



Audit Sistem Informasi Akademik Berdasarkan Aktifitas Pengguna

Aris Susanto¹, La Ija², La Ode Bakrim³

STMIK Bina Bangsa Kendari
¹arissusantoh@gmail.com

Abstrak

Sistem Informasi berbasis database telah di implementasikan STMIK Bina Bangsa Kendari untuk membantu mendokumentasikan proses kegiatan akademik. Pada proses implementasi sistem informasi, terjadi hal yang tidak diinginkan seperti adanya pihak yang mencari celah yang dimiliki aplikasi dan bertujuan untuk memanipulasi dapat menyebabkan perubahan data pada database. Oleh karena itu, perlu dilakukan pemeriksaan secara forensik untuk mengetahui kejadian manipulasi data tersebut untuk mendapatkan barang bukti digital atau histori data yang telah dimanipulasi atau dihapus. Tujuan proses forensik database untuk memonitoring aktifitas pengguna pada database SIMAK agar dapat mengetahui dan mendeteksi aktifitas pengguna database dan mengetahui siapa yang merubah, data apa yang dirubah, dan kapan dilakukannya. Proses pengumpulan data dilakukan dengan merekam aktifitas pengguna disetiap aktifitas dengan menggunakan tools *log helper* yang *include* dengan SIMAK. Dari hasil analisa disimpulkan bahwa telah terjadi perubahan data yaitu menghapus data pada database SIMAK. Data yang dihapus yaitu data mahasiswa dengan nomor pokok 201752067 yang terdaftar pada semester 20191. Waktu penghapusan data dilakukan pada tanggal 03-09-2019 pukul 09:53:40 melalui IP 180.251.168.165.

Kata Kunci: Database Forensik, *Log Aktifitas*, Log Helper, SIMAK.

Abstract

Database-based Information System that has been implemented by STMIK Bina Bangsa Kendari to help document the process of academic activities. In the process of implementing an information system, something untoward happens like a party looking for loopholes that an application has and aims to manipulate can cause changes to the data in the database. Therefore, it is necessary to do a forensic examination to determine the occurrence of data manipulation to obtain digital evidence or historical data that has been manipulated or deleted. The purpose of the database forensic process is to monitor user activity on the SIMAK database so that it can find and detect the activities of the database user and find out who changed, what data was changed, and when. The process of collecting data is done by recording user activity in each activity using the log helper tools that include with (SIMAK). From the results of the analysis it is concluded that there has been a change in data that is removing data in the SIMAK database. The data that was deleted was the student data with the principal number 201752067 registered in semester 20191. The time of data deletion was carried out on 09-03-2019 at 09:53:40 through IP 180.251.168.165.

Keywords: Forensic Database, Activity Log, Log Helper, SIMAK.

1. Pendahuluan

Sistem informasi merupakan suatu terobosan yang harus diterapkan pada setiap instansi pemerintah atau perusahaan swasta agar dapat membantu menyelesaikan pekerjaan dengan cepat dan menyajikan laporan-laporan yang sesuai secara efisien, efektif, transparan, dan akuntabel kepada pimpinan instansi atau perusahaan serta pihak-pihak yang terkait. Sistem informasi perlu menggunakan teknologi informasi seperti personal komputer, server, dan infrastruktur jaringan untuk menjalankan sistem informasi yaitu berupa perangkat lunak (*software*).

Pemanfaatan sistem informasi tidak hanya diterapkan di lingkungan instansi pemerintahan dan perusahaan swasta, akan tetapi banyak pula diterapkan di institusi pendidikan

dimana salah satu tujuannya adalah untuk membantu menyelesaikan tugas-tugas yang berkaitan dengan kegiatan akademik. Salah sistem informasi yang diterapkan STMIK Bina Bangsa Kendari yaitu Sistem Informasi Manajemen Akademik (SIMAK) yang berbasis database.

