Analisis Forensik Database Menggunakan Metode Forensik Statis

Imam Riadi[a], Rusdy Umar[b] , Dora Bernadisman[c]

[a] Program Studi Sistem Informasi, Universitas Ahmad Dahlan Yogyakarta
[b,c] Program Studi Teknik Informatika, Universitas Ahmad Dahlan Yogyakarta

Naskah Diterima : 12 November 2018; Diterima Publikasi : 29 April 2019

DOI : DOI : 10.21456/vol9iss1pp9-17

Abstract

SIMDA (Regional Management Information System) is a system created by the BPKP (Financial and Development Supervisory Agency) to assist local governments in implementing regional financial management so that it complies with applicable, efficient, effective, transparent, accountable and auditable regulations. Management data is stored in the SIMDA database on a server connected to a computer network, it is possible that the database is always infiltrated and indicated by data manipulation by hackers. The purpose of this study is to monitor database activity and detect data manipulation done by hackers, then forensic processes are carried out using static forensic methods with stages, namely data collection, data checking, data analysis, and reporting so as to provide evidence and instructions to do analysis on the SIMDA Planning database. The results obtained using static forensic methods show that there has been manipulation or change in the budget ceiling of the activity that exceeds the program budget ceiling (mark-up in budget planning) carried out by hackers who enter through the SIMDA database. Output from forensic processes can prove manipulation data that is carried out by hackers can be detected using SQL Profiler and SQL Log Analyzer tools so that output can be used as digital evidence to assist law enforcement in revealing cybercrime crime cases and can be accounted for in court proceedings.

Keywords **:** Forensik; Database; SIMDA; Manipulasi, SQL Injection

Abstrak

SIMDA (Sistem Informasi Manajemen Daerah) merupakan sistem yang dibuat oleh BPKP (Badan Pengawasan Keuangan dan Pembangunan) untuk membantu pemerintah daerah dalam melaksanakan pengelolaan keuangan daerah sehingga sesuai dengan peraturan yang berlaku, efisien, efektif, transparan, akuntabel, dan auditable. Data pengelolaan tersimpan pada *database* SIMDA dalam server yang terhubung dengan jaringan komputer, ada kemungkinan *database* selalu disusupi dan terindikasi adanya manipulasi data oleh *hacker* (peretas). Tujuan penelitian ini untuk memonitoring aktivitas *database* dan mendeteksi adanya perbuatan manipulasi data yang telah dilakukan oleh peretas, kemudian dilakukan proses forensik yang menggunakan metode forensik statis dengan tahapan yaitu pengumpulan data, pemeriksaan data, analisa data, dan pelaporan sehingga dapat memberikan bukti serta petunjuk untuk melakukan analisis pada *database* SIMDA Perencanaan. Hasil penelitian yang didapat menggunakan metode forensik statis menunjukan bahwa telah terjadinya manipulasi atau perubahan data pagu anggaran kegiatan yang melebihi pagu anggaran program (mark-up dalam perencanaan anggaran) yang dilakukan oleh peretas yang masuk melalui *database* SIMDA, Output dari proses forensik dapat membuktikan terjadinya manipulasi data yang dilakukan oleh peretas yang dapat terdeteksi menggunakan tools SQL Profiler dan SQL Log Analyzer sehingga output dapat dijadikan barang bukti digital untuk membantu penegak hukum dalam mengungkapkan kasus kejahatan cybercrime dan dapat dipertanggungjawabkan pada proses hukum dipengadilan.

Kata kunci**:** Forensik; Database; SIMDA; Manipulasi, SQL Injection

1. Pendahuluan

Sistem informasi pada pemerintahan daerah pada saat ini perlu menggunakan teknologi informasi seperti personal komputer, server dan infrastruktur jaringan untuk mendukung jalannya sistem informasi yang berupa software atau sistem yang dimanfaatkan oleh pemerintah daerah di setiap bidang, baik bidang keuangan daerah, bidang perencanaan daerah, bidang asset daerah maupun bidang lainnya yang berada di seluruh dinas-dinas di pemerintah daerah. Pemanfaatan teknologi dan sistem informasi di pemerintah daerah, sangatlah dibutuhkan untuk mempercepat penyelesaian tugas – tugas yang bersifat manual, tentu dengan adanya pemanfataan Teknologi Informasi pada pemerintah daerah dapat menyelesaikan tugasnya dengan cepat dan mengirimkan data ke pemerintah pusat dengan cepat.

*)Penulis korespondensi: dora1689048030@webmail.uad.ac.id

Pemanfaatan sistem informasi merupakan suatu terobosan yang harus dilakukan oleh pemerintah daerah dengan mengembangkan dan menggunakan aplikasi berbasis database dan didukung dengan jaringan komputer yang memadai diseluruh OPD (Organisasi Perangkat Daerah) yang dapat membantu pemerintah daerah dalam menyajikan laporan – laporan yang sesuai dengan peraturan yang berlaku, cepat, efisien, efektif, transparan, akuntabel dan auditabel yang dibutuhkan pihak terkait seperti bupati, wakil bupati, kepala dinas, pihak eksekutif dan pihak legislatif di pemerintah daerah.

Aplikasi berbasis database yang dikembangkan oleh BPKP (Badan Pengawasan Keuangan dan Pembangunan) untuk memberikan pendampingan terhadap pemerintah daerah dalam penerapan aplikasi berbasis database, aplikasi yang digunakan adalah SIMDA (Sistem Informasi Manajemen Daerah), yang terdiri dari SIMDA Keuangan, SIMDA Perencanaan, SIMDA Asset Daerah, SIMDA Pendapatan daerah. SIMDA merupakan sebuah sistem informasi untuk mengelola perencanaan anggaran daerah, pendapatan daerah, belanja daerah, realisasi keuangan daerah, penggajian daerah, pajak daerah yang terintegrasi dengan aplikasi yang berada di pemerintah pusat.

