Pelatihan Investigasi Digital Forensik

Rizdqi Akbar Ramadhan[a], Abdul Kudus Zaini[b], dan Jerika Mardafora[c]
[ac]Program Studi Teknik Informatika, Universita Islam Riau, Pekanbaru, 28284, INDONESIA
[b]Program Studi Teknik Sipil, Universitas Islam Riau, Pekanbaru, 28284, INDONESIA

Penulis Koresponden: Rizdqi Akbar Ramadhan (e-mail: rizdqiramadhan@eng.uir.ac.id)

ABSTRAK Dalam era digital pada revolusi industri 4.0, perangkat komputer telah menjadi suatu benda yang berdampingan dengan manusia. Komputer memiliki peran dalam pesatnya perkembangan peradaban, hal ini karena efisiensi kerja yang ditawarkannya. *Digital forensic* adalah bidang ilmu serta teknik penyelidikan melalui analisis komputer untuk menentukan potensi bukti legal, secara khusus yaitu *cyber crime*. Berbeda dari pengertian forensik pada umumnya, *computer forensic* dapat diartikan sebagai pengumpulan dan analisis data dari berbagai sumber daya komputer yang mencakup sistem komputer, jaringan komputer, jalur komunikasi, dan berbagai media penyimpanan yang layak untuk diajukan dalam sidang pengadilan. Ada beberapa tahapan dalam *computer forensic*, yaitu; pengumpulan data, pengujian, analisis serta dokumentasi dan laporan. Dari tahapan – tahapan tersebut akan diketahui apa, di mana, bagaimana, siapa dan kapan kasus terjadi. Pada tahapan pengumpulan data akan dilakukan suatu proses *image* data dalam artian *cloning* bukti digital yang telah diperoleh sehingga ketika terjadi suatu kesalahan tidak akan merusak bukti digital atau *evidence* yang asli. Segala prosedur dari tahapan-tahapan yang dijabarkan diatas, dalam ilmu digital forensic disebut dengan akuisisi. Pelatihan yang dilaksanakan pada Universitas Islam Indragiri ini diikuti oleh 15 peserta mahasiswa semester 7 yang telah mengenal arsitektur komputer secara mendasar. Materi pada pelatihan ini mencakup pada pengenalan dasar digital forensic, dilanjutkan dengan praktek akuisisi bukti digital. Metode yang digunakan pada pelatihan akuisisi bukti digital ini adalah *static forensic.*

KATA KUNCI Akuisisi, Cyber Crime, Digital forensic, Pelatihan, Revolusi Industri 4.0

1. PENGANTAR

Kejahatan dunia maya setiap tahunnya mengalami peningkatan yang sangat pesat, hal ini dikarenakan semakin berkembangnya teknologi komputer yang berdampak pada kehidupan manusia. Segala kemudahan yang didapat dari teknologi komputer pada kenyataannya tidak hanya berdampak baik bagi kehidupan manusia karena beberapa diantaranya ternyata juga ikut memberikan dampak yang buruk. Banyak orang yang memanfaatkan teknologi komputer sebagai media untuk melakukan tindak kejahatan yang bertentangan dengan hukum. Beragam tujuan yang dimiliki para pelaku ini beberapa diantaranya adalah untuk mencari kesenangan, mencari keuntungan dengan memanipulasi transaksi keuangan perbankan dan ada juga untuk kepentingan mata – mata antara beberapa negara. Banyak cara yang dilakukan untuk mempermudah kegiatan kejahatan yang melibatkan teknologi komputer ini salah satunya adalah memanfaatkan kelemahan sistem jaringan komputer dengan menyusupkan program yang digunakan sebagai media untuk mencuri informasi dari sebuah sistem komputer. Penanganan tindak kejahatan yang melibatkan teknologi komputer masih sangat awam untuk saat ini. Digital forensik adalah ilmu yang mempelajari tentang bagaimana cara untuk menangani berbagai kejahatan yang melibatkan teknologi komputer. Ada beberapa teknik didalam digital forensik salah satunya adalah static forensics yang digunakan untuk menangani kejahatan komputer yang menggunakan pendekatan terhadap sistem komputer yang sederhana merupakan suatu jejak digital yang tersimpan dalam penyimpanan komputer (non-volatile). Static forensics menjadi solusi yang sangat tepat untuk mengatasi permasalahan terkait jejak digital, artefak digital serta pola kejahatan digital dengan bantuan sistem komputer. Jejak digital dapat ditelusuri menggunakan teknik akusisi digital forensik dengan menggunakan aplikasi pendukung.

