Analisis Forensik Digital Recovery Data Smartphone pada Kasus Penghapusan Berkas Menggunakan Metode National Institute Of Justice (NIJ)

Steven Marcellino[1], Henki Bayu Seta[2], Wayan Widi[3]
Program Studi Informatika / Fakultas Ilmu Komputer
Universitas Pembangunan Nasional Veteran Jakarta
Jl. RS. Fatmawati , Pondok Labu, Jakarta Selatan, DKI Jakarta, 12450, Indonesia
stevenmarcellino@upnvj.ac.id[1] , henkiseta@upnvj.ac.id[2], wayan.widi@upnvj.ac.id[3]

Abstrak. Smartphone merupakan bentuk semakin berkembangnya jaman dan teknologi, salah satunya adalah Smartphone berjenis Android yang sudah maju sangat pesat, Smartphone dapat memberikan dampak negatif sekaligus dampak positif , Smartphone digunakan untuk melakukan tindak pidana. Saat ini, banyak kasus yang yang dilakukan dengan menghilangkan jejak kejahatan. Barang bukti yang dihapus itu menjadi salah satu bukti penting untuk pihak berwenang melakukan investigasi untuk menyelesaikan tindak pidana kejahatan di pengadilan. Metode yang digunakan dalam penelitian ini adalah Metode National Institute of Justice (NIJ). Metode ini merupakan sebuah tahapan yang dapat dilakukan untuk forensic digital metode ini memiliki urutan tahapan identification, Collection, Examination, Analysis, dan Reporting. Pada penelitian ini menggunakan data file excel, File image, File Audio, File Video dan File Zip pada Smartphone Android, Setelah dilakukan percobaan kemudian dilakukan analisis sehingga terdapat hasil berupa temuan yang digunakan untuk penyelidikan dan didapatkan bukti digital. Pada penelitian ini didapatkan hasil dengan tools Wondershare Dr Fone berdasarkan hasil perhitungan data yang berhasil dikembalikan yaitu Wondershare Dr Fone mendapatkan hasil 63% sedangkan untuk EaseUS Data Recovery mendapatkan hasil 100% dan tools EaseUS Data Recovery dapat mengembalikan file atau data terhapus dengan baik berdasarkan data yang berisi 30 variabel data dan dapat dikembalkan 30 variabel data, hasil yang didapat lebih maksimal dibandingkan dengan tools Wondershare Dr Fone yang hanya dapat mengembalikan 19 variable data dari total 30 data yang ada.

Kata Kunci: Smartphone, Investigasi, Mobile Forensic, cybercrime

1 Pendahuluan

Indonesia sebagai negara berkembang merupakan contoh salah satu negara yang memiliki perkembangan teknologi yang cukup baik, termasuk teknologi mengenai *Smartphone* berjenis *Android* yang semakin banyak dikembangkan oleh perusahaan *Smartphone Android*. Sistem *Android* dibuat untuk memanjakan pengguna nya. Dengan berkembangnya teknologi di masa ini, semakin banyak orang yang menggunakan *Smartphone* berbasis *Android,* dan tidak jarang kehilangan data dan *file* dalam *Smartphone Android*.[1]

Semakin majunya dunia teknologi banyak orang yang dengan sengaja melakukan tindak kejahatan pada zaman sekarang dengan menggunakan *Smartphone Android* dan sengaja membuang *file* atau data kejahatan untuk menghilangkan barang bukti digital agar menghindari tindak pidana yang membebani dakwaan dengan barang bukti digital (Riadi, Sunardi & Sahiruddin, 2019).[8]

Smartphone dapat dijadikan sebagai alat kejahatan *cybercrime* dengan berbagai macam fungsi. Pelaku tindak kejahatan *cybercrime* menggunakan salah satu media yaitu *Smartphone* sebagai alat komunikasi untuk melakukan tindakan kejahatan.[4**]** Pelaku kejahatan pemalsuan data dapat menggunakan *Smartphone* sebagai alat untuk melakukan Tindakan kejahatan. Hal ini termasuk dalam kejahatan yang masuk ke dalam kejahatan elektronik, karena menggunakan sarana elektronik *Smartphone* sebagai alat dalam melakukan Tindakan kejahatan.[7]

Penelitian ini bertujuan untuk menggunakan metode NIJ untuk melakukan proses penelitian pada *Smartphone* andorid dengan dua *tools* yang telah disiapkan dan untuk menjalankan pengujian untuk memperoleh data bukti digital pada data bukti *Smartphone*.[10] Keuntungan dari penelitian ini dapat sebagai acuan referensi untuk penyelidikan lain, membahas *forensic* digital dan membantu penyidik pidana untuk memperoleh bukti digital melalui *forensic* digital secepat mungkin.[5]

ISSN: 2655-139X (ONLINE)
ISSN: 0216-4221 (PRINT)

2 Tinjauan Pustaka

2.1 Digital Forensik

Digital forensik adalah kegiatan penelitian untuk membuktikan suatu kejahatan dengan menemukan bukti digital untuk memperkuat suatu bukti dari kasus yang sedang diproses.**[**3] Namun kini cakupannya lebih luas, dengan menganalisis perangkat yang digunakan sebagai penyimpanan data dalam bentuk digital. Forensik digital berguna karena pada data perangkat digital biasanya diblokir, dihapus, disembunyikan dan diganti.[9]

2.2 Mobile Forensik

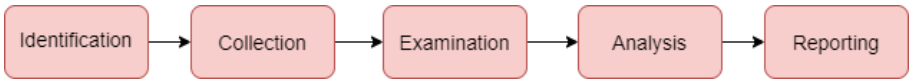
Mobile Forensik merupakan cabang atau turunan dari digital forensik, Forensik seluler adalah ilmu yang menggunakan metode forensik untuk memulihkan bukti digital dari perangkat seluler. Forensik perangkat seluler adalah forensik yang melibatkan penggalian data dari ponsel yang dapat digunakan sebagai bukti. Bukti ini dapat digunakan sebagai dasar untuk penyelidikan penegakan hukum terhadap suatu kasus.[6]

2.3 Data *Recovery*

Data *Recovery* adalah proses memulihkan data dari keadaan rusak, hilang, terhapus atau tidak dapat diakses ke dalam kondisi normal atau awal, Pemulihan data adalah suatu bagian yang penting dari analisis *forensic* dan itu harus dilakukan untuk mengetahui apa yang terjadi dan mengambil *file* data yang sebelumnya dihapus. Data yang dikembalikan dapat berasal dari harddisk, flashdisk, *Smartphone* dan media penyimpanan lainnya.\

2.4 Metode NIJ

Dalam penelitian ini, *Metode National Institute of Justice* (NIJ) diadaptasi dan diimplementasikan. Metode NIJ ini digunakan sebagai penjelasan tentang tahapan-tahapan penyelidikan yang digunakan guna menentukan secara sistematis proses dan langkah-langkah penyelidikan sehingga digunakan sebagai pedoman untuk memecahkan masalah-masalah yang ada.[7] Tahapan penyelidikan ini digambarkan pada Gambar 1.



