LOGIC: Jurnal Penelitian Informatika
Vol. 1, Issue 1, pp. 29–45 (2023)
doi: http:/doi.org/10.25124/jibr.v1i1.6442

RESEARCH ARTICLE

Testing Tools Data Wiping dalam Kegiatan Anti Forensik

Ryan Austin Andika, Niken Dwi Wahyu Cahyani* and Rio Guntur Utomo

Fakultas Informatika, Universitas Telkom, Bandung, 40257, Jawa Barat, Indonesia
*Corresponding author: nikencahyani@telkomuniversity.ac.id
Received on 4 August 2023; accepted on 3 September 2023

Abstrak

Salah satu kegiatan anti forensik untuk mengamankan data adalah dengan melakukan penghapusan data dari media penyimpanan, yang dapat membuat para penegak hukum kesulitan untuk mengumpulkan bukti-bukti digital. Pada praktik nya ada banyak metode yang dapat membuat penghapusan data tersebut benar-benar aman dan tidak mudah untuk dipulihkan dengan berbagai tools recovery, salah satunya adalah dengan wiping data. Metode penghapusan dengan teknik wiping data, dalam kegiatan anti forensik biasanya digunakan pada media penyimpanan yang menyimpan data ilegal yang berkaitan dengan bukti tindak kejahatan. Jika pada media penyimpanan ini berisi data tindak kejahatan maka pemilik data tersebut akan berusaha untuk melakukan menyembunyikan atau menghapus data tersebut, salah satunya dengan metode wiping data, selain data utama ada juga data lain yang akan terhapus dalam perangkat penyimpanan jika menggunakan metode *wiping data*, yang mencakup metadata dan tracedata. Dalam upaya membantu kegiatan forensik memahami *tools wiping data*, pada pengujian tugas akhir ini akan diambil enam tools atau aplikasi sampel yang telah dipilih sebelumnya yang dapat melakukan data wiping pada media penyimpanan, dengan tujuan untuk membandingkan hasil data wiping antara tools atau aplikasi tersebut lalu dianalisa kelebihan dan kekurangannya untuk keperluan sebagai data untuk kegiatan forensic. Metode yang diambil pada sampel tools atau aplikasi adalah metode-metode *Zero Overwrite*, *Random Data Overwrite*, U.S. DoD 5220.22-M (E), U.S. DoD 5220.22-M (ECE), dan Bruce Schneier's *Algorithm*. Metode-metode ini dapat menghapus dan menimpa data sehingga data tidak dapat dibaca oleh orang yang tidak berwenang, sehingga dapat dipakai untuk mencegah pengungkapan kejahatan.

Key words: Anti Forensik, *Wiping Data*, Media Penyimpanan, Penghapusan

Pendahuluan

Informasi saat ini merupakan suatu hal yang penting dan harus dijaga, namun dalam hal perlindungan informasi pada saat ini untuk individu maupun organisasi masih dibilang sangat kurang diperhatikan[1]. Padahal informasi sendiri merupakan hal yang sangat penting dan beberapa bersifat rahasia bagi beberapa orang, informasi juga dapat menimbulkan ancaman bagi pemilik informasi apabila informasinya jatuh kepada orang yang salah, bahkan dapat mengakibatkan kerugian yang besar hanya karena informasi nya tidak terjaga dengan baik[10].

Dalam melakukan perlindungan informasi sendiri tidak lepas dari bidang ilmu anti-forensics, yang merupakan metode untuk menyembunyikan suatu informasi atau file yang dianggap sebagai barang bukti digital [13], dalam hal ini berarti lawan atau kebalikan dari ilmu forensic yang bertujuan untuk mencari bukti digital dari sebuah kasus digital yang terjadi. Pada anti-forensics umumnya perlindungan informasi atau data dapat mengacu pada dua hal, yang pertama yaitu melakukan tindakan agar data yang tersimpan pada media penyimpanan tidak dapat dibuka ataupun ditemukan dengan menggunakan berbagai metode dari antiforensics, kemudian hal yang kedua yaitu mengupayakan agar data atau file bukti yang berhasil ditemukan tidak dapat digunakan ataupun tidak sesuai dengan standar hukum, yang dalam hal ini berarti data atau file bukti tersebut tidak dapat dijadikan barang bukti pada saat proses persidangan[12]. Mengikuti hal pertama tadi yaitu agar data tidak dapat di temukan salah satu nya dengan penghapusan data, metode ini merupakan salah satu metode anti-forensics yang paling sering digunakan oleh para pemilik informasi yang terdapat pada media penyimpanan elektronik. Pada umumnya metode ini dilakukan dengan menekan tombol *delete* dan mengosongkan *recycle bin* atau *trash* pada sistem.

Pemilik informasi beranggapan bahwa proses yang dilakukan telah benar-benar menghapus data, namun proses tersebut hanya menghilangkan pointer pada blok media penyimpanan yang menyimpan data dan kemudian dianggap sebagai ruang kosong untuk dapat diisi kembali dengan data yang baru[3]. Data yang dianggap telah terhapus sangat berpotensi untuk dilakukan proses recovery dengan menggunakan ilmu digital forensik, atau dengan kata lain bahwa data tersebut masih memungkinkan untuk didapatkan. namun proses tersebut hanya menghilangkan pointer pada blok media penyimpanan yang menyimpan data dan kemudian dianggap sebagai ruang kosong untuk dapat diisi kembali dengan data yang baru[16]. Data yang dianggap telah

terhapus sangat berpotensi untuk dilakukan proses *recovery* dengan menggunakan ilmu digital forensik, atau dengan kata lain bahwa data tersebut masih memungkinkan untuk didapatkan. Untuk mengatasi tindakan tersebut perlu dilakukan proses penghapusan data pada media penyimpanan yang benar-benar aman sehingga data tersebut tidak dapat dilakukan proses *recovery* [1]. Salah satu yang dapat dilakukan untuk menghilangkan bukti yang terdapat pada media penyimpanan dengan menggunakan teknik data *wiping* [15], namun metode wiping sendiri sangat beragam jenis nya ada yang melakukan overwrite setelah penghapusan data dengan 1 fase, 7 fase sampai 35 fase[15]. Pada penelitian ini yang akan dilakukan mempunyai tujuan untuk melakukan analisis tools yang sudah di tentukan sebelumnya, untuk mencari seberapa besar efesiensi keberhasilan menggunakan data wiping yang ada dan mengetahui perbedaan pada setiap tools dalam menjalankan metode wiping untuk membantu kegiatan forensic terkait penggunaan tools dalam menjalankan metode *wiping* nantinya. Karena fakta nya tidak semua alat anti forensik bekerja sesempurna yang diiklankan, sehingga meninggalkan bekas dan jejak[12]. Dalam penelitaan ini untuk menguji tools dilakukan metode-metode wiping yang sama yang terdapat pada tools, dan metode yang dipilih menjadi acuan yaitu *Zero Overwrite*, Random Data Overwrite, U.S. DoD 5220.22-M (E), U.S. DoD 5220.22-M (ECE), dan Bruce Schneier's *Algorithm*.

Adapun alasan pada penelitian ini mengapa menggunakan metode-metode wiping data seperti yang di sebutkan di atas adalah. Pertama pada metode yang paling simple yaitu zero overwrite dipilih karena ingin membuktikan apakah ada kesalahan pada setiap *tools* yang dipilih untuk melakukan penghapusan dengan satu fase yang data nya hanya ditimpa dengan nol[15], jika ada maka *tools* tersebut tidak terbilang berhasil melakukan wiping data. Lalu pada metode random *data overwrite* yang persis sama dengan metode sebelumnya tapi mempunyai perbedaan ada pada data yang ditimpa dengan aliran byte yang dihasilkan secara acak, pada algoritma ini dilakukan observasi apakah setiap tools menghasilkan random yang berpola sama atau berbeda total[16]. Dan metode sisanya dipilih karena merupakan metode yang popular digunakan untuk melakukan wiping data, yang mempunyai fase *overwrite* setelah penghapusannya lebih dari satu. Dari yang melakukan wiping data dengan 3 fase *overwrite* setelah penghapusan yaitu U.S. DoD 5220.22-M (E)[13]. dan ada yang menggunakan 7 fase overwrite yaitu U.S. DoD 5220.22-M (ECE), dan Bruce Schneier's Algorithm setelah penghapusan[13].

Tinjauan Pustaka

Anti-Forensik

Anti forensik adalah teknik yang digunakan untuk melakukan tindakan kriminal agar para penyidik menjadi esulitan saat melakukan investigasi terhadap suatu masalah untuk mengumpulkan barang bukti digital[1]. Menurut Rogers [1], Anti Forensik merupakan usaha untuk menimbulkan efek negatif terhadap keberadaan dan kualitas dari barang bukti dari lokasi kejadian, atau membuat sebuah proses anlisa barang bukti menjadi susah dilakukan. Alat dan teknik *anti-forensics* (AFT) digunakan untuk menargetkan ketersediaan, kegunaan bukti digital dengan melakukan beberapa tindakan seperti mengubah, mengganggu, dan menghancurkan validitas ilmiah dari bukti [14]. AFT membutuhkan beberapa bentuk tergantung pada penggunaan dan tujuan diantaranya sebagai berikut *data hiding, data destruction, trail obfuscations*, dan attack *against forensic processing / tools*[14]. Dan pada penelitian ini membahas jenis anti-forensics data destruction yaitu *data wiping* dengan fokus penelitian menguji performance tools yang melakukan *data wiping*.

Data Destruction Methods

Data Destruction Method adalah metode penghancuran data pada media penyimpanan dengan tujuan untuk menghapus seluruh data *sensitive* pada media penyimpanan, terdapat banyak metode yang digunakan data destruction dengan melakukan wiping data, yaitu dengan melakukan penulisan ulang pada blok yang sudah dilakukan penghapusan dan mengisi data baru agar tidak dapat dilakukan proses pemulihan Kembali[15]. Pada penelitian ini menggunakan beberapa metode data Destruction untuk melakukan data wiping, diantaranya adalah *Zero Overwrite*, *Random Data Overwrite*, U.S. DoD 5220.22-M (E), U.S. DoD 5220.22-M (ECE), dan *Random Data Overwrite*.

1. ***Zero Overwrite***
   Metode *data wiping* menggunakan *Zero Overwrite* artinya melakukan overwrite dari penghapusan data 4 dengan satu fase *overwrite* yang data nya hanya ditimpa dengan nol.
2. ***Random Data Overwrite***
   Sedangkan *Random Data Overwrite* sama seperti *Zero Overwrite kecuali pada data yang ditimpa dengan, aliran byte yang dihasilkan* secara acak. Perhitungan tambahan untuk menghasilkan keacakan membuat skema ini sedikit lebih lambat dari 1-pass nol[10].
3. ***U.S. DoD 5220.22- M (E)***
   Lalu pada Metode U.S. 5220.22-M (E) yang merupakan sebuah standar dikembangkan oleh Defense Security Service (DSS) untuk memecahkan masalah penghapusan data secara permanen. Metode penghapusan ini menggunakan tiga kali *overwriting* penulisan setelah penghapusannya yaitu[13].:
   Fase 1: Menimpa dengan byte 0 F
   ase 2: Menimpa dengan byte 1
   Fase 3: Menimpa dengan byte random.
4. ***U.S. DoD 5220.22- M (ECE)***
   Mirip seperti metode sebelumnya, ada pula metode U.S. DoD 5220.22-M (ECE). Metode ini merupakan varian lanjutan dari DoD 5220.22-M. Varian Standar DoD ini digunakan untuk menimpa data tujuh kali overwriting penulisan setelah penghapusannya yaitu[10]:
   Fase 1 - 3: Menimpa dengan U.S. 5220.22-M (E)
   Fase 4: Mnimpa dengan nilai random berdasarkan DoD 5220.22-M (C) *Standard*
   Fase 5 - 7: Menimpa dengan U.S. 5220.22-M (E).
5. ***Schneier's Algorithm***
   Selanjutnya mirip seperti metode yang menggunakan 7 fase overwriting, ada pula metode Schneier's *Algorithm*. Fase pertama menimpa dengan pola bit "00", yang kedua dengan "11", dan lima berikutnya dengan pola bit yang dihasilkan secara acak. Metode ini memiliki efek yang mirip dengan standar VSITR, tetapi sifat acak dari pola bit yang ditulis dalam lima lintasan terakhir membuat sangat sulit bagi penyerang untuk menentukan bagaimana penimpaan mungkin memengaruhi sisa-sisa data di sekitar tepi lintasan pada disk, atau pada transisi bit pada disk. Meskipun mungkin metode yang lebih aman untuk menghapus data daripada VSITR, waktu yang dibutuhkan untuk membuat pola bit acak membuat metode ini jauh lebih lambat. Bagian ini berisi teori/studi/literatur yang mendukung (terkait erat) dengan topik TA yang dikerjakan. Bagian ini bisa bernama Tinjauan Pustaka atau Landasan Teori. Dalam bahasa Inggris disebut sebagai *RelatedWork* atau *Literature Review*. Studi Terkait dapat dituliskan pada bagian terpisah seperti contoh ini atau digabungkan dengan bagian Pendahuluan. Materi yang dijelaskan pada bagian ini adalah yang benar-benar terkait erat dengan topik TA, meskipun tidak digunakan pada TA yang dikerjakan.

