PERANCANGAN APLIKASI CLONING-HASHING UNTUK PEMELIHARAAN BUKTI DIGITAL

Muhammad Nur Faiz[1*], Abdul Rohman Supriyono[2]
[1,2]Rekayasa Keamanan Siber, Politeknik Negeri Cilacap, Indonesia

*Email: *faiz@pnc.ac.id*

ABSTRAK

Perkembangan kejahatan dunia siber terus meningkat akhir ini, seiring dengan digitalisasi di Indonesia. Kejahatan yang melibatkan teknologi semakin bervariasi dan terstruktur, maka dibutuhkan penanganan kejahatan siber dengan baik. Kejahatan siber memiliki dua jenis barang bukti yaitu bukti fisik dan bukti digital. Penanganan bukti digital saat ini masih belum sepenuhnya bagus karena bukti digital ini rawan dimanipulasi sehingga membutuhkan teknik pengamanannya. Salah satu penanganan bukti digital mengacu pada Metodologi forensik digital NIST 80086 yang dimulai dari tahap pengumpulan, pengujian, analisis, dan tahap pelaporan. Pada tahapan pengujian, unsur utamanya adalah bukti digital, bukti digital ini harus digandakan dan dicek integritas file atau lebih dikenal dengan cloning dan hashing. Bukti digital berperan penting dalam mengungkapkan kejahatan pada persidangan. Permasalahan saat ini adalah tools dalam mengelola bukti digital yang digunakan masih beragam dan belum diatur oleh Pemerintah sehingga terlalu banyak tools yang digunakan oleh penyidik dalam cloning dan hashing bukti digital. Tools tersebut dapat merusak dan berdampak pada keabsahan bukti digital. Pada penelitian ini akan merancang aplikasi yang diharapkan dapat membantu penyidik dalam menggandakan (cloning) barang bukti digital kemudian dicek integritas file (hashing) sehingga nantinya dapat mempermudah penyidik untuk pemeliharaan bukti digital.

Kata kunci : Aplikasi, Cloning-Hashing, Bukti Digital

ABSTRACT

The development of cybercrime continues to increase lately, along with digitalization in Indonesia. Crimes involving technology are increasingly varied and structured, so it is necessary to handle cybercrimes properly. Cybercrime has two types of evidence, namely physical evidence, and digital evidence. The current handling of digital evidence is still not entirely good because this digital evidence is prone to manipulation, so it requires security techniques. One of the handlings of digital evidence refers to the NIST 80086 digital forensic methodology which starts from the collection, testing, analysis, and reporting stages. At the testing stage, the main element is digital evidence, this digital evidence must be duplicated and checked for file integrity or better known as cloning and hashing. Digital evidence plays an important role in revealing crimes at trial. The current problem is that the tools in managing digital evidence used are still diverse and have not been regulated by the Government so too many tools are used by investigators in cloning and hashing digital evidence. These tools can damage and impact the validity of digital evidence. In this research, we will design an application that is expected to assist investigators in cloning digital evidence and then checking file integrity (hashing) so that later it can make it easier for investigators to maintain digital evidence.

Keywords : Application, Cloning-Hashing, Evidence

PENDAHULUAN

Perkembangan kejahatan dunia digital yang dibuktikan dengan semakin maraknya kasus yang menyangkut UU ITE. Menurut (Patroli Siber, n.d.) kasus yang terjadi sepanjang Januari 2020 hingga Februari 2022, jumlah laporan masyarakat mengenai pengancama 6500, jumlah penghinaan/pencemaran 5619, pemerasan 3039, hoax 669 dan lainnya. Tren kejahatan dunia digital juga masih menyentuh angka 200-an kasus pada tahun 2022.