SIMDA merupakan aplikasi berbasis database yang telah diimplementasikan pada 391 pemerintah daerah di Indonesia (www.bpkp.go.id, 2018), pada proses implementasi Sistem Informasi Manajemen Daerah di pemerintah daerah ditemukan hal yang tidak diinginkan berupa adanya pihak yang mencari celah kerawanan yang dimiliki oleh aplikasi dan *database* SIMDA untuk sekedar mengetahui tingkat keamanan aplikasi maupun *database*, yang bertujuan untuk memanipulasi data atau mencuri data sehingga mengakibatkan data dapat berubah pada *database* SIMDA.

Database SIMDA merupakan tempat penyimpanan data pengelola keuangan daerah, yang diduga sering disusupi oleh peretas (hacker) untuk memanipulasi data maupun mencuri data, hal tersebut sangat merugikan pemerintah daerah maka berdasarkan kejadian tersebut *database* SIMDA perlu dilakukan pemeriksaan secara forensik untuk mengetahui atau mengungkap kejadian manipulasi data tersebut untuk mendapatkan barang bukti digital atau artefak data atau histori data yang telah dihapus atau dirubah.

Tujuan dari proses forensik *database* adalah untuk memonitoring aktivitas *database* SIMDA agar dapat mengetahui aktivitas apa saja dan siapa saja yang masuk ke dalam *database* SIMDA, kemudian untuk mendeteksi aktivitas manipulasi data yang dilakukan oleh peretas untuk mengetahui siapa yang merubah, apa saja yang dirubah, dimana data dirubah dan kapan dilakukannya.

2. Kerangka Teori

Forensik Digital adalah cabang ilmu forensik yang mencakup pemulihan dan investigasi yang ditemukan dalam perangkat digital untuk melakukan pemeriksaaan dan analisa terhadap barang bukti yang memiliki keterkaitannya dengan tindakan kejahatan (Kalbande dan Jain, 2013).

Digital forensik secara umum terbagi menjadi dua, yaitu *static forensics* dan *live forensics*. Penentuan penggunaan teknik ini ketika peneliti pertama kali melakukan penyitaan alat bukti digital. Penentuan teknik berdampak pada waktu dan tingkat kesulitan dalam menganalisis barang bukti yang diperoleh, teknik *live forensics* digunakan jika keadaan komputer sedang menyala, sedangkan *static forensics* digunakan jika keadaan komputer mati (Faiz *et al.*, 2017).

Faktor yang mendukung penggunaan *live forensics* antara lain :

a. Penyimpanan sementara berisi artefak, seperti gangguan menjalankan proses, dan koneksi jaringan yang aktif dengan sendirinya (Casey, 2010).
b. Artefak ini bisa dikendalikan dari jarak jauh maka perlu audit memori untuk mencari artefak tersebut (Casey, 2010).
c. Beberapa kode berbahaya hanya tinggal penyimpanan sementara saja. Hal ini berarti tidak ada file yang tertinggal pada penyimpanan permanen (Casey, 2010).
d. Beberapa kode berbahaya berisi data penting, seperti kata sandi, atau bahkan segmen kode, dalam bentuk terenkripsi yang hanya mendeteksi dipenyimpanan permanen (Casey, 2010).
e. Data *volatile* dapat dikumpulkan lebih cepat daripada data permanen secara penuh (Casey, 2010).
f. Data *volatile* memakan lebih sedikit ruang penyimpanan dari pada data permanen secara penuh (Casey, 2010).

Statics Forensics menggunakan prosedur dan pendekatan konvensional dimana barang bukti elektronik diolah ketika tidak terhubung dengan jaringan. Proses forensiknya sendiri berjalan pada sistem yang tidak dalam keadaan sistem sedang berjalan (Sulianta, 2014).

*Statics Forensic*s difokuskan pada pemeriksaan hasil umtuk menganalisis isi dari bukti digital, seperti file yang dihapus, history dari proses penginputan data transaksi, koneksi jaringan, *history* login user guna membuat ringkasan tentang kegiatan yang dilakukan pada bukti digital sewaktu digunakan. Dalam analisis statics, segala kebutuhan analisis forensik diperoleh dengan menggunakan perangkat keras seperti USB dan Hardisk.

Database forensik mengacu pada cabang ilmu forensik digital yang berkaitan dengan studi forensik database dan metadata terkait (Subli *et al.*, 2017).

Database forensik bertujuan untuk melihat siapa yang mengakses dan tindakan apa saja yang dilakukan pada database (Fowler, 2007). Pemeriksaan dari suatu basis data berhubungan dengan waktu yang berlaku pada waktu pembaharuan suatu baris data dalam tabel relasional yang sedang diperiksa dan diuji validitasnya untuk memverifikasi tindakan-tindakan pengguna basis data, pemeriksaan fukus pada identifikasi transaksi dalam basis data atau aplikasi yang menunjukan barang bukti.

Barang bukti merupakan bagian yang sangat penting dalam sebuh kasus kejahatan. dari barang bukti ini tim investigasi dan analis forensik dapat mengungkap kasus dengan kronologis yang lengkap (Al-Azhar, 2012).

3. Metode

Metode yang digunakan untuk melakukan analisis terhadap bukti digital atau tahapan dalam mendapatkan informasi dari bukti digital yaitu dengan metode forensik statis (Riadi *et al.*, 2014).

3.1. Pengumpulan (Collection)

Pada tahap ini melakukan kegiatan mengumpulkan data untuk mendukung proses penyelidikan dalam rangka pencarian bukti. Tahapan pengumpulan data merupakan tahap yang menentukan karena bukti yang didapat merupakan pendukung dalam proses penyidikan sebagai barang bukti digital untuk mengungkap kejahatan. Media digital yang dapat dijadikan barang bukti, misalnya komputer, server, laptop, flash disk, hardisk, log file, sms.

3.2. Pemeriksaaan (Examination)

Pada tahap ini, akan dilakukan pemeriksaaan pada database untuk mencari data yang telah di edit, pemeriksaaan dilakukan secara komprehensit dengan maksud untuk mendapatkan data digital yang sesuai dengan investigasi, ini artinya analisis forensik harus mendapatkan gambaran fakta kasus yang lengkap, sehingga apa yang dicari dan akhirnya ditemukan oleh analisis forensik adalah sama (*matching*) untuk pengembangan investigasinya, kemudian setelah mendapatkan gambaran fakta maka dilakukan proses pencarian untuk mendapatkan file atau data yang diinginkan.