Data Wiping

Tujuan Data Wiping adalah penghapusan data yang tidak diinginkan atau rahasia secara aman, dan data dapat dibuat tidak dapat dipulihkan. Namun, tidak setiap penggunaan data wiping memiliki motif yang baik. Beberapa kasus data wiping yang tidak tepat adalah menghilangkan bukti digital, sehingga aktivitas *data wiping* ini bersifat ilegal di banyak negara[10]. Data wiping sendiri merupakan suatu proses dengan sengaja, permanen, dan ireversibel untuk menghapus atau menghancurkan data yang tersimpan pada media penyimpanan agar tidak dapat dipulihkan kembali. Sebuah media penyimapanan yang telah melakukan data wiping tidak akan memiliki data residual yang berfungsi dan bahkan alat-alat forensic canggih pun seharusnya tidak pernah dapat memulihkan data yang telah diwiping tersebut. *Data wiping* ini dilakukan untuk melindungi data-data rahasia yang tidak boleh diketahui oleh orang lain[11].

Tools Data Wiping

Saat menghapus file atau folder dari perangkat penyimpanan, data aktual tetap ada di perangkat penyimpanan hingga ditimpa oleh data baru. Data wiping dianggap sebagai teknik *anti-forensics* yang dirancang untuk sepenuhnya menghapus dan menghancurkan data[14]. Penghapusan artefak atau penghapusan aman dapat diterapkan pada file, seluruh disk, atau partisi[14]. Tools yang tersedia yang dapat melakukan data wiping dan di gunakan pada penelitian adalah *Eraser, Disk Wipe, AOMEI Partition Assistant Professional, AOMEI Backupper, Hardwipe*, dan *Hard Drive Eraser*.

1. ***Eraser***
   Eraser merupakan aplikasi gratis untuk menghapus data yang sepenuhnya dapat menghilangkan data 5 sensitif dari *hard disk* yang menggunakan sistem operasi Windows 10 atau versi dibawahnya. Memiliki berbagai metode algoritma dalam penghapusan data, *Eraser* cocok untuk pengguna yang ingin menggunakan berbagai metode algoritma berbeda dalam penghapusan data[19]. *Eraser* dapat bekerja sebagai aplikasi Windows tersendiri untuk menghapus secara aman semua file pada *hard disk*, dan dapat di boot dari media eksternal. Serta mendukung berbagai teknik algoritma penghapusan data seperti DOD 5022, Gutmann (35 passes), AFSSI-5020, HMG IS5. Schneier (7 passes). Dan dapat digunakan untuk menghapus seluruh *hard disk* atau folder tertentu pada sistem. Pengguna juga dapat membuat dan menyimpan beberapa tugas penghapusan disk sesuai dengan pengaturan yang telah dibuat. Serta untuk penghapusan data dapat dijadwalkan secara otomatis dimulai pada waktu tertentu. Pengguna dapat mengatur tugas penghapusan data agar dapat diulang dalam periode waktu tertentu.
2. ***Disk wipe***
   Disk Wipe merupakan salah satu aplikasi yang paling populer lainnya untuk menghapus data hard disk. Perangkat lunak sumber terbuka yang dibuat untuk sistem operasi Windows ini sepenuhnya gratis dan menyediakan cara mudah untuk menghapus data dari hard disk. Dan tidak memerlukan instalasi apa pun[7]. Disk Wipe Mudah untuk digunakan, termasuk ke dalam aplikasi portable untuk menghapus data di *hard disk* secara gratis. Juga mendukung partisi sistem di Windows seperti FAT32 dan NTFS. Dan mendukung pula media penyimpanan eksternal seperti kartu SD dan *flash disk*. Dalam disk wipe menggunakan algoritma penghapusan data seperti Peter Guttman, DOD 5220-22 M.
3. ***AOMEI Partition Assistant Professional***
   AOMEI Partition Assistant Profesional Ini memungkinkan untuk menggunakan metode Gutmann untuk menghapus *hard drive*. Selain itu, ia juga menyediakan 3 metode penghapusan lainnya: mengisi sektor dengan nol, mengisi sektor dengan data acak, dan DOD 5220.22-M[4]. Utilitas penghapusan Gutmann ini dirancang untuk sistem operasi Windows, mendukung Windows 10/8/7, Windows XP, Windows Vista. Dan antarmuka intuitifnya membuat semua operasi menjadi sangat mudah[4].
4. ***AOMEI Backupper***
   AOMEI Backupper dapat memenuhi berbagai kebutuhan dalam menghapus disk. Tidak hanya untuk menghapus disk dengan mudah tetapi juga untuk menghapus partisi dan ruang yang tidak terisi. Dalam hal fungsi penghapusan disk, ini mendukung metode penghapusan Gutmann dan mudah dioperasikan. Selain itu, ia juga menyediakan tiga metode penghapusan lainnya. Mereka adalah *zero sector*, random sector, DoD 52220.22-M[5].
5. ***Hardwipe***
   Hardwipe adalah perangkat sanitasi data gratis yang digunakan oleh aktivis, jurnalis, teknisi IT, dan siapa saja yang perlu memastikan bahwa informasi yang dibuang, tidak akan pernah dapat dipulihkan oleh orang lain. Hardwipe menyediakan interface pengguna yang apik dengan dukungan opsional untuk menu konteks 'klik kanan' di Windows *File Explorer*. Gunakan *Hardwipe* untuk menghapus (atau 'hard wipe') data pada disk dan media penyimpanan portabel dengan mudah dan permanen. Itu dapat dengan mudah menghancurkan file dan isi folder sesuai permintaan, menghapus *drive* dan media USB, dan membersihkan Windows *Recycler*. *Hardwipe* memberi kebebasan untuk menghapus dengan aman: Perangkat Fisik, Volume Logis, File/Folder, Recycler Bins, Ruang *Drive* Gratis (tidak terpakai) dan Windows Pagefile. Ia juga menawarkan verifikasi baca kembali, log laporan, dan mendukung semua skema sanitasi utama, termasuk: GOST R 50739-95, DOD 5220.22-M, Schneier dan Gutmann. Hardwipe gratis untuk penggunaan non-komersial (beberapa fitur premium memerlukan upgrade berbayar)[9].
6. ***Hard Drive Eraser***
   Hard Drive Eraser adalah aplikasi Windows gratis yang secara permanen menghapus data di seluruh volume (*hard drive*). Dengan cara mengisi permukaan magnet berkali-kali dengan data biner yang acak. fakta nya diketahui bahwa tidak mungkin untuk menghancurkan data secara permanen hanya dengan memformat *hard drive*[6]. Penghapusan *hard drive* aman adalah metode di mana serangkaian data biner acak telah ditulis ke dalam hard drive, sehingga hampir tidak mungkin untuk memulihkan informasi yang terhapus tersebut. Metode ini lebih lambat daripada pemformatan sederhana tetapi memastikan bahwa informasi di *hard drive* tidak akan terekspos.

Metodologi Penelitian

Dengan tujuan untuk mengetahui tingkat keamanan serta keberhasilaan kinerja setiap tools anti-forensics dari proses data wiping, yang menerapkan metode-metode Zero Overwrite, Random Data Overwrite, U.S. DoD 5220.22-M (E), U.S. DoD 5220.22-M (ECE), dan Bruce Schneier's Algorithm. Dalam penelitian ini dilakukan proses uji menggunakan Functional dan Non-functional Testing. Pada functional testing yaitu unit testing, melakukan test pada salah satu unit program atau fitur yang ada pada tools anti-forensics. Pada penelitian ini melakukan test unit fitur dari data wiping pada tools. Pada Non-functional testing yaitu performance testing, yang melakukan test utama nya dalam melakukan testing tools yaitu:

1. Kecepatan: dengan menentukan apakah aplikasi merespons dengan cepat dan membandingkan kecepatan wiping data, o
2. Skalabilitas: dengan menentukan beban data untuk wiping data yang sama dan membandingkan respons antar tools terkait beban tersebut, o

Gambar 1. Performance Testing menurut Thomas Hamilton

3. Stabilitas dengan menentukan apakah tools stabil di bawah beban yang ditentukan

Terdapat 7 proses yang dilakukan dalam performance testing dari gambar 1 yang akan dilakukan pada penelitian ini pada tools data wiping.

Identify Test Environment

Proses pertama adalah melakukan identifikasi terhadap lingkungan pengujian yang akan digunakan dalam penelitian ini. Berikut adalah perangkat keras yang digunakan:

1. Laptop HP Pavilion 15-dk0xxx
2. Sistem Operasi: Windows 10 Home Single
3. Hard Disk Drive:
    - Kapasitas: 256GB
    - File Sistem: FAT32
    - Teknologi S.M.A.R.T (Self-Monitoring, Analysis and Reporting Technology) untuk deteksi berbagai kondisi pada hard disk.

Determine Performance Criteria

Selanjutnya, melakukan identifikasi terhadap kriteria performansi yang akan digunakan dalam pengujian. Kriteria ini mencakup:

Functional Testing Criteria

Pada functional testing, kriteria yang digunakan adalah unit testing pada fitur data wiping pada tools anti-forensics. Kriteria keberhasilan adalah ketidakmampuan pemulihan data setelah proses data wiping.

Non-functional Testing Criteria

Pada non-functional testing, kriteria yang digunakan meliputi:

- Kecepatan: Mengukur waktu yang diperlukan oleh tools saat menjalankan proses data wiping.
- Skalabilitas: Menghitung penggunaan CPU sebagai tolak ukur skalabilitas tools dalam melakukan data wiping.
- Stabilitas: Menghitung penggunaan memori sebagai tolak ukur stabilitas tools dalam melakukan data wiping.

Plan & Design

Pembuatan tata cara dan desain untuk melakukan pengujian dilakukan berdasarkan framework yang melibatkan 7 proses ini. Pengujian data wiping pada tools akan mengikuti kriteria yang telah ditetapkan dan akan diakhiri dengan proses analisis hasil.

Configure Test Environment

Langkah selanjutnya adalah melakukan konfigurasi dengan menyiapkan tools, sumber daya, dan elemen lain yang dibutuhkan untuk pengujian. Tools yang digunakan untuk melakukan data wiping termasuk:

- Eraser
- Disk Wipe
- AOMEI Partition Assistant Professional
- AOMEI Backupper
- Hardwipe
- Hard Drive Eraser

Sedangkan untuk pengujian pemulihan data, digunakan 3 tools berikut:

1. MiniTool Power Data Recovery 11.4
2. EaseUS Data Recovery Wizard
3. Recuva

Implement Test Design

Selanjutnya, dilakukan implementasi dari desain pengujian dengan menggunakan desain pengujian yang telah dibuat sebagai tahap pengujian.

Run Test

Pengujian dilakukan dengan menjalankan proses data wiping menggunakan tools yang telah dipilih. Performansi testing dilakukan berdasarkan framework yang telah dipilih.

Analyze

Langkah terakhir adalah melakukan analisis terkait keseluruhan pengujian. Hasil akhir dari pengujian ini diharapkan dapat mencapai tujuan penelitian dan memberikan pemahaman baru terkait tools data wiping.

Tahapan Pengerjaan

Perancangan alur penelitian merupakan proses atau tahapan yang dilakukan dalam penelitian ini, tahapan ini dibuat berdasarkan dari metodologi performance testing sebelumnya. Untuk lebih jelasnya, perancangan alur penelitian dapat dilihat pada gambar 2.

Test Data Preparation

Dalam penelitian ini, pada perancangan datanya akan disiapkan beberapa file yang berbeda untuk di tempatkan pada media penyimpanan yang sudah ditetapkan, berikut ini adalah file yang akan dijadikan sebagai dataset yang nanti nya akan disalin kedalam *hard disk* yang di gunakan sebagai penelitian.

