Forensik Metadata Foto Sebagai Alat Bukti Digital

Forensic Photo Metadata As Digital Evidence Tool

Andria*[1], Saifulloh[2]
[1,2] *Universitas PGRI Madiun*
[1, 2] *Madiun, Indonesia*
e-mail: ***[1]andria@unipma.ac.id**, [2]saifulloh@unipma.ac.id

Abstrak – Forensik metadata foto merupakan suatu upaya pendekatan ilmiah dalam menemukan, mengidentifikasi beragam informasi yang terkandung pada sebuah foto. Perkembangan teknologi fotografi dan aplikasi editing foto tentu dapat memudahkan dalam melakukan manipulasi pada sebuah foto, sehingga tidak menutup kemungkinan terjadi adanya insiden siber yang memanfaatkan media foto untuk menyebarkan berita bohong maupun kejahatan dunia maya lainnya yang dapat merugikan suatu pihak. Metadata merupakan informasi terstruktur yang mendeskripsikan, menemukan, menjelaskan serta menjadikan suatu informasi tersebut menjadi mudah untuk ditemukan kembali. Sedangkan forensik digital merupakan salah satu cabang ilmu forensik, terutama untuk penyelidikan dan penemuan konten perangkat digital yang dapat dijadikan sebagai alat bukti dalam menemukan dan mengumpulkan barang bukti dalam suatu kejahatan siber. Penelitian ini bertujuan untuk melakukan forensik digital terhadap suatu foto dengan menggunakan Exiftool yang merupakan salah satu alat analisis forensik yang dapat digunakan untuk menampilkan metadata dari sebuah foto, sehingga dari informasi yang didapatkan bisa dijadikan sebagai alat bukti apabila diperlukan dalam suatu persidangan.

Kata kunci – Digital, Exiftool, Forensik, Metadata

Abstract - Forensic photo metadata is an attempt of a scientific approach in finding, identifying various information contained in a photo. The development of photography technology and photo editing applications can certainly make it easier to manipulate a photo, so it does not rule out the possibility of cyber incidents that use photo media to spread fake news or other cyber crimes that can harm a party. Metadata is structured information that describes, finds, explains and makes that information easy to find again. While digital forensics is a branch of forensic science, especially for the investigation and discovery of digital device content that can be used as evidence in finding and collecting evidence in a cyber crime. This study aims to perform digital forensics on a photo using Exiftool which is a forensic analysis tool that can be used to display metadata from a photo, so that the information obtained can be used as evidence if needed in a trial.

Keywords – Digital, Exiftool, Forensic, Metadata

I. PENDAHULUAN

Jumlah kasus kejahatan siber di Indonesia semakin marak, sebagai contoh sebaran isu hoaks di media sosial yang tentunya memerlukan penanganan khusus seperti pengajuan takedown maupun upaya penegakan hukum. Media yang digunakan dalam menyebar berita bohong atau hoaks tersebut diantaranya dengan menggunakan foto. Foto yang digunakan bisa saja foto asli dari sumbernya maupun foto yang telah disunting atau direkayasa dengan memberikan narasi yang berbeda dari faktanya yang kemudian diupload ke media sosial maupun dikirimkan atau ditransmisikan secara digital. Berdasarkan data Kominfo [1], penanganan sebaran isu hoaks dan pengajuan takedown sebaran hoaks Covid-19 di Media Sosial periode 23 Januari 2020 hingga 18 April 2021 dapat ditunjukkan pada gambar 1 sebagai berikut.

Gambar 1. Penanganan Sebaran Isu Hoaks dan Pengajuan Takedown Sebaran Hoaks Covid-19 di Media Sosial [1]

Diperlukan alat bukti yang tepat dalam menangani kasus insiden siber tersebut dalam proses peradilan, sebagaimana dicontohkan media yang digunakan untuk menyebar isu hoaks apabila menggunakan foto maka diperlukan analisis forensik mengenai metadata foto tersebut. Metadata merupakan informasi terstruktur yang mendeskripsikan, menemukan, menjelaskan serta menjadikan suatu informasi tersebut menjadi mudah untuk ditemukan kembali. Sedangkan forensik digital merupakan salah satu cabang ilmu forensik, terutama untuk penyelidikan dan penemuan konten perangkat digital yang dapat dijadikan sebagai alat bukti dalam menemukan dan mengumpulkan barang bukti dalam suatu kejahatan siber.