Penggunaan database dalam pengelolaan sistem informasi menjadi hal yang sangat penting untuk menyimpan data yang suatu waktu dapat di tambah, diubah, dan dihapus. Pemanfaatan database pada sistem informasi perlu perhatian khusus untuk menjaga kerahasiaan data dan akses dari pihak-pihak yang tidak bertanggung jawab.

Sistem Informasi berbasis database yang telah di implementasikan STMIK Bina Bangsa Kendari untuk membantu mendokumentasikan proses kegiatan akademik kedalam sebuah database digunakan sebagai tempat penyimpanan data mahasiswa dan proses kegiatan mahasiswa selama melaksanakan proses perkuliahan.

Pada proses implementasi sistem informasi, terjadi hal yang tidak diinginkan seperti adanya pihak yang mencari celah yang dimiliki aplikasi dan bertujuan untuk memanipulasi data atau mencuri data sehingga dapat menyebabkan perubahan data pada database. Oleh karena itu, perlu dilakukan pemeriksaan secara forensik untuk mengetahui kejadian manipulasi data tersebut untuk mendapatkan barang bukti digital atau histori data yang telah dimanipulasi atau dihapus.

Tujuan proses forensik database untuk memonitoring aktifitas pengguna pada database SIMAK agar dapat mengetahui dan mendeteksi aktifitas dalam memanipulasi data yang dilakukan oleh pengguna database dan mengetahui siapa yang merubah, data apa yang dirubah, dan kapan dilakukannya.

2. Metode

2.1. Forensik Digital

Forensik digital merupakan ilmu yang digunakan untuk kepentingan bukti hukum, yang dalam hal ini adalah membuktikan kejahatan komputer secara ilmiah untuk bisa didapatkan bukti digital yang valid [1]. Forensika digital merupakan ilmu pengetahuan dan teknologi komputer untuk melakukan pemeriksaan dan analisa terhadap barang bukti elektronik dan barang bukti digital dalam melihat keterkaitannya dengan kejahatan [2].

2.2. Database Forensik

Database Forensik adalah bidang penting yang harus memerlukan kesadaran penelitian. Kurangnya penelitian adalah karena kompleksitas yang melekat dari database yang belum sepenuhnya dipahami dalam konteks forensik. Dikatakan bahwa database secara inheren multidimensi dari perspektif forensik [3].

Database forensik mengacu pada cabang ilmu forensik digital yang berkaitan dengan studi *forensic database* dan metadata terkait [4]. Menurut Fowler yang dikutip [5] database forensik bertujuan untuk melihat siapa yang mengakses dan tindakan apa saja yang dilakukan pada database.

Barang bukti merupakan bagian yang sangat penting dalam sebuah kasus kejahatan, dari barang bukti ini tim investigasi dan analis forensik dapat mengungkap kasus dengan kronologis yang lengkap [6].

2.3. Penelitian Terkait

Penulis [7] menyoroti alasan ancaman dan risiko yang tidak terkendali pada basis data sebagai kendala anggaran, dan terlalu banyak staf TI yang memiliki akses *rooting* ke basis data dan kurangnya keterampilan keamanan basis data. Dalam [8] penulis mengeksplorasi fitur forensik di MySQL 5.5. Namun, *SQL Trace* tidak dapat menjadi sumber yang dapat diandalkan untuk memantau database karena kurangnya pemantauan berkelanjutan ke sistem database. Ini menghabiskan banyak memori dan CPU, dan menyimpan sejumlah besar data tanpa mekanisme penyaringan. Mereka mengeksplorasi utilitas MySQL untuk menggali database untuk analisis

forensik, seperti (1) *'mysqldump'* untuk membuang database untuk cadangan nanti dan untuk membuat ulang tabel untuk mengisi pernyataan SQL, (2) *'mysqlaccess'* untuk memeriksa hak akses, dan (3) *'myisamlog'* untuk menampilkan konten *log* ISAM untuk melakukan operasi pemulihan.