3.3. Analisa (Analysis)

Melakukan Analisa terhadap database yang telah ditemukan untuk mendapatkan barang bukti untuk dijadikan barang bukti yang syah. Setelah mendapatkan data digital yang diinginkan dari proses pemeriksaan, maka data digital dianalisa secara detail dan komperhensif untuk dapat membuktikan kejahatan atau manipulasi data yang terjadi dalam *database.* Hasil analisis terhadap data digital menjadi barang bukti digital yang harus dapat dipertanggungjawabkan secara ilmiah dan di depan pengadilan.

3.4. Laporan (Reporting)

Setelah diperoleh barang bukti digital dari proses pemeriksaan data analisis sesuai dengan aturan investigasi maka hasil dari pemeriksaan dan analisa dituangkan dalam laporan penyelidikan yang telah diperkuat oleh bukti-bukti yang telah teruji, yang nantinya bisa di fungsikan untuk memperkuat bukti yang telah dilakukan. Pelaporan harus dilakukan dengan baik agar dapat dengan mudah dipahami oleh pihak-pihak yang punya otoritas. Pelaporan harus dapat menjelaskan dan harus mencantumkan hal yang perlu dicantumkan pada laporan forensik adalah tanggal dan waktu terjadinya pelanggaran, tanggal dan waktu saat investigasi, permasalahan yang terjadi, waktu analisa laporan, dan waktu ditemukan barang bukti.

Metodologi yang digunakan untuk penelitian ini adalah dengan menggunakan metode statis forensik. metode ini dapat dilakukan pada saat komputer tidak terkoneksi dengan jaringan. metode forensik statis pada database ini dilakukan proses backup database terlebih dulu dan database direstore di komputer lain (Cohen, 2013). hal ini dilakukan agar proses forensik database selanjutnya tidak mengganggu proses database yang sedang berjalan. Analisis forensik digital dengan metode statis lebih menekankan pendekatan tradisonal untuk pengimplementasiaanya. Metode ini paling banyak digunakan, telha ditetapkan prosedur dan memiliki definisi validitas hukum dari bukti-bukti yang dikumpulkan. Dalam analisis *statics forensics,* Salinan forensik yang telah disyahkan dan semua media barang bukti telah ditentukan agar tidak terkena potensi kontaminasi.

Gambar 1. Proses Analisis forensik

4. Hasil dan Pembahasan

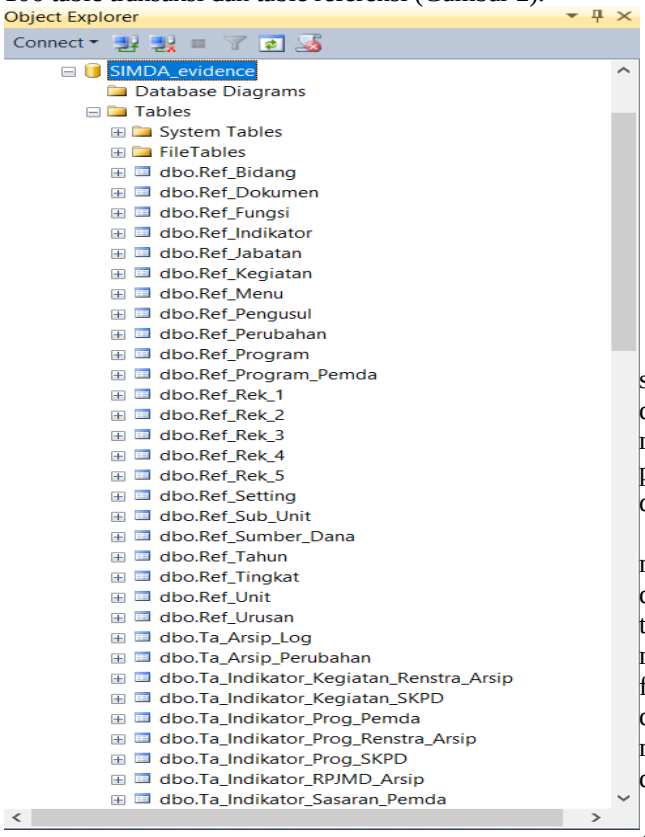
Pada pembahasan ini, *database* SIMDA perencanaan menggunakan software Microsoft SQL Server untuk di *restore* menjadi *database* untuk

membuktikan *database* SIMDA perencanaan, melalui metode *statics forensics* maka pemeriksaan dan analisa memberikan barang bukti digital dapat sehingga sudah aman dari penyusup yang memanipulasi data perencanaan keuangan daerah. pada latar belakang yang telah dijelaskan sebelumnya maka permasalahan yang paling mendasari adalah dapat melakukan proses forensik pada database dan mendapatkan barang bukti digital.

4.1. Tahap Pengumpulan data

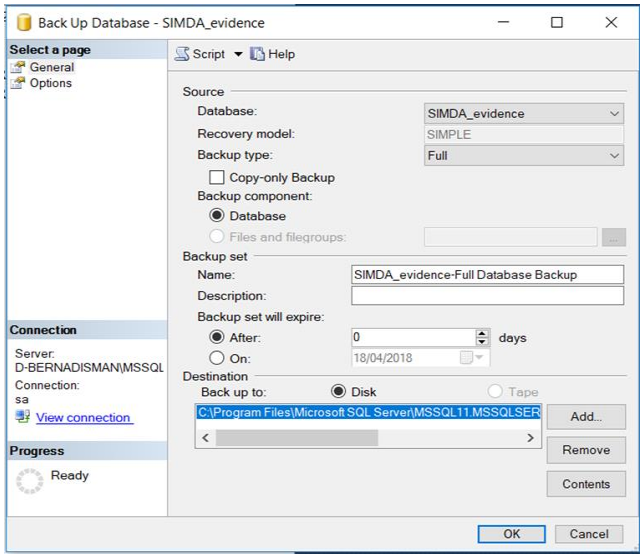
Tahap pengumpulan data dilakukan untuk memperoleh informasi dan data yang dibutuhkan dalam rangka mencapai tujuan penelitian, Proses pengumpulan informasi dan data yang pertama untuk dilakukan ialah mengambil *database* SIMDA dengan cara membackup *database* dari server, proses backup data menggunakan software Microsoft SQL Server untuk dijadikan bukti.

