MENGUNGKAP DAN MENGUJI KEASLIAN BUKTI DIGITAL PADA KEJAHATAN *CYBERCRIME* DENGAN METODE *DIGITAL FORENSIC RESEARCH WORKSHOP*

Imam Wahyudi[1], Arif Muntasa[2], Muhammad Yusuf[3], Ardi Hamzah[4]
[1,2,3,4]Magister Akuntansi, Fakultas Ekonomi dan Bisnis, Universitas Trunojoyo Madura
[1]hectorsmaga@gmail.com, [2]arifmuntasa@trunojoyo.ac.id, [3]muhammadyusuf@trunojoyo.ac.id, [4]ardihamzah@trunojoyo.ac.id

ABSTRAK

Bukti pada dasarnya memiliki dua jenis yaitu digital dan fisik. Dimana bukti digital memiliki karakteriskti kerentanan, mudah dihapus, dihilangkan, serta diubah oleh karena itu perlu sebuah cara khusus dalam penanganan bukti digital berkaitan dengan maraknya cyber crime. Salah satu kasus mengenai cyber crime adalah berita hoax yang disajikan dengan gambar ataupun informasi yang sudah direkayasa sehingga diperlukan pencegahan dan investigasi lebih lanjut.Artikel ini bertujuan untuk mengungkap bukti yang dihapus pada direktori flashdisk dan menguji keaslian bukti tersebut dengan menggunakan metode *Digital Forensic Research Workshop* (DFRWS). Alat analisis yang digunakan menggunakan *Forensic Tool Kit* (FTK) *Imager* yang memiliki fungsi untuk me*recovery* file yang telah dihapus dan JPEGSNOOP memiliki fungsi untuk mendeteksi dan menguji apakah gambar atau foto tersebut original atau telah dilakukan rekayasa. Hasil dari penelitian ini menunjukkan bahwa pengujian dan validasi mengenai bukti digital berupa gambar mendapatkan hasil yang baik yaitu bukti dapat ditemukan dan dikembalikan dengan bentuk yang sama serta telah didapatkan informasi mengenai originalitasnya.

Kata kunci: *Digital Forensic*, DFRWS, FTK Imager, JPEGSNOOP

ABSTRACT

Evidence basically has two types namely digital and physical. Digital evidence has characteristic vulnerabilities, it is easy to delete, delete, and change, therefore it needs a special way to handle digital evidence related to the rise of cyber crimes. One of the cases regarding cyber crime is hoax news which is presented with images or information that has been engineered so that prevention and further investigation are needed. This article aims to reveal evidence that was deleted in the flash directory and test the authenticity of the evidence using the Digital Forensic Research Workshop method. (DFRWS)). The analysis tool used uses the Image Forensic Tool Kit (FTK) which has a function to recover deleted files and JPEGSNOOP has a function to detect and test whether the image or photo is original or has been engineered. The results of this study indicate that testing and validation of digital evidence in the form of images get good results, namely evidence can be found and returned in the same form and information about its originality is obtained.

Keywords: *Digital Forensics, DFRWS, FTK Imager, JPEGSNOOP*

1. LATAR BELAKANG

Teknologi informasi memiliki dampak yang cukup signifikan terhadap perkembangan hukum. Salah satu implikasi adalah diakuinya keberadaan bukti elektronik dalam pembuktian di persidangan, baik dalam perkara pidana, perdata maupun perkara lainnya. Di Indonesia, bukti elektronik diperkenalkan pada 2001 Dengan munculnya bukti elektronik dalam Pasal 26A UU No. 20 Tahun 2001 tentang Perubahan Atas UU No. 31 Tahun 1999 tentang Pemberantasan Tindak Pidana Korupsi [1]. Sejak saat itu hampir seluruh undang-undang yang di dalamnya mengatur hukum acara juga memuat aturan yang mengakui dapat digunakannya bukti elektronik sebagai bukti dalam persidangan, terlebih dengan diundangkannya Undang-undang No. 11 Tahun 2008 tentang Informasi dan Transaksi Elektronik [2].