Penelitian ini bertujuan untuk melakukan forensik digital terhadap suatu foto dengan menggunakan *Exiftool* yang merupakan salah satu alat analisis forensik yang dapat digunakan untuk menampilkan *metadata* dari sebuah foto, sehingga dari informasi berupa *metadata* yang didapatkan bisa dijadikan sebagai alat bukti apabila diperlukan dalam suatu persidangan. Adapun perangkat yang digunakan pada penelitian ini yaitu *Smartphone* bersistem operasi *Android*. Penggunaan alat analisis forensik digital yaitu *Exiftool* dijalankan melalui aplikasi *Termux* yang dipasang pada *Smartphone*. *Termux* merupakan *terminal emulator* dan *environment* berbasis *Linux.* Hasil dari analisis forensik terhadap foto yang diuji dapat menampilkan *metadata* foto berupa informasi yang sangat detail mencakup hal-hal seperti tanggal dan waktu foto tersebut diambil, jenis kamera yang digunakan, resolusi gambar, dan dibeberapa hasil temuan dapat juga menampilkan lokasi dimana foto tersebut diambil serta beberapa informasi penting lainnya yang menyertai pada sebuah foto tersebut.

II. LANDASAN TEORI

Kejahatan siber atau yang dikenal dengan istilah *cybercrime* tentu menjadi suatu ancaman serius yang perlu diantisipasi dan ditangani dengan tepat [2]. 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 [3].

Metadata adalah informasi yang terstruktur yang menggambarkan, menjelaskan, menempatkan, atau membuat lebih mudah untuk mengambil, menggunakan, atau mengelola

sebuah sumber informasi. Metadata sering disebut data tentang data atau informasi tentang informasi. Selama ini fokus dari analisis forensik itu lebih banyak kepada menemukan file-file yang contennya itu sesuai dengan tujuan investigasi. Cara lain yang bisa dilakukan yaitu dengan melakukan pendekatan metadata, mengapa metadata karena metadata menyimpan informasi lain dari sebuah file. Apabila ini dilakukan, maka diharapkan proses ini bisa melihat langsung metadata file secara umum dan juga dapat menemukan file-file berdasarkan korelasi file dengan parameter dari metadata file tersebut. Cara ini umumnya belum terfasilitasi oleh alat-alat forensik yang ada, sehingga perlu dilakukan penelitian untuk melihat sejauh mana kemungkinan kemanfaatan metadata untuk mendukung proses investigasi digital [4].

Digital Forensik atau komputer forensik adalah penggunaan sekumpulan prosedur untuk melakukan pengujian secara menyeluruh suatu sistem komputer dengan mempergunakan *software* dan *tools* untuk mengekstrak dan memelihara barang bukti tindakan kiriminal [5]. Dilansir dari laman exiftool.org [6]. *Exiftool* merupakan aplikasi gratis (*open source*) yang dapat digunakan untuk membaca, menulis, dan melakukan manipulasi terhadap *metadata* dari berbagai macam file. *Exiftool* dapat dijalankan pada sistem operasi *Windows* maupun *MacOS*, baik dalam *library* untuk bahasa pemrograman Perl maupun sebagai tool yang dapat diakses melalui *command line interface.*

2.1. Penelitian Terdahulu

Berikut penelusuran berdasarkan penelitian terdahulu dapat ditunjukkan pada tabel 1 sebagai berikut:

Tabel 1. Penelitian Terdahulu

No	Judul	Tahun, Penulis	Metode	Hasil/Kesimpulan
1	Forensik Digital Sistem Informasi Berbasis Web	2021, Andria dan Sekreningsih Nita	*Metode Footprinting*	Berdasarkan hasil dan pembahasan, maka didapatkan kesimpulan bahwa aplikasi Maltego dapat digunakan untuk keperluan forensik digital pada suatu situs web dalam upaya mengumpulkan informasi dan memetakan jaringan komunikasi apa saja yang tekait didalamnya dengan melakukan teknik footprinting yang dapat ditentukan sesuai dengan kebutuhan. Adapun beberapa informasi yang dapat ditampilkan Maltego diantaranya seperti: nameserver, domain, block IP hosting, backend technology dan peta jaringan situs web [2]
2	Analisis Forensik Recovery pada Smartphone Android Menggunakan Metode National Institute Of Justice (NIJ)	2019, Imam Riadi, Sunardi dan Sahiruddin	*Metode National Institute of Justice (NIJ)*	Data yang telah dihapus pada perangkat smartphone android masih dapat dikembalikan menggunakan tool Wondershare dan Bekasoft. Tool forensik yang digunakan tidak cukup baik untuk mengembalikan data