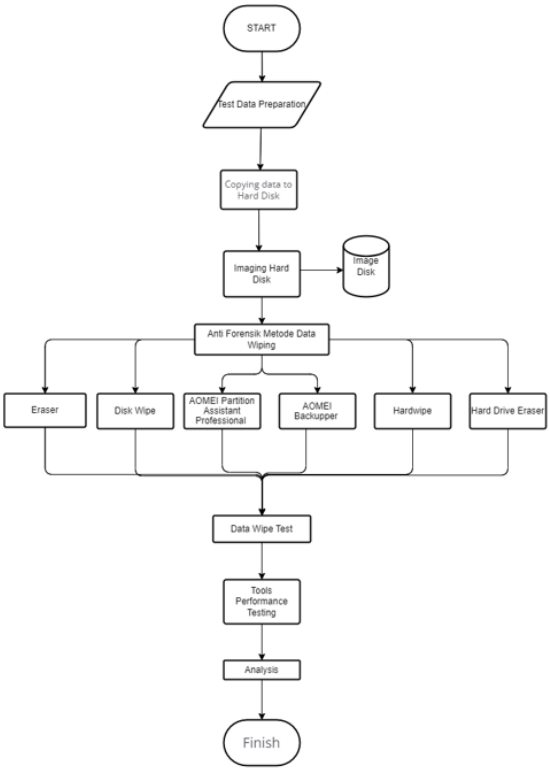
Tujuan dari pengambilan data seperti yang dijelaskan di atas adalah untuk mengetahui perbedaan dalam proses *data wiping* pada berbagai jenis file yang berbeda. Selain itu, diperlukan berbagai jenis file yang berbeda dalam jumlah yang lebih banyak agar hasilnya lebih mudah untuk dianalisis.

Imaging Hard Disk

Dalam penelitian ini, sebelum proses data wiping dilakukan, terlebih dahulu dilakukan proses imaging pada hard disk. Hal ini dilakukan untuk mendapatkan hasil image hard disk yang akan digunakan dalam pengujian *data wiping* pada setiap *tools*. Dengan menggunakan hasil image yang sama, memungkinkan perbandingan yang konsisten antara hasil pengujian.

Anti-Forensics Method Data Wiping

Dalam pengujian data wiping, penghapusan data dilakukan dengan cara menghapus data yang telah ditentukan sebelumnya. Data kemudian dipindahkan ke dalam hard disk dan dihapus menggunakan



Gambar 2. Arsitektur Solusi Sistem

Table 1. Tabel Data

Jenis File	Ekstensi	Jumlah
Microsoft Word	.docx	10
Microsoft Excel	.xlsx	10
Microsoft Power Point	.pptx	10
File Dokumen	.pdf	10
Gambar	.png	10
Gambar	jpg	10
Audio	.mp3	10
Video	.mp4	10
File Aplikasi (executable)	.exe	10
File Kompres	.zip	10
Total		**100**

tools yang telah ditentukan. Proses penghapusan data menggunakan metode-metode berikut:

- Zero Overwrite
- Random Data Overwrite
- U.S. DoD 5220.22-M (E)
- U.S. DoD 5220.22-M (ECE)
- Bruce Schneier's Algorithm

Data Wipe Test

Dalam pemilihan tools atau aplikasi yang akan digunakan dalam pengujian, dilakukan seleksi berdasarkan metode penghapusan data yang digunakan, termasuk Zero Overwrite, Random Data Overwrite, U.S. DoD 5220.22-M (E), U.S. DoD 5220.22-M (ECE), dan Bruce Schneier's Algorithm. Setelah melakukan literasi, dipilih 6 *tools* atau aplikasi yang sesuai dengan kriteria tersebut, yaitu:

- Eraser
- Disk Wipe
- AOMEI Partition Assistant Professional
- AOMEI Backupper
- Hardwipe
- Hard Drive Eraser

Selanjutnya, dilakukan pengujian performansi penghapusan data menggunakan stopwatch untuk mengukur waktu yang diperlukan oleh *tools* atau aplikasi untuk menghapus data. Hasil pengukuran diambil dalam satuan detik.

Pada pengujian performansi tools, juga dilakukan pengamatan terhadap tingkat kehancuran data yang dihapus. Ini mencakup adanya nama file, ukuran file, dan jumlah file yang dapat dipulihkan. Semakin sedikit *file* yang dapat dipulihkan, maka semakin baik kinerja aplikasi tersebut.

Untuk pengujian keamanan data, digunakan 3 aplikasi pemulihan data berikut:

1. MiniTool Power Data Recovery 11.4
2. EaseUS Data Recovery Wizard
3. Recuva

Analisis

Setelah selesai melakukan pengujian terhadap data wiping, tahapan pengerjaan diakhiri dengan proses analisis terhadap keseluruhan hasil uji coba *tools data wiping*.

Hasil dan Pembahasan

Hasil Pengujian

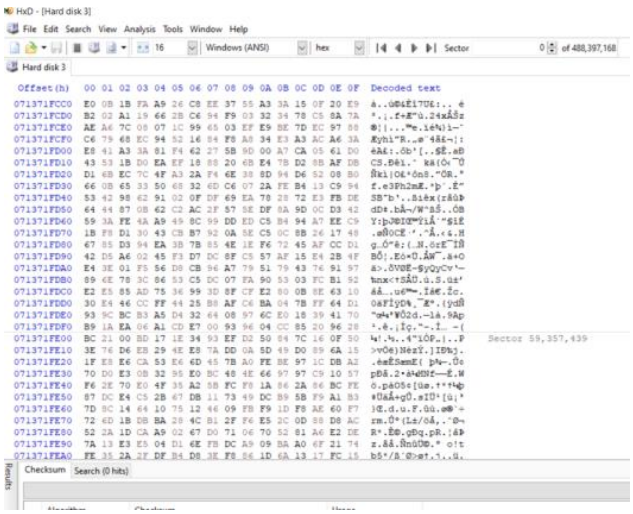
Berdasarkan pada perancangan pengujian yang terdapat pada Gambar 2, proses Analisa pertama yang dilakukan yaitu uji kinerja dari metode wiping data berupa Zero Overwrite, Random Data Overwrite, U.S. DoD 5220.22-M (E), U.S. DoD 5220.22-M (ECE), dan Bruce Schneier's Algorithm. Pada *tools* yang akan di uji yaitu Eraser, Disk Wipe, AOMEI *Partition Assistant Professional*, AOMEI Backupper, Hardwipe, dan *Hard Drive Eraser*. Pengujian tools ini dilakukan pada media penyimpanan Hardisk Drive, yang dilakukan clone dari image Harddisk yang sudah diisi data yang di tentukan sebelumnya.

A. Eraser

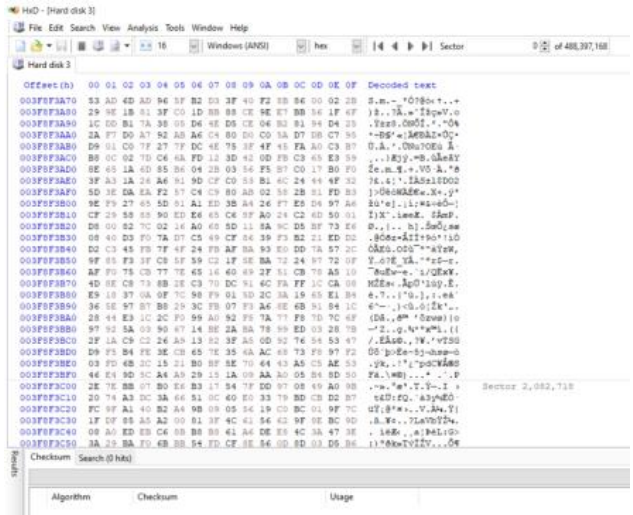
Pada *tools* ini *wiping* data menggunakan metode *Random Data Overwrite*, U.S. DoD 5220.22-M (E), U.S. DoD 5220.22-M (ECE), dan Bruce Schneier's Algorithm. Karena tidak tersedia metode wiping Zero Overwrite, namun dalam aplikasi nya terdapat metode wiping data lain yang beragam seperti *Britsih* HMG IS5 (baseline), Russian GOST P50739-95, US Army AR380-19, US *Air Force* 5020, German VSITR, RCMP TSSIT OPS-II, dan Peter Guttman.

Random Data Overwrite

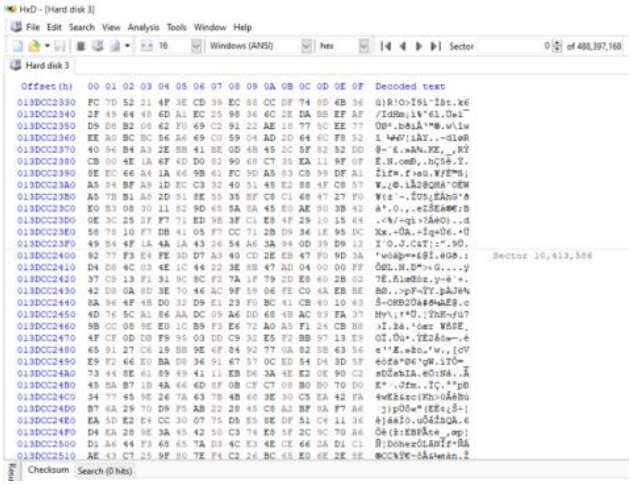
Pada Gambar 3 merupakan hasil yang didapat setelah dilakukan wiping data pada tool eraser dengan menggunakan metode Random Data Overwrite yang mendapatkan hasil bahwa seluruh dataset telah terhapus dan terisi dengan nilai random. Pada Tools ini dalam melakukan Random Data Overwrite membutuhkan waktu 01:35:36 dengan Kebutuhan CPU 1.5% (15 Threads) dan kebutuhan Memory 38.7 MB.



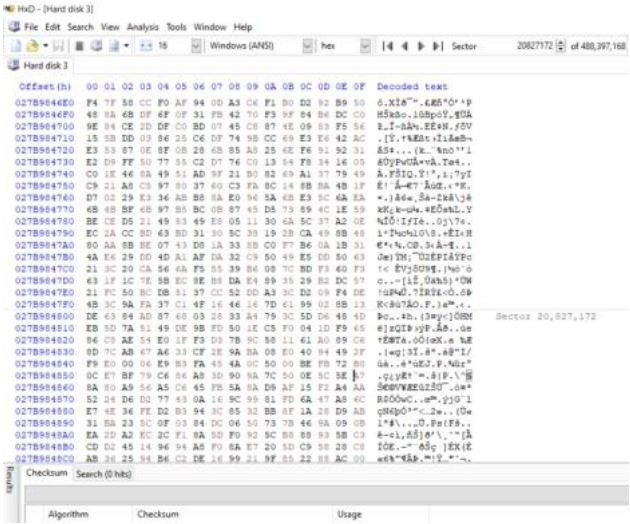
Gambar 3. Tampilan HxD setelah wiping data dengan metode Random Data pada tools Eraser



Gambar 4. Tampilan HxD setelah wiping data dengan metode U.S DoD 5220.22-M (E) pada tools Eraser



Gambar 5. Tampilan HxD setelah wiping data dengan metode U.S DoD 5220.22-M (ECE) pada tools Eraser



Gambar 6. Tampilan HxD setelah wiping data dengan metode Bruce Schneier's Algorithm pada tools Eraser

U.S. DoD 5220.22-M (E)

Pada Gambar 4 merupakan hasil yang didapat setelah dilakukan wiping data dengan menggunakan metode U.S DoD 5220.22-M (E) yang mendapatkan hasil bahwa seluruh dataset telah terhapus dan terisi dengan nilai random. Pada Tools ini dalam melakukan U.S DoD 5220.22-M (E) membutuhkan waktu 04:51:42 dengan Kebutuhan CPU 3.2% (13 Threads) dan kebutuhan Memory 29.2 MB.

U.S. DoD 5220.22-M (ECE)

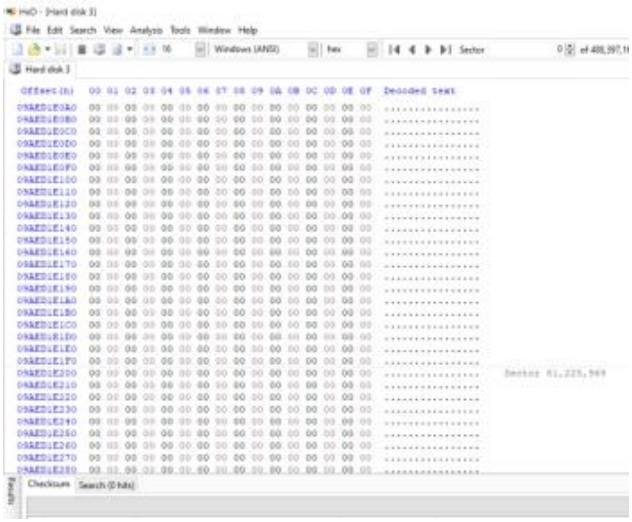
Pada Gambar 5 merupakan hasil yang didapat setelah dilakukan wiping data dengan menggunakan metode U.S DoD 5220.22-M (ECE) yang mendapatkan hasil bahwa seluruh dataset telah terhapus dan terisi oleh nilai random. Pada Tools ini dalam melakukan U.S DoD 5220.22-M (ECE) membutuhkan waktu 11:21:33 dengan Kebutuhan CPU 3.3% (13 Threads) dan kebutuhan Memory 27.3 MB.

