Open Science and Technology
Vol. 02 No. 02, (190-197)
ISSN (Print) :2776-169X
ISSN (Online) :2776-1681

Analisis Kerangka Kerja yang Logis untuk Menyusun SOP Penanganan Pertama pada CCTV

Logical Framework analysis for ordering the standard operating procedure of first respond to CCTV

Danang Mulyadipa Suratno[1*], Alya Triska Sutrisno[1], Novrianti[1]

[1]Sekolah Tinggi Teknologi Nasional
*email: danangmulyadipasuratno@stiteknas.ac.id

Submitted:11 Agustus 2022 Accepted: 29 Desember 2022 Published: 4 Januari 2023

ABSTRAK

Ketika petugas berwenang melakukan aktivitas investigasi forensik digital, hal penting yang harus diperhatikan adalah menggunakan dan mengikuti proses di setiap tahapan yang ada pada kerangka investigasi. Tidak hanya mengikuti mekanisme yang tepat tetapi juga harus mengikuti aturan hukum yang berlaku. Namun ditemukan kejadian saat barang bukti yang dihadirkan dipersidangan ditolak pada perkara nomor: 85/PID.B/2012/PN.pwt, dikarenakan hasil rekaman CCTV tidak disertai alat bukti proses hashing yang dicetak dalam bentuk surat untuk melihat keaslian dari suatu file. Hal ini menunjukkan bahwa pihak pengadilan tidak bisa menerima begitu saja bukti yang diserahkan jika mereka tidak bisa memastikan bagaimana bukti tersebut ditangani. Oleh karena itu, dilakukan penelitian untuk menghasilkan framework penangan awal untuk forensik CCTV melalui identifikasi ketentuan dan proses penting dari standar yang berlaku. Pengamatan pada penelitian ini menggunakan kolaborasi dari dokumen SNI 27037:2014 dan SWGIT 1.0 2013.09.27, sehingga diperoleh tahapan kegiatan terhadap alat bukti digital dimulai dari perolehan hingga diputarkan di pengadilan, dan sesuai dengan prosedur ini maka alat bukti digital tersebut dinyatakan sah di persidangan. Metode teknik analisa yang logis terhadap kerangka kerja yang akan dilakukan (logical framework approach (LFA) dapat diterapkan dalam menyusun sebuah framework forensik untuk penanganan awal forensik barang bukti sistem kamera pengawas CCTV

Kata kunci: *CCTV, Framework, SNI/ISO, SWGIT.*

ABSTRACT

When officers are authorized to carry out digital forensic investigation activities, the important thing that must be considered is to use and follow the process at each stage in the investigation framework. Not only following the right mechanism but also having to follow the applicable legal regulations. However, an incident was found when the evidence presented at trial was rejected in case number: 85/PID.B/2012/PN.pwt, because the CCTV footage was not accompanied by evidence of the hashing process printed in the form of a letter to see the authenticity of a file. This suggests that the courts cannot simply accept the evidence presented if they cannot be certain how it will be handled. Therefore, research was carried out to produce an initial handling framework for CCTV forensics by identifying the important provisions and processes of the applicable standards. Observations in this study used a collaboration of documents SNI 27037:2014 and SWGIT 1.0 2013.09.27, so that the stages of activity regarding digital evidence were obtained starting from acquisition to being played in court, and in accordance with this procedure, the digital evidence was declared valid in court. The logical framework approach (LFA) can be applied in compiling a forensic framework for the initial handling of forensic evidence of CCTV surveillance camera systems.

Keywords: *CCTV, Framework, SNI/ISO, SWGIT.*

Open Science and Technology
Vol. 02 No. 02, (190-197)
ISSN (Print) :2776-169X
ISSN (Online) :2776-1681

PENDAHULUAN

Menurut Terry (2006), informasi merupakan suatu data/berita penting yang dapat memberikan pengetahuan yang bermanfaat bagi penerimanya. Sementara itu menurut Burch & Starter (1974), informasi ialah pengumpulan dan pengolahan data untuk memberikan suatu keterangan atau pengetahuan. Hal ini tentunya menjadikan informasi merupakan hal yang sangat dibutuhkan guna mendapatkan kejelasan dari berbagai berita ataupun kejadian terkait. Informasi yang benar, tentulah harus nyata kejelasannya dan valid berdasarkan sumber yang dapat dipercaya, apalagi hal ini menyangkut masa depan kehidupan perorangan, kelompok, bangsa, bahkan negara. Pada hakikatnya informasi dan/atau dokumen dapat dituangkan ke dalam media apa saja, salah satunya adalah melalui media elektronik.

