Jurnal Mobile and Forensics (MF)
Vol. 1, No. 2, September 2019, pp. 76-84
P-ISSN: 2656-6257, E-ISSN: 2714-6685, DOI: http://dx.doi.org/10.12928/mf.v1i2.XXXX

ANALISIS BUKTI DIGITAL PADA *STORAGE SECURE DIGITAL CARD* MENGGUNAKAN METODE *STATIC FORENSIC*

[1]Muh Fadli Hasa, [2]Anton Yudhana, [3]Abdul Fadlil
[1]Program Studi Magister Teknik Informatika, Universitas Ahmad Dahlan, Yogyakarta
[2] Program Studi Teknik Elektro, Universitas Ahmad Dahlan, Yogyakarta
[3] Program Studi Teknik Elektro, Universitas Ahmad Dahlan, Yogyakarta
E-mail: fadlyhaza16@gmail.com[1)], eyudhana@ee.uad.ac.id[2)], fadlil@mti.uad.ac.id[3)]

Abstrak

Secure Digital Card (SD Card) merupakan salah satu media untuk mendapatkan bukti digital dalam proses penyelidikan suatu kasus *cybercrime*. Oleh kerena itu, perlu adanya penelitian tentang analisa bukti digital pada media penyimpanan *SD Card*. Penelitian ini membahas tentang proses eksaminasi dan analisis bukti digital yang terdapat pada media penyimpanan *SD Card* yang bertujuan untuk membantu proses penyelidikan kasus *cybercrime*. Proses penelitian menggunakan *tools forensic FTK Imager* dan *Autopsy* serta menggunakan metode *forensic static* dimana barang bukti eletronik diproses secara *bit-by-bit image* dalam melakukan proses forensik. Hasil dari penelitian ini adalah barang bukti yang berupa *SD Card* dilakukan proses *examinasi* dan *recovery* data yang hilang, data yang berhasil di *recovery* dibedakan berdasarkan cara pelaku menghapus datanya. Data yang didapatkan pada *SD Card* dapat dijadikan sebagai barang bukti pada proses persidangan kasus *cybercrime*.

Kata kunci : *SD Card, Forensic,* Bukti Digital, *Recovery, forensic static .*

PENDAHULUAN

Perkembangan teknologi yang sangat pesat pada saat ini telah membawa perubahan pada bidang perangkat lunak *(software),* perangkat keras *(hardware)*, dan budaya pengguna *(brainware)*. Dalam aktifitas penggunaan teknologi memiliki nilai positif dan nilai negatif. Nilai positif didapat dari proses memanfaatkan teknologi sesuai dengan kebutuhan yang bertujuan untuk memudahkan aktifitas yang dilakukan baik dari individu maupun suatu kelompok. Terlepas dari nilai positif atau manfaat yang sangat besar dari teknologi, terdapat pula nilai negatif yang sama besarnya dengan nilai positif. Nilai negatif didapat dari aktifitas penyalahgunaan teknologi yang dilakukan oleh suatu individu atau kelompok untuk melakukan tindak kejahatan *cybercrime* yang dapat merugikan targetnya.

Saat ini tindak kejahatan *cybercrime* merupakan ancaman yang sangat serius ditandai dengan pembentukan Undang-Undang untuk penanganan kasus *cybercrime* di Indonesia yang dimuat dalam UU no. 11 tahun 2008 tentang Informasi dan Transaksi Elektronik (ITE) (Fauzan, Riadi, & Fadlil, 2017). Begitu besarnya dampak dari tindak kejahatan tersebut membuat semua pihak turut andil dalam melakukan proses penanganan sehingga para pelaku kejahatan dapat diberikan hukuman setimpal sesuai dengan peraturan undang-undang yang berlaku. Para pelaku tindak kejahatan *cybercrime* dapat dihukum berdasarkan bukti yang ditemukan dengan mekanisme komputer forensik. (Yudhana, Riadi, & Ridho, 2018)

Kasus *cybercrime* yang dilakukan oleh pelaku pada umumnya akan meninggalkan jejak aktivitas kejahatan atau *history* dan kemudian *history* yang terkait dengan tindak kejahatan tersebut dapat dijadikan sebagai barang bukti dalam suatu kasus *cybercrime* (Rosalina, Suhendarsah, & Natsir, 2016). Barang bukti kasus