Bruce Schneier's Algorithm

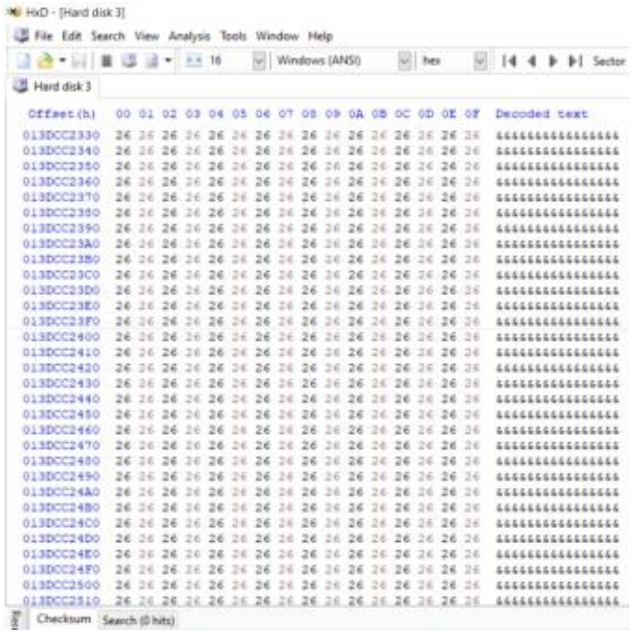
Pada Gambar 6 merupakan hasil yang didapat setelah dilakukan wiping data dengan menggunakan metode Bruce Schneier's Algorithm yang mendapatkan hasil bahwa seluruh dataset telah terhapus dan terisi oleh random. Pada Tools ini dalam melakukan Bruce Schneier's Algorithm membutuhkan waktu 11:12:57 dengan Kebutuhan CPU 2.4% (12 Threads) dan kebutuhan Memory 28.0 MB. Selanjutnya pengujian Harddisk yang sudah dilakukan wiping data random overwrite menggunakan tools recovery.

B. Disk Wipe

Pada tools ini, proses wiping data menggunakan metode Zero Overwrite, Random Data Overwrite, U.S. DoD 5220.22-M (E), dan U.S. DoD 5220.22-M (ECE). Meskipun tidak tersedia metode wiping Bruce Schneier's Algorithm, namun dalam aplikasinya terdapat beragam metode wiping data lain seperti British HMG IS5 (baseline), Russian GOST P50739-95, dan Peter Guttman.



Gambar 7. Tampilan HxD setelah wiping data dengan metode Zero Overwrite pada tools Disk Wipe



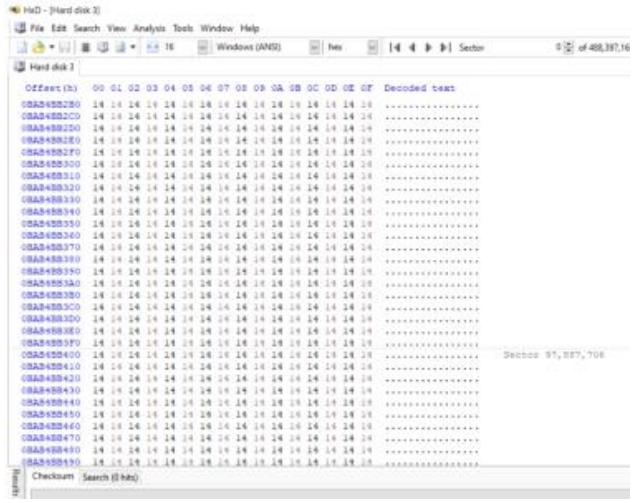
Gambar 8. Tampilan HxD setelah wiping data dengan metode Random Data pada tools Disk Wipe

Zero Overwrite

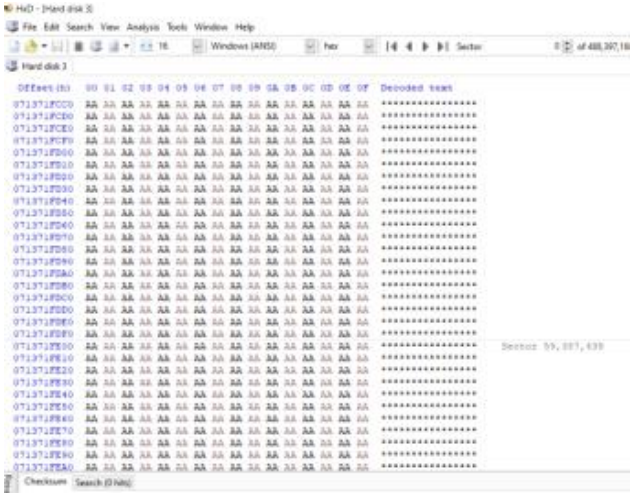
Pada Gambar 7 merupakan hasil yang didapat setelah dilakukan wiping data dengan menggunakan metode Zero Overwrite yang mendapatkan hasil bahwa seluruh dataset telah terhapus dan diisi oleh nilai zero. Pada Tools ini dalam melakukan Zero Overwrite membutuhkan waktu 03:16:10 dengan Kebutuhan CPU 1.4% (2 Threads) dan kebutuhan Memory 2.8 MB.

Random Data Overwrite

Pada Gambar 8, hasil yang didapat setelah dilakukan wiping data dengan menggunakan metode Random Data Overwrite adalah bahwa seluruh dataset telah terhapus dan diisi dengan nilai 26. Pada Tools ini dalam melakukan Random Data Overwrite membutuhkan waktu



Gambar 9. Tampilan HxD setelah wiping data dengan metode U.S. DoD 5220.22-M (E) pada tools Disk Wipe



Gambar 10. Tampilan HxD setelah wiping data dengan metode U.S. DoD 5220.22-M (ECE) pada tools Disk Wipe

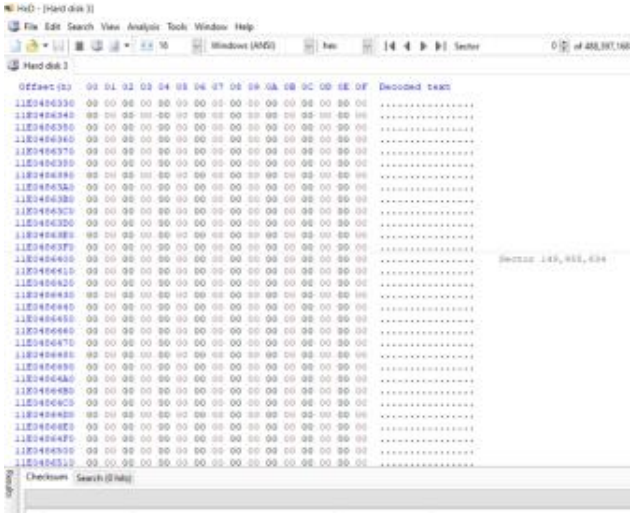
03:16:51 dengan Kebutuhan CPU 1.8% (2 Threads) dan kebutuhan Memory 2.8 MB.

U.S. DoD 5220.22-M (E)

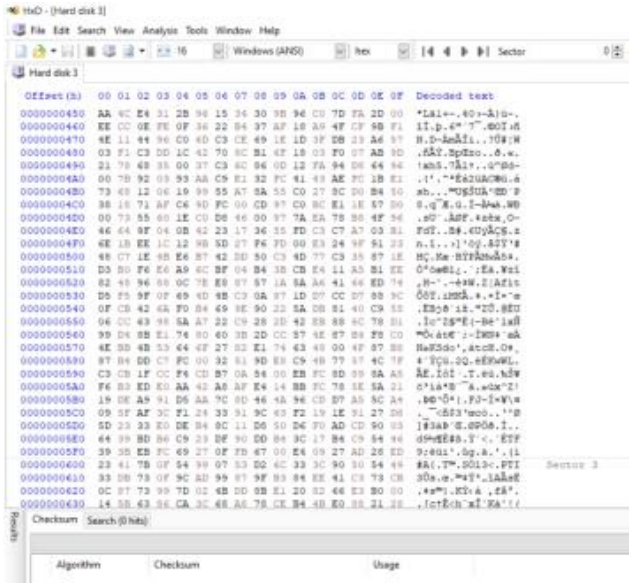
Pada Gambar 9, hasil yang didapat setelah dilakukan wiping data dengan menggunakan metode U.S. DoD 5220.22-M (E) adalah bahwa seluruh dataset telah terhapus dan nilai ditimpa oleh angka 14. Pada Tools ini dalam melakukan U.S. DoD 5220.22-M (E) membutuhkan waktu 03:18:51 dengan Kebutuhan CPU 2.1% (2 Threads) dan kebutuhan Memory 2.8 MB.

U.S. DoD 5220.22-M (ECE)

Pada Gambar 10, hasil yang didapat setelah dilakukan wiping data dengan menggunakan metode U.S. DoD 5220.22-M (ECE) adalah bahwa seluruh dataset telah terhapus dengan menimpa nilai AA. Pada Tools ini dalam melakukan U.S. DoD 5220.22-M (ECE) membutuhkan waktu 03:23:35 dengan Kebutuhan CPU 3.0% (2 Threads) dan kebutuhan Memory 2.9 MB.



Gambar 11. Tampilan HxD setelah wiping data dengan metode Zero Overwrite pada tools AOMEI Partition Assistant Professional



Gambar 12. Tampilan HxD setelah wiping data dengan metode Random Data Overwrite pada tools AOMEI Partition Assistant Professional

C. AOMEI Partition Assistant Professional

Pada tools ini, proses wiping data menggunakan metode Zero Overwrite, Random Data Overwrite, U.S. DoD 5220.22-M (E), dan U.S. DoD 5220.22-M (ECE). Meskipun tidak tersedia metode wiping Bruce Schneier's Algorithm, namun dalam aplikasinya terdapat metode wiping data lain, yaitu Peter Guttman.

Zero Overwrite

Pada Gambar 11, hasil yang didapat setelah dilakukan wiping data dengan menggunakan metode Zero Overwrite adalah bahwa seluruh dataset telah terhapus dan semua nilai diubah menjadi zero. Pada Tools ini dalam melakukan Zero Overwrite membutuhkan waktu 02:12:29 dengan Kebutuhan CPU 0.2% (3 Threads) dan kebutuhan Memory 2.8 MB.

Random Data Overwrite

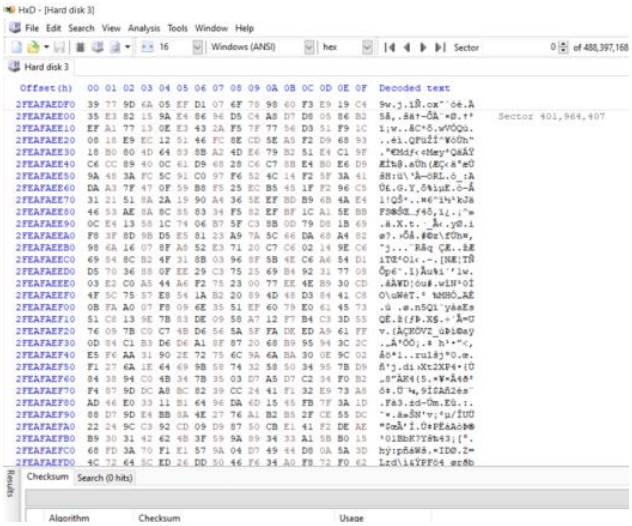
Pada Gambar 12, hasil yang didapat setelah dilakukan wiping data dengan menggunakan metode Random Data Overwrite adalah bahwa seluruh dataset telah terhapus. Pada Tools ini dalam melakukan Random Data Overwrite membutuhkan waktu 02:12:29 dengan Kebutuhan CPU 0.1% (10 Threads) dan kebutuhan Memory 10.5 MB.

U.S. DoD 5220.22-M (E)

Pada Gambar 13, hasil yang didapat setelah dilakukan wiping data dengan menggunakan metode U.S. DoD 5220.22-M (E) adalah bahwa seluruh dataset telah terhapus dan nilai ditimpa oleh random karakter. Pada Tools ini dalam melakukan U.S. DoD 5220.22-M (E) membutuhkan waktu 06:37:27 dengan Kebutuhan CPU 0.2% (4 Threads) dan kebutuhan Memory 5.8 MB.

U.S. DoD 5220.22-M (ECE)

Pada Gambar 14, hasil yang didapat setelah dilakukan wiping data dengan menggunakan metode U.S. DoD 5220.22-M (ECE) adalah bahwa seluruh dataset telah terhapus dan ditimpa oleh nilai random. Pada Tools ini dalam melakukan U.S. DoD 5220.22-M (ECE) membutuhkan waktu 15:27:24 dengan Kebutuhan CPU 0.3% (7 Threads) dan kebutuhan Memory 10.8 MB.