Bukti elektronik identic dengan kejahatan cybercrime, salah satu kejahatan yang sedang marak adalah berita hoax dimana tahun 2020 Polda Metro Jaya telah menangani sebanyak 443 kasus *hoax* dan *hate speech* serta 1.448 akun media sosial telah dilakukan *take down.* Berita *hoax*

biasanya disajikan dalam rekayasa gambar atau informasi yang tidak benar dengan cara memfitnah seseorang, organisasi maupun instansi negara akan berurusan dengan hukum hal ini telah diatur dalam UU ITE [3]. Bukti elektronik merupakan data yang tersimpan dan/atau ditransmisikan melalui sebuah perangkat elektronik, jaringan, atau sistem komunikasi. Data inilah yang dibutuhkan untuk membuktikan sebuah kejahatan yang terjadi di persidangan, bukan bentuk fisik dari perangkat elektroniknya [4]. Karakteristik dari bukti elektronik diantarnya membutuhkan alat khusus untuk melihat/ membacanya, yang terdiri dari perangkat keras (hardware) dan perangkat lunak (software) dan Bersifat rentan (fragile) yaitu mudah diubah, dimanipulasi serta dimusnahkan. Atas kerentanan tersebut diperlukan sebuah penanganan khusus dalam mengelola bukti elektronik [5].

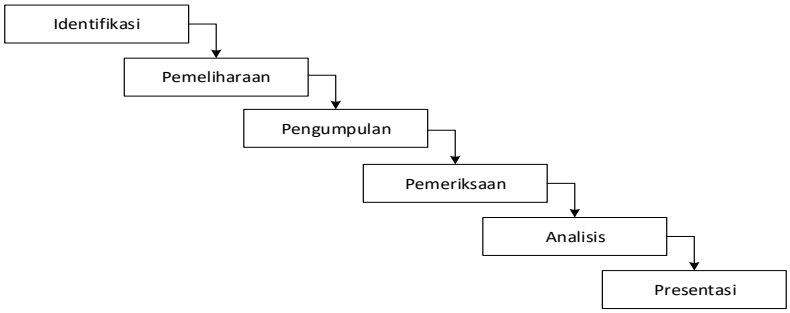
Atas kerentanan bukti digital tersebut, pelaku cyber crime dapat menghindar atau lolos dari kasus yang menjeratnya dengan cara mengubah dan melenyapkan bukti yang dimilikinya hal ini disebut dengan tindakan anti fraud, Tindakan anti fraud menurut investigator digital, anti forensik dapat menghambat pengumpulan bukti, memperpanjang waktu penyelidikan, bukti yang tidak bisa dipastikan keamanannya dapat membahayakan penyelidikan, serta menghalangi deteksi kejahatan digital [6].

Pentingnya permasalahan cybercrime diperlukan sebuah panduan tentang teknik investigasi sehingga cara, proses dan pembuktiannya dihasilkan secara ilmiah [7]. Factor penting dalam menangani cybercrime diperlukan kerangkan kerja atau *framework* supaya proses investigasi tindak kejahatan cybercrime lebih efektif dan efisien [8]. Beberapa *framework* forensik yang telah banyak digunakan untuk menginvestigasi kasus digital forensik diantaranya National Institute of Justice (NIJ) [9], Digital Forensics Research Workshop (DFRWS) [10], National Institute of Standard and Technology (NIST), Digital Forensics Investigation Framework (DFIF) [11], dan Generic Computer Forensic Investigation Model (GCFIM) [12] [13]

Penelitian ini untuk mengungkap bukti menggunakan metode framework DFRWS dan melakukan ekstraksi file yang telah disisipi pesan steganografi. DFRWS dipilih karena memiliki kerangka forensik standar dan konsisten yang dapat memberikan kemudahan dalam penggunaan serta mudah dipahami oleh pengguna teknis ataupun non-teknis. Sedangkan untuk validasi bukti, akan menggunakan software JPEGSNOOP untuk mengetahui keaslian bukti, yang diungkap, software ini dipilih karena memberikan hasil analisis atas gambar yang akan dijadikan sebagai bukti serta proses dan penggunaannya mudah untuk dipahami.

2. METODE PENELITIAN

Penelitian ini menggunakan metode *live forensic* yang dibuat oleh *Digital Forensics Research Workshop* dengan analisis data menggunakan FTK Imager. Metode DFRWS membantu mendapatkan bukti dan mekanisme terpusat untuk merekam informasi yang dikumpulkan.



