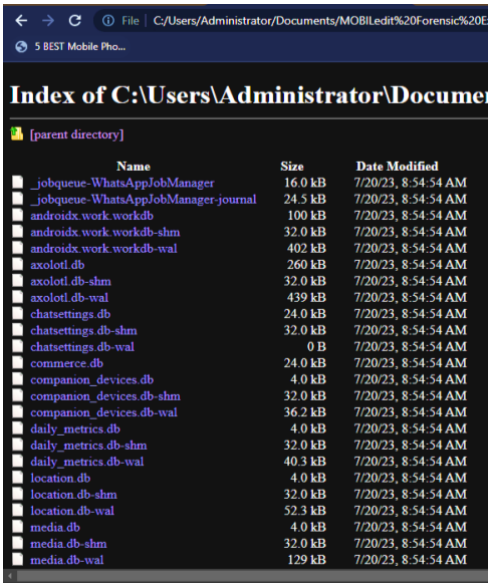


Gambar 5. Ekstraksi dengan MOBILedit Forensic Express Pro



Gambar 6. *Report* Hasil MOBILedit Forensic Express Pro

Pada *report* tersebut terdapat semua detail mengenai *case* yang sedang dilakukan penyelidikan, mulai dari detail *case* yang sebelumnya diisi, rangkuman dari hasil ekstraksi data, hingga semua data di dalam *smartphone* yang berhasil di-*recovery*. Hasil ekstraksi dengan MOBILedit Forensic Express Pro, dari data sampel disiapkan seluruh data kontak, gambar dan dokumen berhasil di-*recovery*. Sedangkan data pesan whatsapp tidak dapat diperoleh. MOBILedit Forensic Express Pro berhasil mengembalikan *database* WhatsApp, namun tidak dapat membaca isi dari *database* tersebut. Gambar 7 menunjukkan hasil *recovery database* WhatsApp oleh *tool* MOBILedit Forensic Express Pro.



Gambar 7. *Recovery database Whatsapp*

MOBILedit Forensic Express Pro juga dapat melakukan *recovery* terhadap data data yang telah dihapus dari *smartphone*. Hal ini dapat dilihat pada *report* yang dihasilkan setelah pengujian sebagaimana terlihat di Gambar 8 berikut:

Gambar 8. Hasil *recovery* data terhapus pada *report*

Data-data yang telah terhapus pada *smartphone* dan berhasil di-*recovery* juga lebih lanjut dapat dilihat keterangannya pada halaman *deleted files* yang juga merupakan bagian dari laporan yang dibuat ketika pengujian tes forensik.

6. *Analysis*

Selanjutnya dilakukan *analysis* berdasarkan hasil ekstraksi di tahap sebelumnya. Hasil ekstraksi menggunakan Andriller data pesan whatsapp dan kontak tidak dapat di-*recovery* seluruhnya, sedangkan data kontak berhasil di-*recovery* sebagian (5 kontak dari 15 data sampel yang disiapkan). Hal ini terjadi dikarenakan kelima kontak tersebut terlebih dahulu telah disinkronkan oleh aplikasi whatsapp sehingga dapat tersimpan sebagai kontak whatsapp, sedangkan 10 kontak yang lain belum disinkronisasi. Dengan demikian dapat dapat dihitung bahwa dari total 30 data sampel yang disiapkan, hanya 15 data sampel yang dapat di-*recovery* dengan baik oleh *tool* Andriller. Adapun hasil perhitungan tingkat *recovery tool* Andriller dapat dilihat di Tabel 2 berikut:

Tabel 2. Hasil *Recovery* Data Sampel Andriller

Jenis Data Sampel	Total Data Sampel	Data Sampel Di-*recovery*
Kontak Seluler	15	5
Gambar	5	5
Dokumen (Word & PDF)	5	5
Pesan Whatsapp	5	0
Total	30	15

$$hasil\ recovery\ tool = \frac{15}{30}\ x\ 100\% = 50\%$$

Hasil dari perhitungan hasil *recovery tool* dapat disimpulkan bahwa dari total 30 data sampel, Andriller dapat melakukan *recovery* hingga 50% data sampel yang telah dimasukkan ke dalam *smartphone*.