No	Judul	Tahun, Penulis	Metode	Hasil/Kesimpulan
				gambar, video dan file dokumen. 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 [3]
3	Metadata Forensik Untuk Mendukung Proses Investigasi Digital	2017, Moh. Subli, Bambang Sugiantoro dan Yudi Prayudi	*Korelasi File Metadata Forensik*	Setelah melakukan korelasi metadata file, dapat ditemukannya file-file yang ada didalam komputer dari hasil pencarian korelasi berdasarkan parameter dari Metadata File Date, Size, File Type dan Owner yang ditampilkan dengan Value File Name, Size, Date dan Path [4]
4	Analisis Forensik Deteksi Keaslian Metadata Video Menggunakan Exiftool	2018, Alfiansyah Imanda Putra, Rusydi Umar, Abdul Fadlil	*Metode Processing Exiftool*	Setelah melakukan beberapa hal, terkait dengan perancangan deteksi dan analisis deteksi keaslian metadata pada video. konsep dasar dalam melakukan analisis deteksi video ini adalah dengan membuat sample video editing, dimana sample video editing digunakan untuk membandingkan metadata rekaman video asli dan kemudian selanjutnya tahap Processing Exiftool, dimana tahap ini adalah proses membaca metadata video dengan exiftool dan tahap akhir adalah analisa hasil metadata [5]
5	Analisis Image Forensic Dalam Mendeteksi Rekayasa File Image Dengan Metode Nist	2021, Muhammad Rizky Al-Fajri, Caruddin, Dadang Yusup	*Metode NIST (Nasional Institute of Standart and Technology)*	Dari dua foto yang dijadikan barang bukti ditemukan bahwa salah satu dari kedua foto tersebut merupakan hasil rekayasa. Dari kedua foto tersebut dilakukan scan dengan Jpegsnoop dan didapatkan metadata dari kedua foto tersebut. Setelah diketahui metadata dari kedua

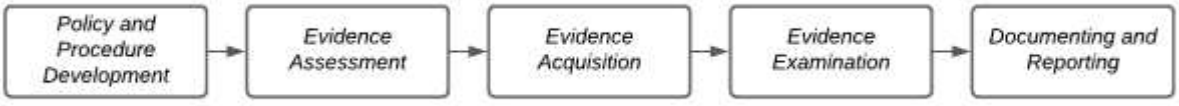
No	Judul	Tahun, Penulis	Metode	Hasil/Kesimpulan
				foto tersebut dilanjutkan dengan analisis tingkat error atau error level analysis dengan menggunakan tools bantuan yaitu Forensically beta [7]
6	Deteksi Pemalsuan Foto Digital Menggunakan Image Forensics	2019, Imam Riadi, Anton Yudhana dan Wicaksono Yuli Sulistyo	*Metode Forensik Citra Digital*	Tools yang sudah digunakan dari ketiga tools dapat memberikan hasil pendeteksian. Komparasi ketiga tools berhasil dilakukan dengan masing-masing analisis yang sudah berjalan, sehingga didapat hasil pendeteksian foto. Bahan foto yang digunakan masih menggunakan foto asli dan foto manipulasi yang diedit dari foto asli, bukan dari foto yang sudah beredar di media sosial dan internet [8]

III. METODE

Bahan dan alat yang digunakan pada penelitian ini dapat dirinci sebagai berikut:

1. Satu unit *Smartphone* bersistem operasi *Android*
2. Aplikasi *Termux* sebagai *terminal emulator* dan e*nvironment* berbasis *linux* untuk dapat menjalankan *Exiftool*
3. *Exiftool* merupakan salah satu alat analisis forensik yang dapat digunakan untuk menampilkan *metadata* dari sebuah foto
4. Koneksi internet untuk melakukan *update* dan *upgrade* maupun paket instalasi yang diperlukan untuk menjalankan *Exiftool* di aplikasi *Termux*