Dalam suatu persidangan, berbagai uraian informasi akan diperdebatkan oleh dua kubu yang saling bertolak belakang. Setiap data yang diberikan yang tidak sesuai dengan informasi terkait lainnya, akan berdampak fatal bahkan tidak menutup kemungkinan hal tersebut akan menjadi serangan dari pihak yang menjadi oposisi pada persidangan tersebut. Informasi atau data yang akan menjadi barang bukti untuk suatu kasus bisa berbentuk barang elektronik, ataupun data digital. Sebuah penyelidikan yang terjadi terkadang menjadikan file data tersimpan dari peralatan elektronik sebagai alat bukti yang potensial (Panende, 2018). Hal ini dikarenakan pada file data tersebut mengandung informasi mengenai kronologis kejadian yang bisa dijadikan bukti dalam penyelidikan. File data yang ada tentu akan digunakan sebagai penunjang alat bukti dalam memperoleh informasi penyelidikan suatu perkara.

Salah satu jenis data yang dapat memberikan informasi di persidangan adalah rekaman CCTV dari tempat kejadian perkara. Barang bukti berupa rekaman CCTV tersebut akan diterima di pengadilan, jika video yang ditampilkan dapat dibuktikan keasliannya, yakni berupa adanya dokumen catatan nilai HASH tentang keorisinilan video CCTV tersebut, berita acara pengemasan, hingga kepenyimpanan barang bukti digital tersebut. Disamping itu, dokumen histori perjalanan barang bukti juga harus lengkap.

Terkadang penyidik di daerah mengalami tertolak barang bukti digitalnya yang dihadirkannya saat di hadapan sidang peradilan karena tidak bisa menunjukkan keasliannya. Maka diperlukan perlakuan khusus agar terjaga keutuhan dan keaslian barang bukti digital tersebut karena biasanya yang dipertanyakan dari barang bukti digital adalah originalitasnya. Diperlukan adanya suatu mekanisme yang harus dilakukan untuk memastikan keamanan, privasi dan integritas dari data yang diolah sesuai standar yang berlaku (Endang, 2018). Mekanisme khusus untuk pengambilan barang bukti digital diperlukan, sehingga barang bukti digital tersebut dapat dipertanggungjawabkan keasliannya.

Hal yang menjadi temuan pada kasus nomor 85/PID.B/2012/PN.pwt yang terjadi di salah satu pengadilan tinggi adalah bahwasanya terdapat barang bukti elektronik berupa tiga keping CD rekaman CCTV yang tidak mempunyai kekuatan hukum yang mengikat dikarenakan tidak diajukannya surat pelengkap alat bukti digital yang merupakan hasil proses *hash* untuk melihat keaslian dari suatu file. Hal ini tentu menjadikan pembela tidak dapat melanjutkan tugasnya dengan baik sebelum nilai *hash* dari barang bukti digital dapat ditunjukkannya. Proses *hash* adalah proses untuk memperoleh nilai bit data yang terperinci saat data itu diperoleh sehingga memiliki nomor

atau nilai hash yang unik. Bila terjadi perubahan pada data, maka nilai *hash* pun akan berubah sedemikian rupa sehingga terdeteksi sebagai barang bukti yang telah dimanipulasi. Hal ini ditujukan agar barang bukti tersebut bisa dipertanggungjawabkan di persidangan. Titik penting dalam proses ini adalah menerapkan panduan aktivitas khusus dalam penanganan bukti digital potensial berupa prosedur standar yang telah diatur dalam standar yang berlaku (Sudyana, 2016) Oleh karena itu surat keterangan hash ini sangat dibutuhkan dan disertakan ketika menyerahkan alat bukti digital.