Penulis dalam [9] menekankan pada fitur audit yang tersedia di berbagai DBMS dan bagaimana mereka semua mempengaruhi kesiapan forensik dari database. Mereka mengeksplorasi pengaturan default untuk enam fitur *logging* DBMS dan menunjukkan bagaimana standar ini biasanya tidak akan berkontribusi dalam peristiwa rekonstruksi dan forensik. Selain itu, mereka menunjukkan bagaimana menyeimbangkan pertukaran antara mengaktifkan pengaturan *logging* yang kuat yang akan membantu dalam proses forensik, dan ruang memori yang besar dan volume *file log* yang besar. Mereka menyarankan fitur ideal untuk *logging* di mana keseimbangan dipertahankan, dan kesiapan forensik tercapai.

2.4. Identifikasi dan Pengumpulan Data

Pada tahapan ini identifikasi dilakukan sebagai rangkaian kegiatan yang mencakup proses pengumpulan data untuk mendukung proses penyidikan dalam pencarian barang bukti. Media digital yang dijadikan sebagai barang bukti yaitu file database, Identifikasi dilakukan untuk mencari informasi tentang aktifitas yang dilakukan oleh pengguna database.

2.5. Penyimpanan

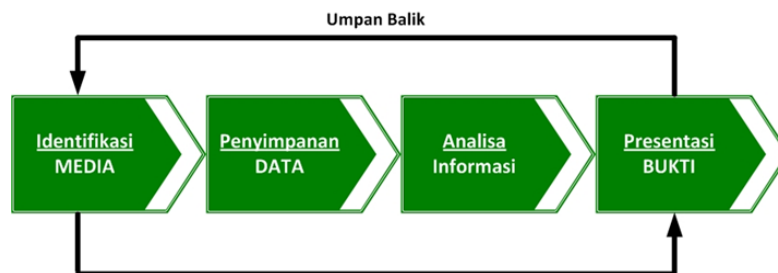
Tahapan ini merupakan proses penyimpanan data aktifitas pengguna, media yang digunakan sebagai penyimpanan data adalah database MySQL, Tools yang digunakan dalam mendukung tahapan ini yaitu menggunakan *log helper* yang *include* dengan aplikasi Sistem Informasi Manajemen Akademik yang berfungsi merekam setiap aktifitas pengguna.

2.6. Analisa

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

2.7. Laporan Hasil Analisa

Pada tahapan ini barang bukti digital dari proses pemeriksaan data yang sudah dianalisis sesuai dengan aturan investigasi maka hasil dari pemeriksaan dan analisa dituangkan dalam laporan. 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.