ISSN: 2655-139X (ONLINE)
ISSN: 0216-4221 (PRINT)

Gambar. 1. Tahapan *Metode National Institute of Justice* (NIJ,2021)

2.5 Tahapan Metode NIJ

Fase penelitian ini berdasarkan gambar 1 terdiri dari 5 fase yaitu fase persiapan, fase pengumpulan, fase pemeriksaan, fase analisis dan fase pelaporan. Uraian lengkap fase metode NIJ adalah sebagai berikut:

a) Fase pertama adalah Persiapan, yaitu tahap dalam mempersiapkan tim untuk melakukan penyelidikan.

b) Fase kedua adalah pengumpulan/koleksi adalah tahap menemukan *file* dan membuat Salinan terhadap objek fisik yang berisi alat bukti digital.

c) Fase ketiga adalah tahap pemeriksaan. Tahapan ini merupakan tahapan pengecekan secara manual atau otomatis terhadap barang bukti yang diperoleh melalui proses *forensic* dan memastikan bahwa barang bukti digital yang diterima sama otentiknya dengan yang diterima di TKP.

d) Fase keempat adalah analisis, tahap diperoleh alat bukti digital yang digunakan untuk tahap penyidikan, dilakukan analisis rinci terhadap barang alat bukti digital.

e) Fase kelima adalah tahap pelaporan, Setelah analisis barang bukti digital yang diterima, laporan meliputi analisis kegiatan yang dilakukan dalam penyidikan, uraian alat penyidikan, definisi metode penyidikan, dan tindakan pendukung.

2.6 *HashMyFiles*

HashMyFiles merupakan sebuah *tools* yang dapat digunakan untuk menghitung nilai *hash* MD5 dan SHA1 dari 1 *file* maupun lebih yang ada.

Hash/checksum adalah baris kode komputer yang bertindak sebagai identitas suatu *file* pada waktu tertentu dan dalam kondisi tertentu, sehingga jika *file* tersebut sedikit berubah (dengan kata lain: integritas data berubah), *hash*/checksum juga akan berubah.[12]

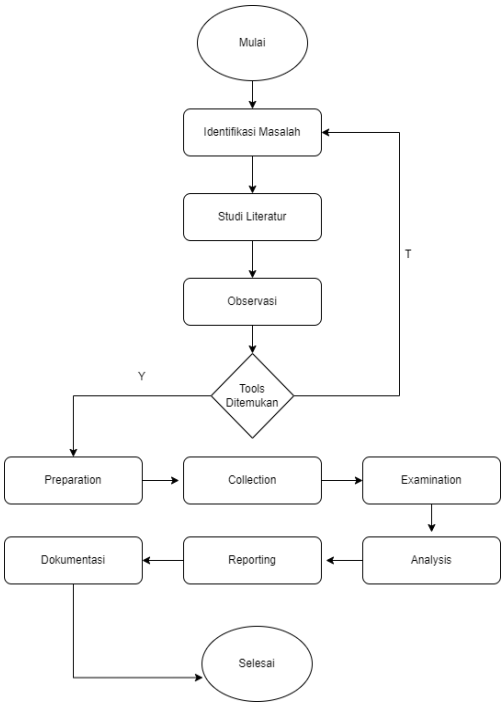
2.7 *Wondershare Dr Fone*

Wondershare Dr Fone merupakan sebuah *Software* pada computer yang dapat digunakan untuk melakukan pengembalian data yang terhapus atau terformat pada *Smartphone Android*. *Wondershare* merupakan salah satu aplikasi *Recovery* terbaik untuk mengembalikan data berupa kontak, pesan, log panggilan, foto, video dan dokumen.[2]

2.8 *EaseUS Data Recovery*

EaseUS Data Recovery merupakan sebuah *Software Recovery* yang ada untuk windows yang mendukung *Recovery file*, partisi dan pemulihan data.

3. Metodologi Penelitian



Gambar. 2. Tahapan Penelitian

3.1 Identifikasi Masalah

Tahapan ini digunakan untuk menentukan masalah yang muncul di lingkungan penelitian. Selain itu, pada titik ini, identifikasi ini mengarah pada definisi tujuan penelitian.

Pada tahap ini, terdapat proses perumusan masalah di balik penggunaan *Metode National Institute of Justice* (NIJ) untuk mempelajari analisis *Mobile* forensik. Sesuai dengan pertanyaan yang disebutkan di latar belakang. Pertanyaan yang diangkat dalam investigasi ini adalah menggunakan *Metode National Institute of Justice* (NIJ) untuk menganalisis proses investigasi *Mobile* forensik.

3.2 Studi Literatur

Pada fase ini peneliti melakukan penelusuran literatur pada buku, jurnal penelitian, atau literatur lain yang berhubungan dengan penelitian. Penulis mengumpulkan literatur tentang konsep forensik seluler, proses analisis forensik digital, *Metode National Institute of Justice* (NIJ), dan informasi terkait.

3.3 Observasi

Pada tahap observasi adalah merupakan teknik mengumpulkan data yand dilakukan dengan mengamati objek secara langsung maupun dengan mencatatnya secara sistematis. Pengamatan dilakukan oleh peneliti melalui

pengamatan dan pencatatan, dan hasil yang diperoleh berupa kegiatan, peristiwa, objek, keadaan, atau emosi manusia.

3.4 *Preparation*

Preparation adalah tahapan untuk mempersiapkan peralatan yang digunakan dalam menjalankan tugas-tugas yang diperlukan dalam proses penyelidikan. Pada tahap ini dilakukan proses penyiapan alat-alat yang akan digunakan pada proses penyidikan. Pada penelitian ini peneliti menggunakan *tools Wonderhsare Dr Fone* dan *EaseUS* Data *Recovery*.