Penelitian ini menggunakan metode analisa forensik dari *National Institute of Justice (NIJ).* Metode ini untuk menjelaskan bagaimana tahapan penelitian yang akan dilakukan sehingga dapat diketahui alur dan langkah-langkah penelitian secara sistematis sehingga dapat dijadikan pedoman dalam menyelesaikan permasalahan yang ada [9]. Berdasarkan dokumen *National Institute of Justice (NIJ),* terdapat 5 tahapan dalam menangani dan mengidentifikasi bukti digital terkait dengan aktivitas forensik digital (digital forensic), seperti yang ditunjukkan pada gambar 1 sebagai berikut:



Gambar 2. Tahapan Forensik Digital Berdasarkan Dokumen NIJ

Pada gambar 2 dapat dijelaskan bahwa 5 tahapan forensik digital tersebut masing-masing dapat diuraikan sebagai berikut:

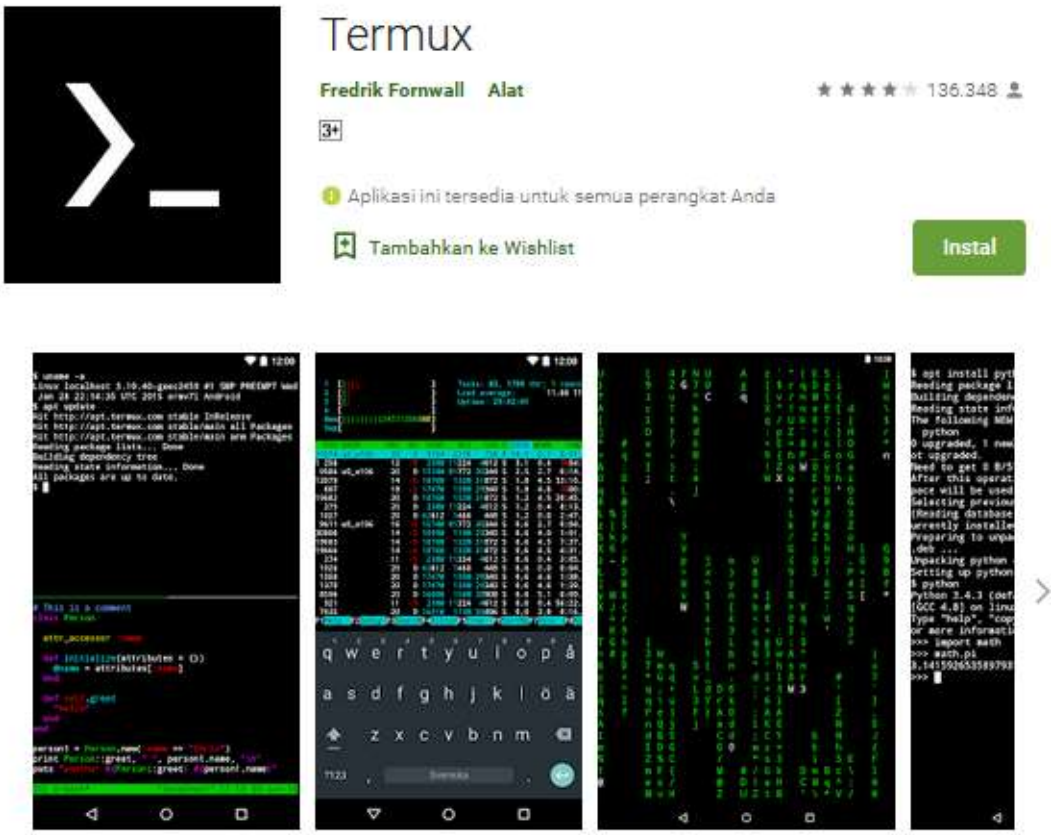
1. *Policy and Procedure Development*
   Memahami prosedur dan kebijakan pengembangan terkait dengan aturan atau regulasi pada objek yang akan dilakukan forensik digital

2. *Evidence Assessment*
   Penilaian barang bukti yang dapat berupa data, informasi rekam jejak, alur dan lain sebagainya yang terkait dengan konten digital sebagai barang bukti
3. *Evidence Acquisition*
   Pengumpulan barang bukti dari hasil penilaian barang bukti yang dianggap relevan sesuai dengan yang akan dilakukan forensik digital.
4. *Evidence Examination*
   Pemeriksaan barang bukti dari hasil pengumpulan barang bukti
5. *Documenting and Reporting*
   Dokumentasi dan pelaporan dari hasil forensik digital [2]

