JISKa, Vol. 1, No. 2, September, 2016, Pp. 75 – 83
ISSN 2527 - 5836

INSTRUMEN EVALUASI *FRAMEWORK* INVESTIGASI FORENSIKA DIGITAL MENGGUNAKAN SNI 27037:2014

Didik Sudyana [(1)], Bambang Sugiantoro [(2)], Ahmad Luthfi [(3)]
Magister Teknik Informatika Universitas Islam Indonesia[(1)]
Jl. Kaliurang Km 14,5 Sleman, Yogyakarta
Teknik Informatika UIN Sunan Kalijaga Yogyakarta [(2)]
e-mail : didik_sudyana@yahoo.co.id

Abstract

The important thing that had to considered by every digital forensic investigator in performing digital forensics activity is followed every stage and procedures in digital forensics. The stages are referred to as frameworks or SOP investigations. Stages in the digital forensics process had to comply with the rule of law and also the appropriate mechanism. But the investigation framework developed at this time was still a shortfall in which there are stages set out in the applicable standards such as SNI 27037:2014, it was not stipulated in the framework. So that when the stage was missed in the investigation, it would be a problem and could be sued in the courts as well as the cancellation of the results of an investigation carried out related to the procedures that were not implemented. Therefore by identified the conditions and processed important in the document SNI 27037:2014 to then produced an evaluation instrument that could be used by the investigator or digital forensics practitioners to made adjustments or evaluation of the framework is used for this.

Keywords : Digital forensics investigation framework, SNI 27037:2014

Hal penting yang harus diperhatikan oleh setiap petugas investigator forensika digital dalam menjalankan aktivitas forensika digital adalah diikutinya setiap tahapan dan prosedur dalam forensika digital. Tahapan tersebut dikenal dengan istilah *framework*s ataupun SOP investigasi. Tahapan dalam proses forensika digital harus sesuai dengan aturan hukum dan juga mekanisme yang tepat. Namun *framework* investigasi yang berkembang saat ini ternyata masih terdapat kekurangan dimana ada tahapan-tahapan yang diatur dalam standar yang berlaku seperti SNI 27037:2014, ternyata tidak diatur dalam *framework* tersebut. Sehingga ketika tahapan tersebut terlewatkan dalam proses investigasi, tentu akan menjadi sebuah masalah dan bisa digugat di pengadilan serta dibatalkannya hasil investigasi yang dilakukan terkait adanya prosedur yang tidak dilaksanakan. Oleh karena itu dilakukan penelitian dengan melakukan identifikasi terhadap ketentuan dan proses penting dalam dokumen SNI 27037:2014 untuk kemudian menghasilkan instrument evaluasi yang dapat digunakan oleh penyidik atau praktisi forensika digital untuk melakukan penyesuaian atau evaluasi terhadap *framework* yang digunakan selama ini.

Kata Kunci : *framework* investigasi, SNI 27037:2014

1. PENDAHULUAN

Perkembangan kejahatan komputer saat ini terus meningkat, bahkan berdasarkan berita yang diterbitkan oleh kompas menyebutkan Indonesia berada diurutan kedua dalam daftar lima besar negara dengan kejahatan siber tertinggi. Masih berdasarkan berita yang diterbitkan kompas juga menyebutkan bahwa dalam jangka waktu tiga tahun belakangan ini, tercatat ada 36,6 juta serangan cyber crime yang terjadi di Indonesia, dan Subdit IT / Cybercrime Bareskrim Polri sendiri telah menangkap 497 orang tersangka sejak tahun 2012 sampai april 2015. Kerugian ditaksir mencapai 33,29 miliar (Kompas.com, 2015). Berdasarkan statistik tersebut dapat dilihat pesatnya perkembangan kejahatan komputer ini.