Hal ini jelas memberikan masalah untuk penyidik karena jumlahnya, dokumentasi dan kompleksitas terhadap bukti digital. Bukti digital harus dikelola dengan baik karena akan mementukan integritas saat bukti digital dipertanyakan pada persidangan (Bonomi et al., 2018). Bukti digital sendiri memiliki risiko tinggi untuk digandakan, disebarluaskan, dihapus dan dimanipulasi oleh siapa saja (A. S. Putra & Prayudi, 2021). Semua file bukti digital yang akan dianalisis seharusnya disimpan dalam suatu tempat dengan prosedur penyimpanan tertentu (A. I. Putra et al., 2018) (Sidiq & Faiz, 2019). Seorang penyidik harus paham jenis- jenis barang bukti, sehingga ketika datang ke tempat kejadian perkara (TKP) yang berhubungan dengan kasus kejahatan dunia digital, penyidik dapat mengenali keberadaan barang bukti untuk kemudian diperiksa dan dianalisa lebih lanjut (Dirman et al., 2021). Supaya barang bukti dapat digunakan di dalam proses penegakan hukum, maka barang bukti tersebut harus terjaga dan sama persis dengan ketika pada saat pertama kali ditemukan. Dalam dunia forensik digital, salah satu pembuktian secara ilmiah adalah dengan tahap dokumentasi bukti digital dan bukti fisik (Nur Faiz et al., 2018). Menurut (Prayudi & SN, 2015) juga mengungkapkan bahwa agar bukti digital dan bukti fisik dapat diterima di pengadilan, Chain of Custody (dokumentasi barang bukti) dan aspek informasi dari Chain of Custody menjadi domain penting yang harus diperhatikan. Menurut (Harbawi & Varol, 2017) terdapat empat prinsip dalam penanganan bukti digital. Berikut adalah empat prinsip penanganan bukti digital menurut ACPO.

1. Seorang penyidik tidak diperbolehkan untuk mengubah data karena hal ini akan dipertanggung jawabkan di pengadilan.
2. Pada situasi tertentu dan jika memang diharuskan, seseorang diperbolehkan untuk mengakses data yang asli, namun orang tersebut harus kompeten dan ia harus dapat menjelaskan tentang relevansi terhadap barang bukti serta implikasi terhadap kegiatan yang dilakukan terhadap barang bukti tersebut.
3. Proses pencatatan dan audit yang berisi semua proses dalam penanganan bukti digital harus dibuat dan ketika pihak ketiga memeriksa catatan dan audit tersebut, hasilnya harus sama dengan yang dimiliki oleh pihak penyidik.

4. Orang yang bertanggung jawab dalam investigasi ini harus memastikan bahwa hukum dan semua prinsip ini dipatuhi oleh orang-orang yang terlibat.