Pada database SIMDA Perencanaan terdiri dari beberapa table yang digunakan untuk penampungan data transaksi dari hasil penginputan aplikasi SIMDA Perencanaan, adapun data table – table yang berada di database SIMDA perencanaan total nya ada 106 table transaksi dan table referensi (Gambar 2).



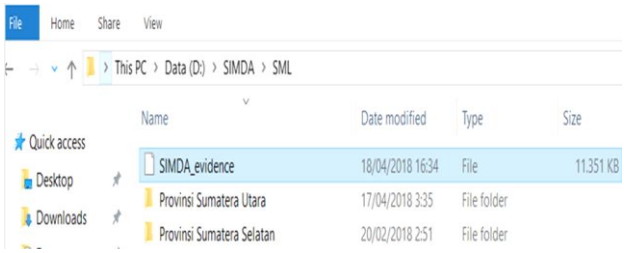
Gambar 2. Database SIMDA perencanaan

Sebelum proses backup *database* dilakukan maka perlu diberikan identitas pada file back up database tersebut dengan nama *SIMDA_Evidence*, dengan type back up adalah *Full Database Backups* (Gambar 3).



Gambar 3. Proses backup database

Setelah proses backup *database* SIMDA dari server selesai, maka menghasil satu file bernama SIMDA_evidence yang disimpan pada drive D. seperti gambar dibawah ini yang berwarna biru.



Gambar 4. File backup database

File backup *database* dari server tersebut sebagai salah satu barang bukti yang di kumpulkan untuk dilakukan pemeriksaan lebih lanjut dalam mendapatkan barang bukti terkait perubahan, penghapusan atau informasi terkait memanipulasi data perencanaan keuangan daerah.

Pengumpulan data bertujuan untuk mengidentifikasi berbagai sumber daya yang dianggap penting dan bagaimana semua data dapat terhimpun dengan baik. Pengumpulan data merupakan langkah pertama dalam melakukan proses forensik untuk mengidentifikasi sumber-sumber yang dianggap potensial untuk dijjadikan bukti, dan menjelaskan langkah-langkah yang dibutuhkan dalam mengumpulkan data (Bernadisman, 2017).

4.2. Tahap Pemeriksaan data

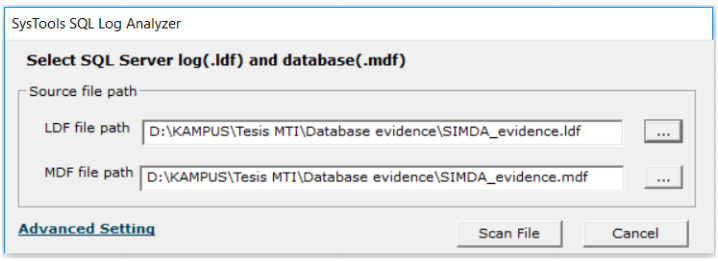
Setelah melalui proses pengumpulan data, maka selanjutnya melakukan pemeriksaaan mencakup didalamnya menilai dan melakukan ekstraksi data yang relevan dari data-data yang dikumpulkan, tahapan ini melibatkan *bypassing* atau meminimalisasi fitur-fitur basis data dan sistem aplikasi, untuk mengidentifikasi data didalamnya

akan sangat menyita waktu dan perhatiaan serta akan sangat melelahkan, filtrasi akan mengeliminir sebagaian data yang tidak dibutuhkan.

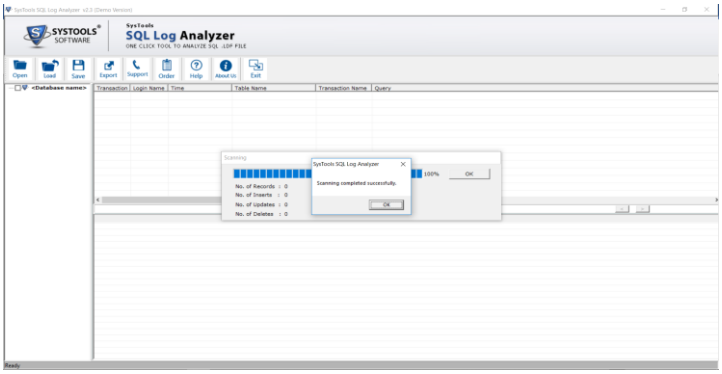
Pada tahap pemeriksaan data akan dilakukan pada *database* SIMDA Perencanaan keuangan daerah sebagai bahan pemeriksaan untuk mendapatkan barang bukti, sebelum melakukan pemeriksaan pada *database* SIMDA Perencanaan, kemudian direstore kan kembali pada komputer atau laptop yang sudah disiapkan sebagai peralatan forensik, yang sudah di install software Microsoft SQL Server disetting pada menu Task untuk di take offline atau *database* di non aktifkan, agar proses mengambilan *database* SIMDA Perencanaan dapat dilakukan, file yang dibutuhkan adalah file Media Descriptor File (.mdf) dan Log file (.ldf).

File .mdf dan file .ldf dari *database* SIMDA Perencanaan ini lah yang akan menjadi bahan untuk melakukan pemeriksaan data pada proses pemeriksaan data dibawah ini menggunakan tool forensik SQL Log Analyzer (Gambar 5 dan 6).