IV. HASIL DAN PEMBAHASAN

Pada penelitian ini, forensik digital dilakukan menggunakan perangkat mobile yaitu *Smartphone* bersistem operasi *Android*, kemudian diperlukan instalasi aplikasi *Termux* untuk menjalankan *terminal emulator* agar dapat menjalankan *Exiftool* yang merupakan alat untuk melakukan analisa metadata pada foto atau gambar yang akan dilakukan forensik digital. Langkah awal yang perlu dilakukan yaitu melakukan instalasi aplikasi *Termux* di *smartphone* bersistem operasi *Android,* aplikasi *Termux* tersebut dapat diunduh secara gratis melalui *Play Store.* Selanjutnya setelah terinstall maka diperlukan *update* dan *upgrade packages* atau paket-paket yang dibutuhkan dengan mengetikkan perintah atau *command* di dalam aplikasi *Termux* [10].

Tampilan aplikasi *Termux* yang dapat diinstall melalui *Google Play Store* seperti ditunjukkan pada gambar 4 sebagai berikut.



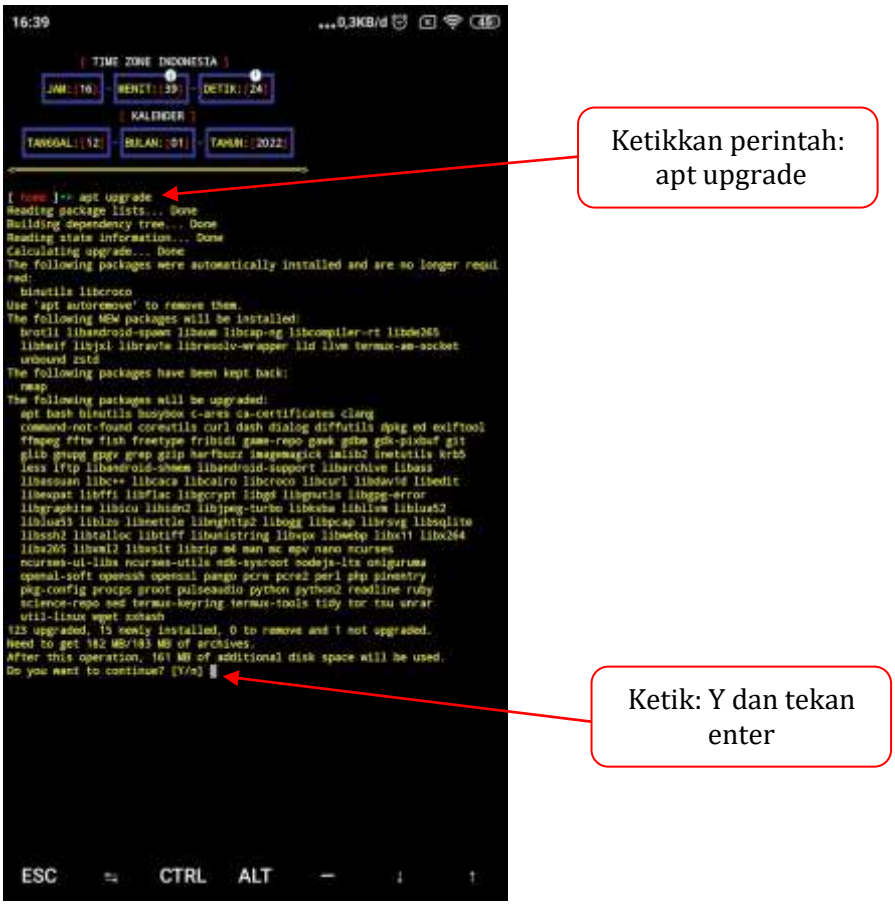
Gambar 4. Halaman *Termux* di *Google Play Store* [11]

Setelah aplikasi *Termux* selesai di install, kemudian perlu dilakukan *update* dan *upgrade packages* dengan cara mengetikkan perintah *apt update* dan *apt upgrade* melalui terminal pada aplikasi *Termux.* Hal tersebut diperlukan untuk memperbarui dan meningkatkan versi paket-paket yang terdapat pada repositori. Repositori merupakan lokasi penyimpanan yang berisikan

sekumpulan paket-paket program aplikasi untuk sebuah sistem operasi. Tampilan *update packages* seperti ditunjukkan pada gambar 5 sebagai berikut.