Lebih jauh, seperti yang pernah disampaikan oleh (Dezfoli et al., 2013) bahwa digital forensic merupakan "*the procedure of investigating computer crimes in the cyber world*". Sementara itu, (Prayudi et al., 2014) menjelaskan bahwa upaya pengungkapan *Cybercrime* dilakukan melalui proses investigasi yang dikenal dengan istilah Forensika Digital (*Digital Forensics*). Masih menurut (Prayudi et al., 2014) juga menyebutkan bahwa digital forensic adalah penggunaan ilmu dan metode untuk menemukan, mengumpulkan, mengamankan, menganalisis, menginterpretasi dan mempresentasikan barang bukti digital dalam rangka kepentingan rekontruksi kejadian serta memastikan keabsahan pada proses peradilan. Jauh sebebelumnya, dalam artikel yang dikutip oleh (Beebe & Clark, 2005), sudah pernah menyampaikan terminologi awal dari istilah digital forensics, yaitu "*The use of scientifically derived and proven methods toward the preservation, collection, validation, identification, analysis,*

*interpretation, documentation, and presentation of digital evidence1 derived from digital sources for the purpose of facilitation or furthering the reconstruction of events found to be criminal, or helping to anti*cipate *unauthorized actions shown to be disruptive to planned operations*." Salah satu aspek penting dalam pelaksanaan investitasi digital forensic adalah *Scientific Method*, artinya setiap tahapan dan langkah yang dilakukan oleh Tim investigasi ataupun oleh lembaga hukum harus menjunjung tinggi kaidah metode ilmiah. Berdasarkan beberapa definisi dan deskripsi sebelumnya, dapat dirumuskan bahwa digital forensic merupakan sebuah langkah yang terstruktur dalam melakukan proses investigasi serta penanganan barang bukti untuk meminimalkan adanya kesalahan dalam proses investigasi (Mabuto & Venter, 2011).

Secara harfiah, aktivitas digital forensic melibatkan banyak aktor. Seperti apa yang pernah disampaikan oleh (Jasmin & Cosic, 2015), bahwa aktivitas digital forensic akan melibatkan sejumlah pihak seperti *first responder, forensics investigator, court expert witness, attorney, judge, police officer, victim, suspect* dan *passerby*. Seharusnya terdapat pula gambaran tentang bagaimana interaksi diantara petugas (*investigator*) serta interaksi dengan bukti digital dalam keseluruhan rangkaian proses investigasi. Salah satu metode atau pendekatan yang dapat dijadikan solusi dalam fenomena ini adalah dengan pendekatan model bisnis. Dengan pendekatan ini, maka gambaran atau potret tentang bagaimana interaksi antar aktor atau entitas yang dimaksud dapat terhubung dan integrasi dengan baik.

2. STUDI KEPUSTAKAAN

2.1 Komputer/Digital Forensik

Menurut, (Dezfoli et al., 2013) forensik merupakan serangkaian metode teknik dan prosedur untuk mengumpulkan bukti dari peralatan dan berbagai perangkat penyimpanan media komputasi digital, yang dapat disajikan di pengadilan dalam format yang koheren dan bermakna. Menurut (ADELSTEIN, 2006) Pemeliharaan, identifikasi, ekstraksi, interpretasi, dan dokumentasi bukti komputer, untuk memasukan aturan bukti, proses hukum, integritas bukti, pelaporan faktual dari informasi yang ditemukan, dan memberikan pendapat ahli dalam pengadilan hukum atau lainnya hukum dan atau proses administratif sebagaimanadengan apa yang ditemukan. Digital Forensik adalah aktivitas yang berhubungan dengan pemeliharaan, identifikasi, pengambilan/penyaringan, dan dokumentasi bukti digital dalam kejahatan komputer. (Ramadhan et al., 2017)