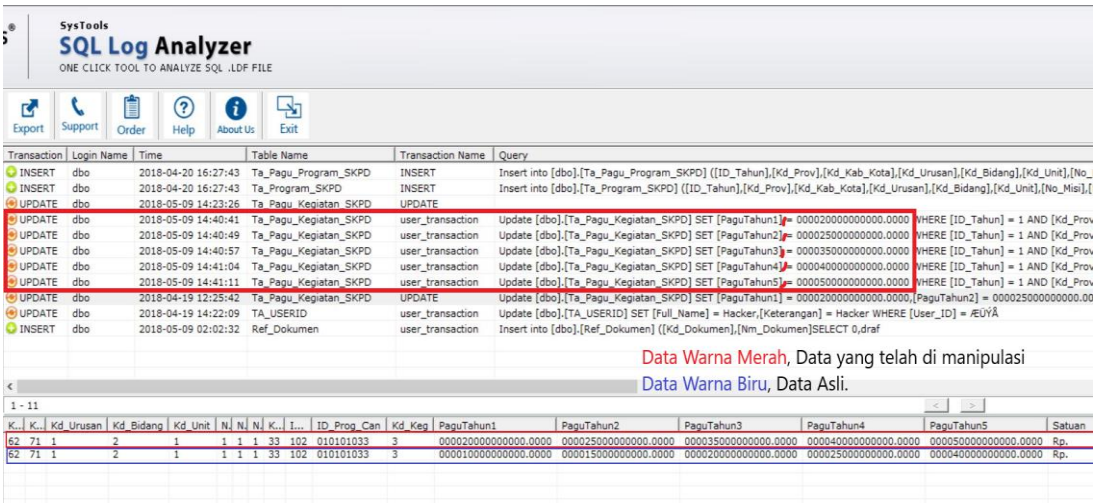
Pada Gambar 5 adalah menu untuk menentukan file mdf dan ldf yang akan di scanning menggunakan tool sysTools Log Analyzer, jika hasil scanning database tidak ditemukan penyimpangan maka akan seperti gambar 6, dimana file hasil scanning file bernilai 0, artinya data yang diperiksa tidak ditemukan perubahan, pengeditan atau penghapusan maka hasil pemeriksaan tidak ditemukan data yang rusak atau korup dikarenakan penyimpangan atau kejahatan, berbeda hal nya dengan Gambar 7.



Gambar 5. SysTools SQL Log Analyzer



Gambar 6. Hasil Scanning File yang tidak ada perubahan data.



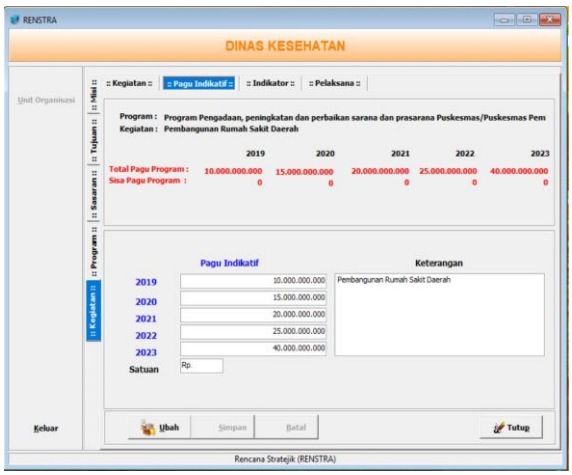
Gambar 7. Hasil Scanning data yang termanipulasi

Pada Gambar 7 diatas, menjelaskan proses Scanning file yang menghasilkan data transaksi yang telah dirubah atau di edit bukan dari aplikasi SIMDA Perencanaan. Metode SQL Injection merupakan Perubahan data yang menggunakan cara menyisipkan syntax command SQL yang bertujuan mengganggu keamanan basis data untuk Penyerang atau menyusup ke dalam basis data (Murniati *et al.*,, 2018).

Dengan menggunakan tool sysTools SQL Log Analyzer akan terlihat data apa saja yang telah dirubah dan siapa pelakunya. pada gambar 7, telah ditemukan barang bukti berupa transaksi log pada saat seseorang mengedit data pagu anggaran kegiatan SKPD melalui database, perubahan dapat dilihat pada tabel Ta_Pagu_Kegiatan_SKPD, pada tanggal 09 April 2018 pukul 14:41, dapat dilihat data yang dikotak warna merah adalah data yang telah dirubah melalui database, sedangkan data pada kotak warna biru merupakan data sebelum perubahan.

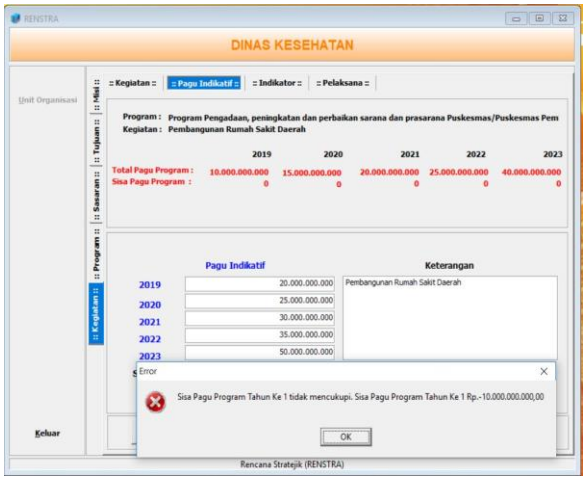
Pada tahap ini akan dilakukan proses pemeriksaaan pada aplikasi SIMDA dengan membandingkan 2 menu yang sama. Aplikasi pada gambar 7 ini adalah aplikasi SIMDA Perencanaan pada menu pagu anggaran kegiatan SKPD yang sedang berjalan dengan data kegiatan pembangunan rumah sakit.

Pada Gambar 8, terlihat bahwa pagu indikatif yang diinput menunjukan hasil total sisa pagu anggaran program pada program pengadaan sudah habis digunakan untuk kegiatan pembangunan rumah sakit. Total sisa pagu anggaran jika sudah habis tidak bisa ditambah lagi melalui aplikasi.



