Nama : I Putu Agus Putra Negara  
Nim : 2105551044  
Matakuliah : IT Forensic (C)

**Review Paper Forensic**

1. Jurnal 1

|  |  |
| --- | --- |
| Judul | INVESTIGASI FORENSIK TERHADAP BUKTI DIGITAL DALAM MENGUNGKAP CYBERCRIME |
| Jurnal | CyberSecurity dan Forensik Digital |
| Volume & Halaman | 3 & 12-21 |
| Tahun | 2020 |
| Penulis | Moh. Riskiyadi |
| Reviewer | Agus Putra |
| Tanggal | 1 november 2022 |

|  |  |
| --- | --- |
| Abstrak | Teknologi yang berkembang pesat sejalan dengan tindakan cybercrime yang meningkat drastis, sehingga teknik dan modus baru cybercrime sulit untuk dideteksi dan dipecahkan oleh para investigator forensik digital. Tujuan dari penelitian ini adalah memberikan referensi terkait dengan kehandalan tools digital forensic dalam mengungkap cybercrime agar diperoleh bukti digital yang berintegritas, handal dan legal dalam proses ligitasi. Penelitian ini menggunakan metode static forensic dengan framework dari National Institute of Justice (NIJ) dengan skenario kasus cybercrime berupa carding dengan bukti elektronik flash disk menggunakan tools digital forensic FTK Imager dan Autospy. Hasil penelitian ini menunjukkan penggunaan FTK Imager dan Autospy mampu mengakuisisi dan menganalisis file yang dihapus permanen maupun file yang tersimpan sebelum flash disk diformat ulang. Sedangkan penghapusan permanen dan penggunaan password pada flash disk dengan tools BitLocker Drive Encryption, kedua tools tersebut tidak dapat mengakuisisi dan menganalisis file yang dihapus permanen ataupun diformat ulang. |
| Pengantar | Teknologi yang meningkat pesat memberikan manfaat dan dampak yang sama besar bergantung dari pengguna dari teknologi tersebut. Manfaat positif yang dapat diperoleh dari teknologi adalah memudahkan individu atau kelompok dalam melakukan aktifitasnya, sedangkan dampak negatif timbul karena penyalahgunaan teknologi oleh individu atau kelompok untuk tindakan kejahatan dunia maya (cybercrime) yang dapat merugikan orang lain (Akbar and Riadi, 2019; Gani, 2018; dan Hasa, Yudhana and Fadlil, 2019). Kemajuan teknologi yang semakin pesat juga diiringi dengan sistem keamanan yang semakin meningkat sebagai respon dari tindakan cybercrime yang semakin meningkat drastis. Akibatnya pelaku cybercrime selalu lebih aktif dan cepat membuat terobosan baru terhadap sistem keamanan yang dibentuk oleh anti cybercrime. Kondisi yang sangat menghawatirkan terjadi apabila pelaku cybercrime adalah ahli juga dalam tindakan anti cybercrime, sehingga modus baru cybercrime sulit untuk dideteksi dan dipecahkan oleh para investigator forensik digital. |
| Pembahasan | Berdasarkan hasil analysis menggunakan Autospy atas file image dengan FTK Imager pada flash disk, berikut perbandingan hasil temuan file untuk masing-masing perlakuan:  1. Perlakuan pertama yaitu tanpa dilakukan penghapusan atas file-file simulasi, diperoleh hasil seluruh file simulasi terdeteksi, sekaligus dengan file-file yang pernah ada dalam flash disk sebelum dilakukan format ulang, adapun file simulasi tersebut adalah: masing-masing 1 file untuk file berekstensi (docx, xlsx, pdf, jpg, mp3, mp4, rar, txt, exe, html) dan 1 forlder memuat (9 css, 11 html, 22 js.download, 4 non extention, 1 gif, 2 jpeg, 7 jpg. 1 php, 8 png dan 9 txt).  2. Perlakuan kedua yaitu menghapus pemanen (shift + delete) seluruh file simulasi, diperoleh hasil seluruh file simulasi terdeteksi, sekaligus dengan file-file yang pernah ada dalam flash disk sebelum dilakukan format ulang, adapun file simulasi tersebut adalah: masing-masing 1 file untuk file berekstensi (docx, xlsx, pdf, jpg, mp3, mp4, rar, txt, exe, html) dan 1 forlder memuat (9 css, 11 html, 22 js.download, 4 non extention, 1 gif, 2 jpeg, 7 jpg. 1 php, 8 png dan 9 txt).  3. Perlakuan ketiga, yaitu dengan menghapus pemanen (shift + delete) seluruh file serta mengpassword flash disk dengan tools bawaan Windows 10 BitLocker Drive Encryption, tidak terdeteksi file apapun. |
| Simpulan | Berdasarkan hasil penelitian dari proses investigasi forensik bukti digital dari bukti elektronik flash disk, perbedaan perlakuan pada flash disk memberikan hasil yang berbeda, yang ditunjukkan dengan nilai hash yang berbeda dari masing-masing perlakuan. Hasil analisis file untuk perlakuan yang pertama dan kedua, seluruh file simulasi serta file-file lainnya yang pernah disimpan dalam flash disk sebelum dilakukan format ulang dapat terdeteksi atau terecovery, sedangkan dengan perlakuan ketiga tidak ditemukan jenis file apapun. Tools FTK Imager dan Autopsy masih belum mampu melakukan akuisisi dan analisis data dengan perlakuan penghapusan permanen dan enkripsi (password) pada flash disk menggunakan tools bawaan Windows 10 yaitu BitLocker Drive Encryption. |
| Kekuatan Penelitian | 1. Teori dan Metode yang digunakan tepat dengan menggunakan perbandingan dari masing masing tools forensic. 2. Bahasa yang digunakan oleh penulis mudah dipahami beserta disertakan gambar untuk lebih mudah melihat situasi. |
| Kelemahan Penelitian | 1. Penulis kurang lengkap dalam menyimpulkan seluruh kesimpulan dari masing masing tools forensic yang digunakan. 2. Penulis kurang detail dalam menjelaskan apa saja yang didapatkan dari tools forensic yang digunakan yang dapat berhubungan dengan data yang dicari. |

1. Jurnal 2

|  |  |
| --- | --- |
| Judul |  |
| Jurnal |  |
| Volume & Halaman |  |
| Tahun |  |
| Penulis |  |
| Reviewer |  |
| Tanggal |  |

|  |  |
| --- | --- |
| Abstrak |  |
| Pengantar |  |
| Pembahasan |  |
| Simpulan |  |
| Kekuatan Penelitian |  |
| Kelemahan Penelitian |  |