Received October 31, 2018; Revised November 20, 2019; Accepted November 20, 2019

cybercrime terbagi menjadi dua, yaitu barang bukti *digital* dan barang bukti elektronik. Barang bukti elektronik merupakan barang bukti yang berupa bentuk fisik dari perangkat elektronik dan juga dapat berupa media penyimpanan *(storage device)*, sedangkan barang bukti digital merupakan barang bukti berupa *file* dokumen, *file history,* atau *file log* yang berisi tentang data-data terkait dengan suatu kasus *cybercrime* dan dapat dijadikan sebagai informasi pendukung pengambilan keputusan dalam penyelidikan suatu kasus *cybercrime*. (Riadi, Umar, & Nasrulloh, 2018)

Para pelaku *cybercrime* pada umumnya akan berusaha menghilangkan barang bukti apapun dalam melakukan suatu tindak kejahatan. Proses menghilangkan barang bukti tersebut dilakukan dengan cara menghapus, memformat serta melakukan proses *wipe data* terhadap media penyimpanan sehingga data atau informasi yang berkaitan dengan tindakan yang dilakukan tidak dapat ditemukan. Teknik ataupun cara yang biasanya digunakan oleh para user dalam melakukan penghapusan data ialah dengan menekan tombol *detele* dan mengosongkan *folder recycle bin* atau *trash* pada sistem. (Al Anhar, Satrya, & Yulianto, 2014) Untuk itu perlu adanya proses forensik yang bertujuan untuk mendapatkan kembali data atau informasi tersebut sehingga para penyidik dapat menyimpulkan atau menyelesaikan suatu kasus *cybercrime.*

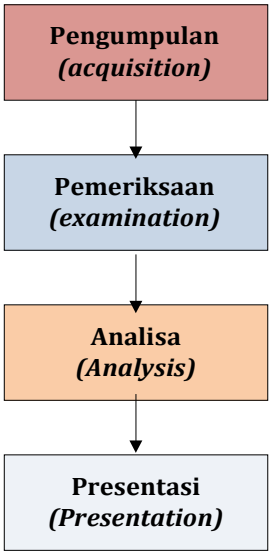
Berdasarkan kajian penelitian terdahulu yang digunakan sebagai acuan dalam penelitian ini, *tools* yang digunakan dalam penelitian menggunakan *tools* yang lazim dalam melakukan proses *recovery data* dan menerapkan satu skenario proses menghilangkan barang bukti yang biasa dilakukan oleh pelaku *cybercrime*. Pada gambaran skenario kasus dalam penelitian sebelumnya proses penghapusan data hanya menggunakan perintah *shift+delete,* dan cara penghapusan tersebut pada dasarnya masih sangat memungkinkan untuk mengangkat bukti digital yang dibutuhkan dalam proses investigasi suatu kasus *cybercrime.* Dalam penelitian ini, dilakukan dua gambaran skenario proses penghapusan data pada media penyimpanan *SD Card* yaitu dengan perintah *shift+delete* dan proses penghapusan *wipe data.* Dalam proses penghapusan menggunakan satu *tools* dan kemudian menggunakan dua *tools* yang berbeda dalam proses pengangkatan barang bukti. Hasil dalam penelitian ini nantinya akan membandingkan barang bukti yang didapat dari dua proses penghapusan data yang terapkan dalam skenario kasus.

Penelitian ini membahas tentang bagaimana memperoleh, mengambil, melestarikan, dan menyajikan data atau informasi tentang jejak aktivitas kasus *cybercrime* yang terdapat pada media penyimpanan *memory SD Card* yang telah dihapus dan bertujuan untuk membantu proses penyelidikan pelaku tindak kejahatan dengan menggunakan ilmu digital forensik. Pada penelitian ini menggunakan metode *forensic static* dan menggunakan *Eraser Tools* dalam penerapan skenario penghapusan data, serta *FTK Imager* sebagai *tool forensic* dan *Autopsy* sebagai *tools recovery data. Tolls forensic FTK Imager* dapat digunakan dalam proses mekanisme pengambilan data atau *file* secara otomatis maupun manual, dan dapat digunakan pada media penyimpanan termasuk *SD Card.*

METODE PENELITIAN

Digital Forensic dibagi menjadi dua metode, yaitu *Static Forensics* dan *Live Forensics* (Umar, Yudhana, & Faiz, 2018). Metodologi dalam penelitian ini menggunakan metode *forensic static.* Prosedur dan pendekatan konvesional yang digunakan pada metode *forensic static* dimana barang bukti eletronik diproses secara *bit-by-bit image* dalam melakukan proses forensik. Proses forensik berjalan pada *system running off* atau sistem tidak dalam keadaan berjalan (Ramadhan, Prayudi, &