Digital forensic adalah penyelidikan dan analisis komputer untuk menentukan potensi bukti legal. Berbeda dari pengertian forensik pada umumnya, *computer forensic* dapat diartikan sebagai pengumpulan dan analisis data dari berbagai sumber daya komputer yang mencakup sistem komputer, jaringan komputer, jalur komunikasi, dan berbagai media penyimpanan yang layak untuk diajukan dalam sidang pengadilan. Menurut (Prayudi & SN, 2015) dalam publikasi yang berjudull Problema dan Solusi Digital Chain of Custody Dalam Proses Investigasi Cybercrime, salah satu faktor penting dalam proses investigasi adalah hal terkait dengan barang bukti. Dalam hal ini terdapat dua istilah yang hampir sama, yaitu barang bukti elektronik dan barang bukti digital. Barang bukti elektronik adalah bersifat fisik dan dapat dikenali secara visual (komputer, Handphone, Camera, CD, Hardisk, dan lain- lain). Sementara barang bukti digital adalah barang bukti yang diekstrak atau di- recover dari barang elektronik (file, email, sms, imafe, video, log, text). Definisi sederhana "Penggunaan sekumpulan prosedur untuk melakukan pengujian secara menyeluruh suatu sistem komputer dengan mempergunakan Software dan tool untuk mengekstrak dan memelihara barang bukti tindakan kriminal". Menurut Judd Robin, seorang ahli *computer forensic*: "Penerapan secara sederhana dari penyelidikan komputer dan teknik analisisnya untuk menentukan bukti-bukti hukum yang mungkin". New Technologies memperluas definisi Robin dengan: "*Computer forensic* berkaitan dengan pemeliharaan, identifikasi, ekstraksi dan dokumentasi dari bukti-bukti komputer yang tersimpan dalam wujud informasi magnetik".

2.2 Bukti Digital

Barang bukti pada dasarnya sama yaitu merupakan informasi dan data, hanya saja kompleksitas dan media penyimpanannya yang mengubah sudut pandang dalam penanganannya. Barang bukti digital dalam komputer forensik secara garis besar terbagi menjadi 3 jenis, yaitu (Mrdovic et al., 2009):

1. Data aktif, yaitu data yang terlihat dengan mudah karena digunakan untuk berbagai kepentingan yang berkaitan erat dengan kegiatan yang sedang dilakukan, misalnya program, file gambar, dan dokumen teks.
2. Data arsip, yaitu data yang telah disimpan untuk keperluan backup misalnya dokumen file yang didigitalisasi untuk disimpan dalam format TIFF dengan tujuan menjaga kualitas dokumen.
3. Data laten, disebut juga data ambient yaitu data yang tidak dapat dilihat langsung karena tersimpan pada lokasi yang tidak umum dan dalam format yang tidak umum misalnya, database log dan internet log. Data laten juga disebut sebagi Resudial data yang artinya adalah data sisa ataupun data sementara.

2.3 Akuisisi Barang Bukti

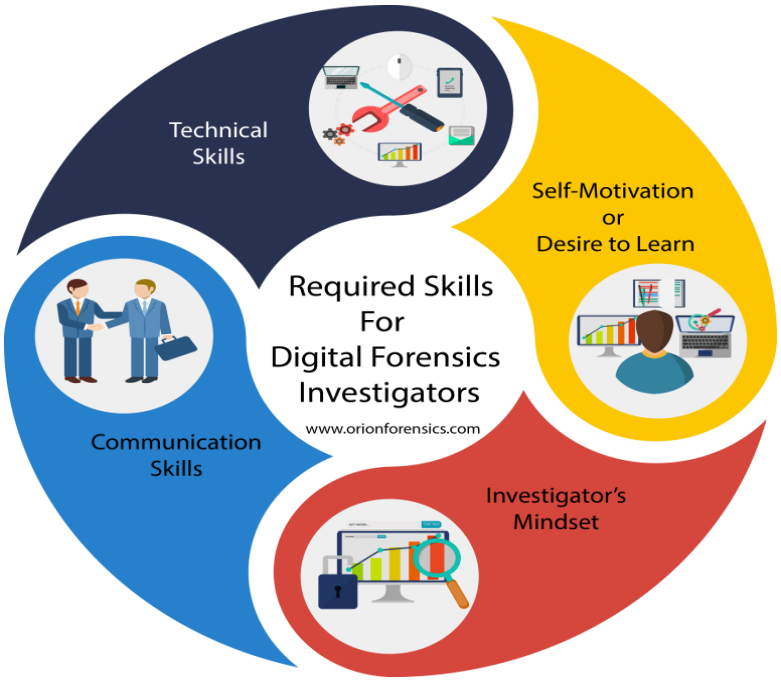
Menurut dokumen SNI 27037:2014, akuisisi merupakan proses untuk membuat salinan barang bukti digital dan mendokumentasikan metodologi yang digunakan serta aktifitas yang dilakukan. Petugas yang melakukan akuisisi harus memilih metode yang paling sesuai berdasarkan situasi, biaya dan waktu, dan mendokumentasikan keputusan yang dipilih untuk menggunakan metode tertentu dan tool yang sesuai. Metode yang dipilih juga harus dapat dipraktekkan, dapat diulang kembali prosesnya dengan hasil yang sama, dan dapat diverifikasi bahwa hasil salinan sama persis dengan barang bukti yang asli. Dalam keadaan dimana proses verifikasi tidak dapat dilakukan, sebagai contoh ketika proses akuisisi yang sedang berjalan, tiba-tiba salinan asli yang sedang dibuat mengalami error sectors, maka dalam kasus seperti ini petugas investigasi yang melakukan akuisisi harus memilih metode yang paling memungkinkan untuk melakukan proses akuisisi ulang dan mendokumentasikannya, lalu dapat menjelaskan kenapa dilakukan akuisisi ulang dan dapat mempertahankan argumennya (Riadi et al., 2018).