Gambar 5. Perintah *Update Packages* di *Termux*

Tunggu proses *update* tersebut hingga selesai, kemudian dapat dilanjutkan dengan melakukan perintah *upgrade packages.* Tampilan *upgrade packages* seperti ditunjukkan pada gambar 6 sebagai berikut.

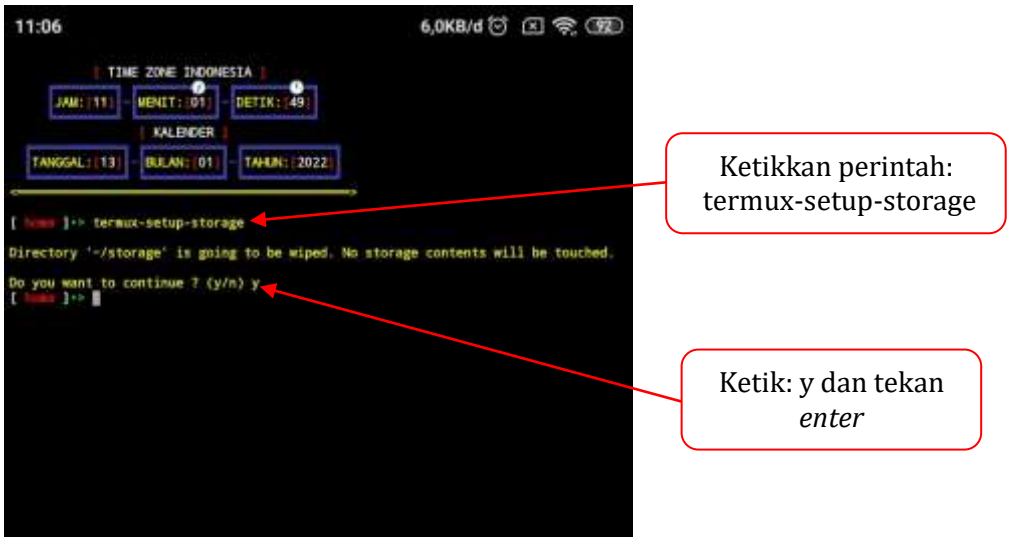


Gambar 6. Perintah *Upgrade Packages* di *Termux*

Ketik **Y** pada terminal untuk mengonfirmasi *upgrade* seperti yang ditunjukkan arah panah

pada gambar 6, kemudian tekan *enter* dan tunggu proses *upgrade packages* hingga selesai.

Selanjutnya, ketikan perintah *termux-setup-storage* untuk dapat mengakses *internal memory* atau *SDCARD* di *Termux.* Lebih jelasnya seperti yang ditunjukkan pada gambar 7 sebagai berikut.



Gambar 7. Perintah Akses *SDCARD* di *Termux*

Kemudian, ketikan perintah *pkg install exiftool* untuk menginstall paket program aplikasi *Exiftool.* Lebih jelasnya seperti yang ditunjukkan pada gambar 8 sebagai berikut.

Gambar 8. Perintah Instalasi *Exiftool* di *Termux*

Selanjutnya, setelah proses instalasi *exiftool* selesai maka forensik digital pada metadata foto dapat mulai dilakukan. Pada penelitian ini dicontohkan dua buah file foto yang terdiri dari:

1. Satu foto yang diambil dengan kamera ponsel dengan kondisi file foto belum dilakukan *editing* sama sekali (*original*)
2. Satu foto yang sudah dilakukan proses *editing* (foto editan)

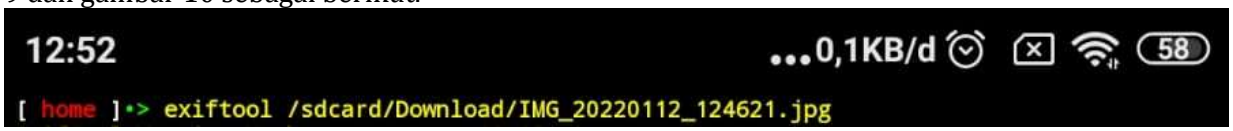
Lebih jelasnya, kedua file foto tersebut seperti ditunjukkan pada tabel 1 sebagai berikut.