Sugiantoro, 2017). Dalam proses penelitian dilakukan dengan 4 tahapan proses forensik, seperti Gambar 1 sebagai berikut:



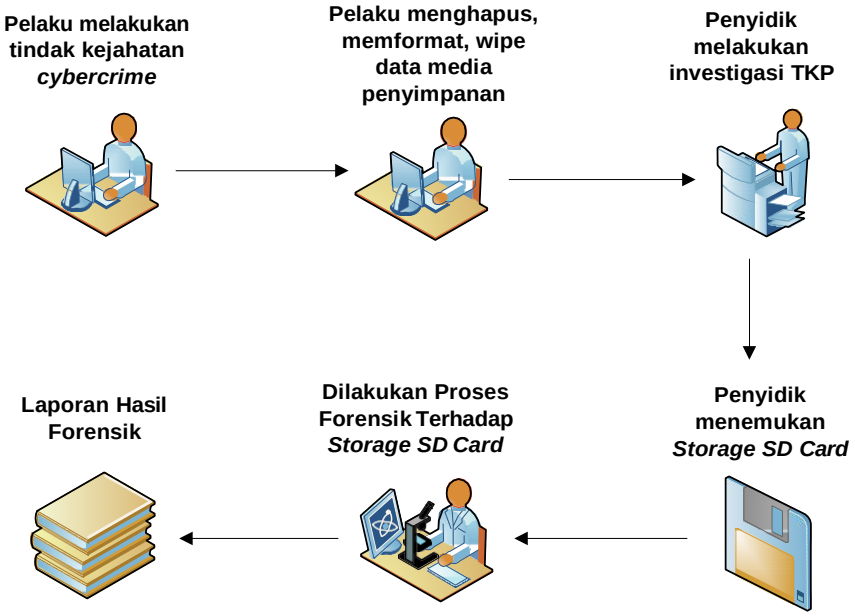
Gambar 1. Tahapan Proses Forensik

1. *Acquisition* (Pengumpulan)
   Proses *acquisition* merupakan tahapan menemukan bukti yang mendukung penyelidikan. Media elektronik yang dapat dijadikan sebagai barang bukti diantaranya sistem komputer, media penyimpanan dan lainnya.
2. *Examination* (Pemeriksaan)
   Proses *Examination* merupakan proses mencari data yang tersembunyi atau yang dihapus dan kemudian didokumentasikan. Media dalam mencari data adalah dengan menggunakan software atau *tools* diantaranya *OS Forensic, Belkasoft, FTK Imager, Autopsy).*
3. *Analysis* (Analisa)
   Proses *Analysis* merupakan proses analisis data terhadap bukti yang telah ditemukan. Proses analisa dapat dilakukan pada data file yang dihapus atau diformat, *registry windows, password, log event viewers, hidden file, log* aplikasi serta pengecekan metadata.
4. *Presentation* (Presentasi)
   Proses *presentation* merupakan proses menguraikan data secara detail, untuk melaporkan hasil penyelidikan dengan bukti yang telah diproses secara mendalam serta dapat dipertanggungjawabkan secara ilmiah di hadapan pihak yang memiliki wewenang. (Riadi, Umar, & Sukarno, 2016)

Fokus objek pada penelitian ini yaitu *Storage Secure Digital Card.* Penentuan objek pada penelitian ini dikarenakan *Storage Secure Digital Card (SD Card)* merupakan barang bukti yang sangat potensial menurut (Institute of Justice, 2001) dapat berisi informasi seperti pesan email, riwayat penjelajahan internet, catatan obrolan dan teman internet daftar, foto, file gambar, database, catatan keuangan, dan catatan peristiwa yang bisa menjadi bukti berharga dalam investigasi atau penuntutan. Untuk lebih jelasnya, gambar *Storage Secure Digital Card (SD Card)* dapat dilihat pada Gambar 2 sebagai berikut :