Gambar 1. Proses Analisis

3. Hasil dan Pembahasan

3.1. Tahap Identifikasi dan Pengumpulan Data

Proses pengumpulan data dilakukan dengan merekam aktifitas pengguna disetiap aktifitas yang dilakukan dengan menggunakan *tools log helper* yang *include* dengan Sistem Informasi Manajemen Akademik (SIMAK), Tipe aktifitas pengguna yang terjadi pada database SIMAK yaitu *login*, *add*, *edit*, *view*, *delete*, *update*, dan *logout*. Berikut adalah *script log helper* yang digunakan pada aplikasi SIMAK.

```
1 <?php if ( ! defined('BASEPATH')) exit('No direct script access allowed');
2 function helper_log($tipe = "", $str = ""){
3     $CI =& get_instance();
4     if (strtolower($tipe) == "login"){
5         $log_tipe = 0;
6     }
7     elseif(strtolower($tipe) == "logout"){
8         $log_tipe = 1;
9     }
10    elseif(strtolower($tipe) == "add"){
11        $log_tipe = 2;
12    }
13    elseif(strtolower($tipe) == "edit"){
14        $log_tipe = 3;
15    }
16    elseif(strtolower($tipe) == "view"){
17        $log_tipe = 4;
18    }
19    elseif(strtolower($tipe) == "delete"){
20        $log_tipe = 5;
21    }elseif(strtolower($tipe) == "update"){
22        $log_tipe = 6;
23    }
24    else {
25        $log_tipe = 7;
26    }
27    $param['log_user'] = $CI->session->userdata('username');
28    $param['log_name'] = $CI->session->userdata('nama_lengkap');
29    $param['log_tipe'] = $log_tipe;
30    $param['log_desc'] = $str;
31    $param['log_ip'] = $_SERVER['REMOTE_ADDR'];
32    $param['log_url'] = $_SERVER['REQUEST_URI'];
33    $CI->load->model('m_log');
34    $CI->m_log->save_log($param);
35 }
36 function helper_login($level = "", $desc = ""){
37     $CI =& get_instance();
38     if (strtolower($level) == "mahasiswa"){
39         $log_tipe = "Mahasiswa";
40     }
41     if (strtolower($level) == "admin"){
42         $log_tipe = "Admin";
43     }
44     if (strtolower($level) == "bendahara"){
45         $log_tipe = "Bendahara";
46     }
47     if (strtolower($level) == "dosen"){
48         $log_tipe = "Dosen";
49     }
50     $datalogin['log_user'] = $CI->session->userdata('username');
51     $datalogin['log_name'] = $CI->session->userdata('nama_lengkap');
52     $datalogin['log_tipe'] = $log_tipe;
53     $datalogin['log_desc'] = $desc;
54     $datalogin['log_ip'] = $_SERVER['REMOTE_ADDR'];
55     $CI->load->model('m_log');
56     $CI->m_log->save_login($datalogin);
57 }
58 function helper_logout($level = "", $desc = ""){
59     $CI =& get_instance();
60     $CI->load->model('m_log');
61     $CI->m_log->hapus_login();
62 }
```

Gambar 2. Script Log Helper

Pengumpulan data dilakukan dengan menyisipkan *log helper* disetiap fungsi yang berpotensi untuk disalahgunakan oleh pengguna atau pihak-pihak yang tidak bertanggungjawab. Proses pengumpulan data ini merupakan langkah pertama dalam melakukan proses forensik untuk mengidentifikasi sumber-sumber yang dianggap potensial untuk dijadikan bukti. Adapun *script* yang digunakan pada salah satu fungsi seperti pada gambar 3 :

```
//fungsi untuk mengupdate data mahasiswa
function update data mahasiswa (){
    helper log("update", "Mengupdate data mahasiswa");
    $id = $this->input->post('id_mahasiswa');
    $tgl_lahir = $this->input->post('tanggal_lahir');
    $thn=substr($tgl_lahir,0,4);
    $bln=substr($tgl_lahir,5,2);
    $tgl=substr($tgl_lahir,8,2);
    $tanggal_lahir=$thn.$bln.$tgl;
```

Gambar 3. Script Log Helper Update Data Mahasiswa

3.2. Tahap Penyimpanan Data

Tahap penyimpanan data dilakukan untuk memperoleh data dan informasi yang dibutuhkan. Data aktifitas pengguna yang dilakukan disetiap fungsi pada aplikasi Sistem Informasi Manajemen Akademik (SIMAK) disimpan pada database dengan nama *tabel_log*, Adapun data yang disimpan berupa *log_time*, *log_user*, *log_name*, *log_tipe*, *log_desc*, *log_ip*, dan *log_url*. Script *log helper* yang digunakan untuk menyimpan data aktifitas pengguna seperti pada gambar 4.

```
$param['log_user'] = $CI->session->userdata('username');
$param['log_name'] = $CI->session->userdata('nama_lengkap');
$param['log_tipe'] = $log_tipe;
$param['log_desc'] = $str;
$param['log_ip'] = $_SERVER['REMOTE_ADDR'];
$param['log_url'] = $_SERVER['REQUEST_URI'];
$CI->load->model('m_log');
$CI->m_log->save_log($param);
```