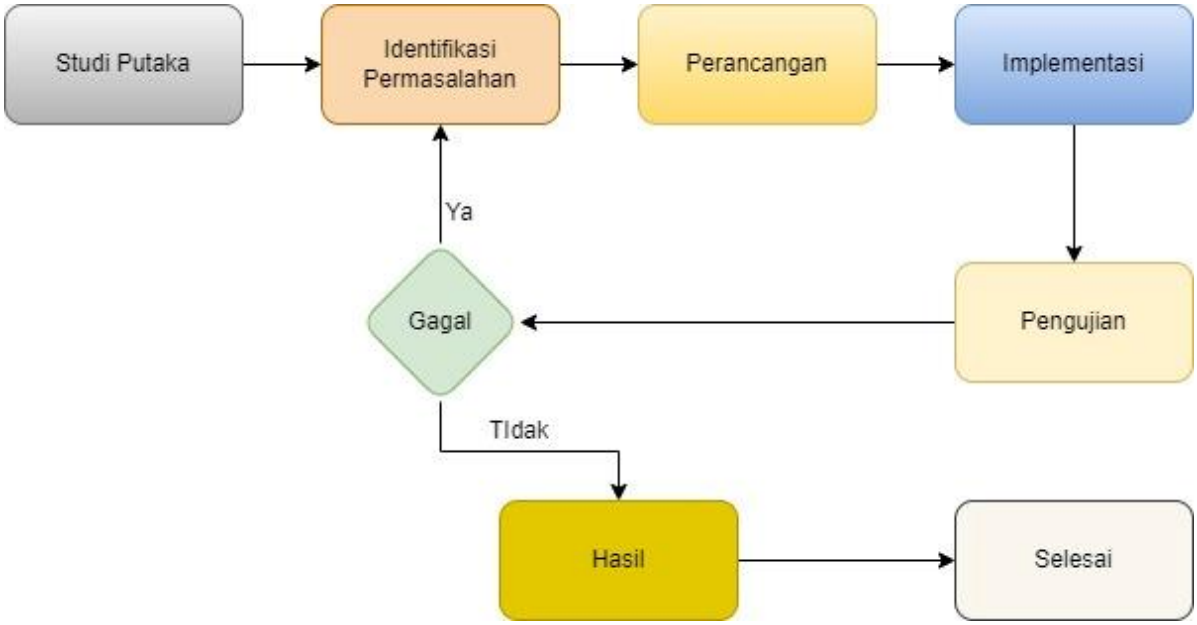
Beberapa penelitian mengenai penanganan bukti digital, penelitian (Efendi et al., 2020) mengimplementasikan konsep data inventory yaitu konsep manajemen barang bukti fisik melalui kontrol barang bukti fisik dan segala aktivitas yang berkaitan dengan bukti fisik dapat terjaga serta dapat terdokumentasi dengan baik. Penelitian ini berfokus pada penyimpanan data yang masih menggunakan DBMS sehingga data bukti fisik yang tersimpan masih terlihat. Pengembangan selanjutnya difokuskan terhadap keamanan data yang tersimpan baik menggunakan metode enkripsi maupun metode lainnya. Diperlukan satu sistem terintegrasi antara sistem penyimpanan bukti fisik dengan bukti digital. Penelitan selanjutnya mengenai bukti digital yaitu penelitian (A. S. Putra & Prayudi, 2021) penerapan multi smart contract menjelaskan bahwa bukti digital memiliki karakteristik berbeda-beda dan detail informasi yang berbeda-beda antara satu jenis bukti digital gambar, audio, video, dan dokumen atau jenis bukti digital lainnya. Penambahan informasi yang lebih detail pada bukti digital dengan Multi Smart Contract maka dapat meningkatkan integritas dan akurasi bukti digital serta dapat membantu mempermudah dan mempercepat penyidik atau ahli menentukan tindakan dalam memeriksa bukti digital yang dikelola. Penelitian ini membangun middleware dengan cara menghubungkan naive chain ke multi smart contract mengunakan API dalam bentuk url yang diakses menggunakan fungsi curl pada multi smart contract. Penelitian selanjutnya (Ali et al., 2019), mengenai repositori fleksibilitas berdasarkan SAN (Storage Area Network) dan teknologi berbasis web digunakan sebagai arsitektur penyimpanan terpusat berbasis jaringan. Sistem ini diharapkan dapat membantu antar penegak hukum dalam hal pengelolaan lacak balak untuk barang bukti digital. Penelitian selanjutnya mengenai bukti digital, yaitu penelitian (Pakarti et al., 2021) yang hasilnya mengembangkan sistem pengelolaan bukti digital yang diusulkan dapat meningkatkan aksesibilitas bukti digital yang sangat berpengaruh dalam proses investigasi. Mulai dari tahap penyerahan bukti digital, unduh bukti digital penyimpanan hingga proses unduh formulir chain of custody dilakukan secara daring tanpa harus datang ke laboratorium forensika digital sehingga proses investigasi berjalan lebih cepat dan meminimalisir risiko kerusakan pada bukti digital dan keselamatan petugas. Penelitian ini juga berfokus penganggulangan covid-19 karena dapat diakses secara daring oleh petugas. Meskipun banyak penelitian terkait penanganan bukti digital, namun saat ini belum ada penelitian khusus mengenai pengembangan tools untuk pemeliharaan bukti digital untuk proses

ISSN: 2963-2277

menggandakan (cloning) dan hashing. Berdasarkan alasan tersebut maka penelitian ini dilaksanakan dengan tujuan untuk mengembangkan tools untuk pemeliharaan bukti digital khususnya proses menggandakan (cloning) dan hashing.

METODE PENELITIAN

Pada gambar di bawah dapat dilihat alur penelitian yang dimulai dengan studi pustaka pada penelitian sebelumnya kemudian identifikasi permasalahan. Tahap selanjutnya adalah merancang aplikasi/tools. Kemudian dilakukan tahap implementasi terhadap rancangan yang sudah dibuat. Selanjutnya dilakukan proses pengujian yang dilakukan benar-benar valid. Pengujian dilakukan dengan membandingkan dengan sistem yang sudah ada.