2.4 Static Forensic

Penelitian (Rafique & Khan, 2013) telah menjelaskan bahwa Digital Forensic dibagi menjadi dua metode, yaitu Static Forensics dan Live Forensics. Static Forensics menggunakan prosedur dan pendekatan konvensional di mana barang bukti elektronik di olah secara bit-by-bit image untuk melakukan proses forensik. Proses forensiknya sendri berjalan pada sistem yang tidak dalam keadaan menyala atau running (off). Static Forensic difokuskan pada pemeriksaan hasil imaging untuk menganalisis isi dari bukti digital, seperti file yang dihapus, history web browsing, berkas fragmen, koneksi jaringan, file yang diakses, history login user, dll guna membuat timeline berupa ringkasan tentang kegiatan yang dilakukan pada bukti digital sewaktu digunakan. Dalam analisis Static, segala kebutuhan analisis forensik diperoleh dengan menggunakan berbagai jenis perangkat eksternal seperti USB. Kemudian data ini dibawa ke laboratorium forensik untuk investigator melakukan berbagai jenis operasi / langkah-langkah untuk analisa forensik.

3. METODOLOGI

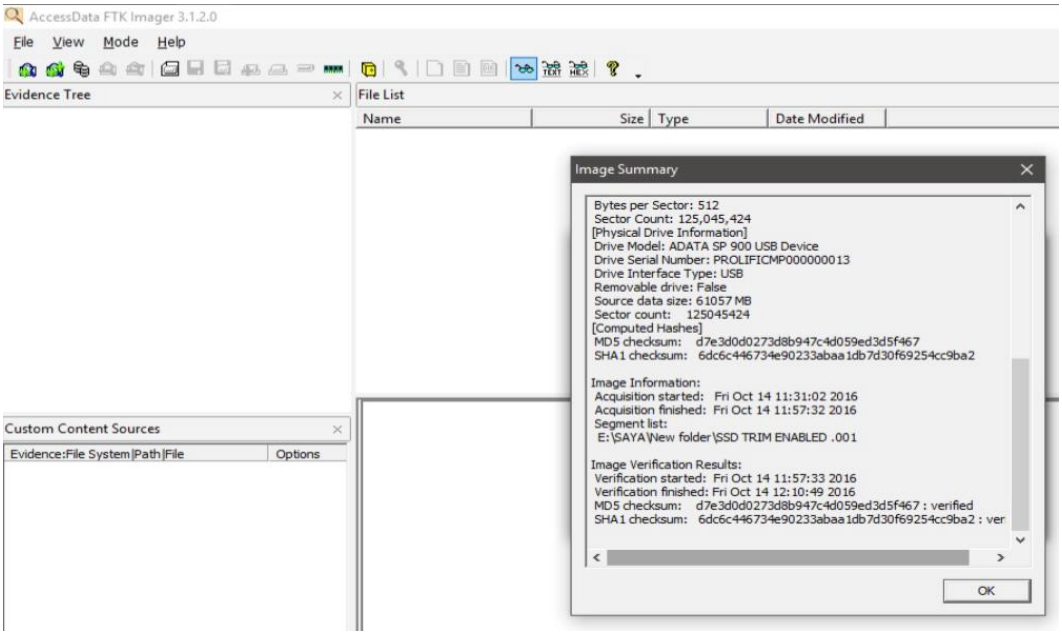
Sebelum digital forensic berkembang, ketika terjadi suatu kasus ahli forensik kedokteran amat sangat dibutuhkan, namun sekarang tidak hanya ahli forensik kedokteran saja, akan tetapi ahli forensik dibidang teknologi juga sangat dibutuhkan untuk mencari bukti dari suatu kasus sehingga kasus tersebut dapat dipecahkan. Ketika seorang tersangka menggunakan barang digital maka akan terdapat bukti atau log pada barang tersebut, yang mana barang itu dapat dijadikan bukti kejahatan dihadapan pengadilan, untuk mendapatkan bukti digital dibutuhkan komputer/digital forensik. Pada gambar 1 dijelaskan terdapat 4 keahlian mendasar dalam urgensi investigasi digital forensik.