Gambar 4. Script Log Helper Penyimpanan Data Aktifitas Pengguna

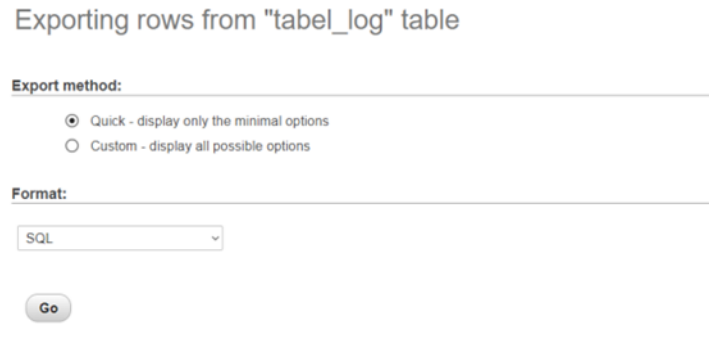
3.3. Tahap Analisa

Tahap analisa data dilakukan setelah melalui proses pengumpulan dan penyimpanan data. Selanjutnya dilakukan analisa berdasarkan data yang tersimpan pada *tabel log*. Adapun data yang tersimpan pada *tabel log* seperti pada gambar 5.

| log_time | log_user | log_name | log_tipe | log_desc | log_ip | log_url |
|---------------------|------------|---------------|----------|--|---|---------|
| 2019-05-08 13:16:32 | 201452052 | ANDRI SUGANDI | 4 | Menampilkan halaman login mahasiswa | 36.90.148.134 / | |
| 2019-05-08 13:16:32 | 201452052 | ANDRI SUGANDI | 4 | Menampilkan halaman login mahasiswa | 36.90.148.134 / | |
| 2019-05-08 13:16:33 | 9909913396 | Anis Susanto | 4 | Menampilkan halaman login mahasiswa | 36.75.143.235 / | |
| 2019-05-08 13:16:34 | 9909913396 | Anis Susanto | 4 | Menampilkan halaman login mahasiswa | 36.75.143.235 / | |
| 2019-05-08 13:16:34 | 9909913396 | Anis Susanto | 4 | Menampilkan halaman login mahasiswa | 36.75.143.235 / | |
| 2019-05-08 13:16:41 | 9909913396 | Anis Susanto | 4 | Menampilkan halaman login mahasiswa | 36.75.143.235 / | |
| 2019-05-08 13:16:42 | 9909913396 | Anis Susanto | 4 | Menampilkan halaman login mahasiswa | 36.75.143.235 / | |
| 2019-05-08 13:16:42 | 9909913396 | Anis Susanto | 4 | Menampilkan halaman login mahasiswa | 36.75.143.235 / | |
| 2019-05-08 13:16:59 | 201452052 | ANDRI SUGANDI | 6 | Mengupdate data mahasiswa | 36.90.148.134 /c_mahasiswa/update_data_mahasiswa_ | |
| 2019-05-08 13:16:59 | 201452052 | ANDRI SUGANDI | 4 | Menampilkan data mahasiswa di portal mahasiswa | 36.90.148.134 /c_mahasiswa/biodata_mahasiswa | |
| 2019-05-08 13:16:59 | 201452052 | ANDRI SUGANDI | 4 | Menampilkan halaman login mahasiswa | 36.90.148.134 / | |
| 2019-05-08 13:17:00 | 201452052 | ANDRI SUGANDI | 4 | Menampilkan halaman login mahasiswa | 36.90.148.134 / | |
| 2019-05-08 13:17:00 | 201452052 | ANDRI SUGANDI | 4 | Menampilkan halaman login mahasiswa | 36.90.148.134 / | |
| 2019-05-08 13:17:00 | 201452052 | ANDRI SUGANDI | 4 | Menampilkan halaman login mahasiswa | 36.90.148.134 / | |
| 2019-05-08 13:17:05 | 201452058 | SUNTORO | 0 | Melakukan login di halaman mahasiswa | 36.90.148.134 /auth/login_mahasiswa | |
| 2019-05-08 13:17:06 | 201452058 | SUNTORO | 4 | Menampilkan halaman login mahasiswa | 36.90.148.134 / | |
| 2019-05-08 13:17:09 | 201452058 | SUNTORO | 4 | Menampilkan halaman login mahasiswa | 36.90.148.134 / | |
| 2019-05-08 13:17:10 | 201452058 | SUNTORO | 4 | Menampilkan halaman login mahasiswa | 36.90.148.134 / | |
| 2019-05-08 13:17:24 | 9909913396 | Anis Susanto | 4 | Menampilkan halaman login mahasiswa | 36.75.143.235 / | |
| 2019-05-08 13:17:45 | 201452052 | ANDRI SUGANDI | 1 | Melakukan logout dari halaman mahasiswa | 36.90.148.134 /auth/logout_mahasiswa | |
| 2019-05-08 13:17:45 | 201452052 | ANDRI SUGANDI | 4 | Menampilkan halaman login mahasiswa | 36.90.148.134 /auth/logout_mahasiswa | |