Gambar 1. Kerangka Kerja Penelitian

Langkah yang akan dilaksanakan dalam penelitian ini mulai dari awal sampai akhir adalah sebagai berikut :

A. Studi Pustaka

Pada tahapan ini mempersiapkan alat yang akan digunakan dalam penelitian berdasarkan sintesa dari hasil penelusuran pustaka yang telah dilaksanakan, terutama dari penelitian terdahulu.

B. Identifikasi Permasalahan

Peneliti mengidentifikasi permasalahan sesuai dengan hasil studi pustaka dan mencari aplikasi serupa pada internet.

C. Perancangan sistem

Peneliti merancang sistem yang akan dibuat. Rancangan ini diperlukan agar mempermudah dalam pembangunan sistem. Hal ini juga dapat mempercantik tampilan sistem untuk mempermudah pengguna dalam mengoperasikan sistem tersebut.

D. Implementasi Sistem

Implementasi sistem merupakan tahap meletakkan sistem yang diusulkan atau dikembangkan supaya nantinya sistem tersebut siap untuk dioperasikan sesuai dengan yang diterapkan.

E. Pengujian Sistem

Peneliti melakukan pengujian dilakukan dengan membandingkan hasil keluaran sistem ini dengan sistem yang sudah ada sebelumnya sebagai acuan supaya sistem tetap memiliki fungsi dan peran yang sesuai dengan kebutuhan. Peneliti juga akan menguji penggunaan CPU dan nilai hashing sistem tersebut dengan sistem yang sudah ada sebelumnya.

HASIL DAN PEMBAHASAN

Hasil dan pembahasan pada penelitian ini adalah melakukan perancangan aplikasi untuk mempermudah dalam proses implementasi sistem.

A. Identifikasi Permasalahan

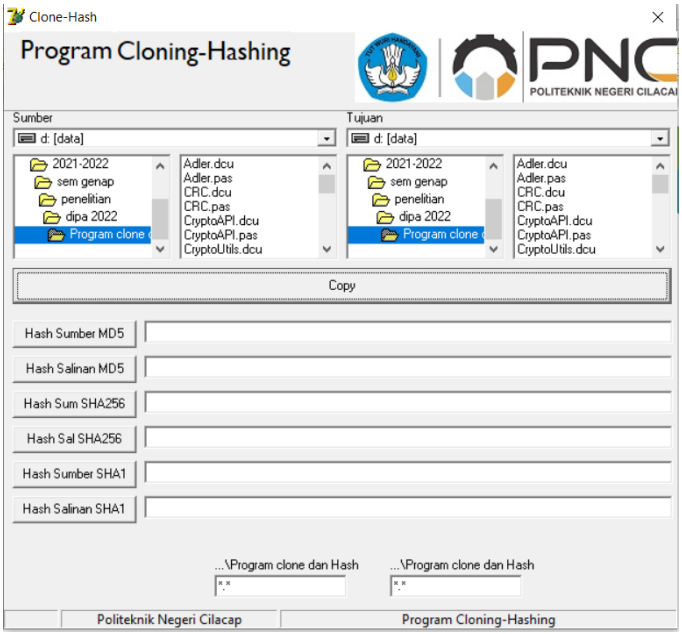
Pada tahapan ini mengumpulkan segala kebutuhan termasuk tools pembanding dan penguji dari tools sebelumnya.

B. Perancangan Sistem

Perancangan antarmuka atau solusi desain dibuat untuk menggambarkan bentuk aplikasi Cloning dan hashing yang akan dirancang. Pada tahap selanjutnya membentuk perancangan antarmuka diterjemahkan ke dalam bahasa pemograman yang nantinya akan dijadikan sebuah aplikasi