3.5 *Collection*

Collection adalah tahapan untuk menemukan / mendapatkan *file* yang dicari dan dengan mengumpulkan data atau menyalin objek fisik yang berisi alat bukti digital dan mengumpulkan data digital yang didapatkan dari sumber yang relevan untuk melindungi keaslian alat bukti digital dari gangguan atau ancaman.

3.6 *Examination*

Examination adalah melakukan pengecekan secara manual atau otomatis terhadap barang bukti yang diperoleh dari hasil observasi di lapangan dan menyerahkannya kepada penyidik *Mobile* forensik untuk diolah datanya, dan menyerahkan data yang ditemukan setelah diserahkan kepada penyidik sebagai tahap pemeriksaan barang bukti. proses melalui proses forensik dan memastikan bahwa bukti digital yang diterima sama otentiknya dengan yang diterima di TKP.

3.7 *Analysis*

Analysis adalah tahap setelah diperoleh alat barang bukti digital yang digunakan untuk fase penyidikan sebelumnya, barang bukti digital yang didapatkan lalu dlakukan analisis secara mendalam dengan menggunakan metode ilmiah dan hukum untuk menentukan nilai signifikan dari barang bukti digital tersebut.

3.8 *Reporting*

Reporting merupakan tahap akhir setelah semua tahapan forensik selesai dilakukan. Sebuah laporan ringkasan rinci dihasilkan yang menggambarkan semua langkah dan kesimpulan yang diambil selama penyelidikan.

4. Hasil dan Pembahasan

4.1 *Preparation*

Pada tahap *Preparation* yang dilakukan sesuai dengan scenario yang bertujuan untuk mendapatkan bukti digital pada kasus kejahatan yang sebenarnya maka dibuatlah scenario yaitu: user melakukan kegiatan akses internet, membuka *file*, melakukan pengeditan dan mengunduh *file excel, File image, File Audio, File Video dan File Zip* pada *Smartphone Android*, untuk membuktikan validitas *file* yang dibuat terhadap hasil Analisa *forensic* dan *Recovery file* maka dilakukan pengecekan nilai *hash* pada setiap *file* yang dibuat pada *Smartphone* tersebut.

ISSN: 2655-139X (ONLINE)
ISSN: 0216-4221 (PRINT)

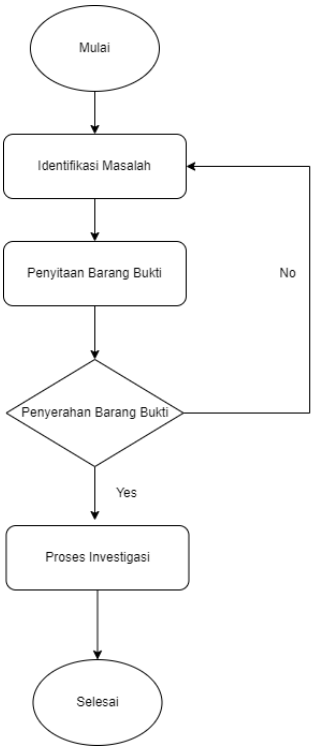
Kemudian dilakukan kegiatan mematikan dan menghidupkan Kembali *Smartphone Android* seolah olah bahwa *Smartphone Android* tersebut telah digunakan dan langkah selanjutnya dilakukan penghapusan data untuk dilakukan Tindakan pengujian *Mobile forensic*s *Recovery*.

4.2 Metode NIJ

Setelah skenario berhasil berjalan maka langkah selanjutnya yang harus dilakukan adalah mencari data dan menganalisa *Smartphone Android* untuk kebutuhan *forensic*, setelah itu dilakukan langkah langkah analisis *forensic* sebagai berikut:

4.2.1 Identification

Identifikasi adalah proses mempersiapkan peralatan yang digunakan dalam tahap penyidikan yang pada saat ini mengumpulkan semua bukti seperti *Smartphone* beserta datanya dari korban dan pelaku diamankan, guna menjaga keaslian barang bukti. Dalam memudahkan tahapan mengidentifikasi masalah yang terjadi antara korban dan pelaku, penyidik membuat alur penyelidikan untuk mendapatkan barang bukti yang didapat oleh pelaku.



Gambar. 3. Flowchart Alur Investigasi

Berikut alur investigasi ke pengungkapan bukti, seperti yang ditunjukan pada gambar 3 Flowchart Alur Investigasi:

a) Identifikasi masalah dilakukan oleh pihak yang berwenang untuk mengetahui detail masalah yang terjadi
dengan korban dan pelaku.
b) Penyitaan barang bukti dilakukan untuk mengamankan barang bukti dan menyimpan keadaan aslinya.

c) Proses penyidikan dilakukan pada saat pihak berwenang menyerahkan barang bukti kepada penyidik untuk
melaksanakan hasil penyidikan untuk memperoleh bukti.

4.2.2 *Collection*

Pada tahap ini, dilakukan pengumpulan bukti fisik, dokumentasi, yang akan dilakukan. Proses pada tahap ini adalah dilakukan dengan memeriksa jenis barang bukti, spesifikasi, sistem operasi, versi *Android*, dan lainnya yang terkait data. Berikut merupakan barang bukti yang telah didapat untuk melanjutkan proses penyelidikan.

Gambar 4. *Smartphone* Oppo A37f

Tabel 1. Spesifikasi *Smartphone*

Detail Perangkat	***Spesifikasi***
Nama Perangkat	*Oppo A37f*
Nomor Model	*Andorid 5.1 (lollipop,*
Versi Android	*ColorOS 3*
Processor	*Snapdragon 410*
RAM	*2 GB*
ROM	*16 GB*

Setelah berhasil mengumpulkan bukti yang digunakan oleh pelaku, maka barang bukti itu diberikan kepada penyidik untuk sebuah investigasi.