Pada dasarnya dalam aspek sistem digital, informasi yang asli dengan salinannya tidak relevan lagi untuk dibedakan, sebab pada sistem digital yang beroperasi dengan cara penggandaan mengakibatkan informasi yang asli dan salinannya terlihat sangat identik. Barang bukti elektronik dan digital pada dasarnya adalah bersifat volatile, yakni rentan untuk berubah, ataupun rusak, bahkan hampir mungkin hilang isi datanya karena kegiatan yang disengaja ataupun tidak disengaja. Seperti RAM pada leptop yang akan menghilangkan data ketika leptop dimatikan. Oleh karena itu jika penanganan barang bukti dilakukan secara tidak prosedural maka kemungkinan yang terjadi adalah barang bukti yang tersimpan dalam barang bukti elektronik dapat berubah, rusak, bahkan hilang sehingga tidak dapat di-*recover* kembali, dan sebagai akibatnya barang bukti tidak layak untuk dihadirkan saat persidangan.

Sebagai bagian dari metode ilmiah maka diperlukan *framework* yang dapat menuntun proses pembuktian yang prosedural (Lizarti, 2017). Berdasarkan hal tersebut maka tujuan pada penelitian ini adalah untuk memperoleh *framework* investigasi untuk penangan awal forensik *CCTV* yang sesuai dengan standar SNI ISO/IEC 27037:2014 dan standar penanganan yang terdapat pada SWGIT version 1.0 2013.09.27.
Diharapkan nantinya prosedur ini dapat digunakan sebagai acuan dalam mempertimbangkan langkah-langkah yang dilakukan untuk memperoleh bukti digital potensial (Wahyudi, 2018).

METODE PENELITIAN

Pada bagian ini akan dijelaskan metode penelitian yang dilakukan sehingga dapat diketahui apa saja tahapan penelitian yang dilakukan sehingga dapat dijadikan pedoman dalam menyelesaikan permasalahan serta kendala yang dihadapi.

Langkah awal dari penelitian ini adalah menemukan video yang dianggap bermasalah sehingga tidak dapat digunakan dalam persidangan di pengadilan. Hal ini dikarenakan hasil proses hash yang tidak dilampirkan beserta alat bukti elektronik tersebut. Berdasarkan video yang telah ditetapkan untuk ditelaah, maka akan dilakukan penyusunan *logframe matrix*.

Penyusunan *logframe matrix* untuk perencanaan evaluasi yang dilakukan menghasilkan matrik yang akan dirincikan kembali menjadi beberapa bagian matrik, yaitu Deskripsi, Indikator, Verifikasi, dan Asumsi sehingga diperoleh alur aktivitas yang terstruktur untuk mencapai tujuan. *Logframe matrix* yang digunakan dalam penelitian ini dapat dilihat pada Tabel 1.

Open Science and Technology
Vol. 02 No. 02, (190-197)
ISSN (Print) :2776-169X
ISSN (Online) :2776-1681

Tabel 1. *Logframe matrix*

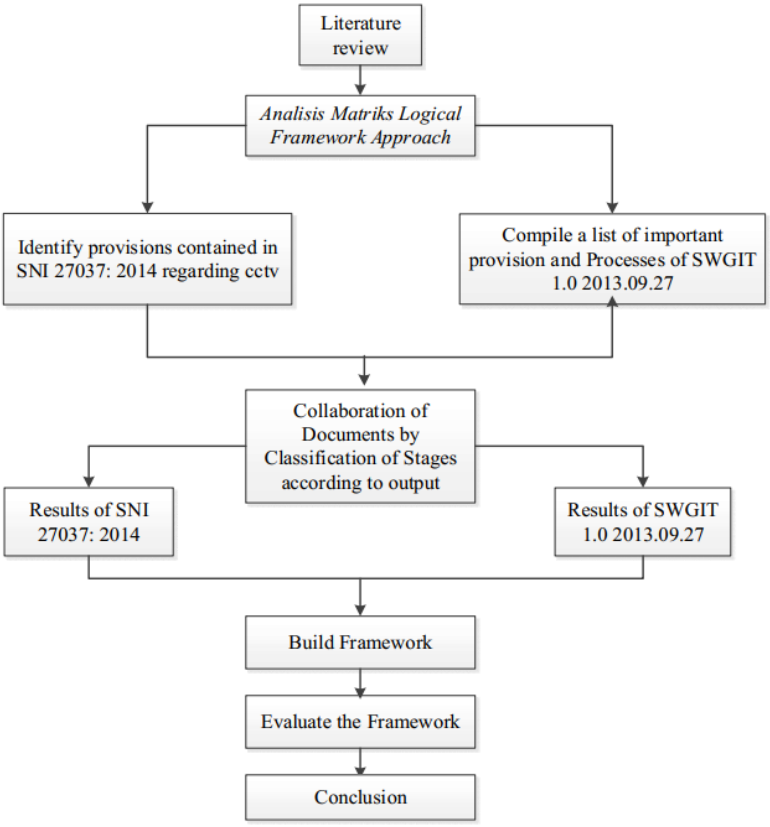
Deskripsi	Indikator	Verifikasi	Asumsi
Tujuan ***First Respond Framework*** untuk forensik CCTV	*Framework investigation* untuk forensik CCTV	Memenuhi kebutuhan penyidik	Mengikuti aturan baku penyelidikan forensik digital
Sasaran Framework investigasi untuk forensik CCTV	*Framework* memenuhi S&K	Memenuhi standar evaluasi	Mengikuti aturan baku penyelidikan forensik digital
Keluaran framework hasil kolaborasi	Framework hasil evaluasi yang telah mengalami peningkatan	Mengikuti SNI 27037: 2014 Mengikuti metode praktis menurut SWGIT	When the activity is done the output is obtained Setelah kolaborasi diselesaikan, diperoleh framework
Melaksanakan kegiatan yang penting	Semua aktifitas penting terpenuhi		Ketika data tersedia, maka aktivitas bisa dilaksanakan.