Gambar 2. *Storage Secure Digital Card (SD Card)*

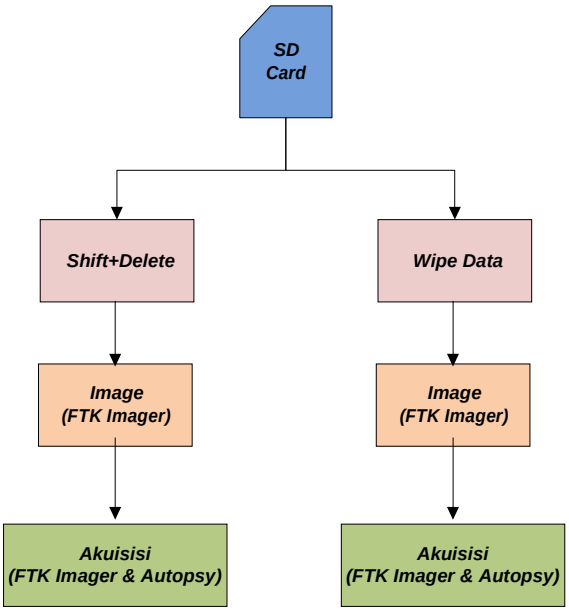
Dalam penelitian ini dibuat suatu skenario proses menghilangkan barag bukti yang dilakukan oleh pelaku tindak kejahatan. Gambar skenario proses menghilangkan barang bukti oleh pelaku tindak kejahatan dapat dilihat pada Gambar 3 berikut ini:



Gambar 3. Skenario proses menghilangkan barang bukti

Tools forensic yang digunakan pada penelitian ini yaitu *FTK Imager* dan *Autopsy* sebagai *tools recovery data*. *Access data FTK Imager* merupakan suatu perangkat lunak yang sering digunakan untuk melakukan analisa pemulihan data secara *forensic*. Pemulihan data menggunakan *FTK Imager* ini dilakukan dengan melakukan *mounting* pada *SD Card* yang digunakan untuk melakukan penghapusan file untuk kemudian akan dianalisa. Sedangkan *Autopsy* merupakan perangkat lunak yang cukup baik dalam melakukan pemulihan data yang telah terhapus. (Khalifa et al., 2016)

Objek diambil berdasarkan skenario yang telah dibuat sebelumnya yaitu *SD Card.* Objek dibagi menjadi dua berdasarkan proses penghapusan file pada *SD Card* yaitu dengan perintah *Shift+Delete* dan *wipe data*. Setelah objek dibagi berdasarkan proses penghapusan file, kemudian dilakukan proses *image* pada objek menggunakan tools *FTK Imager.* Tahapan selanjutnya yaitu melakukan akuisisi terhadap *SD Card* yang bertujuan untuk menganalisa *file-file* apa saja yang dapat di *recovery* setelah proses penghapusan. Proses *recovey* menggunakan *FTK Imager* dan *Recuva.* Tahapan yang dijabarkan diatas, akan dijelaskan pada Gambar 4 berikut ini:

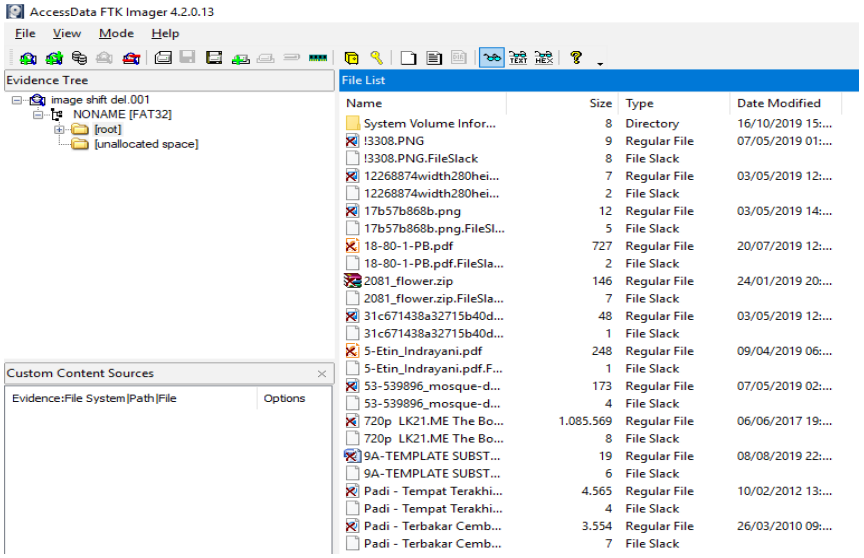


Gambar 4. Tahapan Proses Forensik *SD Card*

Hasil dan Pembahasan

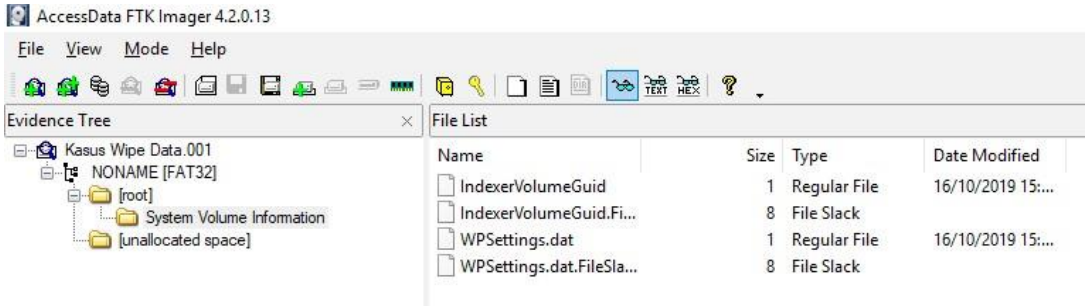
Proses pertama yang dilakukan adalah melukukan proses *acquisition* yaitu dengan melalukan proses *image* dengan menggunakan *FTK Imager.* Proses ini dilakukan untuk mengakuisisi data atau pun file yang berada pada barang bukti yang sesuai dengan gambaran skenario yaitu pada *SD Card.* Proses dilakukan dengan menghubungkan *SD Card* pada laptop menggunakan *Card Reader,* setelah itu menjalankan *tools FTK Imager* dan memulai proses *image data.*

Proses *image* data dengan *FTK Imager* pada *SD Card* dengan cara hapus *Shift+Delete* didapatkan berbagai jenis file yang pernah tersimpan di dalam *SD Card.* Hasil dari proses *image file* pada *SD Card* dengan cara hapus *Shift+Delete* dapat dilihat pada Gambar 5 berikut ini:



Gambar 5. Hasil *image* pada *SD Card* dengan cara hapus *Shift+Delete*

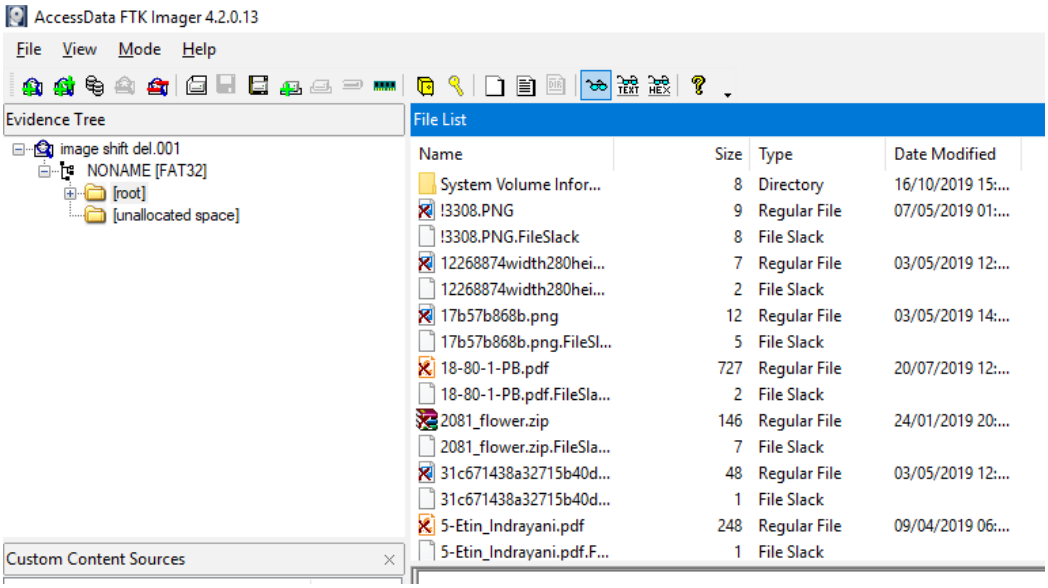
Proses *image* data dengan *FTK Imager* pada *SD Card* dengan cara hapus *Wipe data* hanya mendapatkan beberapa *file residu* dari *file* yang pernah tersimpan di dalam *SD Card.* Hasil dari proses *image file* pada *SD Card* dengan cara hapus *Wipe data* dapat dilihat pada Gambar 6 berikut ini:



Gambar 6. Hasil *image* pada *SD Card* dengan cara hapus *Wipe Data*

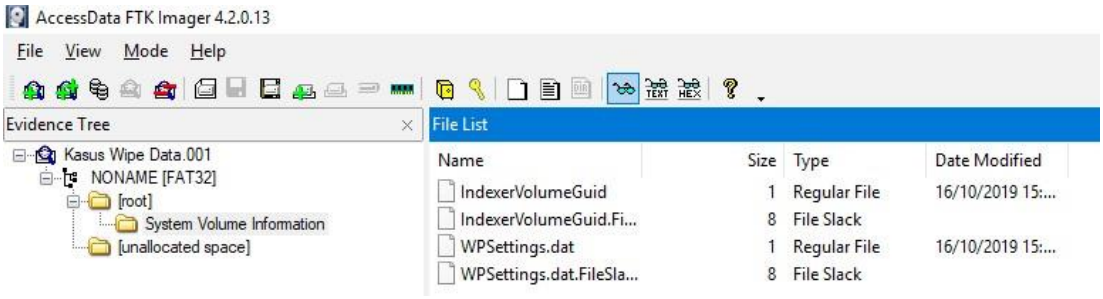
Proses kedua yang dilakukan adalah proses *Examination,* tahap *examination* ini bertujuan untuk mengungkap dan melakukan analisis terhadap hasil dari tahap *acquisition* untuk memperoleh data (Kunang & Khristian, 2016). Proses dilakukan dengan mencari data yang tersembunyi atau dihapus pada *SD Card.* Setelah itu melakukan dokumentasi terhadap *file* yang telah ditemukan.

Proses *Examination* data dengan *FTK Imager* pada *SD Card* dengan cara hapus *Shift+Delete* didapatkan berbagai jenis file, diantaranya yaitu *PDF, PNG, MP4, Doc*, *Zip,* dan *metadata file* yang pernah tersimpan di dalam *SD Card.* Hasil *Examination* menggunakan *FTK Imager* pada *SD Card* dengan cara hapus *Shift+Delete* dapat dilihat pada Gambar 7 berikut ini:



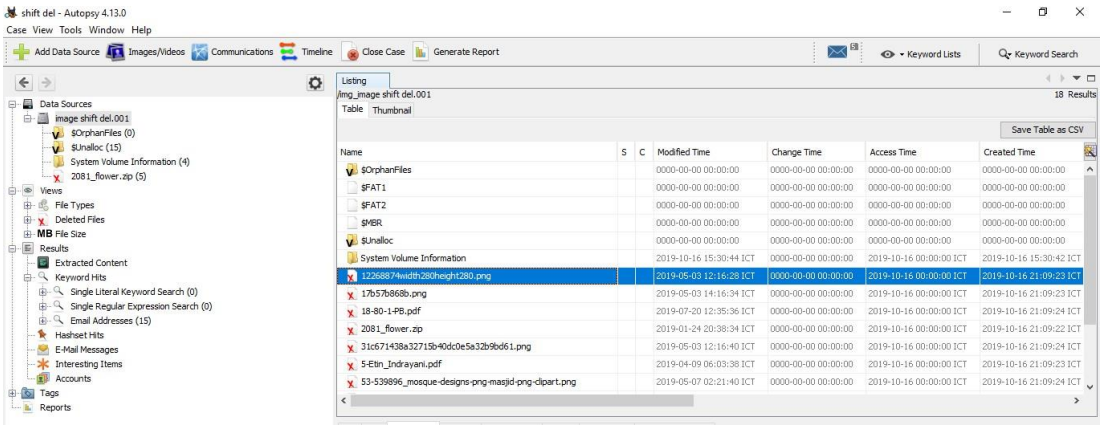
Gambar 7. Hasil *Examination* menggunakan *FTK Imager* pada *SD Card* dengan cara hapus *Shift+Delete.*

Hasil *Examination* menggunakan *FTK Imager* pada *SD Card* dengan cara hapus *Wipe Data* hanya didapatkan beberapa *file residu.* Hasil *Examination* menggunakan *FTK Imager* pada *SD Card* dengan cara hapus *Wipe Data* dapat dilihat pada Gambar 8 berikut ini:



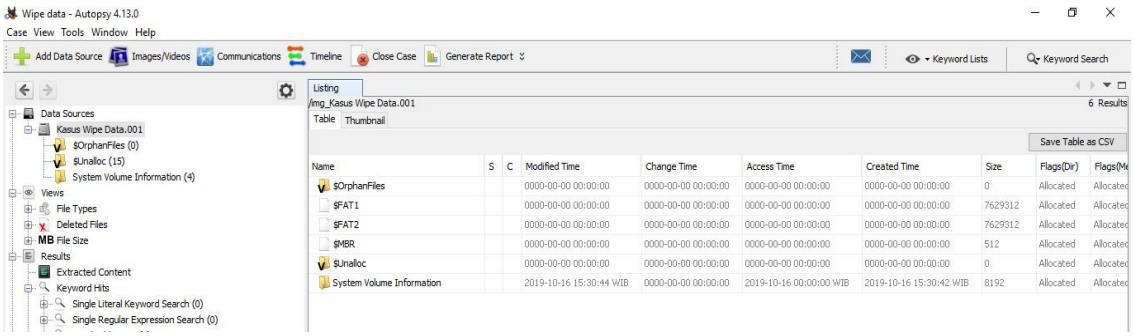
Gambar 8. Hasil *Examination* menggunakan *FTK Imager* pada *SD Card* dengan cara hapus *Wipe Data.*

Proses *Examination* data dengan *Tools Autopsy* pada *SD Card* dengan cara hapus *Shift+Delete* didapatkan berbagai jenis *file*, diantaranya yaitu *PDF, PNG, MP4, Doc*, *Zip*, dan *metadata file* yang pernah tersimpan di dalam *SD Card.* Hasil *Examination* menggunakan *Tools Autopsy* pada *SD Card* dengan cara hapus *Shift+Delete* dapat dilihat pada Gambar 9 berikut ini:



Gambar 9. Hasil *Examination* menggunakan *Autopsy* pada *SD Card* dengan cara hapus *Shift+Delete.*

Hasil *Examination* menggunakan *Tools Autopsy* pada *SD Card* dengan cara hapus *Wipe Data* hanya didapatkan beberapa *file residu.* Hasil *Examination* menggunakan *Tools Autopsy* pada *SD Card* dengan cara hapus *Wipe Data* dapat dilihat pada Gambar 10 berikut ini:



Gambar 10. Hasil *Examination* menggunakan *Autopsy* pada *SD Card* dengan cara hapus *Wipe Data.*

Proses selanjutnya yaitu menganalisa bukti-bukti yang telah ditemukan pada *SD Card.* Jenis *File* barang bukti yang telah ditemukan dapat dilihat pada Tabel 1 berikut ini:

Tabel 1. Jenis *file* barang bukti

Tools /Proses Hapus	Jenis File					
	PDF	PNG	MP4	MP3	Doc	Zip
Shift+Delete/FTK Image	2	5	1	2	1	1
Wipe Data/FTK Imager	-	-	-	-	-	-
Shift+Delete/Autopsy	2	5	1	2	1	1
Wipe Data/Autopsy	-	-	-	-	-	-

Berdasarkan table diatas, barang bukti yang ditemukan pada *SD Card* dengan cara hapus *Shift+Delete* yang menggunakan *FTK Imager* dan *Autopsy* yaitu berupa file *PDF, PNG, MP4, Doc, dan Zip*. Sedangkan pada memori dengan cara hapus *Wipe Data, FTK Imager* dan *Autopsy* hanya mendapatkan *file residu.*

Kesimpulan

Berdasarkan hasil penelitian yang dilakukan, hasil yang didapatkan dari proses pengangkatan barang bukti pada *SD Card* sangat dipengaruhi oleh proses penghapusan data yang diterapkan. Barang bukti pada *SD Card* dapat ditemukan tergantung pada cara menghapus data yang berada pada *SD Card* tersebut. Hasil pengangkatan barang bukti yang ditemukan pada *SD Card* dengan cara hapus *Shift+Delete* yang menggunakan *Tools FTK Imager* dan *Autopsy* yaitu berupa *file PDF, PNG, MP4, Doc*, *Zip,* dan *metadata file*. Sedangkan hasil pengangkatan barang yang ditemukan pada *SD Card* dengan cara hapus *Wipe Data* dengan menggunakan *Tool FTK Imager* dan *Autopsy* hanya mendapatkan *file residu.* Data yang didapatkan pada *SD Card* dapat dijadikan sebagai barang bukti dalam persidangan kasus *cybercrime.*

Daftar Pustaka

Al Anhar, A., Satrya, G. B., & Yulianto, F. A. (2014). *Analisis Perbandingan Keamanan Teknik Penghapusan Data pada Hardisk dengan Metode DoD 5220 . 22 dan Gutmann Comparative Analysis of Data Deletion Technique Security on Hard disk with DoD 5220 . 22 and Gutmann Method*. *1*(1), 607–613.