Gambar 8. Menu pagu anggaran sebelum dimanipulasi

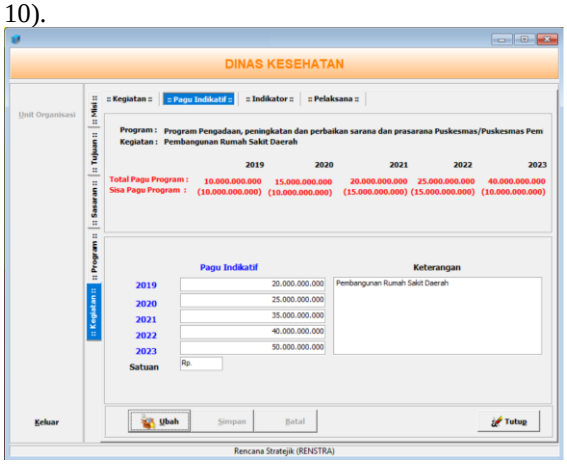
Jika aplikasi melakukan penginputan data pagu anggaran kegiatan SKPD melebihi pagu anggaran program SKPD maka aplikasi akan memberikan kontrol atau peringatan bahwa sisa pagu anggaran program tidak mencukupi untuk digunakan pada data kegiatan. Kontrol tersebut sudah di buat dan ditanam dalam aplikasi SIMDA Perencanaan sebagai indikator keamanan agar setiap operator yang menginput atau mengedit data yang melebihi data sisa pagu program maka tidak akan bisa merubahnya, adapun menu pagu anggaran yang sudah diberikan kontrol pesan dialog sebagai berikut :



Gambar 9. Menu pagu anggaran dengan peringatan

Pada Gambar 9 menjelaskan bahwa aplikasi tidak akan menyimpan proses penginputan pagu anggaran kegiatan yang melebihi sisa pagu program.

Dampak dari adanya perubahan data yang diarahkan langgung ke database menggunakan syntax yang dibuat menggunakan SQL Injection untuk merubah pagu anggaran kegiatan, sehingga data pagu anggaran kegiatan dapat melebihi sisa pagu program yang telah disediakan. Perubahan data juga dapat dilihat dalam aplikasi SIMDA Perencanaan (Gambar 10).



Gambar 10. Menu pagu anggaran termanipulasi

Pada Gambar 10, pada aplikasi SIMDA Perencanaan di menu anggaran kegiatan terlihat, program pengadaan, peningkatan dan perbaikan sarana dan prasarana, dengan kegiatan pembangunan rumah sakit daerah mengalami perubahan data yang tidak lazim, dimana total pagu program pada tahun pertama (2019) sebesar 10.000.000.000 tetapi sisa pagu program menjadi minus sebesar (10.000.000.000) sedangkan pagu kegiatannya sebesar 20.000.000.000. Total pagu program tahun

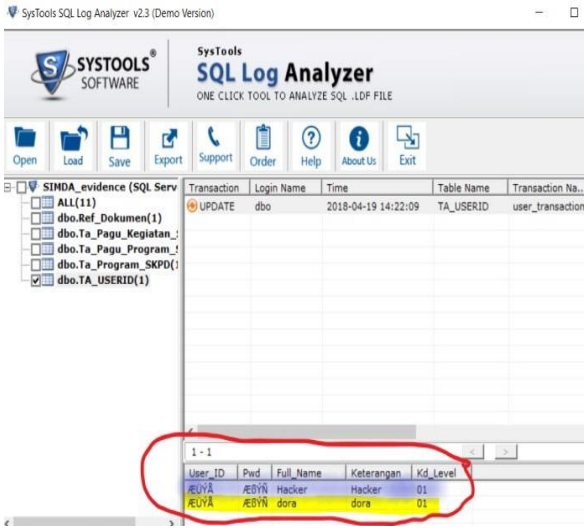
kedua (2020) sebesar 15.000.000.000 tetapi sisa pagu program menjadi minus sebesar (10.000.000.000), sedangkan pagu kegiatannya sebesar 25.000.000.000. Total pagu program tahun ketiga (2021), dimana total pagu program sebesar 20.000.000.000 sedangkan sisa pagu program menjadi minus sebesar (15.000.000.000) sedangkan pagu kegiatannya sebesar 35.000.000.000. Kemudian total pagu program tahun keempat (2022) sebesar 25.000.000.000 sedangkan sisa pagu program menjadi minus sebesar (15.000.000.000) sedangkan pagu kegiatan sebesar 40.000.000.000. Kemudian total pagu program tahun kelima (2023) sebesar 40.000.000.000, sedangkan sisa pagu program menjadi minus sebesar (10.000.000.000) data pada pagu kegiatan sebesar 50.000.000.000.

Pada aplikasi SIMDA di menu pagu anggaran kegiatan, nilai sisa pagu program dari tahun kesatu (2019) sampai tahun kelima (2023) nilai sisa pagu program menjadi minus, hal ini tidak bisa terjadi pada aplikasi simda jika proses penginputannya sesuai dengan Standar Operasional yang berlaku, maka aplikasi simda perencanaan akan memberikan pesan bahwa pagu kegiatan melebihi dari pagu program sehingga proses penyimpanan data tidak bisa diproses, proses penyimpanan akan dapat diproses jika nilai pagu kegiatan sama dengan nilai pagu program atau nilai pagu kegiatan lebih kecil dari nilai pagu program.

Nilai sisa pagu program menjadi minus dikarenakan adanya perubahan data dari *database* yang dilakukan menggunakan syntax command pada SQL yang bertujuan untuk memasukan secara paksa nilai pagu kegiatan melalui *database*.

Pada tool SysTools SQL Loq Analyzer juga dapat terlihat ada perubahan data yang terjadi pada table Ta_USERID, table ini berfungsi sebagai penampung data user name dan password, pada gambar 11 terlihat pada Query adanya perubahan user name dora menjadi hacker, hal ini agar pelaku juga dapat mengakses data tersebut melalu aplikasi SIMDA Perencanaan yang dirubah menggunakan SQL Injection pada *database*.