Pada mulanya, dilakukan proses identifikasi dengan mengekstrak dokumen yang dijadikan landasan penelitian, dan berdasarkan alur langkah kegiatan yang dipakai. Hal ini dilakukan untuk mempermudah pemodelan logik yang mengklasifkasikan tahapan-tahapan tersebut berdasarkan kesamaannya.

Tindakan yang selanjutnya yang dilakukan adalah menggabungkan atau mengkolaborasikan antar dokumen tersebut kedalam beberapa tahapan yang sesuai dengan variabel keluarannya yang terbagi menjadi identifikasi, pengumpulan, akuisisi dan preservasi. Kegiatan ini dideskripsikan berdasarkan dokumen SNI dan SWGIT.

Tahapan hasil identifikasi dari dokumen SWGIT akan diberikan indikator *role model* berdasarkan penjelasaan pada prosesnya atau terminologi dengan mengadaptasi dari pendekatan logika agar mempermudah penyusunannya saat dilakukan kolaborasi. Bila terdapat kesamaan terminologi maka tahapan tersebut dikatakan *implies*, yang kemudian bila tahapan tersebut merupakan tahapan yang dianggap penting dan tidak ada pada dokumen SNI/ISO maka dikatakan sebagai *prohibit*, sedangkan yang terakhir dikatakan sebagai *don't care* jika tahapan tersebut tetap berada pada tahapan semula, karena tidak dapat dikolaborasikan dan tidak memiliki terminologi yang sama dengan tahapan pada dokumen SNI/ISO. Diagram alir dari penelitian ini dapat dilihat pada gambar di bawah ini:

Open Science and Technology
Vol. 02 No. 02, (190-197)
ISSN (Print) :2776-169X
ISSN (Online) :2776-1681



Gambar 1. Diagram alir penelitian

HASIL DAN PEMBAHASAN

Hasil Penelitian

Pada penelitian sebelumnya yang penah dilakukan oleh para peneliti adalah dokumen yang mengenai penanganan barang bukti digital dengan metode yang berbeda, SNI/ISO saja, atau SWGIT saja. Guna untuk mempermudah penyidik menghasilkan barang bukti digital dalam hal ini CCTV, sehingga layak digunakan dipersidangan dengan tidak merusak meta data yang ada di dalamnya. Sementara pada penelitian ini menghasilkan *framework* forensik investigasi yang disebut *First Respond Framework* untuk Forensik *CCTV* dengan menggunakan kolaborasi dari SNI/ISO sekaligus SWGIT.

Hasil analisis dan evaluasi Framework untuk Forensik CCTV yang diperoleh dengan mengkolaborasikan hasil identifikasi ketentuan penting dari SNI/ISO Forensik Digital dan SWGIT v1.0 Digital Forensic. Pada uraian selanjutnya, akan dirincikan bagaimana hasil indentifikasi sesuai dengan standar, dan juga hasilnya berdasarkan SWGIT dari digital forensik tersebut.