Faiz, M. N., Umar, R., & Yudhana, A. (2017). Implementasi Live Forensics untuk Perbandingan Browser pada Keamanan Email. *JISKA (Jurnal Informatika Sunan Kalijaga)*, *1*(3), 108. https://doi.org/10.14421/jiska.2017.13-02

Fauzan, A., Riadi, I., & Fadlil, A. (2017). Analisis Forensik Digital Pada Line Messenger Untuk Penanganan Cybercrime. *Annual Research Seminar (ARS)*, *2*(1), 159 – 163. Retrieved from http:// seminar.ilkom.unsri.ac.id/ index.php/ars/article/view/832/752

Hartono, R. (2013). *Perancangan Sistem Data Logger Temperatur Baterai Berbasis Arduino Duemilanove*. Retrieved from http:// chemistrahmah.com/ caramenulisdaftarpustaka.%5Cnhtml

Institute of Justice, N. (2001). *Special REPORT Electronic Crime Scene Investigation: A Guide for First Responders, Second Edition*. Retrieved from www.ojp.usdoj.gov/nij

Khalifa, H. R., Yulianto, F. A., Jadied, E. M., Informatika, S. T., Informatika, F., & Telkom, U. (2016). *Implementasi Teknik Penghapusan Data Dengan Metode DoD 5220 . 22M Pada Sistem Operasi Android Implementation Of Data Deletion Using DoD 5220 . 22M method On Android Operating System*. *3*(1), 897–913.

Kunang, Y. N., & Khristian, A. (2016). *Implementasi Prosedur Forensik untuk Analisis Artefak Whatsapp pada Ponsel Android*. *2*(1), 59–68. Retrieved from http://ars.ilkom.unsri.ac.id

Kurniawan, H. (2011). Keamanan jaringan dengan komputer forensik. *Computer Science Research and Its Development Journal*, *Vol.3*(3), 175–184.

Ramadhan, R. A., Prayudi, Y., & Sugiantoro, B. (2017). Implementasi dan Analisis Forensika Digital Pada Fitur Trim Solid State Drive (SSD). *Teknomatika*, *9*(2), 1–13. Retrieved from http:// teknomatika.stmikayani.ac.id/wp-content/uploads/2017/07/1.pdf

Riadi, I., Umar, R., & Nasrulloh, I. M. (2018). *Analisis Forensik Digital Pada Frozen Solid State Drive Dengan Metode National Institute of Justice (Nij)*. *3*(1), 70–82. https://doi.org/10.21831/elinvo.v3i1.19308

Riadi, I., Umar, R., & Sukarno, W. (2016). Analisis Forensik Serangan Sql Injection Menggunakan Metode Statis Forensik. *Prosiding Interdisciplinary Postgraduate Student Conference 1st*, *I*(I), 102–103.

Rosalina, V., Suhendarsah, A., & Natsir, M. (2016). Analisis Data Recovery Menggunakan Software Forensic : Winhex and X-Ways Forensic. *Jurnal Pengembangan Riset Dan Observasi Sistem Komputer*, *3*(1), 51–55.

Ruci Meiyanti, & Ismaniah. (2015). Perkembangan Digital Forensik. *Jurnal Kajian Ilmial UBJ*, *15*(September 2015).

Ruuhwan, R., Riadi, I., & Prayudi, Y. (2016a). Analisis Kelayakan Integrated Digital Forensics Investigation Framework Untuk Investigasi Smartphone. *Jurnal Buana Informatika*, *7*(4). https://doi.org/10.24002/jbi.v7i4.767

Ruuhwan, R., Riadi, I., & Prayudi, Y. (2016b). Penerapan Integrated Digital Forensic Investigation Framework v2 (IDFIF) pada Proses Investigasi Smartphone. *Jurnal Edukasi Dan Penelitian Informatika (JEPIN)*, *2*(1). https://doi.org/10.26418/jp.v2i1.14369

Umar, R., Yudhana, A., & Faiz, M. N. (2018). Experimental analysis of web browser sessions using live forensics method. *International Journal of Electrical and Computer Engineering*, *8*(5), 2951–2958. https://doi.org/10.11591/ijece.v8i5.pp.2951-2958

Yudhana, A., Riadi, I., & Ridho, F. (2018). DDoS classification using neural network and naïve bayes methods for network forensics. *International Journal of Advanced Computer Science and Applications*, *9*(11), 177–183. https://doi.org/10.14569/ijacsa.2018.091125