Gambar 1. Keahlian Dasar yang Dibutuhkan Dalam Investigasi Digital Forensik

3.1 Pengenalan dan Implementasi Forensic Tool Kit

Berdasarkan *guidelines* yang di terbitkan oleh ACPO, NIST, NIJ; Bukti digital yang dapat dianalisa secara forensik harus di *image* terlebih dahulu. Imaging merupakan salah satu tahapan awal akuisisi dimana ini memungkinkan bukti fisik (seperti penyimpanan *storage non-volatile*) di kloning/digandakan menjadi bukti secara digital. Hal ini memungkinan integritas barang bukti asli, karena investigator hanya diperbolehkan menaganalisa hasil kloning barang bukti asli saja. Tentunya hal ini menggunakan *tools* forensik, diantaranya adalah FTK *Image*r yang merupakan bagian dari FTK (*Forensc ToolKit*). Setelah proses imaging selesai dilakukan maka akan dilakukan analisis terhadap bukti tersebut. Dalam pelatihan ini, penggunaan FTK merupakan awal dari simulasi proses investigasi. Pada gambar 2 ditampilkan logo beserta *interface* dari FTK:



Gambar 2. User Interface dari Forensic Tool Kit Imager (FTK)

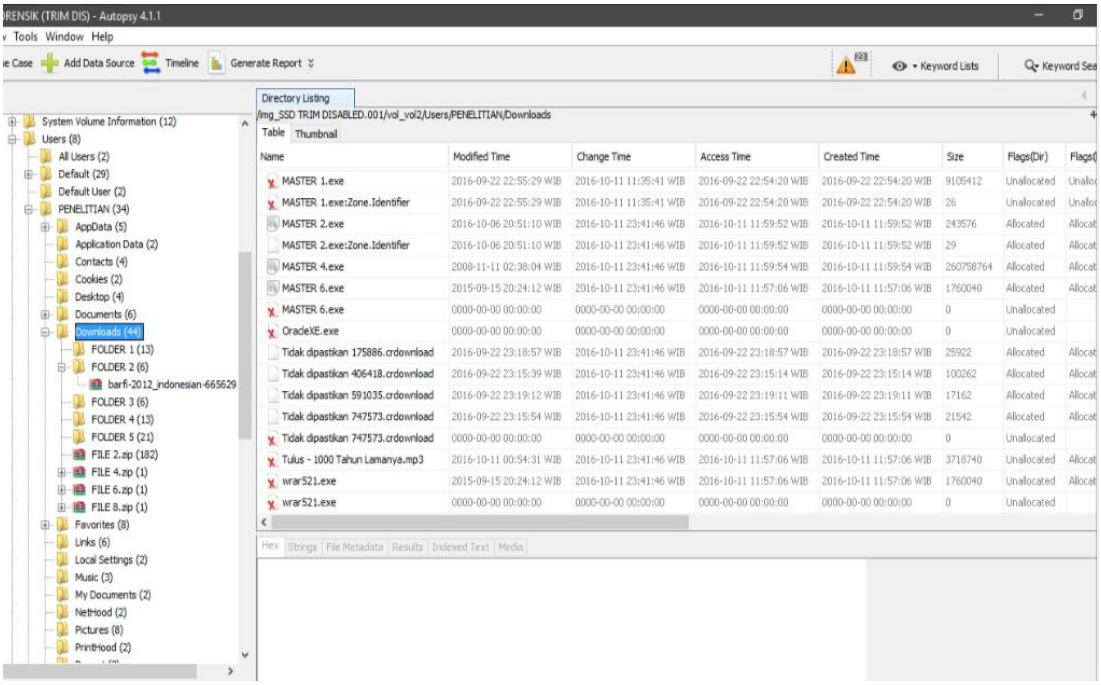
3.2 Pengenalan dan Implementasi Tools Autopsy Forensic