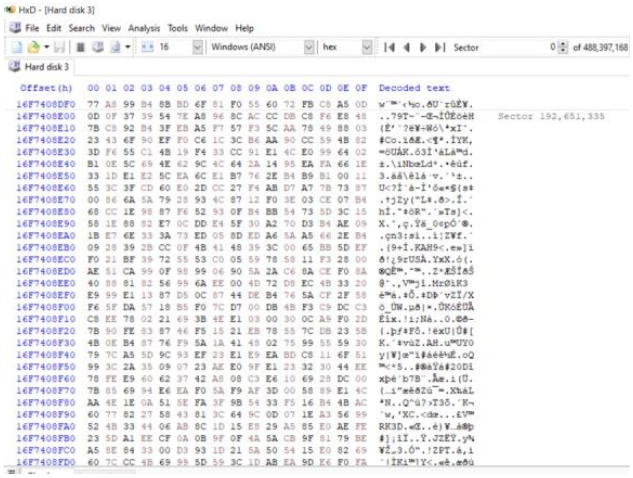
Gambar 13. Tampilan HxD setelah wiping data dengan metode U.S. DoD 5220.22-M (E) pada tools AOMEI Partition Assistant Professional

D. AOMEI Backupper

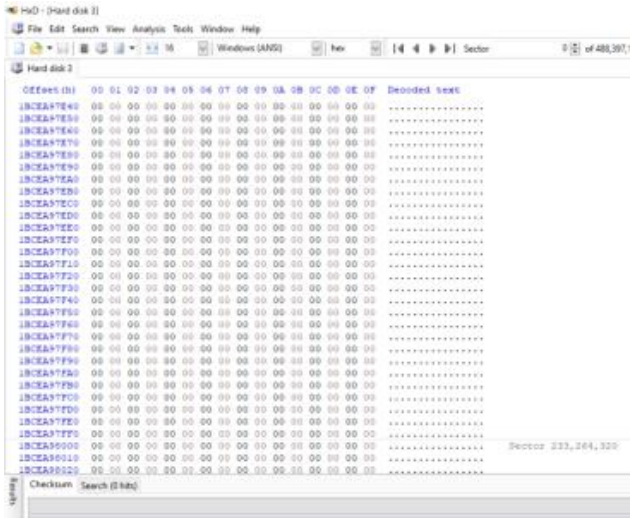
Pada tools ini, proses wiping data menggunakan metode Zero Overwrite, Random Data Overwrite, U.S. DoD 5220.22-M (E), dan U.S. DoD 5220.22-M (ECE). Meskipun tidak tersedia metode wiping Bruce Schneier's Algorithm, namun dalam aplikasinya terdapat metode wiping data lain, yaitu Peter Guttman.

Zero Overwrite

Pada Gambar 15, hasil yang didapat setelah dilakukan wiping data dengan menggunakan metode Zero Overwrite adalah bahwa seluruh dataset telah terhapus dan nilai pada sector ditimpa dengan zero. Pada Tools ini dalam melakukan Zero Overwrite membutuhkan waktu 01:35:41 dengan Kebutuhan CPU 0,3% (5 Threads) dan kebutuhan Memory 27.6 MB.



Gambar 14. Tampilan HxD setelah wiping data dengan metode U.S. DoD 5220.22-M (ECE) pada tools AOMEI Partition Assistant Professional



Gambar 15. Tampilan HxD setelah wiping data dengan metode Zero Overwrite pada tools AOMEI Backupper

Random Data Overwrite

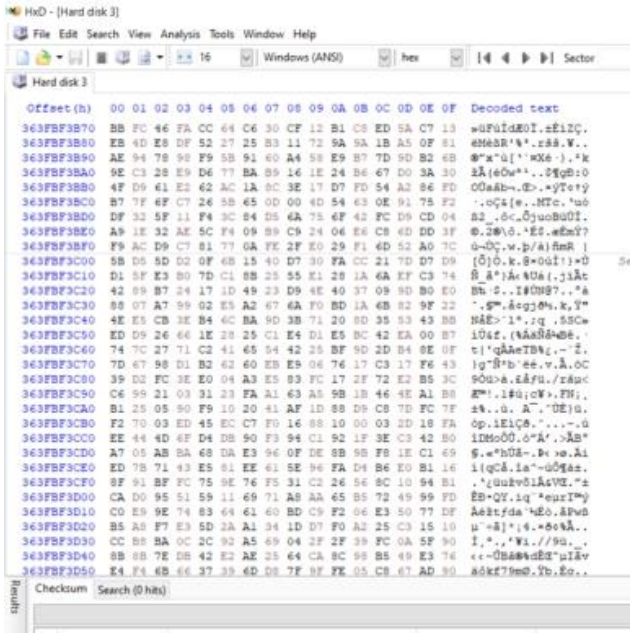
Pada Gambar 16, hasil yang didapat setelah dilakukan wiping data dengan menggunakan metode Random Data Overwrite adalah bahwa seluruh dataset telah terhapus dan diisi oleh nilai random. Pada Tools ini dalam melakukan Random Data Overwrite membutuhkan waktu 02:12:51 dengan Kebutuhan CPU 0.2% (2 Threads) dan kebutuhan Memory 11.6 MB.

U.S. DoD 5220.22-M (E)

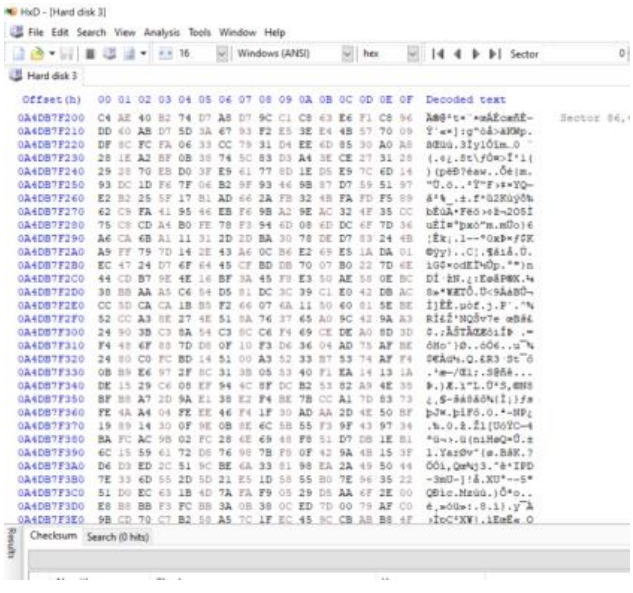
Pada Gambar 17, hasil yang didapat setelah dilakukan wiping data dengan menggunakan metode U.S. DoD 5220.22-M (E) adalah bahwa seluruh dataset telah terhapus dan diisi oleh nilai random. Pada Tools ini dalam melakukan U.S. DoD 5220.22-M (E) membutuhkan waktu 06:56:49 dengan Kebutuhan CPU 0.3% (2 Threads) dan kebutuhan Memory 27.5 MB.

U.S. DoD 5220.22-M (ECE)

Pada Gambar 18, hasil yang didapat setelah dilakukan wiping data dengan menggunakan metode U.S. DoD 5220.22-M (ECE) adalah bahwa seluruh dataset telah terhapus dan diisi oleh nilai random. Pada Tools



Gambar 16. Tampilan HxD setelah wiping data dengan metode Random Data Overwrite pada tools AOMEI Backupper

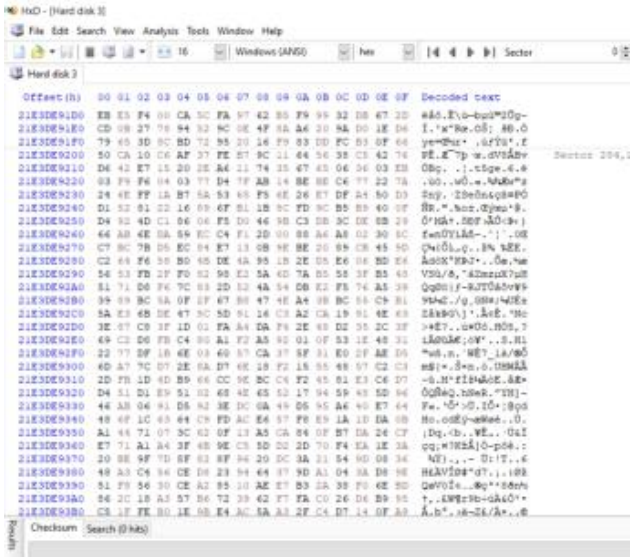


Gambar 17. Tampilan HxD setelah wiping data dengan metode U.S. DoD 5220.22-M (E) pada tools AOMEI Backupper

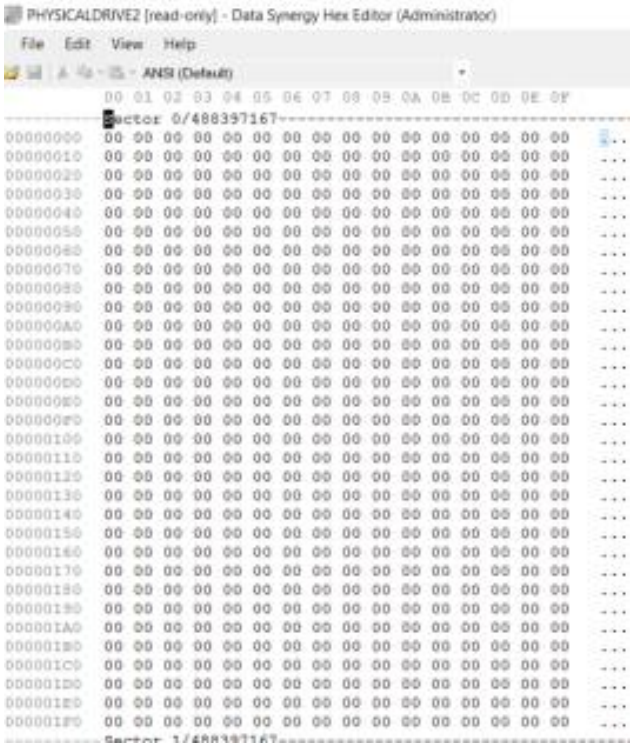
ini dalam melakukan U.S. DoD 5220.22-M (ECE) membutuhkan waktu 15:20:23 dengan Kebutuhan CPU 0.4% (5 Threads) dan kebutuhan Memory 27.6 MB.

E. Hardwipe

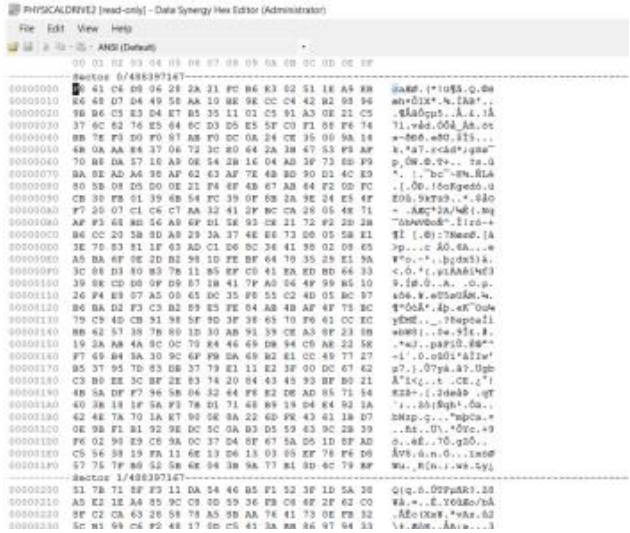
Pada tools ini, proses wiping data menggunakan metode Zero Overwrite, Random Data Overwrite, U.S. DoD 5220.22-M (E), dan Bruce Schneier's Algorithm. Meskipun tidak tersedia metode wiping U.S. DoD 5220.22-M (ECE), namun dalam aplikasinya terdapat metode wiping data lain yang beragam seperti GOST R 50739-95, RAZER, RAZER+, RAZER++, VSITR, dan Peter Guttman.