Tahapan dalam melakukan digital forensik adalah identifikasi, koleksi, akuisisi, dan preservasi. Pelaksanaan keempat tahapan tersebut adalah seperti halnya *waterfall diagram*, yakni pada setiap tahapan haruslah diselesaikan terlebih dahulu seluruh kegiatannnya, barulah kemudian kegiatan berpindah ketahapan selanjutnya. Kegiatan dinyatakan selesai jika telah dilakukan seluruh kegiatan pada tahapan terakhir (preservasi).

Tahapan identifikasi adalah pengarahan yang diberikan pada anggota penyidik yang akan terjun ke lokasi TKP. Pada tahapan koleksi hal yang dilakukan adalah memastikan bukti digital yang ada di TKP serta kesesuaian isinya terkait dengan kasus yang dihadapi. Kemudian dilanjutkan dengan tahapan akuisisi, yakni mengambil alih barang bukti yang ada di TKP untuk diamankan oleh penyidik demi menjaga keutuhan barang bukti baik secara fisik ataupun digital. Pada tahapan terakhir, yakni memastikan bukti yang diambil dari TKP adalah dipindahkan dalam keadaan tersegel dan memiliki histori perpindahannya dalam bentuk dokumen.

Hasil Pengamatan SNI/ISO Digital Forensik

Berdasarkan dari hasil pengamatan yang dilakukan, diperoleh 23 proses penting/kegiatan terkait dengan *forensic* CCTV., Uraian proses penting tersebut ditunjukan pada Tabel 2.

Tabel 2. Hasil Identifikasi SNI/ISO Digital Forensik.

No	Identification	Collection	Acquisition	Preservation
1	Briefing	Ensure contents	Determination of acquisition media	Verify the acquisition
2	Preparation and planning	Make sure the camera	Logical acquisition	Seal of evidence
3	Precautions at the scene	Overwrite schedule	Examination of acquisition	Examination of security aspects of transporting evidence
4	Risk assessment	Documentation	Label evidence	Transporting evidence
5	Search evidence	Verbal remarks	Documentation	Keeping evidence
6	Documentation			Travel document
7	Chain of custody			

Setiap hasil pengamatan, berdasarkan tabel tersebut dapat dilihat bahwa kegiatan yang dilakukan dibagi kedalam empat tahapan utama dalam alur penyelidikan, yaitu identifikasi, koleksi, akuisisi, dan preservasi. Pembagian golongan ini didasarkan kepada deskripsi kegiatan yang dipaparkan pada dokumen tersebut. Masing-masing tahapan memiliki arahan kegiatan yang akan dilakukan untuk memastikan perolehan alat bukti yang pantas dan diterima di pengadilan. Sangat penting untuk melengkapi dokumen atau melaksanakan kegiatan dari tiap tahapan untuk pengarsipan, ataupun untuk dibawa ke persidangan.

Hasil Identifikasi SWGIT Digital Forensic

Berdasarkan hasil dari identifikasi yang dilakukan diperoleh 22 proses penting terkait dengan forensik *CCTV*. Kegiatan yang merupakan hasil Identifikasi SWGIT ditunjukan pada Tabel 3.

Tabel 3. Hasil Identifikasi SWGIT V1.0 Digital Forensik.

No	Identification	Collection	Acquisition	Preservation
1	Observe	Note	Test retrieval	Chain of Custody
2	Type CCTV	Review recorded	Posisible output	Audit trail
3	Feature CCTV	Maintain schedule	Amount of the time	Transfering

Open Science and Technology
Vol. 02 No. 02, (190-197)
ISSN (Print) :2776-169X
ISSN (Online) :2776-1681

4	Time display	Evaluation of output	Keeping evidence
5	Metadata	Legal output	
6	Native file		
7	Operator assist		
8	Scene contact		
9	Photograph system		
10	Sketch camera placement		

Keterangan:

Tahapan dengan role model *Implies* dan *Prohibit*
Tahapan dengan role model *Don't Care*

Langkah selanjutnya adalah menerapkan *role model* pada tahapan-tahapan yang sudah diperoleh agar mudah untuk melakukan kolaborasi. Tahapan yang akan dikolaborasikan hanyalah tahapan yang bersifat *implies* dikarenakan memiliki kesamaan.