Bukti digital yang telah dilakukan praktek imaging menggunakan FTK imager, merupakan satu bentuk file yang berukuran sesuai dengan kapasitas barang bukti yang didapatkan. Namun, FTK imager tidak memiliki kemampuan untuk melakukan ekstraksi terhadap artefak-artefak dari kesatuan file storage yang telah di-kloning. Dalam hal analisa ini, investigator digital forensik menggunakan kontribusi dari tools yang bernama Sleuth Kit Autopsy Forensik, yang biasa disebut dengan Autopsy Forensik. Autopsy Forensik memungkinkan investigator melakukan analisa secara detail hingga pada hirarki paling bawah dari suatu organisasi komputer khususnya sistem operasi. Tools ini bekerja sesuai dengan volume serta kekuatan perangkat keras yang dijalankan, *Obstacle* atau kendala tentunya potensial terhadap aktifitas apapun, tidak terkecuali dalam aktifitas investigasi forensik ini. Permasalahan durasi pemrosesan serta reliabilitas perangkat adalah yang lazim terjadi, oleh karena itu dokumentasi serta *timestamp* dalam aktifitas ini sangat diperlukan. Dapat disimpulkan bahwa antara FTK Imager dan Autopsy Forensik bekerja secara parsial namun kedua tools ini saling memiliki ketergantungan atas luaran yang dihasilkan. Dalam pelatihan ini penggunaan tools ini dibebankan kepada barang bukti yang ber-volume kecil sehingga dapat menghasilkan efisiensi waktu baik serta meminimalisir aspek reliabilitas yang potensial. Baik FTK maupun autopsy merupakan tools freeware yang dapat diimplementasikan pada sistem operasi berbasis desktop seperti Windows, Linux, dan Macintosh. Tampilan dari tools Sleuth Kit Autposy Forensik dapat dilihat pada Gambar 3.

4. HASIL DAN PELAKSANAAN

Pelatihan Investigasi Digital Forensik yang dilaksanakan pada Universitas Islam Indragiri (UNISI) Fakultas Ilmu Komputer, 8 September 2022 pukul 07.30 hingga 12.00 WIB. Pelatihan ini diawali dengan kata sambutan oleh Dekan Fasilkom UNISI yaitu Bapak Dr. Abdullah S.Si., M.Kom dilanjutkan dengan kunjungan ke laboratorium dimana segala kebutuhan perangkat keras dan

perangkat lunak disediakan. Pelatihan ini dipimpin oleh Bapak Rizdqi Akbar Ramadhan, M.Kom yang sekaligus berperan sebagai pemateri.



Gambar 3. User Interface dari Sleuth Kit Autopsy Forensic

Acara pelatihan ini terbagi atas 4 sesi yaitu; pembukaan/perkenalan, pemaparan teori, praktek investigasi forensik, lalu diakhiri dengan tanya jawab beserta foto bersama. Pelatihan terdiri dari 30 mahasiswa/i, yang awalnya hanya ditargetkan untuk 20 peserta saja. Hal ini tentunya merupakan hal yang baik, karena antusiasme peserta dalam ingin mempelajari ilmu baru terbilang tinggi. Peserta yang sebagian merupakan mahasiswa semester 5 ini memiliki kemampuan dasar di bidang organisasi dan arsitektur komputer. Dari sisi komunikasi dua arah pada saat kegiatan berlangsung juga terbilang cukup baik, hal ini dibuktikan dengan aktifnya peserta dalam memberikan pertanyaan yang relevan dengan materi pelatihan dilanjutkan dengan kompetensi peserta dalam menjawab pertanyaan-pertanyaan dari pemateri. Selanjutnya untuk memberikan apresiasi terhadap peserta pelatihan ini, tim pemateri dari Universitas Islam Riau memberikan sertifikat pelatihan yang ditandatangani oleh pemateri yakni Bapak Rizdqi Akbar Ramadhan. Pada Gambar 4 diperlihatkan aktiftas yang berjudul "Pelatihan Investigasi Digital Forensik" ini.