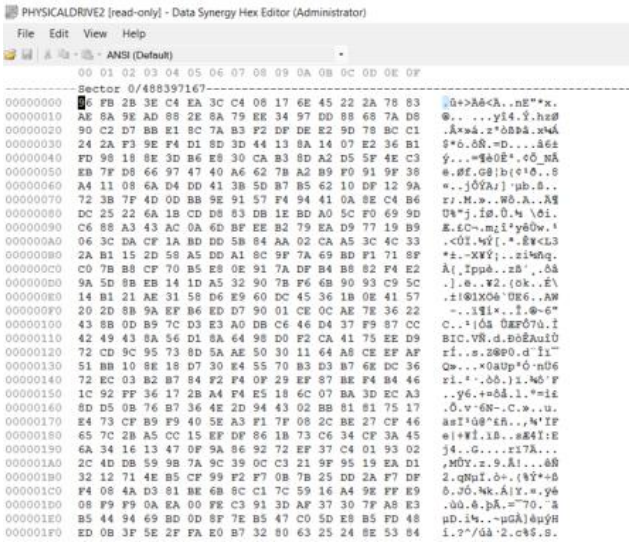
Gambar 18. Tampilan HxD setelah wiping data dengan metode U.S. DoD 5220.22-M (ECE) pada tools AOMEI Backupper



Gambar 19. Tampilan nilai hexa Harddisk setelah wiping data dengan metode Zero Overwrite pada tools Hardwipe



Gambar 20. Tampilan nilai hexa Harddisk setelah wiping data dengan metode Random Data Overwrite pada tools Hardwipe



Gambar 21. Tampilan nilai hexa Harddisk setelah wiping data dengan metode U.S. DoD 5220.22-M (E) pada tools Hardwipe

Zero Overwrite

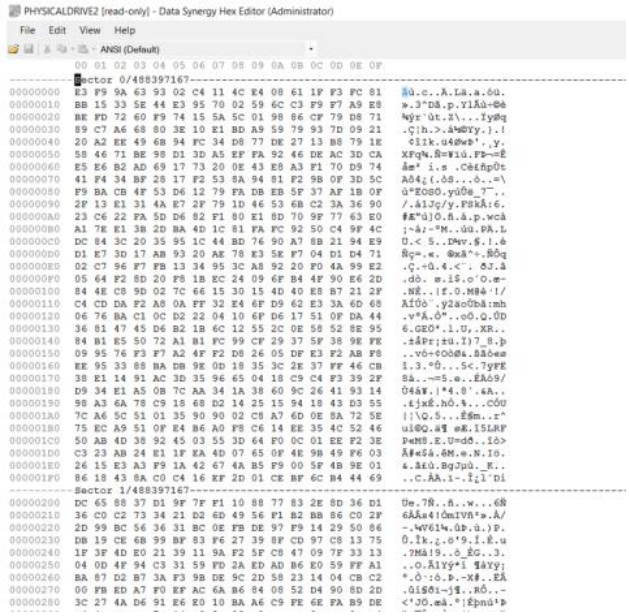
Pada Gambar 19, hasil yang didapat setelah dilakukan wiping data dengan menggunakan metode Zero Overwrite adalah bahwa seluruh dataset telah terhapus dan menimpa dengan nilai zero. Pada Tools ini dalam melakukan Zero Overwrite membutuhkan waktu 01:34:49 dengan Kebutuhan CPU 2.8% (7 Threads) dan kebutuhan Memory 16.7 MB.

Random Data Overwrite

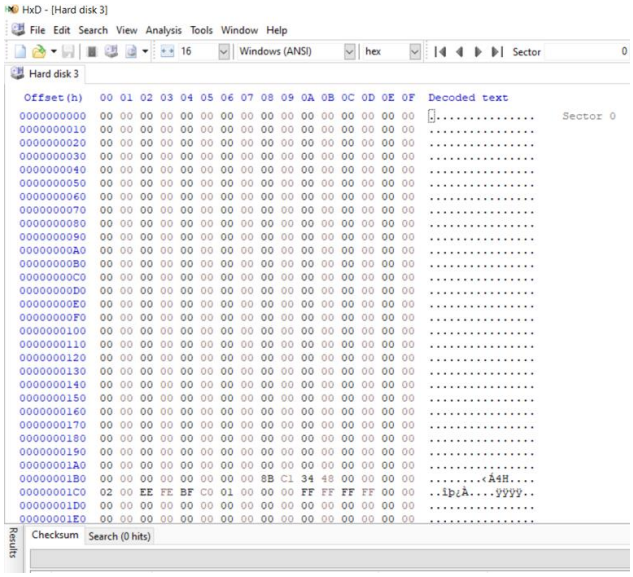
Pada Gambar 20, hasil yang didapat setelah dilakukan wiping data dengan menggunakan metode Random Data Overwrite adalah bahwa seluruh dataset telah terhapus dan diisi oleh nilai yang random. Pada Tools ini dalam melakukan Random Data Overwrite membutuhkan waktu 01:35:10 dengan Kebutuhan CPU 2.4% (7 Threads) dan kebutuhan Memory 16.7 MB.

U.S. DoD 5220.22-M (E)

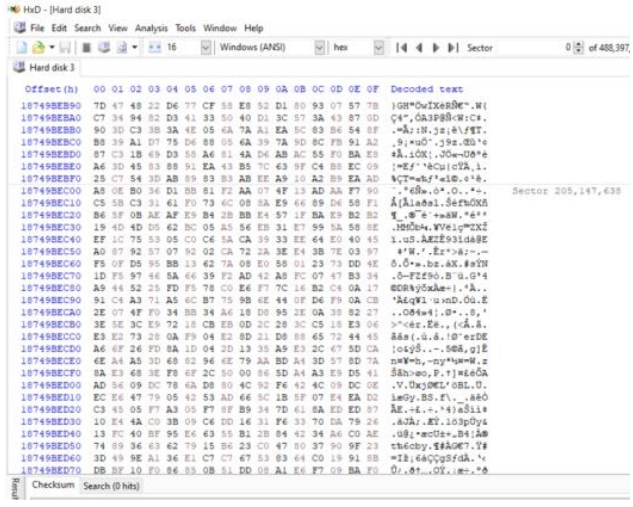
Pada Gambar 21, hasil yang didapat setelah dilakukan wiping data dengan menggunakan metode U.S. DoD 5220.22-M (E) adalah bahwa seluruh dataset telah terhapus dan diisi oleh nilai yang random. Pada Tools ini dalam melakukan U.S. DoD 5220.22-M (E) membutuhkan waktu 04:14:30 dengan Kebutuhan CPU 3.2% (7 Threads) dan kebutuhan Memory 16.7 MB.



Gambar 22. Tampilan nilai hexa Harddisk setelah wiping data dengan metode Bruce Schneier's Algorithm pada tools Hardwipe



Gambar 23. Tampilan HxD setelah wiping data dengan metode Zero Overwrite pada tools Hard Drive Eraser



Gambar 24. Tampilan HxD setelah wiping data dengan metode U.S. DoD 5220.22-M (E) pada tools Hard Drive Eraser

Bruce Schneier's Algorithm

Pada Gambar 22, hasil yang didapat setelah dilakukan wiping data dengan menggunakan metode Bruce Schneier's Algorithm adalah bahwa seluruh dataset telah terhapus dan diisi oleh nilai yang random. Pada Tools ini dalam melakukan Bruce Schneier's Algorithm membutuhkan waktu 11:08:42 dengan Kebutuhan CPU 3.6% (7 Threads) dan kebutuhan Memory 16.7 MB.

Hard Drive Eraser

Pada tools ini, proses wiping data menggunakan metode Zero Overwrite, U.S. DoD 5220.22-M (E), dan 5220.22-M (E). Meskipun tidak tersedia metode wiping Random Data Overwrite, U.S. DoD 5220.22-M (ECE), dan Bruce Schneier's Algorithm, namun dalam aplikasinya terdapat metode wiping data lain yang beragam seperti US Army AR380-19, dan Peter Guttman.

Zero Overwrite

Pada Gambar 23, hasil yang didapat setelah dilakukan wiping data dengan menggunakan metode Zero Overwrite adalah bahwa seluruh dataset telah terhapus dan diisi oleh nilai zero. Pada Tools ini dalam melakukan Zero Overwrite membutuhkan waktu 01:44:37 dengan Kebutuhan CPU 18.9% (5 Threads) dan kebutuhan Memory 4.4 MB.

U.S. DoD 5220.22-M (E)

Pada Gambar 24, hasil yang didapat setelah dilakukan wiping data dengan menggunakan metode U.S. DoD 5220.22-M (E) adalah bahwa seluruh dataset telah terhapus dan diisi oleh nilai random. Pada Tools ini dalam melakukan U.S. DoD 5220.22-M (E) membutuhkan waktu 01:49:48 dengan Kebutuhan CPU 19.7% (5 Threads) dan kebutuhan Memory 4.4 MB.

Analisis Hasil Pengujian

Berdasarkan pada perancangan alur penelitian mengenai testing tools dengan performance testing yang terdapat pada gambar 2, proses analisa yang dilakukan setelah pengujian penghapusan adalah pengujian perfomansi tools. Hasil pengamatan yang dilakukan pada saat proses penerapan metode wiping data, menghasilkan data dari tiap proses, dan data tersebut akan di uji. Pada Tabel 8 menunjukkan perbedaan performa dari masing-masing metode.

Berdasarkan Tabel 2 yang menunjukkan perbedaan proses dari *tools* dan bebagai metode yang dicoba, jika dilihat dari variabel *running time*, bahwa proses *wiping data* pada *tools eraser* mempunyai running time yang sesuai, karena dilhiat dari tingkat kompleksitas metode wiping data yang berbeda maka adanya perbedaan pada *running time* memperlihatkan bahwa metode nya dijalankan dengan baik.

Sedangkan pada tools Disk Wipe mempunyai running time yang hampir sama dan dapat dilihat dari nilai hexa pada harddisk setelah dilakukan wiping data, pada metode Random Data Overwrite nilai dari harddisk ditimpa oleh angka 26 seharusnya metode ini menimpa harddisk dengan karakter random, pada metode U.S. DoD 5220.22-M (E) nilai dari harddisk ditimpa oleh angka 14 seharusnya metode ini menimpa harddisk dengan karakter random, dan pada metode U.S.

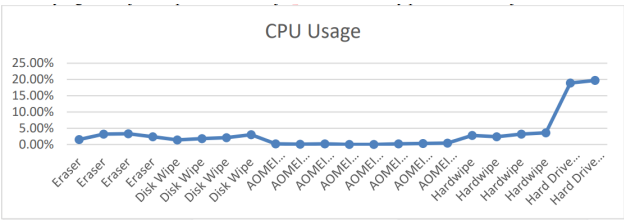
Table 2. Trade-off Tools

Metode	Tools	Running TIme	Memory Usage	CPU Usage
Random Data Overwrite	Eraser	1:35:36	38.7 MB	1.50%
U.S. DoD 5220.22-M (E)	Eraser	4:51:42	29.2 MB	3.20%
U.S. DoD 5220.22-M (ECE)	Eraser	11:21:33	27.3 MB	3.30%
Bruce Schneief's Algorithm	Eraser	11:12:57	28.0 MB	2.40%
Zero Overwrite	Disk Wi	3:16:10	2.8 MB	1.40%
Random Data Overwrite	DiskWi	3:16:51	2.8 MB	1.80%
U.S. DoD 5220.22-M (E)	Disk Wi	3:18:51	2.8 MB	2.10%
U.S. DoD 5220.22-M (ECE)	Disk Wi e	3:23:35	2.9 MB	3.00%
Zero Overwrite	AOMEI Partition Assistant Professional	2:12:29	2.8 MB	0.20%
Random Data Overwrite	AOMEI Partition Assistant Professional	2:12:29	10.5 MB	0.10%
U.S. DoD 5220.22-M (E)	AOMEI Partition Assistant Professional	6:37:27	5.8 MB	0.20%
U.S. DoD 5220.22-M (ECE)	AOMEI Partition Assistant Professional	15:27:24	10.8 MB	0,3%
Zero Overwrite	AOMEI Backupper	1:35:41	27.6 MB	0,3%
Random Data Overwrite	AOMEI Backupper	2:12:51	11.6 MB	0.20%
U.S. DoD 5220.22-M (E)	AOMEI Backupper	6:56:49	27.5 MB	0.30%
U.s. DoD 5220.22-M (ECE)	AOMEI Backupper	15:20:23	27.6 MB	0.40%
Zero Overwrite	Hardwipe	1:34:49	16.7 MB	2.80%
Random Data Overwrite	Hardwipe	1:35:10	16.7 MB	2.40%
U.s. DoD 5220.22-M (E)	Hardwipe	4:14:30	16.7 MB	3.20%
Bruce Schneier's Algorithm	Hardwipe	11:08:42	16.7 MB	3.60%
Zero Overwrite	Hard Drive Eraser	1:44:37	4.4 MB	18.90%
U.s. DoD 5220.22-M (E)	Hard Drive Eraser	1:49:48	4.4 MB	19.70%

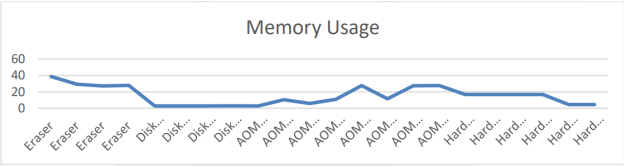
DoD 5220.22-M (ECE) nilai dari harddisk ditimpa oleh karakter AA seharusnya metode ini menimpa harddisk dengan karakter random. Ini menunjukkan bahwa pada tools Disk Wipe tidak menerapkan ketiga metode tadi dengan benar jika dilihat dari running time dan hasil 19 dari nilai harddisk yang diliat dalam hexa.