Tabel 1. Foto *Original* dan Foto *Editing*

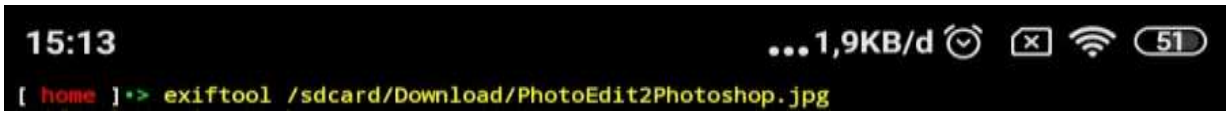
No	Keterangan	
	Foto Original	**Foto Editan**
1		
	IMG_20220112_124621.jpg	PhotoEdit2Photoshop.jpg

Langkah berikutnya, ketikkan perintah pada *Termux* dengan format sebagai berikut:
exiftool /sdcard/NamaDirektori/NamaFile

Pada penelitian ini dicontohkan lokasi file foto berada pada direktori *Download* dengan file foto yang masih asli belum diedit atau *original* bernama **IMG_20220112_124621.jpg** sedangkan untuk nama file foto yang sudah diedit bernama **PhotoEdit2Photoshop.jpg**, sehingga perintah yang diketikkan pada *terminal* untuk memanggil fungsi *exiftool* disesuaikan dengan lokasi direktori atau folder dan nama file beserta ekstensinya seperti ditunjukkan pada gambar 9 dan gambar 10 sebagai berikut.



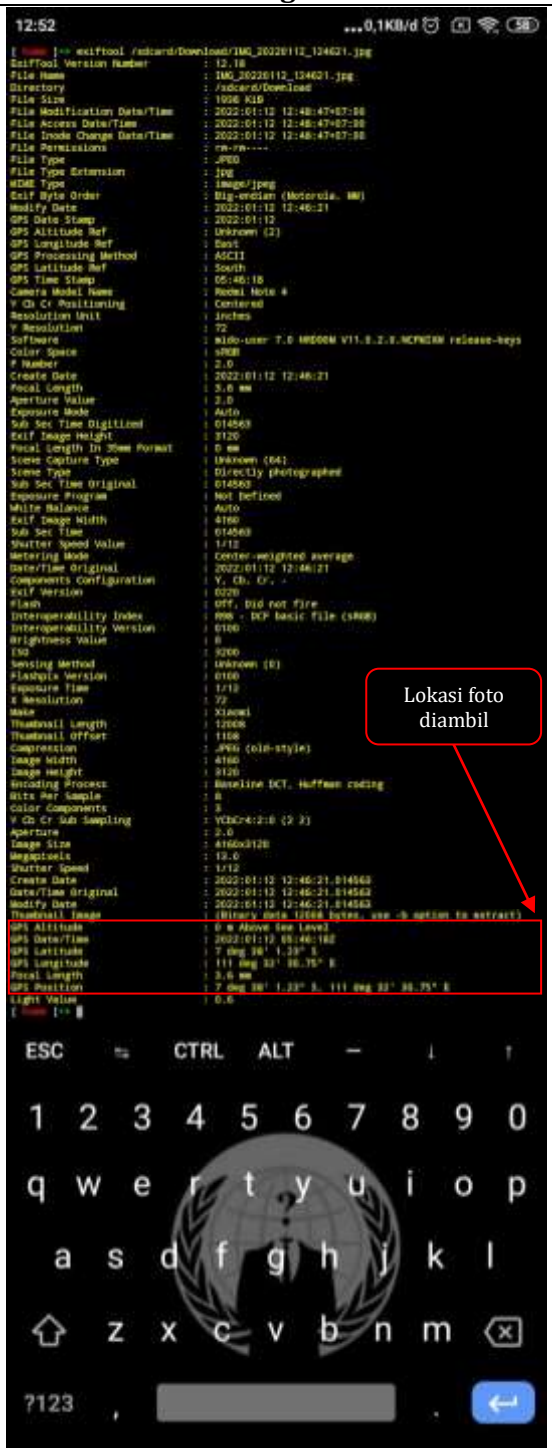
Gambar 9. Perintah untuk forensik *metadata* foto *original*



Gambar 10. Perintah untuk forensik *metadata* foto editan

Hasil dari forensik *metadata* pada kedua foto tersebut dapat ditunjukkan pada tabel 2 sebagai berikut:

Tabel 2. Hasil Forensik Metadata Foto

No	Keterangan	
	Foto Original	**Foto Editan**
1		

Berdasarkan hasil forensik metadata foto yang ditampilkan pada tabel 2 menunjukkan bahwa pada foto original maupun foto editan masing-masing mengandung informasi yang sangat detail, diantaranya seperti ukuran file, tanggal, jam, ukuran panjang dan lebar foto, dan lain sebagainya. Menariknya, pada foto *original* menampilkan informasi lokasi dimana foto tersebut diambil. Sedangkan pada foto editan menampilkan informasi mengenai nama aplikasi *editing* foto yang digunakan.