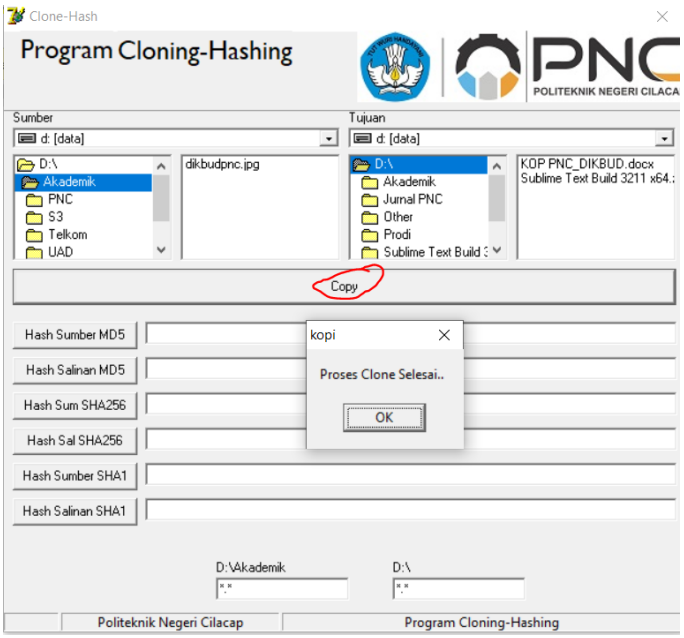
C. Implementasi Sistem

ISSN: 2963-2277



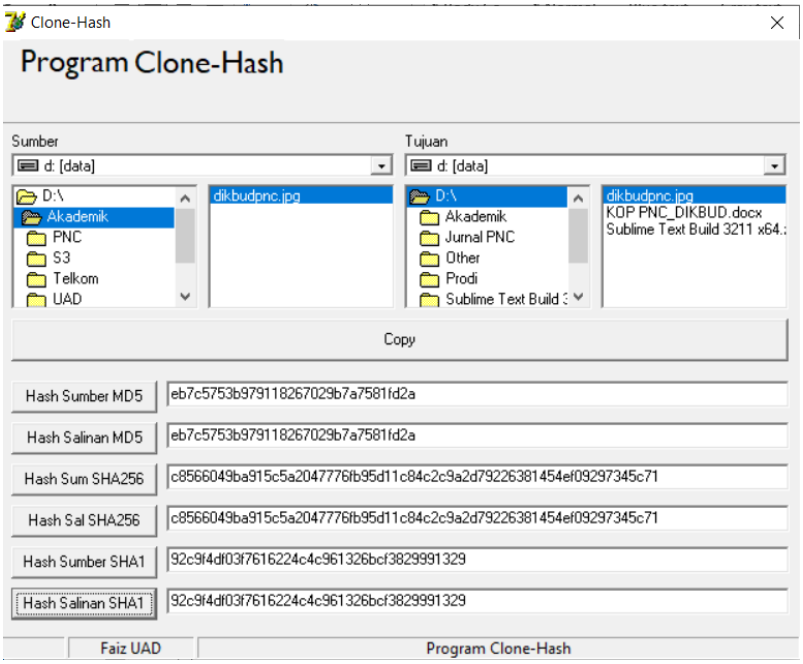
Gambar 2. Rancangan Beranda Aplikasi Cloning-Hashing

Rancangan Rancangan Beranda Aplikasi Cloning-Hashing ditunjukkan pada Gambar 2. Pada Beranda terdapat Tab sumber yang berisi daftar file yang akan digandakan, Tab Tujuan untuk memilih letak penyimpanan tujuan file yang telah digandakan. Pada Beranda juga terdapat seluruh menu termasuk button copy untuk memproses cloning file dan button hash sumber dan tujuan, dengan lengkap .



Gambar 3. Rancangan proses Clone

Pada Gambar 3 merupakan gambaran proses penggandaan file dan jika berhasil maka muncul notifikasi proses clone selesai. Tahap selanjutnya adalah cek integritas file pada file sumber dan file tujuan.



Gambar 4. Rancangan Hasil Hashing

Pada Gambar 4 merupakan gambaran proses hashing untuk cek integritas file sumber dan file tujuan, karena pada proses digital forensik integritas merupakan syarat untuk keabsahan bukti digital. Terdapat beberapa hasil hash dari MD5, SHA256 dan SHA1. Hal ini sangat penting karena semua file akan dicek nilai hashing.