Pada tools AOMEI Partition Assistant Professional dan AOMEI Backupper memiliki running time yang mendekati sama dan running time nya sudah sesuai diliat dari tingkat kompleksitas metode wiping data. Dan dianggap kedua tools ini sudah menerapkan metode wiping data secara benar jika dilihat dari running time. Lalu pada tools Hardwipe jika dilihat memiliki running time yang mirip dengan tools eraser dan tools ini dianggap sudah menerapkan metode secara benar jika diliat dari running time. Dan pada tools Hard Drive Eraser mempunyai running time yang sama seperti tools Disk Wipe yang menunjukkan bahwa pada tools Hard Drive Eraser tidak menerapkan metode wiping data dengan benar jika dilihat dari running time.

Terdapat juga perbedaan hasil wiping data pada tools yang dilakukan dengan penelitian terhadulu, pada jurnal "Implementasi Anti Forensik pada Harddisk Menggunakan Metode DoD 5220.22 M dan British HMG IS5 E" [10], melakukan penghapusan dengan metode 5220.22 M dengan tools yang sama yaitu eraser mendapatkan hasil running time yang lebih cepat, namun file yang berhasil dilakukan recovery lebih banyak. Sedangkan pada jurnal "Analisis Metode Wiping Air Force System Security Instruction 5020 dan Department of Defense 5220.22 M Sebagai Usaha Anti Forensik Pada Media Penyimpanan Flash Disk dan Hard Disk Drive" yang menggunaakan metode 5220.22 M pada tools yang sama juga yaitu eraser memiki running time yang lebih cepat lagi dari jurnal sebelumnya, dan menghasilkan tidak dapat terdeteksi file untuk recovery.



Gambar 25. CPU Usage



Gambar 26. Memory Usage

Untuk kinerja dari CPU dan Memory sendiri sangat beragam dari semua tools dapat dilihat di gambar 25 dan gambar 26 yang menunjukkan perbedaan kinerja CPU dan Memory pada tools lebih jelas.

Berdasarkan gambar 25 penggunaan CPU yang paling berat adalah pada tools Hard Drive Eraser, dengan menunjukan perbedaan yang signifikan diantara yang lain, sedangkan yang paling ringan adalah tools AOMEI Partition Assistant Professional. Penggunaan CPU ini menunjukan seberapa banyak operasi yang dilakukan pada aplikasi,

Table 3. MiniTool Power Data Recovery 11.4

Metode	Tools	File	Keterangan
Random Data Overwrite	Eraser	86	Tidak Teridentifikasi
U.S. DoD 5220.22-M (E)	Eraser	81	Tidak Teridentifikasi
U.s. DoD 5220.22-M (ECE)	Eraser	66	Tidak Teridentifikasi
Bruce Schneier's Algorithm	Eraser	93	Tidak Teridentifikasi
Zero Overwrite	Disk Wipe	117	Tidak Teridentifikasi
Random Data Overwrite	Disk Wipe	117	Tidak Teridentifikasi
U.s. DoD 5220.22-M (E)	Disk Wipe	117	Tidak Teridentifikasi
U.S. DoD 5220.22-M (ECE)	Disk Wipe	117	Tidak Teridentifikasi
Zero Overwrite	AOMEI Partition Assistant Professional	0	Tidak Teridentifikasi
Random Data Overwrite	AOMEI Partition Assistant Professional	0	Tidak Teridentifikasi
U.S. DoD 5220.22-M (E)	AOMEI Partition Assistant Professional	0	Tidak Teridentifikasi
U.s. DoD 5220.22-M (ECE)	AOMEI Partition Assistant Professional	0	Tidak Teridentifikasi
Zero Overwrite	AOMEI Backupper	0	Tidak Teridentifikasi
Random Data Overwrite	AOMEI Backupper	0	Tidak Teridentifikasi
U.s. DoD 5220.22-M (E)	AOMEI Backupper	0	Tidak Teridentifikasi
U.s. Doro 5220.22-M (ECE)	AOMEI Backupper	0	Tidak Teridentifikasi
Zero Overwrite	Hardwipe	0	Tidak Teridentifikasi
Random Data Overwrite	Hardwipe	80	Tidak Teridentifikasi
U.s. DoD 5220.22-M (E)	Hardwipe	74	Tidak Teridentifikasi
Bruce Schneier's Algorithm	Hardwipe	88	Tidak Teridentifikasi
Zero Overwrite	Hard Drive Eraser	117	Tidak Teridentifikasi
U.s. DoD 5220.22-M (E)	Hard Drive Eraser	117	Tidak Teridentifikasi

dari hasil ini didapat kan bahwa umumnya pada tools yang menggunakan metode wiping berbeda memiliki CPU usage yang tidak jauh berbeda artinya penggunaan CPU tidak terlalu ditentukan pada metode wiping data, namun dari tools, yang artinya tools yang mempunyai pemrosesan data lebih baik akan memakai lebih sedikit CPU.

Berdasarkan gambar 26 penggunaan Memory dapat dilihat ada dua tools yaitu Disk Wipe dan Hard Drive Eraser yang mempunyai perbedaan diantara yang lain, padaa kedua tools ini memiliki penggunaan memory yang relatif sedikit. Penggunaan memory ini menunjukan seberapa besar proses yang dilakukan pada memory, dalam hal ini berbeda dengan CPU yang mempunyai sedikit perbedaan pada setiap metode wiping data dalam satu tools, pada memory usage mempunyai perbedaan yang cukup berpengaruh pada tools dalam setiap metode wiping data nya. Tahap selanjutnya dalam pengujian perfomansi tools adalah dari sisi keamanan data setelah melakukan wiping data, Seperti ada tidaknya nama file dan ukuran file dan juga jumlah file yang dapat di deteksi, atau bahkan dilakukan recovery. Untuk melakukan pengujiannya menggunakan 3 tools recovery data yaitu :

1. MiniTool Power Data Recovery 11.4
2. EaseUS Data Recovery Wizard
3. Recuva

Pada tools recovery pertama yaitu MiniTool Power Data Recovery 11.4 yang dapat dilihat pada tabel 3.

Berdasarkan Tabel 3 yang menunjukkan kemiripan hasil pemulihan pada tools Eraser dan Hardwipe, AOMEI Partition Assistant Professional dan AOMEI Backupper, Disk Wipe dan Hard Drive Eraser. Lalu tools recovery yang kedua yaitu EaseUS Data Recovery Wizard dapat dilihat pada tabel 4.

Berdasarkan Tabel 4 hasil recovery tidak jauh berbeda pada tools recovery sebelumnya, namun pada terdapat lebih sedikit jumlah file yang dapat di recovery dibanding tools sebelumnya. Pada tools recovery yang terakhir yaitu Recuva dapat dilihat pada tabel 5.

Berdasarkan Tabel 5 hasil recovery tidak jauh berbeda pula namun pada rools recover ini tidak berhasil mendeteksi file apapun pada tools Hardwipe. Sedangkan pada setiap metode wiping data yaitu Zero Overwrite, Random Data Overwrite, U.S. DoD 5220.22-M (E), U.S. DoD 5220.22-M (ECE), dan Bruce Schneier's Algorithm. Menghasilkan hasil pada tools sebagai berikut.

1. *Zero Overwrite*
   Berdasarkan Tabel 6 Mengenai hasil wiping data menggunakan metode Zero Overwrite pada setiap tools, dapat diambil kesimpulan pada penelitian kali ini tools yang optimal melakukan wiping data dengan metode Zero Overwrite adalah AOMEI Partition Assistant Professional, AOMEI Backupper, dan Hardwipe.
2. *Random Data Overwrite*
   Berdasarkan Tabel 7 Mengenai hasil wiping data menggunakan Random Data Overwrite pada setiap tools, dapat diambil kesimpulan pada penelitian kali ini tools yang optimal melakukan wiping data dengan metode Random Data Overwrite adalah AOMEI Partition Assistant Professional, dan AOMEI Backupper.
3. U.S. DoD 5220.22-M (E)
   Berdasarkan Tabel 8 Mengenai hasil wiping data menggunakan U.S. DoD 5220.22-M (E) pada setiap tools, dapat diambil kesimpulan pada penelitian kali ini tools yang optimal melakukan wiping

Table 4. EaseUS Data Recovery Wizard

Metode	Tools	File	Keterangan
Random Data Overwrite	Eraser	4	Teridentifikasi
U.S. DoD 5220.22-M (E)	Eraser	3	Teridentifikasi
U.s. DoD 5220.22-M (ECE)	Eraser	2	Teridentifikasi
Bruce Schneier's Algorithm	Eraser	2	Teridentifikasi
Zero Overwrite	Disk Wipe	117	Tidak Teridentifikasi
Random Data Overwrite	Disk Wipe	117	Tidak Teridentifikasi
U.s. DoD 5220.22-M (E)	Disk Wipe	117	Tidak Teridentifikasi
U.S. DoD 5220.22-M (ECE)	Disk Wipe	117	Tidak Teridentifikasi
Zero Overwrite	AOMEI Partition Assistant Professional	0	Tidak Teridentifikasi
Random Data Overwrite	AOMEI Partition Assistant Professional	0	Tidak Teridentifikasi
U.S. DoD 5220.22-M (E)	AOMEI Partition Assistant Professional	0	Tidak Teridentifikasi
U.s. DoD 5220.22-M (ECE)	AOMEI Partition Assistant Professional	0	Tidak Teridentifikasi
Zero Overwrite	AOMEI Backupper	0	Tidak Teridentifikasi
Random Data Overwrite	AOMEI Backupper	0	Tidak Teridentifikasi
U.S. DoD 5220.22-M (E)	AOMEI Backupper	0	Tidak Teridentifikasi
U.S. DoD 5220.22-M (ECE)	AOMEI Backupper	0	Tidak Teridentifikasi
Zero Overwrite	Hardwipe	0	Tidak Teridentifikasi
Random Data Overwrite	Hardwipe		Teridentifikasi
U.S. DoD 5220.22-M (E)	Hardwipe	0	Tidak Teridentifikasi
Bruce Schneier'sAl orithm	Hardwipe	5	Teridentifikasi
Zero Overwrite	Hard Drive Eraser	117	Tidak Teridentifikasi
U.s. DoD 5220.22-M (E)	Hard Drive Eraser	117	Tidak Teridentifikasi

data dengan metode U.S. DoD 5220.22-M (E) adalah AOMEI Partition Assistant Professional, dan AOMEI Backupper.

4. U.S. DoD 5220.22-M (ECE)
   Berdasarkan Tabel 9 Mengenai hasil wiping data menggunakan U.S. DoD 5220.22-M (ECE) pada setiap tools, dapat diambil kesimpulan pada penelitian kali ini tools yang optimal melakukan wiping data dengan metode U.S. DoD 5220.22-M (ECE) adalah AOMEI Partition Assistant Professional, dan AOMEI Backupper.
5. Bruce Schneier's *Algorithm*
   Berdasarkan Tabel 10 Mengenai hasil wiping data menggunakan Bruce Schneier's Algorithm pada setiap tools, dapat diambil kesimpulan pada penelitian kali ini belum ada tools yang dapat dengan optimal melakukan wiping data dengan metode Bruce Schneier's Algorithm.

Analisis Dampak dari Hasil Pengujian

Berdasarkan hasil dari pengujian yang dilakukan, mempunyai tujuan untuk membantu penyidik dalam melakukan penyidikan terhadap jenis *anti-forensics data destruction* yaitu *data wiping*. Merujuk ke pasal 6 UU ITE yang mensyaratkan bahwa suatu informasi harus berbentuk tertulis atau asli, Informasi Elektronik dan/atau Dokumen Elektronik dianggap sah sepanjang informasi yang tercantum di dalamnya dapat diakses, ditampilkan, dijamin keutuhannya, dan dapat dipertanggung jawabkan sehingga menerangkan suatu keadaan.

Kaitannya dengan *data wiping* terhadap syarat sah informasi elektronik dan/atau dokumen elektronik dalam persidangan adalah setelah dilakukan data wiping penyidik dapat mengetahui gambaran tentang data apakah masih bisa dijadikan bukti dalam persidangan atau tidak, dan dengan adanya pengujian ini dapat dijadikan sebagai usaha untuk membantu penyidik untuk melihat sejauh mana dampak *anti-forensics* terhadap kepentingan penyidikan, seperti yang dapat di lihat dari hasil pengujian *tools data wiping*, sejauh mana *data wiping* ini berpengaruh terhadap kepentingan penyidikan.

Data wiping mempunyai banyak algoritma yang diimplementasi pada tools data wiping, dapat dilihat dampak dari setiap algoritma yang di implementasikan setiap tools, seperti contoh pada tools Hardwipe dengan metode *Zero Overwrite* yang memberikan hasil bahwa 100% persen tidak data dapat di recover. Dengan pengujian ini dapat membantu penyidik jika melihat pada komputer ternyata ada yang menggunakan tools Hardwipe yang dengan metode Zero Overwrite menjalankan data wiping, harapan saya dengan penyidik melihat hasil dari penelitian ini, dan penyidik nanti nya dapat mengukur suatu data dapat *direcover* jika data wiping nya menggunakan tools selain *Hardwipe*. Itulah kontribusi dari penelitan ini sepanjang pengemasan dan rekomendasi nya baik. dengan melakukan metode *software testing* yang valid dan jelas, yang pada penelitian ini menggunakan metodologi dari *Performance Testing* menurut Thomas Hamilton sebagai expert software testing, sehingga nanti nya hasil test nya sesuai dan hasil nya dapat di pertanggung jawabkan. Dan hasil dari tugas akhir ini dapat membantu penyidik untuk mengukur sejauh mana dampak data wiping ini dalam penyidik melakukan data *recovery*.