Kolaborasi

Setelah setiap proses identifikasi dilakukan, baik berdasarkan dokumen SNI ataupun SWGIT, diklasifikasikan berdasarkan variabel output dan idikator *role model* yang ditetapkan. Maka proses selanjutnya adalah mengkolaborasikan setiap tahapan ataupun kegiatan dengan indikator *role model implies* akan menjadi satu tahapan. Hasil kolaborasi dari dokumen yang dijadikan landasan penelitian ini dirunut pada tabel 4 berikut.

.

Tabel 4. Hasil Kolaborasi kegiatan berdasarkan dokumen SNI dan SWGIT

No	Identification	Collection	Acquisition	Preservation
1	Briefing	Review recorded	Test retrieval	Verify the acquisition
2	Preparation and planning	Make sure the camera	Posisible output	Audit trail
3	Precautions at the scene	Overwrite schedule	Amount of the time	Seal of Evidence
4	Risk assessment	Documentation	Evaluation of output	Travel document
5	Search evidence	Time display	Logical Acquisition	Examination of security aspects of transporting evidence
6	Observe	Metadata	Examination of acquisition	Transporting evidence
7	Type CCTV	Native file	Label evidence	Keeping evidence
8	Feature CCTV	Verbal remarks	Chain of Custody	
9	Documentation	Operators assist		
10		Scene contact		
11		Photograph system		
12		Sketch camera placement		

Pada prosesnya, pengkolaborasian ini terjadi karena memiliki kesamaan terminology., Maka pada tahapan terminologi yang sama, kejadian tersebut akan diberikan penamaan/istilah sesuai dengan literatur, buku maupun dokumen resmi persidangan. Pada bagian ini bukan terjadi proses eliminasi, tetapi proses *merger*.

SIMPULAN

Berdasarkan hasil penelitian, diperoleh kesimpulan bahwa metode teknik analisa yang logis terhadap kerangka kerja yang akan dilakukan (*logical framework approach* (LFA) dapat diterapkan dalam menyusun sebuah *framework* forensik untuk penanganan awal forensik barang bukti sistem kamera pengawas CCTV, yakni dengan cara mengidentifikasi, mengklasifikasi dan mengkolaborasi dokumen forensik yang berbeda dengan menggunakan pemodelan logika berdasarkan terminologi. Berdasarkan hasil identifikasi tersebut maka perlu dilakukan tahapan kolaborasi terhadap proses penting yang diperoleh, sehingga dihasilkan suatu *framerwork* perbaikan untuk penangan awal dilokasi kejadian perkara yang berfokus pada pengambilan video dari sistem CCTV. Jika hal tersebut diterapkan, maka *framework* tersebut mampu memenuhi ketentuan standar yang berlaku dalam menjaga integritas data.

DAFTAR PUSTAKA

Badan Standarisasi Nasional. (2014). SNI 27037:2014 tentang Teknologi Informasi - Teknik Keamanan - Pedoman Identifikasi, Pengumpulan, Akuisisi, dan Preservasi bukti digital.

Lizarti, N., Sugiantoro, B., & Prayudi, Y. (2017). Penerapan Composite Logic dalam mengkolaborasikan Framework Terkait Multimedia Forensik, JISKa, 2(1), 26-33. https://doi.org/10.14421/jiska.2017.21-04.

Panende, M. F., Prayudi, Y., & Riadi, I. (2018). Konsep Attribute Based Access Control (ABAC) pada Lemari Penyimpanan Bukti Digital (LPBD). Jurnal Teknik Informatika, 11(1), 85-94. http://dx.doi.org/10.15408/jti.v11i1.7220.

Strater & Burch (1974) In Information system: Theory and practice. Santa Barbara California: Hamilton Publicity Company, 1974.

Sudyana, D., Sugiantoro, B., & Luthfi, A. (2016). Instrumen evaluasi framework investigasi forensika digital menggunakan SNI 27037: 2014, JISKa, 1(2), 75-83.

SWGIT. (2013). Section 24 Best Practices for Retrieval of Digital Video, 1.0 2013.09.27

Terry, G. R. (2006). Prinsip-prinsip manajemen (Translate from: Guide to management), Jakarta: Bumi Aksara, 2006.

Wahyudi, E., Riadi, I., & Prayudi, Y. (2018). Virtual machine forensic analysis and recovery method for recovery and analysis digital evidence. International Journal of Computer Science And Information Security , 16(2), 1-7.