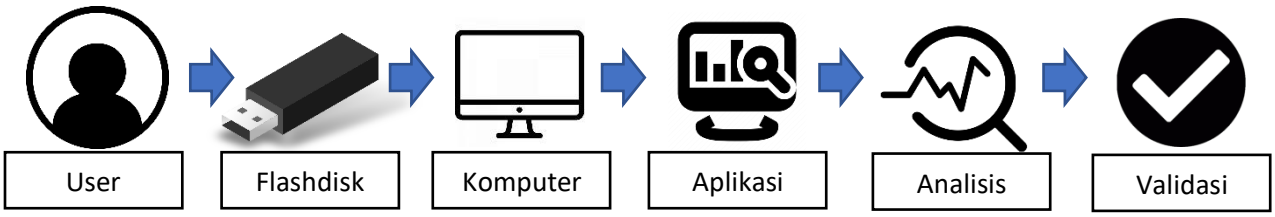
Gambar 1 Tahapan metode DFRWS

Gambar 1 menunjukkan tahapan yang dilakukan berdasarkan metode yang digunakan yaitu DFRWS (Digital Forensics Research Workshop). Pemaparannya adalah sebagai berikut:

A. Identifikasi (*Identification*)
   Identifikasi dilakukan untuk melakukan penentuan kebutuhan yang diperlukan pada penyelidikan dan pencarian bukti.
B. Pemeliharaan (*Preservation*)
   Pemeliharaan dilakukanan untuk menjaga bukti digital agar memastikan keaslian bukti dan membantah klaim bukti telah dilakukan sabotase.
C. Pengumpulan (*Collection*)
   Pengumpulan merupakan tahap untuk melakukan identifikasi bagian tertentu dari bukti digital dan melakukan identifikasi sumber data
D. Pemeriksaan (*Examination*)
   Pemeriksaan dilakukan untuk menentukan filterisasi data pada bagian tertentu dari sumber data, filterisasi data dilakukan dengan melakukan perubahan bentuk data namun tidak melakukan perubahan pada isi data karena keaslian data merupakan hal yang sangat penting.
E. Analisis (*Analysis*)
   Analisis merupakan tahap untuk melakukan penentuan tentang dimana data tersebut dihasilkan, oleh siapa data tersebut dihasilkan, bagaimana data tersebut dihasilkan dan kenapa data tersebut dihasilkan
F. Presentasi (*Presentation*)
   Presentasi dilakukan dengan menyajikan informasi yang dihasilkan dari tahap analisis.

2.1 Simulasi Perancangan Sistem

Sebuah rancangan untuk mendapatkan suatu bukti digital untuk dilakukan analisis. Tahapan Gambar dibawah ini menjelaskan tentang rancangan yang digunakan dalam penelitian.



Gambar 2 Tahapan pengambilan bukti digital

Gambar 2 diatas menjelaskan mengenai langkah analisis pada *flashdisk* dimana pada langkah terakhir nanti akan mengeluarkan suatu data analisis dari perangkat lunak FTK imager dan diverivikasi oleh JPEGSNOOP. Penggunaan analisis forensik pada flashdisk atau komputer di butuhkan sebuah metode dan tools guna membantu peneliti guna mencari data untuk di investigasi forensik. Penelitian ini diawali dengan membuka isi dari flashdisk yang dianggap sebagai barang bukti, selanjutnya isi dari flasdisk tersebut dihapus permanen (SHIFT + Delete). Setelah itu melakukan pemilihan tools untuk mengambil data pada isi file flashdisk tersebut. Pada tahap analisis tools yang akan digunakan adalah FTK Imager yang berguna sebagai pencari data yang akan di analisis. Tahap selanjutnya mencari nilai hash data fungsi nya yaitu

meyakinkan bahwa file tersebut akan menjadi nilai yang merepresentasikan string asli atau akun asli. Pengecekan barang bukti untuk menguji validitasnya di analisis ulang dengan aplikasi JPEGSNOOP. Pada tahapan terakhir dilakukan reporting atau laporan hasil penelitian mengenai data pada *flashdisk* berupa barang bukti data yang valid pada media sosial tersebut, dalam reporting juga menjelaskan tahapan-tahapan atau proses yang digunakan untuk mendapatkan barang bukti yang dibutuhkan agar data tersebut terbukti asli atau valid.