(a) (b)

Gambar 4. Aktifitas Pelatihan Digital Forensik (a) Simulasi Laboratorium Forensik (b) Peserta Pelatihan Digital Forensik.

5. KESIMPULAN

Kegiatan Pelatihan ini merupakan kewajiban Tri Dharma yang dilaksanakan pada Universitas Islam Indragiri Hilir. Kegiatan ini dilaksanakan sesuai dengan perencanaan yang telah ditetapkan. Judul Pelatihan Investigasi Digital Forensik ini dipilih berdasarkan bidang keahlian pemateri kegiatan ini. Secara teknis lapangan, kegiatan ini bertempat pada Kabupaten Indragiri Hilir, Kota Tembilahan yang berjarak 330 KM dari Universitas pemateri, yaitu Universitas Islam Riau. Dalam pelaksanaanya, kegiatan ini diharapkan dapat memberikan ilmu terkait digital forensik beserta pengembangan kedepannya dari sudut pandang mahasiswa peserta pelatihan. Saran kedepannya untuk pelatihan ini adalah diharapkannya antusiame yang lebih tinggi lagi dari peserta lalu lebih tersedianya lagi fasilitas yang lebih mendukung sesuai dengan relevansi perkembangan zaman di era teknologi ini.

UCAPAN TERIMA KASIH

Penulis mengucapkan terima kasih kepada Direktorat Penelitian dan Pengabdian kepada Masyarakat (DPPM) Universitas Islam Riau yang telah mendukung kegiatan ini melalui skema pengabdian internal, serta ucapan terima kasih kepada Fakultas Ilmu Komputer Universitas Islam Indragiri atas terlaksananya kegiatan Pelatihan Investigasi Digital Forensik.

DAFTAR PUSTAKA

ADELSTEIN, F. (2006). Diagnosing your system without killing it first. *Live Forensics: Diagnosis Your System Without Killing It First*, *49*(2), 63–66.

Dezfoli, F. F. N., Dehghantanha, A., Mahmoud, R., Sani, N. F. B. M., & Daryabar, F. (2013). Digital Forensic Trends and Future. *International Journal of Cyber-Security and Digital Forensics (IJCSDF)*, *2*(2), 48–76. http://sdiwc.net/digital-library/digital-forensic-trends-and-future.html

Jasmin, Ć., & Cosic, J. (2015). Leveraging DEMF to Ensure and Represent 5ws & 1h in Digital Forensic Domain. *International Journal of Computer Science and Information Security*, *13*(2), 5–9. https://www.researchgate.net/publication/288592139_Leveraging_DEMF_to_Ensure_and_Represent_5ws1h_in_Digital_Forensic_Domain

Mabuto, E. K., & Venter, H. S. (2011). State of the art of Digital Forensic Techniques. *Information Security for South Africa (ISSA)*, 1–7.

Mrdovic, S., Huseinovic, A., & Zajko, E. (2009). Combining static and live digital forensic analysis in virtual environment. *2009 XXII International Symposium on Information, Communication and Automation Technologies*, *August 2016*, 1–6. https://doi.org/10.1109/ICAT.2009.5348415

Prayudi, Y., Ashari, A., & K Priyambodo, T. (2014). Digital Evidence Cabinets: A Proposed Framework for Handling Digital Chain of Custody. *International Journal of Computer Applications*, *107*(9), 30–36. https://doi.org/10.5120/18781-0106

Prayudi, Y., & SN, A. (2015). Digital Chain of Custody: State of The Art. *International Journal of Computer Applications*, *114*(5), 1–9. https://doi.org/10.5120/19971-1856

Rafique, M., & Khan, M. N. A. (2013). Exploring Static and Live Digital Forensics: Methods, Practices and Tools. *International Journal of Scientific & Engineering Research*, *4*(10), 1048–1056. http://www.ijser.org/researchpaper%5CExploring-Static-and-Live-Digital-Forensic-Methods-Practices-and-Tools.pdf

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. 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). *Elinvo (Electronics, Informatics, and Vocational Education)*, *3*(1), 70–82. https://doi.org/10.21831/elinvo.v3i1.19308