Sedangkan hasil ekstraksi dengan MOBILedit Forensic Express Pro, dari data sampel disiapkan seluruh data kontak, gambar dan dokumen berhasil di-*recovery*, namun data pesan whatsapp tidak berhasil diperoleh. Berdasarkan hasil ekstraksi tersebut, dapat disimpulkan hasil *recovery* data sampel seperti di Tabel 3.

Tabel 3. Hasil Recovery Data Sampel MOBILedit Forensic

Jenis Data Sampel	Total Data Sampel	Data Sampel ter-*recovery*
Kontak Seluler	15	15
Gambar	5	5
Dokumen (Word & PDF)	5	5
Pesan Whatsapp	5	0
Total	30	25

$$hasil\ recovery\ tool = \frac{25}{30}\ x\ 100\% = 83{,}33\%$$

Hasil dari perhitungan hasil *recovery tool* dapat disimpulkan bahwa dari total 30 data sampel, MOBILedit Forensic Express Pro dapat melakukan *recovery* hingga 83,33% data sampel yang telah dimasukkan kedalam *smartphone*.

Berdasarkan hasil di atas, dapat dibuat rekapan persentase hasil *recovery* oleh kedua *tools*, yaitu Andriller dan MOBILedit Forensic Express Pro sebagaimana disajikan di Tabel 4.

Tabel 4. Hasil Analisis Uji *Mobile Forensic*

Tools	Data Sampel Awal	Data Sampel Ter-*recovery*	Persentase Hasil *recovery*
Andriller	30	15	50%
MOBILedit Forensic Express Pro	30	25	83,33%

Tabel 4 menunjukkan bahwa Andriller mampu melakukan *recovery* terhadap data sampel yang disediakan sebanyak 50%, sedangkan MOBILedit Forensic Express Pro dapat melakukan *recovery* sebesar 83,33% data sampel.

7. *Conclusion*

Berdasarkan hasil analisis di tahap sebelumnya, dapat disimpulkan bahwa kedua *tools* yang digunakan dapat menjalankan fungsi masing-masing yaitu untuk melakukan akuisisi dan *extract* data. Selain itu kedua *tools* dapat membuat sebuah laporan dalam bentuk yang ditentukan masing-masing untuk kemudian dapat dilihat sebagai hasil uji. Andriller memiliki presentase *recovery* terhadap data sampel yang disediakan sebanyak 50%, sedangkan untuk MOBILedit Forensic Express Pro dapat melakukan *recovery* data dengan persentase yang lebih tinggi yaitu sebesar 83,33% data sampel.

Selain itu, kedua *tools* dapat menjalankan extract data secara menyeluruh meskipun tanpa

adanya akses *root* pada *smartphone* yang digunakan sebagai objek penyelidikan. Hal ini tentunya dapat juga menjadi pertimbangan untuk pemakaian *tools*.

Perbedaan lain dari kedua *tools* di atas yaitu pada kemampuan *tools* untuk melakukan *recovery* terhadap data yang telah dihapus pada *smartphone* yang menjadi objek penyelidikan. MOBILedit Forensic Express Pro memiliki keunggulan yaitu dapat melakukan *recovery* terhadap data data yang telah dihapus dari *smartphone*, sedangkan Andriller tidak dapat me-*recovery* file yang telah dihapus. Kemampuan *recovery* data pada Andriller hanya sebatas terhadap seluruh data yang masih ada dalam *smartphone* dan belum terhapus.

Hasil selanjutnya mengenai *recovery* terhadap data sampel pesan whatsapp, kedua *tools* tidak sepenuhnya gagal dalam melakukan *recovery*, melainkan kedua *tools* hanya sebatas dapat melakukan *recovery* terhadap *database* whatsapp yang telah di-*backup* sebelumnya oleh sistem *smartphone* namun tidak dapat membaca isi *database*. Hal tersebut dikarenakan *database* whatsapp dienkripsi sehingga untuk melakukan ektrak lebih lanjut, dibutuhkan *tools* lain.