2.2 Persiapan Alat dan Bahan

Alat yang digunakan pada penelitian ini disajikan pada tabel berikut:

No	Nama Alat	Spesifikasi	Keterangan
1	PC All In One	All In One HP 20, 4 GB DDR 3, Memory 500 GB	Perangkat Keras
2	Windows	Windows 8.1	Sistem Operasi
3	FTK Imager	Versi 3.0.0.1443	Tools Akuisisi
4	JPEGSNOOP	Versi 1.8.0	Tools Analisis

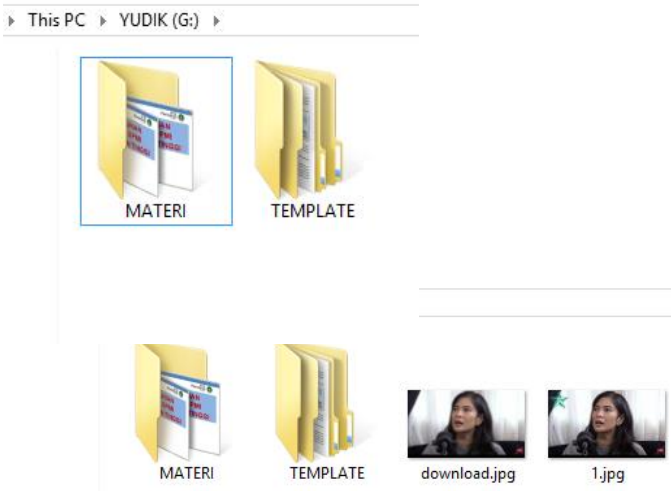
Bahan yang digunakan berupa stego text dan stego image yang telah dilakukan pengecekan nilai hash pada masing-masing file seperti ditampilkan pada tabel di bawah ini:

No	Nama File	Format	Nilasi Hash (MD5)
1	1	.jpg	E530323130357E314A5047200081006E

3. HASIL DAN PEMBAHASAN

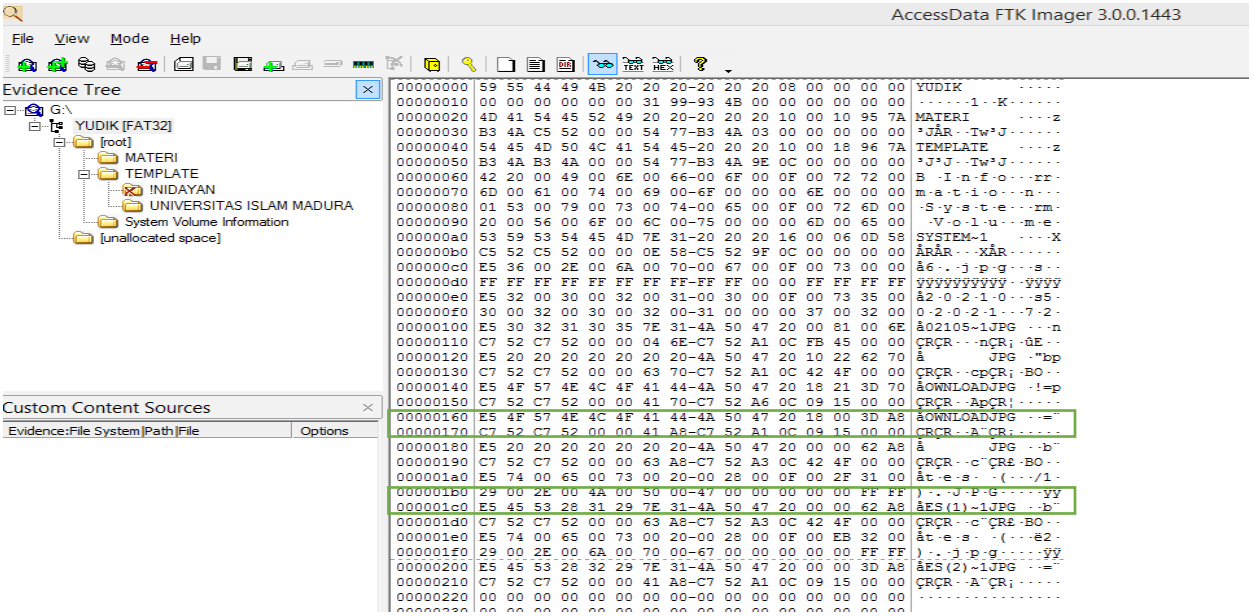
3.1 Analisis Bukti Digital

Analisis digital forensik memiliki cakupan yang cukup luas, sehingga dapat dikelompokan berdasarkan pada bentuk fisik maupun logis. Barang bukti yang dianalisis dengan cakupan komputer forensik yaitu, mobile forensik, audio forensik, video forensik, image forensik, dan cyber forensik. Dalam penelitian ini sendiri akan menggunakan image forensik, dimana forensik ini berkaitan dengan jenis barang bukti digital yang berupa file gambar digital [14]. Analisis bukti digital pada tahapan ini dilakukan identifikasi menggunakan metode analisis Digital Forensics Research Workshop dimana disimulasikan dengan file dari flashdisk dengan gambar berikut:



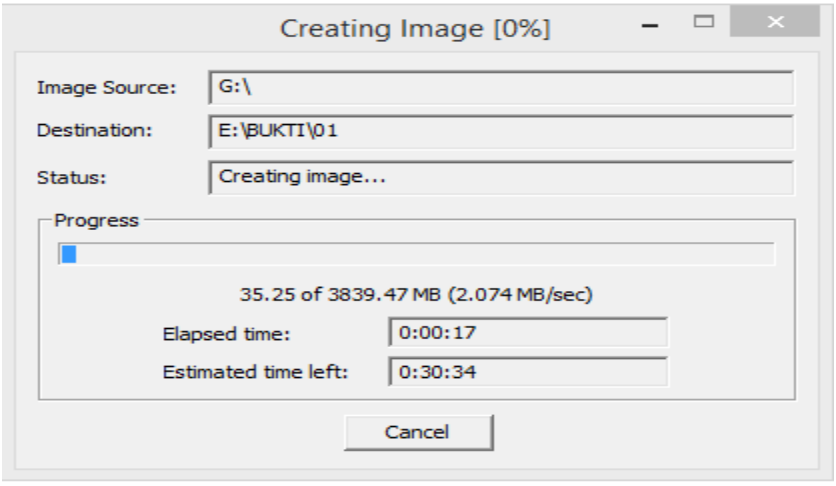
Gambar 3 File yang terdapat dalam *flashdisk*

Gambar 3 diatas menjelaskan bahwa isi file berupa dua gambar telah dihapus oleh pelaku dimana gambar tersebut sebagai barang bukti tindak kejahatan. Pengumpulan bukti digital selanjutnya adalah untuk menemukan barang bukti yang telah dihapus oleh pelaku dimana mencari pada flashdisk dengan menggunakan program FTK Imager, sehingga akan tampil sebagai berikut:



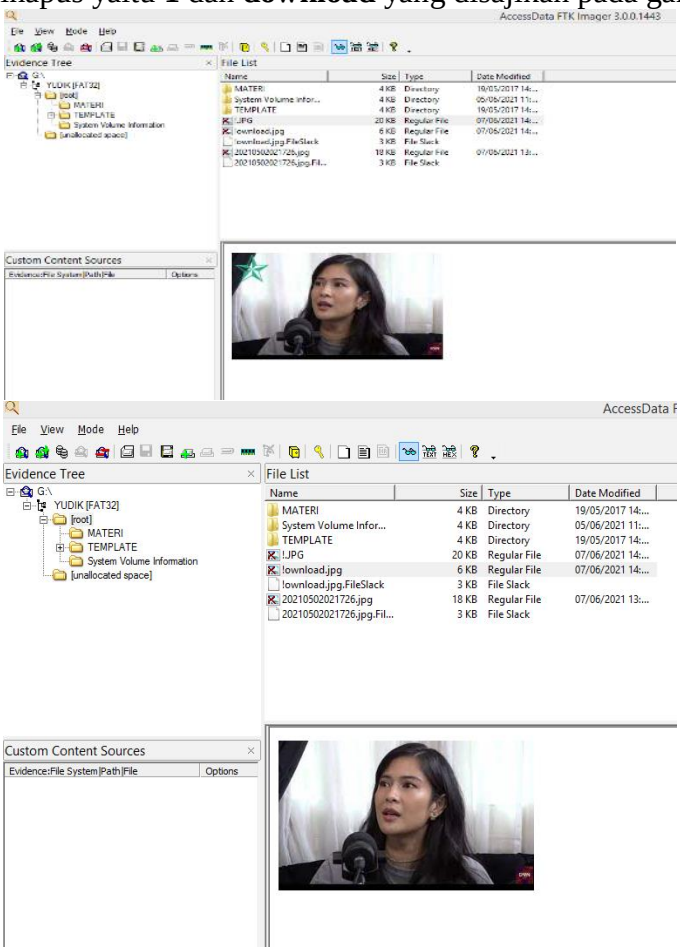
Gambar 4 Nilai hash file

Pada gambar 4 tersebut dapat diketahui kedua nilai hash file yang telah dihapus, kemudian dilakukan analisis untuk mengetahui isi dari file tersebut. Gambar berikut menjenlaskan proses creating image karena file yang dihapus berupa file gambar