Gambar 5. Data Aktifitas Pengguna

Setelah melalui proses penyimpanan data, proses selanjutnya yaitu menganalisa atau memeriksa data yang dikumpulkan. Tahapan yang dilakukan yaitu mengekspor tabel *log* dalam bentuk file *sql* yang selanjutnya di import pada komputer *local* yang tidak terkoneksi dengan jaringan internet. Proses *export* tabel *log* seperti pada gambar 6.



Gambar 6. Export Table Log

Database yang sudah sudah di *export* selanjutnya disimpan ke komputer *local* untuk dilakukan analisa data. Pemeriksaan yang telah dilakukan melalui aplikasi SIMAK dan database SIMAK menggunakan tools *Log Helper* dapat dilihat pada gambar 7 :

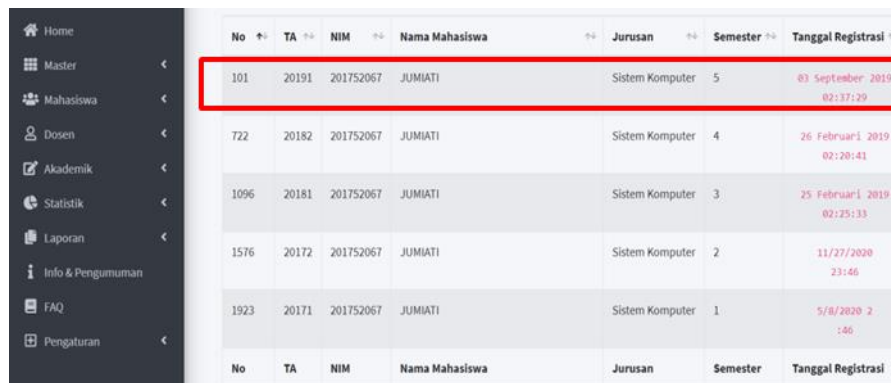
| log_time | log_user | log_name | log_type | log_desc | log_ip | log_url |
|---------------------|--------------------|----------|----------|--|-----------------|---|
| 2019-09-03 09:53:20 | Asma | | 4 | Menampilkan halaman login mahasiswa | 182.1.168.39 | / |
| 2019-09-03 09:53:35 | RISALDIN | | 0 | Melakukan login di halaman mahasiswa | 182.1.168.223 | /auth/login_mahasiswa |
| 2019-09-03 09:53:36 | RISALDIN | | 4 | Menampilkan data mahasiswa di portal mahasiswa | 182.1.168.223 | /ic_mahasiswa/boddata_mahasiswa |
| 2019-09-03 09:53:37 | RISALDIN | | 4 | Menampilkan halaman login mahasiswa | 182.1.168.223 | / |
| 2019-09-03 09:53:37 | RISALDIN | | 4 | Menampilkan halaman login mahasiswa | 182.1.168.222 | / |
| 2019-09-03 09:53:38 | RISALDIN | | 4 | Menampilkan halaman login mahasiswa | 182.1.168.223 | / |
| 2019-09-03 09:53:40 | RISALDIN | | 1 | Melakukan logout dari halaman mahasiswa | 182.1.168.223 | /auth/logout_mahasiswa |
| 2019-09-03 09:53:40 | RISALDIN | | 4 | Menampilkan halaman login mahasiswa | 182.1.168.223 | /auth/logout_mahasiswa |
| 2019-09-03 09:53:42 | @Irbadibrahim Asma | | 4 | DELETE FROM tb_reg_20191 | 180.251.168.165 | /ic_mahasiswa/telusur_log.php/201752067/20191 |
| 2019-09-03 09:53:42 | @Irbadibrahim Asma | | 4 | Menampilkan form registrasi mahasiswa per semester | 180.251.168.165 | /ic_mahasiswa/reg_mhs_per_semester |
| 2019-09-03 09:53:50 | MUH ALAM AMBEMALJ | | 4 | Menampilkan data mahasiswa di portal mahasiswa | 180.249.200.175 | /ic_mahasiswa/boddata_mahasiswa |