KESIMPULAN

Berdasarkan hasil dari perancangan aplikasi cloning hashing ini dapat disimpulkan Perancangan Aplikasi cloning hashinh ini dilakukan untuk merancang sebuah sistem, baik dari awal maupun untuk rencana pengembangan kedepan dari sebuah sistem informasi dengan tepat dan cepat. Tujuan merancang aplikasi ini adalah nantinya aplikasi dapat digunakan untuk membantu penyidik dalam menggandakan (cloning) barang bukti digital kemudian dicek integritas file (hashing) sehingga penyidik dapat mengamankan bukti digital.

UCAPAN TERIMAKASIH

Penelitian ini dapat terlaksana dengan bantuan Dana dari Daftar Isian Pelaksanaan Anggaran (DIPA) Politeknik Negeri Cilacap.

DAFTAR PUSTAKA

Ali, M., Prayudi, Y., & Sugiantoro, B. (2019). Storage Area Network Architecture to support the Flexibility of Digital Evidence Storage. *International Journal of Computer Applications*, *182*(41), 30–35. https://doi.org/10.5120/ijca2019918496

Bonomi, S., Casini, M., & Ciccotelli, C. (2018). *B-CoC: A Blockchain-based Chain of Custody for Evidences Management in Digital Forensics*. https://doi.org/10.4230/OASIcs.Tokenomics.2019.12

Dirman, D., Prayudi, Y., & Ramadhani, E. (2021). Model Alur Kerja Penanganan Bukti Digital Untuk Data Multimedia. *JATISI (Jurnal Teknik Informatika Dan Sistem Informasi)*, *8*(3), 1214–1225. https://doi.org/10.35957/jatisi.v8i3.987

Efendi, T. F., Rahmadi, R., & Prayudi, Y. (2020). Rancang Bangun Sistem Untuk Manajemen Barang Bukti Fisik dan Chain of Custody (CoC) pada Penyimpananan Laboratorium Forensika Digital. *Jurnal Teknologi Dan Manajemen Informatika*, *6*(2), 53–63. https://doi.org/10.26905/jtmi.v6i2.4177

Harbawi, M., & Varol, A. (2017). An improved digital evidence acquisition model for the Internet of Things forensic I: A theoretical framework. *2017 5th International Symposium on Digital Forensic and Security (ISDFS)*, 1–6. https://doi.org/10.1109/ISDFS.2017.7916508

Nur Faiz, M., Adi Prabowo, W., & Fajar Sidiq, M. (2018). Studi Komparasi Investigasi Digital Forensik pada Tindak Kriminal. *Journal of Informatics, Information System, Software Engineering and Applications (INISTA)*, *1*(1), 63–70. https://doi.org/10.20895/INISTA.V1I1

Pakarti, M. B., Fudholi, D. H., & Prayudi, Y. (2021). Manajemen Pengelolaan Bukti Digital Untuk Meningkatkan Aksesibilitas Pada Masa Pandemi Covid-19. *Jurnal Ilmiah SINUS*, *19*(1), 27. https://doi.org/10.30646/sinus.v19i1.502

Patroli Siber. (n.d.). *Jumlah Laporan Polisi yang dibuat masyarakat*. Retrieved February 2, 2022, from https://patrolisiber.id/statistic

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

Putra, A. I., Umar, R., & Fadlil, A. (2018). Analisis Forensik Deteksi Keaslian Metadata Video Menggunakan Exiftool. *Seminar Nasional Informatika 2018 (SemnasIF 2018)*, *2018*(November), 21–25.

Putra, A. S., & Prayudi, Y. (2021). Implementasi Multi Smart Contract pada Bukti Digital dan

Chain of Custody dalam Meningkatkan Keamanan dan Integritas Bukti Digital. *JUSTINDO (Jurnal Sistem Dan Teknologi Informasi Indonesia)*, *6*(2), 98–108. https://doi.org/10.32528/justindo.v6i2.3945

Sidiq, M. F., & Faiz, M. N. (2019). Review Tools Web Browser Forensics untuk Mendukung Pencarian Bukti Digital. *Jurnal Edukasi Dan Penelitian Informatika (JEPIN)*, *5*(1), 67. https://doi.org/10.26418/jp.v5i1.31430

ISSN: 2963-2277