V. KESIMPULAN

Pada setiap file foto yang dihasilkan oleh kamera digital, seperti misalnya hasil foto dari ponsel masing-masing memiliki informasi lain selain informasi berupa nama, ukuran dan ekstensi file. Informasi tersebut adalah *exif (exchangeable image file format)* atau lebih dikenal dengan sebutan *metadata*. Pada penelitian ini, dapat ditunjukkan hasil bahwa forensik *metadata* pada sebuah foto dapat dilakukan dengan perangkat S*martphone* dengan menginstall aplikasi *Termux* untuk menjalankan program bernama *Exiftool* yang digunakan untuk melihat *metadata* pada sebuah foto. Hasil yang didapat menampilkan beragam informasi, diantaranya seperti nama, ukuran dan ekstensi file, panjang dan lebar ukuran foto, tanggal dan jam, lokasi foto hingga aplikasi *editing* yang digunakan. Hasil dari forensik *metadata* foto tersebut dapat digunakan sebagai alat bukti dipersidangan misalnya ketika terjadi suatu kasus atau tindak pidana dengan barang bukti berupa file foto.

DAFTAR PUSTAKA

[1] Kominfo, "Penanganan Sebaran Isu Hoaks Covid-19 Minggu (18/04/2021)," *Kementerian Komunikasi dan Informatika*, 2018. https://www.kominfo.go.id/content/detail/33952/penanganan-sebaran-isu-hoaks-covid-19-minggu-18042021/0/infografis.

[2] Andria dan S. Nita, "FORENSIK DIGITAL SISTEM INFORMASI BERBASIS WEB," *J. Ahli Muda Indones.*, vol. 2, 2021, [Online]. Available: https://journal.akb.ac.id/index.php/jami/article/view/73.

[3] I. Riadi, S. Sunardi, and S. Sahiruddin, "Analisis Forensik Recovery pada Smartphone Android Menggunakan Metode National Institute Of Justice (NIJ)," *J. Rekayasa Teknol. Inf.*, vol. 3, no. 1, pp. 87–95, 2019.

[4] B. S. dan Y. P. M. Subli, "METADATA FORENSIK UNTUK MENDUKUNG PROSES INVESTIGASI DIGITAL," *J. Ilm. DASI*, vol. 18, pp. 44-50, 2017.

[5] R. U. dan A. F. A. I. Putra, "ANALISIS FORENSIK DETEKSI KEASLIAN METADATA VIDEO MENGGUNAKAN EXIFTOOL," *", Semin. Nas. Inform.*, 2018.

[6] Https://exiftool.org/, "Exiftool." .

[7] C. dan D. Y. M.R. Al-Fajri, "Analisis Image Forensic Dalam Mendeteksi Rekayasa File Image Dengan Metode Nist," *J. Sist. dan Teknol. Inf.*, vol. 6, 2021.

[8] A. Y. dan W. Y. S. I. Riadi, "DETEKSI PEMALSUAN FOTO DIGITAL MENGGUNAKAN IMAGE FORENSICS," *J. Mob. Forensics*, vol. 1, 2019.

[9] I. Riadi, R. Umar, and I. M. Nasrulloh, "Analisis Forensik Digital Pada Frozen Solid State Drive Dengan Metode National Institute of Justice (Nij)," *Elinvo (Electronics, Informatics, Vocat. Educ.*, vol. 3, no. 1, pp. 70–82, 2018.

[10] W. A. Andria;Ningrum and I. Mubarok, "PENGUJIAN KEAMANAN BASIS DATA SISTEM INFORMASI BERBASIS WEB," *Pros. SNAST*, pp. 66–74, 2021.

[11] Termux, "Termux on Google Play Store," *Google Play Store*. https://play.google.com/store/apps/details?id=com.termux.

.