Pada sistem *database* dengan menggunakan SQL, perintah-perintah dapat dimasukkan sesuai yang diinginkan oleh pengguna walaupun pengguna tersebut bukan yang berwenang akan hal itu. perusak yang dilakukan oleh pengguna tersebut yang bisa menimbulkan akibat fatal yang dapat dilakukan dengan menggunakan SQL Injection, sama halnya dengan data pagu anggaran kegiatan yang dirubah melalui database dapat berakibat fatal pada pembengkakan pagu anggaran kegiatan, hal ini dapat merugikan pemerintah daerah.



Gambar 11. Perubahan User Id

4.3. Tahap Analisa Data

Berdasarkan proses pemeriksaan yang dilakukan melalui aplikasi SIMDA dan basis data SIMDA yang menggunakan tool SQL Log Analyzer maka pada hasil scanning file menggunakan Tool systools Log SQL Analyzer bisa di analisa sebagai berikut, adanya perubahan data pada table pagu anggaran kegiatan SKPD, pada satuan kerja perangkat daerah yang mempunyai kode urusan = 1, kode bidang = 2, kode unit = 1, dapat diketahui kode tersebut adalah kode Dinas Kesehatan, dengan kode program gabungannya adalah 010101033 (program pengadaan, peningkatan, dan perbaikan sarana dan prasarana) dan kode kegiatan 33 (Pembangunan rumah sakit) data yang telah dirubah adalah pagu Angaran kegiatan tahun pertama (2019) sebesar 10.000.000.000 berubah menjadi 20.000.000.000, pagu anggaran tahun kedua (2020) sebesar 15.000.000.000 dirubah menjadi 25.000.000.000, pagu anggaran tahun ketiga (2021) sebesar 20.000.000.000 dirubah menjadi 35.000.000.000, pagu anggaran tahun keempat (2022) sebesar 25.000.000.000 dirubah menjadi 40.000.0000.000, pagu anggaran tahun kelima((2023) sebesar 40.000.000.000 dirubah menjadi 50.000.000.000. dari kegiatan pembangunan rumah sakit tersebut pagu anggaran di naikan atau dibesarkan nilai anggaranya, hal tersebut tidak sesuai dengan Standard Prosedur yang sudah berjalan sehingga hal ini termasuk kegiatan yang menyalahi aturan hukum yang berlaku dan dapat dikaitkan pada tindakan korupsi.

Di lihat dari pemeriksaan aplikasi SIMDA Perencanaan maka dapat ditemukan bahwa ada program kegiatan yang dibuat oleh dinas kesehatan yang mana pagu anggaran kegiatannya melebihi pagu anggaran program.

Jika dibandingkan hasil pemeriksaan *database* SIMDA Perencanaan menggunakan tool SQL Log Analyzer dengan pemeriksaan terhadap aplikasi

SIMDA Perencanaan, maka dapat dibandingkan bahwa perubahan data yang terjadi memiliki perubahan data dari nilai pagu anggaran kegiatan yang sama, dan dapat disimpulkan bahwa perubahan data tersebut dilakukan menggunakan syntax command SQL (*SQL Injection*) yang di inject ke dalam *database* SIMDA Perencanaan.

4.4. Tahapan Laporan

Dari hasil Analisa maka dapat disimpulkan bahwa telah terjadi manipulasi data pada *database* SIMDA Perencanaan, adapun tabel yang mengalami perubahan adalah tabel Ta_Pagu_Kegiatan_SKPD, tabel Ta_Pagu_Program_SKPD dan Ta_Userid. Perubahan data yang terjadi diakibatkan menggunakan syntax command SQL (SQL Injection) dengan perintah UPDATE Ta_Pagu_Anggaran_Kegiatan yang dapat merubah nilai pagu anggaran sehingga pagu anggaran kegiatan dapat melebihi nilai pagu anggaran program SKPD.

Perubahan data juga terjadi pada table Ta_USERID, table ini berfungsi sebagai penampung data user name dan password, perubahan data user name yang dirubah menjadi nama user name hacker, dan merubah otorisasi sebagai administrator, sedangkan data pagu anggaran kegiatan skpd yang dirubah dari database simda menggunakan metode SQL Injection pada tanggal 19 April 2018 pada jam 12:25:42 yang terekam pada SQL Log Analyzer. Serangan ini terjadi pada jaringan internal pemerintah daerah. Data yang telah dimanipulasi pada program pengadaan, peningkatan sarana dan prasarana, dengan kegiatan pembangunan rumah sakit daerah, dapat dilihat pada Tabel 1.

Tabel 1. Hasil pemeriksaan *database* menggunakan tool SQL Log Analyzer.

Tahun Anggaran	Pagu Anggaran Sebelum dimanipulasi	Pagu anggaran Setelah dimanipulasi
2019	Rp. 10.000.0000.000	Rp. 20.000.0000.000
2020	Rp. 15.000.0000.000	Rp. 25.000.0000.000
2021	Rp. 20.000.0000.000	Rp. 35.000.0000.000
2022	Rp. 25.000.0000.000	Rp. 40.000.0000.000
2023	Rp. 40.000.0000.000	Rp. 50.000.0000.000