Untuk dapat mengungkap kasus-kasus kejahatan komputer tersebut, maka digunakan sebuah proses dengan metode *scientific* yang dikenal dengan sebutan forensika digital. Menurut Palmer (2001) forensika digital merupakan ilmu dan metode yang digunakan di dalam pelestarian, pengumpulan, identifikasi, analisis, dokumentasi, dan presentasi barang bukti digital dengan tujuan untuk memfasilitasi atau membuat kemajuan dalam proses rekonstruksi

kejadian kriminal. Dari definisi tersebut dapat diketahui bahwa forensika digital berguna dalam proses investigasi suatu tindak kejahatan kriminal yang melibatkan penggunaan teknologi.

Hal penting yang harus diperhatikan oleh setiap petugas investigator forensika digital dalam menjalankan aktivitas forensika digital adalah diikutinya setiap tahapan dan prosedur dalam forensika digital. Tahapan tersebut dikenal dengan istilah *framework*s. Dalam hal ini menurut Pollitt (1995) tahapan dalam proses forensika digital harus sesuai dengan aturan hukum dan juga mekanisme yang tepat. Hal ini juga didukung oleh Rahayu & Prayudi (2014) yang menyebutkan bahwa menggunakan *framework* dalam investigasi sebuah kasus dapat menuntun proses pembuktian yang prosedural dan menjaga proses tersebut dari kontaminasi barang bukti dan dapat dipertanggungjawabkan dimata hukum. Oleh karena pentingnya panduan yang menghasilkan pembuktian bersifat kajian ilmiah ini, maka dalam penyelesaian sebuah investigasi harus menggunakan *framework* yang telah terstruktur dengan baik.

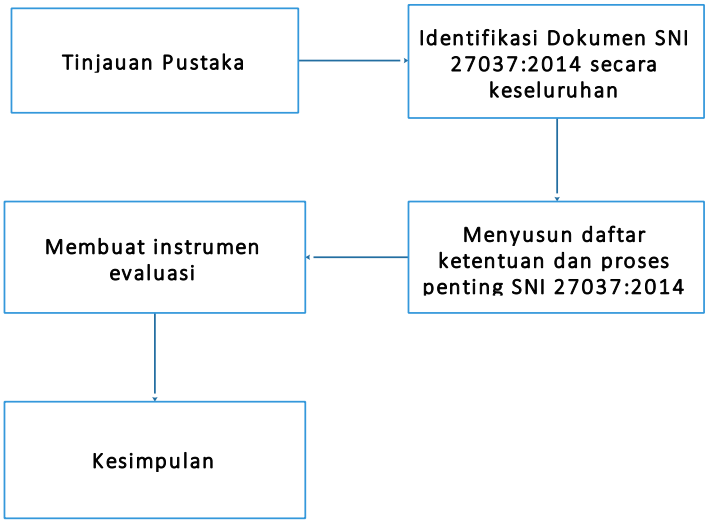
Namun *framework* investigasi yang berkembang saat ini ternyata masih terdapat kekurangan dimana ada tahapan-tahapan yang diatur dalam standar yang berlaku seperti SNI 27037:2014, ternyata tidak diatur dalam *framework* tersebut. Sehingga ketika ada ketentuan dalam standar yang terlewatkan dalam proses investigasi dikarenakan *framework* ataupun SOP yang digunakan tidak mengacu terhadap standar, tentu akan menjadi sebuah masalah dan bisa digugat di pengadilan serta dibatalkannya hasil investigasi yang dilakukan terkait adanya prosedur yang tidak dilaksanakan.

Sebagai contoh *framework* yang dibangun oleh Yusoff, Ismail, & Hassan (2011), ternyata tidak ada tahapan ataupun penjelasan dari tahapan dalam melakukan pengamanan tempat kejadian perkara yang mana hal tersebut diatur dalam SNI 27037:2014. Contoh berikutnya yaitu *framework* yang dibangun oleh Saleem et al. (2014), yang dalam tahapan-tahapan *framework* nya juga tidak terdapat tahapan pengamanan tempat kejadian perkara.