4.2.3 *Examination*

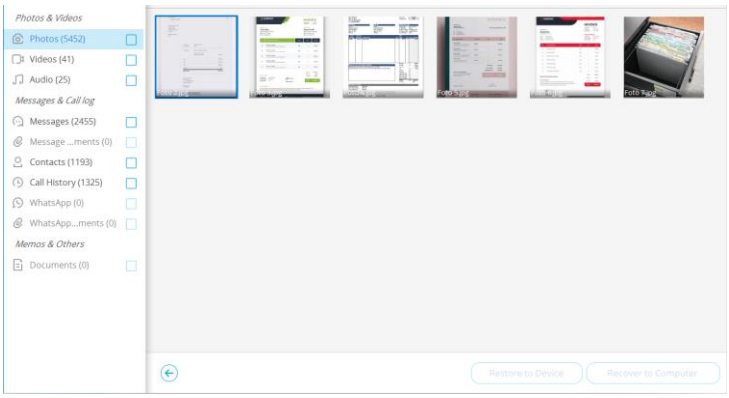
Pada proses penyelidikan dilakukan uji coba yaitu merupakan tahap percobaan *tools forensic* untuk mendapatkan bukti digital yang akan digunakan untuk mendapatkan bukti digital yang digunakan untuk

ISSN: 2655-139X (ONLINE)
ISSN: 0216-4221 (PRINT)

memecahkan masalah yang tengah diselidiki. Pada proses uji *tools forensic* pada penelitian ini dilakukan sebagai berikut:

4.2.3.1 *Examination* menggunakan *Dr Fone Wondershare*

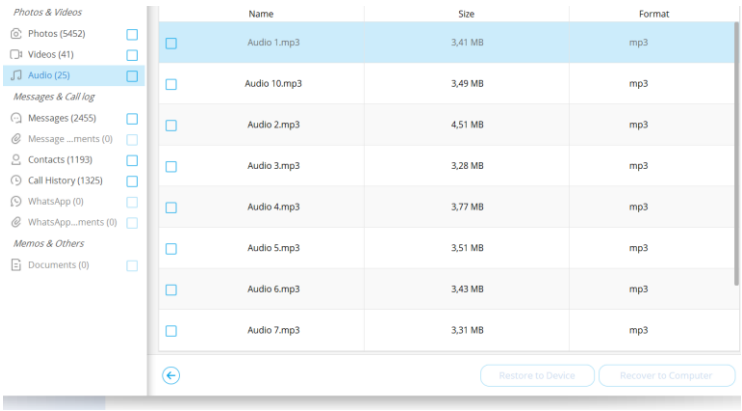
Pada proses penyelidikan dilakukan dengan mengambil, mencari dan menganalisis data dari bukti fisik yang ditemukan, di dalam proses penyelidikan ini dilakukan dengan melakukan pencarian data hanya pada *Smartphone* oppo A37f



Gambar 5. Hasil *Scanning File Images*

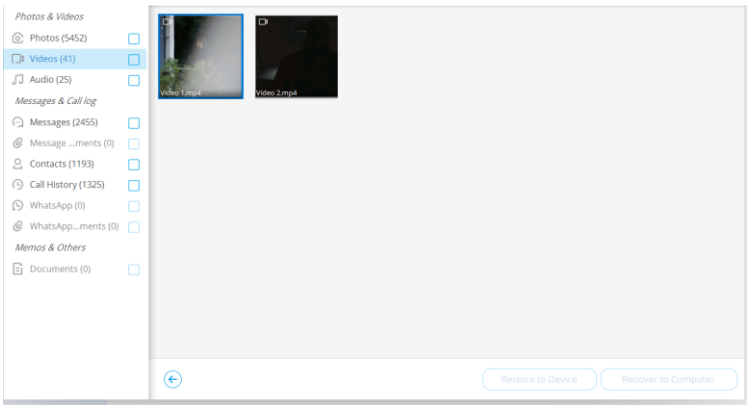
Setelah dilakukan *scanning Device* dapat ditemukan data *recovery* berupa gambar atau foto pada *Device* tersebut, pada *tools*

Dr Fone berhasil ditemukan hasil *recovery* data berupa gambar.



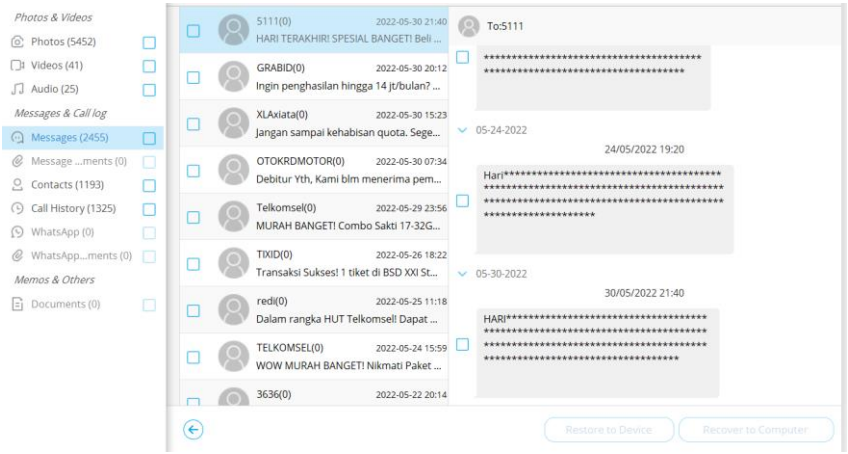
Gambar 6. Hasil *Scanning File Audio*

Pada proses *scanning* terhadap *device* tersebut ditemukan berikutnya merupakan *file* berjenis audio, *tools Dr Fone* berhasil menemukan *file* berjenis audio pada *device* tersebut.



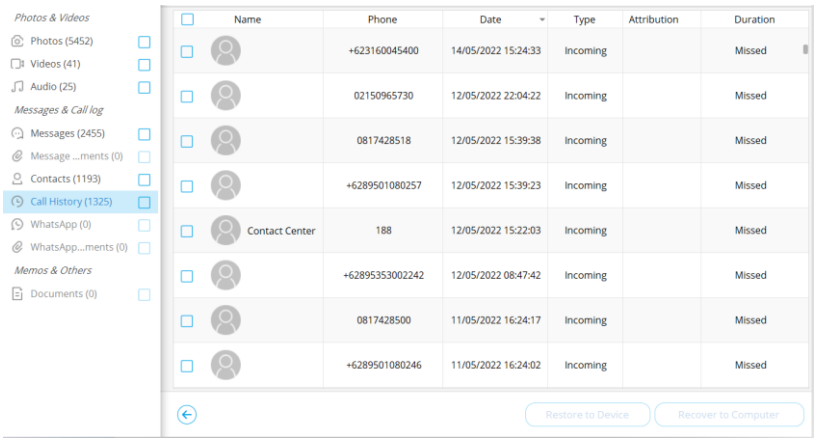
Gambar 7. Hasil *Scanning File Video*

Setelah dilakukan *scanning* pada hasil berikutnya ditemukan juga hasil *recovery* yang berhasil dilakukan oleh *tools Dr Fone* yaitu berupa data berjenis video.