Gambar 5 Proses *creating image*

Sehingga temuan hasil analisis yang telah dilakukan aplikasi FTK Imager ini, sesuai dengan nama file yang telah dihapus yaitu **1** dan **download** yang disajikan pada gambar berikut:

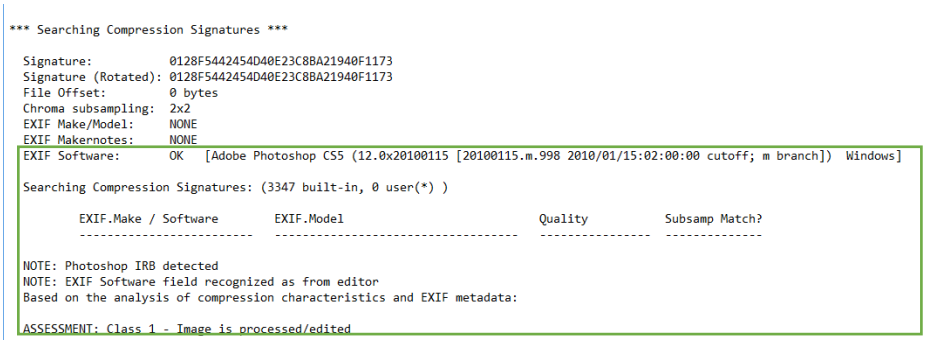


Gambar 6 Komparasi gambar

Selanjutnya, adalah melihat keaslian gambar yang telah diungkap dengan menggunakan tools JPEGSNOOP dengan hasil laporan dari analisis image yang disajikan pada gambar dibawah:

```
JPEGsnoop 1.8.0 by Calvin Hass
  http://www.impulseadventure.com/photo/
  ---------------------------------------

  Filename: [E:\1.jpg]
  Filesize: [20290] Bytes

Start Offset: 0x00000000
*** Marker: SOI (xFFD8) ***
  OFFSET: 0x00000000

*** Marker: APP1 (xFFE1) ***
  OFFSET: 0x00000002
  Length          = 4492
  Identifier      = [Exif]
  Identifier TIFF = 0x[4D4D002A 00000008]
  Endian          = Motorola (big)
  TAG Mark x002A  = 0x002A

  EXIF IFD0 @ Absolute 0x00000014
    Dir Length = 0x0007
    [Orientation                        ] = 1 = Row 0: top, Col 0: left
    [XResolution                        ] = 720000/10000
    [YResolution                        ] = 720000/10000
    [ResolutionUnit                     ] = Inch
    [Software                           ] = "Adobe Photoshop CS5 (12.0x20100115 [20100115.m.998 2010/01/15:02:00:00 cutoff; m branch])  Windows"
    [DateTime                           ] = "2021:06:07 14:03:00"
    [ExifOffset                         ] = @ 0x00EC
    Offset to Next IFD = 0x00000118

  EXIF IFD1 @ Absolute 0x00000124
    Dir Length = 0x0006
    [Compression                        ] = JPEG
    [XResolution                        ] = 72/1
    [YResolution                        ] = 72/1
    [ResolutionUnit                     ] = Inch
    [JpegIFOffset                       ] = @ +0x0176 = @ 0x0182
    [JpegIFByteCount                    ] = 0x[0000100E] / 4110
    Offset to Next IFD = 0x00000000
```

Gambar 7 Metadata gambar



Gambar 8 Hasil analisis

Hasil analisis dari tool JPEGSNOOP dapat diketahui bahwa gambar tersebut telah dimanipulasi dengan menggunakan aplikasi adobe Photoshop CS5.

4. KESIMPULAN

Penelitian ini menggunakan DFRWS sebagai metode, metode ini memiliki beberapa tahapan yaitu (*Identification, Preservation, Collection, Examinition, Analysis dan Presentation*). Metode tersebut kemudian dijalankan menggunakan perangkat lunak (FTK Imager) sebagai bahan pendukung untuk mengetahui data dari flashdiks yang telah dihapus. Dalam meyakinkan bahwa bukti yang merepresentasikan asli dilakukan dengan analisis gambar pada aplikasi JPEGSNOOP Berdasarkan beberapa hasil dari tahapan-tahapan metode yang telah dilakukan, proses analisis mengenai data pada data flashdisk dapat dikatakan bahwa bukti digital berupa barang bukti data yang valid.