Oleh karena itu diperlukan sebuah penelitian untuk melakukan identifikasi terhadap ketentuan-ketentuan dan proses penting yang terdapat dalam standar yang berlaku. Dimana pada penelitian ini menggunakan SNI 27037:2014. Untuk kemudian dapat menghasilkan sebuah instrument evaluasi sehingga praktisi forensika digital dapat menggunakan instrument tersebut untuk melakukan evaluasi dan menyesuaikan kembali *framework* ataupun SOP nya sehingga dapat memenuhi seluruh ketentuan yang ada dalam standar seperti SNI 27037:2014.

2. METODE PENELITIAN

Secara ringkas metode dan tahapan penelitian yang dilakukan dapat digambarkan seperti pada gambar 1 dibawah ini.



Gambar 1. Metode Penelitian

3. HASIL DAN PEMBAHASAN

SNI 27037:2014 yang berjudul Teknologi Informasi – Teknik Keamanan – Pedoman identifikasi, pengumpulan, akuisisi, dan preservasi bukti digital, merupakan standar forensika digital yang keseluruhan isi dokumennya diadopsi dari ISO 27037:2012 dengan metode republikasi-reprint. SNI 27037:2014 ini merupakan standar nasional yang membahas tentang panduan spesifik terkait aktifitas investigasi forensika digital. Yang mana aktifitas tersebut meliputi identifikasi, pengumpulan, akuisisi, dan preservasi. Kesemua proses ini merupakan proses penting yang harus dilakukan secara hati-hati untuk tetap menjaga integritas barang bukti. Metodologi yang digunakan dalam mengumpulkan barang bukti digital akan berpengaruh terhadap diterima atau tidaknya barang bukti tersebut di pengadilan. Selain membahas barang bukti digital, SNI juga membahas tentang panduan umum tentang bagaimana mengumpulkan non-digital evidence. Karena selain barang bukti digital, barang bukti yang tidak digital juga berpotensi memberikan petunjuk terkait investigasi sebuah kasus kejahatan (Badan Standarisasi Nasional, 2014).

SNI 27037:2014 terdiri dari 7 bab atau 7 bagian yang terdiri dari :

1) *Scope*
   Berisi penjelasan tentang apa yang tercakup atau diatur dalam SNI 27037:2014. Pada bagian ini dijelaskan bahwa SNI merupakan panduan yang secara spesifik mengatur tentang aktivitas penanganan barang bukti digital.

2) *Normative Reference*
   Pada bagian ini berisi tentang dokumen referensi yang digunakan untuk mengembangkan SNI ini. Ada 4 ISO atau standar internasional yang dijadikan dokumen referensi yaitu ISO/TR 15801, ISO/IEC 17020, ISO/IEC 17025:2005, dan ISO/IEC 27000.

3) *Terms and definitions*
   Pada bagian ini berisi tentang istilah-istilah yang digunakan dan penjelasan dari istilah tersebut.

4) *Abbreviated Terms*
   Pada bagian ini berisi tentang singkatan-singkatan yang digunakan. Sebagai contoh AVI yang merupakan singkatan dari *Audio Video Interleave*.

5) *Overview*
   Pada bagian ini berisi tentang overview tentang penjelasan kegiatan penanganan barang bukti digital. Overview terdiri dari 4 bagian yaitu 1) konteks pengumpulan barang bukti, 2) prinsip barang bukti digital, 3) syarat-syarat penanganan barang bukti, dan 4) proses penanganan barang bukti digital.

6) *Key Components of identification, collection, acquisition, and preservation of digital evidence*
   Pada bagian ini berisi penjelasan tentang kegiatan penting yang dilakukan dalam identifikasi, pengumpulan, akuisisi, dan preservasi. Bagian ini terdiri dari 9 pembahasan yaitu 1) chain of custody, 2) tindakan di tempat kejadian perkara, 3) peran dan tanggung jawab petugas, 4) kompetensi yang harus dimiliki petugas, 5) Hal yang harus dilakukan sewajarnya, 6) Dokumentasi, 7) Briefing, 8) Prioritas pengumpulan dan akuisisi, 9) preservasi barang bukti digital yang berpotensi.