Table 5. Recuva

Metode	Tools	File	Keteran an
Random Data Overwrite	Eraser	3	Teridentifikasi
U.s. DoD 5220.22-M (E)	Eraser	1	Teridentifikasi
U.S. DoD 5220.22-M (ECE)	Eraser	3	Teridentifikasi
Bruce Schneier'sAl orithm	Eraser	2	Teridentifikasi
Zero Overwrite	Disk Wipe	117	Tidak Teridentifikasi
Random Data Overwrite	Disk Wipe	117	Tidak Teridentifikasi
U.s. DoD 5220.22-M (E)	Disk Wipe	117	Tidak Teridentifikasi
U.s. DoD 5220.22-M (ECE)	Disk Wipe	117	Tidak Teridentifikasi
Zero Overwrite	AOMEI Partition Assistant Professional	0	Tidak Teridentifikasi
Random Data Overwrite	AOMEI Partition Assistant Professional	0	Tidak Teridentifikasi
U.s. DoD 5220.22-M (E)	AOMEI Partition Assistant Professional	0	Tidak Teridentifikasi
U.S. DoD 5220.22-M (ECE)	AOMEI Partition Assistant Professional	0	Tidak Teridentifikasi
Zero Overwrite	AOMEI Backupper	0	Tidak Teridentifikasi
Random Data Overwrite	AOMEI Backupper	0	Tidak Teridentifikasi
U.S. DoD 5220.22-M (E)	AOMEI Backupper	0	Tidak Teridentifikasi
U.S. DoD 5220.22-M (ECE)	AOMEI Backupper	0	Tidak Teridentifikasi
Zero Overwrite	Hardwipe	0	Tidak Teridentifikasi
Random Data Overwrite	Hardwipe	0	Tidak Teridentifikasi
U.s. DoD 5220.22-M (E)	Hardwipe	0	Tidak Teridentifikasi
Bruce Schneier's Algorithm	Hardwipe	0	Tidak Teridentifikasi
Zero Overwrite	Hard Drive Eraser	117	Tidak Teridentifikasi
U.s. DoD 5220.22-M (E)	Hard Drive Eraser	117	Tidak Teridentifikasi

Table 6. Metode Wiping Data Zero Overwrite pada setiap Tools

Tools	Running Time	Memory Usage	CPU Usage	Recovery (MiniTool Power Data Recovery 11.4	Recovery (Easeus Data Recovery Wizard)	Recovery (Recuva)
Eraser	-	-	-	-	-	-
Disk Wipe	3:16:10	2.8 MB	1.40%	117	117	117
AOMEI Partition Assistant professional	2:12:29	2.8 MB	0.20%	0	0	0
AOMEI Backupper	1:35:41	27.6 MB	0.3%	0	0	0
Hardwipe	1:34:49	16.7 MB	2.80%	0	0	0
Hard Drive Eraser	1:44:37	4.4 MB	18.90%	117	117	117

Table 7. Metode Wiping Data Random Data Overwrite pada setiap Tools

Tools	Running Time	Memory Usage	CPU Usage	Recovery (MiniTool Power Data Recovery 11.4	Recovery (Easeus Data Recovery Wizard)	Recovery (Recuva)
Eraser	1:35:36	38.7 MB	1.5%	86	4	3
Disk Wipe	3:16:51	2.8 MB	1.8%	117	117	117
AOMEI Partition Assistant professional	2:12:29	10.5 MB	0.1%	0	0	0
AOMEI Backupper	2:12:51	11.6 MB	0.2%	0	0	0
Hardwipe	1:35:10	16.7 MB	2.4%	80	1	0
Hard Drive Eraser	-	-	-	-	-	-

Table 8. Metode Wiping Data U.S. DoD 5220.22-M (E) pada setiap Tools

Tools	Running Time	Memory Usage	CPU Usage	Recovery (MiniTool Power Data Recovery 11.4	Recovery (Easeus Data Recovery Wizard)	Recovery (Recuva)
Eraser	4:51:42	29.2 MB	3.20%	81	3	1
Disk Wipe	3:18:51	2.8 MB	2.10%	117	117	117
AOMEI Partition Assistant professional	6:37:27	5.8 MB	0.20%	0	0	0
AOMEI Backupper	6:56:49	27.5 MB	0.30%	0	0	0
Hardwipe	4:14:30	16.7 MB	3.20%	74	0	0
Hard Drive Eraser	4:14:30	16.7 MB	3.20%	117	117	117

Table 9. Metode Wiping Data U.S. DoD 5220.22-M (ECE) pada setiap Tools

Tools	Running Time	Memory Usage	CPU Usage	Recovery (MiniTool Power Data Recovery 11.4	Recovery (Easeus Data Recovery Wizard)	Recovery (Recuva)
Eraser	11:21:33	27.3 MB	3.3%	66	4	3
Disk Wipe	3:23:35	2.9 MB	3.0%	117	117	117
AOMEI Partition Assistant professional	15:27:24	10.8 MB	0,3%	0	0	0
AOMEI Backupper	15:20:23	27.6 MB	0.4%	0	0	0
Hardwipe	-	-	-	-	-	-
Hard Drive Eraser	-	-	-	-	-	-

Kesimpulan

Berdasarkan hasil pengujian yang dilakukan pada tools wiping data dalam melakukan berbagai metode pada wiping data, dari 6 tools yang di uji terhadap pengujian wiping data yaitu:

1. *Eraser*
2. *Disk Wipe*
3. AOMEI *Partition Assistant Professional*
4. AOMEI *Backupper*
5. *Hardwipe*
6. *Hard Drive Eraser*

Dapat berikan 3 tingkat terhadap keberhasilan *tools* melakukan *wiping data*. Pada tingkat yang pertama adalah *tools* yang benar-benar berhasil melakukan *wiping data* karena tidak ada file yang di deteksi atau *recovery* setelah melakukan *wiping data* yaitu, AOMEI *Partition Assistant Professional* dan AOMEI *Backupper*, tingkat kedua yang sudah berhasil namun masih terdapat sedikit kesalahan karena file yang masih dapat di deteksi atau *recovery* setelah melakukan *wiping data* yaitu *Eraser* dan *Hardwipe*, tingkat ketiga yang belum bisa sepenuhnya berhasil melakukan *wiping data* serta menerapkan metode *wiping data* dengan baik karena hampir seluruh file yang dapat di deteksi atau *recovery* setelah melakukan *wiping data* pada *tools* nya yaitu *Disk Wipe* dan *Hard Drive Eraser*.

Saran yang dapat diberikan terkait *tools* kepada para pembuat *tools* yang dilakukan pengujian pada penelitian kali ini, sebaiknya melakukan perbaikan metode *wiping data*, sementara pada *user* yang menggunakan *tools* anti forensik dapat lebih cermat dalam memilih *tools* karena tidak semua *tools* berjalan sesuai dengan yang dijanjikan. Dan terakhir saran untuk penelitian selanjutnya untuk pengujian metode *wiping data* dapat menambahkan metode lain seperti metode guttman, serta dapat menguji pada media penyimpanan yang beragam, seperti pada media penyimpanan flashdisk, atau pun media penyimpanan *smartphone*. dan dapat menambahkan pengujian *reverse engineering* pada

Table 10. Metode Wiping Data Bruce Schneier's Algorithm pada setiap Tools

Tools	Running Time	Memory Usage	CPU Usage	Recovery (MiniTool Power Data Recovery 11.4	Recovery (Easeus Data Recovery Wizard)	Recovery (Recuva)
Eraser	11:12:57	28.0 MB	2.4%	93	2	2
Disk Wipe	-	-	-	-	-	-
AOMEI Partition Assistant professional	-	-	-	-	-	-
AOMEI Backupper	-	-	-	-	-	-
Hardwipe	11:08:42	16.7 MB	3.6%	88	5	0
Hard Drive Eraser	-	-	-	-	-	-

tools untuk melihat algoritma seperti apa yang dilakukan pada setiap metode *wiping data*.

Daftar Pustaka

1. Agustya MPM, Chayani NDW. Analisis Metode Wiping Air Force System Security Instruction 5020 Dan Department of Defense 5220.22 M Sebagai Usaha Anti Forensik Pada Media Penyimpanan Flash Disk Dan Hard Disk Drive. 2021.
2. Ahn NY, Lee DH. Schemes for privacy data destruction in a NAND flash memory. IEEE Access. 2019;7:181305–181313. Available from: https://doi.org/10.1109/access.2019.2958628.
3. AlHarbi R, AlZahrani A, Bhat WA. Forensic analysis of anti-forensic file-wiping tools on Windows. Journal of Forensic Sciences. 2021;67(2):562–587. Available from: https://doi.org/10.1111/1556-4029.14907.
4. Aomei Partition assistant professional;. Accessed: June 17, 2022. Available from: https://www.diskpart.com/partition-manager-proedition.html.
5. Best backup, recovery, clone software for any devices and everyone: Aomei Data Protection;. Accessed: May 17, 2022. Available from: https://www.ubackup.com/.
6. Destroys all data on your hard drive, once for all. free software. no spyware or adware.;. Accessed: May 17, 2022. Available from: https://www.harddriveeraser.org/.
7. Disk wipe - free software;. Accessed: June 17, 2022. Available from: https://www.diskwipe.org/.
8. Performance testing tutorial – types (example), Guru99;. Accessed: September 17, 2022. Available from: https://www.guru99.com/performance-testing.html.
9. Hardwipe;. Accessed: June 17, 2022. Available from: https://www.majorgeeks.com/files/details/hardwipe.html.
10. Hasa MF, Yudhana A, Fadlil A. Implementation of anti forensics on hard drives using the DOD 5220.22 m method and British HMG IS5 E. Jurnal RESTI (Rekayasa Sistem Dan Teknologi Informasi). 2020;4(4):736–744. Available from: https://doi.org/10.29207/resti.v4i4.2165.
11. Horsman G. Digital Tool Marks (dtms): A forensic analysis of file wiping software. Australian Journal of Forensic Sciences. 2019;53(1):96–111. Available from: https://doi.org/10.1080/00450618.2019.1640793.
12. Kessler GC. Anti-Forensics and the Digital Investigator.; 2007. Available from: https://doi.org/10.4225/75/57ad39ee7ff25.
13. Khalifa HR, Yulianto MFA ST, Jadied MEM ST. Implementasi Teknik Penghapusan Data Dengan Metode DoD 5220.22 M Pada Sistem Operasi Android. Implementasi Teknik Penghapusan Data Dengan Metode DoD 522022M Pada Sistem Operasi Android. 2016;3:897. Available from: https://doi.org/10.4225/75/57ad39ee7ff25.
14. Majed H, Noura HN, Chehab A. Overview of digital forensics and Anti-Forensics Techniques. In: 2020 8th International Symposium on Digital Forensics and Security (ISDFS); 2020. Available from: https://doi.org/10.1109/isdfs49300.2020.9116399.
15. Oh DB, Park KH, Kim HK. De-Wipimization: Detection of data wiping traces for investigating NTFS file system. Computers & Security. 2020;99:102034. Available from: https://doi.org/10.1016/j.cose.2020.102034.
16. Olvecky M, Gabriska D. Wiping techniques and Anti-Forensics Methods. In: 2018 IEEE 16th International Symposium on Intelligent Systems and Informatics (SISY); 2018. Available from: https://doi.org/10.1109/sisy.2018.8524756.
17. Sarjimin, Herman, Yudhana A. Perbandingan Tool Forensik Pada Mozilla firefox private mode menggunakan metode NIST. Jurnal Algoritma. 2021;18(1):283–291. Available from: https://doi.org/10.33364/algoritma/v.18-1.873.
18. Setiawan NA, Ferdiansyah MD ST, Kurniawan MI ST. Analisis Perbandingan Penghapusan Data Digital Dengan Menerapkan Metode DoD 5220.22M Dan Metode Gutmann. 2017. Available from: http://repository.unpas.ac.id/31437/.
19. Wire, cable & tube cutters, strippers, twisters, and more...;. Accessed: June 16, 2022. Available from: https://www.eraser.com/.
20. Wu CH, Lin PL, Hu YH, Du MY. A data sanitization method for mobile devices with NAND flash memory. In: Proceedings of the Conference on Research in Adaptive and Convergent Systems; 2019. Available from: https://doi.org/10.1145/3338840.3355639.