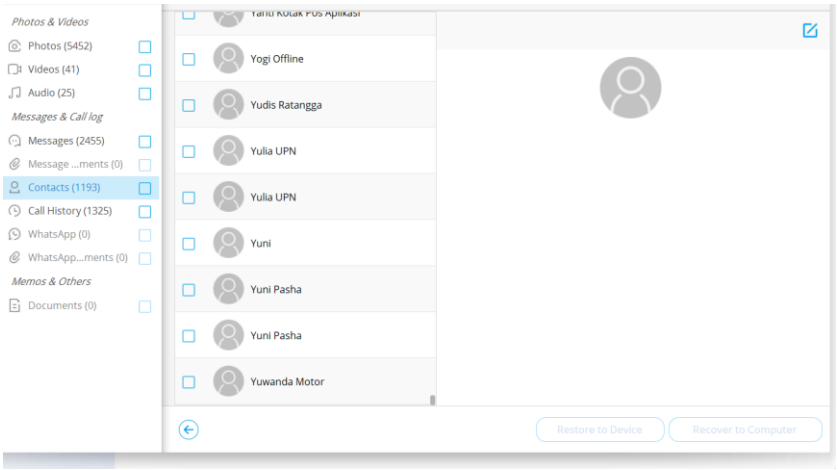
Gambar 8. Hasil *Scanning File Message*

Setelah berhasil melakukan *scanning* pada *device* maka ditemukan data *recovery* berupa message atau pesan pada *device smartphone* tersebut.



Gambar 9. Hasil *Scanning File Call History*

Pada hasil berikutnya setelah dilakukan *scanning* maka ditemukan data berupa histori panggilan pada perangkat tersebut.



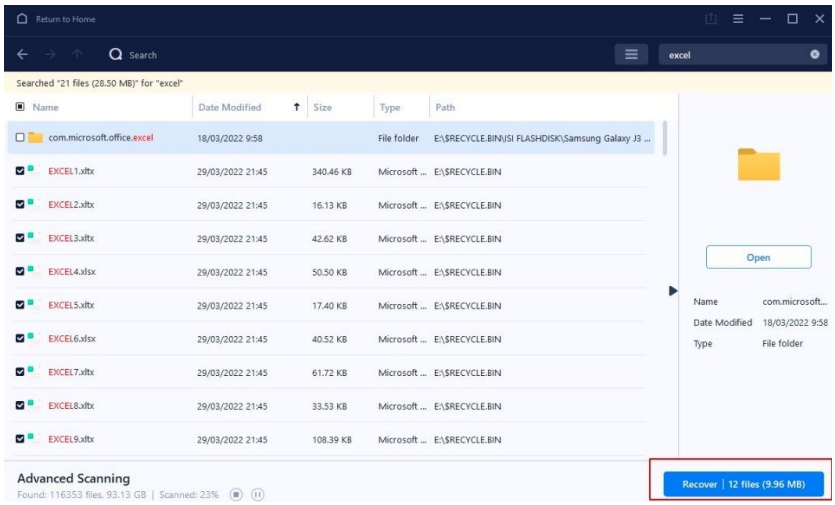
Gambar 10. Hasil *Scanning File Contacts*

Setelah dilakukan proses *Examination* menggunakan *tools Wondershare Dr Fone* Data *Recovery* memperoleh hasil data yang dihapus berupa gambar, video, audio, pesan, kontak dan log panggilan tetapi untuk *file zip dan file excel* tidak dapat dibaca oleh *tools Dr Fone* pada perangkat *Smartphone* OPPO A37f.

Pada penelitian ini *Dr Fone* peneliti tidak memiliki *access* yang *full* dikarenakan *tools* yang digunakan penulis menggunakan *tools* yang versi trial dan bukan versi berbayar.

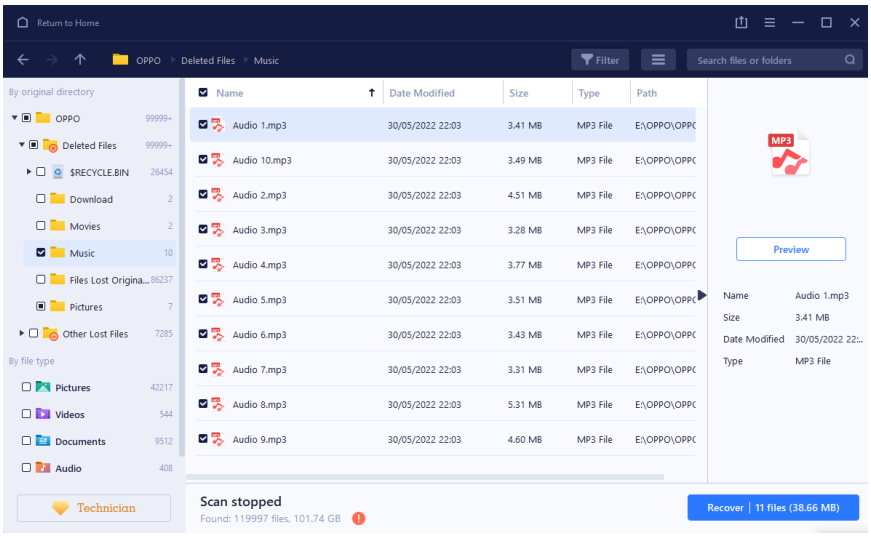
4.2.3.2 *Examination* menggunakan *EaseUS* Data *Recovery*

Pada proses penyelidikan ini dilakukan *Examination* dengan mengambil, mencari dan menganalisis data dari bukti fisik yang ditemukan, di dalam proses penyelidikan ini dilakukan menggunakan *tools EaseUS Data Recovery* dan dilakukan pencarian data hanya pada *Smartphone* oppo A37f .