7) *Instance of identification, collection, acquisition, and preservation*
   Bagian ini berisi tentang hal-hal atau kegiatan apa saja yang dilakukan dalam identifikasi, pengumpulan, akuisisi, dan preservasi.

Ada 4 tahapan utama yang diatur dalam SNI 27037:2014 yaitu tahapan identifikasi, pengumpulan, akuisisi, dan preservasi. Proses identifikasi terhadap hal-hal atau proses penting

dalam investigasi forensika digital dilakukan dengan melakukan penelitian terhadap keseluruhan isi dokumen SNI 27037:2014. Pengurutan proses dalam hasil identifikasi ini dilakukan berdasarkan tahapan utama yaitu identifikasi, pengumpulan, preservasi, dan akuisisi untuk kemudian isi dari masing-masing tahapan utama disusun berdasarkan penjelasan yang diberikan dalam dokumen SNI 27037:2014. Adapun hasil identifikasi terhadap SNI 27037:2014 untuk memetakan daftar proses penting dalam melakukan investigasi forensika digital yaitu :

A. Identifikasi

1. Perencanaan Investigasi
   Perencanaan investigasi ini diatur oleh SNI pada bagian 6.7.2. Perencanaan dilakukan untuk menyusun strategi terkait investigasi yang akan dilakukan. Mulai dari perencanaan tools yang digunakan, perencanaan teknis investigasi, dan hal terkait lainnya.

2. Persiapan & pengarahan team
   Persiapan & pengarahan team diatur oleh SNI pada bagian ke 6.7. Persiapan dilakukan dengan mempersiapkan seluruh kebutuhan baik itu hal administrasi maupun hal teknis untuk proses investigasi. Pengarahan team dilakukan untuk memastikan seluruh anggota tim investigasi paham dengan kasus yang akan ditangani, apa yang harus dilakukan dan tidak dilakukan selama investigasi, dan mengingatkan untuk selalu menjaga integritas barang bukti.

3. Penilaian resiko keamanan TKP
   Penilaian resiko keamanan TKP diatur dalam SNI pada bagian ke 6.2.2. Penilaian resiko dilakukan untuk menjaga keamanan tim investigasi dan barang bukti. Sebagai contoh untuk menilai apakah di TKP terdapat senjata atau material yang dapat menyebabkan kerusakan fisik.

4. Pengamanan TKP
   Hal ini diatur dalam SNI pada bagian ke 6.2.1. Pengamanan TKP dilakukan untuk melindungi barang bukti. Pengamanan juga dilakukan untuk membatasi tidak semua orang bisa masuk ke TKP dan hanya orang-orang yang telah diziinkan oleh tim.

5. Pencarian barang bukti
   Hal ini diatur dalam SNI pada bagian ke 5.4.2. Pencarian barang bukti merupakan proses dimulainya melihat keseluruh TKP dan mencari apa saja yang berpotensi sebagai barang bukti.

6. Identifikasi barang bukti
   Hal ini diatur dalam SNI pada bagian ke 5.4.2. Melakukan identifikasi baik itu dari sisi jenis, bentuk, dan fungsinya terhadap barang bukti yang ditemukan dari hasil pencarian apakah bisa menjadi barang bukti yang berpotensi. Identifikasi juga melakukan pengecekkan terhadap status barang bukti yang ditemukan semisal apakah dalam keadaan menyala atau tidak.

7. Menentukan prioritas barang bukti
   Hal ini diatur dalam SNI pada bagian ke 6.8. Memberikan prioritas terhadap barang bukti yang ditemukan terhadap aspek kerentanan data tersebut. Barang bukti yang mudah hilang seperti data dalam RAM yang hilang jika komputer mati harus diberikan prioritas. Sehingga barang bukti dengan prioritas tinggi diberikan tindakan yang lebih.