| 2019-09-03 09:53:51 | MUH ALAM AMBEMALJ | | 4 | Menampilkan halaman login mahasiswa | 180.249.200.175 | / |
| 2019-09-03 09:53:51 | MUH ALAM AMBEMALJ | | 4 | Menampilkan halaman login mahasiswa | 180.249.200.175 | / |
| 2019-09-03 09:53:52 | MUH ALAM AMBEMALJ | | 4 | Menampilkan halaman login mahasiswa | 180.249.200.175 | / |
| 2019-09-03 09:53:58 | @Irbadibrahim Asma | | 2 | Melakukan registrasi mahasiswa per semester | 180.251.168.165 | /ic_mahasiswa/tampilan_reg_mahasiswa |
| 2019-09-03 09:53:58 | @Irbadibrahim Asma | | 4 | Menampilkan form registrasi mahasiswa per semester | 180.251.168.165 | /ic_mahasiswa/reg_mhs_per_semester |
| 2019-09-03 09:53:59 | RISALDIN | | 0 | Melakukan login di halaman mahasiswa | 182.1.168.223 | /auth/login_mahasiswa |

Gambar 7. Hasil Pemeriksaan Log Aktifitas

Berdasarkan pemeriksaan yang telah dilakukan melalui database SIMAK maka dapat dianalisa sebagai berikut, pada *tb_reg_semester* terjadi penghapusan data mahasiswa, dimana data yang dihapus yaitu data mahasiswa dengan nomor pokok 201752067 yang terdaftar pada semester 20191. Waktu penghapusan data dilakukan pada tanggal 03-09-2019 pukul 09:53:40 dan dilakukan oleh name user @Irbadibrahim melalui IP 180.251.168.165.

3.4. Tahap Laporan Hasil Analisa

Dari hasil analisa dapat disimpulkan bahwa telah terjadi perubahan data dengan cara menghapus data pada database SIMAK. Adapun tabel yang mengalami perubahan yaitu *tb_reg_semester* dimana data yang dihapus adalah mahasiswa yang memiliki Nomor Pokok Mahasiswa 201752067 yang terdaftar pada semester 20191. Adapun data mahasiswa yang terhapus ditunjukkan pada gambar 8.



| No | TA | NIM | Nama Mahasiswa | Jurusan | Semester | Tanggal Registrasi |
|------|-------|-----------|----------------|-----------------|----------|-------------------------------|
| 101 | 20191 | 201752067 | JUMIATI | Sistem Komputer | 5 | 03 September 2019 02:37:29 |
| 722 | 20182 | 201752067 | JUMIATI | Sistem Komputer | 4 | 26 Februari 2019 02:20:41 |
| 1096 | 20181 | 201752067 | JUMIATI | Sistem Komputer | 3 | 25 Februari 2019 02:25:33 |
| 1576 | 20172 | 201752067 | JUMIATI | Sistem Komputer | 2 | 11/27/2020 23:46 |
| 1923 | 20171 | 201752067 | JUMIATI | Sistem Komputer | 1 | 5/8/2020 2 :46 |
| No | TA | NIM | Nama Mahasiswa | Jurusan | Semester | Tanggal Registrasi |