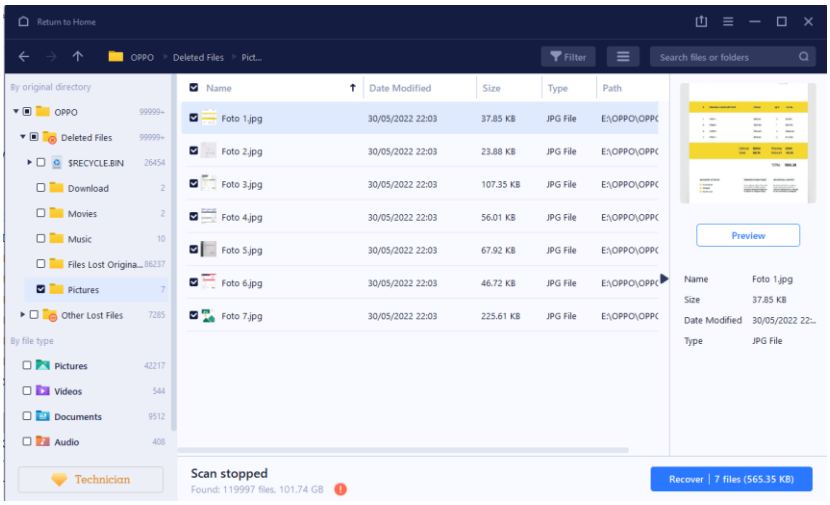
Gambar 11. Hasil *Recover File Excel*

Setelah berhasil dilakukan advance scan maka akan muncul *delete file directory* yang berisi hasil data yang berhasil ditemukan oleh *EaseUS* Data *Recovery* data *file* excel.



Gambar 12. Hasil *Recover File Audio*

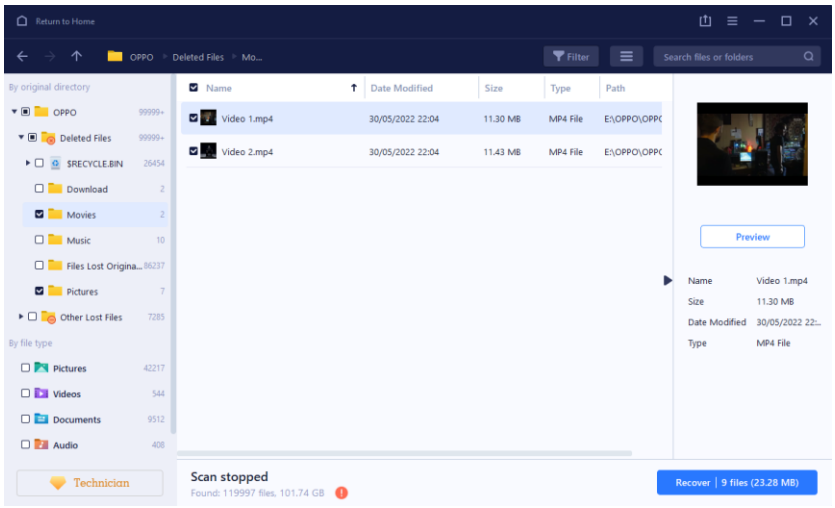
Setelah dilakukan advance scan menggunakan *EaseUS* Data *Recovery* maka ditemukan folder *deleted file* dan pada *tools EaseUS* Data *Recovery* dilakukan penyesuaian *file* berdasarkan jenis *file* tersebut, pada percobaan ini didapatkan data berupa *file* berjenis Audio.



Gambar 13. Hasil *Recover File Images*

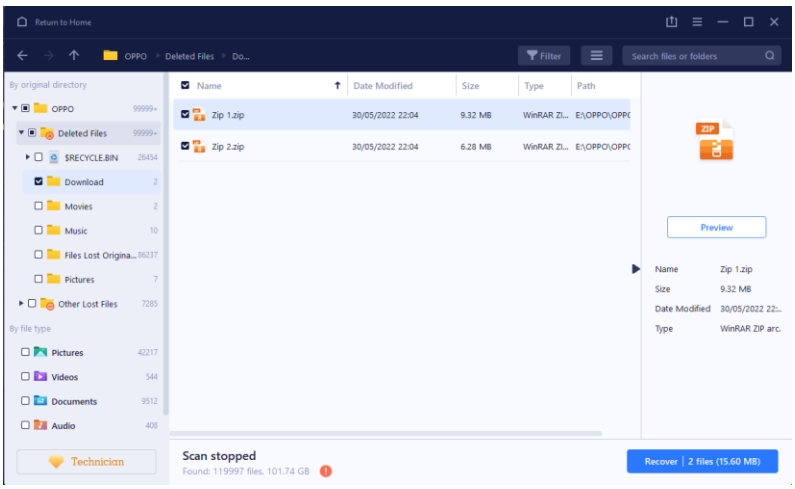
Setelah dilakukan advance scan menggunakan *EaseUS* Data *Recovery* maka ditemukan folder *deleted file* dan pada *tools EaseUS* Data *Recovery* dilakukan penyesuaian *file* berdasarkan jenis *file* tersebut, pada percobaan ini didapatkan data berupa *file* gambar.

ISSN: 2655-139X (ONLINE)
ISSN: 0216-4221 (PRINT)



Gambar 14. Hasil *Recover File Video*

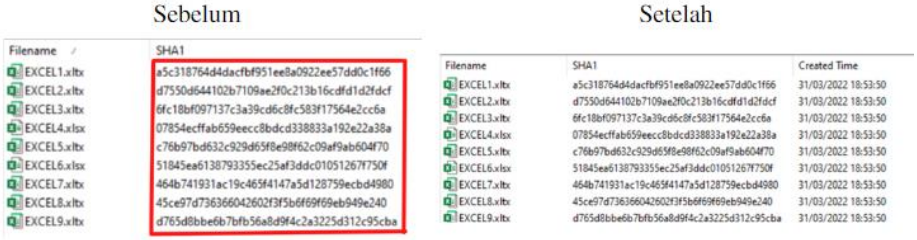
Setelah dilakukan advance scan menggunakan *EaseUS* Data *Recovery* maka ditemukan folder *deleted file* dan pada *tools EaseUS* Data *Recovery* dilakukan penyesuaian *file* berdasarkan jenis *file* tersebut, pada percobaan ini didapatkan data berupa *file* berjenis video.