8. Dokumentasi
   Hal ini diatur dalam SNI pada bagian ke 6.6. Segala aktivitias terkait penemuan barang bukti harus didokumentasikan. Dan dokumentasi disini juga mencakup keseluruhan aspek proses yang dilakukan mulai tahapan identifikasi sampai tahapan akhir investigasi yang harus selalu didokumentasikan. Dokumentasi dilakukan untuk menjaga integritas barang bukti.

9. Pencatatan barang bukti (Chain of custody)

Hal ini diatur dalam SNI pada bagian ke 6.1. Chain of custody merupakan catatan rantai perjalanan barang bukti. Jadi ketika barang bukti ditemukan, harus dicatat informasinya dan selanjutnya kemana saja barang bukti tersebut berpindah atau apa saja yang dilakukan terhadap barang bukti harus dicatat di form chain of custody. Hal ini juga dilakukan untuk menjaga integritas barang bukti.

B. Pengumpulan

1. Menentukan barang bukti disita atau diakuisisi di TKP
   Hal ini diatur dalam SNI pada bagian ke 6.8 dan 7.1.1.3. Dari hasil pemberian prioritas barang bukti, akan ditentukan apakah barang bukti yang ditemukan dapat langsung disita atau harus diakuisisi di TKP terkait datanya yang mudah hilang.

2. Melakukan penyitaan barang bukti
   Hal ini diatur dalam SNI pada bagian ke 7.1.2. Penyitaan barang bukti dibagi menjadi dua tahapan yaitu prosedur penyitaan perangkat dalam keadaan menyala dan dalam keadaan mati.
   (a) Barang bukti dalam keadaan menyala
   - Menganalisis apakah membutuhkan data *volatile* dari perangkat
     Hal ini diatur dalam SNI pada bagian ke 7.1.2.1. Analisis dilakukan untuk menentukan apakah dari perangkat yang menyala tersebut membutuhkan data *volatile* yang akan hilang apabila perangkat dimatikan.
   - Jika butuh lakukan prosedur *Live* akuisisi
     Hal ini diatur dalam SNI pada bagian ke 7.1.3.1. Jika hasil analisis menyimpulkan dibutuhkan data *volatile,* maka lakukan prosedur *live* akuisisi terhadap perangkat.
   - Jika tidak butuh lakukan pemeriksaan aspek keamanan dan kerentanan data terhadap listrik
     Hal ini diatur dalam SNI pada bagian ke 7.1.2.1. Jika tidak butuh data *volatile*, atau proses *live* akuisisi telah selesai, lakukan pemeriksaan aspek keamanan data apakah data akan rusak apabila perangkat langsung dimatikan. Jika ternyata data akan rusak jika perangkat langsung dimatikan, lakukan prosedur *shutdown* secara sistem normal.
   - Melakukan prosedur *shutdown* perangkat
     Hal ini diatur dalam SNI pada bagian ke 7.1.2.1. Jika data stabil atau tidak bermasalah apabila perangkat langsung dimatikan, cabut secara langsung kabel power untuk mematikan perangkat.

   (b) Barang bukti dalam keadaan tidak menyala
   - Cabut semua kabel yang terkoneksi dan baterai (jika ada baterai)
     Hal ini diatur dalam SNI pada bagian ke 7.1.2.2. Cabut semua kabel dan amankan kabel tersebut, lalu label seluruh port yang terkoneksi dengan kabel untuk memudahkan proses rekonstruksi. Setelah prosedur ini selesai, maka lakukan prosedur selanjutnya yaitu memberikan label barang bukti.

3. Memberikan label barang bukti
   Hal ini diatur dalam SNI pada bagian ke 7.1.2. Label seluruh barang bukti untuk memudahkan proses rekonstruksi dan memudahkan mengenali barang bukti tersebut.