Gambar 8. Hasil Pemeriksaan Aplikasi SIMAK

Hasil dari pemeriksaan menggunakan tools *Log Helper* memberikan informasi perubahan data yang telah dilakukan melalui database SIMAK, sedangkan hasil pemeriksaan menggunakan Aplikasi SIMAK memberikan informasi dari hasil analisa pada gambar 8 yaitu data mahasiswa telah di input kembali pada tanggal 03 September 2019 pada pukul 02:37:29, dari hasil analisa tersebut bahwa perubahan yang dilakukan aplikasi akan menyimpan data *log* aktifitas pengguna sehingga didapat laporan data yang dihapus oleh pengguna.

4. Kesimpulan dan Saran

4.1 Kesimpulan

Dari hasil perekaman data yang dilakukan pada aplikasi SIMAK menggunakan tools *Log Helper* kemudian di simpan pada database yaitu di *tabel_log* dan selanjutnya dianalisa. Berdasarkan hasil analisa yang dilakukan maka didapatkan perubahan data pada salah satu tabel yaitu *tb_reg_semester* dengan menghapus salah data mahasiswa yang terdaftar pada semester 20191.

4.2 Saran

Dari kesimpulan yang telah di uraikan maka dapat di berikan saran sebagai berikut:

1. Saran yang bisa diberikan berdasarkan hasil analisa diharapkan pengelola aplikasi SIMAK agar membatasi akses bagi pengguna yang tidak memiliki hak akses pada fungsi-fungsi tertentu.
2. Saran kepada programmer aplikasi agar menutup celah terjadinya penyusupan yang dilakukan dengan cara menginjeksi *sintax* SQL agar *SQL Injection* tidak terjadi pada database.

Daftar Pustaka

- [1] I. Riadi, R. Umar, dan A. Firdonsyah, "Identification Of Digital Evidence On Android 's," vol. 15, no. 5, pp. 3–8, 2017.
- [2] Kalbande, D. & Jain, N. (2013). Comparative Digital Forensic Model. International Journal of Innovative Research in Science, Engineering and Technology(IJRSET), Vol. 2 No. 8, 3414-3419.
- [3] Martin S. Olivier. (2009, March), "On metadata context in Database Forensics, Digital Investigation", Elsevier, www.sciencedirect.com, Volume 5, Issues 3-4, Pages 115-123.

- [4] 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.
- [5] Riadi, I, Umar, R., Bernadisman, D., 2019. Analisis Forensik Database Menggunakan Metode Forensik Statis. *Jurnal Sistem Informasi Bisnis*.
- [6] Al-Azhar, M. N. (2012). *Digital Forensic Panduan Praktis Investigasi Komputer*. Jakarta: Penerbit Salemba Infotek.
- [7] Harmeet Kaur Khanuja and Dr. D. S. Adane (2011), “Database Security Threats and challenges in Database Forensic: A survey”, *Proceedings of 2011 International Conference on Advancements in Information Technology (AIT 2011)*.
- [8] Khanuja, H. K., & Adane, D. S. (2012). A framework for database forensic analysis. *Computer Science & Engineering: An International Journal (CSEIJ)*,2(3), 27-41.
- [9] Adedayo, O. M., & Olivier, M. S. (2015). Ideal log setting for database forensics reconstruction. *Digital Investigation*, 12(0), 27-40.
- [10] Riadi, I, Umar, R , Wasito., 2014. Analisis Forensik Serangan SQL Injection Menggunakan Metode Statis Forensik. *Volume 1 No.1*, 1-2.