5. KESIMPULAN DAN SARAN

5.1. Kesimpulan

Berdasarkan penelitian yang telah dilakukan mengenai perbandingan hasil uji *tools recovery* mobile forensic pada *smartphone* Android menggunakan metode NIJ dapat ditarik kesimpulan: 1) uji *mobile forensic* dengan menggunakan Andriller dan MOBILedit Forensic Express Pro dapat dilakukan meski tanpa akses Root pada *smartphone* yang digunakan; 2) dari total 30 data sampel yang digunakan dalam uji coba *mobile forensic*, *tool* Adriller memiliki tingkat *recovery* data lebih rendah yaitu sebesar 50%, sedangkan pada MOBILedit Forensic Express pro dapat melakukan *recovery* data hingga 83,33% data sampel di*recovery*; 3) hanya MOBILedit Forensic Express Pro yang dapat melakukan *recovery* data yang telah dihapus dari objek penyelidikan sedangkan Andriller tidak dapat melakukan *recovery* terhadap data yang dihapus; 4) *tools recovery* terhadap WhatsApp hanya dapat memulihkan pesan dari *database* yang sudah di-*backup* oleh sistem. Jika ingin melakukan ekstraksi lebih lanjut dari *database* dengan enkripsi tertentu, diperlukan *tools* khusus.

5.2. Saran

Saran bagi penelitian selanjutnya perlu mempertimbangkan menggunakan *tools* lain yang lebih *powerfull* dan memiliki banya fungsi atau fitur.

DAFTAR PUSTAKA

Ahdiat, A., 2023. *67% Penduduk Indonesia Punya Handphone pada 2022, Ini Sebarannya*. [online] Available at: <https://databoks.katadata.co.id/datapublish/2023/03/08/67-penduduk-indonesia-punya-handphone-pada-2022-ini-sebarannya>.

Anon. 2021. *Current Smartphone Developments in Indonesia*. [online] Available at: <https://bamai.uma.ac.id/2021/09/28/perkembangan-smartphone-saat-ini-di-indonesia/?%2F2021%2F09%2F28%2Fperkembangan-smartphone-saat-ini-di-indonesia%2F=>.

Anon. 2022. *Kejahatan Siber di Indonesia Naik Berkali-kali Lipat*. [online] Available at: <https://pusiknas.polri.go.id/detail_artikel/kejahatan_siber_di_indonesia_naik_berkali-kali_lipat>.

Anon. 2023. *Mobile Operating System Market Share Indonesia*. [online] Available at: <https://gs.statcounter.com/os-market-share/mobile/indonesia>.

Ashcroft, J., Daniels, D.J. & Hart, S. V, 1994. *Forensic Examination of Digital Evidence: A Guide for Law Enforcement*. [online] Washington. Available at: <https://www.ncjrs.gov/App/Publications/abstract.aspx?ID=199408>.

Clough, J., 2015. *Principles of Cybercrime*. 2nd ed. Victoria: Cambridge University Press.

Mahendra, K.D.O. & Ari Mogi, I.K., 2021. Digital Forensic Analysis Of Michat Application On Android As Digital Proof In Handling Online Prostitution Cases. *JELIKU (Jurnal Elektronik Ilmu Komputer Udayana)*, 9(3),p.381.https://doi.org/10.24843/jlk.2021.v09.i03.p09.

Riadi, I., Sunardi & Sahiruddin, 2019. Analisis Forensik Pada Platform Android Menggunakan Metode NIJ. *Jurnal Rekayasa Teknologi Informasi (JURTI)*, 3(1), pp.87–95.

Riadi, I., Sunardi & Sahiruddin, 2020. Perbandingan Tool Forensik Data Recovery Berbasis Android Menggunakan Metode Nist. *Jurnal Teknologi Informasi dan Ilmu Komputer (JTIIK)*, 7(1), pp.197–204. https://doi.org/10.25126/jtiik.202071921.

Sadya, S., 2023. *Pengguna Smartphone Indonesia Terbesar Keempat Dunia pada 2022*. [online] Available at: <https://dataindonesia.id/digital/detail/pengguna-smartphone-indonesia-terbesar-keempat-dunia-pada-2022>.

Umar, R. & Sahiruddin, 2019. Metode Nist Untuk Analisis Forensik Bukti Digital Pada Perangkat Android. *Prosiding SENDU_U_2019*, pp.978–979.

Zbrog, M., 2022. *A Guide to Digital Forensics and Cybersecurity tools (2022-2023)*. [online] Available at: <https://www.forensicscolleges.com/blog/res

ources/guide-digital-forensics-tools>.

Zuhriyanto, I., Yudhana, A. & Riadi, I., 2018. Perancangan Digital Forensik pada Aplikasi Twitter Menggunakan Metode Live Forensics. *Seminar Nasional Informatika 2008 (semnasIF 2008)*, 2018(November), pp.86–91.