4. Mempacking barang bukti
   Hal ini diatur dalam SNI pada bagian ke 7.1.2. *Packing* atau lakukan proses pengemasan barang bukti dengan memasukkan barang bukti ke dalam alat pembungkus barang bukti. Perhatikan aspek keamanan barang bukti ketika akan dikemas. Sebagai contoh, perangkat yang terkoneksi ke jaringan wireless seperti *smartphone* harus dikemas dalam alat pembungkus khusus yang dapat menetralisir sinyal tersebut.

5. Mengumpulkan keterangan verbal dari saksi-saksi
   Hal ini diatur dalam SNI pada bagian ke 7.1.1.2. Hal ini dilakukan untuk mendapatkan petunjuk lebih dan mencari informasi terkait barang bukti yang ditemukan. Sebagai contoh menanyakan password sistem yang ditemukan dalam barang bukti.

C. Akuisisi

1. Pemeriksaan aspek keamanan barang bukti
   Hal ini diatur dalam SNI pada bagian ke 7.1.1.1. Pemeriksaan aspek keamanan untuk memastikan bahwa proses akuisisi yang dilakukan tidak akan merusak barang bukti.

2. Penentuan model akuisisi yang dilakukan
   Hal ini diatur dalam SNI pada bagian ke 7.1.3. Proses akuisisi terbagi menjadi 3 jenis yaitu akuisisi pada perangkat menyala, akuisisi pada perangkat yang tidak menyala dan partial akuisisi. Penentuan model akuisisi yang digunakan sesuai hasil identifikasi yang telah dilakukan terhadap barang bukti.
   (a) Akuisisi pada perangkat yang menyala
   - Lakukan prosedur *live akuisisi* untuk mendapatkan data *volatile*
     Hal ini diatur dalam SNI pada bagian ke 7.1.3.1. Data *volatile* akan dapat hilang apabila perangkat digitalnya dimatikan, oleh karena itu *live* akuisisi dilakukan ketika perangkat masih dalam keadaan menyala. Beberapa contoh data *volatile* yaitu data di RAM, data proses yang berjalan, data koneksi jaringan. Petugas harus berkompetensi dan menggunakan tools yang valid untuk melakukan prosesdur ini.
   - Jika data *non volatile* juga dibutuhkan saat itu, lakukan juga prosedur akuisisi pada data *non volatile*
     Hal ini diatur dalam SNI pada bagian ke 7.1.3.1. Lakukan juga prosedur *live* akuisisi jika data *non volatile* seperti data yang tersimpan di *logical* juga dibutuhkan.
   - Jika perangkat bisa disita, lakukan prosedur pengumpulan barang bukti
     Hal ini diatur dalam SNI pada bagian ke 7.1.3.1. Jika setelah proses akuisisi pada data *volatile* selesai dan perangkat dapat disita lakukan prosedur pengumpulan barang bukti. Perangkat yang tidak dapat disita sebagai contoh komputer server yang sangat krusial terhadap sistem yang sedang berjalan.

   (b) Akuisisi pada perangkat yang tidak menyala
   - Lakukan prosedur *static* akuisisi dengan melakukan *imaging* terhadap media penyimpanan data
     Hal ini diatur dalam SNI pada bagian ke 7.1.3.2. Proses *static* akuisisi dijalankan dengan melakukan *bitstream copy.*

   (c) *Partial* Akuisisi
   - Dapat dilakukan dengan menggunakan perpaduan prosedur *live* dan *static* akuisisi
     Hal ini diatur dalam SNI pada bagian ke 7.1.3.4. *Partial* akuisisi dilakukan untuk perangkat yang krusial dan tidak dimungkinkannya melakukan akuisisi terhadap keseluruhan data seperti dikarenakan jumlah data yang sangat besar.

3. Pelaksanaan akuisisi
   Setelah proses penentuan metode akuisisi dipilih, berikutnya adalah dilaksanakan proses akuisisi sesuai dengan metode akuisisi yang telah ditentukan sebelumnya.