Gambar 15. Hasil *Recover File Zip*

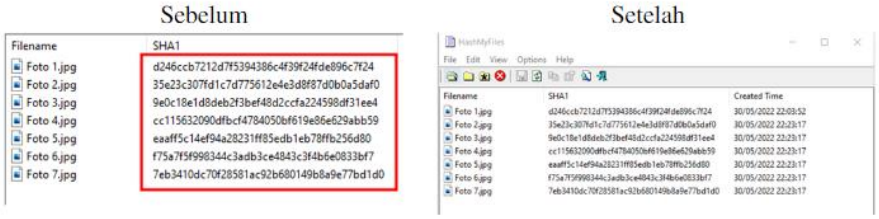
Pada data yang telah di *Recovery* tadi peneliti melakukan pengecekan nilai *hash* terhadap *file* yang telah di*Recovery*, setelah dilakukan pengecekan nilai *hash* pada *file* yang telah di*Recovery* bahwa didapatkan kesamaan nilai *file* awal dan setelah di*Recovery*.

Untuk melihat keaslian dari *file* maka dilakukan pengecekan nilai *hash*, jika nilai *hash* dari kedua *file* tersebut memiliki nilai *hash* yang sama maka dapat dikatakan *file* tersebut indentik dan sama.



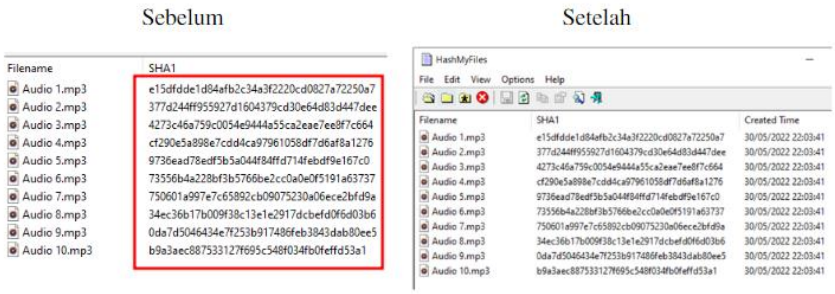
Gambar 16. Nilai *Hash File Excel* sebelum dan setelah di *Recovery*

Pada data yang telah di*recovery* pada *file* excel dan dilakukan pengecekan terhadap nilai *hash* dapat dinyatakan bahwa *file* tersebut memiliki nilai *hash* yang sama .



Gambar 17. Nilai *Hash File* Gambar sebelum dan setelah di *Recovery*

Pada pengecekan nilai *hash* pada *file* gambar setelah dilakukan proses *recovery* memiliki nilai *hash* yang sama.



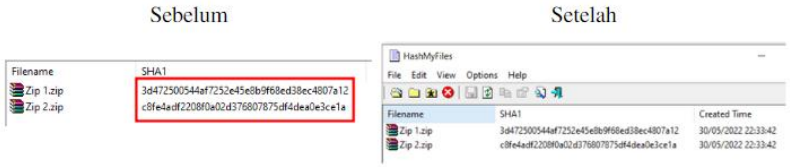
Gambar 18. Nilai *Hash File Audio* sebelum dan setelah di *Recovery*

Nilai *hash* pada *file* audio setelah dilakukan Tindakan *recovery* pada *file* tersebut memiliki nilai *hash* yang sama .

Gambar 19. Nilai *Hash File Video* sebelum dan setelah di *Recovery*

Nilai *hash* yang didapatkan pada *file* video setelah dilakukannya proses *recovery* didapatkan nilai *hash* yang sama.

ISSN: 2655-139X (ONLINE)
ISSN: 0216-4221 (PRINT)



Gambar 20. Nilai *Hash File Zip* sebelum dan setelah di *Recovery*

Pada proses *recovery file* zip nilai *hash* yang ditemukan setelah dilakukan *recovery* ditemukan memiliki nilai *hash* yang sama.

4.2.4 *Analysis*

Hasil analisa dari masing-masing *tools* tersebut dapat membuktikan bahwa data yang terhapus pada *Smartphone* OPPO A37f dapat dipulihkan dan akan menjadi data pendukung untuk kasus kejahatan.

Analisa dilakukan dari hasil tahapan *Examination* atau ekstraksi data *file Smartphone* dengan hasil yang didapatkan oleh peneliti bahwa *tools Wondershare Dr Fone* tidak dapat mengembalikan data *file* yang telah dihapus, hanya mengembalikan kontak, log panggilan dan pesan, sedangkan menggunakan *tools EaseUS Data Recovery* dapat mengembalikan *file* yang telah dihapus dan dapat dilakukan *Recovery*.

Tabel 2. Hasil Analisis *Tools* Forensik

Tools	***Excel***	***Image***	***Audio***	***Video***	***Zip***
Wondershare Dr Fone	*No*	*Yes*	*Yes*	*Yes*	*No*
EaseUS Data *Recovery*	*Yes*	*Yes*	*Yes*	*Yes*	*Yes*

Dari hasil analisis *tools forensic* pada data tabel diatas tersebut ada yang bisa membaca *file excel, image, audio, video* dan *zip* , yaitu menggunakan *tools EaseUS Data Recovery* sedangkan menggunakan *tools Wondershare Dr Fone* hanya dapat *membaca file image, file audio, dan file video sedangkan untuk file Excel* dan *zip* tidak dapat terbaca.

4.2.5 *Reporting*

Berdasarkan penelitian yang dilakukan terhadap kasus penghapusan berkas maka ditemukan bukti pada *Smartphone* berjenis *Android* dengan jenis *Smartphone* Oppo A37f dimana *Smartphone* tersebut merupakan barang bukti yang dapat dijadikan sebagai alat bukti digital dalam kasus penghapusan berkas, dari hasil investigasi *forensic* digital maka dilakukan tahapan identifikasi untuk mengidentifikasi masalah yang terjadi, mengumpulkan barang bukti sebagai pemeriksaan terhadap barang bukti yang ditemukan, penyelidikan dilakukan untuk mencari dan menemukan bukti bukti digital tersebut, analisis barang bukti

tersebut dilakukan untuk mendapatkan suatu kesimpulan dari barang bukti yang telah didapatkan dan dilakukan pengembalian data atau *Recovery* pada alat bukti yang ditemukan pada kasus penghapusan berkas.