DAFTAR PUSTAKA

[1] U. RI, *UNDANG-UNDANG REPUBLIK INDONESIA NOMOR 20 TAHUN 2001 TENTANG PEMBERANTASAN TINDAK PIDANA KORUPSI*, vol. 123, no. 10. 2001, pp. 2176–2181.

[2] RI, "UU-2008-11 Informasi Dan Transaksi Elektronik," *Undang-undang*, vol. 11, pp. 1–18, 2008, [Online]. Available: papers3://publication/uuid/8C845E4E-CD67-4476-BB4F-7123C56F0449.

[3] Y. Ernes, "Polda Metro Tangani 443 Kasus Cyber Selama 2020, 1.448 Akun Di-take Down," *News Detik*, Jakarta, 2020.

[4] I. Riadi, Sunardi, and P. Widiandana, "Investigasi Cyberbullying pada WhatsApp Menggunakan Digital Forensics," *J. RESTI (Rekayasa Sist. dan Teknol. Informasi)*, vol. 4, no. 4, pp. 730–735, 2020.

[5] Kemitraan, *BUKTI ELEKTRONIK DI INDONESIA PENGATURAN TENTANG PEROLEHAN, PEMERIKSAAN, DAN PENGELOLAAN BUKTI ELEKTRONIK (ELECTRONIC EVIDENCE)*. 2020.

[6] B. Rahardjo and I. P. A. E. Pratama, "Pengujian Dan Analisa Anti Komputer Forensik Menggunakan Shred Tool," *Lontar Komput. J. Ilm. Teknol. Inf.*, vol. 7, no. 2, p. 104, 2016, doi: 10.24843/lkjiti.2016.v07.i02.p04.

[7] A. Fauzan, I. Riadi, and A. Fadlil, "Analisis Forensik Digital Pada Line Messenger Untuk Penanganan Cybercrime," in *Annual Research Seminar (ARS)*, 2017, vol. 2, no. 1, pp. 159–163, [Online]. Available:

http://seminar.ilkom.unsri.ac.id/index.php/ars/article/view/832/752.

[8] Subektiningsih, Y. Prayudi, and I. Riadi, "Digital Forensics Workflow as A Mapping Model for People, Evidence, and Process in Digital Investigation," *Int. J. Cyber-Security Digit. Forensics*, vol. 7, no. 3, pp. 294–304, 2018, doi: 10.17781/p002463.

[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, doi: 10.21831/elinvo.v3i1.19308.

[10] A. Yudhana, I. Riadi, and I. Zuhriyanto, "Analisis Live Forensics Aplikasi Media Sosial Pada Browser Menggunakan Metode Digital Forensics Research Workshop (DFRWS)," *TECHNO*, vol. 20, no. 2, pp. 125–130, 2019.

[11] I. Riadi, A. Yudhana, and M. C. F. Putra, "Analisis Recovery Bukti Digital Instagram Messangers Menggunakan Metode National Institute of Standards and Technology (NIST)," *Semin. Nas. Teknol. Inf. dan Komun. - Semant.*, pp. 161–166, 2017.

[12] R. Ruuhwan, I. Riadi, and Y. Prayudi, "Penerapan Integrated Digital Forensic Investigation Framework v2 (IDFIF) pada Proses Investigasi Smartphone," *J. Edukasi dan Penelit. Inform.*, vol. 2, no. 1, 2016, doi: 10.26418/jp.v2i1.14369.

[13] Y. Yusoff, R. Ismail, and Z. Hassan, "Common Phases of Computer Forensics Investigation Models," *Int. J. Comput. Sci. Inf. Technol.*, vol. 3, no. 3, pp. 17–31, 2011, doi: 10.5121/ijcsit.2011.3302.

[14] I. Irwansyah and H. Yudiastuti, "Analisis Digital Forensik Rekayasa Image Menggunakan Jpegsnoop Dan Forensically Beta," *J. Ilm. Matrik*, vol. 21, no. 1, pp. 54–63, 2019, doi: 10.33557/jurnalmatrik.v21i1.518.