4. Verifikasi hasil akuisisi
   Hal ini diatur dalam SNI pada bagian ke 7.1.4. Verifikasi dilakukan untuk memastikan data hasil akuisisi identic dengan data aslinya. Verifikasi dapat dilakukan dengan menggunakan fungsi hash.

D. Preservasi

1. Memberikan segel barang bukti
   Hal ini diatur dalam SNI pada bagian ke 6.9.2. Barang bukti yang telah dipacking, harus disegel untuk memastikan selama proses pemindahan barang bukti tetap dalam kemasannya dan berguna menjaga integritas barang bukti.

2. Pemeriksaan aspek keamanan pemindahan barang bukti
   Hal ini diatur dalam SNI pada bagian ke 6.9.2. Pemeriksaan aspek keamanan dilakukan untuk memastikan barang bukti aman selama proses pemindahan barang bukti dari

TKP ke tempat penyimpanan ataupun laboratorium. Pemeriksaan aspek keamanan mencakup pemeriksaan pengemasan barang bukti untuk menjaga pengemasan yang dilakukan tidak merusak barang bukti.

3. Pemindahan barang bukti
   Hal ini diatur dalam SNI pada bagian ke 6.9.2. Selama proses pemindahan barang bukti, petugas harus berhati-hati dan selalu memperhatikan keamanan barang bukti. Selain itu juga harus melakukan update di form chain of custody.

4. Penyimpanan barang bukti
   Hal ini diatur dalam SNI pada bagian ke 6.9.2. Barang bukti harus disimpan dalam tempat penyimpanan yang memiliki fasilitas keamanan yang baik dan fasilitas penyimpanan yang baik. Sebagai contoh harus memiliki fasilitas untuk menjaga suhu ruangan penyimpanan tidak terlalu panas atau tidak terlalu dingin sehingga dapat menyebabkan kerusakan barang bukti.

Berdasarkan hasil identifikasi terhadap ketentuan dan proses penting yang terdapat dalam SNI 27037:2014 tersebut, maka dapat dihasilkan sebuah instrument yang dapat digunakan praktisi forensika digital untuk melakukan evaluasi dan menyesuaikan kembali *framework* ataupun SOP nya sehingga dapat memenuhi seluruh ketentuan yang ada dalam SNI 27037:2014. Adapun bentuk instrument tersebut dapat dilihat pada tabel 2 dibawah ini.

Tabel 2. Instrumen Evaluasi *Framework*/SOP Berdasarkan SNI 27037:2014

Proses Penting SNI 27037:2014	**Kelengkapan dalam *Framework* / SOP**	
	Ada	**Tidak**
Identifikasi		
Perencanaan investigasi		
Persiapan peralatan & pengarahan team		
Penilaian resiko keamanan TKP		
Pengamanan TKP		
Pencarian barang bukti		
Identifikasi barang bukti		
Menentukan prioritas barang bukti		
Dokumentasi		
Pencatatan barang bukti *(Chain of custody)*		
Pengumpulan		
Menentukan barang bukti disita atau diakuisisi di TKP		
Melakukan penyitaan barang bukti		
• Barang bukti dalam keadaan menyala		
- Menganalisis apakah membutuhkan data *volatile* dari perangkat		
- Jika butuh lakukan prosedur *Live* akuisisi		
- Jika tidak butuh lakukan pemeriksaan aspek keamanan dan kerentanan data terhadap listrik		
- Melakukan prosedur *shutdown* perangkat		
• Barang bukti dalam keadaan tidak menyala		
- Cabut semua kabel yang terkoneksi dan baterai (jika ada baterai)		
- Lakukan prosedur pengumpulan berikutnya		
Memberikan label barang bukti		
Mempacking barang bukti		