Tabel 3. Hasil *Reporting Tools* Forensik

Bukti Digital	***Data Smartphone***	***Wondershare Dr Fone***	***EaseUs Data Recovery***
xcel	*9*	*0*	*9*
Image	*7*	*7*	*7*
Audio	*10*	*10*	*10*
Video	*2*	*2*	*2*
Zip	*2*	*0*	*2*
Total	*30*	*19*	*30*

Perbandingan hasil terhadap kedua *tools* diatas menggunakan *Wondershare Dr Fone* dan *EaseUS Data Recovery* dalam mengembalikan data yang terhapus yaitu *Wondershare Dr Fone* memiliki hasil 63,3% dalam upaya untuk mengembalikan *file* atau data yang terhapus, sedangkan untuk *tools EaseUS Data Recovery* mencapai hasil 100% karena dapat mengembalikan *file* atau data yang terhapus secara menyeluruh sehinggga setelah dilakukan Analisa hingga pelaporan didapatkan *tools EaseUS Data Recovery* memiliki hasil yang lebih maksimal.

Hasil ini didapatkan mengunakan perhitungan sebagai berikut

Wondershare Dr Fone :

Perhitungan hasil $\frac{19}{30}$ X $100\% = 63{,}3\%$

EaseUS Data Recovery :

Perthitungan hasil $\frac{30}{30}$ X $100\% = 100\%$

5. Kesimpulan dan Saran

5.1 Kesimpulan

1. Proses Investigasi *Mobile forensic* dilakukan dengan melakukan indentifikasi masalah, melakukan pengumpulan alat bukti, melakukan penyidikan, melakukan analisis setelah didapatkan hasil, dan dilakukan *Reporting* terhadap barang bukti yang ditemukan. Pada penelitian ini didapatkan hasil pada *tools EaseUS Data Recovery* memiliki hasil yang lebih maksimal dibandingan dengan *tools Wondershare Dr Fone* berdasarkan hasil perhitungan data yang berhasil dikembalikan yaitu *Wondershare Dr Fone*

mendapatkan hasil 63% sedangkan untuk *EaseUS Data Recovery* mendapatkan hasil 100% dalam penelitian yang dilakukan.

2. Pada penelitian yang dilakukan *tools EaseUS Data Recovery* dapat mengembalikan *file* atau data terhapus dengan baik berdasarkan data yang berisi 30 variabel data dan dapat dikembalkan 30 variabel data, hasil yang didapat lebih maksimal dibandingkan dengan *tools Wondershare Dr Fone* yang hanya dapat mengembalikan 19 variable data dari total 30 data yang ada.
3. Bukti digital merupakan suatu hal penting dalam mengungkap sebuah kasus kejahatan, karena setiap Tindakan kejahatan memiliki jejak digital sehingga digital *forensic* dapat digunakan untuk membantu membuktikan suatu kasus kejahatan.

5.2 Saran

1. Untuk penelitian lebih lanjut diharapkan dapat menggunakan *tools forensic* lainya seperti Tenorshare UltData for *Android* dan masih banyak lagi dan metode lain seperti metode NIST dan masih banyak lagi sebagai penunjang atau untuk melengkapi penelitian sebelumnya untuk mendapatkan hasil terbaik.
2. Masih banyak *tools* yang dapat diexplore dan digunakan untuk penelitian berikutnya, untuk penggunaan *tools* yang berbeda diharapkan memberikan banyak informasi karena setiap *tools* yang berbeda akan memberikan hasil yang berbeda, karena setiap *tools* memliki kekurangan dan kelebihan masing-masing *tools* tersebut.

Referensi

[1] Ahmadi, ahwan, Akbar, T., & Mandala Putra, H. (2021). Perbandingan Hasil *Tool* Forensik Pada *File* Image *Smartphone Android* Menggunakan Metode Nist. JIKO (Jurnal Informatika Dan Komputer), 4(2), 92–97. https://doi.org/10.33387/jiko.v4i2.2812

[2] [2]Angamutu, K. A., Rahman, N. A. A., & Suki, N. N. A. N. (2020). A Customized Data *Recovery Tool*. Journal of Physics: Conference Series, 1712(1). https://doi.org/10.1088/1742-6596/1712/1/012019

[3] [3]Aziz, M. A., Riadi, I., & Umar, R. (2018). 2616-6260-1-Sm. Seminar Nasional Informatika UPN "Veteran" Yogyakarta, 2018(November), 51–57.

[4] Ikhsani, S., & Hidayanto, B. C. (2016). Analisa Forensik Whatsapp dan LINE Messenger Pada *Smartphone Android* Sebagai Rujukan Dalam Menyediakan Barang Bukti yang Kuat dan Valid di Indonesia. Jurnal Teknik ITS, 5(2). https://doi.org/10.12962/j23373539.v5i2.17271

[5] Madiyanto, S., Mubarok, H., & Widiyasono, N. (2017). *Mobile Forensic*s Investigation Proses Investigasi *Mobile Forensic*s Pada *Smartphone* Berbasis IOS. Jurnal Rekayasa Sistem & Industri (JRSI), 4(01), 93–98. https://doi.org/10.25124/jrsi.v4i01.149

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

[7] Riadi, I., Sunardi, S., & Sahiruddin, S. (2019). Analisis Forensik *Recovery* pada *Smartphone Android* Menggunakan *Metode National Institute of Justice* (NIJ). Jurnal Rekayasa Teknologi Informasi (JURTI), 3(1), 87. https://doi.org/10.30872/jurti.v3i1.2292

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

[9] Riadi, I., Umar, R., & Nasrulloh, I. M. (2018). Analisis Forensik Digital Pada Frozen Solid State *Dr*ive 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

[10] Riadi, I., Yudhana, A., & Barra, M. Al. (2021). Forensik *Mobile* pada Layanan Media Sosial LinkedIn. JISKA (Jurnal Informatika Sunan Kalijaga), 6(1), 9–20. https://doi.org/10.14421/jiska.2021.61-02

[11] Saad, S. K., Umar, R., Fadlil, A., Ahmad, U., Jl, D., & Soepomo, S. H. (2020). Analisis Forensik Aplikasi *Dr*opbox pada *Android* menggunakan Metode NIJ pada Kasus Penyembunyian Berkas. Jurnal Sains Komputer & Informatika (J-SAKTI, 4(September), 293.

[12] Santoso, M. H., Girsang, N. D., Siagian, H., Wahyudi, A., & Sitorus, B. A. (2019). Perbandingan Algoritma Kriptografi *Hash* MD5 dan SHA-1. Seminar Nasional Teknologi Informatika, 2(1), 54–59