Setelah dianalisa melalui hasil pemeriksanaan *database* menggunakan tool *SQL Log Analyzer* (Tabel 1) dan analisa melalui hasil pemeriksaan menggunakan aplikasi SIMDA (Tabel 2) maka ditemukan perubahan data yang sama, yang dilakukaan dengan cara SQL Injection ke dalam *database* SIMDA Perencanaan untuk merubah salah satu program dan kegiatan yang dilaksanakan oleh dinas kesehatan. Adapun perubahan data yang ditemukan berdasarkan pemeriksaan menggunakan aplikasi SIMDA dan *database* menggunakan tool maka ditemukan perubahan data program dan kegiatan yang sama, yaitu : program pengadaan, peningkatan dan perbaikan sarana dan prasarana, dengan kegiatan pembangunan rumah sakit daerah mengalami perubahan data yang tidak lazim, dimana total pagu program pada tahun pertama (2019) sebesar 10.000.000.000 tetapi sisa pagu program menjadi minus sebesar (10.000.000.000) sedangkan pagu kegiatannya sebesar 20.000.000.000. Total pagu program tahun kedua (2020) sebesar 15.000.000.000 tetapi sisa pagu program menjadi minus sebesar (10.000.000.000), sedangkan pagu kegiatannya sebesar 25.000.000.000. Total pagu program tahun ketiga (2021), dimana total pagu program sebesar 20.000.000.000 sedangkan sisa pagu program menjadi minus sebesar (15.000.000.000) sedangkan pagu kegiatannya sebesar 35.000.000.000. Kemudian total pagu program tahun keempat (2022) sebesar 25.000.000.000 sedangkan sisa pagu program menjadi minus sebesar (15.000.000.000) sedangkan pagu kegiatan sebesar 40.000.000.000. Kemudian total pagu program tahun kelima (2023) sebesar 40.000.000.000, sedangkan sisa pagu program menjadi minus sebesar (10.000.000.000) data pada pagu kegiatan sebesar 50.000.000.000.

Tabel 2. Hasil pemeriksaan menggunakan Aplikasi SIMDA

Tahun Anggaran	Pagu Anggaran Sebelum dimanipulasi	Pagu anggaran Setelah dimanipulasi
2019	Rp. 10.000.0000.000	Rp. 20.000.0000.000
2020	Rp. 15.000.0000.000	Rp. 25.000.0000.000
2021	Rp. 20.000.0000.000	Rp. 35.000.0000.000
2022	Rp. 25.000.0000.000	Rp. 40.000.0000.000
2023	Rp. 40.000.0000.000	Rp. 50.000.0000.000

Hasil dari pemeriksaan *database* menggunakan tool SQL Log Analyzer memberikan informasi perubahan data yang telah dilakukan melalui *database* SIMDA Perencanaan, sedangkan Hasil Pemeriksaaan menggunakan Aplikasi SIMDA Perencanaan memberikan informasi dari hasil analisa pada gambar 10 yaitu menu pagu anggaran yang telah termanipulasi, dari hasil analisa tersebut bahwa perubahan yang dilakukan aplikasi tidak akan bisa jika perubahan yang pada pagu anggaran kegiatan melebihi pagu anggaran program.

5. Kesimpulan

Dari hasil pemeriksanaan dan Analisa data yang telah dilakukan pada *database* SIMDA Perencanaan

untuk RPJMD dan Renstra SKPD menggunakan metode forensik statis, Berdasarkan hasil Analisa pada *database* SIMDA masih ada celah yang dapat disusupi oleh pihak yang tidak bertanggung jawab untuk memanipulasi data, dengan mencari celah untuk menembus *database* dengan cara menginject sintax command SQL kedalam *database*.

Berdasarkan hasil Analisa dan laporan yang disajikan, peneliti menyarankan agar pemerintah daerah, membentuk team khusus dalam dalam pengelolaan aplikasi SIMDA Perencanaan agar pengelolaan dapat dikelola secara professional. Berdasarkan hasil Analisa dan laporan yang disajikan, peneliti menyarankan kepada administrator atau pengelola aplikasi agar mengaktifkan *software profiler* yang berada di SQL Server untuk memonitor transaksi yang sedang berjalan dan dapat menganalisa data berjalan yang sedang berjalan, *Profiler* juga mampu menyajikan kapan data tersebut di proses insert, update dan delete. Selain itu, peneliti juga menyarankan kepada programmer aplikasi agar dapat menutup celah terjadinya penyusupan yang dilakukan dengan cara menginjection command syntax SQL pada *database* SIMDA Perencanaan, agar *SQL Injection* pada *database* tidak terjadi dikemudian hari.

Daftar Pustaka

Al-Azhar, M., 2012. Digital Forensik Panduan Praktis Investigasi Komputer. anwar, nuril, & Riadi, I., 2017. Analisis Investigasi Forensik WhatsApp Messanger Smartphone Terhadap WhatsApp Berbasis Web. Jurnal Ilmiah Teknik Elektro Komputer Dan Informatika, 3(1), 1–10. Retrieved from

Cohen, F., & Ph, D., 2013. *Digital Forensic EvidenceExamination*(Copyright,p.517).Retrived, from http://all.net/books/2013-DFE-Examination.pdf.

Bernadisman, D., 2017. Analisis Forensik Basis Data Menggunakan Framework Open Web Application Security Project (OWASP), *Prosiding Seminar Nasional Informatika, Vol.1, Jakarta, November 18, 45-58*.

Casey, E., 2010. Handbook of Digital Forensics and Investigation, Unites states of America, academi Press.

Faiz, M.N., Umar, R. dan Yudhana, A., 2017. Implementasi Live Forensics untuk perbandingan Browser pada Keamanan Email.(JISKa), Vol. 1, No. 3, 108-114.

Fowler, K., 2007, Forensic Analysis of a SQL Server 2005 Database Server.USA: emergis.

Kalbande, D. & Jain, N., 2013. Comparative Digital Forensic Model. International Journal of Innovative Research in Science, Engineering and Technology (IJIRSET), Vol. 2 No. 8, 3414-3419.

Murniati, Munandi, R., Arif, T.Y., 2018. Analysis of Web Server Security Against Structure Query Language Injection Attacks in ASEAN Senior High Schools. 3 (1), 1-7

Subli, M., Sugiantoro, B., Prayudi, Y., 2017. Metadata Forensik Untuk Mendukung Proses Investigasi Digital. Jurnal Ilmiah Data Manajemen dan Teknologi Informasi 18 (1), 44-50

Riadi, I, Umar, R , Wasito., 2014. Analisis Forensik Serangan SQL Injection Menggunakan Metode Statis Forensik. Volume 1 No.1, 1-2.

Sistem Informasi Manajemen Daerah, 2018. Website:http://www.bpkp.go.id/sakd/konten/333/Versi-2.1.bpkp diakses tanggal 20 Februari 2019.

Sulianta, F. 2014. Teknik Forensik. Jakarta : PT Elex Media Komputindo.