Proses Penting SNI 27037:2014	Kelengkapan dalam *Framework* / SOP	
Mengumpulkan keterangan verbal dari saksi-saksi		
Akuisisi		
Pemeriksaan aspek keamanan data barang bukti		
Penentuan model akuisisi yang dilakukan		
• Akuisisi pada perangkat yang menyala		
- Lakukan prosedur *live akuisisi* untuk mendapatkan data *volatile*		
- Jika data *non volatile* juga dibutuhkan saat itu, lakukan juga prosedur akuisisi pada data *non volatile* tersebut		
- Jika perangkat bisa disita, lakukan prosedur pengumpulan barang bukti		
• Akuisisi pada perangkat yang tidak menyala		
- Lakukan prosedur *static* akuisisi dengan melakukan *imaging* terhadap media penyimpanan data		
• *Partial* Akuisisi		
- Dapat dilakukan dengan menggunakan perpaduan prosedur *live* dan *static* akuisisi		
Pelaksanaan akuisisi		
Verifikasi hasil akuisisi		
Preservasi		
Memberikan segel barang bukti		
Pemeriksaan aspek keamanan pemindahan barang bukti		
Pemindahan barang bukti		
Penyimpanan barang bukti		

Dengan menggunakan instrument ini, maka praktisi forensika digital yang ikut terlibat dalam melakukan investigasi forensika digital dapat menyesuaikan kembali SOP atau *framework* yang digunakan sehingga investigasi yang dilakukan tidak melewatkan ketentuan yang telah diatur dalam standar yang berlaku seperti SNI 27037:2014.

4. KESIMPULAN

Berdasarkan hasil penelitian yang dilakukan, maka didapatkan kesimpulan yaitu berdasarkan hasil identifikasi terhadap dokumen SNI 27037:2014, didapatkan bahwa terdapat 38 proses penting yang diatur oleh SNI 27037:2014 dalam melakukan investigasi forensika digital. Dari hasil identifikasi tersebut maka dapat dihasilkan sebuah instrument yang dapat berguna bagi penyidik ataupun praktisi forensika digital untuk melakukan penyesuaian atau pengecekkan terhadap SOP / *framework* investigasinya sehingga proses investigasi yang dilakukan telah mengikuti standar yang berlaku.

DAFTAR PUSTAKA

Badan Standarisasi Nasional. (2014). *SNI 27037:2014 tentang Teknologi Informasi - Teknik Keamanan - Pedoman Identifikasi, pengumpulan, Akuisisi, dan Preservasi Bukti Digital*. Jakarta.

Palmer, G. (2001). A Road Map for Digital Forensic Research. *Proceedings of the 2001 Digital Forensics Research Workshop (DFRWS 2004)*, 1–42. http://doi.org/10.1111/j.1365-2656.2005.01025.x

Permana, F. A. (2015, May 12). Indonesia Urutan Kedua Terbesar Negara Asal Cyber Crime di Dunia. *Kompas.com*. Jakarta. Retrieved from http://nasional.kompas.com/read/2015/05/12/06551741/Indonesia.Urutan.Kedua.Terbesar.Negara.Asal.Cyber.Crime.di.Dunia

Pollitt, M. (1995). Computer Forenscs: And Approach to Evidence in Cyberspace. *National Information System Security Conference*, 487–491.

Rahayu, Y. D., & Prayudi, Y. (2014). Membangun Integrated Digital Forensics Investigation *Framework*s (IDFIF) Menggunakan Metode Sequential Logic. *Seminar Nasional SENTIKA*, *2014*(Sentika).

Saleem, S., Popov, O., & Bagilli, I. (2014). Extended abstract digital forensics model with preservation and protection as umbrella principles. *Procedia Computer Science*, *35*(C), 812–821. http://doi.org/10.1016/j.procs.2014.08.246

Yusoff, Y., Ismail, R., & Hassan, Z. (2011). Common Phases of Computer Forensics Investigation Models. *International Journal of Computer Science and Information Technology*, *3*(3), 17–31. http://doi.org/10.5121/ijcsit.2011.3302